NetScaler® Console service

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

Overview 64

- How NetScaler Console works 65
- Features and solutions 66

Release notes 70

- What's new 70
  - October 03, 2026 70
    - Management and Monitoring 70
  - September 27, 2026 71
    - Management and Monitoring 71
  - September 15, 2026 75
    - Fixed issues 75
  - September 01, 2026 75
    - What's new 75
    - Fixed issues 77
  - August 19, 2026 78
    - Management and Monitoring 78
  - August 04, 2026 79
    - What's new 79
    - Fixed issues 79
  - July 14, 2026 80
    - What's new 80
    - Fixed issues 81
  - June 30, 2026 82
    - Management and Monitoring 82
  - June 17, 2026 84
    - Fixed issues 84

© 1997–2026 Citrix Systems, Inc. All rights reserved.

June 03, 2026 85
Fixed issues 85
May 19, 2026 86
Management and Monitoring 86
Fixed issues 90
March 31, 2026 91
Management and Monitoring 91
Fixed issues 92
March 23, 2026 93
Management and Monitoring 93
March 09, 2026 94
What's new 94
Fixed Issues 95
February 20, 2026 96
What's new 96
Fixed Issues 96
February 04, 2026 97
Miscellaneous 98
Fixed Issues 99
November 11, 2025 100
Management and Monitoring 100
November 06, 2025 101
Fixed issues 101
October 15, 2025 101
Management and Monitoring 101
Fixed issues 102
September 17, 2025 102
Infrastructure 102

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues 103
September 08, 2025 104
Licensing 104
September 03, 2025 105
Fixed issues 105
August 26, 2025 105
Management and Monitoring 105
August 20, 2025 107
Infrastructure 107
Fixed issues 108
July 17, 2025 108
Infrastructure 108
Fixed issues 109
July 02, 2025 109
Telemetry 109
Security 110
Fixed issues 110
June 25, 2025 111
Management and Monitoring 111
June 17, 2025 111
Management and Monitoring 111
June 03, 2025 112
Fixed issues 112
May 26, 2025 113
Analytics 113
Fixed issues 114
May 06, 2025 114
Fixed issues 114

© 1997–2026 Citrix Systems, Inc. All rights reserved.

April 15, 2025 115
Zero-touch certificate deployment 115
Deprecation of autoscaling of NetScaler instances in public clouds 115
Improvements to Configuration Jobs 115
Improvements to Upgrade Jobs 115
Fixed issues 116
February 19, 2025 116
StyleBooks 116
Fixed issues 117
Analytics 117
February 06, 2025 117
Analytics 117
Infrastructure 117
Fixed issues 118
January 15, 2025 118
Telemetry 118
Analytics 118
Infrastructure 119
StyleBooks 119
Fixed issues 120
December 03, 2024 120
Sharing configuration entities between migrated configurations 120
Migrate analytics from policy-based to profile-based configuration 121
Fixed Issues 121
November 20, 2024 122
Enhanced user experience in NetScaler Console GUI 122
Option to delete SSL certificate from NetScaler 123
Fixed issues 123

© 1997–2026 Citrix Systems, Inc. All rights reserved.

November 12, 2024 123
Management and Monitoring 123
October 15, 2024 124
Telemetry 124
Analytics 125
Fixed issues 125
Infrastructure 125
October 03, 2024 125
Licensing 125
StyleBooks 126
Points to note 126
Fixed issues 126
September 19, 2024 127
Infrastructure 127
Fixed issues 127
September 03, 2024 128
Observability 128
Fixed issues 128
August 27, 2024 129
Analytics 129
Applications 129
StyleBooks 129
Fixed Issues 130
July 25, 2024 130
Fixed issues 130
July 15, 2024 131
Infrastructure 131
Licensing 131

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues 132
July 09, 2024 132
Support for identification and remediation of CVE-2024-5491 and CVE-2024-5492 132
June 18, 2024 133
Telemetry 133
June 11, 2024 133
Analytics 133
Infrastructure 135
Fixed Issues 135
June 5, 2024 136
Analytics 136
Platform 136
StyleBooks 136
Fixed Issues 137
Analytics 137
Infrastructure 137
StyleBooks 137
May 22, 2024 138
Analytics 138
Licensing 138
StyleBooks 139
Fixed issues 139
April 23, 2024 139
Analytics 139
Infrastructure 140
Fixed Issues 140
Infrastructure 140
Licensing 140

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Security 140
April 10, 2024 141
Analytics 141
Infrastructure 141
Fixed Issues 141
Infrastructure 141
Licensing 142
Security 142
March 26, 2024 142
Fixed Issues 142
March 12, 2024 143
Licensing 143
Fixed Issues 143
February 28, 2024 143
Infrastructure 143
Analytics 144
StyleBooks 145
Fixed Issues 146
February 06, 2024 146
Analytics 146
Infrastructure 146
Fixed Issues 147
January 24, 2024 148
Analytics 148
Infrastructure 148
Fixed Issues 148
January 16, 2024 149
Support for identification and remediation of CVE-2023-6548 and CVE-2023-6549 149

© 1997–2026 Citrix Systems, Inc. All rights reserved.

January 09, 2024 150

Analytics 150

Infrastructure 150

Fixed Issues 151

Licensing 151

Known issues 151

Licensing 151

Management and monitoring 152

Infrastructure 152

Data compliance 154

PCI DSS compliance 154

NetScaler® Application Delivery Management service PCI DSS compliance 154

NetScaler® telemetry program 156

Prerequisites 156

Data governance 159

NetScaler® telemetry program 159

How do we collect, store, and transmit data? 159

Data categories 160

Customer content 160

Logs 160

Detailed customer content and logs 161

Security 163

Data retention policy for NetScaler Console Service 163

Third-party services 164

References 164

CONDITIONS FOR USE OF IoC INFORMATION 165

Getting started 166

Step 1: Sign Up for Citrix Cloud™ 166

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 2: Manage NetScaler Console with an Express account 166
Step 3: Select a NetScaler deployment type 167
Install an agent on a hypervisor 168
Install an external VM agent on public cloud 169
Install an agent as a microservice 169
Use the built-in agent 170
Add instances 170
Onboard NetScaler instances by using the NetScaler Console GUI dashboard 171
Agent actions 172
View agent diagnostics and receive alerts for endpoint verification 173
Email notification 174
Configure the built-in agent to manage instances 174
Prerequisites 175
Configure the built-in agent 176
Configure license server through NetScaler® built-in agent 179
Troubleshooting 179
Install a NetScaler agent on-premises 180
Install a NetScaler agent on Microsoft Azure cloud 182
Prerequisites 183
Install a NetScaler agent on Amazon Web Services (AWS) 193
Prerequisites 193
Launch from a Website 196
Launch with EC2 199
Install a NetScaler agent on GCP 212
Prerequisites 212
Install the NetScaler agent on GCP 212
Install NetScaler agent in Kubernetes cluster using YAML 216
Install a NetScaler agent operator using the OpenShift console 217

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prerequisites 217
Install the Agent Operator 220
Delete an agent instance 223
Uninstall the agent operator 223
Install a container-based agent using helm chart 224
How to Get Help and Support 224
Create a Citrix Cloud account 224
Sign in to your account 225
Change your password 225
Citrix Cloud support forums 226
Support articles and documentation 226
Citrix Cloud Resource Center 226
Citrix Tech Zone 227
Technical Support 227
Service Health Dashboard 228
Service health subscriptions 231
Enhanced Graphical User Interface 234
Hover-to-Display menu 234
Streamlined menu hierarchy 235
Updated submenu labels 235
Infrastructure > Configuration 235
NetScaler Licensing > Pooled Licensing 236
Gateway > HDX Insight 237
Settings 237
Collapsible menu 238
Expanded menu 238
Collapsed menu 238
Sidebar Toggle 238

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Show sidebar 239
Hide sidebar 239
Set as home screen 239
Pin favorite items 240
Low-touch onboarding of NetScaler instances using Console Advisory Connect 241
Overview: components of NetScaler Console onboarding workflow 241
A quick tour of onboarding 243
Onboard NetScaler instances using Console Advisory Connect 244
Step 1: Get started 244
Step 2: Insights on your NetScaler and Gateway instances 247
Step 3: Select NetScaler and Gateway instances to onboard 252
Step 4: Onboard NetScaler instances to NetScaler Console 254
Onboard NetScaler instances using a built-in agent 255
Onboard NetScaler instances using an external agent 258
Install an agent on a public cloud 262
Test onboarding readiness of NetScaler instances 262
Email Settings 264
Configure Email Settings 264
Enable emails for all admins 266
Enable / disable emails for specific admins in the org 266
Disable emails for all admins 268
Troubleshoot issues using the diagnostic tool or the NetScaler Console GUI 269
Manually use the diagnostic tool 269
Validate the NetScaler instance readiness for onboarding using the diagnostic tool 271
View NetScaler diagnostic information in NetScaler Console GUI 271
Troubleshoot 272
Invalid user name or password 273
DNS configuration error 273

© 1997–2026 Citrix Systems, Inc. All rights reserved.

No internet connection 274
No connection to NetScaler Console endpoint 274
Built-in agent dry run timeout 274
Red outline on the device profile dropdown 275
Transition from a built-in agent to an external agent 276
Before you start 276
Transition from a built-in agent to an external agent 276
Connect SAML as an identity provider to NetScaler Console 278
Prerequisites 278
Cloud Connectors 278
Active Directory 279
SAML SSO configuration 279
System requirements 292
Supported browsers 292
Agent installation requirements 292
Lightweight agent for pooled or flexed licensing 294
Supported ports 295
Ports for the NetScaler agent 295
Ports for NetScaler instances 297
Ports for NetScaler Built-in agent 298
Requirements for NetScaler Console Analytics solution 299
Minimum Citrix Virtual Apps and Desktops versions required 299
Thin clients supported for HDX™ Insight 299
NetScaler instance license required for HDX Insight 300
Supported operating systems and Citrix Workspace versions 300
Licenses 301
NetScaler licensing required for NetScaler Console features 301
View expiry checks for virtual server subscriptions 303

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View the type of analytics enabled on the virtual servers 303
Upgrade Advisory 305
View upgrade advisory 306
Set the preferred builds 308
Upgrade NetScaler instances 309
Security Advisory 313
Security advisory landing page 313
Secure Configuration Recommendations 315
CVE Detection 315
File Integrity Monitoring 315
Scan Now 315
Scan History 316
NetScalers impacted 317
Settings 318
Secure configuration recommendations 320
Severity-based prioritization 320
Benefits of a detailed instance-level view 321
Remediate configuration recommendations 322
CVE Detection 326
Instance view 328
CVE view 330
CVE repository 330
Points to note 331
File integrity monitoring 333
Console-Detected 334
Points to note 335
Device-Reported 336
Indicators of Compromise detection in NetScaler Console 336

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prerequisites 337
Benefits 337
Remediate vulnerabilities 338
Identify and remediate vulnerabilities for CVE-2026-88779 340
Remediate CVE-2026-88779 340
Remediate vulnerabilities for CVE-2026-88778 341
Remediate CVE-2026-88778 341
Step 1: Upgrade the vulnerable NetScaler instances 342
Step 2: Apply configuration commands 342
Step 2: Select the instance 343
Identify and remediate vulnerabilities for CVE-2026-88777 344
Remediate CVE-2026-88777 344
Identify and remediate vulnerabilities for CVE-2026-88776 345
Remediate CVE-2026-88776 345
Identify and remediate vulnerabilities for CVE-2026-88775 346
Remediate CVE-2026-88775 346
Identify and remediate vulnerabilities for CVE-2026-88774 347
Remediate CVE-2026-88774 347
Identify and remediate vulnerabilities for CVE-2026-88773 348
Remediate CVE-2026-88773 348
Identify and remediate vulnerabilities for CVE-2026-88772 349
Remediate CVE-2026-88772 349
Identify and remediate vulnerabilities for CVE-2026-88771 350
Remediate CVE-2026-88771 350
Identify and remediate vulnerabilities for CVE-2026-19490 351
Remediate CVE-2026-19490 351
Identify and remediate vulnerabilities for CVE-2026-19489 352
Remediate CVE-2026-19489 352

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Identify and remediate vulnerabilities for CVE-2026-13474 353
Remediate CVE-2026-13474 353
Step 1: Upgrade the impacted NetScaler instances 354
Step 2: Apply configuration commands 354
Identify and remediate vulnerabilities for CVE-2026-10817 357
Remediate CVE-2026-10817 357
Identify and remediate vulnerabilities for CVE-2026-10816 358
Remediate CVE-2026-10816 358
Identify and remediate vulnerabilities for CVE-2026-8655 359
Remediate CVE-2026-8655 359
Identify and remediate vulnerabilities for CVE-2026-8452 360
Remediate CVE-2026-8452 360
Identify and remediate vulnerabilities for CVE-2026-8451 361
Remediate CVE-2026-8451 361
Identify and remediate vulnerabilities for CVE-2026-4368 362
Remediate CVE-2026-4368 362
Identify and remediate vulnerabilities for CVE-2026-3055 363
Remediate CVE-2026-3055 363
Identify and remediate vulnerabilities for CVE-2025-12101 364
Remediate CVE-2025-12101 365
Identify and remediate vulnerabilities for CVE-2025-8424 365
Remediate CVE-2025-8424 366
Identify and remediate vulnerabilities for CVE-2025-7776 367
Remediate CVE-2025-7776 368
Identify and remediate vulnerabilities for CVE-2025-7775 368
Remediate CVE-2025-7775 369
Identify and remediate vulnerabilities for CVE-2025-6543 370
Remediate CVE-2025-6543 371

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Identify and remediate vulnerabilities for CVE-2025-5349 372
Remediate CVE-2025-5349 373
Remediate vulnerabilities for CVE-2025-5777 374
Remediate CVE-2025-5777 375
Step 1: Upgrade the vulnerable NetScaler instances 376
Step 2: Apply configuration commands 376
Step 2: Select the instance 377
Remediate vulnerabilities for CVE-2024-8535 378
Remediate CVE-2024-8535 379
Step 1: Upgrade the vulnerable NetScaler instances 380
Step 2: Apply configuration commands 380
Step 2: Select the instance 381
Remediate vulnerabilities for CVE-2020-8300 383
Remediate CVE-2020-8300 384
Step 1: Upgrade the vulnerable NetScaler instances 385
Step 2: Apply configuration commands 386
Step 2: Select the instance 389
Points to note for NetScaler Console Express account 392
Scenario 393
Remediate vulnerabilities for CVE-2021-22927 and CVE-2021-22920 397
Remediate CVE-2021-22927 and CVE-2021-22920 399
Step 1: Upgrade the vulnerable NetScaler instances 400
Step 2: Apply configuration commands 401
Step 2: Select the instance 404
Scenario 406
Identify and remediate vulnerabilities for CVE-2021-22956 409
Identify CVE-2021-22956 impacted instances 410
Remediate CVE-2021-22956 411

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 1: Upgrade the vulnerable NetScaler instances 412
Step 2: Apply configuration commands 412
Step 2: Select the instance 413
Identify and remediate vulnerabilities for CVE-2022-27509 416
Identify CVE-2022-27509 impacted instances 417
Remediate CVE-2022-27509 417
Unsupported CVEs in Security Advisory 418
Setting up 419
Adding multiple agents 419
Configure agents for multisite deployment 421
Architecture 422
Agent failover 423
Configuring agent upgrade settings 424
Upgrade agent manually 425
Dual NIC support on NetScaler Console 426
Adding instances 429
How to create a NetScaler® profile 430
To add a NetScaler instance to NetScaler Console 434
To add NetScaler CPX instance in NetScaler Console 435
To add a standalone NetScaler BLX instance in NetScaler Console 436
To add high-availability NetScaler BLX instances in NetScaler Console 438
To access an instance GUI from the NetScaler Console 439
Resolve instance warnings 440
Configuring syslog on instances 440
Logstream overview 442
Enable Logstream as Transport Mode 443
How to assign more permissions to delegated admin users 445
Assigning Super Admin Permissions to a Delegated Admin 445

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Assigning Custom Role to a Delegated Admin 446
Integration with the ServiceNow instance 450
Generate ServiceNow incidents for any NetScaler events 451
Generate ServiceNow incidents for SSL certificates that are about to expire 451
Generate ServiceNow incidents for NetScaler Console license expiry 452
Customize NetScaler Console event policies 452
Actionable tasks and recommendations 453
Tasks 456
Recommendations 462
How to use the Guide me workflow and complete the recommendation? 465
Configure notifications 465
FAQs 466
A unified dashboard to view instance key metric details 468
Applications 468
NetScaler Infrastructure 469
Application Security 470
Gateway 471
API Analytics 472
Customize dashboard 472
View agent details 474
Create and apply filters 475
Edit filters 477
Create custom dashboards to view instance key metric details 478
More options in the dashboard 481
Share dashboard to other users 483
API Security 484
Benefits of API Security 485
Grant API Security configuration and management permissions 485

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create or upload an API definition 487
Upload the OAS specification 487
Create an API definition 488
View API definitions 489
Deploy an API instance 489
Add an API proxy 489
Deploy an API instance using the API proxy 491
Enable the API analytics 493
Add policies to an API deployment 494
Policy types 496
Authentication and Authorization 497
Rate limit 499
WAF 500
Bot 500
Header Rewrite 500
URI Path Rewrite 501
Deny 501
View API analytics 502
API endpoint distribution 502
API instances 503
API endpoints 504
Authentication failures 504
View different API insights 505
View top API endpoints in an instance 506
View most accessed APIs 507
View geo-location of an endpoint 508
View HTTPS response status 509
View API requests trend 509

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View bandwidth consumption of an endpoint 510
View SSL errors and usage 511
Discover API endpoints 512
View API endpoints 513
Create API definitions from discovered API endpoints 514
Update an existing API definition with discovered API endpoints 516
Undeploy an API instance 517
Undeploy an API policy 517
Undeploy an API deployment 517
Undeploy an API proxy 518
Use APIs to manage API Security 518
API examples for policy types 520
Rate limit 520
OAuth 522
Basic authentication 523
No authentication 524
Bot 525
WAF 526
Header Rewrite 526
URI Path Rewrite 527
Authorization 530
Deny 531
Create WAF and BOT profiles using StyleBooks 532
Create a WAF profile using StyleBooks 532
Create a BOT profile using the StyleBook 533
Applications 535
Prerequisites 535
Application overview 535

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Discrete applications 535
Custom applications 536
Points to note 536
Microservices applications 536
Application management and application dashboard 536
Manage applications 536
Application dashboard 537
Sort data on dashboard columns 537
Updates in the new dashboard behavior compared to the earlier dashboard 538
Manage applications 539
View application details 539
Add an application 540
Create an application using the StyleBook 543
Edit or delete an application 543
Export reports of app dashboard and security dashboard 543
View applications 544
View microservices applications 545
Configure and associate an application to multiple custom applications 547
Application dashboard overview 549
Search and filter results using the search bar 552
Save filter 552
Create and apply tags to applications 554
Application details 556
Check monitor status of an application 561
Select App Score components and set thresholds 562
Application details for microservices applications 566
Intelligent App Analytics 571
Configure Intelligent App Analytics 572

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Performance indicators for application analytics 574
Response time 575
Active services 575
Average CPU usage 576
Average application CPU usage 577
Memory usage 577
NIC discards 578
Service flaps 579
Low session reuse 580
Improper persistence type 581
Unstable Server 582
SSL Real Time Traffic 584
Unusually Large HTTP packets 584
TCP reassembly queue limit hits 585
Surge Queue Buildup 586
SSL rating 587
Troubleshoot App Dashboard 588
Troubleshooting scenario 589
Application is licensed 589
Metrics collector is enabled 590
NetScaler instance earlier than 47.x builds 592
NetScaler instance later than 47.x builds 593
Application usage and anomalies 597
Peak and lean usage analytics 600
Assess app scale limits 600
Identify top 5 app maintenance window 601
Application usage analytics 604
View metrics details in graphical format 614

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Automate SSL certificate management 618
Configure a Venafi server on NetScaler Console 618
Manage SSL certificate lifecycle 620
A+ SSL rating analytics 624
Upgrade to A+ SSL rating 625
Roll back SSL rating 626
Determine the impact of SSL-rating on the application traffic 628
Web Insight dashboard 629
View details for cipher related issues 632
Integrated cache requests 634
Other use case 636
Analyze the root cause for application slowness 637
Application drill-down 638
Response Time 639
Service Graph 642
Service graph for applications across all NetScaler instances 642
Service graph for Kubernetes applications 643
Service graph for 3-tier Web applications 643
Service graph for Kubernetes apps 645
Service Graph - Simplified onboarding 645
Automatically deploying an agent as a Kubernetes job 645
Manually configuring service graph 651
Setting up service graph 659
Software requirements 659
Single tier or Unified ingress topology 660
Dual tier or Service Mesh Lite topology 660
Service mesh topology 661
View details in service graph 662

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service graph dashboard 663
View key metrics trends using the tabular view 666
View Pxx value for the service response time 666
View service details 667
View client metrics 668
View TCP and SSL metrics 670
Apply filters 672
Settings option 674
Analyze the errors 675
View HTTP transaction details 676
Configure thresholds in service graph 678
Single threshold 679
Double threshold 680
View service details 680
Metrics details 683
View backend pod details 683
Monitor services using the golden signal metrics 684
View ingress details for troubleshooting issues 687
Distributed tracing 692
Prerequisites 693
View service trace details 698
View the transaction details 699
View diagnostic details for partial or no data in service graph 702
Diagnostics for no data 703
Diagnostics for partial data 703
Troubleshooting 704
Service graph for 3-tier web applications 705
Application view 705

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Network functions view 706
Service graph view for no active transactions 708
Analyze metrics 708
Client metrics 708
Network function metrics 709
Service metrics 710
NetScaler metrics (only for GSLB applications) 710
Holistic view of all applications in service graph 712
View client metrics 713
View NetScaler details 713
View discrete applications 715
View microservice applications 718
Search bar to filter results 720
StyleBooks 722
StyleBook categories 724
Default and custom StyleBooks 724
Public and private StyleBooks 724
Example of a StyleBook marked as private 725
View StyleBooks 725
Download custom StyleBooks 727
Update custom StyleBook 728
Delete custom StyleBooks 729
View StyleBook dependencies 729
To view StyleBook dependencies 730
Forward dependencies 730
Reverse dependencies 730
Audit NetScaler configuration against config packs 731
Download the support bundle of a config pack 732

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a tag for the StyleBook 733
Clone a StyleBook 735
Import and synchronize StyleBooks from an external repository 736
Add a repository 739
Repository options 742
Steps to import StyleBooks and config packs from GitHub/GitLab 743
Use default StyleBooks 743
NetScaler features 743
Web Application Firewall features 745
Application Security features 746
Bot management features 747
NetScaler network configurations 747
What's next? 749
Web application firewall StyleBook 749
Deploying application firewall configurations 749
SNMP configuration StyleBook 761
NetScaler network configurations StyleBook 773
Deploy basic networking components 773
Deploy advanced networking components 775
Prometheus analytics StyleBook 778
Prerequisite 778
Migrate NetScaler application configuration using StyleBooks Configuration Builder 779
Sharing configuration entities between migrated configurations 780
Supported NetScaler Features 781
Create a StyleBook to migrate the NetScaler application configuration 781
Limitations 784
Business application StyleBooks 784
SSO Google Apps StyleBook 785

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To deploy SSO Google apps StyleBook 786
SSO Office 365 StyleBook 789
To deploy SSO Microsoft Office 365 StyleBook 790
Microsoft Skype for Business StyleBook 799
Configuring NetScaler instances in an enterprise 801
Microsoft Exchange StyleBook 808
NetScaler features configured by using Microsoft Exchange StyleBook 808
Prerequisites 809
Configuring Microsoft Exchange StyleBook 809
To configure Microsoft Exchange application 809
Microsoft SharePoint StyleBook 811
Prerequisites 812
Microsoft ADFS proxy StyleBook 822
Benefits of using NetScaler as ADFS proxy 822
Oracle e-business StyleBook 843
To create a configuration for Oracle E-Business Suite 12.2 843
Create and use custom StyleBooks 845
Before you begin 845
Anatomy of a StyleBook 846
Create and edit a configuration pack 847
Create a configuration pack 848
Reuse configurations created outside of StyleBooks and share configurations between ConfigPacks 849
Change the StyleBook of a configuration pack 850
Export or import config packs 854
Save a config pack as a draft 857
Create a schedule for a config pack 859
Detach a target instance from a configuration pack 861

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Build your StyleBooks 862
StyleBook to create a load balancing virtual server 866
Header 866
Components 871
Build your StyleBook 873
StyleBook to create a basic load balancing configuration 876
Header 876
Components 879
Outputs 883
Build your StyleBook 884
Create a composite StyleBook 889
Build your StyleBook 889
Use GUI attributes in a custom StyleBook 893
Add a label with tooltip for parameters 893
Set a collapsible pane for the parameter 894
Set the user options as radio buttons 895
Import custom StyleBooks 896
Use HTML formatting tags in the StyleBook description and header 897
To import your StyleBook 898
Create a StyleBook to upload files 903
StyleBook configuration 903
Build your StyleBook - 1 903
Build your StyleBook - 2 905
Creating configurations to upload files 907
Create a StyleBook to upload SSL certificate and certificate key files 908
StyleBook configuration 908
Creating configurations to upload SSL files 912
Build your StyleBook 913

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Manage SSL certificates from the certificate store using StyleBooks 917
Parameters 918
Components 919
Build your StyleBook 919
Enable analytics and configure alarms on a virtual server defined in a StyleBook 924
Instance roles 926
Target-roles section 926
Role "default" 927
Components with roles 927
Build your StyleBook 931
Using APIs 936
Create a StyleBook to perform non-CRUD operations 938
Supporting the non-CRUD operations 938
Deploying GSLB configurations using DNS domain names 940
Workflow for the admins 941
NetScaler Console REST API for admin workflow 948
Workflow for the application owners 983
NetScaler Console REST API for app owner workflow 985
Build your StyleBook 989
Allow special characters with their literal form in StyleBook 999
Concatenate multiple verbatim strings 1001
Manage data sources 1002
Use a NetScaler instance as the data source 1003
Using the built-in data source without collection 1003
Using the built-in data source with collection 1007
Use target NetScaler instances as data sources 1014
Example StyleBook to use the target NetScaler instance as a data source 1015
Use custom data sources 1017

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Add a data source type 1018
Add a collection schema under data source type 1019
Add a data source 1019
Add a collection data 1020
Use custom data source without collection 1021
Use custom data sources with collection 1023
Use APIs to create configurations from StyleBooks 1026
Example 1 1027
Example 2 1030
Example 3 1033
Example 4 1035
Updating a configuration 1037
Deleting a configuration 1039
Use APIs to create configurations 1040
Use APIs to create configurations to upload any file type 1044
Use APIs to import custom StyleBooks 1045
Use API to update a custom StyleBook 1049
Use APIs to download custom StyleBooks 1050
Use APIs to download dependent StyleBooks and specify compression type 1050
Use API to delete custom StyleBooks 1051
Use APIs to update an existing config pack 1051
Use APIs to update target instances 1058
Use API to config audit 1061
Use API to export a config pack 1061
Use APIs to upgrade the configuration pack to a new StyleBook 1062
Use API to detach a target instance from a config pack 1063
Use API to forcefully delete a NetScaler instance from the config pack 1064
Use APIs to delete config packs 1065

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBooks grammar 1069
Header 1070
Import StyleBooks 1073
Parameters 1074
'name' 1074
'label' 1075
'description' 1075
'type' 1075
'network' 1077
'dynamic-allocation' 1077
'key' 1078
'required' 1079
'allowed-values' 1079
'allow-new-values' 1081
'default' 1082
'pattern' 1083
'min-value' 1083
'max-value' 1084
'min-length' 1084
'max-length' 1085
'min-items' 1085
'max-items' 1086
'gui' 1086
'columns' 1086
'updatable' 1086
'collapse_pane' 1087
'layout' 1092
'dependent-parameters' 1093

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`is_policy_expression` 1095
Parameters-default-sources construct 1096
Parameters-source construct 1104
Parameter conditions 1105
'show' or 'hide' 1106
'set-default' 1106
'set-required' 1107
'set-allowed-values' 1108
'set-label' 1111
'set-description' 1112
'collapse-pane' or 'expand-pane' 1112
'set-pattern' 1113
Nested parameter conditions 1113
Substitutions 1114
Substitution map 1127
Iterate through substitution lists 1128
Components 1131
Helper components 1134
Optional properties 1137
Properties-default-sources construct 1141
Computation of the Properties of the Component 1144
Nested components 1144
Condition construct 1148
Repeat construct 1150
Repeat-condition construct 1155
Nested repeats 1156
Outputs 1160
Parameter reference 1162

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Parent reference 1165
Components reference 1168
Substitutions reference 1172
Variable reference 1172
Operations 1174
Analytics 1181
Target virtual servers and insight types 1185
Alarms 1185
Expressions 1190
Arithmetic expressions 1190
String expressions 1190
List expressions 1191
Relational expressions 1191
Logical expressions - boolean 1192
Splat expressions 1192
Verbatim string expressions 1193
Target expressions 1194
Expression Type Validation 1194
In-place interpolations 1200
Allowed Types Inside Interpolations 1201
Simple interpolations 1202
Automatic type conversions 1202
Sequential interpolations 1202
Nested interpolations 1203
Interpolations with `quotewrap` 1203
Built-in functions 1204
str() 1204
int() 1204

© 1997–2026 Citrix Systems, Inc. All rights reserved.

bool() 1205
len() 1205
min() 1205
max() 1206
bin() 1206
oct() 1207
hex() 1207
lower() 1207
upper() 1207
sum() 1207
pow() 1208
ip() 1208
ip_network() 1209
network_ip() 1209
subnets() 1209
netmask_ip() 1209
is_netmask_ip() 1210
broadcast_ip() 1210
cidr() 1210
is_cidr() 1210
is_in_network() 1211
base64.encode() 1211
base64.decode() 1211
exists() 1211
filter() 1212
if-then-else() 1212
join() 1213
split() 1214

© 1997–2026 Citrix Systems, Inc. All rights reserved.

map() 1214
quotewrap() 1215
replace() 1215
trim() 1216
truncate() 1216
distinct() 1217
url.encode() 1217
url.decode() 1217
is-ipv4() 1217
is-ipv6() 1217
startswith() 1218
endswith() 1218
contains() 1218
substring() 1219
match() 1220
sha256() 1220
relate() 1222
multiple() 1225
reverse() 1225
Dependency detection 1226
Cyclic Dependencies 1229
Security 1232
Application Security Dashboard 1232
Threat index details 1233
Safety index details 1235
Unified Security dashboard 1236
Secured applications 1237
Configure protections for unsecured applications 1237

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View application security violation details 1246
Setting up 1247
Enable Web Transaction settings 1247
Application overview 1248
Violation categories 1250
View WAF violation details 1251
View bot violation details 1254
View events history 1258
Signature auto update 1258
All Violations 1259
Violation categories 1259
Security violations dashboard 1261
Violation details 1262
WAF learning 1262
Get started 1263
WAF recommendations 1265
Prerequisites 1266
Configure the WAF scan settings 1267
WAF scan recommendation process 1270
View scan report 1270
Gateway 1274
Gateway Insight 1274
Enable Gateway Insight 1276
Enable AppFlow for a virtual server in NetScaler Console 1276
Enable AppFlow user name logging on an NetScaler Gateway appliance by using the GUI 1276
View Gateway Insight reports 1277
View EPA, SSO, authentication, authorization, and application launch failures 1277
View summary of session modes, clients, and the number of users 1278

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Users 1278

View user details 1279

Search bar and Geo map view 1282

Applications 1282

View application details 1283

Gateways 1283

View gateway details 1284

Exporting reports 1285

Export a report 1285

Gateway Insight Use Cases 1286

1. User is not able to log on to the NetScaler Gateway appliance or to the internal web servers 1286

Authentication Failures 1286

View the authentication failure details 1286

EPA Failures 1287

View EPA failure details 1288

SSO Failures 1289

View SSO failure details 1289

View application launch failure details 1290

View total bytes and bandwidth consumed by an application 1291

View user access for resources 1292

View summary of session modes, type of clients, and number of users logged on 1293

Troubleshoot Gateway Insight issues 1293

Gateway Insight configuration checklist 1294

Connectivity between NetScaler and NetScaler Console checklist 1294

Record generation in NetScaler checklist 1294

Validations in NetScaler Console 1295

Gateway Insight stats 1295

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Contact Citrix technical support 1295
Known Issues 1296
HDX™ Insight 1296
Identifying the root cause of slow performance issues 1298
Scenario 1 1298
Scenario 2 1300
Geo map for HDX Insight 1302
Create a private IP block 1302
Use Case 1305
Limitations 1306
Enable HDX™ Insight data collection 1307
Enable data collection for NetScaler Gateway appliances deployed in single-hop mode 1307
Enable data collection to monitor NetScalers deployed in transparent mode 1309
Enable data collection for NetScaler Gateway appliances deployed in double-hop mode 1312
Enable data collection to monitor NetScalers deployed in LAN user mode 1317
Create thresholds and configure alerts for HDX™ Insight 1321
Example Use Cases 1322
View HDX™ Insight reports and metrics 1327
Application View Reports and Metrics 1327
Desktop View Reports and Metrics 1336
User View Reports and Metrics 1349
Instance View Reports and Metrics 1366
License View Reports and Metrics 1373
Troubleshoot HDX™ Insight issues 1374
HDX Insight configuration checklist 1374
Connectivity between NetScaler and NetScaler Console checklist 1375
Record generation for HDX/ICA traffic in NetScaler checklist 1375
Error counters 1384

© 1997–2026 Citrix Systems, Inc. All rights reserved.

nstrace validation 1388
Population of records in NetScaler Console checklist 1388
Before contacting Citrix technical support 1388
Known Issues 1389
Metrics information for thresholds 1389
Web 1389
Security 1392
APPANALYTICS 1392
HDX™ 1393
Infrastructure 1394
Infrastructure Analytics 1394
Infrastructure Analytics in NetScaler Console 1395
Instance score 1395
Health indicators explained 1395
View NetScaler Capacity issues 1397
Value of health indicators 1398
Infrastructure analytics dashboard 1399
Circle pack view 1399
Instance circles 1400
Grouped instance circles 1401
Clustered instance circles 1402
How to use Circle Pack 1405
Tabular view 1407
Search bar 1407
How to use the Summary Panel 1408
Instance info 1410
Traffic profile 1411
How to use the settings panel 1412

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View 1412
Select metrics and customize weightage for instance score calculation 1413
Configure notifications 1414
How to visualize data on the dashboard 1415
View instance details in Infrastructure Analytics 1416
View the capacity issues in an NetScaler instance 1424
View recommended actions to solve capacity issues 1425
Enhanced Infrastructure Analytics with new indicators 1427
Tabular view 1429
View details of an anomaly 1430
Instance management 1430
Add an instance 1431
How to use the instance dashboard 1431
How to monitor globally distributed sites 1432
Monitoring globally distributed sites in NetScaler Console 1432
Use case 1433
Configuring Geomaps 1435
How to create tags and assign to instances 1441
How to search instances using values of tags and properties 1444
To search for NetScaler VPX instances 1445
Centralized GeoIP DB Updates through NetScaler® Console 1447
Limitations 1448
Configuring centralized GeoIP DB Updates through NetScaler Console 1448
Manage admin partitions of NetScaler instances 1451
View admin partitions 1451
View the revision history difference 1452
View the template vs running difference 1455
Back up and restore NetScaler instances 1456

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a backup for a selected NetScaler instance by using NetScaler Console 1457
Transfer a backup file to an external system 1458
Restore a NetScaler instance by using NetScaler Console 1460
Export the report of this dashboard 1462
Force a failover to the secondary NetScaler instance 1462
Force a secondary NetScaler instance to stay secondary 1463
Create instance groups 1464
To create an instance group using NetScaler Console 1464
To identify and add unmapped instances to a group 1464
Global Server Load Balancing site groups 1465
Create a GSLB site group 1465
Create SNMP managers and users for NetScaler agent 1466
Add an SNMP v2 manager 1466
Add an SNMP v3 manager 1467
Add an SNMP user 1468
Managing SNMP views 1472
Provision NetScaler VPX instances on SDX 1472
Step 1 - Add a VPX instance 1473
Step 2 - Allocate licenses 1474
Step 3 - Allocate resources 1475
Step 4 - Add instance administration 1476
Step 5 - Specify network settings 1477
Step 6 - Specify Management VLAN settings 1479
View the provisioned VPX instance 1480
Rediscover multiple NetScaler instances 1480
Polling overview 1481
How NetScaler Console polls managed instances and entities 1481
Different ways of polling instances 1486

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unmanage an instance 1488
Trace the route to an instance 1489
View NetScaler-owned IP addresses 1489
Export NetScaler-owned IP addresses 1490
Schedule the export of NetScaler-owned IP addresses 1491
How to change the NetScaler MPX or VPX root password 1494
Change password using the Configuration Jobs feature 1494
How to change a NetScaler SDX nsroot password 1498
Change password 1499
How to generate a technical support bundle for a NetScaler® instance 1501
Events 1504
Use events dashboard 1505
Create event rules 1507
Configure an event rule 1509
Step 1 - Specify name and instance family 1509
Step 2 - Configure event age 1509
Step 3 - Choose severity of event 1510
Step 4 - Specify event category 1511
Step 5 - Specify NetScaler instances 1512
Step 6 - Select failure objects 1512
Step 7 - Specify advanced filters 1513
Step 8 - Add event rule actions 1514
Schedule an event filter 1524
Modify the reported severity of events that occur on NetScaler instances 1524
View events summary 1525
Event messages 1527
Display event severities and SNMP trap details 1527
View and Export syslog messages 1531

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View syslog messages 1531
Search syslog messages 1531
Export syslog messages 1533
Suppress syslog messages 1535
Suppressing syslog messages by creating filters 1535
Disabling the filter 1538
SSL dashboard 1538
Automated certificate renewal by using the ACME protocol 1539
ACME support in NetScaler® Console 1540
Configuration steps for ACME integration 1542
Issuance and renewals 1552
Issue a certificate 1554
Third-party Integration 1558
Limitations 1560
Troubleshoot issues related to automatic certificate renewal 1560
Zero-touch certificate management 1561
Upload certificates 1562
Enable zero-touch certificate management 1563
SSL filter mode support 1565
Use the SSL dashboard 1568
Monitor SSL certificates 1568
View audit logs for SSL certificates 1571
Exclude default NetScaler certificates on the SSL Dashboard 1572
Download SSL certificates 1573
To delete the SSL certificate on the SSL dashboard 1575
View SSL certificate chain 1576
Set up notifications for SSL certificate expiry 1577
Update an installed certificate 1578

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Install SSL certificates on a NetScaler instance 1581
Create a Certificate Signing Request (CSR) 1582
Link and unlink SSL certificates 1584
Configure an enterprise policy 1585
Poll SSL certificates from NetScaler instances 1586
Use the NetScaler Console certificate store to manage SSL certificates 1587
Add SSL certificates to the certificate store 1587
Update SSL certificates in the certificate store 1587
Delete SSL certificates from the certificate store 1588
Install SSL certificates on NetScaler® instances 1588
Import certificates from NetScaler instances 1588
Update server certificates without intermediate uploads 1589
Configuration jobs 1590
Configuration Template 1591
Instance 1591
File 1592
Record and Play 1592
Export the report of this dashboard 1592
Related Articles 1592
Create a configuration job 1593
Use record-and-play to create configuration jobs 1597
Use configuration jobs to replicate configuration from one instance to multiple instances 1600
Use variables in configuration jobs 1602
Create configuration jobs from corrective commands 1606
Replicate running and saved configuration from one NetScaler instance to another 1608
Reuse run configuration jobs 1610
Use SCP (put) command in configuration jobs 1611
Use configuration templates 1614

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use the master configuration template 1614
Schedule jobs created by using built in templates 1622
Schedule a job for configuring export of metrics from NetScaler to Prometheus 1624
Use configuration templates to create audit templates 1628
Reschedule jobs configured by using built in templates 1630
Reuse configuration audit templates in configuration jobs 1631
Import and export configuration templates 1634
Configuration audit 1636
Create audit templates 1637
Poll configuration audit of NetScaler instances 1642
View audit reports 1643
Generate configuration audit diff for ConfigChange SNMP Traps 1649
Audit configuration changes across instances 1650
Get configuration advice on network configuration 1655
Upgrade jobs 1658
Pre-upgrade validation 1659
Schedule upgrading of NetScaler instances 1660
Schedule upgrading of NetScaler SDX instances 1664
Schedule upgrading of NetScaler BLX instances 1665
Schedule upgrading Autoscale™ group 1668
Schedule configuring HA pair of NetScaler instances 1668
Schedule converting HA pair of instances to cluster 1670
Use jobs to upgrade NetScaler instances 1671
Prerequisites 1671
Upgrade considerations for customized NetScaler configurations 1672
NetScaler high-availability pair 1672
NetScaler clusters 1673
Create a NetScaler upgrade job 1673

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pause or resume a scheduled upgrade job 1681
Retry failed upgrade jobs 1682
Clean up the NetScaler disk space 1684
Use custom scripts 1685
NetScaler upgrade options 1687
Scheduling upgrade jobs for a NetScaler high-availability pair 1688
Download a consolidated diff report of a NetScaler upgrade job 1689
Network functions 1690
Generate reports for load balancing entities 1690
Generate a combined load balancing report 1691
Generate an individual load balancing entity report 1693
Export or schedule export of network functions reports 1693
Network reporting 1695
Network reporting dashboard 1696
View network reporting data by applying aggregations 1699
Exporting network reports 1700
How to manage Thresholds for Network Reports on NetScaler Console 1703
Set Performance Polling Interval for Network Reports 1705
Configuring Network Reporting Prune Settings 1705
Provisioning 1706
App-based provisioning in AWS 1706
Prerequisites 1707
Cloud access profile 1708
App environment 1708
Application delivery 1708
FAQs 1709
App-based provisioning in Azure 1713
Prerequisites 1713

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cloud access profile 1714
App environment 1714
Application delivery 1715
FAQs 1715
Provisioning NetScaler VPX instances 1718
Provisioning NetScaler VPX Instances on AWS 1718
Provisioning NetScaler VPX instances on Microsoft Azure 1731
Provisioning NetScaler VPX instances on Google Cloud 1746
Provision NetScaler VPX instances on VMware ESX 1757
NetScaler Global Load Balancing for Hybrid and Multi-Cloud Deployments 1768
Architecture of the NetScaler Hybrid and Multi-Cloud GLB Solution 1768
Configuration by using the NetScaler Console StyleBooks 1772
Using StyleBooks to Configure GLB 1775
Using StyleBooks to Configure GLB on NetScaler LB Nodes 1779
Orchestration 1782
Manage the Kubernetes cluster for Service Graph 1782
Before you begin 1782
Configure NetScaler agent to register with Kubernetes cluster 1783
Configure the NetScaler Console with a secret token to manage a Kubernetes cluster 1783
Add the Kubernetes cluster in NetScaler Console 1784
NetScaler® licenses 1786
License Activation Service 1787
Prerequisites 1789
Automatic enablement and compatibility 1789
NetScaler version compatibility for LAS 1790
Transition to LAS 1792
First-Time LAS user 1793
License NetScaler instances with LAS 1793

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Migrate existing licensed instances to LAS 1794
Existing LAS user 1796
License NetScaler instances with LAS 1796
Migrate the licensed NetScaler instances to LAS 1797
Information sent to LAS during LAS licensing workflow 1798
Best Practices for monitoring your LAS transitioned NetScaler Console service environment 1799
Prerequisites 1799
Monitoring LAS activation blob expiry 1800
View NetScaler instances by using the GUI 1800
View NetScaler instance status by using the CLI 1800
Notifications 1801
Monitoring license entitlement expiry 1802
Notifications 1802
License management 1803
LAS-based license 1804
License server ports 1804
License expiry information 1804
Notification settings 1805
RBAC support for LAS 1809
Manually managed entitlements (file-based licenses) 1809
License files 1810
License server port settings 1813
License expiry information 1813
Notification settings 1814
Minimum and maximum capacity for checkout 1817
Table 1. Supported Flexed capacity for MPX 1818
Table 2A. Supported Flexed capacity for NetScaler SDX version earlier than build 13.0-41.x 1819

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Table 2B. Supported Flexed capacity for NetScaler SDX version 13 (build 13.0-47.x and later), version 13.1 (build earlier than 51.x), and version 14.1 (build earlier 12.x) 1821

Table 2C. Supported Flexed capacity for NetScaler SDX version 13.1 (build 51.x and later), and version 14.1 (build 12.x and later) 1822

Table 3. Supported minimum/maximum bandwidth and minimum/maximum instances for NetScaler CPX instances 1823

Table 4. Supported minimum/maximum bandwidth and minimum/maximum instances for NetScaler VPX instances on Hypervisors and Cloud services 1824

Table 5. Supported minimum/maximum bandwidth and minimum/maximum instances for NetScaler BLX instances 1824

Table 6. Zero capacity license requirement for different form factors 1825

NetScaler agent behavior 1825

LAS-based licensing 1826

Manually managed entitlement (file-based licensing) 1826

Manually select a NetScaler Console agent as LSA 1827

Multiple NetScaler agents behavior 1828

NetScaler agent failover behavior 1828

Configure license server through NetScaler built-in agent 1829

Flexed license 1829

Zero-capacity hardware 1831

Manage and install Z-cap licenses 1831

Standalone NetScaler VPX instances 1832

Standalone NetScaler CPX instances 1832

Standalone NetScaler BLX instances 1833

Bandwidth Pool 1833

Instance pool 1833

Configure license 1834

LAS-based licensing 1835

Prerequisite 1835

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 1 - Validate Entitlement Reflection 1835
Step 2 - Add NetScaler instance to the console service 1835
Step 3 - Activate your license with LAS 1836
Step 4 - Edit flexed throughput capacity for NetScaler instances 1836
Special Licensing for Unlicensed MPX Appliances with an external agent 1836
Manually managed entitlements (file-based licensing) 1837
Before you begin 1838
Step 1 - Apply licenses in NetScaler Console 1839
Step 2 - Register NetScaler Console as a license server and allocate licenses 1839
Step 3 - Based on license type proceed to the relevant license procedure 1842
Configure flexed or pooled capacity on NetScaler instances 1843
License requirements for NetScaler high-availability pair (Common for both LAS and file-based licensing) 1845
NetScaler Flexed licensing states (Common for both LAS and file-based licensing) 1845
License dashboard 1846
Edit the allocated throughput capacity on a NetScaler instance 1848
Release licenses on a NetScaler instance 1849
Troubleshoot licensing issues 1849
License reporting 1850
Transition to Flexed licensing 1854
LAS-based licenses 1855
Manually managed entitlements (file-based licenses) 1855
Pooled bandwidth license to Flexed licensing 1855
Pooled vCPU to Flexed licensing 1856
Fixed subscription or Perpetual license to Flexed licensing 1857
Fixed vCPU to Flexed licensing 1857
CICO to Flexed licensing 1858
Self Managed bandwidth license to Flexed licensing 1858

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Self Managed vCPU to Flexed licensing 1859
Scenarios for Flexed or Pooled license expiry and connectivity issues behavior 1859
LAS-based licenses 1860
Before the term expires 1860
After the term expires 1860
Scenarios for connectivity issues behavior 1860
Manually managed license (file-based license) 1861
Components of Flexed licenses 1861
Scenario: MPX form factor 1861
Scenario: SDX form factor 1862
Scenario: VPX/BLX/CPX form factor 1863
Scenarios for connectivity issues behavior 1864
Configure NetScaler Console server only as the Flexed or Pooled license server 1864
Prerequisites 1866
How to configure NetScaler Console only as the Flexed or Pooled license server 1866
Legacy licenses 1868
Pooled capacity 1868
Upgrade a perpetual license in NetScaler MPX to NetScaler Pooled capacity 1870
Upgrading the perpetual license in NetScaler MPX high availability pair to NetScaler Pooled capacity 1877
Upgrade a perpetual license in a NetScaler SDX to NetScaler Pooled capacity 1882
NetScaler VPX check-in and check-out licensing 1887
Install licenses in NetScaler Console 1888
Allocate NetScaler VPX license to a NetScaler VPX instance by using the NetScaler GUI 1888
Allocate a NetScaler VPX license to a NetScaler VPX instance by using the NetScaler CLI 1889
Configure expiry checks for NetScaler VPX check-in/check-out licenses 1890
NetScaler virtual CPU licensing 1890

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Virtual CPU licensing for NetScaler VPX 1891
FAQs and other resources 1893
Configuration 1894
License Server Agent 1894
Common issues 1896
Migration 1896
Troubleshoot Pooled capacity license issues 1897
Check license status 1898
Check server status 1899
Check usage report of license 1900
Counters and statistics for Pooled capacity licensing 1901
Settings 1903
Console on-prem instances connected with Console service using Cloud Connect 1903
Console on-prem upload 1904
Configure analytics on virtual servers 1908
Configure analytics on the discovered virtual servers 1908
Edit analytics 1910
Disable analytics 1911
Configure global analytics 1912
Custom policy 1912
Global policy 1914
Points to note 1915
Migrate analytics 1915
Configure role-based access control 1916
Configure Users on NetScaler Console 1919
Configure Access Policies on NetScaler Console 1923
Grant StyleBook permissions to users 1927
Configure Roles on NetScaler Console 1928

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure Groups on NetScaler Console 1930
How user access changes based on the authorization scope 1938
Limitations 1939
Assign a net profile for the managed NetScaler instance 1940
Prerequisites 1940
Data storage management 1941
Understand your data storage 1942
State of your data ingestion activity 1943
Total storage consumption 1943
Data pruning status 1944
Storage consumption by features 1947
Manage your storage space 1948
Perform data pruning 1949
Review data retention policy 1950
Notify on exceeding storage limit 1951
Data retention policy 1951
Configure and view system alarms 1954
Configure an alarm 1954
Add threshold limits to disk utilization alarms 1957
Observability Integration 1958
Integration with Splunk 1959
Configure Splunk to receive data from NetScaler Console 1959
Configure NetScaler Console to export data to Splunk 1966
View dashboards in Splunk 1968
Integration with New Relic 1971
Prerequisites 1971
New Relic dashboard 1973
Integration with Microsoft Sentinel 1975

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure the Log Analytics Workspace 1976
Create a Microsoft Entra application 1979
Configure data collection endpoint 1981
Create tables to export data 1982
Create a subscription in NetScaler Console 1995
View logs in Microsoft Azure 1996
Configure NetScaler® instances for the export of insights to Prometheus using the default schema 1997
View logs for failed configurations 1998
Configure the export of NetScaler® metrics and audit logs to Splunk 1998
View logs for failed configurations 1999
Configuring Analytics settings 2000
Creating Thresholds and Alerts for Analytics 2000
Configure notifications 2003
Create an email distribution list 2003
Create an SMS distribution list 2005
Create a Slack profile 2005
Create a PagerDuty profile 2006
View the ServiceNow profile 2007
Export or schedule export reports 2007
Export a report 2008
Schedule export report 2008
View and edit the scheduled export reports 2010
Global Settings 2011
Instance settings 2011
Manage the instance configuration 2011
Configure instance backup settings 2011
Disable notifications for managed devices 2013

© 1997–2026 Citrix Systems, Inc. All rights reserved.

System configurations 2014
Set agent's keep-alive interval 2014
Set the NetScaler Console timezone 2014
Email subscriptions 2014
Unsubscribe Email Notifications 2017
Enable or disable features 2017
Configure an action policy to receive application event notifications 2018
Configure an action policy 2020
Use the search bar 2030
Use the audit logs option 2031
Use audit logs for managing and monitoring your infrastructure 2031
NetScaler instance related audit logs 2031
Configure NetScaler Console as a syslog server 2032
NetScaler Console related audit logs 2033
Application related audit logs 2033
Configure IP address management (IPAM) 2034
Add an external IP address provider 2034
Infoblox DDI as an external provider 2035
Add a network 2036
View allocated IP addresses 2037
How-to articles 2039
Instance management 2039
Configuration management 2039
Certificate management 2040
StyleBooks 2040
Event management 2041
FAQs 2042
How many agents do I need to install? 2042

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How can I install multiple agents? 2042
Does NetScaler agent support AMD processors? 2042
Can I transition from a built-in agent to an external agent? 2042
How do I get a new activation code if I lose it? 2042
How do I log on to the agent VM? What are the default credentials? 2042
What are the resource requirements to install an agent on a hypervisor on-premises? 2043
Do I need to assign an extra disk to the agent while provisioning? 2043
Can I reuse my activation code with multiple agents? 2043
How do I rerun network settings if I have entered an incorrect value? 2043
What do I do if my agent registration fails? 2043
Registration is successful, but how do I know if the agent is running fine? 2043
How can I connect agents to NetScaler Console using a proxy server? 2044
I do not see my Analytics Reports 2044
Which versions of NetScaler instances are supported in NetScaler Console? 2044
How do I export dashboard reports in NetScaler Console? 2044
What does enabling client-side measurements do? 2045
Is SSL traffic from Agent to NetScaler Console service taken through SSL inspection? 2045
index 2046
Analytics 2046
Dashboards 2047
Outbound traffic dashboard 2047
User dashboard 2049
WAF Insight 2053
How WAF insight works 2054
Configure WAF insight 2055
Configure geo locations for security insight reports 2057
Thresholds 2058
WAF insight use cases 2058

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure the learning profile 2061
Network violation details 2064
HTTP Slow Loris 2064
DNS Slow Loris 2065
HTTP Slow Post 2066
NXDOMAIN Flood Attack 2067
HTTP Desync Attack 2068
Bleichenbacher Attack 2070
Segment Smack Attack 2071
SYN Flood Attack 2072
Small Window Attack 2073
View WAF learning Actions Summary 2074
View failed rules 2075
Advanced search 2075
Filter results 2076
View relaxation rules, idle, and deny rules 2077
Manage deny rules 2080
SSL Insight 2080
Prerequisites 2081
Configure SSL Insight 2081
Enable the insight 2082
Enable ULFD mode 2083
Enable SSL Insight parameters 2084
Use case: Obtain an overview of the SSL transactions 2085
Use case: SSL metrics for clients 2086
View analytics for Web transactions 2087
Prerequisites 2087
Detailed Web transactions 2090

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View events 2093
Add columns in the event list 2096
Advanced search 2097
Save search 2099
Export data 2101
Detailed procedures to setup dual tier or service mesh lite topology 2101
Configure a NetScaler agent 2101
Configure static routes in the agent 2101
Download the sample deployment files from GitHub 2103
Add parameters in CPX YAML file 2103
Add VPX or SDX or MPX or BLX instance in NetScaler Console 2105
Add Kubernetes cluster in NetScaler Console 2105
Deploy a sample microservice application 2108
Deploy CPX and register CPX in NetScaler Console 2109
Enable auto select virtual servers for licensing 2109
Enable Web Transaction and TCP Transaction settings 2110
Send traffic to microservices 2111
Detailed procedures to setup service mesh topology 2112
Configure NetScaler agent 2112
Configure static routes in the agent 2112
Configure the required parameters 2114
Deploy a sample application 2116
Add Kubernetes cluster in NetScaler Console 2117
Enable auto select virtual servers for licensing 2120
Enable Web Transaction and TCP Transaction settings 2121
Send traffic to microservices 2123
Detailed procedures to setup single tier or unified ingress topology 2124
Add VPX or SDX or MPX or BLX instance in NetScaler Console 2124

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Add Kubernetes cluster in NetScaler Console 2124
Data governance for NetScaler® telemetry program 2127
Required telemetry data 2129
How to change the NetScaler MPX and VPX root password 2129
Change password using the **Configuration Jobs** feature 2129
Step 1. Create a **Configuration Template** 2130
Create a Configuration Job 2131
Modify the admin profile 2132
Previous releases 2133
December 13, 2023 2134
Infrastructure 2134
Licensing 2134
Analytics 2135
Infrastructure 2135
Fixed Issues 2136
November 29, 2023 2137
Infrastructure 2137
Fixed Issues 2137
November 09, 2023 2138
Analytics 2138
Fixed Issues 2138
October 25, 2023 2139
Analytics 2139
Infrastructure 2140
Fixed issues 2140
October 10, 2023 2140
Management and Monitoring 2140
September 26, 2023 2141

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Analytics 2141

Infrastructure 2141

Fixed Issues 2141

Analytics 2141

September 13, 2023 2141

Infrastructure 2141

Fixed Issues 2142

August 31, 2023 2142

Infrastructure 2142

Security 2143

Fixed Issues 2143

Management and Monitoring 2144

August 11, 2023 2144

Management and Monitoring 2144

August 09, 2023 2144

Infrastructure 2144

Security 2145

Fixed Issues 2145

July 26, 2023 2146

Analytics 2146

Infrastructure 2147

StyleBooks 2147

July 18, 2023 2147

Management and Monitoring 2147

July 12, 2023 2148

Fixed issues 2148

July 03, 2023 2149

Analytics 2149

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infrastructure 2149
Fixed issues 2149
June 14, 2023 2150
Security 2150
StyleBooks 2150
Fixed Issues 2150
May 31, 2023 2151
Analytics 2151
Fixed Issues 2152
May 18, 2023 2152
Analytics 2152
Infrastructure 2153
Fixed Issues 2153
May 09, 2023 2154
Management and Monitoring 2154
April 25, 2023 2154
Analytics 2155
StyleBooks 2155
Fixed Issues 2155
Analytics 2155
April 13, 2023 2155
Analytics 2156
Infrastructure 2157
Fixed Issues 2157
April 05, 2023 2157
Security 2158
Fixed Issues 2158
March 14, 2023 2159

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues 2159
March 02, 2023 2159
Analytics 2159
Infrastructure 2160
Management and Monitoring 2160
Security 2161
Application Performance Analytics 2161
Miscellaneous 2161
Fixed Issues 2162
February 07, 2023 2162
Analytics 2162
Management and Monitoring 2162
Fixed issues 2163
January 24, 2023 2163
Fixed issues 2163
January 10, 2023 2164
Management and Monitoring 2164
StyleBooks 2164
NetScaler® Console service documentation history 2165
fix 2171

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Overview

NetScaler Console service (Formerly known as NetScaler ADM service) is a web-based solution for managing all NetScaler deployments that include NetScaler MPX, NetScaler VPX, NetScaler SDX, NetScaler CPX, NetScaler BLX, and NetScaler Gateway that are deployed on-premises or on the cloud.

You can use this cloud solution to manage, monitor, and troubleshoot the entire global application delivery infrastructure from a single, unified, and centralized cloud-based console. NetScaler Console provides all the capabilities required to quickly set up, deploy, and manage application delivery in NetScaler deployments and with rich analytics of application health, performance, and security.

NetScaler Console provides the following benefits:

- **Agile** – Easy to operate, update, and consume. The service model of NetScaler Console is available over the cloud, making it is easy to operate, update, and use the features provided by NetScaler Console. The frequency of updates, combined with the automated update feature, quickly enhances your NetScaler deployment.
- **Faster time to value** – Quicker business goals achievement. Unlike with the traditional on-premises deployment, you can use your NetScaler Console with a few clicks. You not only save the installation and configuration time, but also avoid wasting time and resources on potential errors.
- **Multi-Site Management** – Single pane of glass for instances across multi-site data centers. With the NetScaler Console, you can manage and monitor NetScalers that are in various types of deployments. You have one-stop management for NetScalers deployed on-premises and in the cloud.
- **Operational Efficiency** – Optimized and automated way to achieve higher operational productivity. With the NetScaler Console, your operational costs are reduced by saving your time, money, and resources on maintaining and upgrading the traditional hardware deployments.
- **Visibility into real-time internet traffic** - Enhanced user experience with the real-time internet traffic analysis. With the NetScaler Console, you can gather real user monitoring data from clients as they access applications across clouds, data centers, and CDNs, and build a holistic

© 1997–2026 Citrix Systems, Inc. All rights reserved.

picture of internet health. Traffic is directed to locations with the lowest latency and best availability to ensure an optimal user experience.

- **Multi-site applications** - Create, configure, and deliver an application in multiple sites. With the NetScaler Console, you can configure, deliver, and manage applications across multiple cloud environments for high availability and reliability.

How NetScaler Console works

NetScaler Console is available as a service on the Citrix Cloud. After you sign up for Citrix Cloud and start using the service, install agents in your network environment or initiate the built-in agent in the instances. Then, add the instances you want to manage to the service.

An agent enables communication between the NetScaler Console and the managed instances in your data center. The agent collects data from the managed instances in your network and sends it to the NetScaler Console.

When you add an instance to NetScaler Console, it implicitly adds itself as a trap destination and collects an inventory of the instance.

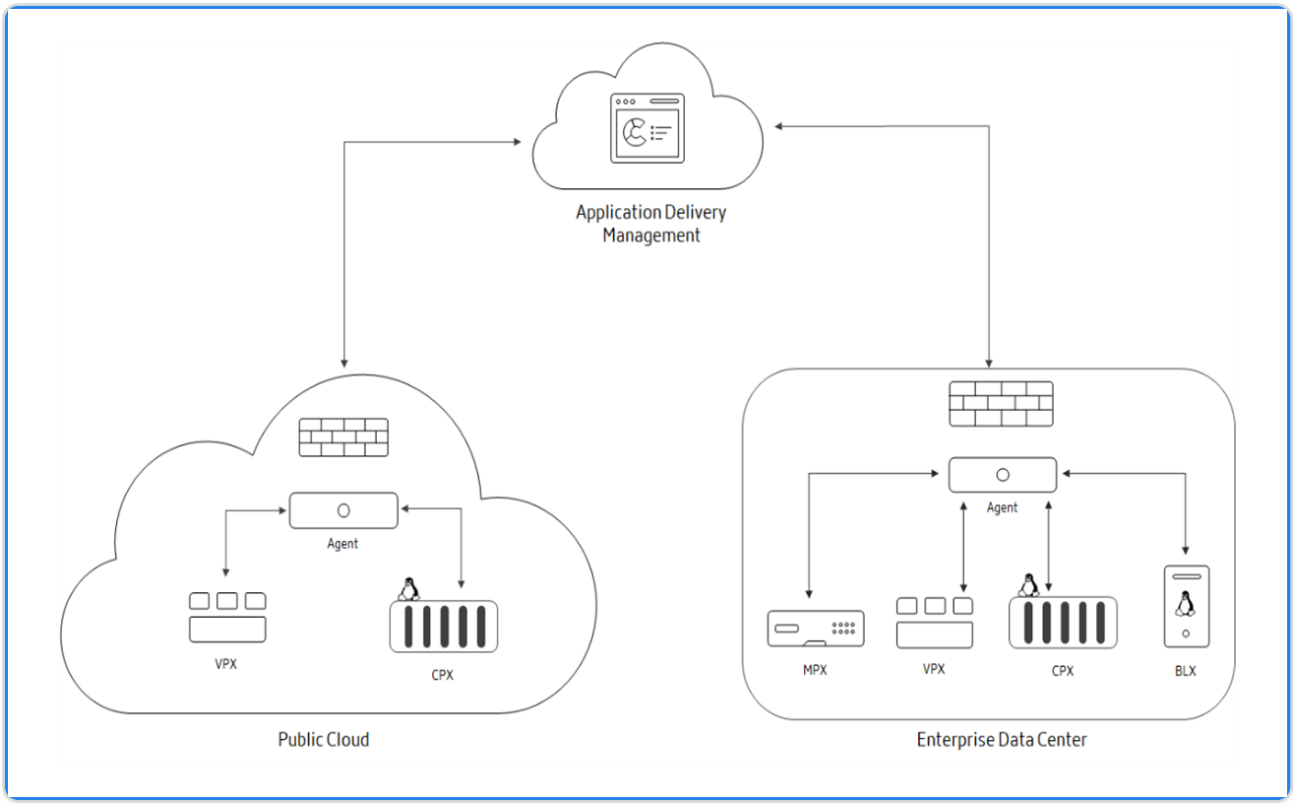
The service collects instance details such as:

- Host name
- Software version
- Running and saved configuration
- Certificates
- Entities configured on the instance, and so on.

NetScaler Console periodically polls managed instances to collect information. For more information, see Data governance.

The following image illustrates the communication between the service, agents, and instances (MPX, VPX, CPX, BLX):

© 1997–2026 Citrix Systems, Inc. All rights reserved.



To onboard to NetScaler Console and see how it works, see Getting Started and its subtopics.

Features and solutions

This document describes the features that are supported on the NetScaler Console.

Application analytics and management

Application Analytics and Management feature of NetScaler Console strengthens the application-centric approach to help you address various application delivery challenges. This approach gives you visibility into the health scores of applications, helps you determine the security risks, and helps you detect anomalies in the application traffic flows and take corrective actions.

- Application performance analytics: App Score is the product of a scoring system that defines how well an application is performing. It shows whether the application is performing well in terms of responsiveness, is not vulnerable to threats, and has all systems up and running.
- Application security analytics: The App Security Dashboard provides a holistic view of the security status of your applications. For example, it shows key security metrics such as security violations, signature violations, threat indexes. App Security dashboard also displays attack related information such as SYN attacks, small window attacks, and DNS flood attacks for the discovered NetScaler instances.
- Intelligent App Analytics: The Intelligent App Analytics feature provides an easy and scalable solution for monitoring and troubleshooting applications that are delivered through NetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

appliances. Intelligent App Analytics not only monitors all the levels of application transactions, but also uses machine learning techniques to define normal traffic patterns in your network and detect anomalies. This feature reduces the overall turnaround time and improves the overall application uptime.

StyleBooks

StyleBooks simplify the task of managing complex NetScaler configurations for your applications. A StyleBook is a template that you can use to create and manage NetScaler configurations. You can create a StyleBook for configuring a specific feature of NetScaler, or you can design a StyleBook to create configurations for an enterprise application deployment such as Microsoft Exchange or Skype for Business.

Instance management

Enables you to manage the NetScaler, NetScaler Gateway, and Citrix Secure Web Gateway instances.

Event management

Events represent occurrences of events or errors on a managed NetScaler instance. For example, when there is a system failure or change in configuration, an event is generated and recorded on NetScaler Console. Following are the related features that you can configure or view by using NetScaler Console:

- Creating event rules
- Using NetScaler Console to export syslog messages

Certificate management

NetScaler Console streamlines every aspect of certificate management for you. Through a single console, you can establish automated policies to ensure the right issuer, key strength, and correct algorithms, while keeping close tabs on certificates that are unused or soon to expire.

Configuration management

NetScaler Console allows you to create configuration jobs that help you perform configuration tasks, such as creating entities, configuring features, replication of configuration changes, system upgrades, and other maintenance activities with ease on multiple instances. Configuration jobs and templates simplify the most repetitive administrative tasks to a single task on NetScaler Console.

Configuration audit

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enables you to monitor and identify anomalies in the configurations across your instances.

- Configuration advice: Allows you to identify configuration anomaly.
- Audit template: Allows you to monitor the changes across a specific configuration.

License management

Allows you to manage NetScaler licenses by configuring NetScaler Console as license manager.

- NetScaler pooled capacity: A common license pool from which your NetScaler instance can check out one instance license and only as much bandwidth as it needs. When the instance no longer requires these resources, it checks them back in to the common pool, making the resources available to other instances that need them.
- NetScaler VPX check-in and check-out licensing: NetScaler Console allocates licenses NetScaler VPX instances on demand. A NetScaler VPX instance can check out the license from the NetScaler Console when a NetScaler VPX instance is provisioned, or check back in its license to NetScaler Console when an instance is removed or destroyed.

Network reporting

You can optimize resource usage by monitoring your network reporting on NetScaler Console.

Analytics

Provides an easy and scalable way to look into the various insights of the NetScaler instances' data to describe, predict, and improve application performance. You can use one or more analytics features simultaneously.

- HDX Insight: Provides end-to end visibility for ICA traffic passing through NetScaler. HDX Insight enables administrators to view real-time client and network latency metrics, historical reports, end-to-end performance data, and troubleshoot performance issues.
- Web Insight: Provides visibility into enterprise web applications. It allows IT administrators to monitor all web applications served by the NetScaler by providing integrated and real-time monitoring of applications. Web Insight processes data from NetScaler using an approximation algorithm. It provides top 1,000 records of the metrics related to the web applications in your enterprise.
- Gateway Insight: Provides visibility into the failures that users encounter when logging on, regardless of the access mode. You can view a list of users logged on at a given time, along with the number of active users, number of active sessions, and bytes and licenses used by all users at any given time.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Security Insight: Provides a single-pane solution to help you assess your application security status and take corrective actions to secure your applications.
- SSL Insight: Provides visibility into secure transactions on the web (HTTPs). It allows IT administrators to monitor all web applications served by the NetScaler by providing integrated, real-time, and historic monitoring of web transactions. SSL insight processes data from NetScaler using an approximation algorithm. It provides top 1,000 records of the metrics related to the web transactions in your enterprise.

Role-based access control

Role-based access control (RBAC) allows you to grant access permissions based on the roles of individual users within your enterprise. The first user of an organization who logs on with Citrix Cloud™ credentials has the super admin role who, by default, has all access permissions. The other users of that organization, who are later created by the admin, are granted non-admin roles.

Subscriptions

Provides a dashboard view of the subscriptions that you have purchased.

You are assigned to an Express account by default. With this account, you can manage limited NetScaler Console resources. For more information, see Manage NetScaler Console resources using Express account.

The following NetScaler Console features are currently not available:

- Deployment
  - Migrating from Citrix Insight Center to NetScaler Console
  - Integrating NetScaler Console with Citrix Virtual Desktop Director
- Analytics: TCP Insight and Video Insight
- Limited System Settings
- Orchestration
  - Integration with OpenStack and VMware NSX Manager
  - NetScaler Automation in Cisco ACI's Hybrid Mode
  - Container Orchestration: Integration with Mesos/Marathon and Kubernetes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Release notes

The NetScaler Console (Formerly known as NetScaler ADM service) release notes describe the new features, enhancements to existing features, fixed issues, and known issues available in a service release.

For more information, see:

- What's new
- Previous Releases

The NetScaler agent are, by default, automatically upgraded to NetScaler Console latest build. You can view the agent details on the **Infrastructure > Instances > Agents** page. You can also specify the time when you want the agent upgrades to happen. For more information, see Configuring Agent Upgrade Settings.

What's new

October 03, 2026

Management and Monitoring

Support for identification and remediation of CVE-2026-88779

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2026-88779.

- Identification for CVE-2026-88779 requires version scan. Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix. For more information, see Remediate CVE-2026-88779.

  NOTE:

  Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For more information about using NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.
- For more information about the CVE, see Security Bulletin.

September 27, 2026

Management and Monitoring

Support for identification and remediation of CVE-2026-88771

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2026-88771.

- Identification for CVE-2026-88771 requires version scan. Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix. For more information, see Remediate CVE-2026-88771.

  NOTE:

  Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

- For more information about using NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.
- For more information about the CVE, see Security Bulletin.

Support for identification and remediation of CVE-2026-88772

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2026-88772.

- Identification for CVE-2026-88772 requires version scan. Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix. For more information, see Remediate CVE-2026-88772.

  NOTE:

  Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For more information about using NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.
- For more information about the CVE, see Security Bulletin.

Support for identification and remediation of CVE-2026-88773

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2026-88773.

- Identification for CVE-2026-88773 requires version scan. Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix. For more information, see Remediate CVE-2026-88773.

  NOTE:

  Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

- For more information about using NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.
- For more information about the CVE, see Security Bulletin.

Support for identification and remediation of CVE-2026-88774

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2026-88774.

- Identification for CVE-2026-88774 requires version scan. Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix. For more information, see Remediate CVE-2026-88774.

  NOTE:

  Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

- For more information about using NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.
- For more information about the CVE, see Security Bulletin.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for identification and remediation of CVE-2026-88775

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2026-88775.

- Identification for CVE-2026-88775 requires version scan. Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix. For more information, see Remediate CVE-2026-88775.

  NOTE:

  Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

- For more information about using NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.
- For more information about the CVE, see Security Bulletin.

Support for identification and remediation of CVE-2026-88776

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2026-88776.

- Identification for CVE-2026-88776 requires version scan. Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix. For more information, see Remediate CVE-2026-88776.

  NOTE:

  Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

- For more information about using NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.
- For more information about the CVE, see Security Bulletin.

Support for identification and remediation of CVE-2026-88777

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2026-88777.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Identification for CVE-2026-88777 requires version scan. Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix. For more information, see Remediate CVE-2026-88777.

  NOTE:

  Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

- For more information about using NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.
- For more information about the CVE, see Security Bulletin.

Support for identification and remediation of CVE-2026-88778

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2026-88778.

- Identification for CVE-2026-88778 requires a version scan, and remediation requires a two-step process:

  a. Upgrade the vulnerable NetScaler instance to a release and build that has the fix.

  b. Apply configuration jobs.

  For more information, see Remediate CVE-2026-88778.

  NOTE:

  Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

- For more information about using NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.
- For more information about the CVE, see Security Bulletin.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

September 15, 2026

Fixed issues

Analytics

In some cases, the bandwidth and volume totals shown for an application in NetScaler Console might be underreported when a metrics update is resent by NetScaler.

Infrastructure

With Cloud Connect, the license entitlements fetch fails when the customer ID configured on NetScaler Console on-premises does not match the capitalization of the customer ID in NetScaler Console service.

In a NetScaler HA setup managed by the Console built-in agent, the built-in agent might fail to start on the secondary node if that NetScaler is running an older build. If a failover occurs, the HA pair might appear as "Down" in NetScaler Console.

September 01, 2026

What's new

Management and Monitoring

- **Certificate source visibility and bound certificate protection**

  Certificate files now display their source, allowing administrators to distinguish between:

  - **Local**: Certificates locally installed on NetScaler (including certificates installed directly or through the Certificate Store).
  - **Remote**: Certificates managed and fetched through Zero Touch Certificate Management (ZTCM).

  This enhancement provides better visibility into the certificate origin and management workflows.

  Bound-Status Indicator is a new status indicator in the certificate inventory that identifies certificates that are currently bound to SSL configurations and actively in use. This enhancement gives administrators a clear view of the certificate dependencies before performing any lifecycle operations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Safe Deletion lets administrators delete certificate files directly from the certificate inventory. To prevent service disruptions, deletion is restricted to unbound certificates only. You cannot delete certificates that are actively bound to SSL entities or managed by certificate workflows until you remove the binding.

- **Unified certificate source experience and certificate import pre-checks for SSL certificates**

  NetScaler Console now provides a unified certificate selection experience by consolidating certificate files from different sources into a single view. Previously, administrators had to choose between separate **Files on NetScaler** and **Files on Console** options. With this enhancement, certificate files are presented through a single consolidated workflow, simplifying certificate management and selection. Additionally, the certificate upload option has been removed from this workflow to streamline the user experience and reduce source selection complexity.

  NetScaler Console also performs pre-validation checks before importing SSL certificates and keys across NetScaler instances to prevent unintended file conflicts and certificate overwrites.

  The following are the key enhancements associated with this feature:

  - **Duplicate file detection**: Before installation, the system validates whether the certificate or key file name already exists on the destination NetScaler instance. Destinations with conflicting file names are identified and flagged before deployment.
  - **Overwrite protection**: Certificate imports no longer overwrite existing certificate or key files. If a conflict is detected, the import is blocked, and the administrator must resolve the conflict by using a different file name or removing the duplicate.
  - **Per-destination validation**: For bulk certificate imports, each destination instance is evaluated independently. Administrators can view which destinations are eligible or ineligible for installation and proceed only with the valid targets.
  - **Backend safety validation**: An additional validation is performed during installation to ensure destination eligibility has not changed. Certificates are installed only on instances that successfully pass the final validation checks.

  The following are the benefits of this enhancement:

  - Prevents accidental overwriting of existing certificates and private keys.
  - Reduces the risk of certificate chain disruptions caused by file replacement.
  - Improves visibility into deployment readiness across multiple NetScaler instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Provides a safer and more predictable certificate deployment experience.

Fixed issues

Analytics

Web App Firewall and BOT threshold breach email alerts are not sent because the job reads the wrong IP address column, which is always empty.

NetScaler Console analytics scheduler repeatedly pushes the configuration settings to NetScaler instances even when the configuration is successfully applied during the first push. This issue triggers false failure alerts even though everything is working properly.

NetScaler Console audit logs might not reach Microsoft Sentinel if they are sent to an undeclared stream instead of the documented `console_syslog_messages_CL`, causing Azure to reject every batch.

Infrastructure

Users are unable to apply WAF recommendations on NetScaler when the **Prompt credentials for stylebook operations** option is enabled.

In Azure environments, SNMPv3 traps sent from NetScaler to the NetScaler Console cloud agent might fail with an "Unknown user name" authentication error.

NetScaler Console sends false vulnerability notifications when no managed NetScaler instance qualifies for the File Integrity Monitoring scan, and the Slack notifications for these scans are blank, with no scan details.

The NetScaler Console agent might fail to route traffic through a configured proxy, causing connectivity issues between the agent and NetScaler Console.

GSLB virtual server entries might not appear in the virtual servers list in NetScaler Console when a GSLB site group is configured.

NetScaler Console incorrectly shows packet drops due to a throughput rate limit.

During a config audit poll of selected instances, NetScaler Console deleted the cached instance configuration before downloading its replacement. As a result, the configuration remained unavailable throughout the polling period. In the event of a poll failure, the configuration remained unavailable until the next successful run.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

During `mastools` registration on Azure devices, NetScaler Console logs an error in the `mastools_reg.py` log. However, this error does not block mastools registration for Azure devices.

August 19, 2026

Management and Monitoring

Support for identification and remediation of CVE-2026-19489

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2026-19489.

- Identification for CVE-2026-19489 requires version scan. Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix. For more information, see Remediate CVE-2026-19489.

  NOTE:

  Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

- For more information about using NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.
- For more information about the CVE, see Security Bulletin.

Support for identification and remediation of CVE-2026-19490

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2026-19490.

- Identification for CVE-2026-19490 requires version scan. Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix. For more information, see Remediate CVE-2026-19490.

  NOTE:

  Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For more information about using NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.
- For more information about the CVE, see Security Bulletin.

August 04, 2026

What's new

Management and Monitoring

- **File integrity monitoring support for NetScaler VPX Linux-based platform**

  The file integrity monitoring feature is now supported for NetScaler VPX instance on Linux platform. With this feature, you can easily detect unauthorized file and configuration changes.

Fixed issues

Analytics

The Web Applicatioon Firewall and BOT policies configured on the NetScaler Console disappear after a few days and reappear only after manually editing or toggling the policy.

Infrastructure

When the Infoblox DNS provider is used for DNS-01 domain validation in NetScaler Console, ACME certificate issuance and renewal fail during domain validation.

On the **Zero-touch Certificate Management** page in NetScaler Console, changing from **Custom sync** to **Global sync** might fail. The instance remains in Custom sync.

Attempting to download an SSL certificate from the SSL Dashboard fails with a `404 - File not found error`, even when the certificate exists on NetScaler® and its details are visible in NetScaler Console. This issue specifically affects certificates stored in subdirectories under `/nsconfig/ssl/`.

NetScaler Console reports the agent as Down when an inventory core dump occurs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

July 14, 2026

What's new

Management and Monitoring

- **GeoIP database synchronization for NetScaler Console and agents**

  NetScaler Console service now supports centralized GeoIP database synchronization for NetScaler Console, deployed agents, and managed instances from a single workflow. Previously, synchronization was limited only to NetScaler instances.

  The GeoIP synchronization feature includes the following capabilities:

  - **Unified Synchronization**: Synchronize a GeoIP database file to the NetScaler Console, agents, and instances in a single operation.
  - **Sync Now**: The Sync Now option supports two modes:
    - **Sync all**: Automatically push the file to all entities, such as managed NetScaler instances, NetScaler Console, and agents.
    - **Customize**: Select specific Console agents.
  - **Scheduled Synchronization**: Create one-time or recurring synchronization schedules targeting any combination of entity types.
  - **Historical Job Logs**: View a timestamped log of past synchronization jobs, which details the scope, the file used, and per-device results (status, start time, and end time).
  - **Entity-Wise Synchronization Status**: Access an expandable panel on the main page to view per-device synchronization results, filterable by status, IP address, entity type, or version.
  - **Last Synchronization Overview**: Quickly assess synchronization health with an at-a-glance summary displaying the total selected entities, alongside pending, in-progress, successful, failed, and overall completion percentages.

Telemetry

- **Support for telemetry diagnostics**

  The NetScaler Console service now supports telemetry diagnostics to help administrators quickly identify and troubleshoot telemetry collection and upload issues across managed NetScaler instances. This feature introduces detailed telemetry insights, device- and agent-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

level status visibility, error codes with remediation guidance, and live connectivity validation checks.

Administrators can now easily determine whether telemetry upload failures are caused by device reachability, SSH connectivity, agent communication, telemetry package issues, or service connectivity problems, reducing troubleshooting time and improving telemetry coverage.

Some of the benefits are:

- View telemetry status for managed NetScaler instances.
- Access detailed failure diagnostics with error codes and mitigation guidance.
- Monitor agent telemetry health and package execution details.
- Perform live connectivity checks for telemetry-related endpoints and services.

Fixed issues

Analytics

After migrating NetScaler Console on-premises to the cloud, detailed web transaction records are not displayed for the affected NetScaler, while other analytics, such as metrics and bot data, continue to appear normally. This issue occurred because the required storage for these transactions was not fully provisioned for migrated tenants.

Infrastructure

NetScaler Console periodically activates LAS on NetScaler instances, which modifies files under /nsconfig/license/ during token refreshes and results in false-positive "Diff Exists" alerts in Config Audit File Diff.

NetScaler Console cloud agents generate event logs that do not include the source IP address. The source field for these events appears blank instead of showing the IP address of the agent or device that initiated the event.

Downloading SSL certificates where the certificate name starts with two hexadecimal characters (for example, de, ab, ce, or 25) using NetScaler Console SSL Dashboard fails with the "404 - File not found" error. This issue occurs even when the SSL certificate exists on NetScaler and its details are visible in NetScaler Console.

You might encounter an "invalid resource" error when editing user groups under Users and Roles in the NetScaler Console service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Miscellaneous

In rare scenarios, NetScaler Console fails to connect to NetScaler via the agent. As a result, NetScaler might be reported in a Grace state due to incorrect database updates.

June 30, 2026

Management and Monitoring

Support for identification and remediation of CVE-2026-8451

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2026-8451.

- Identification for CVE-2026-8451 requires version scan. Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix. For more information, see Remediate CVE-2026-8451.

  NOTE:

  Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

- For more information about using NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.
- For more information about the CVE, see Security Bulletin.

Support for identification and remediation of CVE-2026-8452

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2026-8452.

- Identification for CVE-2026-8452 requires version scan. Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix. For more information, see Remediate CVE-2026-8452.

  NOTE:

  Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For more information about using NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.
- For more information about the CVE, see Security Bulletin.

Support for identification and remediation of CVE-2026-8655

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2026-8655.

- Identification for CVE-2026-8655 requires version scan. Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix. For more information, see Remediate CVE-2026-8655.

  NOTE:

  Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

- For more information about using NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.
- For more information about the CVE, see Security Bulletin.

Support for identification and remediation of CVE-2026-10816

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2026-10816.

- Identification for CVE-2026-10816 requires version scan. Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix. For more information, see Remediate CVE-2026-10816.

  NOTE:

  Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

- For more information about using NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.
- For more information about the CVE, see Security Bulletin.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for identification and remediation of CVE-2026-10817

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2026-10817.

- Identification for CVE-2026-10817 requires version scan. Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix. For more information, see Remediate CVE-2026-10817.

  NOTE:

  Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

- For more information about using NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.
- For more information about the CVE, see Security Bulletin.

June 17, 2026

Fixed issues

Analytics

If you enable BOT Insight on a virtual server but do not enable metrics, NetScaler Console does not process the BOT violations. This issue occurs because processing the BOT violations depends on metrics enablement.

On the **Analytics** page, users might see other instances in addition to the specific instances that have been authorized for access based on the User, Role, Group, and Access Policy defined for that particular user.

Infrastructure

Users are unable to apply WAF recommendations on NetScaler when the **Prompt credentials for stylebook operations** option is enabled.

In rare cases, an error occurs when you try to access or download a backup file that is initially generated with a size in KB.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When a Microsoft Entra ID (Azure AD) user signs in to NetScaler Console service under an already-onboarded Citrix Cloud tenant, the user is assigned the default `adminExceptSystem` role instead of the role mapped to their Microsoft Entra ID group. As a result, affected users receive broader permissions than intended.

NetScaler Console agent crashes when a cloud provider presents an oversized certificate.

GoDaddy CA is not supported in NetScaler Console service.

Licensing

If a NetScaler instance is deleted and re-added, NetScaler Console does not automatically resume LAS licensing for the NetScaler instance.

NetScaler Console rejects the extension blob if the host ID in the extension blob does not exactly match (case-sensitive) the NetScaler Console GUI host ID.

When a pooled license contains entitlements with different Subscription Advantage (SA) dates, NetScaler Console repeatedly sends license-expiry alert emails (about once every few seconds) instead of sending a single notification per expiry warning.

June 03, 2026

Fixed issues

Infrastructure

NetScaler BLX instance upgrades initiated through NetScaler Console fail even when NetScaler BLX instances are up and operational. This issue occurs because the pre-upgrade check incorrectly reports the instances as unreachable, which prevents the successful upgrade.

In the **NetScaler Console Security Advisory** page, CVE detection shows a CVE count for each instance, but clicking the CVE count does not load the details.

In the SSL Dashboard, issuing an ACME wildcard certificate might fail.

Licensing

In pooled licensing mode, for NetScaler SDX devices, only the Platinum edition is allocated. Standard and Advanced editions are not allocated even when values are provided.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

May 19, 2026

Management and Monitoring

Support for duplicate certificate conflict management

NetScaler now supports the prevention of conflicts caused by duplicate certificate names and content during installation and update processes. Managing duplicate certificate names or content is essential when you install or update certificates, as these duplicates can lead to configuration conflicts. This feature ensures that the system maintains a clean and unique repository of certificates, which simplifies administrative tasks and enhances system reliability.

Update server certificates without intermediate uploads

You can now renew certificates without the repetitive task of re-uploading intermediate certificates. This enhancement reduces manual workload and minimizes the risk of configuration errors.

EFFORTLESS RENEWALS

NetScaler Console now preserves your existing certificate chain during an update by default. This ensures that your chain remains intact and valid, even when you only upload a new server-level certificate.

KEY IMPROVEMENTS

- Reduced complexity: Eliminates mandatory intermediate uploads during standard server certificate updates.
- Safety first: Automatic chain preservation prevents "chain breakage," a common cause of SSL handshake errors.

NEW PARAMETERS

The following parameters provide explicit control when your requirements go beyond a simple renewal:

PARAMETER	FUNCTION
Overwrite Existing Certificate Chain	Use this to replace or remove the current chain. With a bundle: Replaces the existing chain with the new uploaded chain. Without a bundle: Removes the current chain.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	FUNCTION
Add Certificate Chain	Select this to manually upload and append intermediate certificates if they are not included in your primary server certificate file.

For information related to update server certificates without intermediate uploads, see Use the NetScaler Console certificate store to manage SSL certificates.

Custom SNMP trap support

NetScaler Console service now supports custom SNMP traps. You can view the custom SNMP traps under **Event Messages**, where they are tagged as custom to help you distinguish them from the default SNMP alerts.

Related topic: Events.

Upgrade jobs: Warning for duplicate upgrade job schedule

As part of the upgrade job workflow, if a customer attempts to create an upgrade job for NetScaler instances that already have an existing upgrade job scheduled, NetScaler Console displays a warning message. This warning message helps prevent unintentionally scheduling duplicate upgrade jobs on the same NetScaler instance. This enhancement ensures better control over upgrade jobs and avoids potential conflicts during upgrades.

Related topic: Upgrade jobs.

Support for additional Certificate Authorities and DNS providers for ACME-based automated certificate renewal

NetScaler Console Automated Certificate Management Environment (ACME) integration for automated certificate renewal now supports more Certificate Authorities (CAs) and DNS providers. If you are using any of the supported CAs or DNS providers, you can leverage the ACME integration for seamless certificate management.

For the complete list of supported Certificate Authorities (CAs) and DNS providers, see Automated certificate renewal by using the ACME protocol.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

File Integrity Monitoring dashboard displays scan errors

The File Integrity Monitoring (FIM) dashboard now displays scan error results directly within the main dashboard view. You need not click the individual scan results or line items to access error details. Any integrity issues, such as hash mismatches or scan errors, are presented in a clear, accessible format on the dashboard itself. This enhancement streamlines the troubleshooting process, allowing you to quickly identify and understand problems at a glance. As a result, you can respond to integrity issues more efficiently, saving time, and improving overall workflow transparency.

Related topic: File Integrity Monitoring.

Support for Indicators of Compromise (IoC) detection

The Indicators of Compromise (IoC) detection feature in NetScaler Console is designed to detect if your NetScaler appliances have potentially been affected due to a vulnerability.

If there are CVE events, one of the first concerns is that malicious actors exploit the vulnerability. An exploit causes catastrophic damage to a customers business, and hence its critical to detect such incidents immediately. IoC has been distributed for NetScaler in the past through support channels, which meets the customer need but comes at an additional effort of going through the support process of raising a ticket, speaking with a support professional, which might sometimes not be ideal. The IoC detection feature in NetScaler Console is designed to short-circuit the current support-oriented process and help a customer in making a quick assessment of their NetScaler infrastructure.

For more information, see Indicators of Compromise detection in NetScaler Console.

SSL filter mode support

A NetScaler instance can now fetch the metadata of specific SSL certificates and private keys. Implementing this "least privilege" approach ensures that instances access only the assets they require, preventing a compromise on one instance from exposing your entire certificate infrastructure. This feature is especially useful for environments with multiple administrators managing groups of NetScaler instances for distinct purposes.

Some of the benefits are:

- **Security segmentation**: Restricts metadata access at a per-NetScaler level to minimize the attack surface and adhere to organizational security policies.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Streamlined admin experience**: Reduces complexity in multi-tenant or departmental deployments by showing administrators only the assets relevant to their group of NetScaler instances.
- **Optimized resource utilization**: Prevents system memory bloating by fetching the metadata of only the required SSL certificates and private keys.

The filter mode configuration defines how NetScaler instances and SSL files interact through specific synchronization types. You can manage these settings through NetScaler Console to ensure that only the necessary metadata is fetched by each instance.

COMPONENT	SYNC TYPE	DESCRIPTION
NetScaler Instance	Custom Sync	NetScaler instances in this mode fetch only the metadata for certificates and keys specifically mapped to the instance.
NetScaler Instance	Global Sync	NetScaler instances in this mode fetch the metadata for all uploaded certificates and private keys.
SSL Files	Custom Files	These files are specifically mapped to NetScaler instances in Custom Sync mode.
SSL Files	Global Files	Metadata for these files is fetched by all the NetScaler instances in Global Sync mode.

CONFIGURE FILTER MODE SETTINGS

To configure filter mode, define synchronization types for your instances and files. This ensures a secure and optimized distribution of sensitive metadata.

To configure using the GUI:

1. **Upload New Files (Day Zero)**: Navigate to **Certificate Files and NetScaler Instances > Upload** to add new assets. Select one of the following sync types:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **GLOBAL**: Select to use global sync mode and complete the upload.
- **CUSTOM**: Select to use custom sync mode, choose the specific instances for mapping, and then upload the files.

2. **Move Existing Files (Day N)**: To shift certificates and keys from global sync to custom sync mode, select the target NetScaler instances and click **Add Existing Files**.
3. **Select Domains**: Once instances are selected, choose the relevant domains to trigger the shift. NetScaler Console automatically detects and shifts the corresponding certificates and private key files to custom sync mode.
4. **View Assets**: Navigate to the landing page to view all the certificates and private key files mapped to each NetScaler instance in custom sync mode.
5. **Switch Sync Mode**: To return instances to global sync mode, click **Switch to Global Sync** on the landing page.

Fixed issues

Analytics

- When a user launches an ICA session on a server hosted on the IP address containing '0' (for example, 10.0.2.3), NetScaler Console displays the IP address as 10.2.3.

Infrastructure

- The Cloud Connect disconnect operation might fail in NetScaler Console on-premises. NetScaler Console on-premises instance remains connected to NetScaler Console service despite GUI showing Cloud Connect as disconnected. This causes on-premises instances to appear as "Up" in NetScaler Console service.
- In rare cases, the File Integrity Monitoring (FIM) scan results might report errors.
- In rare cases, the telemetry retry mechanism might fail to terminate after a successful operation, resulting in duplicate telemetry processes on the NetScaler device. This has no functional impact on telemetry collection or forwarding.
- In NetScaler Console, the application security violation log details might fail to load even though the violation count graph reflects the data.
- A connection failure occurs when a Redis instance transitions from authenticated to unauthenticated mode and the service continues to use stale authentication credentials.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler Console service might display an Invalid key file password error when you attempt to add password-encrypted key files.

- When an application is associated with a user group and the NetScaler virtual server is renamed, the application is automatically removed from the user group. This results in an inconsistent user group configuration.

March 31, 2026

Management and Monitoring

Exclude files from Config Audit

You can now exclude specific files from Config Audit so that they are not monitored for change. Use exclusions for system-generated or frequently updated files (for example, files that change daily) to reduce noise and avoid false positives in audit results.

Examples for file name (or relative path) to exclude from Config Audit File Diff:

- Valid file name (or relative path)
  - `ns.conf`, `ssl/ns.cert`
- Invalid file name (or relative path)
  - `/ns.txt`, `\nsconfig\ns.conf` (Excluded file name must be a relative path)
  - `ns.conf` (Excluded file name must contain only ASCII characters)
  - `C:/nsconfig/ns.conf` (Excluded file name must not use drive-letter paths)
  - `ssl/../../ns.conf` (Excluded file name must not contain parent-directory traversal (`..`))

NOTE:

- File diff comparison is applicable only to files under the `/nsconfig` directory.
- When excluding files from Config Audit, users must specify relative paths under `/nsconfig`. For example, if there is an `ssl` folder under `/nsconfig`, exclusions can be provided as: `ssl/abc.pem`
- File differences outside `/nsconfig` are not considered as part of the Config Audit diff.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To exclude files from Config Audit, perform the following steps:

1. Navigate to **Infrastructure > Configuration > Configuration Audit**.
2. Select **Settings**.
3. Under **NetScaler Config File Settings**, add the file paths you want to exclude from auditing.
4. Click **Save**.

Instance-level RBAC support for LAS

NetScaler Console on-prem now supports Role-Based Access Control (RBAC) at the instance level for LAS. Previously, administrators had access to licensing for all devices, which could lead to security risks and operational overhead. This enhancement allows administrators to grant restricted access to specific NetScaler instances. As a result, an administrator manages licensing only for the specific NetScaler instance they are authorized to access. This change ensures that licensing tasks follow the same security boundaries as other management activities in NetScaler Console on-prem.

Some of the benefits are:

- **Improved security**: Limits licensing actions to only the scoped devices assigned to an administrator.
- **Granular operational control**: Ensures that administrators cannot inadvertently modify licensing for unauthorized instances.
- **Workflow alignment**: Integrates licensing management seamlessly with established RBAC structures.

Related topics:

- For information on how to configure RBAC, see Role-based access control.
- For information about license management, see License management.

Fixed issues

Analytics

In HA setup, secured applications with WAF or Bot policies might intermittently disappear from the ADM Security Dashboard after the scheduled EMON polls. This issue occurs due to an internal data correlation mismatch.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infrastructure

NetScaler FIPS appliances might not be able to connect to NetScaler Console service in Government Cloud using the built-in agent.

Under **Tasks and Recommendations**, after selecting a security advisory task, clicking **View and Remediate** for the selected CVE or an affected instance loads an empty page.

During the LAS migration workflow, the NetScaler Console service UI might fail to display host names for HA pairs managed by an internal agent.

In an HA setup of NetScaler instances registered with Console service using a built-in agent, release allocation might fail for these instances when the agent_id is missing.

March 23, 2026

Management and Monitoring

Support for identification and remediation of CVE-2026-4368

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2026-4368.

- Identification for CVE-2026-3055 requires version scan. Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix. For more information, see Remediate CVE-2026-4368.

  NOTE:

  Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

- For more information about using NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.
- For more information about the CVE, see Security Bulletin.

Support for identification and remediation of CVE-2026-3055

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2026-3055.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Identification for CVE-2026-3055 requires version scan. Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix. For more information, see Remediate CVE-2026-3055.

  NOTE:

  Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

- For more information about using NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.
- For more information about the CVE, see Security Bulletin.

March 09, 2026

What's new

Management and Monitoring

- **AES encryption for PEM-formatted private keys**

  NetScaler Console service now supports Advanced Encryption Standard (AES) as a PEM encoding algorithm when you create a Certificate Signing Request (CSR). When generating a CSR and creating a new private key, you can select AES256 to encrypt and protect the PEM-formatted private key, providing a more secure alternative to the existing DES and 3DES options. This enhancement ensures that private keys are protected using modern, industry-standard cryptographic algorithms.

  The following are the benefits:

  - **Enhanced security**: Provides stronger encryption for private key protection compared to legacy DES-based methods.
  - **Compliance alignment**: Helps organizations meet modern security best practices and regulatory requirements that mandate AES-based encryption.
  - **Future-proofing**: Aligns CSR generation with contemporary cryptographic standards widely adopted across the industry.

  For information related to configuring the PEM encoding algorithm during CSR generation, see Create a Certificate Signing Request (CSR).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Miscellaneous

- **Flexible scheduling options for secondary HA node upgrades**

  Under **Infrastructure > Upgrade Jobs**, when creating a job, you can specify a delay (in hours) after the first node upgrade completes before the second node upgrade begins. This option is useful in the following scenarios:

  - Additional time is needed to test and validate the first node
  - Upgrade progression depends on operational readiness rather than a fixed clock time
  - Need flexibility without manually rescheduling the task

  Previously, only defining a fixed time-stamp option was available. With only the fixed time-stamp option, if the first node upgrade got delayed, the scheduled time of the second node would elapse, and the upgrade would never begin.

Fixed Issues

Analytics

- The WAF Recommendation option might not be visible in the NetScaler Console service GUI when configuring RBAC policies.

- On the **Analytics** page, users might see all the instances instead of seeing only the specific instances that have been authorized for access based on the User, Role, Group and Access Policy defined for that particular user.

Infrastructure

- After upgrading NetScaler Console on-prem to version 14.1-60.54, the telemetry status for all SDX appliances might display 2500 and 3300 internal errors.

- NetScaler Console agent continuously crashes after an upgrade due to a POCO library upgrade.

- NetScaler Console service certificate synchronization might fail with an HTTP 28 error. This issue occurs when the Zero-Touch feature is enabled and the request times out at 10 seconds before the Console can respond, breaking the synchronization process.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Miscellaneous

NetScaler Console service does not support licensing a NetScaler VPX at 20 Mbps by using LAS based licensing.

```
[ NSHELP-42109 ]
```

February 20, 2026

What's new

Removal of few pre-upgrade validation checks

The following NetScaler Console pre-upgrade checks are removed from the Upgrade Jobs workflow:

- **User Customizations Check**: Existing user customizations check, including startup scripts and cron jobs, that might affect system behavior during or after installation.
- **HDD Errors Check**: System and kernel log checks for disk-related errors, I/O failures, timeouts, and filesystem issues that might impact installation stability.
- **High Availability (HA) Configuration Check**: Configuration synchronization check between HA nodes.

The preceding checks are outdated and resource-intensive. The removal of these checks improves upgrade performance, reduces system overhead, and minimizes false upgrade failures, while all critical validation checks remain in place.

For more information on pre-upgrade checks, see Upgrade jobs.

Fixed Issues

Infrastructure

The severity of the CVE is not shown on the CVE view page under **Security Advisory**.

A decimal validation error might occur during bandwidth allocation when configuring LAS Licensing for NetScaler MPX and SDX platforms. This issue occurs when a limited number of license editions are available for allocation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

February 04, 2026

- **Categorization of pre-upgrade checks in NetScaler Console service**

  Pre-upgrade checks in NetScaler Console for NetScaler upgrades using upgrade jobs are now grouped into the following categories:

  - Critical: Upgrade is blocked.
  - Warning: Upgrade is allowed with administrator approval.
  - Advisory: Upgrade is allowed with administrator approval.

  For more information, see Pre-upgrade validation.

- **Mandatory time parameter for generating technical support files**

  Specifying a time is now mandatory for generating technical support files. You must explicitly choose a time reference when generating a technical support file. You can either select the custom option and specify a custom date and time or use the Now option. The "now" option uses the current system time. This enhancement ensures that the exact time context is explicitly defined.

  For more information, see How to generate a technical support bundle for a NetScaler instance.

- **Upgrade Jobs: A warning is displayed when selected instances are already on the target build**

  To help prevent selection of incorrect instances during upgrade jobs, a warning is displayed if you select instances that are already running the target build. This enhancement helps avoid unnecessary upgrades. If you intend to reupgrade the instances, you can safely ignore the warning and proceed.

- **Instance group visibility and mapping enhancements**

  The **Instance View** tab is introduced under the **Instance Group** page to improve visibility and management of instance groups. The **Instance View** tab is a centralized view that provides:

  - A consolidated list of all managed NetScaler instances
  - Visibility into the instance groups each instance is associated with
  - Clear identification of instances not mapped to any instance group
  - Improved instance identification using both host name and IP address

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Administrators can quickly add unmapped instances to instance groups and identify instances already assigned to prevent duplicate mappings, resulting in simpler and more efficient instance group management.

To view the instance view, navigate to **Infrastructure> Instances Dashboard> Instance Groups> Instances View**.

For more information, see https://docs.netscaler.com/en-us/netscaler-console-service/networks/instance-management/create-instance-groups.

- **File integrity monitoring: Ability to create an exclude list for scans**

  You can create a custom allow list and exclude specific files from file integrity monitoring scans. By defining which files to exclude from the scan, you can streamline monitoring and reduce unnecessary alerts for trusted files. Previously, certain files were incorrectly identified as malicious during file integrity monitoring scans, even though they were not malicious.

  For more information, see https://docs.netscaler.com/en-us/netscaler-console-service/instance-advisory/file-integrity-monitoring%23console-detected.

- **Support for binary signing and verification**

  NetScaler Console service now supports binary signing and verification. This feature enhances security by providing a mechanism to detect and prevent the execution of unauthorized or tampered files on your NetScaler instances. Whenever there is an attempt to run an unauthorized file on NetScaler, a real-time SNMP trap is sent to NetScaler Console and flagged.

  To view the list of NetScaler instances that have reported issues using binary signing and verification, navigate to **Infrastructure > Instance Advisory > Security Advisory**, click **File Integrity Monitoring**, and view the **Device-Reported** tab.

  For more information, see File integrity monitoring.

Miscellaneous

- **On-Demand LAS entitlement synchronization**

  Previously, console-compatible entitlements were synchronized with the License Activation Service (LAS) only once every 24 hours. The new Sync Licenses option allows you to manually trigger this synchronization on demand, ensuring entitlements are up to date immediately.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For information related to LAS, see License Activation Service.

Fixed Issues

Infrastructure

- When you perform a bulk upload of certificates and keys, the GUI confirms a "Successfully Uploaded" status . However, the certificates do not appear in the Zero-Touch view.
- The **Security Advisory Dashboard** might display an incorrect **Next Scheduled Scan** date that does not match the defined **Scheduled Scan Frequency**.
- The DNS challenge might fail during ACME certificate issuance when DNS providers do not respond within the ten-second timeout. This issue occurs due to slow API responses, high network latency, or significant DNS propagation delays.
- Some NetScaler files generated during the upgrade process might be incorrectly flagged as vulnerable by the File Integrity Monitoring scans.
- The Diagnostics status for the NetScaler Agent is incorrectly shown as "Needs Review" in the NetScaler Console Service on Citrix Cloud Japan, even though Japan cloud-related URLs are accessible.
- The NetScaler Console Security Advisory displays an incorrect secure configuration recommendation regarding insecure SSL protocol versions. The recommendation indicates TLS 1.0 and TLS 1.1 are in use for non-primary default profiles even when those protocols are disabled.
- StyleBook config pack operation might fail with an RBAC authorization error if the target instance is an HA pair on which SNIP is configured for management access.
- The NetScaler Cloud API might fail to proxy requests to the NITRO systemfile endpoint. As a result, API calls might fail.
- Email notifications for NetScaler Console SSL certificate expiry events might fail.
- All remote certificates issued by the Automated Certificate Management Environment (ACME) in NetScaler Console are removed from NetScaler if the number of certificates exceeds 20.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Licensing

- In the **LAS Licensed** table under **License Management**, the host name for instances might not be displayed.
- For the Pooled or Flexed license type, the Console on-prem GUI displays the entitlement blob renewal date information. However, it does not alert or send proactive notifications about entitlement blob expiry. Customers are advised to monitor the entitlement blob expiry date displayed in the GUI and renew it before it expires to ensure uninterrupted functioning of the product.

Miscellaneous

- In rare cases, virtual servers on NetScaler might intermittently go down during zero-touch certificate management deployments.
- Migration of NetScaler instances to LAS-based licensing fails when an instance is added using an FQDN instead of an IP address.
- While using LAS licensing based only on pooled entitlements (excluding UHMC/CPL), the **LAS Managed Entitlements** tab of the **Pooled Licensing** dashboard might not display the SDX devices.

StyleBooks

- Editing the resource binding on an existing StyleBook Configpack fails.

November 11, 2025

Management and Monitoring

Support for identification and remediation of CVE-2025-12101

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2025-12101.

- Identification for CVE-2025-12101 requires version scan. Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix. For more information, see Remediate CVE-2025-12101.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

- For more information about using NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.
- For more information about the CVE, see Security Bulletin.

November 06, 2025

Fixed issues

Infrastructure

After a restart, the NetScaler Console on-prem Security Advisory Scan frequency gets incorrectly set to 7 days instead of 24 hours.

Miscellaneous

The **Licensed NetScaler instances** section, under **Pooled Licensing > Throughput Capacity > LAS managed entitlements**, might not display any devices when a customer uses only pooled licenses and does not have flexed licenses.

October 15, 2025

Management and Monitoring

ISSU migration completion in upgrade jobs

The upgrade jobs workflow now supports forceful In-Service Software Upgrade (ISSU) migration. When **Enable ISSU to avoid network outage on NetScaler HA pair** on the **Create Job** is selected, ISSU automatically triggers complete migration after the customer-defined delay period.

During ISSU, NetScaler typically waits for the active connections to close naturally before completing the migration. Sometimes, long-lived connections can delay or block completion. With this enhancement, NetScaler Console triggers forceful ISSU migration by terminating long-lived active connections. Critical management sessions (CLI, GUI, Console) are excluded to ensure uninterrupted administrative access.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Benefits:

- Faster, more predictable ISSU completion.
- Reduced operational delays and failures caused by long-lived connections.
- Improved reliability in upgrade and rollback workflows.

Scenarios supported:

- Migration is in progress and waiting for connections to close.
- Rollback is in progress and waiting for connections to close.

Fixed issues

Infrastructure

Users might not receive email notifications for SSL certificates approaching their expiry date, even though the certificate expiry notification settings are configured correctly.

Some NetScaler instances are incorrectly flagged as vulnerable by File Integrity Monitoring due to the inclusion of non-relevant files in the scan.

The banner displayed on the **Security Advisory > Scan history** page contains incorrect information.

September 17, 2025

Infrastructure

Automated certificate renewal by using the ACME protocol

NetScaler Console now supports the Automated Certificate Management Environment (ACME) protocol to simplify SSL/TLS certificate lifecycle management.

Support for the ACME protocol has the following benefits:

- Prevents downtime by renewing certificates before expiry.
- Reduces manual effort with automated tracking and renewals.
- Ensures stronger security with always-valid, CA-compliant certificates.

NetScaler Console supports ACME Client acme.sh and certificate renewal integration with the following CA vendors:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Let’s Encrypt
- DigiCert

All DNS providers supported by the acme.sh client are also supported by the console for DNS validation.

The following points describe the high-level ACME communication flow:

- NetScaler® Console, acting as the ACME client, sends a request to the ACME server (CA) for a new certificate or renewal.
- The CA initiates a DNS-01 challenge.
- NetScaler Console adds the TXT record with the token provided by CA to the configured DNS provider.
- The CA queries the DNS provider to verify domain ownership.
- On successful validation, the CA issues the certificates.

For more information, see Automated certificate renewal by using the ACME protocol.

Fixed issues

Infrastructure

Historical data might be deleted for some customers with a free license.

Loading configuration jobs is delayed when they are associated with multiple device groups and contain large command sets.

Users might encounter the following issues:

- An **Invalid Resource** error message, when they click **Console on-prem telemetry upload**.
- An **IP address already exists** error message, when they try to create a new profile.

Platform

NetScaler with multiple PEs might incorrectly be flagged as vulnerable with CVE-2021-22956 when scanned from NetScaler Console.

StyleBooks

The config pack update might fail if the pack contains a NetScaler Access Control List that uses a source IP address dataset or a destination IP address dataset.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

September 08, 2025

Licensing

LAS Enforcement on NetScaler and NetScaler Console Service

File-based licensing system (also referred to as ‘manually managed entitlements’), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version. The minimum required NetScaler versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.80, 13.1-60.29, 13.1-37.247 (FIPS)
- NetScaler SVM: 14.1-51.83, 13.1-60.30
- NetScaler Console Service: Supported from early September 2025.
- NetScaler Console on-prem: 14.1-51.83

  Note: LAS support for Console on-prem is from release 14.1-51.83 onwards. However, file-based licensing deprecation/EOL is from Console on-prem release 14.1-51.83 onwards and Console on-prem release 13.1-60.26 onwards.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.

LAS based licenses may not be available to customers where prohibited by law or regulations.

Should you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don't apply where prohibited by law or regulation.

LAS support for NetScaler Console Service

NetScaler console service now supports the License Activation Service (LAS) licensing mechanism. LAS is a new cloud-based licensing solution that offers a modern alternative to

© 1997–2026 Citrix Systems, Inc. All rights reserved.

traditional file-based licensing. LAS introduces new modules for the activation of Citrix and NetScaler products, ensuring a seamless and modern approach to license management.

NetScaler Console Service is now automatically License Activation Service (LAS) enabled. You can view your NetScaler Flexed and Pooled license entitlements by navigating to: **Licenses > License management > License Activation Service (LAS)**.

NetScaler version compatibility for LAS To use LAS, your NetScaler must be running one of the following minimum versions or later:

- NetScaler ADC: 14.1 build 51.x, 13.1 build 60.x, 13.1 build 37.x (FIPS)
- NetScaler SVM: 14.1 build 51.x, 13.1 build 60.x

NOTE:

LAS for NetScaler Console Service supports NetScaler Flexed licenses (CPL/UHMC) and (legacy) NetScaler Pooled licenses. All other forms of legacy NetScaler licenses, such as Pooled vCPU, CICO are not supported with LAS. For more information, see LAS support for Console Service..

September 03, 2025

Fixed issues

Infrastructure

The NetScaler Throughput graph is removed from the admin partition dashboard due to the lack of support for the required "ns" counter group within the admin partition.

August 26, 2025

Management and Monitoring

Support for identification and remediation of CVE-2025-7775

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2025-7775.

- Identification for CVE-2025-7775 requires a custom scan. In this scan, the NetScaler Console connects to the managed NetScaler instance and pushes a script. The script runs on the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

instance to check the pre-condition for the CVE. If the pre-condition is met, a version check is performed on the NetScaler. Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix. For more information, see Remediate CVE-2025-7775.

NOTE:

Security Advisory does not support NetScaler® builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

- For more information about using NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.
- For more information about the CVE, see Security Bulletin.

Support for identification and remediation of CVE-2025-7776

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2025-7776.

- Identification for CVE-2025-7776 requires a combination of version scan and configuration scan. Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix. For more information, see Remediate CVE-2025-7776.

NOTE:

Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

- For more information about using NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.
- For more information about the CVE, see Security Bulletin.

Support for identification and remediation of CVE-2025-8424

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2025-8424.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Identification for CVE-2025-8424 requires version scan. Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix. For more information, see Remediate CVE-2025-8424.

  NOTE:

  Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

- For more information about using NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.
- For more information about the CVE, see Security Bulletin.

August 20, 2025

Infrastructure

Support to opt in or opt out of security scans

You can now customize your security scanning preferences by choosing to opt in or opt out of security scans. Additionally, you can select specific types of scans to include as part of your security assessment. By default, only Common Vulnerabilities and Exposures (CVE) scans are enabled.

To configure security scan settings:

1. Navigate to **Instance advisory > Security Advisory**.
2. Click the settings icon in the top right corner.
3. Under **Configure System Scan**, select the types of scans you want to include.
4. Click **Save**.

File integrity monitoring in system scans

You can now enhance your security posture by including file integrity monitoring as part of your system scans. File integrity monitoring enables you to identify if any changes or additions are made to your NetScaler file system.

To enable file integrity monitoring:

1. Navigate to **Instance advisory > Security Advisory**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Click the settings icon in the top right corner.
3. Under **Configure System Scan**, select **File Integrity Monitoring Scan**.
4. Click **Save**.

Fixed issues

Infrastructure

The **Instance Advisory > Security Advisory> CVE Detection > Switch to CVE View** page might display incorrect severity levels for some CVEs.

July 17, 2025

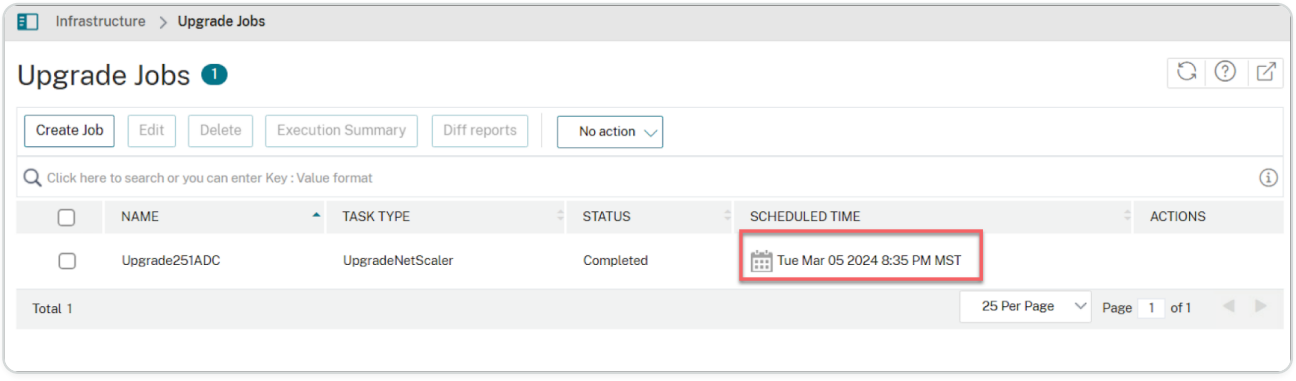
Infrastructure

Time stamp includes time zone information

In the NetScaler Console service GUI where the time stamp is displayed, you can now see the time zone information as well. The time zone is shown based on the time zone selected under **System Settings**. Depending on your configuration, the time zone is displayed as GMT, your local time zone, or UTC (if the local abbreviation is unavailable).

Previously, the time stamp did not display time zone information. With this enhancement, you get clearer and more accurate time stamp details for scheduled jobs.

For example, the following figure displays a scheduled time that includes the time zone.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

Infrastructure

PDF report generation for Secure Config Recommendations feature under **Infrastructure > Instance advisory > Security Advisory** might fail if a single category includes a large number of recommendations.

The **Last Scan Time** field in the **Security Advisory** dashboard does not display the timestamp of the most recent CVE scan.

July 02, 2025

Telemetry

New validation for telemetry data

As part of the NetScaler telemetry program, you must upload your telemetry data at least once every 90 days. The NetScaler Console service now verifies that the latest file in the uploaded payload is within 90 days. If the file is older than 90 days, the upload is rejected. This new validation check ensures that your uploaded telemetry data is up-to-date and compliant.

If your upload is rejected:

1. Download a fresh payload from your Console on-prem.
2. Upload it again.

Removal of telemetry analytics profile from the managed NetScaler instance

The following telemetry metrics profile configuration is no longer required for telemetry collection:

```
add analytics profile telemetry_metrics_profile -type timeseries -outputMode prometheus -metrics ENABLEd -serveMode Pull -schemaFile "./telemetry_collect_ns_metrics_schema.json" -metricsExportFrequency 300
```

As part of the NetScaler telemetry program, the telemetry metrics profile configuration was pushed to the managed NetScaler instances.

NetScaler Console automatically removes this configuration from your NetScaler instances on July 19, 2025, if it still exists. Alternatively, you can manually remove the configuration at any time by using the following command:

```
rm analytics profile telemetry_metrics_profile
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For information about telemetry metrics profile configuration, see NetScaler telemetry program.

Security

Security advisory dashboard enhancements

The Security Advisory dashboard is enhanced and designed to provide administrators and security professionals with immediate insights into the overall health and vulnerability status of their NetScaler infrastructure.

The dashboard offers a comprehensive bird’s-eye view of your NetScaler deployment’s security posture. The key features include:

- A consolidated dashboard displaying active security advisories.
- Summary of affected devices.
- A clear breakdown of potential risks.

You can quickly identify critical vulnerabilities, secure configuration recommendations including mitigation steps, and links to relevant documentation.

For more information, see Security Advisory

Fixed issues

Analytics

Even after editing an API definition and saving the changes, NetScaler Console service fails to update the API definition and incorrectly displays the "Update Successful" notification.

In **HDX™ Insight > Users**, when you drill down to view details under **Current Sessions**, the details appear with the incomplete report when the VDA that is connected to NetScaler is missing.

Infrastructure

The number of instances displayed under the **Instances on older build summary** section of **Upgrade Advisory** is incorrect.

When NetScaler is upgraded from NetScaler Console, the system fails to send the upgrade status as an email PDF attachment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

June 25, 2025

Management and Monitoring

Support for identification and remediation of CVE-2025-6543

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2025-6543.

- Identification for CVE-2025-6543 requires a combination of version scan and configuration scan. Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix. For more information, see Remediate CVE-2025-6543.

  NOTE:

  Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

- For more information about using NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.
- For more information about the CVE, see Security Bulletin.

June 17, 2025

Management and Monitoring

Support for identification and remediation of CVE-2025-5349 and CVE-2024-5777

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2025-5349 and CVE-2025-5777.

- Identification for CVE-2025-5349 requires a combination of version scan and configuration scan. Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix. For more information, see Remediate CVE-2025-5349.
- Identification for CVE-2025-5777 requires a version scan, and remediation requires a two-step process:

  a. Upgrade the vulnerable NetScaler instance to a release and build that has the fix.

  b. Apply configuration jobs.

  For more information, see Remediate CVE-2025-5777.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

- For more information about using NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.
- For more information about the CVE, see Security Bulletin.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2025-5349 and CVE-2025-5777 in the security advisory module. To see the impact sooner, you can start an on-demand scan by clicking **Scan Now**.

June 03, 2025

Fixed issues

Analytics

When you export data for analytics, such as security violations, Gateway Insight, and HDX Insight, the exported CSV report previously contained only 5000 entries. With this update, the limit is increased to 10,000 entries.

Infrastructure

The NetScaler agent intermittently uses the proxy password in an incorrect format while communicating with NetScaler Console service through a proxy server.

When you configure notification settings in **Settings > System Events > Notifications** by selecting multiple categories and clicking **Save**, the changes are not saved.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

May 26, 2025

Analytics

Enhanced HDX Insight visibility at the VPN virtual server level

HDX Insight now allows you to monitor key metrics such as active sessions, desktops, and launched applications at the VPN virtual server level. A new option **Gateway Virtual Servers** is now available under **Gateway > HDX Insight**.

As an administrator, this enhancement enables you to:

- View a list of all virtual servers under **Gateway > HDX Insight > Gateway Virtual Servers**.
- Select a virtual server to access a comprehensive report that provides granular visibility and simplifies performance monitoring specific to that virtual server.

Previously, detailed end-user experience reports were only available at the NetScaler instance level.

Support to view Web Insight analytics for IPv6 virtual servers

You can now view Web Insight analytics for virtual servers that are configured with an IPv6 address. Earlier, Web Insight was not supported for IPv6 addresses. As an administrator, this enhancement provides various details in Web Insight that enable you to analyze and improve the virtual server performance.

For more information, see Web Insight.

Centralized GeoIP DB Updates through NetScaler Console

NetScaler Console allows administrators to upload the GeoIP DB file from MaxMind directly through the NetScaler Console. You can either push the GeoIP DB file immediately to managed NetScaler instances or schedule the update for a later time. These files are essential for accurate IP-to-location mapping, commonly used in GSLB and security policies.

Previously, NetScaler did not have a centralized mechanism for managing GeoIP DB (Geolocation Database) updates on NetScaler. Administrators had to perform the updates manually on each device, which was time-consuming, error-prone, and disruptive in production environments.

This enhancement provides the following benefits:

- Automation: The update process is automated and performed without scheduled downtime and therefore reduces operational overhead.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Effective scalability: Managing updates across multiple NetScaler instances is efficient and easy to scale.
- Version check: If an issue arises, you can track the historical versions, upload, and sync an older GeoIP DB file.

For more information, see Centralized GeoIP DB Updates through NetScaler Console.

Fixed issues

Analytics

- Some processes in NetScaler agent crash and generate core files. As a result, the disk space is full.
- Export of more than 1 MB data from NetScaler Console to Microsoft Sentinel fails.
- In Web Insight, when you click an application to view the anomalies under **Application Metrics**, the client network latency from the **Response Time** tab shows incorrect details.

May 06, 2025

Fixed issues

Cloning a StyleBook might fail with the following error if any StyleBook definition includes the import-stylebooks section that is empty or lacks defined imports:

'NoneType' object is not iterable

Importing a StyleBook definition might fail when StyleBook definition includes an expression that references an output from a component.

Upgrading a NetScaler from NetScaler Console fails due to a corrupted build image. Due to a network issue during image upload, the build image gets corrupted. To detect and prevent discrepancies during file transfer, you can enable checksum verification for the uploaded build image.

In some scenarios, notifications are not triggered when the event status changes. The logs are generated, but the event action is not performed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

April 15, 2025

Zero-touch certificate deployment

You can now configure zero-touch certificate on the managed NetScaler instances running build 14.1-43.x and later. With zero-touch certificate deployment, you can eliminate manual intervention and build the in-memory zero-touch certificate store to serve the application requests. Navigate to **SSL Dashboard > Zero-touch certificate management** to upload all the certificates and keys on NetScaler Console, select the NetScaler instances, and then click **Enable**. After uploading certificates and enabling zero-touch certificate management on the NetScaler instances, NetScaler periodically polls the certificate repository and gets the required certificates.

Previously, in the SSL dashboard, you could only minimize the manual intervention of installing the SSL certificate on each instance.

For more information, see:

- NetScaler zero-touch certificate management
- NetScaler Console zero-touch certificate management

Deprecation of autoscaling of NetScaler instances in public clouds

Autoscaling of NetScaler instance configuration in public clouds is no longer available in NetScaler Console.

Improvements to Configuration Jobs

NetScaler Console now sends the output of show commands, added in Configuration Job, through Email and Slack.

Improvements to Upgrade Jobs

In **Infrastructure > Upgrade Jobs**, when you create a job to upgrade NetScaler in a high availability by using a two-stage upgrade process, you can now delay the HA failover until the start of the second node upgrade.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

Infrastructure

In Configuration Job, when you create a job using the file upload option, the following error message appears: `File upload not allowed. Max file size 15 MB`

The maximum allowed file size for a configuration job is 2GB.

Service to service DeviceAPIProxy calls fail to get the results for the "systemfiles" NITRO call from NetScaler.

In **Infrastructure > Configuration > Configuration Audit > Audit Templates**, the preview of an audit template fails if variables are defined in the template commands.

In NetScaler Console, a new notification channel for Slack cannot be used to schedule exports until March 2025. The existing Slack channels can be used to schedule exports until then, after which a new channel must be created.

The following scopes are required in an app:

- channels:read
- groups:read
- im:read
- mpim:read

For more information, see the Slack documentation.

February 19, 2025

StyleBooks

Support for accessing privately-hosted GitLab/GitHub repositories and Infoblox IPAM

NetScaler Console service StyleBooks now allows you to import and synchronize StyleBooks and Configpacks from GitLab/GitHub repositories that are privately hosted and are accessible only within an enterprise’s intranet.

NetScaler Console service IPAM now allows you to register a privately hosted Infoblox DDI server as an external IPAM provider.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Previously, only publicly accessible GitLab/GitHub repositories and Infoblox DDI servers were supported.

For more information, see Import and synchronize StyleBooks from an external repository and Configure IP address management (IPAM).

Fixed issues

Analytics

To comply with unlimited VIPs, the Subscription details are removed in **Settings > Analytics Configuration**.

February 06, 2025

Analytics

Enable Web transaction analytics at the virtual server level

You can now enable Web transaction analytics at the virtual server level. To do so, when you enable analytics for a virtual server, you must select the new Detailed Web Transactions option to enable the Web transaction analytics.

Earlier, when you enabled analytics for a virtual server, Web transaction analytics was automatically enabled.

For more information, see Web transaction analytics.

Infrastructure

Disable notifications for managed devices during maintenance and troubleshooting windows

Administrators can temporarily disable notifications for specific managed devices during maintenance and troubleshooting windows. This enhancement avoids receiving unnecessary alerts and notifications concerning device-specific issues and status updates during these intervals.

To disable notifications, navigate to **Settings > Administration > Instance Settings > Notification Disable Windows** and add the required details. For more information, see Instance Settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

Infrastructure

In **Job Template**, the following error is displayed while importing the configuration job template using the **Import** button:

`Invalid resource`

January 15, 2025

Telemetry

Changes to Console on-prem telemetry upload

You must now create a profile for each NetScaler Console on-prem instance for uploading the telemetry file to the NetScaler Console service. You might have multiple NetScaler Console on-prem instances deployed globally. By creating a profile for each on-prem instance, you can upload the telemetry file for those on-prem instances and monitor the upload deadline separately.

To create a profile, navigate to **Settings > Console on-prem telemetry upload** and click **Create Profile**.

NOTE:

If you are an existing Console on-prem user and have previously uploaded the telemetry file to the Console service, you must create a new profile and then upload the telemetry file. After creating the new profile, you might observe a discrepancy between the Console on-prem deadline and the Console service deadline. Ensure that you upload the telemetry file to NetScaler Console service on or before the due date that is shown in your Console on-prem. This discrepancy is aligned after you complete one upload using the new profile.

For more information, see Console on-prem upload.

Analytics

Support to enable custom header in analytics settings to fetch the client IP address

When you enable analytics for an application you can now define a custom header, such as X-Real-IP, X-Client-IP, or any other custom header, to fetch the actual client IP address instead of the proxy IP address. The custom header option allows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Compatibility with diverse network proxies that use various headers.
- Accuracy to get the actual client IP address in a complex network environment with multiple layers of proxies.
- Additional security measures than those provided by the standard headers.

Sort and search support in custom dashboard

In Custom Dashboard (**Overview > Custom Dashboard**), you can now use the:

- Sort option to display the custom dashboards alphabetically.
- Search option (both plain text and regular expression) to narrow down the search results.

Infrastructure

Hostname in system event email notifications

NetScaler Console now includes the hostname of associated NetScaler instances in system event email notifications.

StyleBooks

Import and synchronize StyleBooks from GitLab external repository

StyleBooks now support the import and synchronization of StyleBooks and configuration packs from GitLab repositories. Previously, this feature was only available for GitHub repositories.

For more information, see: Synchronize external repository

Selecting multiple items from a StyleBook data source

You can now create StyleBooks that allow users to select multiple items from a data source parameter. StyleBooks now support a datum array as a parameter type, enabling users to select a list of data sources or collection items as input.

For more information, see: Manage StyleBook data sources.

Support a filter for data source collections

StyleBooks now allow you to specify a collection filter for a data source parameter. While providing input for such a parameter in a config pack operations, users will only see and be able to select items from the filtered collection, rather than from all items.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information, see: Built-in data source, Custom data source

Fixed issues

Analytics

- In **Settings > Observability Integrations**, editing or deleting a subscription might fail if a NetScaler command failure occurs.
- In **HDX Insight** and **Web Insight**, the Geolocation report does not resolve the client IP location for the defined IP block.

Infrastructure

- When a user with all default roles in the NetScaler Console attempts to generate the activation code for registering an agent, the action fails with the error **Not Authorized to perform this operation**.
- When a non-nsroot user tries to view the statistics for a specific virtual server in Network Functions (**Infrastructure > Network Functions**), an error message is displayed.

StyleBooks

- When you deploy a config pack on a NetScaler HA pair and a failover occurs, attempting to update the config pack with the instance ID of the new primary fails.
- When you delete a config pack that includes a policy dataset referenced by the Access Control List of NetScaler, and resource reuse is enabled for the associated StyleBook, the policy dataset remains stale in NetScaler.
- When you edit config packs in **Applications > Configurations > Config Packs**, the order of added items is not retained.

December 03, 2024

Sharing configuration entities between migrated configurations

You can now reuse configuration entities when migrating configurations using the **Config Migration** utility. Subsequent migrations successfully reuse existing configuration entities on the target ADC that were created by earlier migrations. Previously, the migration of configurations

© 1997–2026 Citrix Systems, Inc. All rights reserved.

failed with an error **Resource already exists** when migrating two configurations that shared some configuration entities.

For more information, see: Simplified migration using StyleBook

Migrate analytics from policy-based to profile-based configuration

When you enable analytics on virtual servers, the analytics are now applied through profile-based configuration. Earlier, analytics was configured through an AppFlow® policy. The profile-based configuration has the following benefits:

- Improved performance and flexibility
- Easier configuration and management

Enhancements related to analytics configurations are supported only in profile-based configuration. We recommend that you migrate all your existing virtual servers that are enabled for analytics to profile-based configuration.

Navigate to **Settings > Analytics Configuration** and then select **Migrate Analytics**

For more information, see Migrate analytics.

Fixed Issues

Analytics

- In **Web Insight**, the data is not visible if the custom date range is more than one day.

Infrastructure

- NetScaler Console fails to generate a Certificate Signing Request (CSR) from the SSL dashboard.
- When you update the permissions in Identity and Access Management (IAM) for an Azure group, the changes are not reflected in NetScaler Console.
- DeviceAPIProxy calls fail to get the results for the "systemfiles" NITRO call from NetScaler.
- The **PINNED** menu list is visible only when the first level of the menu is expanded in the enhanced GUI of NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBooks

- Attempting to configure a Link Aggregation Control Protocol (LACP) channel using a StyleBook config pack fails.
- Force deleting a configpack fails if it is missing mandatory parameters.
- When you update a StyleBook definition, draft and scheduled configpacks are inadvertently deployed .
- When creating an RBAC policy for StyleBook configuration pack operations, **APIProxy** permissions must be selected manually . If they are not selected, the configuration pack fails.

November 20, 2024

Enhanced user experience in NetScaler Console GUI

The NetScaler Console service now offers an improved Graphical User Interface (GUI) for a better user experience. Key improvements include:

- **Hover-to-Display menu**: The primary menu tree structure is replaced with a hover-to-display feature for easier navigation. Secondary menu items appear when hovered over, displaying a submenu for quicker selection.
- **Streamlined menu hierarchy**: The menu hierarchy is now limited to a maximum of three levels, simplifying access to key options.
- **Updated submenu labels**: Submenu names are revised for options previously nested beyond the third level.
- **Collapsible menu**: The entire menu can now be collapsed or expanded by clicking an icon in the pane, providing more screen space.
- **Sidebar toggle**: A new toggle button on the breadcrumb allows you to hide or show the sidebar, optimizing the workspace.
- **Set home page**: You can now set a displayed page as your homepage by clicking the icon next to the submenu name.
- **Pin favorite items**: Easily pin your favorite menu items for faster access.

For more information, see Enhanced Graphical User Interface.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Option to delete SSL certificate from NetScaler

You can now delete an SSL certificate from NetScaler. Earlier, when you deleted the file from **Infrastructure > SSL Dashboard**, the certificate was removed only from the running configuration. The associated certificate file was not deleted from NetScaler.

For more information, see SSL Dashboard.

Fixed issues

Infrastructure

- When you update certificates using the certificate store (Infrastructure > SSL Dashboard > Certificate Store), NetScaler Console fails to update the intermediate certificates on NetScaler instances.
- If you have more than 1000 applications, NetScaler Console fails to respond and results in a high CPU usage when you:
  - Create a user group (**Settings > Users & Roles > Groups > Add**).
  - Assign specific applications by clicking **Add** in the **Authorization Settings** tab.
- When a read-only user logs in to NetScaler Console, the following error message appears:

  No or invalid session found.

StyleBooks

A config pack update fails when the order of the policy bindings that are initially configured by using the StyleBook config pack is reordered according to priority.

November 12, 2024

Management and Monitoring

Support for identification and remediation of CVE-2024-8534 and CVE-2024-8535

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2024-8534 and CVE-2024-8535.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Identification for CVE-2024-8534 requires a combination of version scan and configuration scan. Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix.
- Identification for CVE-2024-8535 requires a version scan, and remediation requires a two-step process:

  a. Upgrade the vulnerable NetScaler instance to a release and build that has the fix.

  b. Apply configuration jobs.

  For more information, see Remediate CVE-2024-8535.

  NOTE:

  Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

- For more information about using NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.
- For more information about the CVE, see Security Bulletin.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2024-8534 and CVE-2024-8535 in the security advisory module. To see the impact sooner, you can start an on-demand scan by clicking **Scan Now**.

October 15, 2024

Telemetry

NetScaler telemetry page in the NetScaler Console GUI

You can now view the NetScaler telemetry page in the GUI that has information, such as data collection, mode of telemetry, and prerequisites. You must only ensure that the prerequisites are met and no action is required for the telemetry data upload.

The NetScaler telemetry program for the mandatory telemetry data collection was introduced in NetScaler Console 14.1-28.x build.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Analytics

Improvements to SSL usage analytics in Web Insight

In **Web Insight**, the SSL usage analytics is now improved with better visibility on the key metrics, such as cipher, key strength, and protocols during the higher traffic scenarios. Earlier, the visibility of these key metrics during the higher traffic scenarios displayed only limited details.

SSL widget in custom dashboard

In the custom dashboard (**Overview > Custom dashboard**), you can now create dashboards to view metrics related to SSL configuration. For more information on creating a custom dashboard, see Create custom dashboards to view instance key metric details.

Fixed issues

Infrastructure

- In the **Infrastructure > SSL Dashboard**, the root and intermediate certificates in the SSL certificate chain are not displayed.
- In the **Infrastructure > SSL Dashboard**, the issuer of the publicly available certificates is incorrectly displayed as **Not Recommended**.
- In NetScaler Console, event messages containing between "**<"** and "**>"** are not displayed in the email body.
- In the security dashboard (**Security > Security Dashboard**), when you configure protections for the unsecured applications or modify protections, and click **Deploy**, the following error message appears:

  ```
  HTTP Error 502 while accessing the data endpoint: "Unified_appsec_profile"
  ```

October 03, 2024

Licensing

Troubleshoot Flexed/Pooled licensing related issues

In the Flexed or Pooled licensing dashboard, under **Licensed NetScalers**, you can now use the **Troubleshoot** option to view and analyze few licensing related issues. Some possible licensing

© 1997–2026 Citrix Systems, Inc. All rights reserved.

issues are communication from Console to the instances and availability of the License Server Agents (LSA). The **Troubleshoot** option provides the list of issue categories such as License server, LSA, Processes, Communication, and their status. As an administrator, if you find any licensing issues, you can analyze these categories and troubleshoot.

For more information, see Troubleshoot licensing issues.

StyleBooks

Enhanced Integration and Sharing of configuration in Migration Utility config packs

You can now integrate and reuse configurations across various migration config packs. Previously, configurations created outside the Migration Utility could not be reused across multiple config packs.

Points to note

Stricter HTTP header validation is implemented for the NetScaler Console service. API users are now required to use the correct Content-Type header.

Fixed issues

The issues that are addressed in Build Oct 03, 2024.

Analytics

- In **Security > Security Violations**, under **Application Overview**, the details for WAF security violations reported in NetScaler 14.1–21.38 appear blank after you:
  a. Select an application from the **Top Applications** reported under WAF to view more details.
  b. Click **See more** under **Violation details**.
  c. Under **Timeline Details**, click **+** and select all columns.

Infrastructure

- SNMP traps are not received after the MASTools HA device failover.

StyleBooks

- The configuration of ADC resources with mixed case naming, such as 'Interface', is not applied even if the StyleBook configpack operation succeeds.

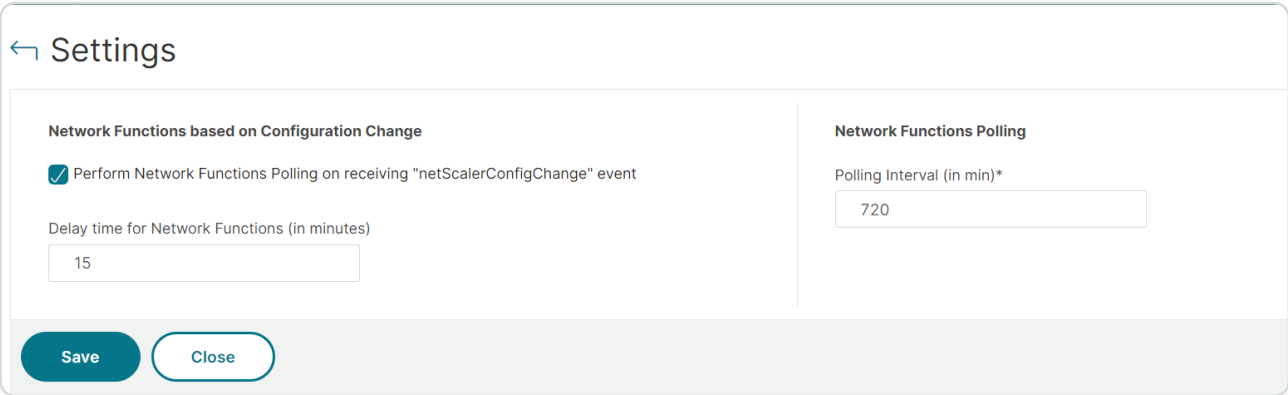
© 1997–2026 Citrix Systems, Inc. All rights reserved.

September 19, 2024

Infrastructure

Changes in Network Functions polling intervals

Along with the existing default polling interval for all NetScaler instances, NetScaler Console can now also poll selected NetScaler instances that have configuration changes earlier than the default poll cycle. With this enhancement, the default polling interval is now changed to 720 minutes. In **Infrastructure > Network Functions**, when you click **Settings**, you can now view a new option **Perform Network Functions Polling on receiving "netScalerConfigChange" event** under **Network Functions based on Configuration Change**. This option is enabled by default with a 15-minute interval in the **Delay time for Network Functions**.



Now, if a configuration change event occurs in NetScaler instances, NetScaler Console only polls these instances after the 15-minute interval.

NOTES:

- You can change the default polling interval (to poll all NetScaler instances) to a value between 30 minutes and 1440 minutes.
- You can change the default interval value of 15 minutes (to poll only selected instances) to a value between 5 minutes and 60 minutes.
- You can disable **Perform Network Functions Polling on receiving "netScalerConfigChange" event**. When disabled, NetScaler Console polls all the NetScaler instances according to the default polling cycle.

For more information, see Polling overview.

Fixed issues

The issues that are addressed in Build Sep 19, 2024.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infrastructure

The contents in the export report notification email are not compliant with RFC 5322.

StyleBooks

- Creating a configpack from a StyleBook definition that has `snmptrap_snmpuser_binding` fails with an error message list index out of range.
- When configuring a StyleBook, the GUID of the selected datasource is shown instead of its readable name in the input summary view.

September 03, 2024

Observability

View NetScaler Console audit logs data in observability tools (Splunk, New Relic, and Microsoft Sentinel)

When you create a new subscription in **Settings > Observability Integration** for the integration of NetScaler Console service with Splunk, New Relic, or Microsoft Sentinel, you can now select the **NetScaler Console Audit Logs** option. After you configure a subscription, you can view NetScaler Console audit logs in these observability tools.

For more information, see:

- Integration with Splunk
- Integration with New Relic
- Integration with Microsoft Sentinel

Fixed issues

The issues that are addressed in Build Sep 03, 2024.

Analytics

- In **Web Insight**, when you schedule export (tabular format) for a daily report, the report displays the same data everyday.
- In **Web Insight**, the data is not visible if the custom date range is more than one day.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

August 27, 2024

Analytics

Configure global analytics

You can now configure global analytics using custom and global policies.

- **Custom policy** - Using the custom policy, you can control instances or virtual servers that only require specific insights.
- **Global policy** - Using the global policy, you can configure and enable analytics on the existing managed virtual servers and any new virtual servers.

You can create up to 10 policies; nine custom policies and one global policy, or 10 custom policies. Navigate to **Settings > Analytics Configuration** and under **Global Analytics Summary**, click **Global Analytics Configuration** to configure a custom or global policy.

For more information, see Configure global analytics.

Applications

If you upgrade an application to A+ SSL rating, you can now revert to its original rating only within 7 days after the upgrade.

App Dashboard - Create and apply tags to applications (virtual servers)

In **App Dashboard**, you can now create and apply tags to applications. These tags improve the search functionality. After you create tags and you click the search bar, you can use the tags and refine the search.

For more information, see Create and apply tags to applications.

StyleBooks

Reuse configurations created outside of StyleBooks and share configurations between ConfigPacks

You can now integrate and manage configurations that were previously created outside of StyleBooks in NetScaler as part of Stylebook config packs. Additionally, you can now share configurations across multiple config packs, enabling more flexible and centralized management.

For more information, see Create and edit a config pack.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed Issues

The issues that are addressed in Build Aug 27, 2024.

Analytics

In **Web Insight**, the data is not visible for the virtual servers that have the same name across all the managed instances.

Infrastructure

- NetScaler Console memory utilization increases if the managed instances are configured with more than 10000 health monitors bound to the service groups. As a result, NetScaler Console might not be accessible.
- When provisioning the NetScaler agent or NetScaler VPX on Microsoft Azure, the NetScaler Console Provisioning service API fails to retrieve Azure subnet details.

July 25, 2024

Fixed issues

Infrastructure

In **Infrastructure > Upgrade Jobs**, when you upgrade a NetScaler instance that has classic policies, the pre-upgrade validation lists the instance as **Instances blocked from upgrade**, and the upgrade does not happen.

Workaround: Before upgrading an instance, we recommend that you convert the classic policies to advanced policies for the features that are supported by the NSPEPI tool. For more information, see Upgrade considerations for configurations with classic policies.

Telemetry

As part of the NetScaler telemetry program, NetScaler Console no longer checks for the following configuration every 24 hours or pushes it to NetScaler instances. Earlier, the configuration was checked every 24 hours and pushed to NetScaler instances, if it was missing:

```
enable ns feature AppFlow

add analytics profile telemetry_metrics_profile -type timeseries
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-outputMode prometheus -metrics ENABLED -serveMode Pull -schemaFile "./
telemetry_collect_ns_metrics_schema.json" -metricsExportFrequency 300
```

July 15, 2024

Infrastructure

Support for 3072 bits encryption key in the NetScaler Console SSL dashboard

You can now configure an enterprise policy with the key strength of 3072 bits for your certificate. In **Infrastructure > SSL Dashboard > Settings > Enterprise Policy > Recommended key strengths**, select a 3072-bit encryption key. Previously, only key strengths of 512, 1024, 2048, and 4096 bits were available.

For more information, see:

For NetScaler Console service: Configure an enterprise policy For NetScaler Console on-prem: Configure an enterprise policy

View and export NetScaler-owned IP addresses in the NetScaler Console GUI

You can now view and export NetScaler-owned IP addresses (**Infrastructure > Instances > NetScaler Owned IPs**) in the NetScaler Console GUI.

For more information, see View NetScaler-owned IP addresses.

Licensing

View details for VPX instances provisioned on an SDX instance in the Flexed licensing dashboard

In the Flexed licensing dashboard (**NetScaler Licensing > Flexed Licensing > Dashboard**), under **Licensed NetScalers**, you can view the number of VPX instances that are checked out for NetScaler SDX. You can now click the count to view the provisioned VPX instance details for that SDX, such as instance Name, IP address, Throughput (MBPS), and Edition.

Earlier, you were able to view only the total number of VPX instances checked out for that SDX.

View MPX/SDX host ID and serial number details in Zero-capacity licenses

In **NetScaler Licensing > Zero-capacity licenses**, you can now view **Host ID** and **Serial Number** details for the MPX and SDX instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

The issues that are addressed in Build Jul 15, 2024.

Infrastructure

- When you modify an instance in **NetScaler Console (Infrastructure > Instances > NetScaler)**, such as changing the site or admin profile, the key-value pairs of the tags associated with the instance are reversed.
- In Config Job, when you run the ShowConfiguration template simultaneously on both the primary and secondary NetScalers in an HA pair, clicking Download Result Files downloads the file only for the secondary instance.
- When a dashboard is not present in Network Reporting (Infrastructure > Network Reporting), you get the following error message:

  "You don't have access to this page"

  This error message can be ignored and it does not prevent you from creating dashboards.
- The SNMP traps are not received in NetScaler Console service when it is configured by using the built-in agent.

StyleBooks

In the NetScaler Console GUI, when you edit a config pack to use a different StyleBook, the upgrade does not work as expected.

July 09, 2024

Support for identification and remediation of CVE-2024-5491 and CVE-2024-5492

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2024-5491 and CVE-2024-5492.

- Identification for CVE-2024-5491 requires a combination of version and configuration scan.
- Identification for CVE-2024-5492 requires a version scan.

Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

For more information on how to use NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.

For more information, see Security Bulletin.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect on the impact of CVE-2024-5491 and CVE-2024-5492 in the security advisory module. To see the impact sooner, you can start an on-demand scan by clicking **Scan Now**.

June 18, 2024

Telemetry

NetScaler telemetry program

As an existing NetScaler Console customer, you are required to be compliant with the NetScaler Telemetry program that requires license and feature usage telemetry data collection. The telemetry data uploads happen every 24 hours automatically and no action is required from your end.

- For more information, see NetScaler Telemetry program.
- For more information about the telemetry parameters, see Data Governance.

June 11, 2024

Analytics

Metrics Collector and lean period usage analytics enabled at the virtual server level

Metrics collector and lean usage analytics are now enabled at the virtual server level instead of the instance level. With this enhancement, metrics collector and lean usage analytics remain enabled only on your active virtual servers with high traffic.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can review your virtual servers and enable **Metrics Collector** and lean usage on other virtual servers by navigating to **Settings > Analytics Configuration** and clicking **Configure Metrics** under **Virtual Server Metrics Summary**.

For more information, see Configure Intelligent App Analytics.

Assign a net profile in NetScaler instances for metrics collection

When you enable metrics collector for the virtual servers in NetScaler Console, the metrics data from the NetScaler is exported to NetScaler Console through the NetScaler subnet IP address (SNIP). In some scenarios, the SNIP might be blocked because of the firewall in the network. In such scenarios, you might have to use a different IP address. For more information about net profile, see Use a specified source IP for back-end communication.

You can now assign a net profile to NetScaler instance for metrics collection. Metrics Collector pushes the NetScaler counter data to NetScaler Console, which is used to detect application issues. Navigate to **Infrastructure > Instances > NetScaler**, select the instance, and from the **Select Action** list, click **Configure Net Profiles for Metrics Collector**.

For more information on assigning a Net Profile, see Assign a net profile for the managed NetScaler instance.

Observability Integration - View details for failed NetScaler subscription

In **Observability Integration**, when you configure a subscription for NetScaler to Splunk or Prometheus, you can now view detailed logs for the failed subscriptions. As an administrator, using these logs, you can analyze the reason for the subscription failure.

For more information, see View logs for failed configurations

Removal of periodic export option for WAF and Bot insight in Observability Integration

The periodic export option for WAF and Bot insight is now removed when you configure the export of insights from NetScaler Console to observability tools (such as Splunk, New Relic, and Microsoft Sentinel). Since WAF and Bot violations are crucial, it is recommended to use the real-time export option to export insights in real time whenever they occur.

Any existing subscription with periodic export configuration for WAF and Bot is automatically changed to real-time export.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infrastructure

Support for "App-based" provisioning

NetScaler Console service introduces "App-based" provisioning for AWS and Azure. This feature streamlines and simplifies NetScaler deployments in cloud data centers, enabling efficient application delivery from these environments.

For more information, see App-based provisioning in AWS and App-based provisioning in Azure.

Fixed Issues

The issues that are addressed in Build Jun 11, 2024.

Analytics

- A process in NetScaler Console/Agent might crash due to memory corruption.
- In **Web Insight**, the details for the load balancing virtual server configured behind content switching virtual server are not visible for daily, weekly, and monthly reports.

Infrastructure

- When non-admin users try to view statistics for the virtual servers in NetScaler Console (**Infrastructure > Network Functions**), the following error message appears:

  "Not authorized to access <vserver_name>"

- In an HA setup, when you use the built-in agent "mastools" along with the partitions, the status of the secondary NetScaler instance is "unknown" in the SSL Dashboard (**Infrastructure > SSL Dashboard**) and in Load Balancing (**Infrastructure > Network Functions > Load Balancing**).

StyleBooks

- When you edit the config packs, any changes you make to ACLs or Policy-Based Routing (PBR) rules such as add, update, or delete are not applied.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

June 5, 2024

Analytics

Integrate NetScaler Console with Microsoft Sentinel

In **Observability Integration**, you can now configure the integration of NetScaler Console with Microsoft Sentinel to export and view insights in Microsoft Sentinel. For a successful integration, ensure that the following prerequisites are met:

- **Azure subscription** - An Azure subscription to deploy and use Microsoft Sentinel.
- **Log Analytics Workspace** - A workspace is required to store and analyze the collected data.
- **IAM roles** - Permission levels such as reader, contributor must be set for the workspace.
- **Custom tables** - To store and send the NetScaler Console data to the workspace.

For more information, see Integration with Microsoft Sentinel

Platform

Support for OpenSSH version 9.x

The OpenSSH version on NetScaler is now upgraded from 8.x to 9.x.

StyleBooks

Save as draft option in config packs

You can now save the config pack as a draft. To save the configuration as a draft, follow these steps:

1. Navigate to **Applications > Configuration > Config Packs**.
2. On the **Configurations** page, click **Add**.
3. Select a stylebook and click **Select**.
4. On the **Create Configuration** page, click **Save as Draft**.

The saved drafts appear in the **Draft Configurations** tab under **Pending Configurations**.

For more information, see Save a config packs as a draft.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schedule option in config packs

You can now schedule the deployment of newly created config packs. To create a schedule for a new config pack, follow these steps:

1. Navigate to **Applications > Configuration > Config Packs**.
2. On the **Configurations** page, click **Add**.
3. Select the stylebook and click **Select**.
4. On the **Create Configuration** page, under **Execution**, choose **Later** from the **Execution Mode** list.
5. Select the desired time and date for scheduling.

For deployed config packs, you can schedule when to publish the updates and when to delete the config pack. The scheduling options are available when you edit a deployed config pack.

For more information, see Create a schedule for a config pack.

Fixed Issues

The issues that are addressed in Build Jun 5, 2024.

Analytics

- The **Application Heath** details in the **Overview** dashboard do not display the same details available at **Application Score** in **App Dashboard**.
- If more than 25000 virtual servers are managed through NetScaler Console, App Dashboard might take more time to load details.

Infrastructure

- The event rules fail to generate the expected actions when the service group state changes.

StyleBooks

- When you add collection data with empty values for fields of type IP address, integer, or boolean to the custom data source in StyleBooks, the operation might fail.
- When you create a config pack from NetScaler Console GUI, the system might return an empty list for the parameters referring to the built-in managed-adc data source.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When you try to create a config pack or perform a dry run, the operations might fail if both of the following conditions are met:
  - The StyleBook definition references another StyleBook within the component section.
  - When you assign parameters of type "datum" to properties between the current StyleBook and the referenced StyleBook.

May 22, 2024

Analytics

Bulk upgrade SSL virtual servers using the SSL A+ rating upgrade task

In **Tasks**, you can now view the **SSL A+ rating upgrade** task. The existing upgrade to A+ SSL rating process in **App Dashboard** enables you to upgrade only one application at a time. Using the **SSL A+ rating upgrade** task, you can do a bulk upgrade.

NetScaler Console reviews the application virtual server SSL configuration with the NetScaler secure front-end profile and identifies the non-A+ rated applications. The **SSL A+ rating upgrade** task displays the non-A+ rated applications. As an administrator, you can select applications and do a bulk upgrade to achieve SSL compliance.

For more information, see Actionable tasks and recommendations.

Licensing

Actual usage details in Flexed license reporting

In **Flexed License Reporting** dashboard (**NetScaler Licensing > Flexed Licensing > Reporting**), you can now view the actual Bandwidth/Throughput usage that enables you to view the consumption details (peak usage and average usage). Earlier, the dashboard displayed only the allocation and entitlement details.

In addition, the following enhancements are also available in the Flexed license reporting dashboard:

- Filter to view details for selected NetScaler instances.
- Option to export details in PDF, PNG, and JPEG format.
- Bandwidth is renamed to throughput capacity.

For more information, see Flexed license reporting

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBooks

Create NetScaler policy expressions in StyleBooks

The StyleBooks GUI now allows you to build NetScaler policy expressions by selecting items from lists, helping you to create expressions faster and more accurately. To make the policy expression editor available for a parameter, specify the `is_policy_expression` GUI attribute in the parameter definition of StyleBooks.

For more information, see Policy expressions in StyleBooks.

Fixed issues

The issues that are addressed in Build May 22, 2024.

Infrastructure

In **Config Job**, when you run the **ShowConfiguration** template simultaneously on both the primary and secondary NetScalers in an HA pair, clicking **Download Result Files** downloads the file only for the secondary instance.

StyleBooks

When you delete a NetScaler instance that uses a subnet IP address (SNIP) for management access from NetScaler Console and then re-add the instance, the operations on config packs created before deleting the instance might fail.

April 23, 2024

Analytics

Support to export periodic data for custom NetScaler instances

When you create a subscription for the data export of NetScaler Console to Splunk or New Relic, you can now select **Periodic Export** (daily or hourly) and apply it to the custom instances. Earlier, periodic insights data export to the custom instances was not supported.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infrastructure

Additional event alert for disk utilization

NetScaler Console now allows you to set an additional threshold value for disk utilization alarms. With this threshold value, you can set a lower-level limit to receive alerts before an upper threshold is breached. To configure the lower-level threshold, navigate to **Settings > SNMP > Edit** and enable **Configure a lower-level threshold**.

For more information, see Configure and view system alarms.

Fixed Issues

The issues that are addressed in Build April 23, 2024.

Infrastructure

- When you try to export the NetScaler Console report as a snapshot in **Infrastructure > Instances > NetScaler**, the page becomes unresponsive.
- If more than 10 NetScaler instances are managed through an agent in NetScaler Console, the agent inventory subsystem fails. As a result, NetScaler Console does not fetch the latest NetScaler configuration data.

Licensing

- The number of instances shown on the Flexed License dashboard is incorrect.

Security

- When you export violation records in tabular form through the **Export Now** or **Schedule Export** options in **Security > Security Violations > All Violations > Violation Details**, only the records visible in the current page view are included in the report, regardless of the number of records selected in **Number of Records to Export**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

April 10, 2024

Analytics

Observability Integration - Support to configure the export of NetScaler metrics and Audit logs to Splunk

In **Settings > Observability Integration**, you can now configure the export of NetScaler Metrics and Audit logs to Splunk.

For more information, see Configure the export of NetScaler metrics and audit logs to Splunk.

Infrastructure

Access NetScaler GUI through host name

When you connect to NetScaler through **Infrastructure > Instances > NetScaler**, clicking on the host name now establishes the connection to the NetScaler GUI through the host name. Previously, clicking on either the host name or the IP address initiated the connection to the NetScaler GUI through the NSIP.

View discrepancies between high-availability nodes during upgrade

You can now view configuration discrepancies between the primary node and the secondary node while upgrading the NetScaler high-availability deployment. You can review the discrepancies and decide to continue or halt the upgrade. To use this feature, navigate to **Infrastructure > Upgrade Jobs**, and view the discrepancies in the **Pre-upgrade validation** tab.

For more information, see Upgrade jobs .

Fixed Issues

The issues that are addressed in Build April 10, 2024.

Infrastructure

- The **Infrastructure > Events > Syslog Messages** page appears blank when the syslog messages contain special characters such as superscripts.
- The count of used and unused certificates displayed in **Infrastructure > SSL Dashboard > Usage** is incorrect when the SSL certificates have certificate chains.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Licensing

- The ports 27000 and 7279 required on agent for Pooled or Flexed licenses might become unavailable after the restart of agent processes. In such scenarios, the NetScaler instances using Pooled or Flexed licenses might go into grace period.

Security

- When you navigate to **Security > WAF Recommendation**, you might see the following error message:

  "**HTTP Error 500 () while accessing the data endpoint: "apps"**"

March 26, 2024

Fixed Issues

The issues that are addressed in Build March 26, 2024.

Infrastructure

- While creating or updating an upgrade job, when you try to select an instance in **Infrastructure > Upgrade Jobs > Create Job > Select Instance > Add Instances**, the **Add Instances** page displays the **Partitions** tab which is not applicable to the workflow. If you select a partition, the page becomes unresponsive and you cannot proceed further.

- When you create Slack notifications in **Settings > Notifications > Slack > Create Slack Notifications** and select **Notifications with attachment**, the notifications do not get displayed and the following error message is seen:

  `Invalid token`

StyleBooks

- When the **Secure access only** option is selected in **Settings > Administration > System Configurations > Basic Settings** and you try to perform any Device API Proxy operation, the operation fails.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

March 12, 2024

Licensing

Support to manually select a NetScaler agent as LSA in NetScaler Console service

You can now manually select a NetScaler agent as a license server agent (LSA) for NetScaler Pooled licensing or NetScaler Flexed licensing.

When an LSA is down, the NetScaler Console service waits for 24 hours before auto-electing the next LSA. The admin can manually elect the new LSA in the interim by using this feature. However, the admin must ensure that the status of the new LSA being elected is **UP** and its diagnostic status is **OK**.

For more information, see NetScaler agent behavior for Flexed or Pooled licensing.

Fixed Issues

The issues that are addressed in Build March 12, 2024.

Analytics

- When you enable **Gateway Insight** for the Gateway virtual servers, the **Analytics Status** column in **Settings > Analytics Configuration > All Virtual Servers** shows **Disabled**.
- In **Gateway > Gateway Insight**, the **Authentication** tab does not display user details for the failed authentications.

Infrastructure

- When a user-defined policy is created and a user is added to that policy, GET API requests for specific resources encounter permission issues and the following error is displayed:

  "Not authorized as required permissions were not given"

February 28, 2024

Infrastructure

Updates to VIP licensing and NetScaler Console Service storage

- **Unlimited VIPs on NetScaler Console service**: Starting from NetScaler Console service release 14.1-21.x, the concept of licensed VIPs is removed. An unlimited number of VIPs are

© 1997–2026 Citrix Systems, Inc. All rights reserved.

now available in NetScaler Console service. You no longer have to purchase NetScaler Console virtual server licenses because VIP license SKU will be End of Sale (EOS) & End of Renewal (EOR) shortly.

- **NetScaler Console service storage**:
  - NetScaler Console service storage SKU will be End of Sale (EOS) & End of Renewal (EOR) shortly.
  - The default NetScaler Console service storage entitlement is now 5GB.
  - Any NetScaler Console service storage licenses purchased in the past are honoured until the term ends.
  - Any NetScaler Console VIP licenses purchased in the past that entitled you to a proportionate entitlement of NetScaler Console Service storage are honoured until the term ends.
  - If you purchase any other licensing package that entitles you to a higher NetScaler Console storage entitlement, the default 5GB is changed to match the entitlement.

Updates to analytics and metrics collector

- With unlimited VIPs support from 14.1 21.x build, all existing and new virtual servers are now automatically licensed. You can enable analytics on the virtual servers without explicitly licensing them.
- Metrics collector is now disabled by default for all NetScaler license types in the new NetScaler instances added in NetScaler Console from 14.1 21.x build. The metrics collector configuration for the existing managed instances remain unchanged.

Analytics

Action policies - Configure notifications for application usage

In Action Policies (**Settings > Actions > Action Policies**), you can now configure an action policy for Application Usage and select **Requests per second**, **Throughput**, and **Data Volume** options. These options enable you to configure and receive notifications for request per second average, request per second anomalies, throughput average, throughput anomalies, total data volume, and data volume anomalies. For more information, see Configure an action policy to receive application event notifications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Observability Integration

The configuration workflow for integration with Splunk and New Relic is now enhanced for better user experience and is available under **Settings > Observability Integration**. Earlier, the configuration workflow for integration with Splunk and New Relic was available under **Settings > Ecosystem Integration**.

For more information, see Observability Integration

Observability Integration - Support to configure the export of NetScaler metrics to Prometheus

In **Settings > Observability Integrations**, you can now configure the export of NetScaler metrics to Prometheus by selecting the default schema.

For more information, see Prometheus Integration and Observability Integration.

Gateway Insight - Improvements to export reports

In **Gateway > Gateway Insight**, you can now export report only with the selected options using the settings icon in all tables under each metric (EPA, Authentication, Authorization Failure, SSO, and Application Launch). Earlier, the exported report displayed all information regardless of the selected options.

StyleBooks

Updates to Default StyleBooks

Default StyleBooks based on the NetScaler version 10.5 will be deprecated in upcoming releases. A new set of Default StyleBooks is now available in **Applications > Configuration > StyleBooks > Default StyleBooks**, based on NetScaler version 13.0.

Option to clone a StyleBook

NetScaler Console now allows admins to create a duplicate of a StyleBook, along with their dependencies. Admins can then use this bundle for additional customization such as updating `parameters` and `components`.

To use this feature, navigate to **Applications > Configuration > Stylebooks**, select a default or custom StyleBook and click **Clone**.

For more information, see Clone a StyleBook.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed Issues

The issues that are addressed in Build Feb 28, 2024.

Infrastructure

- Migration from NetScaler Console to NetScaler Console service fails and certain Azure Active Directory groups are not available in the NetScaler Console service. This issue occurs because of the presence of spaces in the Azure Active Directory group names created in NetScaler Console.
- Users are unable to access NetScaler Console if they belong to multiple Azure Active Directory groups.
- In **Web Insight** and **Security Violations**, the Schedule Export workflow in the GUI is enhanced for better user experience.
- In **Infrastructure > Network Reporting**, the tabular export report does not include details such as service, service group, virtual server, and interface name.
- Flexed license dashboard displays NetScaler details only after at least one NetScaler is checked out from the Premium bandwidth license pool.

February 06, 2024

Analytics

App dashboard - Support to view application metrics details from NetScaler admin partition

In **App Dashboard**, you can now view metric details for applications that are created from the NetScaler admin partitions. Earlier, you were able to only view applications from the admin partitions without any metrics.

Infrastructure

NetScaler ADM rebranding in Citrix Cloud™

Starting from 14.1 16.x build, NetScaler ADM service was rebranded to NetScaler Console service. In continuation, Application Delivery Management is now rebranded to NetScaler Console in the following places:

- The tile under **My Services** in Citrix Cloud home page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The service name in **Citrix Cloud menu > My Services**.
- The product name in the Add administrator workflow in **Set access > Custom Access** from **Citrix Cloud menu > Identity and Access Management > Administrators > Add administrator/group**.

Run default validation scripts in upgrade jobs

NetScaler Console now includes an option for default validation scripts in the upgrade job workflow. These default scripts are run both before and after an upgrade job, generating a diff report. You still have the option to run custom default scripts.

For more information, see Upgrade NetScaler instances.

Automate radar object deployment for NetScaler Console Sites

NetScaler supports automating radar object deployment for NetScaler Console sites, eliminating the need for manual deployment on the NetScaler instances.

This enhancement is available only when you edit a NetScaler instance and it is applicable only for site type **Data Center** (with type **Private**) or **Branch**.

When you select **Deploy to NetScaler** from the **Real User Measurements** list, the **NetScaler Instance** list is automatically populated, allowing you to choose the specific instance to deploy the radar object (r20.gif).

For more information, see Automate radar object deployment.

Fixed Issues

The issues that are addressed in Build Feb 06, 2024.

Analytics

- The **XML SQL** attack is not reported in both security dashboard (**Security > Security Dashboard**) and security violations dashboard (**Security > Security Violations**).

Licensing

- Flexed license dashboard displays NetScaler details only after at least one NetScaler is checked out from the Premium bandwidth license pool.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Management and Monitoring

- When a configuration job is created, the status in **Infrastructure > Configuration > Jobs** shows **Completed** but **Details > Execution Summary** displays 0% complete.

- A two-stage upgrade job status for a NetScaler HA displays 'Scheduled' even though the NetScaler HA upgrade is completed. The primary node displays completed (**Status Stage 1: Completed)** but the secondary node displays scheduled (**Stage 2: Scheduled**).

- When a configuration audit template is created with special characters in its name under **Infrastructure > Configuration > Audit Templates > Add**, the template is successfully generated. However, a differential report fails to generate for the template in the **Configuration Audit** dashboard during polling.

  This issue is observed when special characters other than - (dash) and '_' (underscore) are used.

January 24, 2024

Analytics

View Upgrade Advisory details in Tasks

In **Tasks**, you can now view the **Upgrade Advisory** actionable task. Based on your current utilization, if your NetScaler instances have already reached or about to reach End-of-Life (EOL) or End-of-Maintenance (EOM) within 90 days, the **Upgrade Advisory** task displays the details of those instances. You can click **Take Action** and upgrade those instances to a recommended build.

Infrastructure

Enhanced permissions for read-only users

Users with read-only permissions for the following features can now poll NetScaler instances:

- SSL certificates (**Infrastructure > SSL Dashboard > Poll Now**)
- Network functions (**Infrastructure > Network Functions > Poll Now**)
- Configuration audits (**Infrastructure > Configuration > Configuration Audit > Poll Now**)

Fixed Issues

The issues that are addressed in Build Jan 24, 2024.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The built-in agent registration in NetScaler SDX displays a success message but the SDX instance does not appear in **Infrastructure > Instances Dashboard**.

- In **Infrastructure > Network Functions > Load Balancing**, the **Servers** tab indicates the number of servers but does not display any table entries for non-default users.

January 16, 2024

Support for identification and remediation of CVE-2023-6548 and CVE-2023-6549

NetScaler Console service Security Advisory now supports the identification and remediation of CVE-2023-6548 and CVE-2023-6549.

- Identification for CVE-2023-6548 requires a version scan.
- Identification for CVE-2023-6549 requires a combination of version and configuration scan.

Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix.

NOTE:

Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

For more information on how to use NetScaler ADM to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.

For more information, see Security Bulletin.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect on the impact of CVE-2023-6548 and CVE-2023-6549 in the security advisory module. To see the impact sooner, you may start an on-demand scan by clicking **Scan Now**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

January 09, 2024

Analytics

Support to share custom dashboard to other users

As an administrator, you can now share the custom dashboard with other users. In **Overview > Custom Dashboard**, select a dashboard and click **Share**. Type the username and click **Invite** to share the dashboard. The assigned users can view the dashboard in read-only mode.

Infrastructure

Configure ITM Radar in NetScaler Console Sites

The ITM Radar enhances network monitoring capabilities. The sites deployed in data centers, virtual machines, or cloud providers can now host the radar object (r20.gif), providing insights into performance metrics. The ITM Radar object actively collects valuable end-user application statistics, providing the sites with robust ITM radar telemetry for more effective network monitoring and informed traffic management decisions.

For more information, see Configure ITM Radar.

View gateway insights data in Splunk and New Relic

When you create a new subscription in **Settings > Ecosystem Integration** for the integration of NetScaler Console service with Splunk and New Relic, you can now select the **Gateway Insights** option. After you configure the subscription with the **Gateway Insights** option, you can view the gateway insights data in Splunk and New Relic.

For more information, see For more information, see Integration with Splunk and Integration with New Relic.

Export SSL data to Splunk and New Relic immediately

The SSL data is now exported to Splunk and New Relic immediately after an admin creates a subscription by selecting **SSL Certificate Insight** in Splunk and New Relic. Earlier, the admins had to click **Poll Now** (**Infrastructure > SSL Dashboard**) to export the data for the first time.

View Upgrade Advisory details in Tasks

In **Tasks**, you can now view the **Upgrade Advisory** actionable task. Based on your current utilization, if your NetScaler instances have already reached or about to reach End-of-Life (EOL) or

© 1997–2026 Citrix Systems, Inc. All rights reserved.

End-of-Maintenance (EOM) within 90 days, the Upgrade Advisory task displays the details of those instances. You can click **Take Action** and upgrade those instances to a recommended build.

Action policy - Configure notifications for Requests, Bandwidth, and Response Time

In **Action Policies** (**Settings > Actions > Action Policies**), when you configure an action policy in Application Performance, you can now select **Requests**, **Bandwidth**, and **Response Time** options. These options enable you to configure and receive notifications for total requests, total bandwidth, average response time, and response time anomalies. For more information, see Configure an action policy to receive application event notifications.

In addition, you can also now configure an action policy from graph trend in **Web Insight** for these metrics. As an administrator, when you notice any unusual traffic pattern or a sudden spike in these metrics for any application, this enhancement enables you to create a relative action policy by clicking **Create Action Policy** after placing it on a specific point in the graph.

Fixed Issues

The issues that are addressed in Build Jan 09, 2024.

Licensing

- After the Flexed or Pooled license is applied, the **Analytics Configuration** page (**Settings > Analytics Configuration**) is not updated with the correct details.
- The Flexed license dashboard in **NetScaler Licensing > Flexed Licensing > Dashboard** appears blank.
- In **NetScaler Licensing > License Management**, the configuration for the threshold breach through email notification is not working as expected.

Known issues

NetScaler Application Delivery Management (NetScaler Console) has the following known issues:

Licensing

- This issue will impact you if you have an SDX migrated or migrating from any type of NetScaler local license (fixed capacity subscription or perpetual license) file based licensing to any type of

© 1997–2026 Citrix Systems, Inc. All rights reserved.

license with LAS based licensing and the legacy file-based licenses have not been deleted from the SVM.

Impact: If there is any local legacy file-based license yet existing on the SVM after having transitioned to LAS, then the expiry of the file-based license triggers the un-licensing of the SDX (SVM and VPX on SDX) on the date of that license file expiry.

Workaround: Delete the local file-based license(s) on the SVM after the migration to LAS has been done successfully. The file-based licenses would be located in SVM folder /mpsconfig/license and must be deleted from this folder using the shell prompt.

Management and monitoring

- Admin partitions are displayed both when initiating an IOC scan and in the IoC scan results. These entries can be ignored, as the IOC scan covers the entire NetScaler appliance.
- The NetScaler® Console CVE advisory might display an incorrect overall severity when no vulnerabilities are found in File Integrity Monitoring scans. The correct severity is displayed in the detailed CVE view.
- In **Infrastructure > SSL Dashboard > Manage Certificate Store**, when you click **Import NetScaler Certificates**, NetScaler Console fails to import NetScaler certificates of PFX format.

Infrastructure

- In NetScaler Console, when an instance is authorized for a system group and a new partition is added to the instance, the system group authorization setting is automatically assigned to the new partition.
- When you try to install a certificate on a NetScaler BLX™ instance, the installation fails and the **Infrastructure > SSL Dashboard > SSL Audit Logs** page displays the following error message:

  `SCP: Authentication by password fails on _<ip-address>_.`
- When an event rule is created with some entities selected in **Infrastructure > Events > Rules > Create rule > Select Failure Objects**, all the selected entities do not get displayed. This issue is seen when there is a large number of virtual servers, services or service groups.

  Workaround: Contact the NetScaler Support team for assistance with this issue.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The SSH or SCP operation that is used in the **Configuration Jobs** might fail with the following error message:

  "SSH Failure establishing ssh session: -5"

  Workaround:

  a. Log on to NetScaler Console using an SSH client.

  b. Check the output for the following command:

  ```
  ls -l /etc/sshd_config
  ```

  c. In `/etc/sshd_config`, update it to add the following:

  ```
  HostKey /nsconfig/ssh/ssh_host_ecdsa_key
  ```

  d. Apply the changes:

  ```
  ps -aux | grep /usr/sbin/sshd | grep -v grep | tr -s ' ' | cut -d ' ' -f 2 | xargs kill -9
  ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Data compliance

PCI DSS compliance

Payment Card Industry (PCI) Data Security Standard (DSS) is a credit card industry security standard that defines a required level of security for people, processes, and technology that must exist when storing, processing, or transmitting credit card data. PCI DSS applies to merchants, processors, and service providers, and all other entities that store, process, or transmit credit card data. PCI DSS Attestation of Compliance (AOC) is ultimately an attestation by an entity that a specified level of security is required and exists.



NetScaler® Application Delivery Management service PCI DSS compliance

NetScaler Application Delivery Management (ADM) service has achieved the PCI DSS compliance successfully with assessment against the PCI DSS compliance control domains for customers. NetScaler Console service does not store, process, and or transmit customer PCI data. NetScaler Console Service will also undergo a PCI DSS assessment by a Qualified Security Assessor (QSA) annually to evaluate our services and controls.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

While Citrix helps support the customer’s PCI DSS compliance, using NetScaler products and services does not achieve PCI DSS compliance on its own. Customers are responsible for ensuring that they have an adequate compliance program, internal processes, and controls in place to achieve and maintain their PCI DSS compliance requirements.

Click NetScaler Console Service PCI Attestation of Compliance (AOC) to download an offline report.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler® telemetry program

The NetScaler telemetry program is a required data collection program that enables the upload of required license and feature usage data necessary for customers to remain compliant with their maintenance and support license obligations. Citrix collects basic license telemetry data and NetScaler deployment and feature usage telemetry data for its legitimate interests, including license compliance. NetScaler Console configuration and feature usage data is also collected to manage, measure, and improve Citrix products and services. We highly recommend adding NetScaler instances to NetScaler Console to improve and simplify your NetScaler operations overall and support the enhancement of our products and services by sending NetScaler feature usage data. Learn more. The NetScaler telemetry program is enabled automatically starting from 14.1-28.x build.

Prerequisites

Ensure that:

- The agent is running on the latest version. By default, the agents are automatically upgraded. In some scenarios, the agents might still be running on an older version and you must manually upgrade the agent. For more information on how to manually upgrade the agent, see Upgrade agent manually.
- The NetScaler agent must be able to communicate with NetScaler on port 22.
- The port 5140 is allowed in the network to receive the NetScaler Gateway telemetry data. (Only applicable to the NetScaler instances that have VPN virtual server configuration).

NOTES:

- The telemetry upload happens every 24 hours automatically.
- To collect and store the telemetry metrics in your NetScaler instances, the following configuration was pushed to your NetScaler instances through NetScaler Console as part of the NetScaler telemetry program released on 18th June 2024.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
enable ns feature AppFlow

add analytics profile telemetry_metrics_profile -type timeseries
-outputMode prometheus -metrics ENABLED -serveMode Pull -schemaFile "./
telemetry_collect_ns_metrics_schema.json" -metricsExportFrequency 300
```

- You must remove the telemetry metrics profile that was pushed as part of NetScaler telemetry program using the following command:

```
rm analytics profile telemetry_metrics_profile
```

- If you are not using the NetScaler or NetScaler Console analytics features, you can use the following command to remove the AppFlow configuration:

```
disable ns feature AppFlow
```

- The `/nsconfig/.telemetry.conf` file is updated with the following command for the Gateway telemetry. NetScaler Console checks for this command every hour and adds it, if this command is missing. This command is pushed only to the NetScaler instances that have VPN virtual server configuration:

```
ns_telemetry_server,&lt;Console IP>,5140
```

- Some telemetry parameters are collected through scripts that are pushed from NetScaler Console to NetScaler instances. These scripts are read-only and do not change anything in NetScaler.
- The information collected through telemetry, such as email addresses, user names, and IP addresses, is securely pseudonymised by hashing the information at the source using one-way hashing algorithms. As a result, Citrix cannot access or read these values. This telemetry data is used solely for logical asset-matching purposes.

The following table provides the parameter details that are collected as part of NetScaler telemetry program:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATEGORIES	DESCRIPTION	WHAT DO WE USE IT FOR
License, and NetScaler deployment and usage telemetry	Information about license entitlement, allocation, usage, and high-level NetScaler deployment data, and NetScaler feature usage.	License compliance and to manage, measure, and improve the service.
NetScaler Console deployment and feature usage telemetry	Information about Console deployment and feature usage.	To manage, measure, and improve the service.

For more information about the list of telemetry parameters, see Data governance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Data governance

NetScaler Console service is a part of Citrix Cloud services, and it uses Citrix Cloud as the platform for signup, onboarding, authentication, administration, and licensing. Citrix collects and stores data in Citrix Cloud as part of the NetScaler Console service. This document describes what data is collected and methods of data collection, storage, and transmission.

For more information about data protection practices at Citrix, see Citrix Cloud Services Data Protection Overview.

This information is for Security Officers, Compliance Officers, Information Auditors, Network Infrastructure and Operations administrators, and line-of-business owners.

NetScaler® telemetry program

The NetScaler telemetry program is enabled in NetScaler Console service from **14.1-28.x** build. With this program, the required data is automatically uploaded. For more information about the required telemetry collected, see Data Governance for NetScaler Telemetry.

How do we collect, store, and transmit data?

NetScaler Console service collects data from the managed instances and agents. These instances are deployed in the customer's premises and data is transmitted from the agent (deployed in the customer's premise) securely over an SSL channel encrypted using TLS 1.2 protocol to the cloud.

Data is stored in Relational database with multitenant data isolation at the database layer and as files in Elastic File System (EFS) hosted in AWS cloud in the United States, EMEA (Frankfurt), and APJ (Sydney) – depending on the Point of Presence (POP) chosen by the customer. All PoPs are hosted in AWS Commercial regions.

Passwords, SNMP community strings, SSL certificates, and NetScaler config backup are encrypted using a unique per tenant AES 256 key, and stored securely in the database. For more information on the commercial regions that Citrix Cloud uses and the presence of the NetScaler Console service within each region, see Geographical Considerations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Data categories

For data handling practices, the data is classified into:

- **Customer Content** - Any data uploaded to Customer’s account for storage or data in Customer’s computing environment to which NetScaler is provided access to perform certain Services.
- **Logs** - Include records of Services, including, but not limited to:
  - Data and information on performance, stability, usage, security, support
  - Technical information about devices, systems

Customer content

The NetScaler Console Service collects information from various sources:

- NetScaler
- NetScaler Gateway
- NetScaler Web App Firewall (WAF) and Bot Management

NetScaler Console Service also collects information about administrator’s session and activity details in addition to the information mentioned in logs.

Logs

Logs are used to facilitate the provisioning of software updates, license authentication, support, analytics, and other purposes consistent with Citrix User Agreements.

Metadata and telemetry Logs collected include:

- NetScaler Service agent hypervisor or public cloud platform or both agent hypervisor and public cloud platform
- Agent geographical location
- NetScaler version
- NetScaler product type
- Licensing info (Express and subscription)
- Usage of cloud service by the NetScaler Console admin (thereby improving the admin user experience).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Detailed customer content and logs

- **Event Management (Login > Infrastructure > Events)**
  - SNMP traps providing alerts on state and performance of the NetScaler network.
  - Syslog of Web transactions traversing through NetScaler network state information.
  - SMS server, Slack, and PagerDuty profile details for triggering SMS/Slack notifications of events.
  - SMTP server details for email configuration.
  - ServiceNow profile details for creating tickets in ServiceNow.
- **SSL Certificate Management (Login > Infrastructure > SSL Dashboard)**
  - SSL certificates, SSL key, SSL CSR, CA issuer, and signature algorithms of the Web apps optimized by the NetScaler instance.
- **Configuration Audit (Login > Infrastructure > Configuration > Configuration Audit)**
  - Data Tracking for NetScaler Configuration Audit changes pertaining to the NetScaler instances, which include Web app server IP address and NetScaler IP address details.
- **Configuration Jobs (Login > Infrastructure > Configuration > Configuration Jobs)**
  - NetScaler Configuration details, instance IP address, and Web app server IP address details.
- **StyleBooks (Login > Applications > Configuration > StyleBooks)**
  - NetScaler configurations stored as a template, which include Web app server IP address details.
- **Instance Management (Login > Infrastructure > Instances)**
  - IP address of the NetScaler instances, NetScaler instance type, NetScaler config backup, NetScaler critical events, and geolocation of the data center where the NetScaler instance is deployed (if configured).
- **Infrastructure Analytics (Login > Infrastructure > Infrastructure Analytics)**
  - IP address of the NetScaler instances, NetScaler instance type, NetScaler critical events, number of apps associated, and geolocation of the data center where the NetScaler instance is deployed (if configured).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Applications (Login > Applications)**
  - App Dashboard: applications URL, request method, response code, total Bytes, Web app server details, virtual server IP addresses, client details, browser, client OS, client device, SSL protocol, SSL cipher strength, SSL key strength, NetScaler instance IP address, timestamp of server flaps, and response content type.
- **Analytics (AppFlow/ Logstream)**
  - **Web Insights (Login > Applications)**: Virtual server IP address, clients, URLs, browsers, operating systems, requests methods, response statuses, domains, Web app server IP address, SSL certificates, SSL cipher negotiated, SSL key strength, SSL protocol, and SSL failure frontend.
  - **HDX Insight (Login > Gateway)**: ICA user details, ICA application details, VDA server details, desktop details in HDX Insight, geolocation details of app client, HDX active session details, VPN licenses for HDX, client NetScaler IP address, client type, and version.
  - **Gateway Insight (Login > Gateway)**: User details, application details, browsers, operating systems, session modes, Gateway licenses, AAA server details, and AAA policy configured on Gateway.
  - **Security Violations (Login >Security)**: Client IP, URL, security violations (WAF and Bot), attack geolocation, attack timestamp, transaction ID, WAF, and NetScaler security configuration status.
  - **API Analytics (Login > Security > API Gateway)**: Information on API Instances, API Endpoints, total bandwidth, API performance information, total request, response time, errors. Ability to drill down further into each API Instance to get visibility into individual API endpoints, performance. Security related to Auth success, failures; Rate-limiting, SSL cipher, protocol information, and SSL errors.
- **Security Advisory (Login > Infrastructure > Instance Advisory > Security Advisory)**
  - **Version scan**: This scan needs NetScaler Console to compare the version of an NetScaler instance with the versions and builds on which the fix is available. This version comparison helps NetScaler Console security advisory identify whether the NetScaler is vulnerable to the CVE. The underlying logic for this scan is if a CVE is fixed on NetScaler release and build xx.yy, all the NetScaler instances on builds lesser than xx.yy build are considered vulnerable. Version scan is supported today in security advisory.
  - **Configuration scan**: This scan needs NetScaler Console to match a pattern specific to the CVE scan with NetScaler config file. If the specific config pattern is present in the NetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ns.conf file, the instance is considered vulnerable for that CVE. This scan is typically used with version scan.

Configuration scan is supported today in security advisory.

- **Custom scan**: This scan needs NetScaler Console service to connect with the managed NetScaler instance, push a script to it, and run the script. The script output helps NetScaler Console identify whether the NetScaler is vulnerable to the CVE. Examples include specific shell command output, specific CLI command output, certain logs, and existence or content of certain directories or files. Security Advisory also uses custom scans for multiple config patterns matches, if config scan cannot help with the same. For CVEs that require custom scans, the script runs every time your scheduled or on-demand scan runs. Learn more about the data collected and options for specific custom scans in the Security Advisory documentation for that CVE.

Security

The Citrix Services Security Exhibit describes in-depth the security controls applied to Citrix Cloud Services, including access and authentication, system development and maintenance, security program management, asset management, encryption, operations management, HR security, physical security, business continuity, and incident management.

The security of Citrix Cloud products is controlled by encryption and key management policies. Refer to the Security Development Processes whitepaper for more details on how Citrix employs security throughout its product development lifecycle.

Data retention policy for NetScaler Console Service

Data such as statistical measures, dashboards, reports, alerts, events, and logs within the NetScaler Console, and login details are retained for the period the customer subscribes to the service. The user account then converts to an Express account where the user can manage only two virtual servers.

The Express account has a capacity of 500 MB or 1-day of Analytics/Reporting data, whichever limit the account reaches first. If an Express account is not used, or the customer does not log in to the account for more than 30 days, the account and all associated Customer Content are automatically deleted.

For more information about data retention and deletion for Citrix Cloud Services accounts, see the Citrix Cloud Services Data Protection Overview.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

All Analytics data in NetScaler Console is retained for a maximum period of 30 days.

Third-party services

The NetScaler Console Service is hosted within Amazon Web Service (AWS) data centers in the United States, EMEA (Frankfurt) and APJ (Sydney) regions – depending on the Point of Presence (POP) chosen by the customer.

Currently, the NetScaler Console Service uses services and APIs from various third-party technologies:

- Services used for product functionality:
  - AWS EFS, AWS RDS, AWS Elastic Cache, AWS ALB, AWS Route 53, AWS EKS, AWS Secret Manager, AWS ECR repository, and AWS MSK.
- Third-party services and tools used for monitoring and operating NetScaler Console include:
  - PagerDuty for on-call rotation
  - Log analysis with Splunk
  - Fluentd for log aggregation
  - Slack for communication and alerting
  - AWS Cloudwatch, SQS
  - S3 as storage area in AWS –for storing core files and metrics
  - Prometheus and Grafana for monitoring (in Honeycomb deployment)

References

- For more information on how we access the collected data, see Citrix Services Security Exhibit.
- For more information on how long the collected data is kept, see Citrix Cloud Services Data Protection Overview.
- Citrix Cloud Technical Security Overview.
- Citrix Cloud Technical and organizational data security measures.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONDITIONS FOR USE OF IoC INFORMATION

By using the IoC Information (as defined below), you acknowledge and agree to the following as conditions of such use:

Citrix Systems, Inc. and/or its affiliates (“Citrix”) has developed Indicators of Compromise logic script and related guidance concerning Indicators of Compromise (collectively, “IoC Information”) to help organizations determine if their environments are potentially compromised.

The IoC Information does not encompass all techniques, tactics, or procedures (“TTPs”) that threat actors may use when targeting relevant environments. Additionally, threat actors change TTPs and infrastructure frequently. For these reasons and others, the IoC Information may be of limited forensic value and may fail to identify actual compromises. You are strongly advised to retain the services of experienced forensic investigators to assess your environment.

The IoC Information is provided as-is. Citrix makes no warranties or representations, whether express or implied, regarding the IoC Information, including, without limitation, that the IoC Information is error-free or meets any conditions of merchantability or fitness for a particular purpose.

The IoC Information is confidential and proprietary information of Citrix and is subject to the terms and conditions of the applicable confidentiality agreement(s) in place between the recipient of these materials and Citrix. No portion of the IoC Information may be reproduced, redistributed, or transmitted to any third party in any form or by any means without the express prior written permission of Citrix.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Getting started

This document walks you through how to get started with onboarding and setting up NetScaler Console for the first time. This document is intended for network and application administrators who manage Citrix network devices (NetScaler, NetScaler Gateway, Citrix Secure Web Gateway, and so on). Follow the steps in this document irrespective of the type of device you plan to manage using NetScaler Console.

Before you begin onboarding, make sure you review the browser requirements, the agent installation requirements, and the port requirements.

Step 1: Sign Up for Citrix Cloud™

To start using NetScaler Console, you must first create a Citrix Cloud company account or join an existing one that someone else in your company has created. For detailed processes and instructions on how to proceed, see Signing Up for Citrix Cloud.

Step 2: Manage NetScaler Console with an Express account

After you log on to Citrix Cloud, do the following:

NOTE:

- For Japan, you must log on to `citrix.citrixcloud.jp`.
- For Government Cloud, you must log on to `citrix.cloud.us`.

1. Go to the **Available Services** section.
2. On the **NetScaler® Console** tile, click **Manage**.

   The **NetScaler Console** tile moves to the **My Services** section.
3. Select a region that suits your business need.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT

- You cannot change the region later.
- This step is not applicable if you log in from Citrix Cloud Japan (`citrix.citrixcloud.jp`) or Citrix Cloud Government (`citrix.cloud.us`). You must ensure that the endpoint URLs applicable are allowed access. For more information, see System requirements.

4. Select roles and use cases that apply to you.

You can log off from the browser while the initialization completes in the background, which might take some time.

NOTE:

Citrix assigns an Express account to manage NetScaler Console resources. If your NetScaler Console Express account remains inactive for 45 days, the account gets deleted. For more information, see Manage NetScaler Console using Express account.

When you log back on to your Citrix Cloud account, the **NetScaler Console GUI** screen appears. Click **Get Started** to begin setting up the service for the first time.

Step 3: Select a NetScaler deployment type

Perform the following steps to deploy or discover NetScaler instances:

1. Select any of the following environments:
   - **On-premises**
   - **AWS**
   - **Microsoft Azure**
   - **Google Cloud Platform**
2. Install the agent to enable communication between the NetScaler Console and the managed instances in your data center or cloud.

   The **Select Agent Type** step varies the agent installation options depending on the selected environment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **External VM Agent**
  - **On-premises** - If you select **On-premises** and then select **On a Hypervisor**, you can install an agent on any of the hypervisors, such as Citrix Hypervisor™ VMware ESXi, Microsoft Hyper-V, or Linux KVM Server.
  - If you select one of the public clouds, such as AWS, Microsoft Azure, or Google Cloud Platform, you can install **External agent** on the selected cloud.
- **As a microservice** - To deploy an agent as a Kubernetes application.
- **Built-in agent** - To deploy an agent within NetScaler.

3. Click **Next**

   Steps to install an agent vary for every option. The following links guide you to the specific steps to install an agent:

   - Hypervisor
   - External agent
   - As a microservice
   - Built-in agent

Install an agent on a hypervisor

Perform the following steps to set up an agent on a hypervisor:

1. Select the hypervisor and click **Download Image** to download the agent image to your local system.

   A service URL and an activation code are generated and displayed on the GUI.
2. Copy the service URL and an activation code.
3. Specify the copied service URL and the activation code while installing the agent on your hypervisor.

   The agent uses the service URL to locate the service and the activation code to register with the service. For detailed instructions about installing an agent on your on-premises hypervisor, see Install an agent on-premises.
4. After successful agent installation, return to the **Set Up Agent** page and click **Register Agent**.

Next step: Add instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

If you do not want to add agents during the initial setup, click **Skip** to check the features provided by NetScaler Console. You can add the agents and instances later. To add agents later, navigate to **Settings > Set up Agents**. For instructions about how to add instances later, see Adding Instances.

Install an external VM agent on public cloud

You do not have to download the agent image from the **Set Up Agent** page. The agent image is available on the respective cloud marketplace.

1. Copy and save the service URL and the activation code to use during agent installation.

   If you want a new activation code, click **Create new Activation Code**, and then copy and save the code to use during agent installation.

   - For detailed instructions about installing an agent on Microsoft Azure cloud, see Install an agent on Microsoft Azure Cloud.
   - For detailed instructions about installing an agent on AWS, see Install an agent on AWS.
   - For detailed instructions about installing an agent on Google Cloud, see Install an agent on GCP.

2. After successful agent installation, return to the **Set Up Agent** page and click **Register Agent**.

Next step: Add instances.

Install an agent as a microservice

You can deploy an agent as a microservice in the Kubernetes cluster to view **service graph** in NetScaler Console.

For more information to get started with service graph, see Setting up service graph.

1. Specify the following parameters:

   a. **Application ID** – A string id to define the service for the agent in the Kubernetes cluster and distinguish this agent from other agents in the same cluster.

   b. **Agent Password** – Specify a password for CPX to use this password to onboard CPX to NetScaler Console through the agent.

   c. **Confirm Password** – Specify the same password for confirmation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. Click **Submit**.

2. After you click **Submit**, you can download the YAML or Helm Chart.
3. Click **Close**.

   For more information, see Install an agent in Kubernetes cluster.

Use the built-in agent

The NetScaler instances in your environment include a built-in agent. You can initiate the built-in agent and use it to establish communication between the instance and NetScaler Console.

1. Copy the generated **Service URL** and the **Activation Code**. Save them to use while initiating the built-in agent on your NetScaler instance.

   For detailed instructions about initiating the built-in agent on your NetScaler instance, see Initiate Built-in Agent on the NetScaler instance.
2. After the built-in agent is initiated, return to the **Set Up Agent** page and click **Register Instance**.

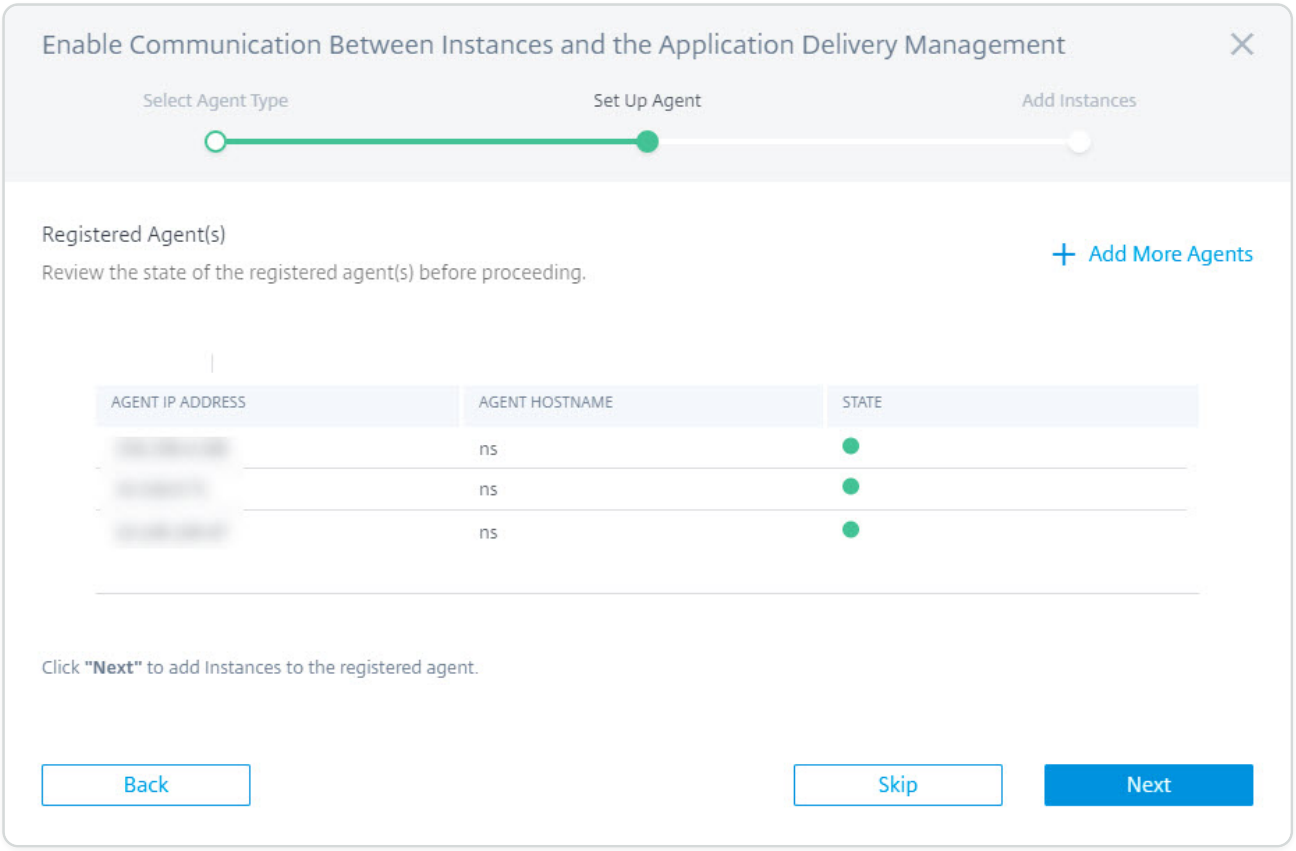
Next step: Add instances.

Add instances

Instances are network appliances or virtual appliances that you want to discover, manage, and monitor from NetScaler Console. To manage and monitor these instances, you must add the instances to the service.

After the successful agent installation and registration, the agents are displayed on the **Set Up Agent** page. When the agent status is in the UP state denoted by a green dot next to it, click **Next** to start adding instances to the service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1. In the **Add Instances** page, view the NetScaler instances that are connected to the registered agent. Ensure that the instance is in the **Up** status and click **Next**.
2. Click **Done** to complete your initial setup and start managing your deployment.

NOTE

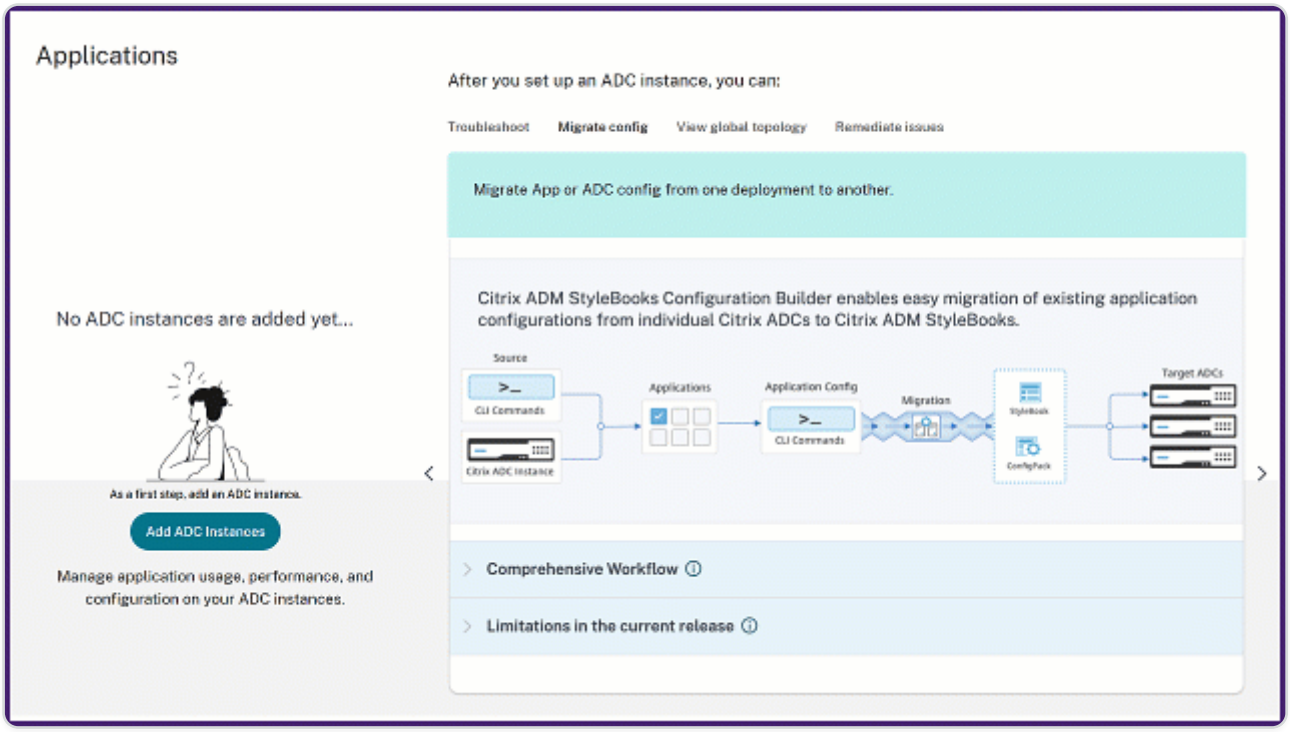
If you do not want to add instances during the initial setup, you can click **Done** to complete the setup and add the instances later. For instructions about how to add instances later to NetScaler Console, see Adding Instances.

Onboard NetScaler instances by using the NetScaler Console GUI dashboard

If you've skipped onboarding the NetScaler instances in the **Getting Started** workflow while setting up NetScaler Console for the first time, you can onboard the instances from the NetScaler Console GUI dashboard. If the NetScaler instances are not yet added, the GUI prompts you to add the instances.

When you click any module on the left-hand navigation bar, on the right-hand side a tabular preview of the features and benefits of that module appears. These features and benefits help you better manage NetScaler instances by using NetScaler Console.

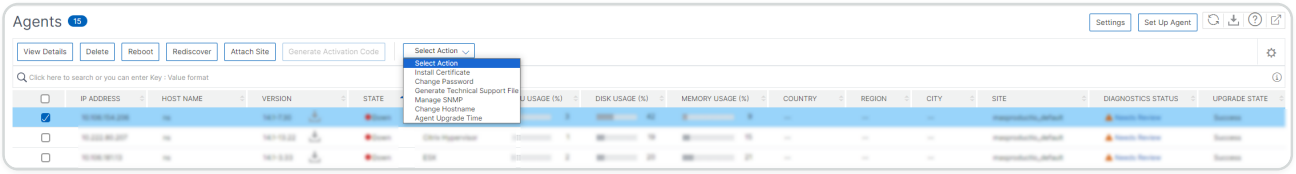
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Click **Add NetScaler instances** to onboard the instances. The **Get Started** workflow restarts. Follow the steps from Step 3: Select an NetScaler deployment type onwards, given in this document, to onboard the instances. If the NetScaler instances are already onboarded, after you log on to NetScaler Console, you see only the NetScaler Console landing page with the navigation bar on the left.

Agent actions

After you've set up your NetScaler Console, you can apply various actions to an agent. Navigate to **Infrastructure > Instances > Agents**.



Under **Select Action**, you can use the following features:

- **Install a new certificate**: if you need a different agent certificate to meet your security requirement, you can add one.
- **Change the agent password**: to ensure security of your infrastructure, change the default password of an agent.
- **Generate a technical support file**: generate a technical support file for a selected agent. You can download this file and send it to Citrix technical support for investigation and troubleshooting.

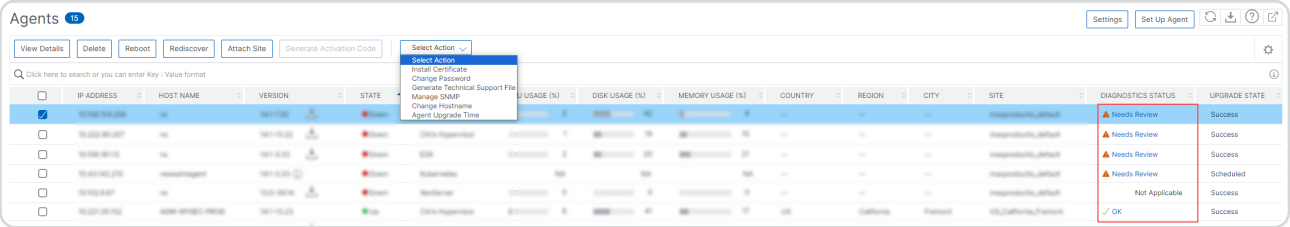
© 1997–2026 Citrix Systems, Inc. All rights reserved.

View agent diagnostics and receive alerts for endpoint verification

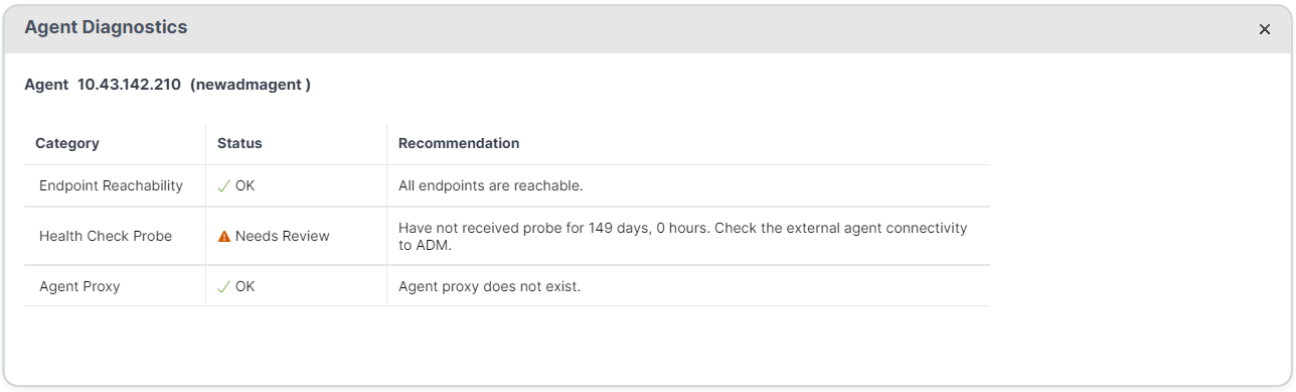
NetScaler Console performs a periodic (every one hour) diagnostic check for the agent and provides the following information:

- **Endpoint reachability** – Checks if all endpoints are reachable. The agent uses various endpoints for the communication between NetScaler Console and NetScaler instances. For more information, see Software Requirements.
- **Health check probe** – Provides the time stamp of the latest health check.
- **Agent proxy** – Checks if the agent proxy exists.

If the agent endpoint reachability status changes (from **OK** to **Needs Review**), the super administrator receives an email notification comprising the issue details. Navigate to **Infrastructure > Instances > Agents** to view the newly added **Diagnostics Status** option that provides the status such as **Needs Review** or **OK**.



Click to view the diagnostic information of an agent.



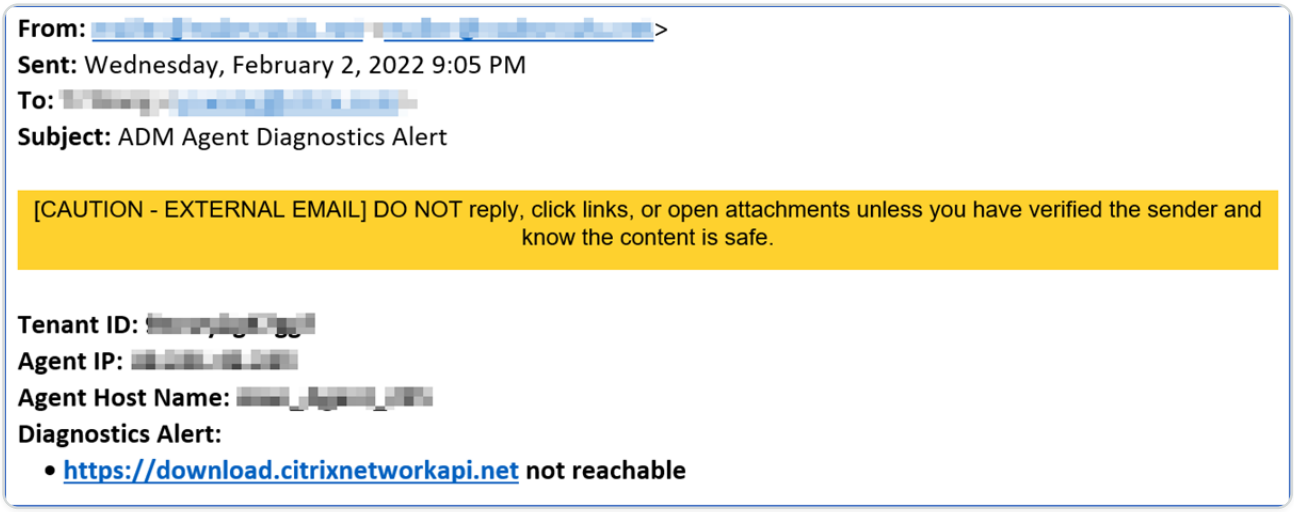
- **Category**. Provides the issue category.
- **Status**. Provides the issue status such as **Needs Review** or **OK**.
- **Recommendation**. Provides the required recommendation to troubleshoot the issue.

After you troubleshoot and the endpoint reachability status changes from **Needs Review** to **OK**, the super administrator receives an email notification mentioning that the issue is resolved.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Email notification

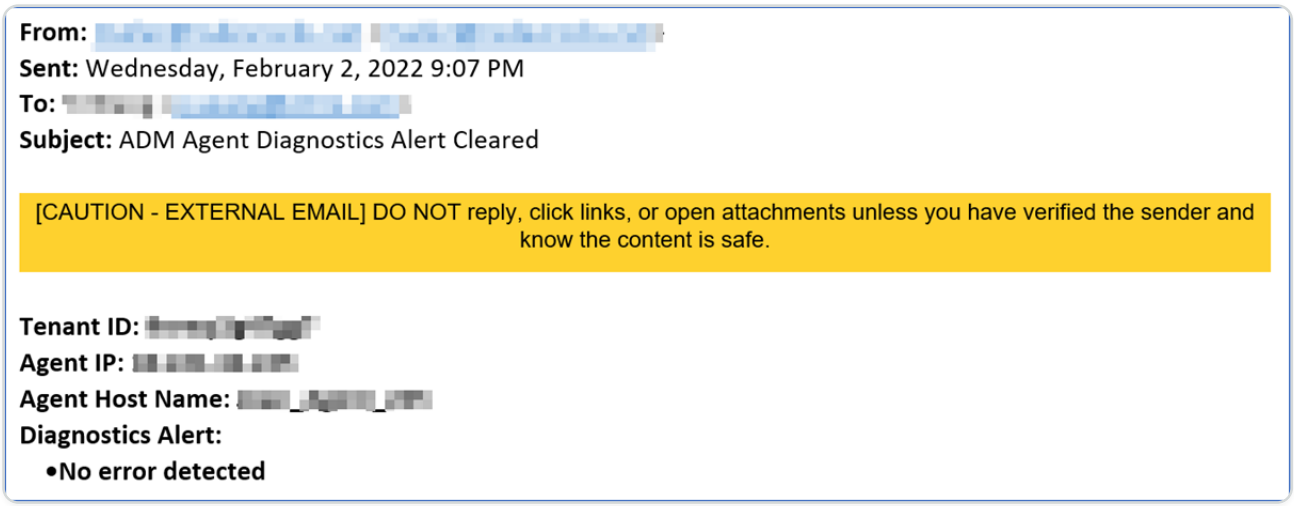
The following example is an email notification after the endpoint reachability status has changed from **OK** to **Needs Review**:


From: [redacted]>
Sent: Wednesday, February 2, 2022 9:05 PM
To: [redacted]
Subject: ADM Agent Diagnostics Alert

[CAUTION - EXTERNAL EMAIL] DO NOT reply, click links, or open attachments unless you have verified the sender and know the content is safe.

Tenant ID: [redacted]
Agent IP: [redacted]
Agent Host Name: [redacted]
Diagnostics Alert:
- **https://download.citrixnetworkapi.net not reachable**

The following example is an email notification after the endpoint reachability status has changed from **Needs Review** to **OK**:


From: [redacted]
Sent: Wednesday, February 2, 2022 9:07 PM
To: [redacted]
Subject: ADM Agent Diagnostics Alert Cleared

[CAUTION - EXTERNAL EMAIL] DO NOT reply, click links, or open attachments unless you have verified the sender and know the content is safe.

Tenant ID: [redacted]
Agent IP: [redacted]
Agent Host Name: [redacted]
Diagnostics Alert:
- **No error detected**

Configure the built-in agent to manage instances

A built-in agent is available on NetScaler MPX, VPX, Gateway instances running the version `12.1.48.13` and later and on NetScaler SDX instances running version 13.0 61.x and later and 12.1 58.x and later. You can initiate this agent on the NetScaler instance instead of installing a dedicated agent in your data center or public cloud. The built-in agent enables communication between the instance and NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The built-in agent is available only on the following NetScaler instance types:

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler Gateway

The built-in agent is ideal for smaller NetScaler standalone or HA pair deployments. If you have multiple NetScaler instances, use a dedicated agent for deployments. This agent ensures you have better data aggregation capabilities than the built-in agent. For more information, see Install an agent on-premises.

NetScaler Console built-in agent supports instance management, monitoring, and Pooled or Flexed licensing. However, the following features are not supported in the built-in agent:

- Application dashboard
- Web Insight
- SSL insight
- HDX™ insight
- Gateway insight
- Security insight
- Advanced analytics
- Pooled or Flexed licensing (file-based licensing)

You can transition from a built-in agent to an external agent. For more information, see Transition from a built-in agent to an external agent.

Prerequisites

Before you configure a built-in agent on the NetScaler instance, ensure the following:

- The NetScaler (MPX, VPX, or Gateway) instance is running on the version `12.1.48.13` or later. The SDX instance is running version `13.0.61.x` and later.
- A DNS name server is added on the NetScaler instance.

  For more information, see Add a name server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You have a Citrix Cloud account. For more information, see Sign up for Citrix Cloud.

NOTE:

For all information related to ports and other system requirements, see System Requirements.

Configure the built-in agent

Perform the following tasks to configure the NetScaler built-in agent:

1. Select the Built-in agent option as instructed in Getting Started.
2. Copy the **Service URL** and **Activation code**.

   The agent uses the service URL to locate the service and the activation code to register with the service. Skip step 7 if you are an MPX or a Gateway customer.
3. Initiate the built-in agent using an SSH client. Gateway users must skip this step.

   a. Log on to your NetScaler instance. For more information, see Access a NetScaler.

   b. Navigate to the `/var/mastools/scripts` directory and type the following command:

   On the SDX instance

	REGISTRATION WITH NETSCALER PROFILE	REGISTRATION WITHOUT NETSCALER PROFILE
Prequisite	Before registering, create a NetScaler profile. For more information, see How to create a NetScaler profile.	
Run this command	`./mastools_init.sh <device-profile-name> <service-url> <activation-code> -sdx -profile`	`./mastools_init.sh <user_name> <service-url> <activation-code> -sdx`
User credential	Enter `nsroot` in `<device_profile_name>`. Alternatively, you can use a user name that has the	Enter `nsroot` in `<user_name>`. Alternatively, you can use a user name that has the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	REGISTRATION WITH NETSCALER PROFILE	REGISTRATION WITHOUT NETSCALER PROFILE
	same access privileges as nsroot.	same access privileges as nsroot.

NOTE:

NetScaler Console discovers all VPX instances running on that SDX and you don't have to register the VPX instances individually.

On VPX instances not running on an SDX appliance and MPX and Gateway instances:

If the NetScaler image version is lower than 13.0 61.x or 12.1 57.x, you must check the `mastools` version by typing the command `cat /var/mastools/version.txt`. If the output is `0.0-0.0`, it is the first time.

Type one of the following commands depending on the software version.

NOTE:

Before registering with a NetScaler profile, you must create the profile. For more information, see How to create a NetScaler profile.

NETSCALER IMAGE VERSION	IS MASTOOLS_VERSION `0.0-0.0` ?	COMMAND FOR REGISTRATION WITH PROFILE	COMMAND FOR REGISTRATION WITHOUT PROFILE
Lower than 13.0 61.xx and 12.1 57.xx	Yes	`./mastools_init.sh <device_profile_name> <service_url> "MAS;<activation_code>" -profile`	`./mastools_init.sh <user_name> <pwd> <service_url> "MAS;<activation_code>"`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETSCALER IMAGE VERSION	IS MASTOOLS_VERSION `0.0-0.0` ?	COMMAND FOR REGISTRATION WITH PROFILE	COMMAND FOR REGISTRATION WITHOUT PROFILE
Lower than 13.0 61.xx and 12.1 57.xx	No	`./mastools_init.sh <device_profile_name> <service_url> <activation_code> -profile`	`./mastools_init.sh <user_name> <pwd> <service_url> <activation_code>`
Higher than 13.0 61.x and 12.1 57.xx	Not applicable	`./mastools_init.sh <device_profile_name> <service_url> <activation_code> -profile`	`./mastools_init.sh <user_name> <pwd> <service_url> <activation_code>`

NOTE:

- In `<device_profile_name>` or `<user_name>`, enter `nsroot`. Alternatively, you can use a user name that has the same access privileges as nsroot.
- In an HA pair, complete the registration on the primary node. If you run the registration commands on the secondary node, the following message appears: **Please run the registration command on the primary node**.

4. Return to the NetScaler Console page and click **Register Instance**.
5. In **Add Instances**, view the instance where you initiated the built-in agent. Ensure that the instance is in the **Up** status and click **Next**.
6. Click **Done**.

After successful built-in agent configuration, you can access the NetScaler Console features such as:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Virtual server and analytics** – Apply licenses to your virtual server to manage NetScaler instances. For more information, see Manage subscriptions.
- **Application dashboard** – To view all applications in a holistic way. For more information, see Application management and dashboard.
- **Infrastructure analytics** – This feature helps you to visualize the factors that resulted or might result in an issue on the instances. For more information, see Infrastructure Analytics.

Configure license server through NetScaler® built-in agent

NOTE:

NetScaler built-in agent cannot be assigned the LSA role.

If you have a License Server Agent (LSA) configured in one site and want to use the same LSA from other sites, you can use a NetScaler built-in agent. While using the built-in agent, you must configure the license server using the following command on the NetScaler instance.

```
add licenseserver 127.0.0.1 -port 27000
```

In this configuration, NetScaler can reach the License Server Agent (LSA) through Console service.

NOTE:

You can also configure the built-in agent by navigating to the **Infrastructure > Instances > Agents > Generate Activation code** page. Copy and paste the URL and activation code to a NetScaler instance and discover that instance.

After the built-in agent is initiated, navigate to **Infrastructure > Instances > NetScaler**. This page displays the details about the managed instance discovered using the built-in agent.

Troubleshooting

You can check logs if registration fails or if registration succeeds but the built-in agent does not appear in the NetScaler Console GUI.

- If registration fails, check logs in `/var/mastools/logs/mastools_reg.py.log`
- If registration succeeds, but the built-in agent does not appear in the NetScaler Console GUI, check:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Mastools_upgrade** logs in `/var/mastools/logs/mastools_upgrade.log`
- **Binary logs** in `/var/log/mastoolsd.log`.

Install a NetScaler agent on-premises

The agent works as an intermediary between the NetScaler Console and the discovered instances in the data center.

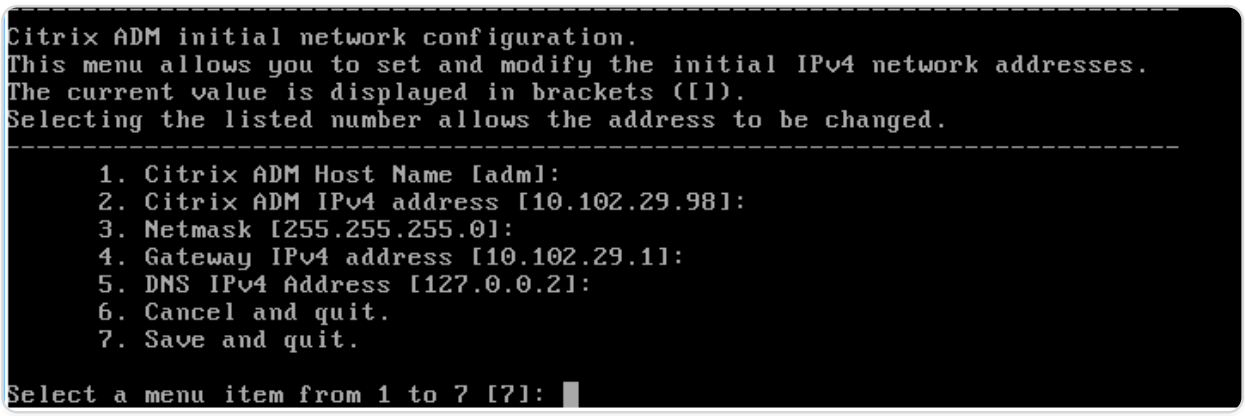
Before you begin installing the agent, ensure that you have the required virtual computing resources that the hypervisor must provide for each agent. For more information, see Agent installation requirements and Lightweight agent for pooled licensing.

NOTE

For all information related to ports and other requirements, see Supported Ports.

To install the NetScaler agent:

1. Download the agent image as instructed in Getting Started.
2. Import the agent image file to your hypervisor.
3. From the **Console** tab, configure the initial network configuration options as shown in the following example:



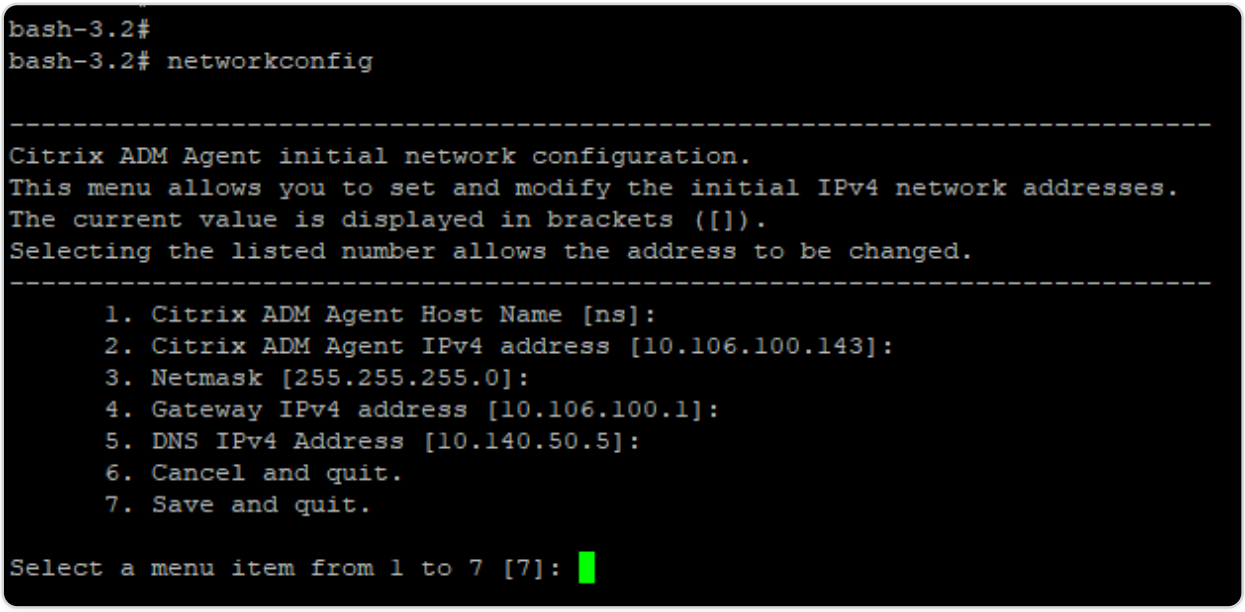
NOTE

Ensure that you configure your DNS to allow Internet access to your NetScaler agent.

4. After completing the initial network configuration, save the configuration settings. When prompted, log on using the default (`nsrecover/nsroot`) credentials.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you want to change the configured network settings on the agent, type the `networkconfig` command and follow the prompts in the CLI.

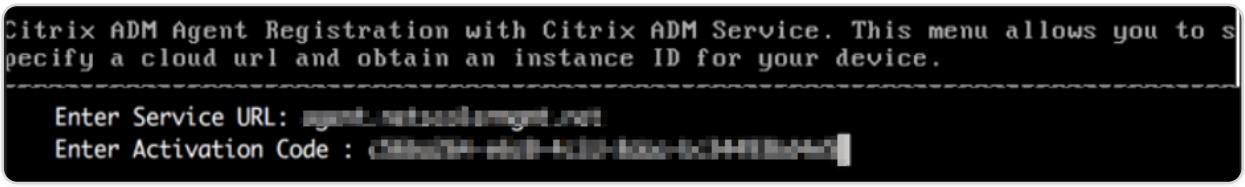


5. If there is no prompt to enter the Service URL, navigate to /mps in the NetScaler agent and then run any one of the following scripts:

```
deployment_type.py
```

```
register_agent_cloud.py
```

6. Enter the **Service URL** and the **Activation Code** that you saved when you had downloaded the agent image. The agent uses the Service URL to locate the service and the activation code to register with the service.

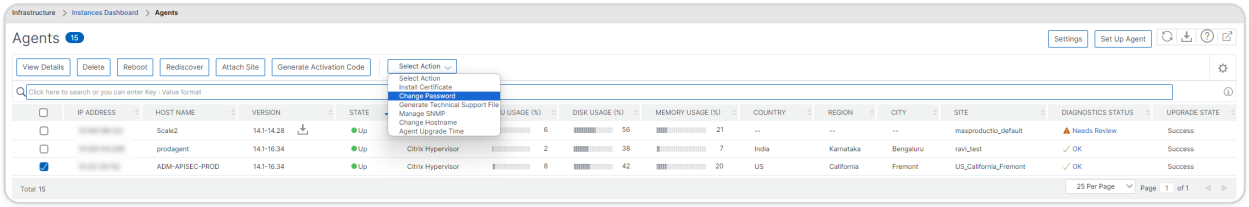


7. After agent registration is successful, the agent restarts to complete the installation process.

After the agent has restarted, access the NetScaler Console GUI and navigate to **Infrastructure > Instances > Agents** to verify the status of the agent. After the agent is configured, you must change the password.

1. Navigate to **Infrastructure > Instances > Agents**
2. Select the agent and from the **Select Action** list, click **Change Password**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Enter the current password (`nsroot`), then specify a new password, and click **OK** to change the password.

   The password must:

   - Be at least six characters in length
   - Have at least one special character
   - Have at least one upper case character
   - Have at least one lower case character
   - Have at least one numeric character

   NOTE:

   After you configure the NetScaler agent on-premises, we recommend waiting up to 10 minutes before applying a license to a NetScaler instance.

Install a NetScaler agent on Microsoft Azure cloud

The agent works as an intermediary between the NetScaler Console and the managed instances in the enterprise data center, or on the cloud.

To install the NetScaler agent on the Microsoft Azure cloud, you have to create an instance of the agent in the virtual network. Obtain the NetScaler agent image from the Azure Marketplace, and then use the Azure Resource Manager portal to create the agent.

Before you begin creating the NetScaler agent instance, make sure that you have created a virtual network with the required subnets where the instance resides. You can create virtual networks during VM provisioning, but without the flexibility to create different subnets. For information, see *Azure documentation*.

Configure DNS server and VPN connectivity that allows a virtual machine to access Internet resources.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prerequisites

Make sure that you have the following:

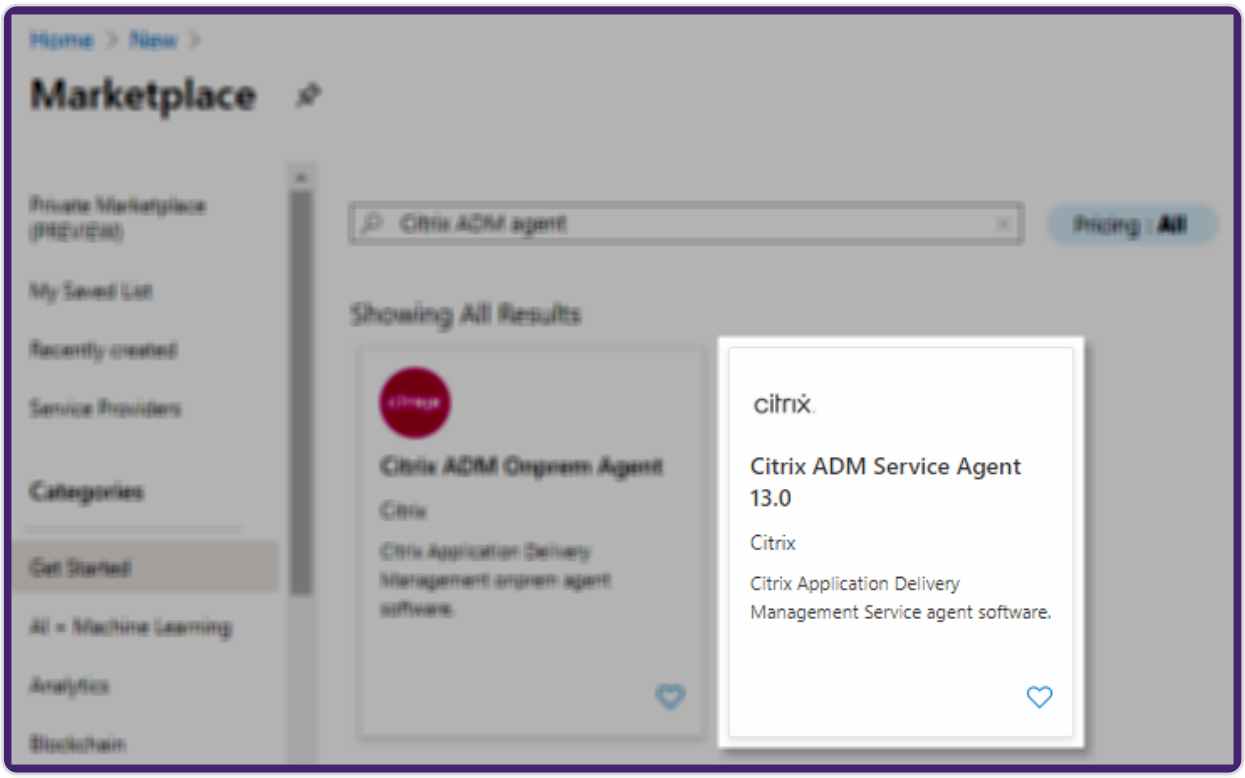
- A Microsoft Azure user account
- Access to Microsoft Azure Resource Manager

NOTES

- We recommend that you create resource group, network security group, virtual network, and other entities before you provision the NetScaler agent virtual machine, so that the network information is available during provisioning.
- For the NetScaler agent to communicate with NetScaler Console and the NetScaler instances, ensure that the recommended ports are open. For complete details about the port requirements for the NetScaler agent, see Ports.

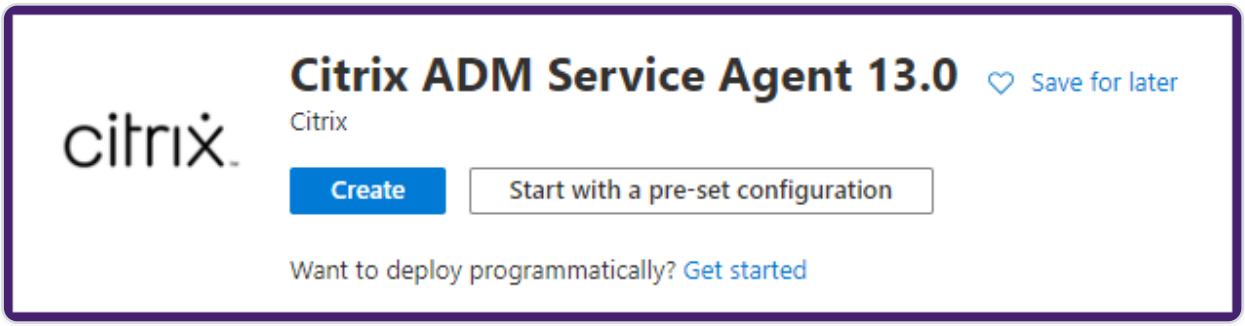
To install the NetScaler agent on Microsoft Azure Cloud:

1. Log on to the Azure portal (https://portal.azure.com) by using your Microsoft Azure credentials.
2. Click **+Create a resource**.
3. Type `NetScaler agent` in the search bar and select **NetScaler agent**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Click **Create**.

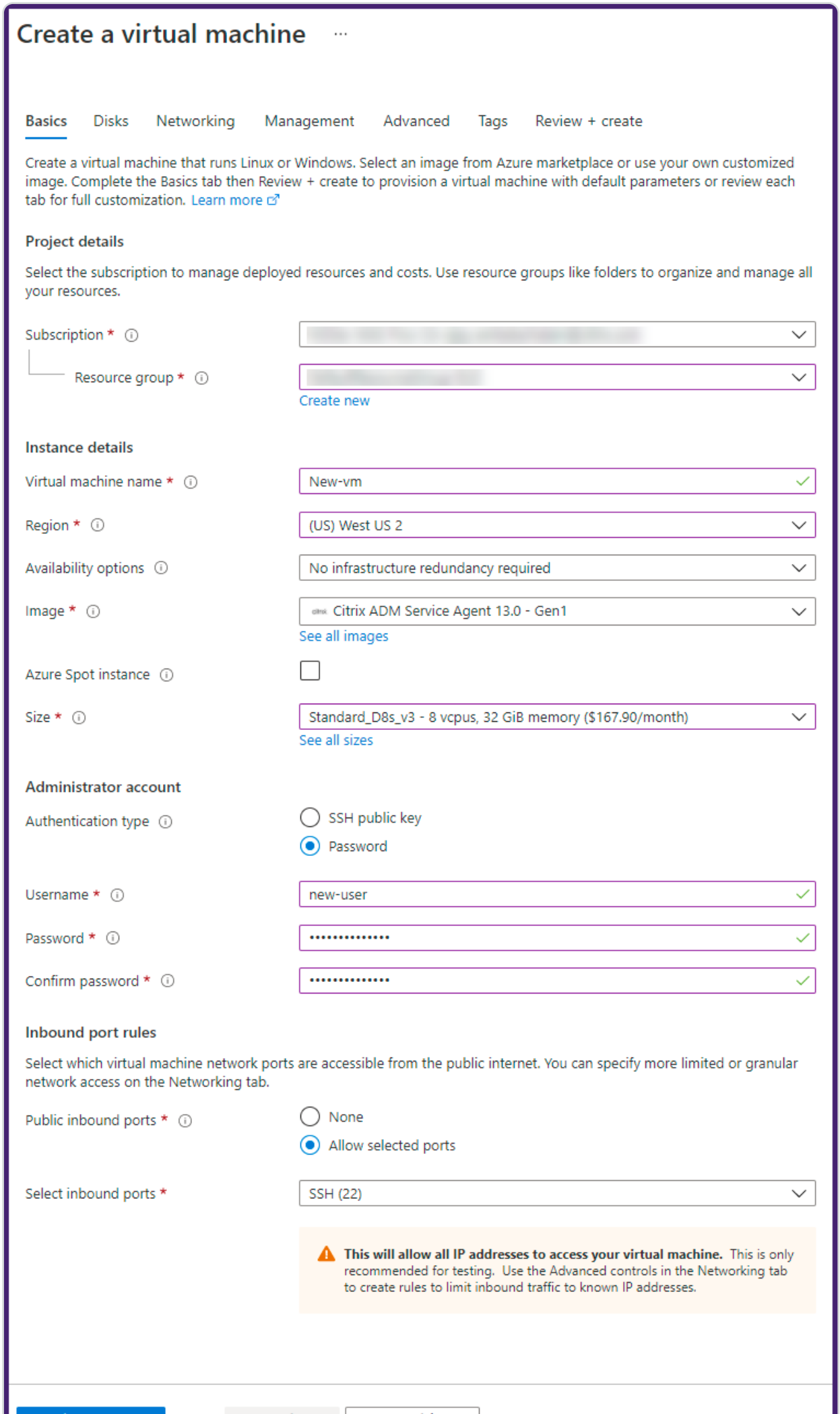


5. In the **Create virtual machine** pane, specify the required values in each section to create a virtual machine.

   Basics:

   In this tab, specify **Project details**, **Instance details**, and **Administrator account**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.


Create a virtual machine
Basics
Disks
Networking
Management
Advanced
Tags
Review + create
Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more
Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription *
Resource group *
Create new
Instance details
Virtual machine name *
New-vm
Region *
(US) West US 2
Availability options
No infrastructure redundancy required
Image *
Citrix ADM Service Agent 13.0 - Gen1
See all images
Azure Spot instance
Size *
Standard_D8s_v3 - 8 vcpus, 32 GiB memory ($167.90/month)
See all sizes
Administrator account
Authentication type
SSH public key
Password
Username *
new-user
Password *
Confirm password *
Inbound port rules
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.
Public inbound ports *
None
Allow selected ports
Select inbound ports *
SSH (22)
This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

- **Resource group** – Select the resource group that you have created from the drop-down list.

  \>**Note**

  You can create a resource group at this point, but we recommend that you create a resource group from

  RESOURCE GROUPS

  in the Azure Resource Manager and then select the group from the drop-down list.

- **Virtual machine name** – Specify a name for the NetScaler agent instance.
- **Region** - Select the region where you want to deploy an agent.
- **Availability options** – Select the availability set from the list.
- **Image** - This field displays the already selected agent image. If you want to change to a different agent image, select the required image from the list.
- **Size** - Specify the type and size of the virtual disk for deploying your NetScaler agent.

  Select the Supported virtual disk type (**HDD** or **SSD**) from the list.

  For more information about supported virtual disk sizes, see Agent installation requirements and Lightweight agent for pooled licensing.
- **Authentication Type** – Select Password.
- **Username and Password** – Specify a username and password to access the resources in the resource group that you have created.

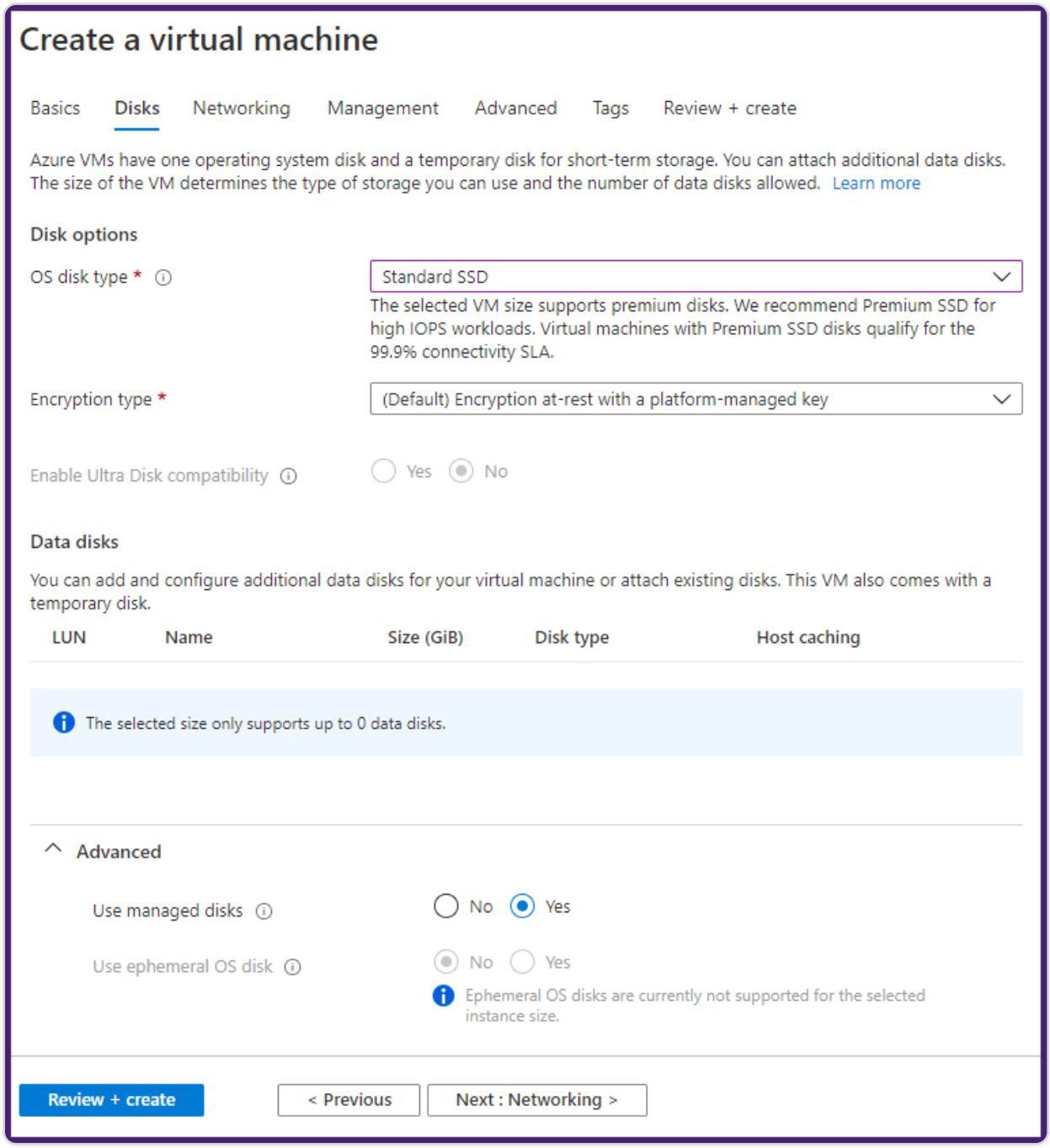
  IMPORTANT

  - We recommend you specify your own username and password for your agent. Do not use `nsrecover` or `nsroot` as the username because they are reserved for agent users.
  - During provisioning, set a username that is not `nsroot` or `nsrecover`. However, the first login after provisioning must use `nsrecover` as the username .

Disks:

In this tab, specify **Disk options** and **Data disks**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

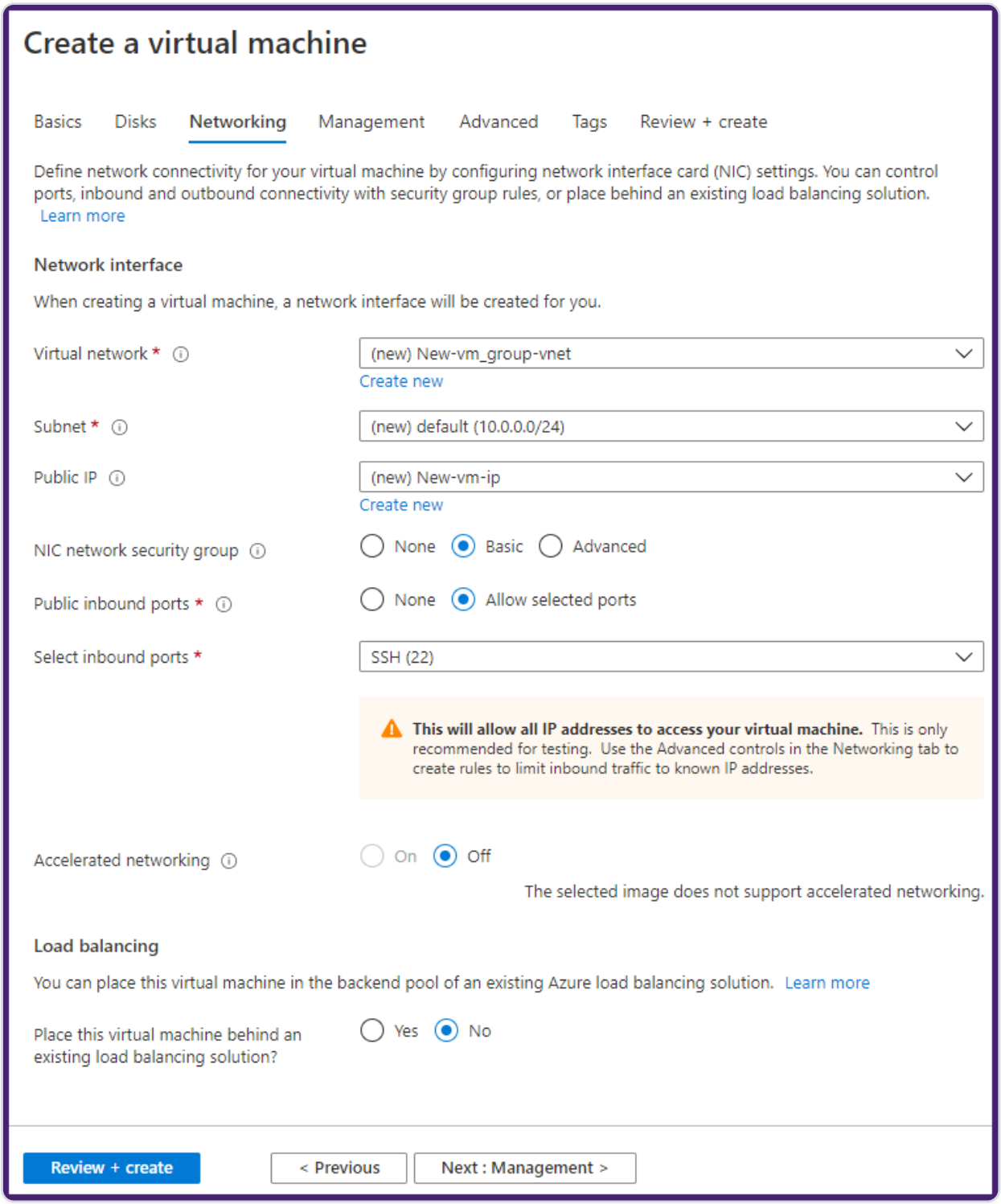


- **OS disk type** - Select the virtual disk type (HDD or SSD).

Networking:

Specify the required networking details:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Virtual network** – Select the virtual network.
- **Subnet** – Set the subnet address.
- **Public IP address** - Optional, select the IP address.
- **Network security group** – Optional, select the security group that you have created.
- **Select inbound ports** - If you allow public inbound ports, ensure the inbound and outbound rules are configured in the security group. Then, select the inbound ports from the list. For more details, see Prerequisites.

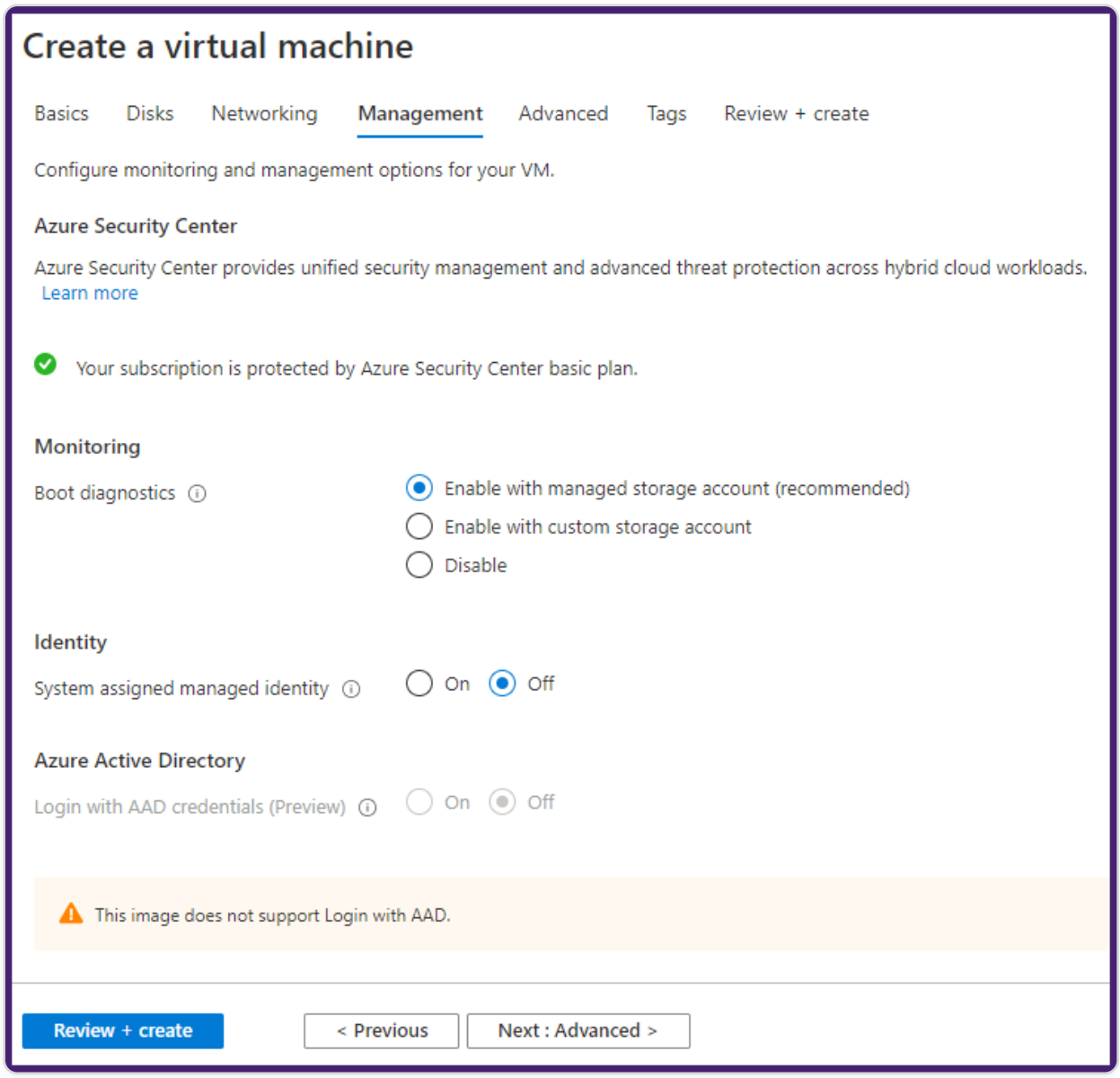
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

Ensure that agent has Internet access.

Management:

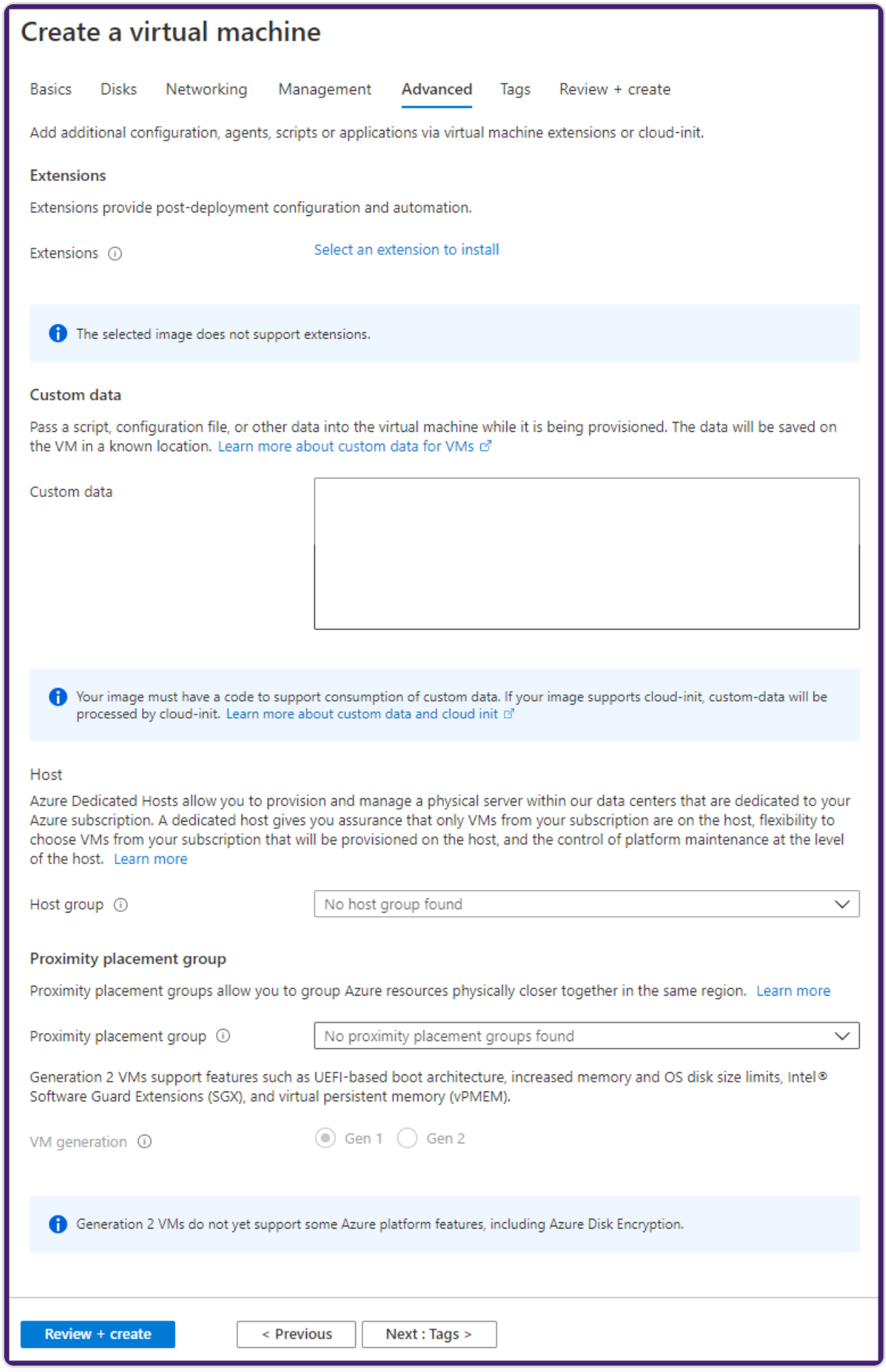
Specify **Azure Security Center**, **Monitoring**, and **Identity**.



Advanced:

Optional, specify **Extensions**, **Custom Data**, and **Proximity placement group**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

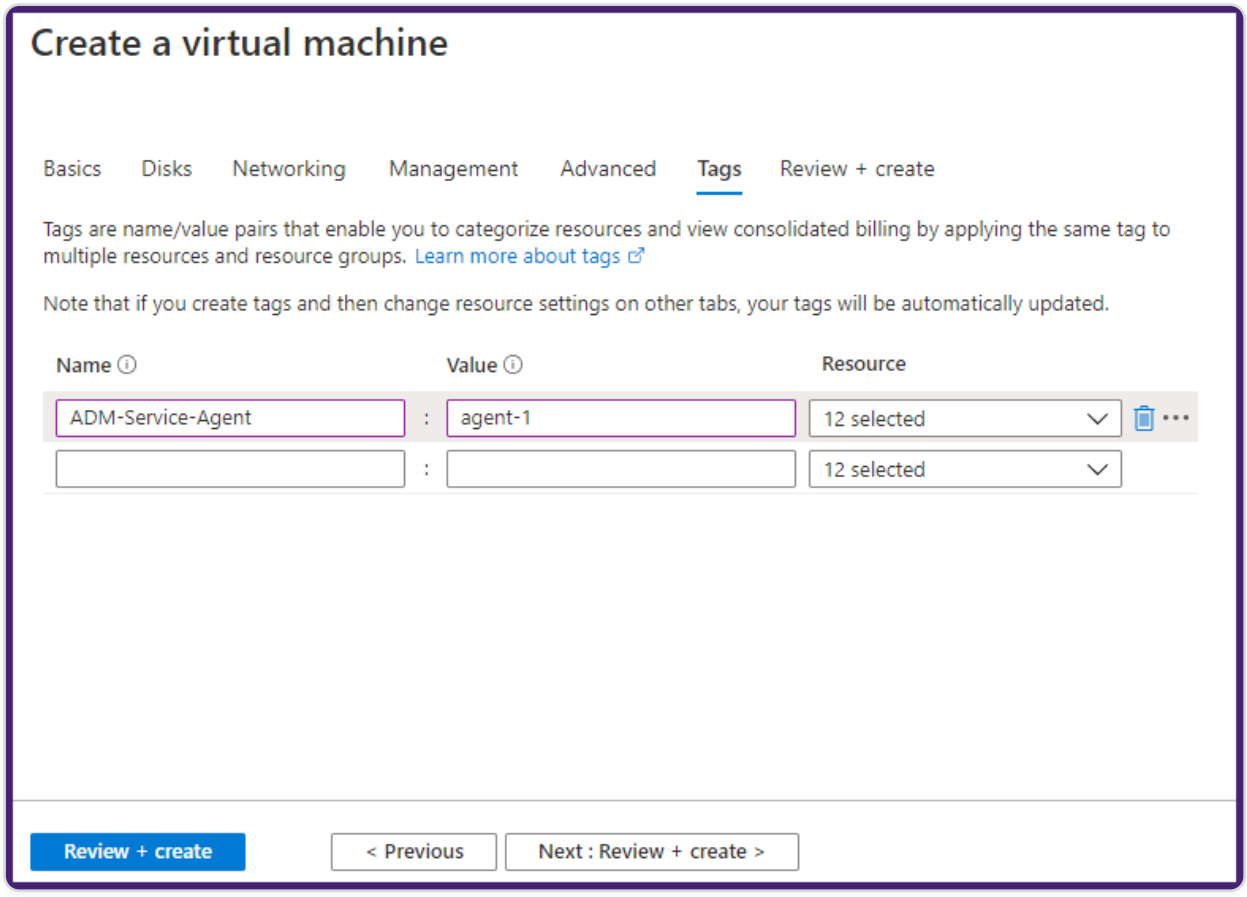
In **Custom Data**, specify the **Service-URL** and **Activation code** that you copied from the **Set Up Agents** page in NetScaler Console as instructed in Getting Started. Enter the details in the following format:

```
registeragent -serviceurl &lt;apigatewayurl> -activationcode
&lt;activationcodevalue>
```

Agent uses this information to auto-register with the NetScaler Console during boot-up.
If you specify this auto-registration script, skip step 7 and 8.

Tags:

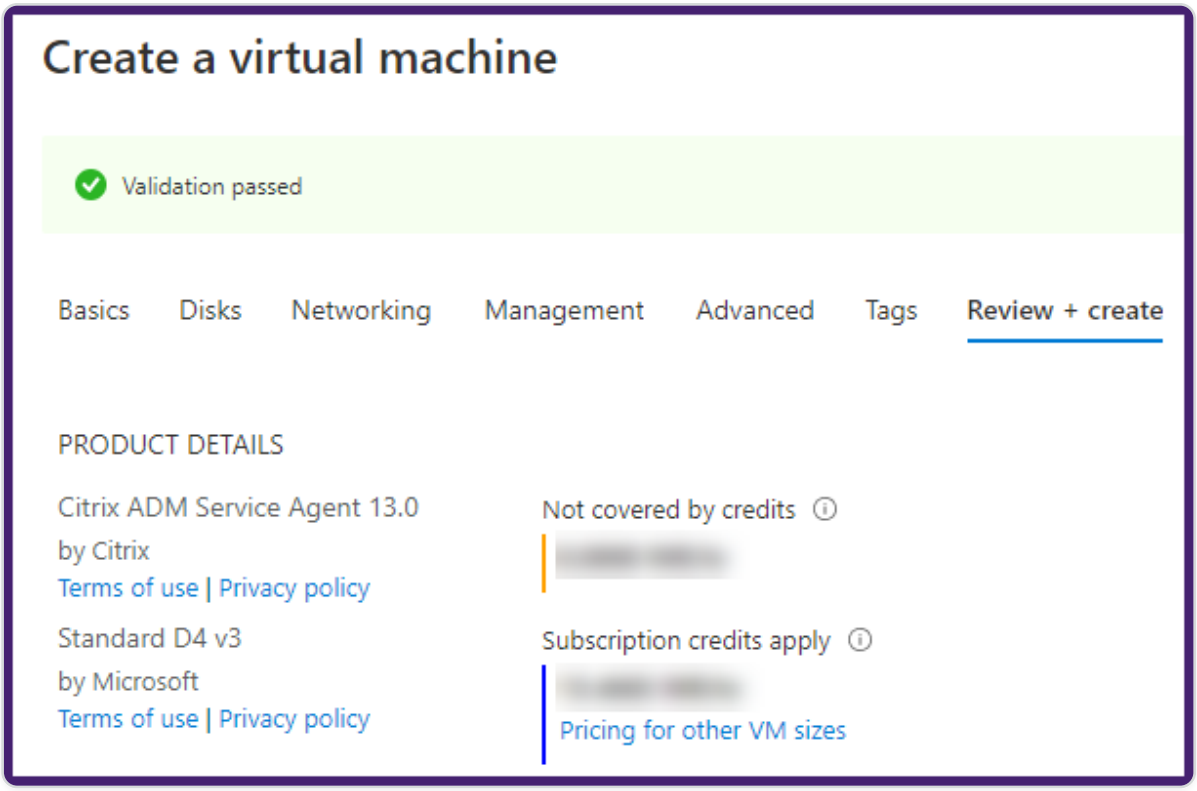
Type the key-value pair for the NetScaler agent tags. A tag consists of a case-sensitive key-value pair. These tags enable you to organize and identify the agent easily. The tags are applied to both Azure and NetScaler Console.



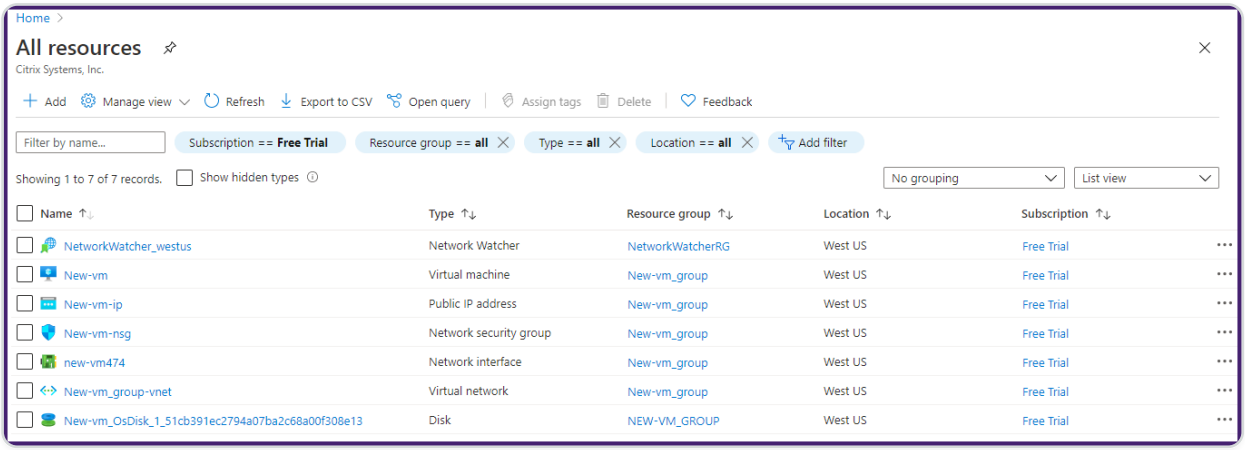
The configuration settings are validated and the **Review and create** tab displays the result of the validation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If the validation fails, this tab displays the reason for the failure. Go back to the particular section and make changes as required.
- If the validation passes, click **Create**. The agent deployment process begins.



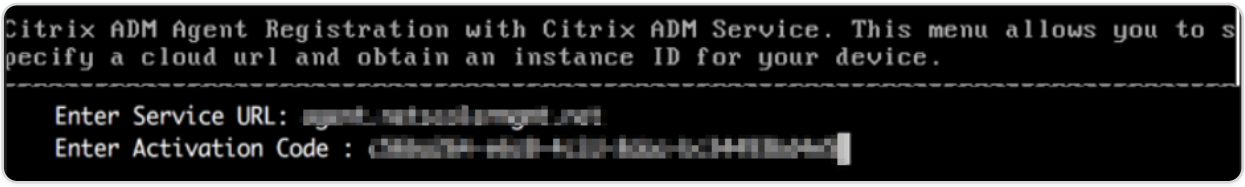
The deployment process might take approximately 10–15 minutes. Once the deployment is successfully completed, you can view your NetScaler agent virtual machine in your Microsoft Azure account.



6. Once the agent is up and running, use an SSH client to log on to your NetScaler agent. Use the username and password that was specified during the virtual machine creation.
7. Run the deployment script by typing the command at the shell prompt: **deployment_type.py**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Enter the **Service-URL** and the **Activation code** that you copied and saved from the **Set Up Agents** page in NetScaler Console as instructed in Getting Started. The agent uses the service URL to locate the service and the activation code to register with the service.



After agent registration is successful, the agent restarts to complete the installation process.

After the agent has restarted, access NetScaler Console and on the **Set Up Agent** page, under **Discovered Agents**, verify the status of the agent.

Install a NetScaler agent on Amazon Web Services (AWS)

The NetScaler agent works as an intermediary between the NetScaler Console and the discovered instances in the data center or on the cloud.

Prerequisites

To launch a NetScaler agent AMI within an Amazon Web Services (AWS) Virtual Private Cloud (VPC) by using the Amazon GUI, you need:

- An AWS account
- An AWS virtual private cloud (VPC)
- An IAM account
- A Service URL and Activation code for the agent to connect to NetScaler Console service. In NetScaler Console service GUI, navigate to **Infrastructure > Instances > Agents** and click **Generate Activation Code** to generate your Service URL and Activation code.

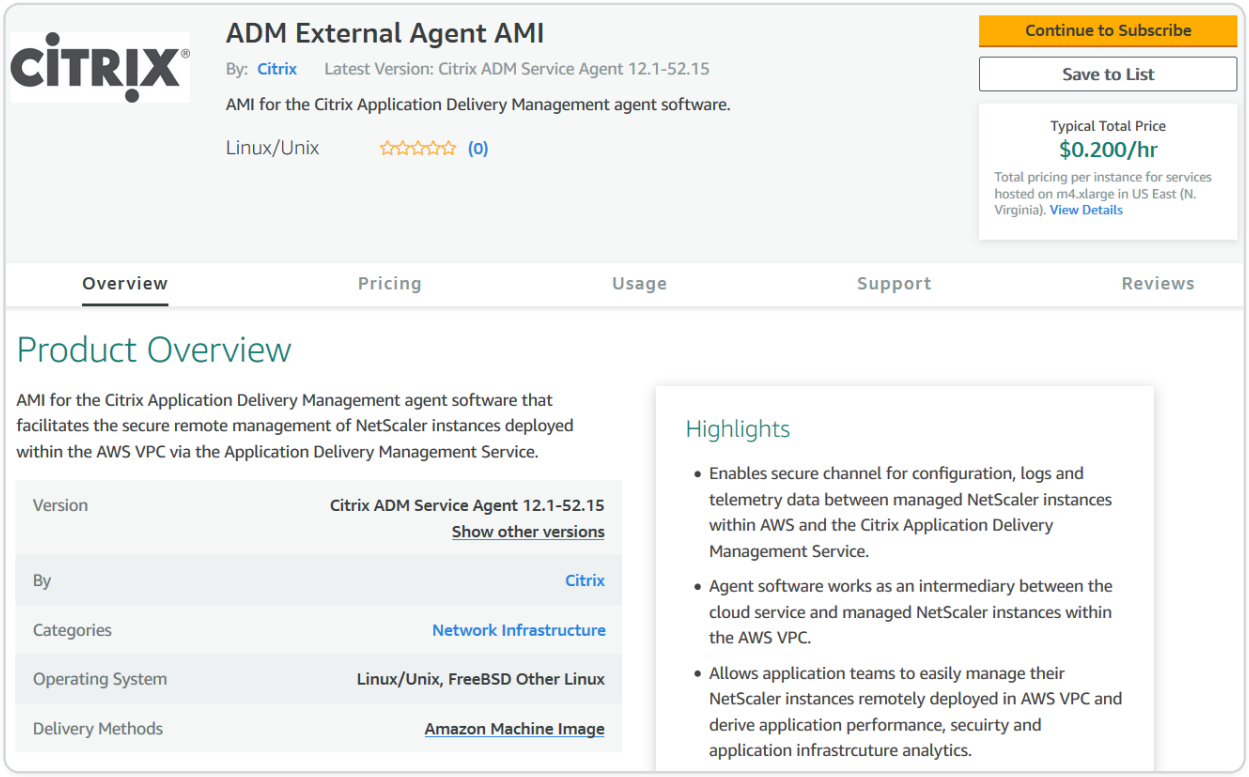
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

- Before you provision a NetScaler agent virtual machine, Citrix recommends creating security group, virtual private network, key pair, subnet, and other entities. So, the network information is available during provisioning.
- For a NetScaler agent to communicate with the NetScaler Console, and the NetScaler instances, ensure that the recommended ports are open. For complete details about the port requirements for a NetScaler agent, see Ports.

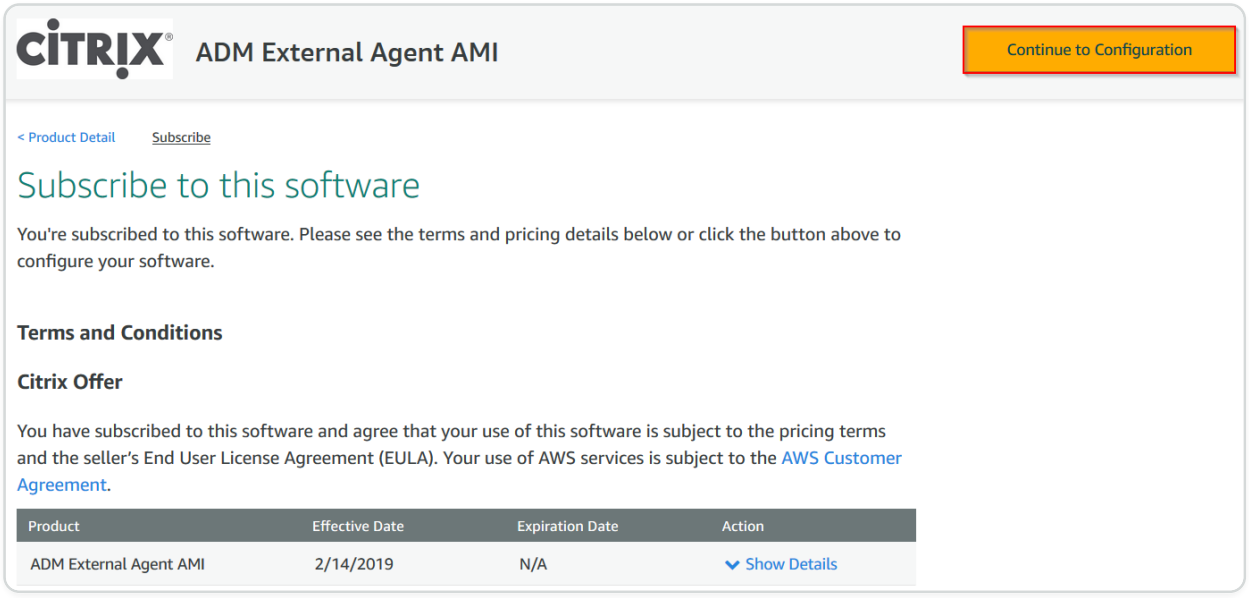
To install the NetScaler agent on AWS:

1. Log on to the AWS marketplace by using your AWS credentials.
2. In the search field, type **NetScaler agent** to search for the NetScaler agent AMI, and click **Go**.
3. On the search result page, click the **NetScaler Console External agent AMI** from the available list.
4. On the **NetScaler Console External Agent AMI** page, click **Continue to Subscribe**.



5. After the subscription is successful, click **Continue to Configuration**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



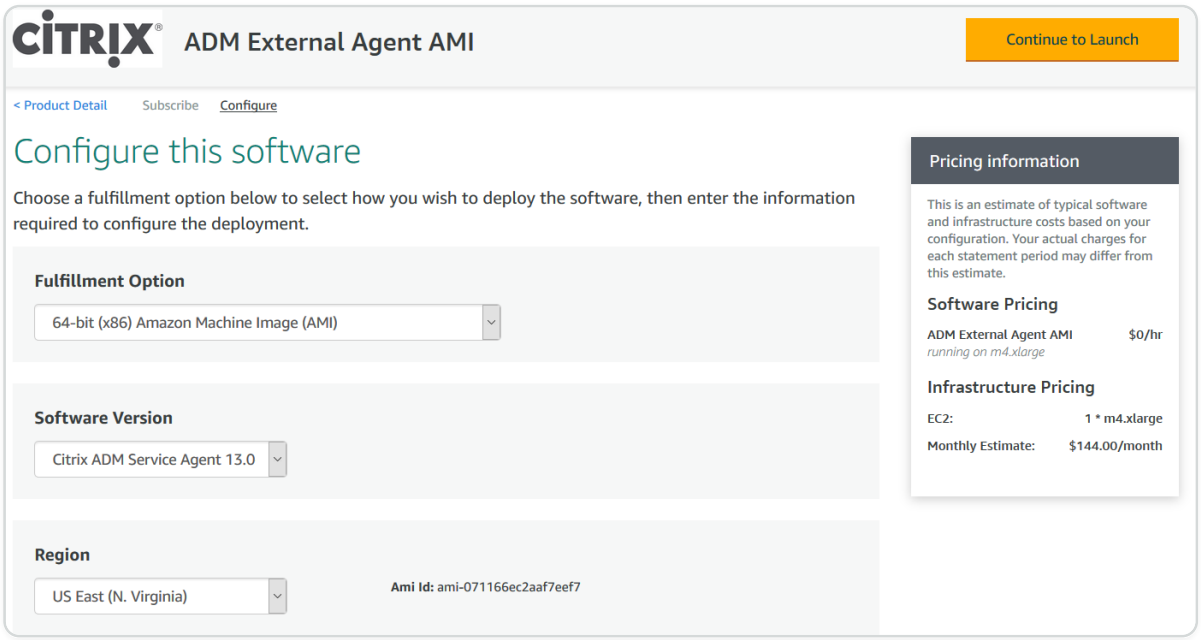
6. On the **Configure this software** page:

   a. Select the AMI from the **Fulfillment option** list.

   b. Select the latest NetScaler agent version from the **Software Version** list.

   c. Select your region from the **Region** list.

   d. Click **Continue to Launch**

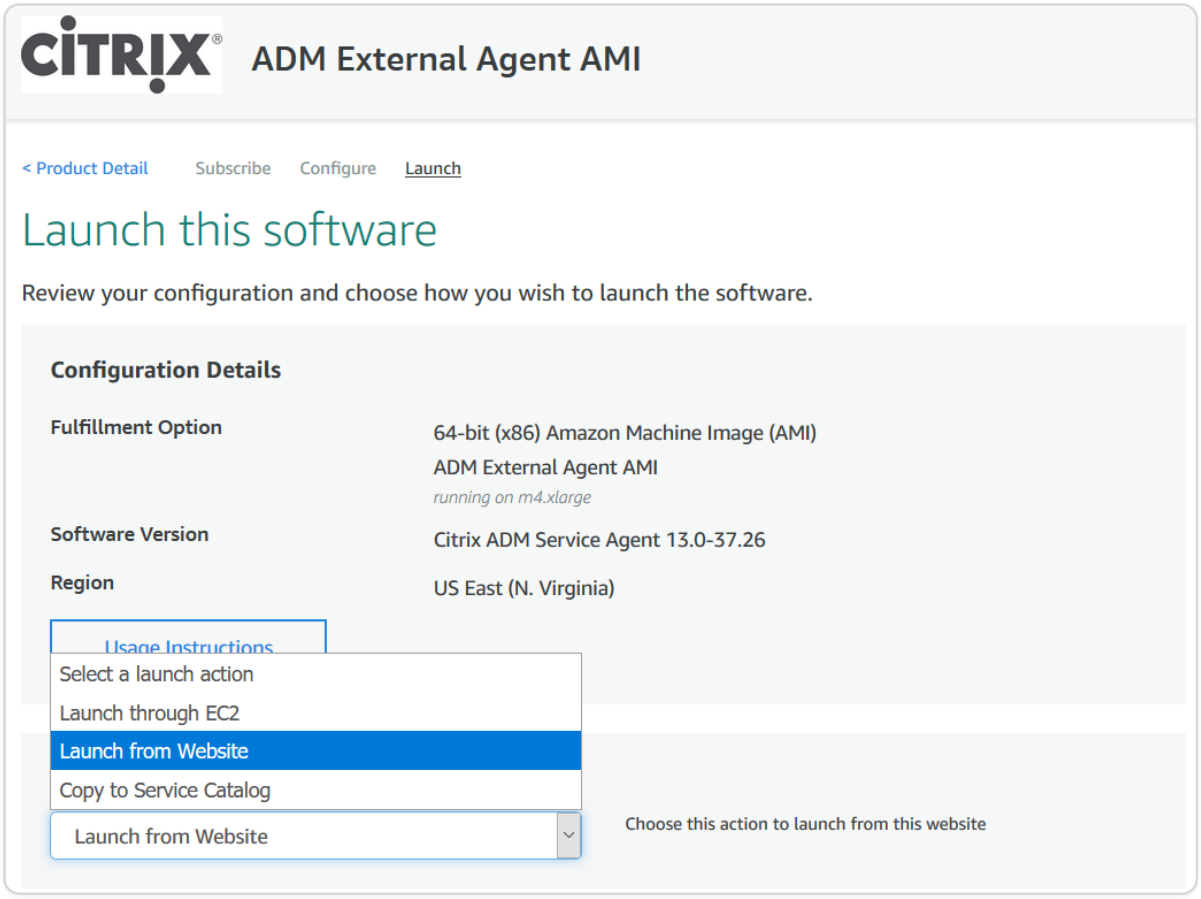


7. On the **Launch this software** page, you have two options to register the NetScaler agent:

   a. **Launch from Website**

   b. **Launch with EC2**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

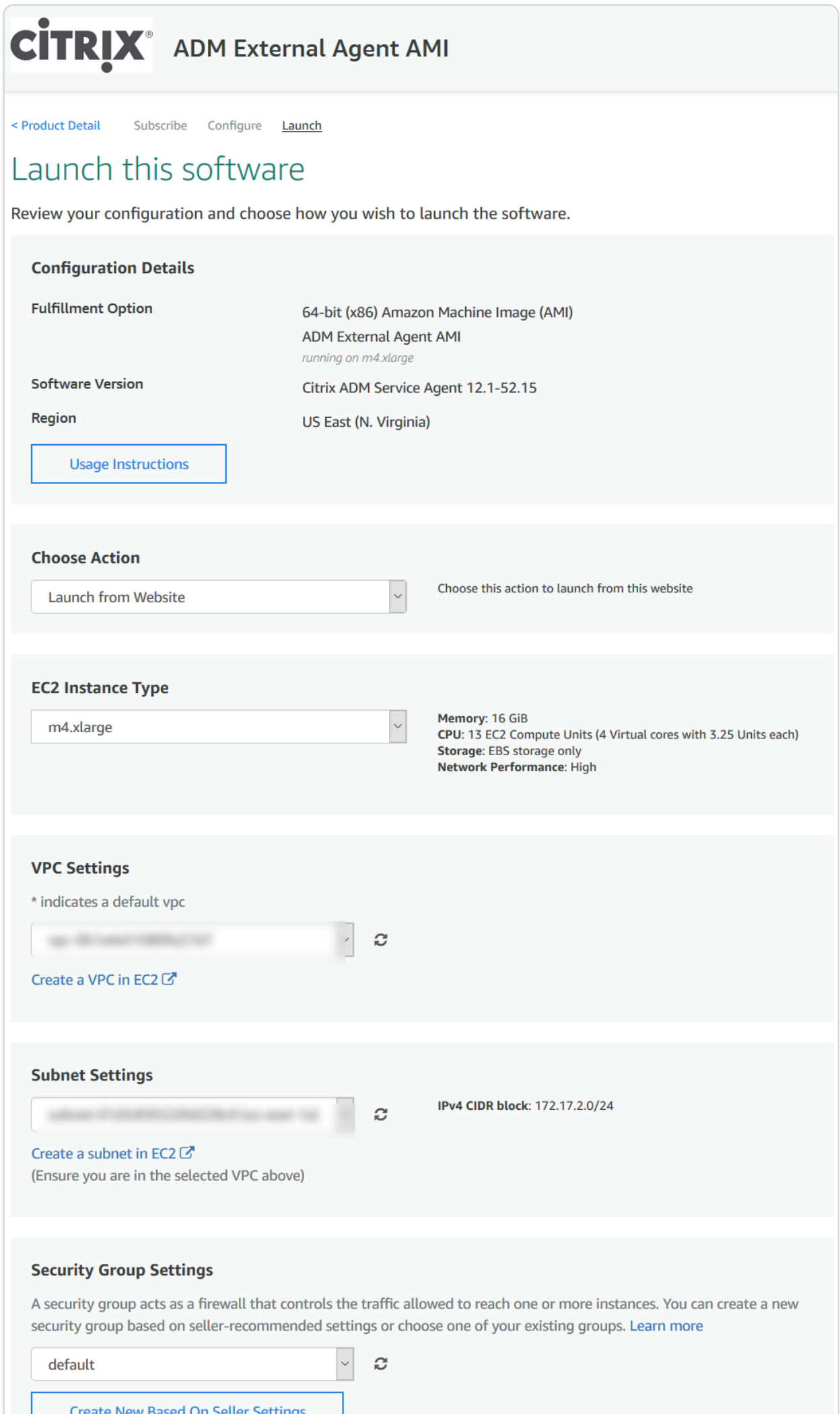


Launch from a Website

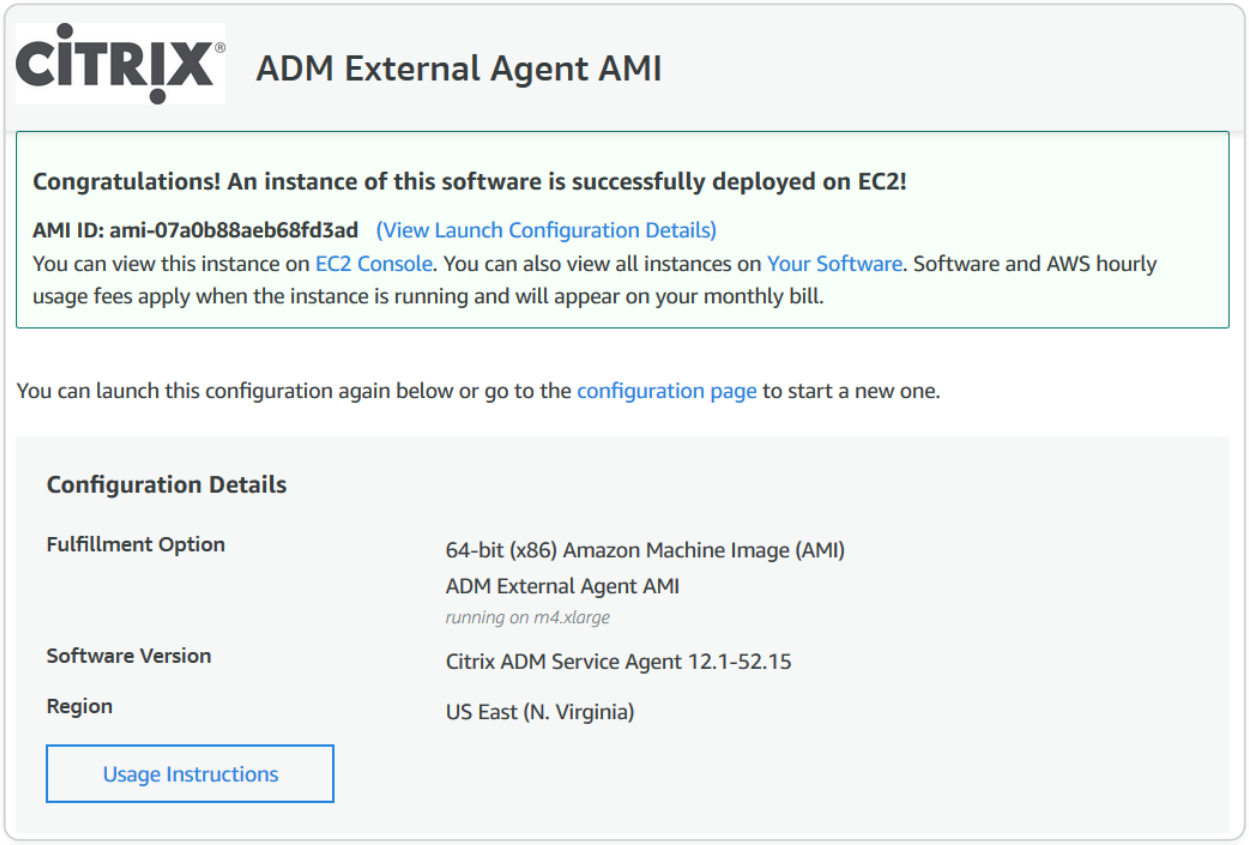
To launch from a Website, select:

1. An EC2 instance type from the **EC2 Instance Type** list
2. A VPC from the **VPC Settings** list. Click **Create a VPC in EC2** to create a VPC for your software.
3. A Subnet from the **Subnet Settings** list. Click **Create a subnet in EC2** to create a subnet after you selected the VPC.
4. A security group for the firewall from the **Security Group Settings** list. Click **Create New Based On Seller Settings** to create a security group.
5. A key pair to ensure access security from the **Key Pair Settings** list. Click **Create a key pair in EC2** to create a key pair for your software.
6. Click **Launch**

© 1997–2026 Citrix Systems, Inc. All rights reserved.


ADM External Agent AMI
< Product Detail
Subscribe
Configure
Launch
Launch this software
Review your configuration and choose how you wish to launch the software.
Configuration Details
Fulfillment Option
64-bit (x86) Amazon Machine Image (AMI)
ADM External Agent AMI
running on m4.xlarge
Software Version
Citrix ADM Service Agent 12.1-52.15
Region
US East (N. Virginia)
Usage Instructions
Choose Action
Launch from Website
Choose this action to launch from this website
EC2 Instance Type
m4.xlarge
Memory: 16 GiB
CPU: 13 EC2 Compute Units (4 Virtual cores with 3.25 Units each)
Storage: EBS storage only
Network Performance: High
VPC Settings
* indicates a default vpc
Create a VPC in EC2
Subnet Settings
IPv4 CIDR block: 172.17.2.0/24
Create a subnet in EC2
(Ensure you are in the selected VPC above)
Security Group Settings
A security group acts as a firewall that controls the traffic allowed to reach one or more instances. You can create a new security group based on seller-recommended settings or choose one of your existing groups. Learn more
default
Create New Based On Seller Settings

7. The launch from a Website is successful.



NOTE

The deployment process might take approximately 10–15 minutes. After the deployment is successfully completed, you can view your NetScaler agent virtual machine on your AWS account.

8. Once the agent is deployed, assign a name for your NetScaler agent.
9. Once the agent is up and running, assign an elastic IP address for your NetScaler agent.

NOTE

Elastic IP address enables NetScaler agent to communicate with NetScaler Console. But, an elastic IP address might not be required if you have configured NAT Gateway to route the traffic to the Internet.

10. Using an SSH client, log on to your NetScaler agent.

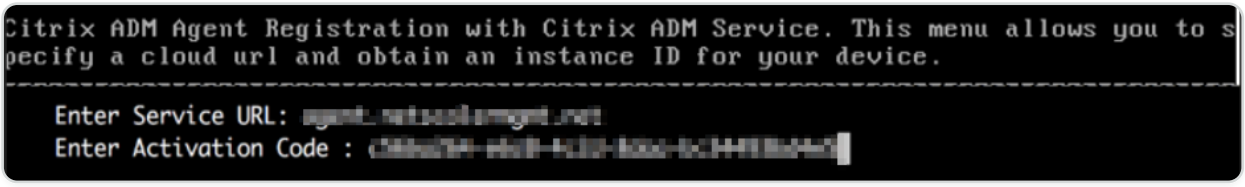
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

You can log on to the NetScaler agent using one of the following ways:

- Use `nsrecover` as the user name and AWS instance ID as the password.
- Use `nsroot` as the user name and a valid keypair as the password.

11. Enter the following command to invoke the deployment screen: **deployment_type.py**
12. Enter the **Service-URL** and the **Activation code** that you had copied and saved from the **Set Up Agents** page in NetScaler Console as instructed in Getting Started. The agent uses the service URL to locate the service and the activation code to register with the service.



After agent registration is successful, the agent restarts to complete the installation process.

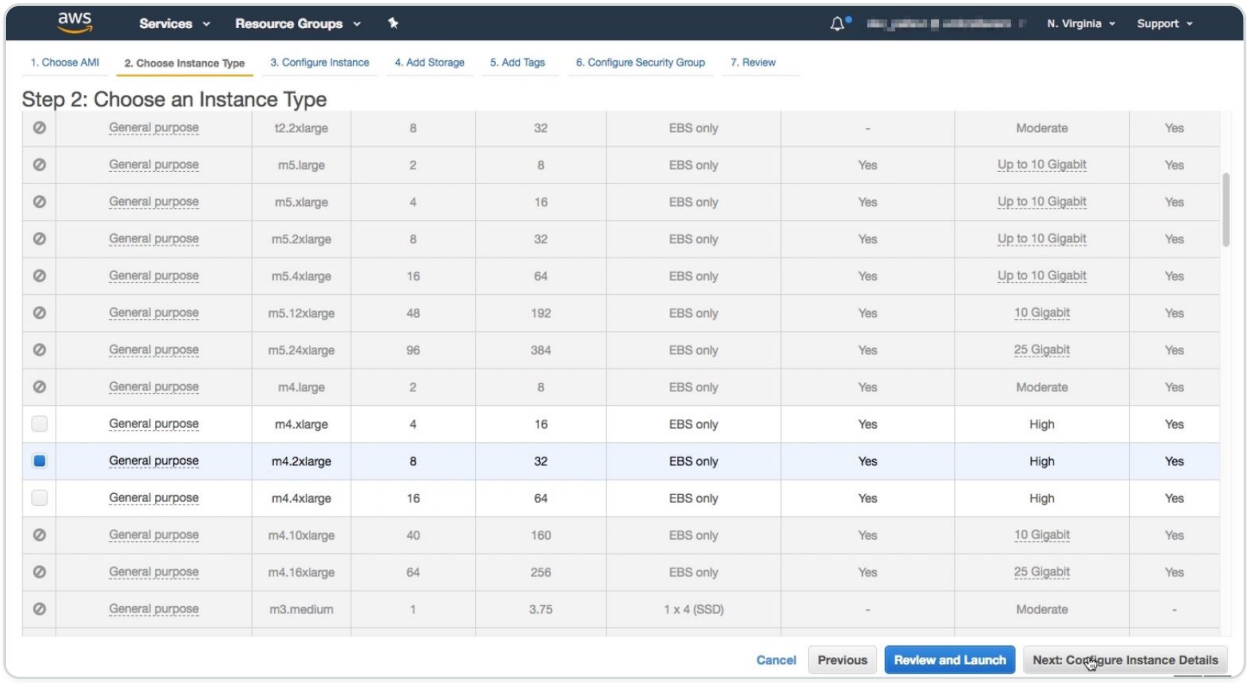
After the agent has restarted, access NetScaler Console and on the **Set Up Agent** page, under **Discovered Agents**, verify the status of the agent.

Launch with EC2

To launch with EC2, select **Launch through EC2** from the **Choose Action** list, and then click **Launch**.

1. On the **Choose an Instance Type** page, select the instance, and click **Next: Configure Instance Details**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. On the **Configure Instance Details** page, specify the required parameters.

   Under the **Advanced Details** section, you can enable a zero-touch agent by specifying authentication details or a script in the **User data** field.

   - **Authentication details** - Specify the **Service-URL** and **Activation code** that you copied from the **Set Up Agents** page in NetScaler Console as instructed in Getting Started. Enter the details in the following format.

     ```
     registeragent -serviceurl <apigatewayurl> -activationcode
     <activationcodevalue>
     ```

     Agent uses this information to auto-register with the NetScaler Console during boot-up.

   - **Script** - Specify an agent auto-registration script as user data. The following is an example script:

     ```
     #!/var/python/bin/python2.7

     import os

     import requests

     import json

     import time
     ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
import re

import logging

import logging.handlers

import boto3



'''

Overview of the Script:

The script helps to register a NetScaler agent with NetScaler
Console. Pass it in userdata to make NetScaler agent in AWS to
autoregister on bootup. The workflow is as follows

1)  Fetch the NetScaler Console API credentials (ID and secret) from
AWS secret store (NOTE: you have to assign IAM role to the NetScaler
agent that will give permission to fetch secrets from AWS secret
store)

2)  Login to NetScaler Console with credentials fetched in step 1

3)  Call NetScaler Console to fetch credentials (serviceURL and
token) for agent registration

4)  Calls registration by using the credentials fetched in step 3

'''



'''

These are the placeholders which you need to replace according to
your setup configurations

aws_secret_id: Id of the AWS secret where you have stored NetScaler
Console Credentials

The secrets value should be in the following json format
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{ "adm_user_id_key": "YOUR_ID", " adm_user_secret_key":
"YOUR_SECRET"}

'''



aws_secret_id = "<AWS_secret_id>"

adm_ip_or_hostname = "<YOUR_ADM_POP>.adm.cloud.com"



'''

Set up a specific logger with your desired output level and log file
name

'''

log_file_name_local = os.path.basename(__file__)

LOG_FILENAME = '/var/log/' + 'bootstrap' + '.log'

LOG_MAX_BYTE = 50*1024*1024

LOG_BACKUP_COUNT = 20



logger = logging.getLogger(__name__)

logger.setLevel(logging.DEBUG)

logger_handler = logging.handlers.RotatingFileHandler(LOG_FILENAME,
maxBytes=LOG_MAX_BYTE, backupCount=LOG_BACKUP_COUNT)

logger_fortmater = logging.Formatter(fmt='%(asctime)-2s:%
(funcName)30s:%(lineno)4d: [%(levelname)s] %(message)s',
datefmt="%Y-%m-%d %H:%M:%S")

logger_handler.setFormatter(logger_fortmater)
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
logger.addHandler(logger_handler)



class APIHandlerException(Exception):

    def __init__(self, error_code, message):

        self.error_code = error_code

        self.message = message



    def __str__(self):

        return self.message + ". Error code '" +
str(self.error_code) + "'"



def parse_response(response, url, print_response=True):

    if not response.ok:

        if "reboot" in url:

            logger.debug('No response for url: reboot')

            resp = {"errorcode": "500", "message": "Error while
reading response."}

            return resp



        if print_response:

            logger.debug('Response text for %s is %s' % (url,
response.text))
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        response = json.loads(response.text)

        logger.debug("ErrorCode - " + str(response['errorcode']) +
". Message -" + str(response['message']))

        raise APIHandlerException(response['errorcode'],
str(response['message']))

    elif response.text:

        if print_response:

            logger.debug('Response text for %s is %s' % (url,
response.text))



        result = json.loads(response.text)

        if 'errorcode' in result and result['errorcode'] > 0:

            raise APIHandlerException(result['errorcode'],
str(result['message']))

        return result



def _request(method, url, data=None, headers=None, retry=3,
print_response=True):

    try:

        response = requests.request(method, url, data=data,
headers=headers)

        result = parse_response(response, url,
print_response=print_response)

        return result

    except [requests.exceptions.ConnectionError,
requests.exceptions.ConnectTimeout]:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        if retry > 0:

            return _request(method, url, data, headers, retry-1,
print_response=print_response)

        else:

            raise APIHandlerException(503, 'ConnectionError')

    except requests.exceptions.RequestException as e:

        logger.debug(str(e))

        raise APIHandlerException(500, str(e))

    except APIHandlerException as e:

        logger.debug("URL: %s, Error: %s, Message: %s" % (url,
e.error_code, e.message))

        raise e

    except Exception as e:

        raise APIHandlerException(500, str(e))



try:

    '''Get the AWS Region'''

    client = boto3.client('s3')

    my_region = client.meta.region_name

    logger.debug("The rgion is %s" % (my_region))



    '''Creating a Boto cleint session'''

    session = boto3.session.Session()
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    client = session.client(

        service_name='secretsmanager',

        region_name=my_region

    )



    '''Getting the values stored in the secret with id:
<aws_secret_id>'''

    get_id_value_response = client.get_secret_value(

        SecretId = aws_secret_id

    )

    adm_user_id = json.loads(get_id_value_response["SecretString"])
["adm_user_id_key"]

    adm_user_secret =
json.loads(get_id_value_response["SecretString"])
["adm_user_secret_key"]



except Exception as e:

    logger.debug("Fetching of NetScaler Console credentials from AWS
secret failed with error: %s" % (str(e)))

    raise e



'''

Initializing common NetScaler Console API handlers

'''
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
mas_common_headers = {

    'Content-Type': "application/json",

    'Accept-type': "application/json",

    'Connection': "keep-alive",

    'isCloud': "true"

}



'''

API to login to the NetScaler Console and fetch the Session ID and
Tenant ID

'''

url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/config/
login"

payload = 'object={"login":{"ID":"' + adm_user_id + '","Secret":"' +
adm_user_secret + '"}}'

try:

    response = _request("POST", url, data=payload,
headers=mas_common_headers)

    sessionid = response["login"][0]["sessionid"]

    tenant_id = response["login"][0]["tenant_name"]

except Exception as e:

    logger.debug("Login call to the NetScaler Console failed with
error: %s" % (str(e)))

    raise e
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
'''

API to fetch the service URL and Token to be used for registering
the agent with the NetScaler Console

'''

mas_common_headers['Cookie'] = 'SESSID=' + str(sessionid)

url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/config/
trust_preauthtoken/" + tenant_id +"?customer="+ tenant_id

logger.debug("Fetching Service URL and Token.")

try:

    response = _request("GET", url, data=None,
headers=mas_common_headers)

    service_name  = response["trust_preauthtoken"][0]
["service_name"]

    token = response["trust_preauthtoken"][0]["token"]

    api_gateway_url = response["trust_preauthtoken"][0]
["api_gateway_url"]

except Exception as e:

    logger.debug("Fetching of the Service URL Passed with error. %s"
% (str(e)))

    raise e



'''

Running the register agent command using the values we retrieved
earlier

'''
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
try:

    registeragent_command = "registeragent -serviceurl
"+api_gateway_url+" -activationcode "+service_name+"\;"+token

    file_run_command = "/var/python/bin/python2.7 /mps/
register_agent_cloud.py "+registeragent_command

    logger.debug("Executing registeragent command: %s" %
(file_run_command))

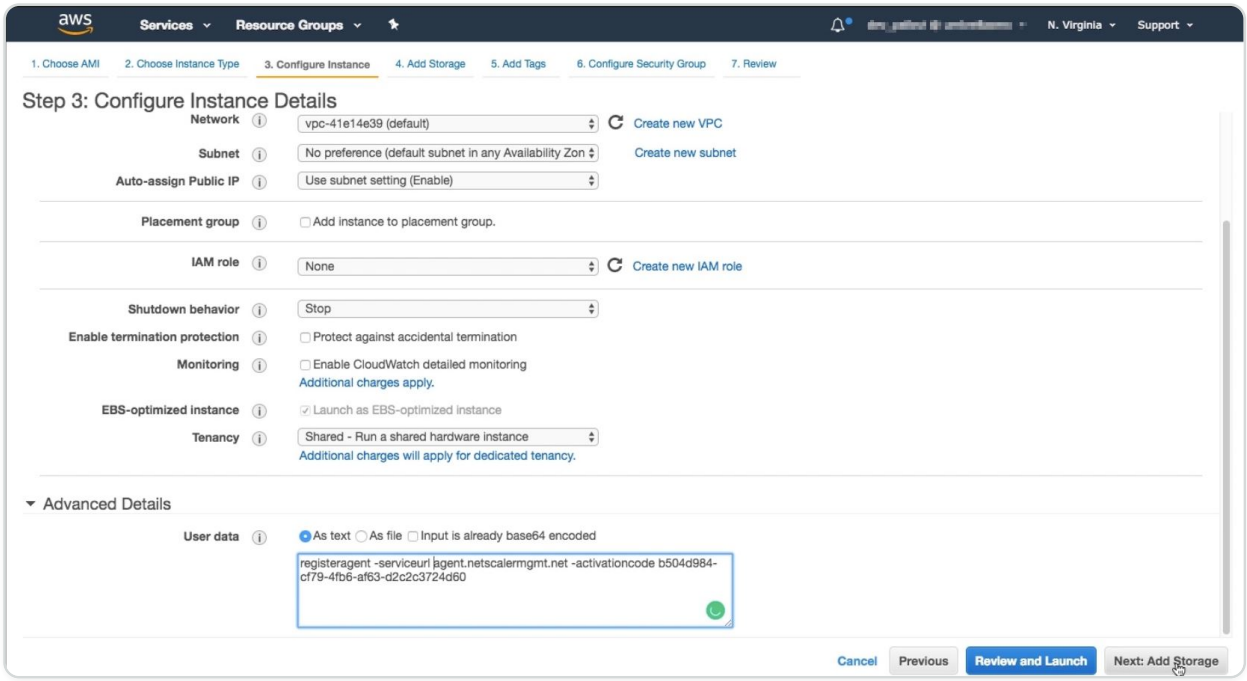
    os.system(file_run_command)

except Exception as e:

    logger.debug("Agent Registeration failed with error: %s" %
(str(e)))

        raise e
```

This script fetches the authentication details from the AWS secrets manager and runs the `deployment.py` script to register the agent with the NetScaler Console.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

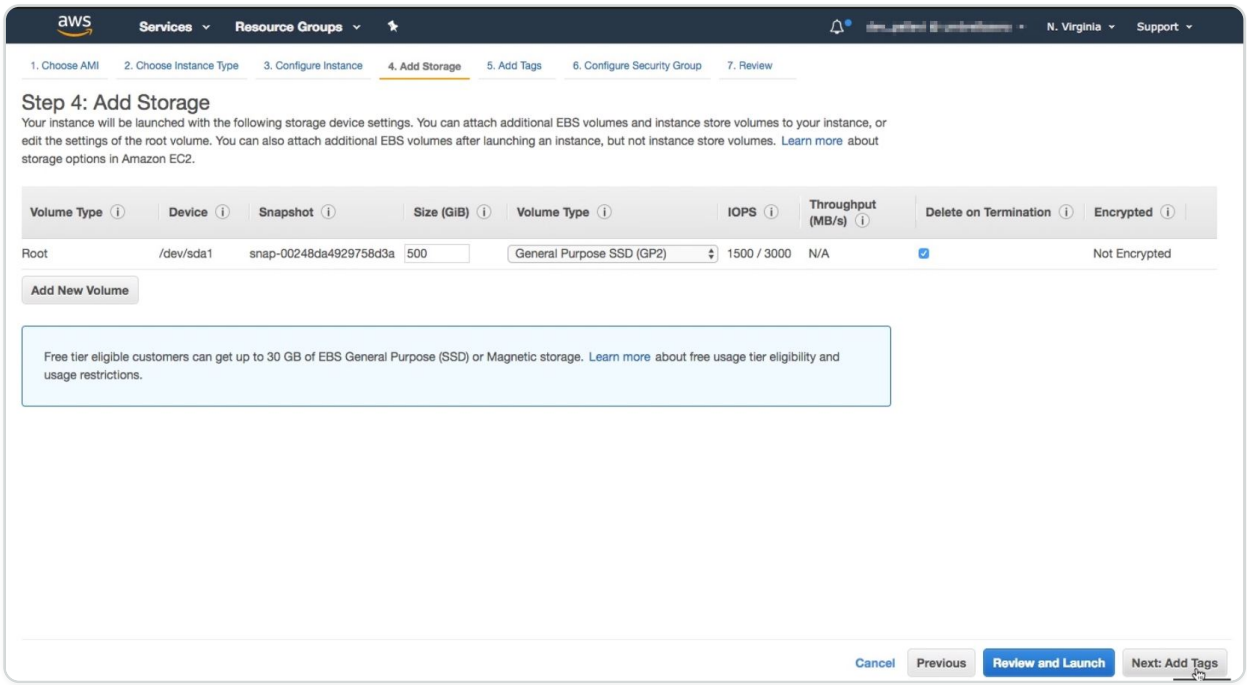
NOTE

While you can auto-assign public IP address, you can also assign elastic IP address. Assigning an elastic IP address is required when NAT Gateway is not configured.

If the elastic IP address is not set in this step, you can still do it on the EC2 console. You can create a new elastic IP address and associate that with the NetScaler agent using the instance ID or ENI-ID.

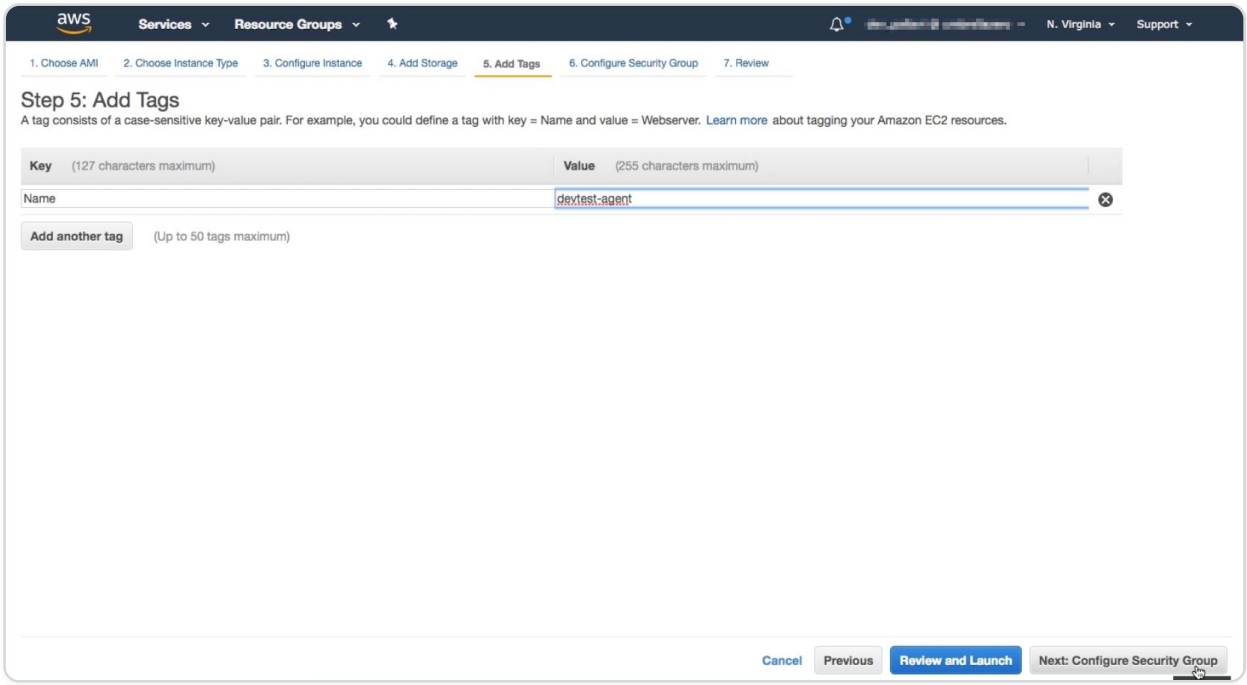
Click **Add Storage**.

3. On the **Add Storage** page, configure the storage device settings for the instance, and click **Next: Add Tags**.

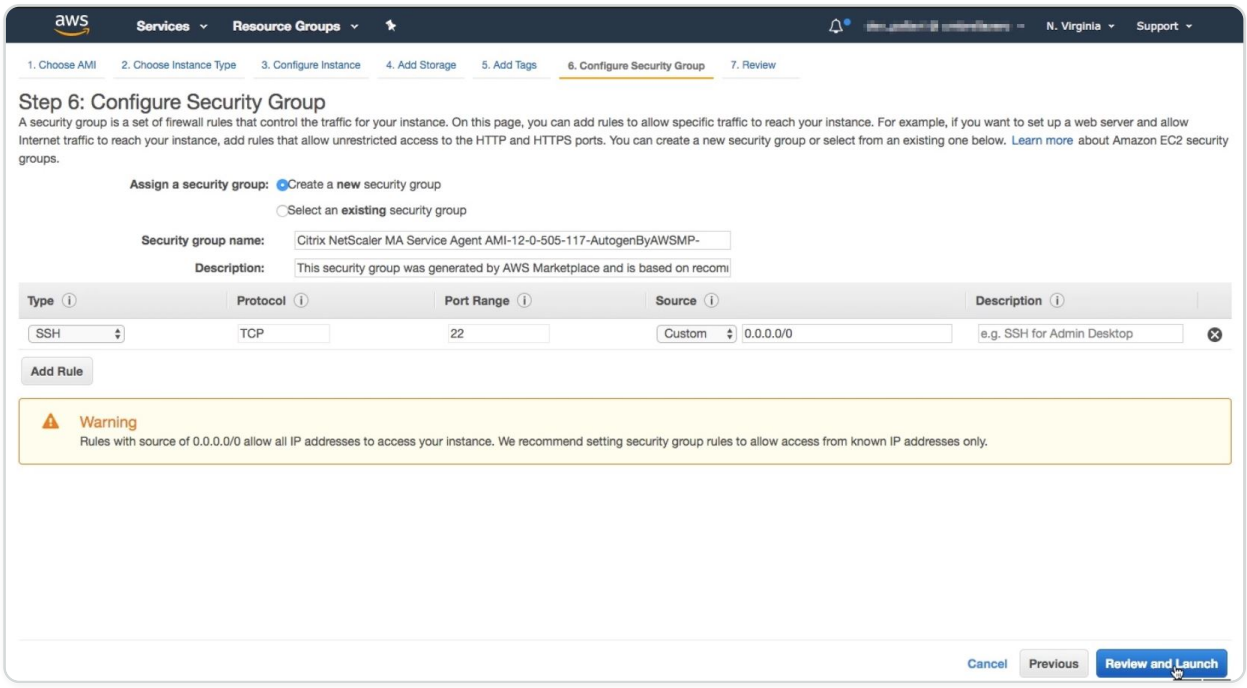


4. On the **Add Tags** page, define the tag for the instance, and click **Next: Configure Security Group**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



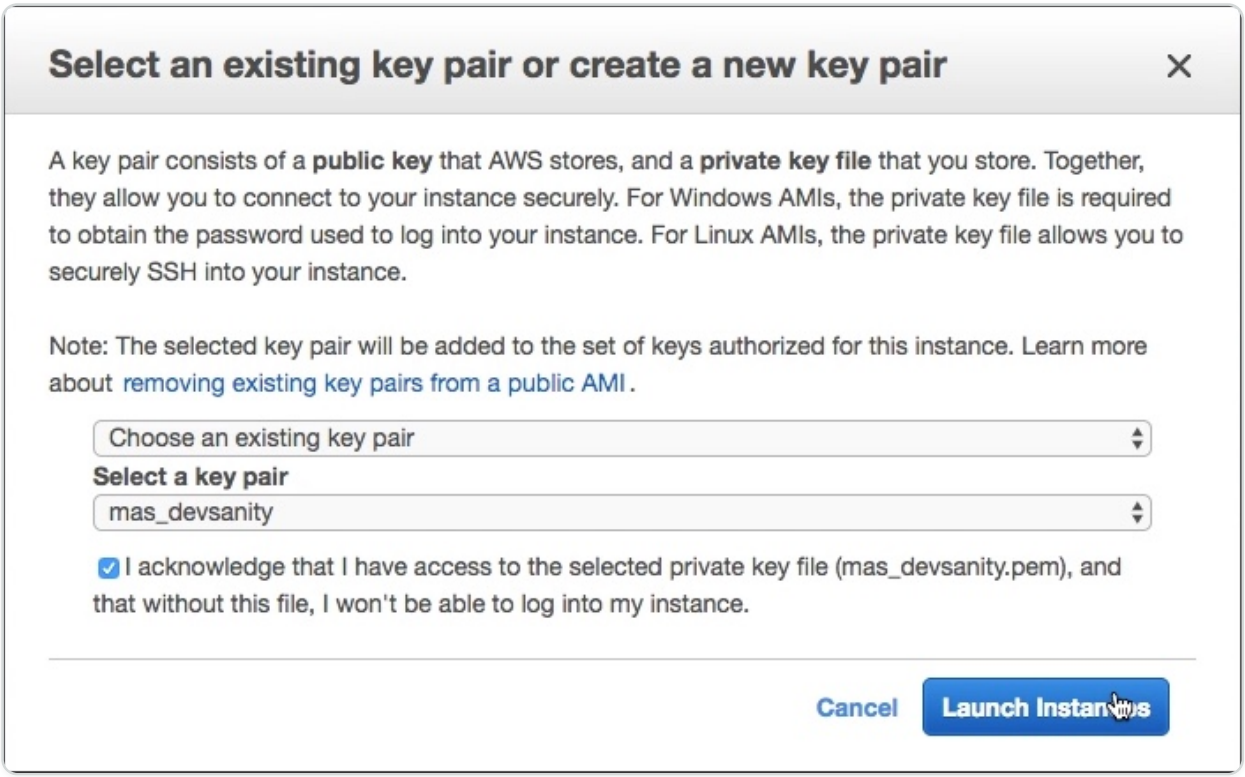
5. On the **Configure Security Group** page, add rules to allow specific traffic to your instance and click **Review and Launch**.



6. On the **Review Instance Launch** page, review the instance settings and click **Launch**.
7. In the **Select an existing key pair or create a new key pair** dialog box, create a key pair. You can also select from the existing key pairs.

   Accept the acknowledgment and click **Launch Instances**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The deployment process might take approximately 10–15 minutes. After the deployment is successfully completed, you can view your NetScaler agent virtual machine on your AWS account.

Install a NetScaler agent on GCP

The NetScaler agent works as an intermediary between the NetScaler Console and the discovered instances in the data center or on the cloud. You can deploy the agent on the Google Cloud Platform (GCP) to facilitate the secure remote management of NetScaler instances deployed within the Google cloud virtual network through NetScaler Console. For more information, see the Google Cloud Platform Marketplace.

Prerequisites

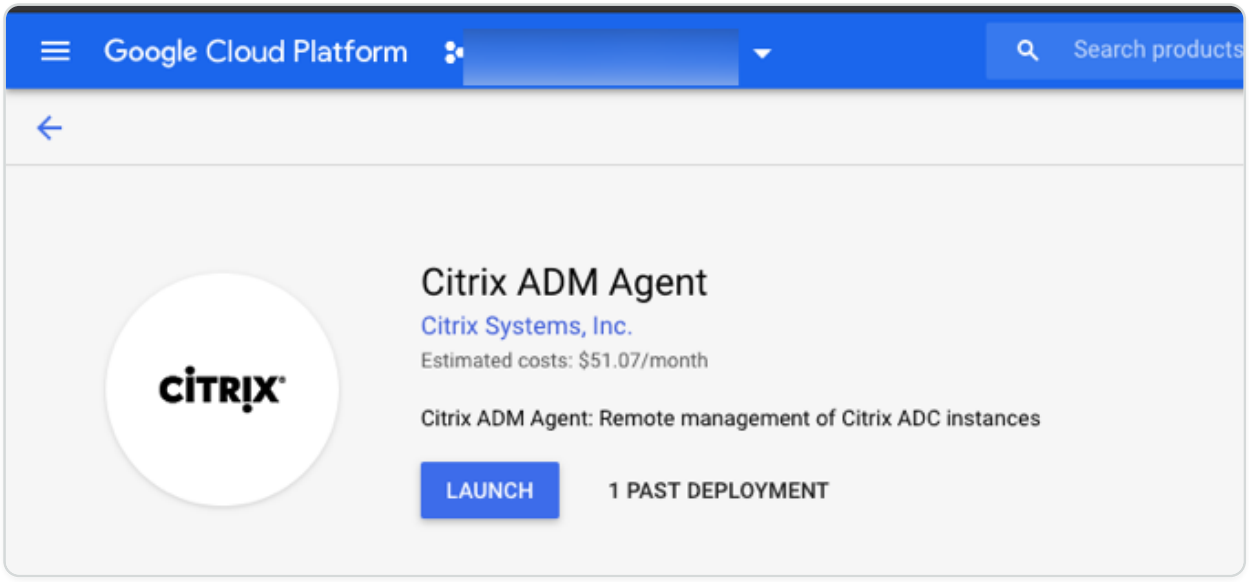
To install a NetScaler agent on GCP, you need a GCP account.

Install the NetScaler agent on GCP

Follow these steps to install a NetScaler agent on GCP.

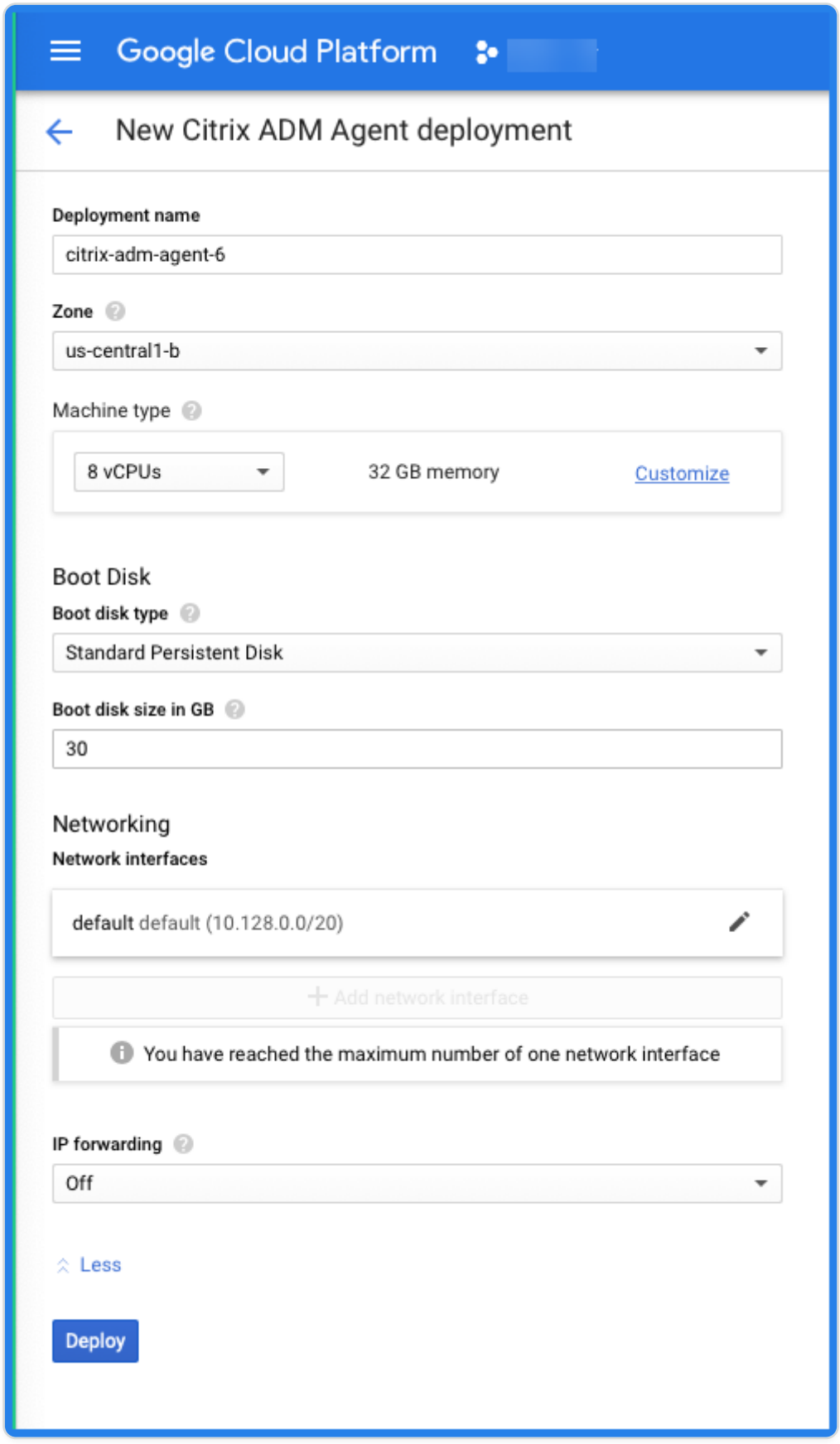
1. Log on to the GCP console (console.cloud.google.com) using your credentials and go to the marketplace.
2. In the search field, type **NetScaler agent**.
3. Click **NetScaler agent** from the results field and then click **Launch**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



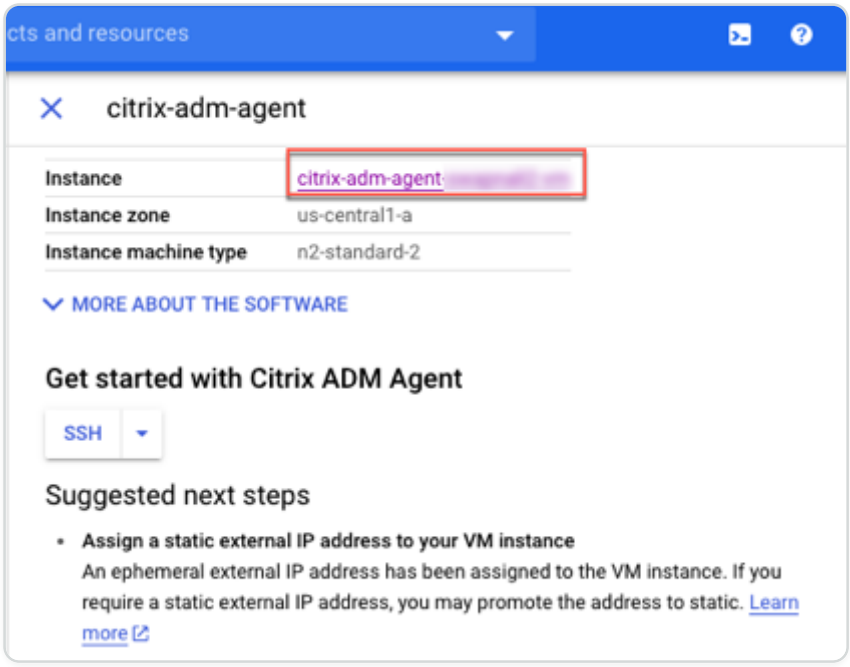
4. In the **New NetScaler agent deployment** page, most of the options are set by default. You can change the default configurations as required and click **Deploy**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. After the agent is deployed, click the instance link and check the details in the **VM instance details page**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

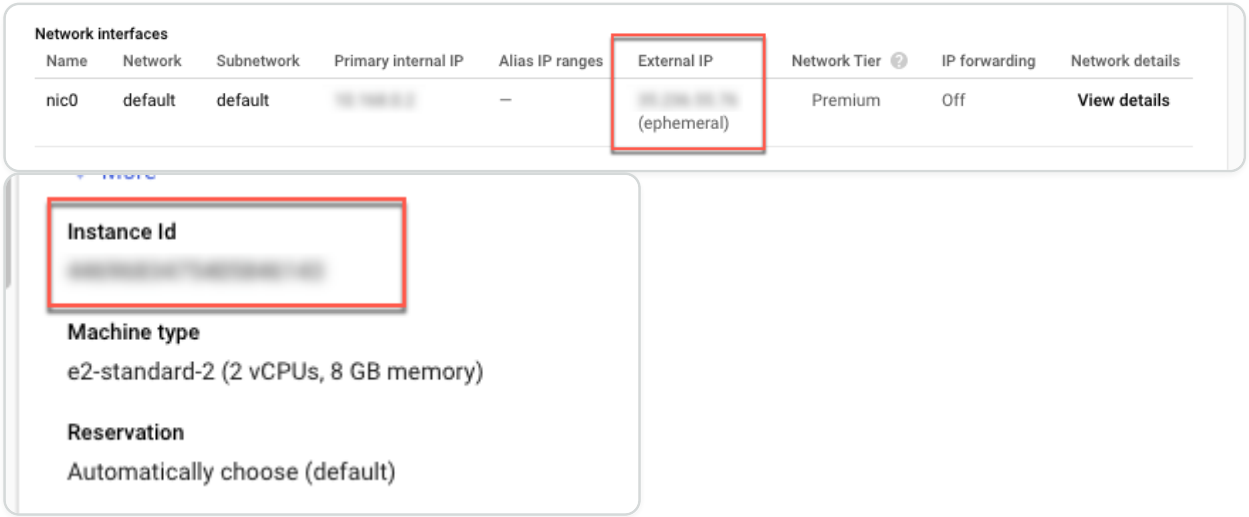


6. Log on to the agent through an SSH client using the agent external IP address. Use the following commands:

   ```
   ssh nsrecover@<external IP address of the agent>
   ```

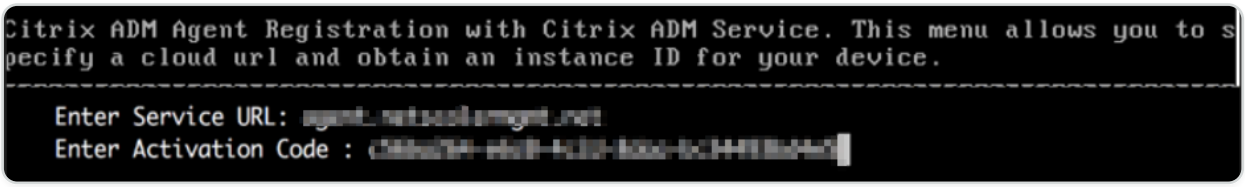
   Password: Instance ID

   Can you find the external IP address and the instance ID in the **VM instance details** page.



7. Enter the following command to invoke the deployment screen: **deployment_type.py**
8. Enter the **Service-URL** and the **Activation code** that you had copied and saved from the **Set Up Agents** page in NetScaler Console as instructed in Getting Started. The agent uses the service URL to locate the service and the activation code to register with the service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



After agent registration is successful, the agent restarts to complete the installation process.

After the agent has restarted, access NetScaler Console and on the **Set Up Agent** page, under **Discovered Agents**, verify the status of the agent.

Install NetScaler agent in Kubernetes cluster using YAML

NOTE

The procedure to install an agent as a microservice is available in the Getting Started section.

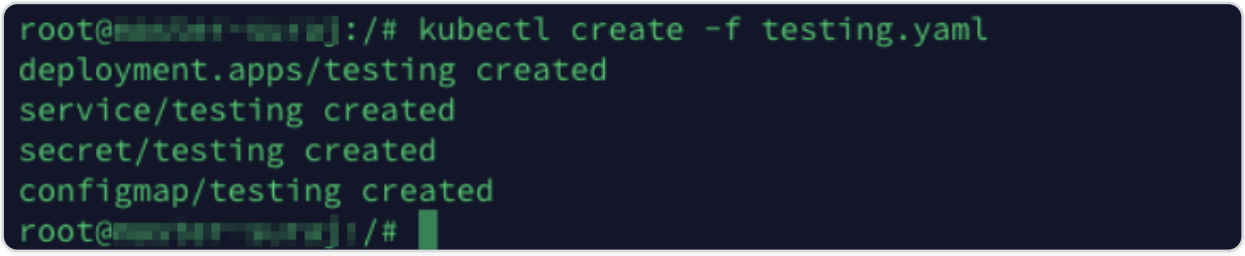
In the Kubernetes master node:

1. Save the downloaded YAML file
2. Run the following command:

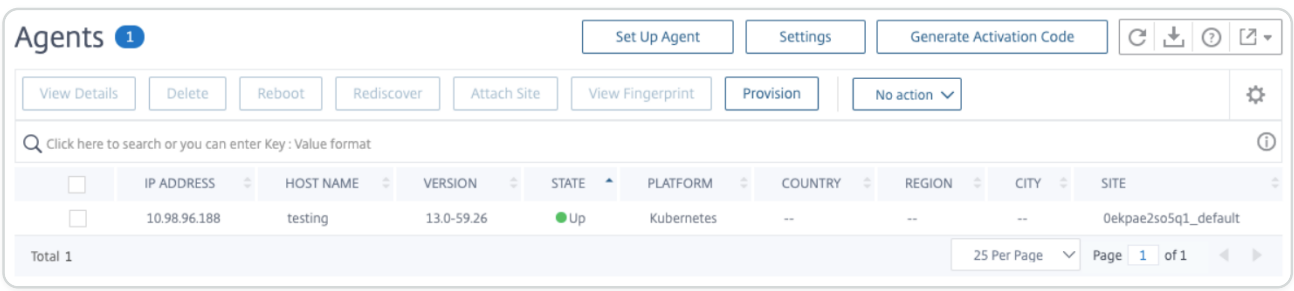
   `kubectl create -f <yaml file>`

   For example, `kubectl create -f testing.yaml`

   The agent is successfully created.



In NetScaler Console, navigate to **Infrastructure > Instances > Agents** to see the agent status.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

NetScaler agent configured in Kubernetes cluster using YAML supports automatic agent upgrade (evergreen upgrade).

Install a NetScaler agent operator using the OpenShift console

NOTE:

OpenShift agent is supported only in NetScaler Console service.

An operator is an open source toolkit that enables you to deploy and manage the Kubernetes applications in an effective, automated, and scalable way. As an administrator, you can deploy an agent in the OpenShift cluster using the **NetScaler® ADM Agent Operator**.

NOTE:

An agent configured in the OpenShift cluster is not automatically upgraded by default.

Prerequisites

Before you deploy, ensure that:

- You have the privileged security context constraints to control permissions for pods. For the agent, run the following command to get the privilege security context constraints to the service account:

  ```
  oc adm policy add-scc-to-user privileged -z adm-agent-serviceaccount
  ```

- Run the following command to create an Agent login secret:

  ```
  kubectl create secret generic admlogin --from-literal=username=nsroot --from-literal=password=<adm-agent-password> -n <namespace>
  ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- `<adm-agent-password>` is an example password. You must set a password for the agent and NetScaler CPX uses these credentials to register with the Agent.
- Provide **admlogin** for `loginSecret` in the agent YAML while creating the instance.

If you are deploying NetScaler CPX™ and agent in different namespaces, ensure to:

- Label namespace with `citrix-cpx=enabled` in which the NetScaler CPX has been deployed.
- Set `helper.required` true or false while installing the agent operator.

NOTE:

By default, `helper.required` is set to **false**. If this parameter is set to false, you must ensure to create **admlogin** secret in every namespace if NetScaler CPX and agent are in different namespaces.

- You have `accessSecret` that is required in the agent YAML. These credentials are required for the agent to connect with NetScaler Console service.

```
kubectl create secret generic <secretname> --from-literal=accessid=<ID> --from-literal=accesssecret=<Secret> -n namespace
```

NOTE:

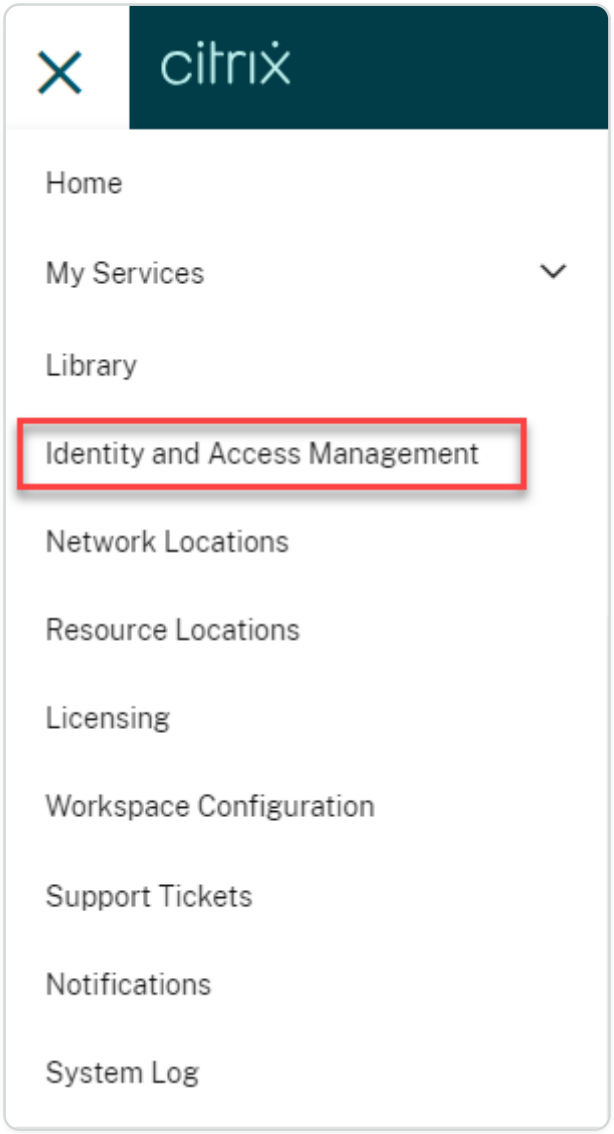
Provide a secret name for accessSecret in agent YAML while creating the instance.

You can get access ID and secret for accessing the NetScaler Console from the following procedure:

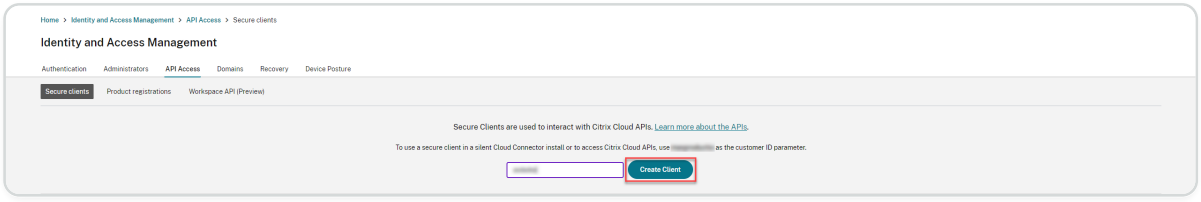
a. Log on to the Citrix Cloud™ management console.

b. From the Citrix Cloud menu, select **Identity and Access Management**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

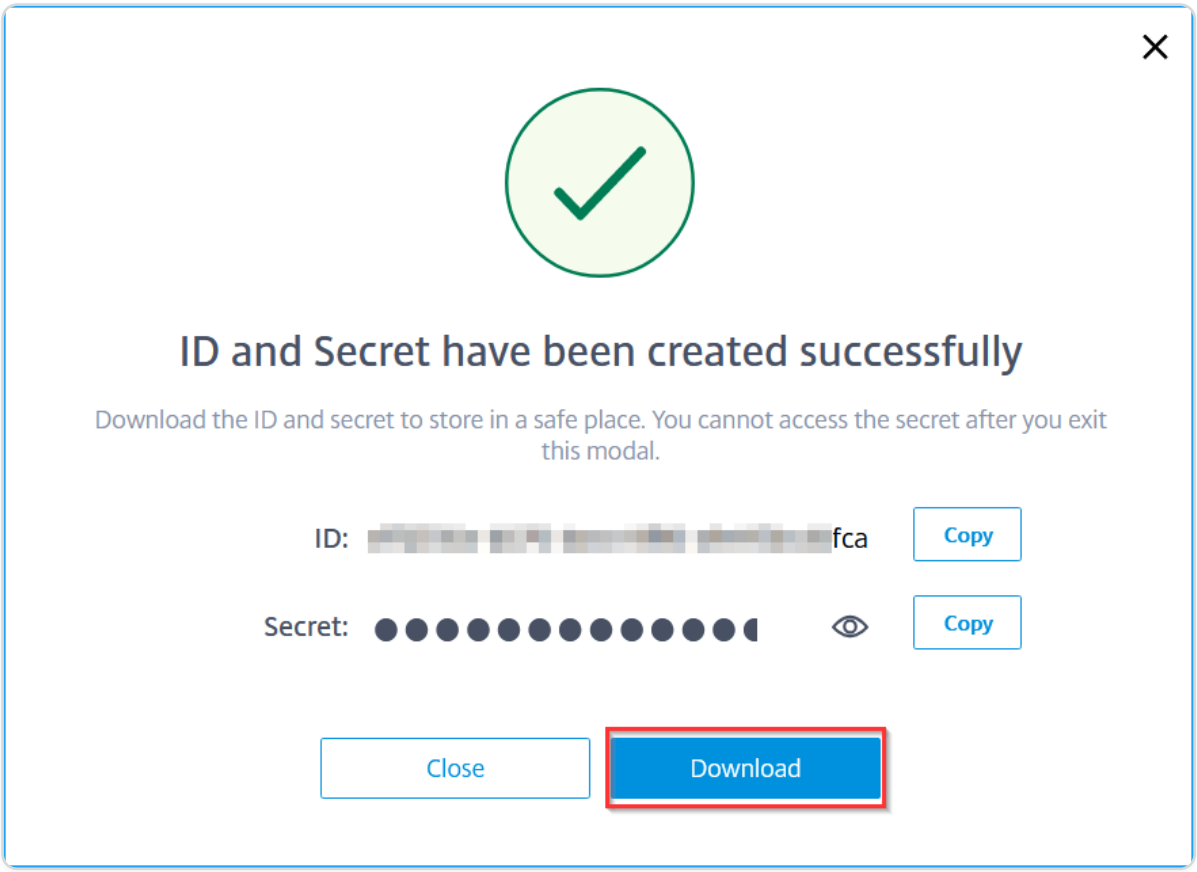


c. From the **API Access** tab, enter a secure client name and click **Create Client**.



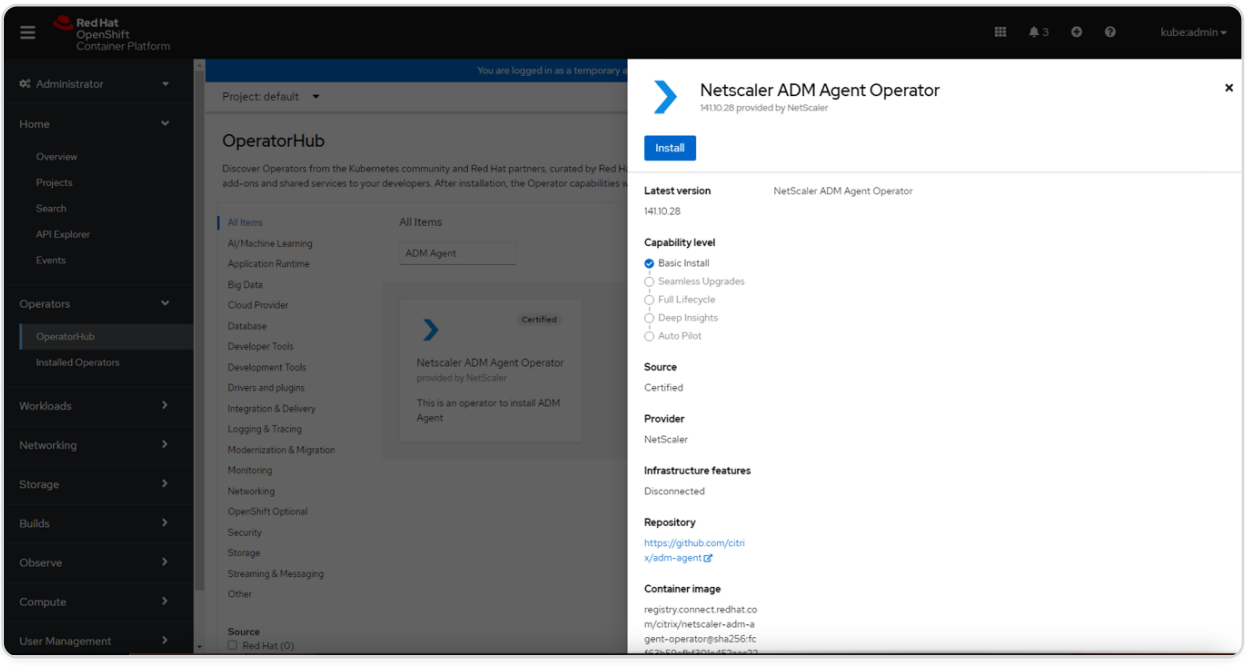
d. ID and Secret are generated. Click **Download** and save the CSV file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Install the Agent Operator

1. Log on to the OpenShift cluster console.
2. Navigate to **Operators > OperatorHub**.
3. In the search bar, provide the agent name and select the **NetScaler ADM Agent Operator** and then click **Install**.

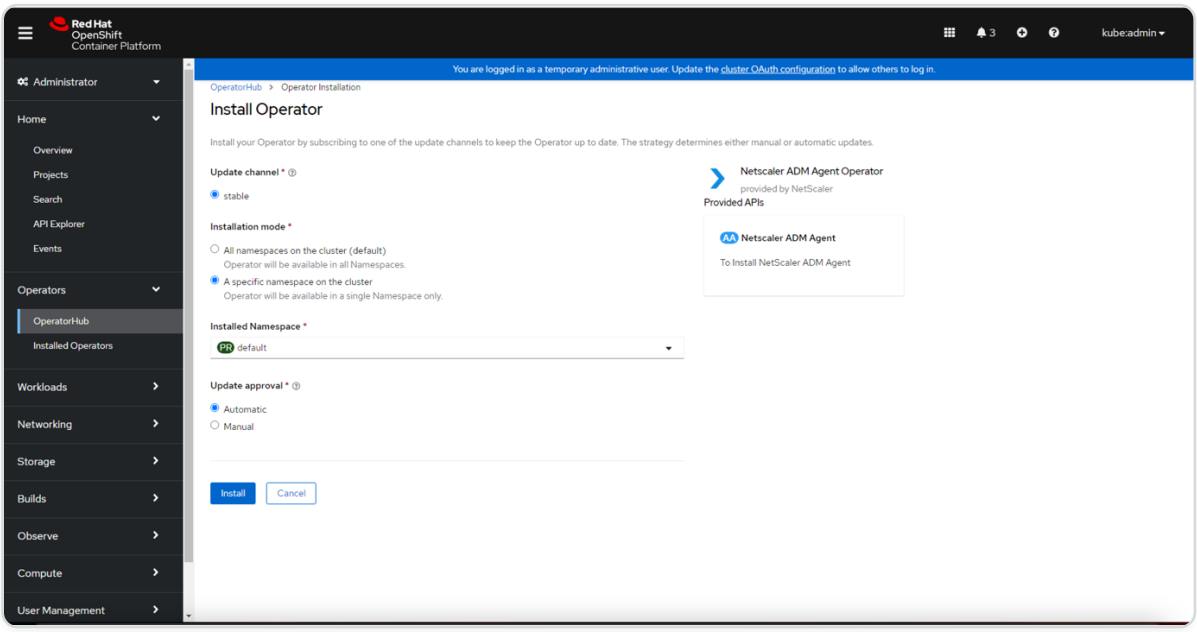


© 1997–2026 Citrix Systems, Inc. All rights reserved.

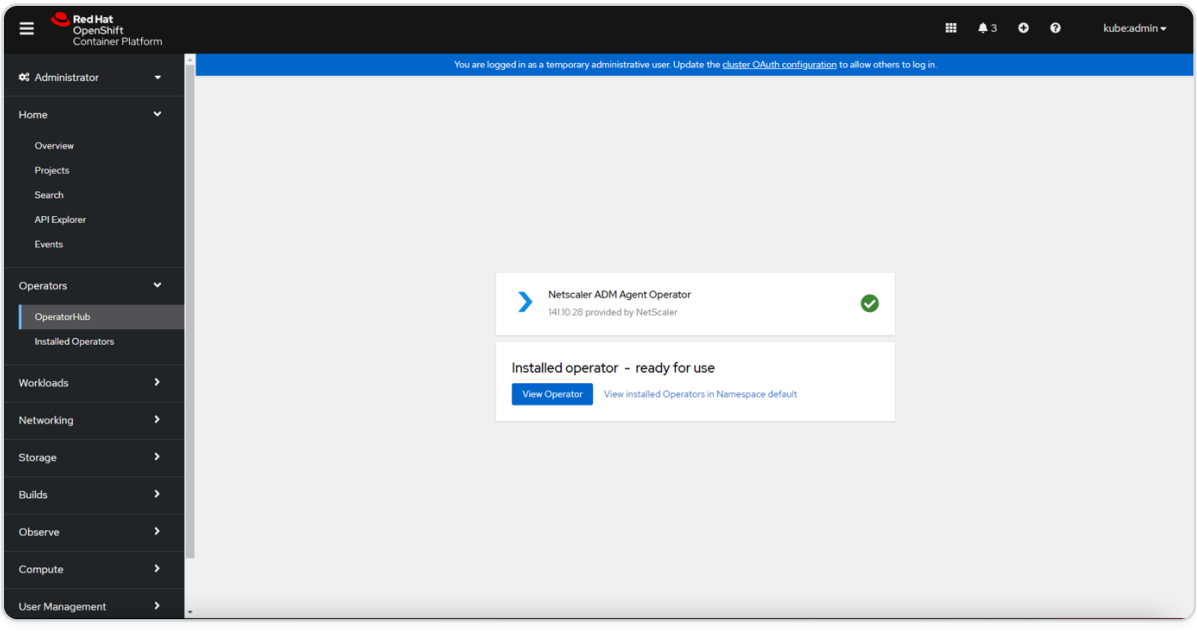
4. In the **Install Operator** page, you have two options:

   - **All namespaces on the cluster (default)** - Enables the Agent operator to subscribe to all namespaces available in the cluster and allows you to initiate the instance of agent operator from any namespace on the cluster.
   - **A specific namespace on the cluster** - Enables the Agent operator to subscribe to a selected namespace on the cluster and you can initiate the instance of agent operator only from the selected namespace.

     In this example, the Agent operator is assigned to a namespace called **Default**. Select **Automatic** under **Update approval**, and click **Install**.

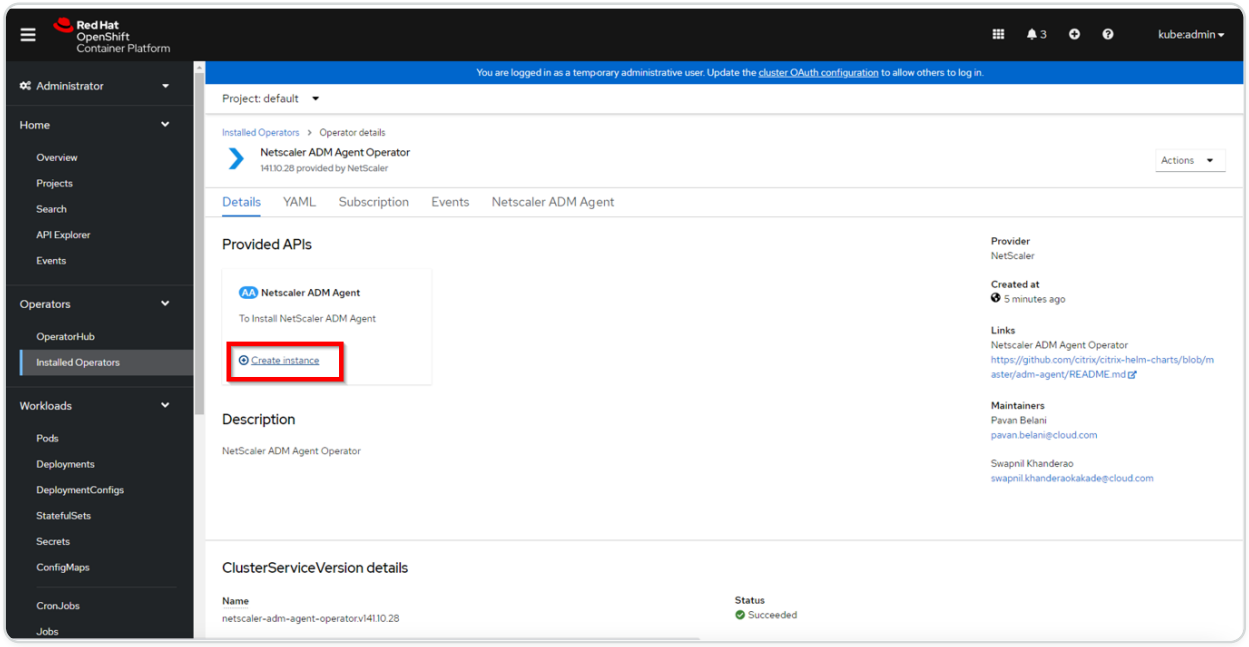


Wait until the Agent operator is successfully subscribed.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

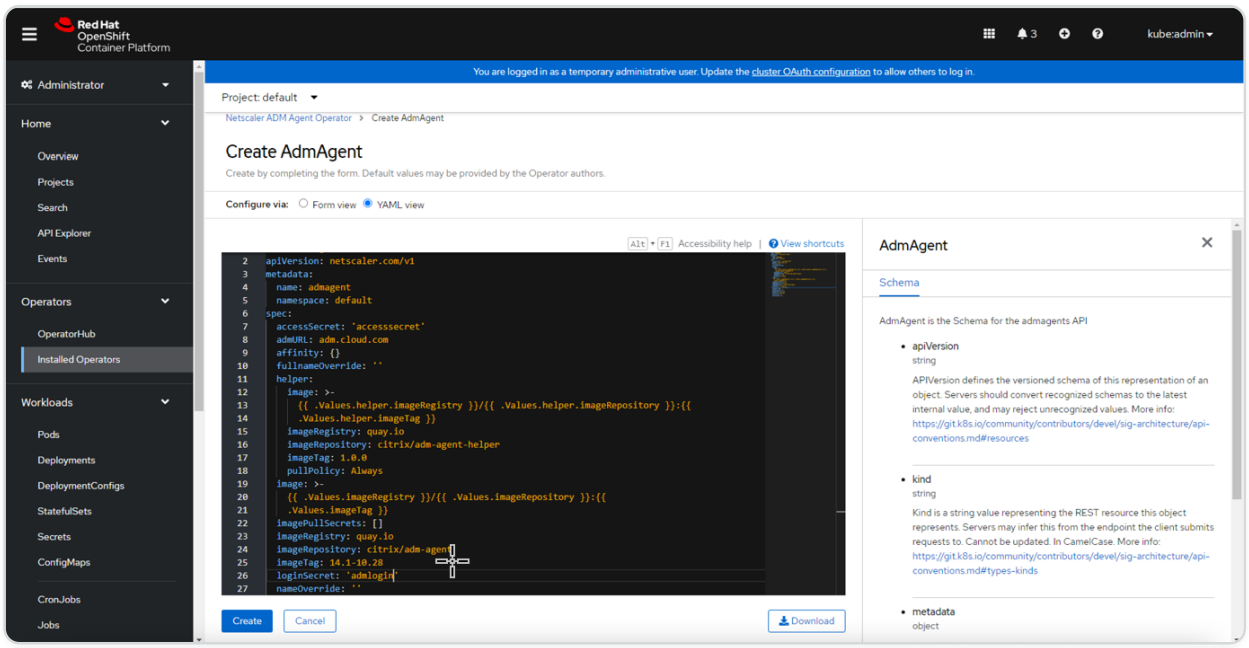
5. Navigate to **Workloads > Pods** and verify that the `netscaler-adm-agent-operator-controller` pod is up and running.
6. After the pod is up and running, click **Create Instance**.



7. Select the **YAML view** to update any parameters and then click **Create**.

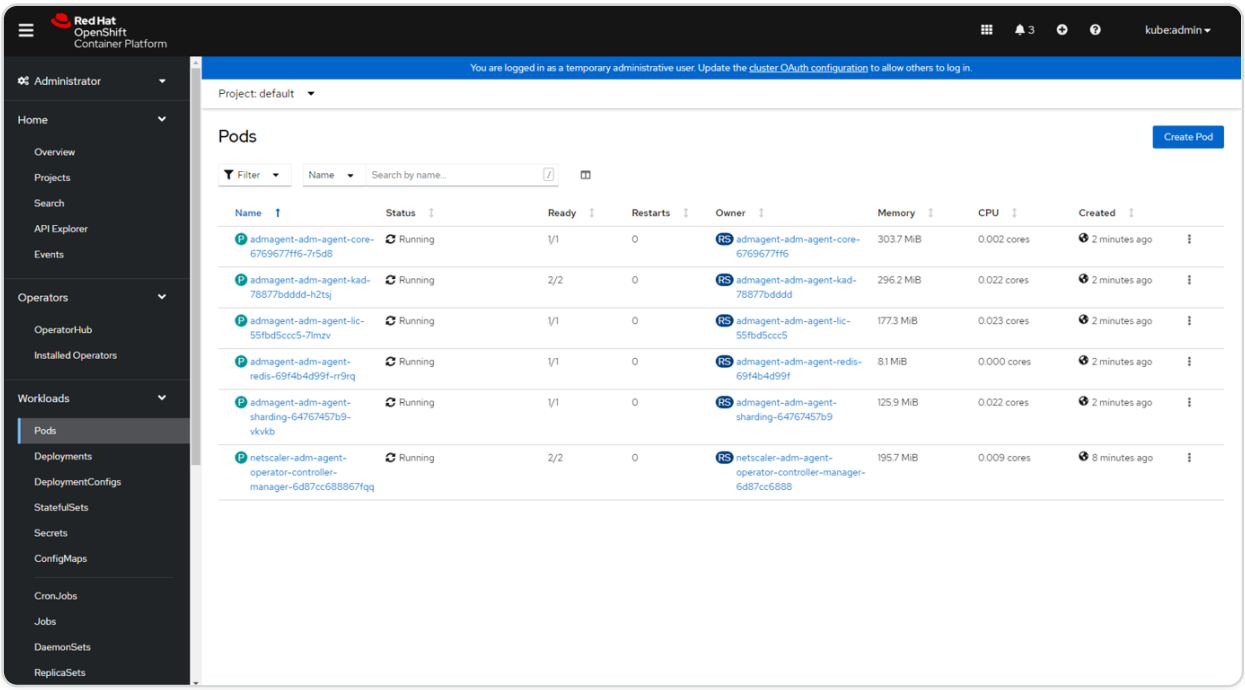
NOTE:

Ensure that there must be only one instance of agent per OpenShift cluster.



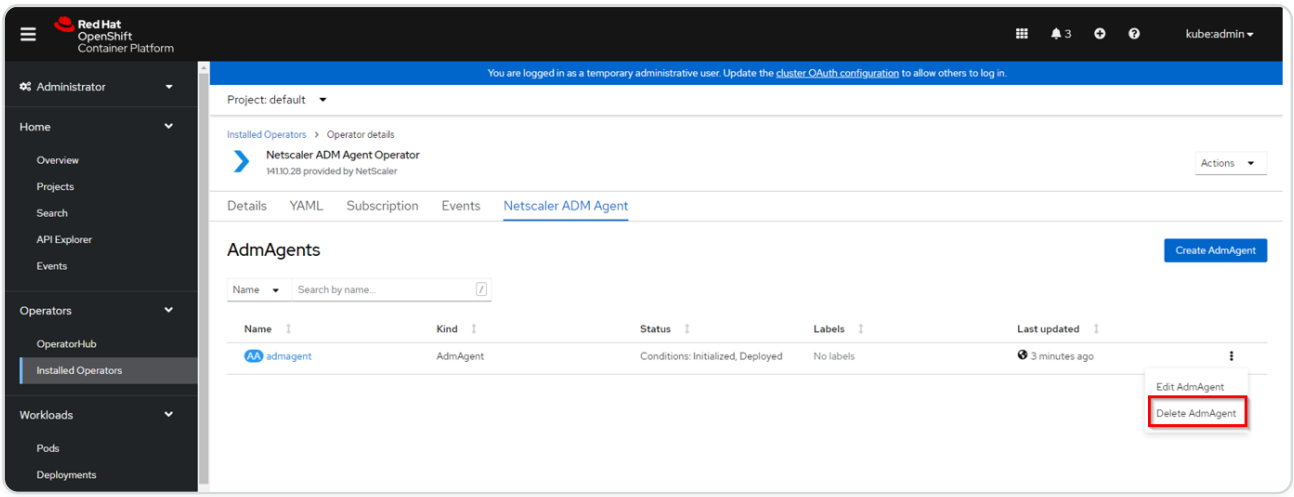
8. Navigate to **Workloads > Pods** and ensure that the agent pods are up and running.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Delete an agent instance

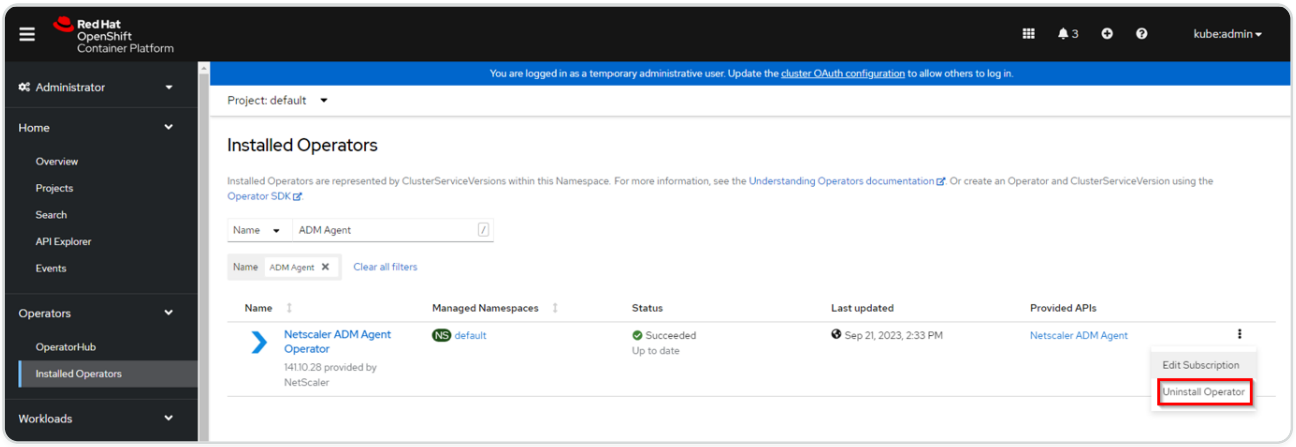
You can delete the instance of agent from the cluster by navigating to **Operators > Installed Operators**. In the **NetScaler ADM Agent Operator** tab, select the instance, and select **Delete AdmAgent** from the list.



Uninstall the agent operator

If you want to uninstall the agent operator pod from the cluster, navigate to **Operators > Installed Operators**, and then select **Uninstall Operator** from the list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Install a container-based agent using helm chart

You can deploy a container-based agent to connect NetScaler CPX with NetScaler Console for managing and monitoring the NetScaler CPX. To deploy a container-based agent, follow the procedure available in this document.

NOTE:

The container-based agent is not automatically upgraded (evergreen upgrade) by default.

How to Get Help and Support

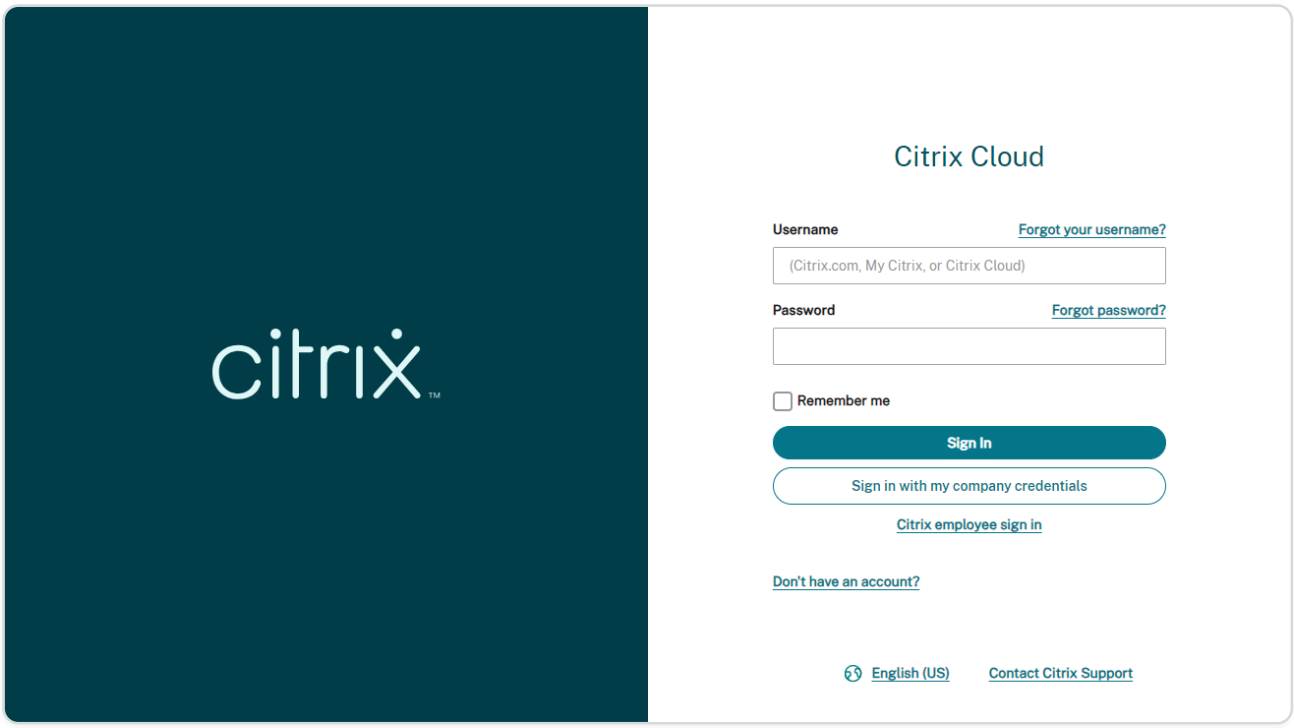
As a Citrix Cloud™ user, sometimes you might need help with making sure a smooth functioning of our infrastructure. This topic provides more information about the different help and supports options and how to access them.

Create a Citrix Cloud account

If you encounter an error when signing up for a Citrix Cloud account, contact Citrix Customer Service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sign in to your account



If you're having trouble signing in to your Citrix Cloud account:

- Make sure you sign in with the email address and password you provided when you signed up for your account.
- Citrix Cloud automatically prompts you to reset your password before you can sign in, if:
  - You haven't signed in to Citrix Cloud in a while
  - Your password doesn't meet Citrix Cloud's requirements
- For more information, see Changing your password in this article.
- If your company allows users to sign in to Citrix Cloud using their company credentials instead of a Citrix account, click **Sign in with my company credentials** and enter your company's sign-in URL. You can then enter your company credentials to access your company's Citrix Cloud account. If you don't know your company's sign-in URL, contact your company's administrator for assistance.

Change your password

If you've forgotten your Citrix Cloud account password, click **Forgot your username or password?**, and you can enter your account email address. You receive an email to reset your password. If you do not receive the password reset email, or you need more assistance, contact Citrix Customer Service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To help you keep your account password safe and secure, Citrix Cloud might prompt you to reset your password when you attempt to sign in. This prompt occurs if:

- Your password doesn't meet Citrix Cloud's complexity requirements. Passwords must be at least 8 characters long and include:
  - At least one number
  - At least one upper-case letter
  - At least one symbol: `! @ # $ % \^ * ? + = -`
- Your password includes dictionary words.
- Your password is listed in a known database of compromised passwords.
- You haven't signed in to Citrix Cloud in the last six months.

When prompted, select **Reset Password** to create a new strong password for your account.

Citrix Cloud support forums

On the Citrix Cloud support forums you can get help, provide feedback and improvement suggestions, view conversations from other users, or start your own topics.

NetScaler® support staff members track these forums and are ready to answer your questions. Other Citrix Cloud community members might also offer help or join the discussion.

You do not need to log in to read forum topics. However, you must log in to post or reply to a topic. To log in, use your existing Citrix account credentials or use the email address and password you provided when you created your Citrix Cloud account. To create a Citrix account, go to Create or request an account.

Support articles and documentation

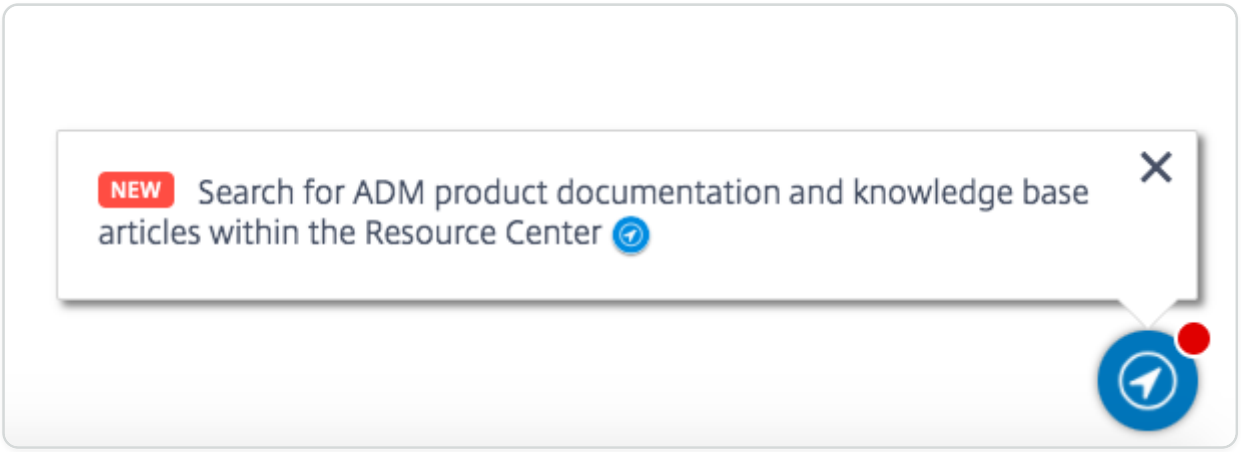
NetScaler provides a wealth of product and support content to help you get the most out of Citrix Cloud and resolve many issues you might experience with NetScaler products.

Citrix Cloud Resource Center

The Citrix Cloud Resource Center provides several resources to help you get started with Citrix Cloud services, learn more about features, and resolve issues. The resources that appear are applicable to the feature or service in Citrix Cloud that you are currently working with. For example, if you're in the Virtual Apps and Desktops service management console, the Resource Center shows you the following resources.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Access the Resource Center anytime by clicking the blue compass icon in the bottom-right of the Citrix Cloud console.



- **Get Started**: Provides a brief guided walkthrough of key tasks specific to the service you're currently working with. You also find links to training and onboarding resources to help you learn more about service capabilities and set up your end-users for success.
- **Announcements**: Provides notifications of newly released features and links to essential Citrix communications. Click a feature notification to receive a brief guided walkthrough of the feature.
- **Search Articles**: Provides a list of product documentation and Knowledge Center articles for common tasks and helps you find more articles, without leaving Citrix Cloud. Enter a search query in the **How do I...** box for a filtered list of articles based on the service you're working with. In general, support articles appear first in the list, followed by product documentation articles.

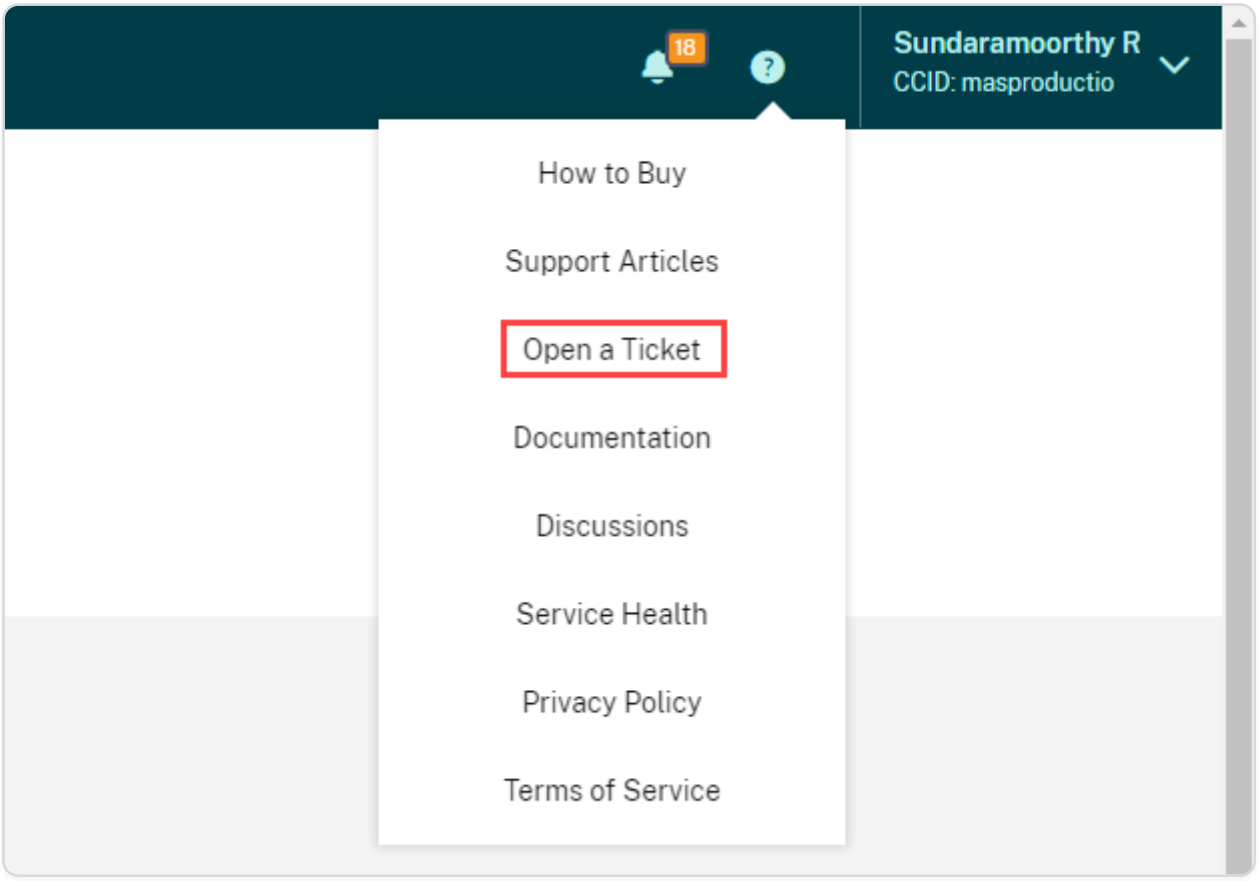
Citrix Tech Zone

Citrix Tech Zone contains a wealth of information to help you learn more about Citrix Cloud and other NetScaler products. Here you find reference architectures, diagrams, videos, and technical papers that provide insights for designing, building, and deploying Citrix technologies.

Technical Support

If you're experiencing an issue that requires technical help, click the **Feedback and Support** icon near the top-right of the screen, and then select **Open a Ticket.**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

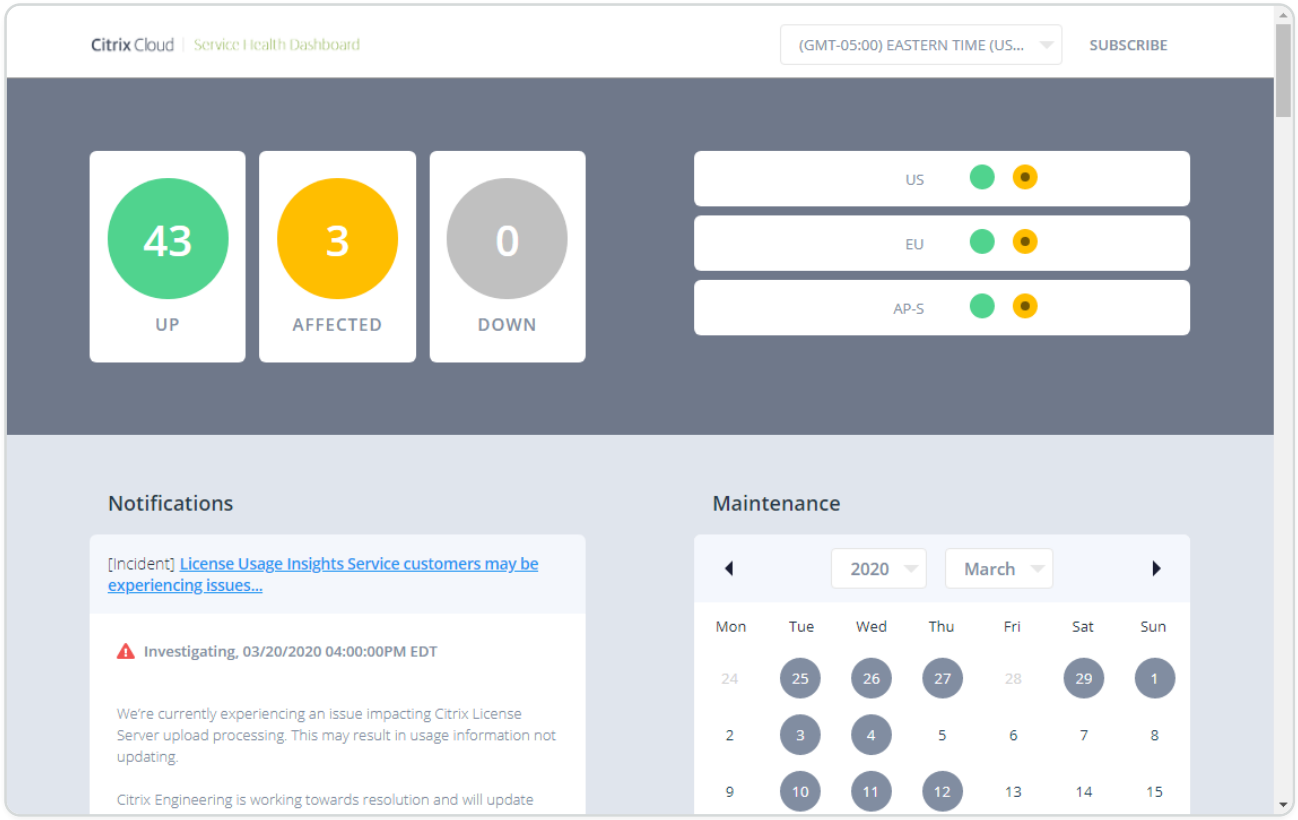


Click **Go to My Support** and then **My Support** to open a ticket through the My Support portal. You can also use the My Support portal to track your existing tickets and view your current product entitlements.

Service Health Dashboard

The Citrix Cloud service Health Dashboard provides an overview of real-time availability of the Citrix Cloud platform and services in each geographical region. If you experience any issues with Citrix Cloud, check the Service Health Dashboard to verify that Citrix Cloud or specific services are operating normally.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

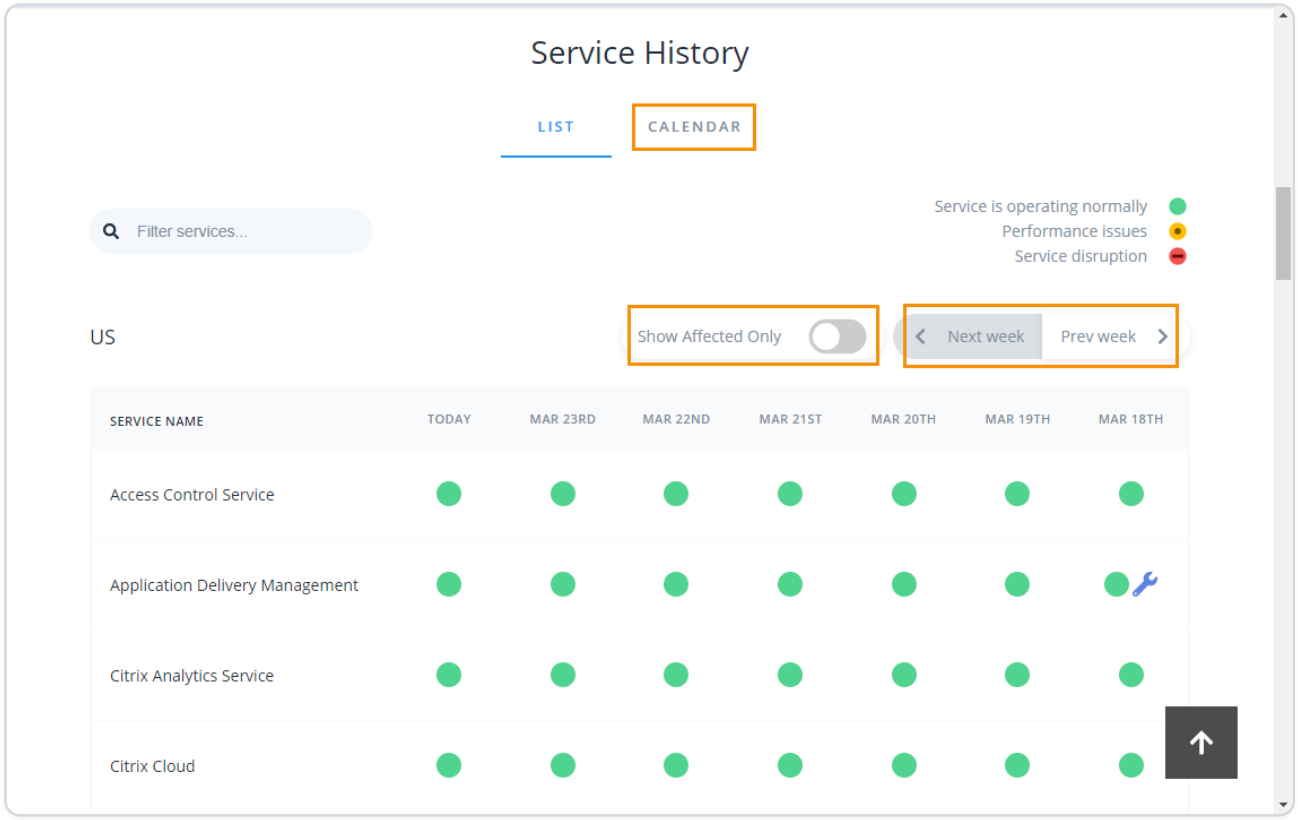


Use the dashboard to learn more about the following conditions:

- The current availability status of all Citrix Cloud services, grouped by geographical region
- The service health history of each service for the last seven days (default) or for previous seven-day increments
- Maintenance windows for specific services

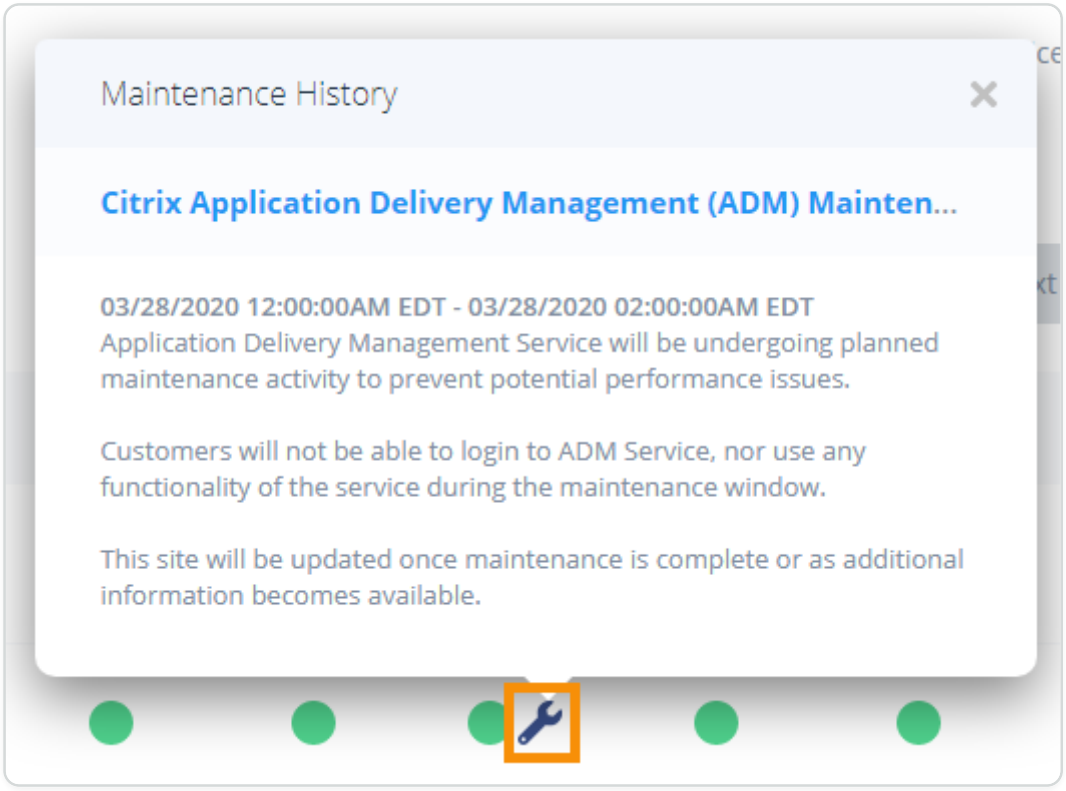
By default, service health status is displayed as a list, but you can also display the status in a calendar view. Select **Next** or **Previous** to scroll through the service health history in seven-day increments. You can also filter the list to display affected services only.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



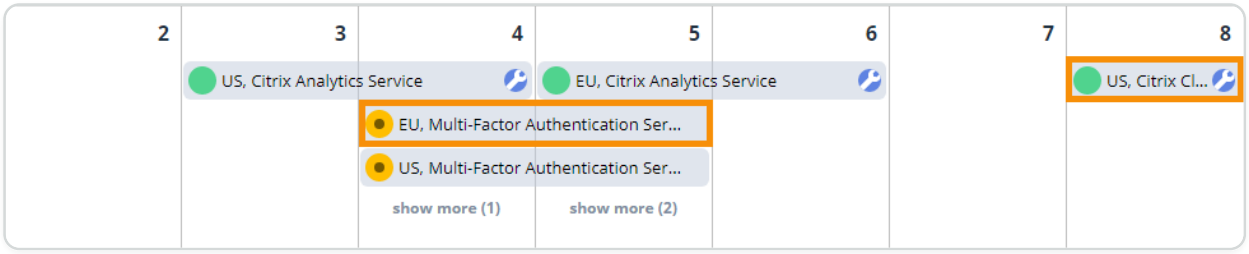
To view more detailed information about the service health incident for an affected service:

- From the list view, click the icon next to the service indicator to view more detailed information about the service health incident.



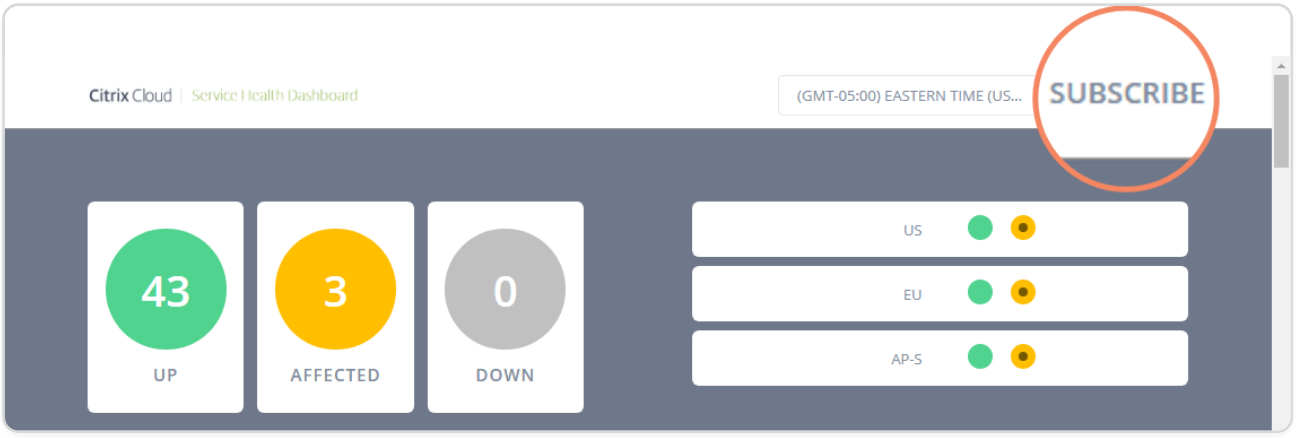
- From the calendar view, click the service entry to view the status for the service health incident.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

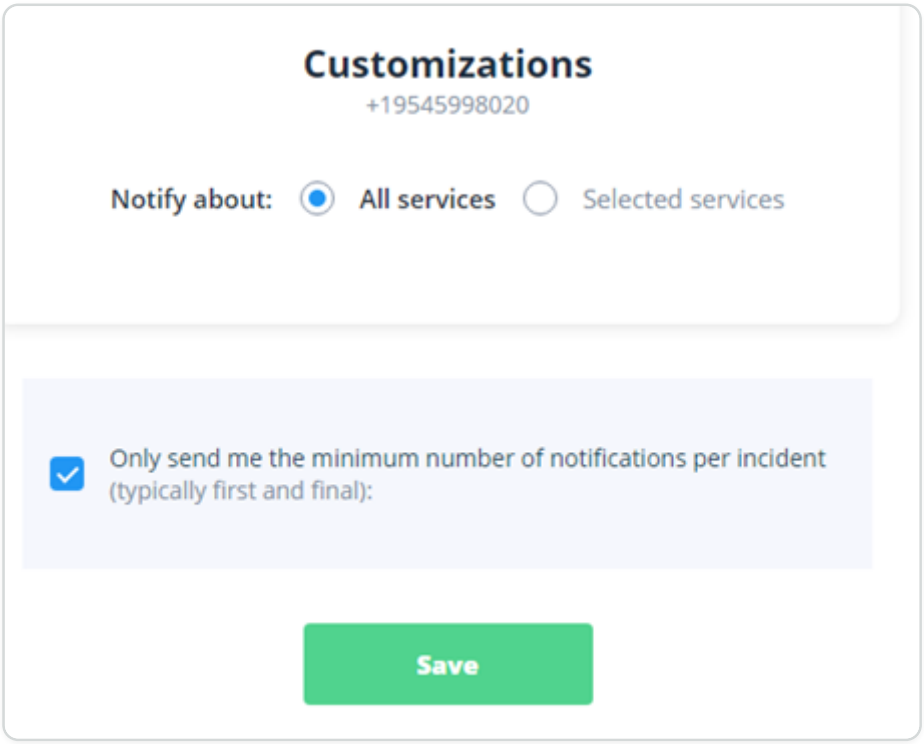


Service health subscriptions

To receive service health notifications, click **Subscribe** in the upper-right of the dashboard and select the notification method you want to use.

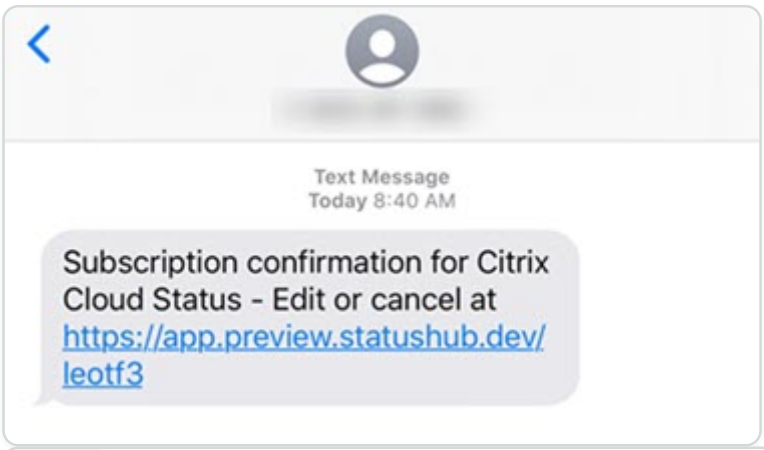


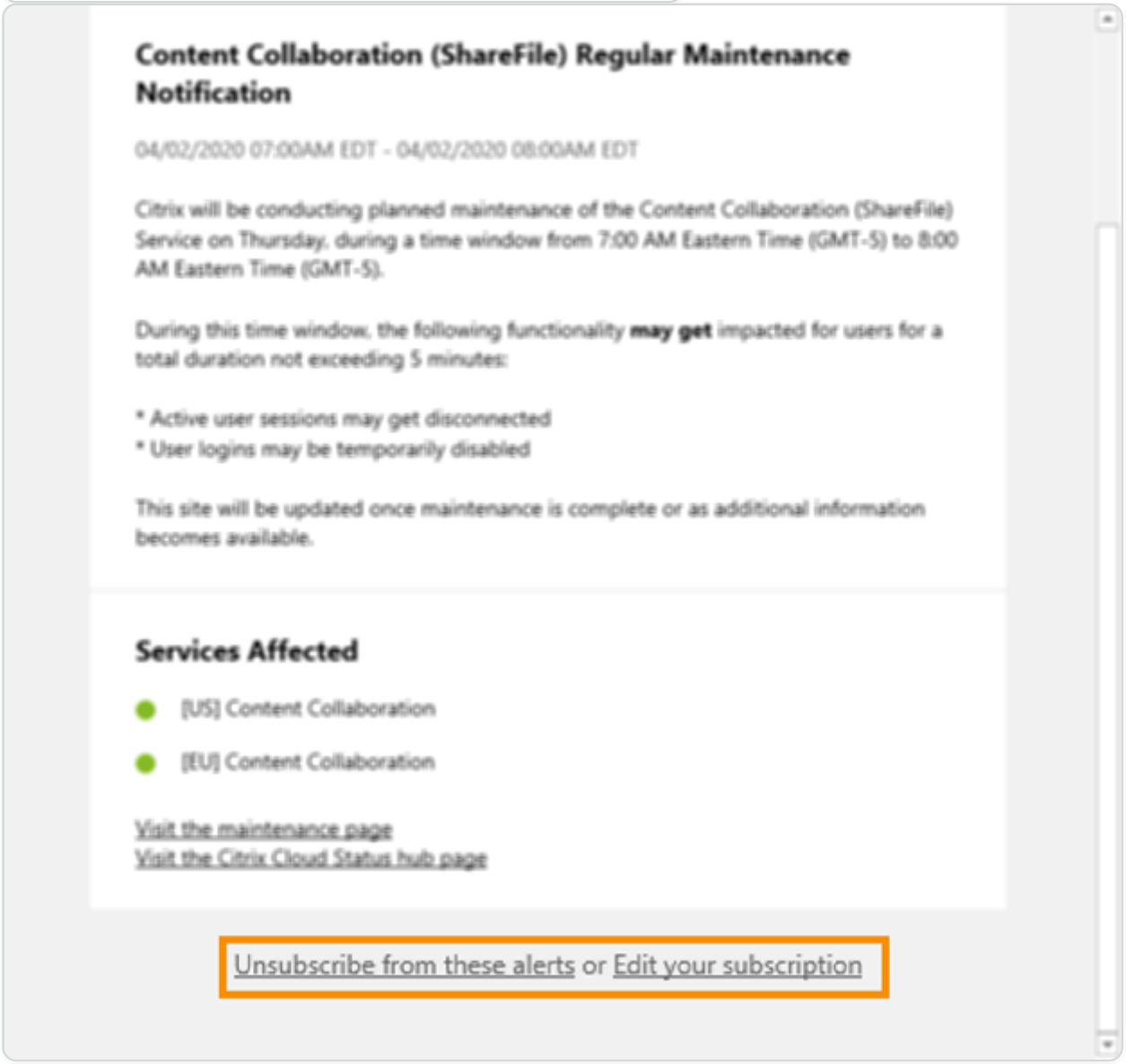
You can subscribe to notifications for all services or only the services you select. By default, you receive all notifications for a service health incident. To limit the frequency of notifications during an incident, you can choose to receive only the first and final notifications.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Depending on the subscription method, links to unsubscribe and to change your preferences are included in the subscription confirmation message you receive (for example, when subscribing to phone notifications) or in each notification message (for example, when you subscribe to email notifications).





To unsubscribe or change your subscription preferences:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Locate an existing notification and select the link to unsubscribe or change your notification preferences.
2. If unsubscribing, select **Unsubscribe** and then select the notification method you want to cancel. To subscribe from all notification methods, select **Remove all subscriptions**.
3. If changing preferences, select the notification method, make the appropriate changes to the services and minimum incident notifications, and then select **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enhanced Graphical User Interface

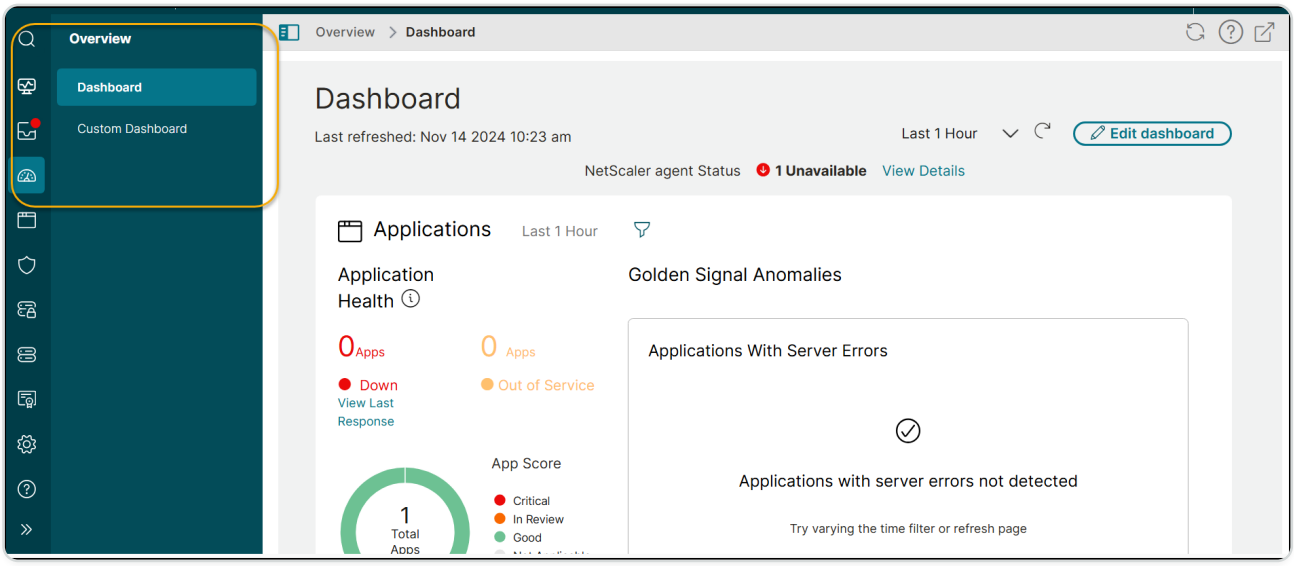
NetScaler Console Graphical User Interface (GUI) provides an enriching experience with several key features. These features provide:

- **Optimized screen space:** Users can show or hide the sidebar based on their preference.
- **Quick access to favorites:** Pin frequently used menu items for faster navigation.
- **Enhanced submenu visibility:** Hover over menu items to reveal submenus, offering a clearer view of all available options.
- **Improved submenu structure:** A consistent, three-level submenu system ensures seamless navigation across NetScaler Console, providing a uniform experience throughout.

This page walks you through the features of the NetScaler Console GUI providing an enriching user experience.

Hover-to-Display menu

Previously, the secondary-level submenu was displayed in a tree structure. NetScaler Console GUI provides a seamless navigation where the secondary menu appears on hover, revealing the submenu. This navigation elevates the viewing experience by displaying all submenu options without the need for scrolling.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Streamlined menu hierarchy

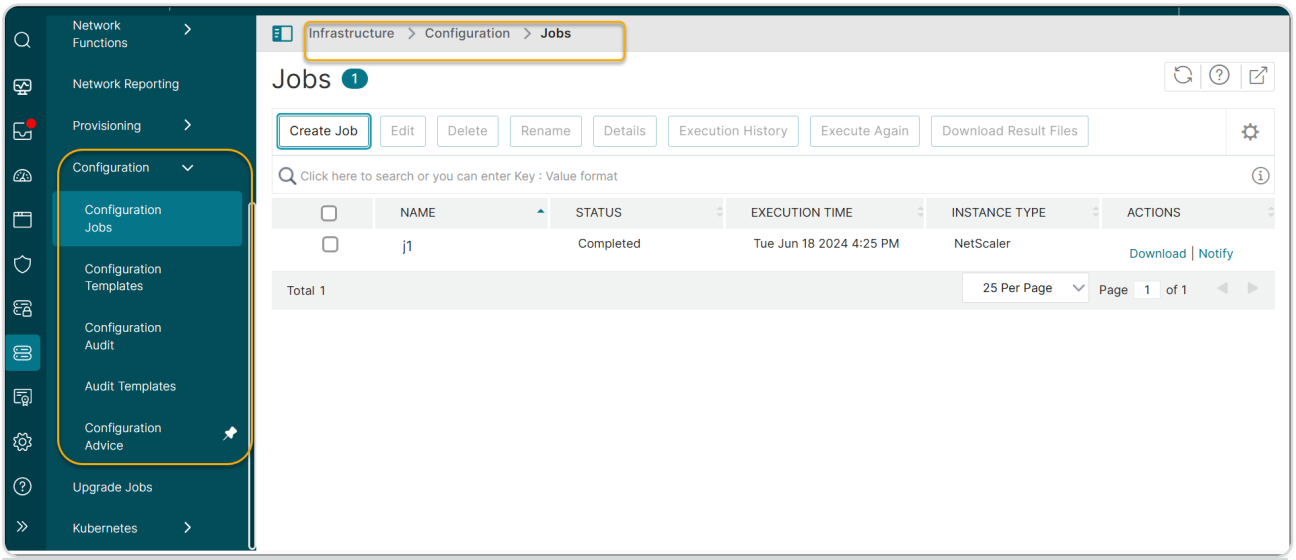
The menu hierarchy is streamlined to a maximum of three levels. Submenus that were previously displayed beyond the third level are now positioned at the third level. Navigation is updated for the following:

- **Infrastructure > Configuration**
- **NetScaler® Licensing > Pooled Licensing**
- **Gateway > HDX™ Insight**

Updated submenu labels

The names of some submenus are changed to align with this navigation approach. Screen navigation changes and submenu label updates are:

Infrastructure > Configuration

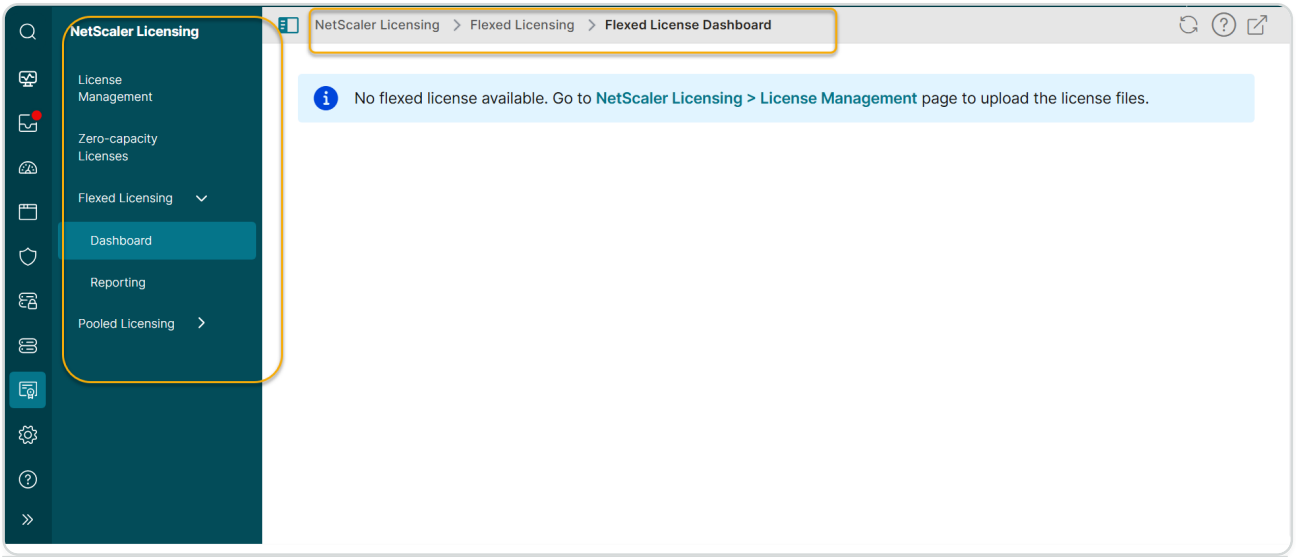


PREVIOUS SCREEN NAVIGATION	CHANGED SCREEN NAVIGATION	IS THERE A CHANGE IN THE SUBMENU LABEL?
Configuration > Configuration Jobs > Jobs	**Configuration > Configuration Jobs**	Yes
Configuration > Configuration Jobs > Configuration Templates	**Configuration > Configuration Templates**	No
Configuration > Configuration Audit > Overview	**Configuration > Configuration Audit**	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PREVIOUS SCREEN NAVIGATION	CHANGED SCREEN NAVIGATION	IS THERE A CHANGE IN THE SUBMENU LABEL?
Configuration > Configuration Audit > Audit Templates	**Configuration > Audit Templates**	No
Configuration > Configuration Audit > Configuration Advice	**Configuration > Configuration Advice**	No

NetScaler Licensing > Pooled Licensing



PREVIOUS SCREEN NAVIGATION	CHANGED SCREEN NAVIGATION	IS THERE A CHANGE IN THE SUBMENU LABEL?
Pooled Licensing > Throughput Capacity Licenses > Throughput Capacity	**Pooled Licensing > Throughput Capacity**	No
Pooled Licensing > Throughput Capacity Licenses > CPX Licenses	**Pooled Licensing > CPX Licenses**	No
Pooled Licensing > Throughput Capacity Licenses > CICO	**Pooled Licensing > CICO**	No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PREVIOUS SCREEN NAVIGATION	CHANGED SCREEN NAVIGATION	IS THERE A CHANGE IN THE SUBMENU LABEL?
Pooled Licensing > Throughput Capacity Licenses > FIPS Instances	**Pooled Licensing > FIPS Instances**	No
Pooled Licensing > Self Managed > License Expiry Information	**Pooled Licensing > Self Managed Expiry Information**	Yes
Pooled Licensing > Self Managed > Throughput Capacity Licenses > Self Managed Pool	**Pooled Licensing > Self Managed Throughtput**	Yes
Pooled Licensing > Self Managed > Self Managed VCPU	**Pooled Licensing > Self Managed VCPU**	No

Gateway > HDX Insight

PREVIOUS SCREEN NAVIGATION	CHANGED SCREEN NAVIGATION	IS THERE A CHANGE IN SUBMENU LABEL?
HDX Insight > Licenses > SSL VPN Licenses	**HDX Insight > Licenses**	Yes

Settings

There are no other changes under **Settings** except for the modification of the submenu label or name.

PREVIOUS SCREEN NAVIGATION	CHANGED SCREEN NAVIGATION	IS THERE A CHANGE IN SUBMENU LABEL?
Settings > Data Storage Management	There is no change in screen navigation.	The submenu label is changed to **Settings > Data Storage**

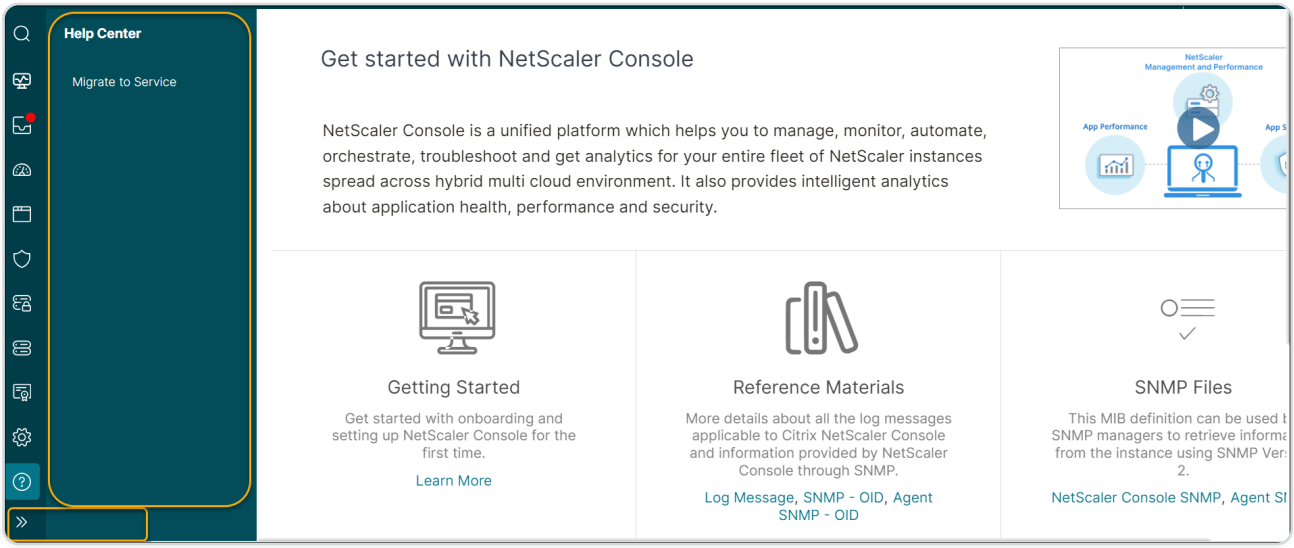
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Collapsible menu

You can collapse or expand the entire menu by clicking an icon.

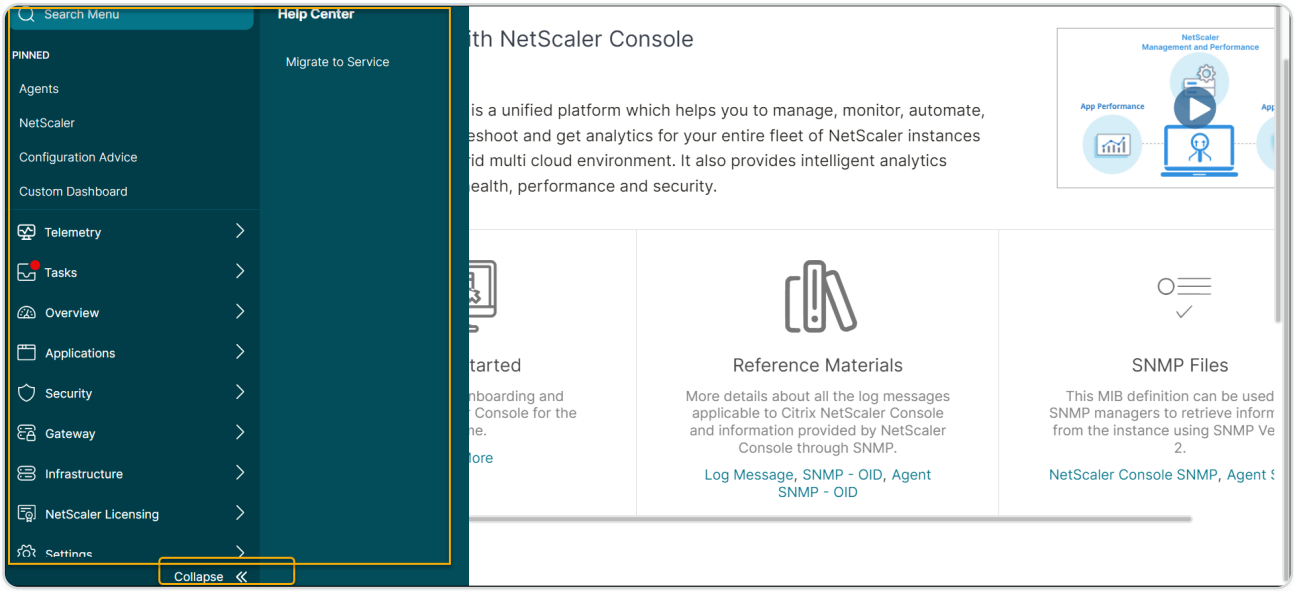
Expanded menu

Click the icon **>>** in the pane to expand the entire menu.



Collapsed menu

Click **Collapse <<** in the pane to collapse the entire menu.

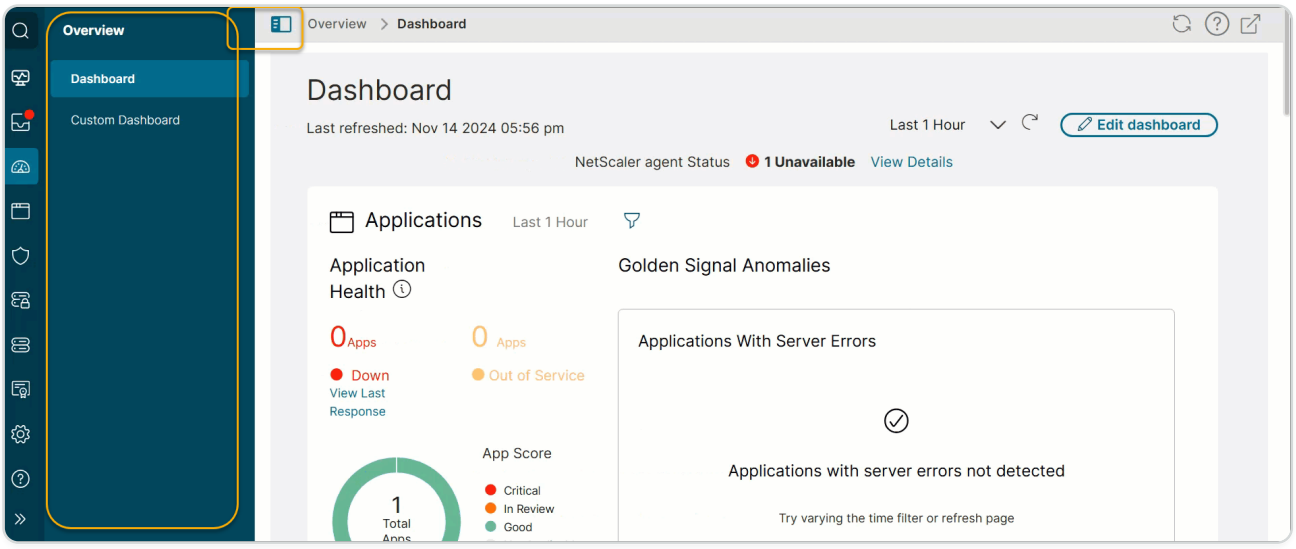


Sidebar Toggle

You can optimize screen space by toggling the sidebar visibility. Click the toggle button in the breadcrumb to hide or show the sidebar.

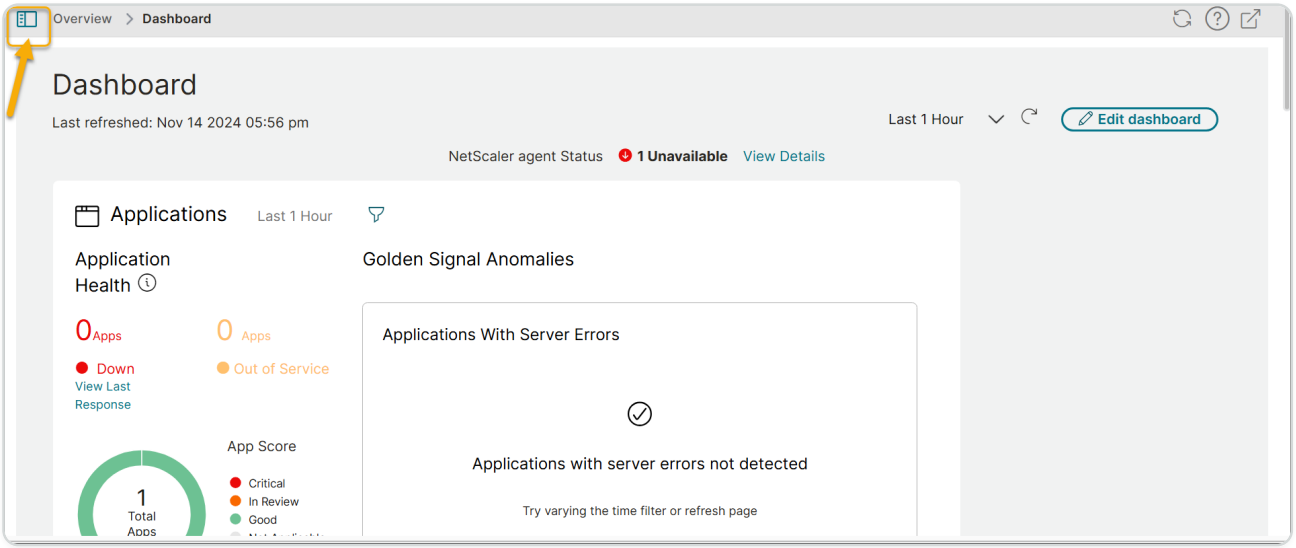
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Show sidebar



Hide sidebar

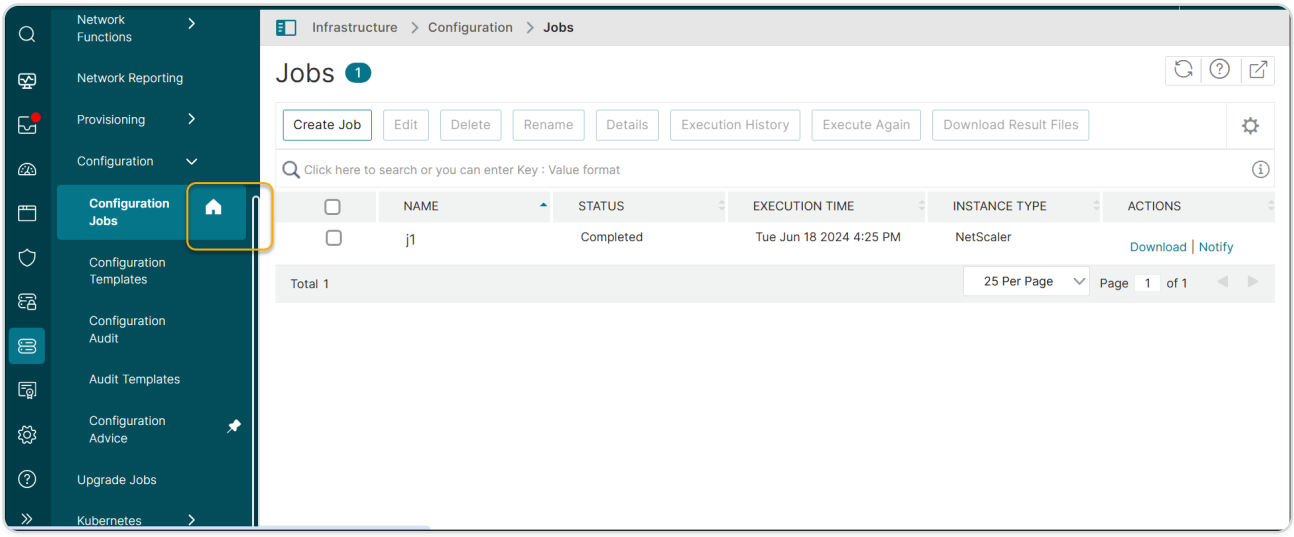
This option optimizes the screen space by hiding the sidebar.



Set as home screen

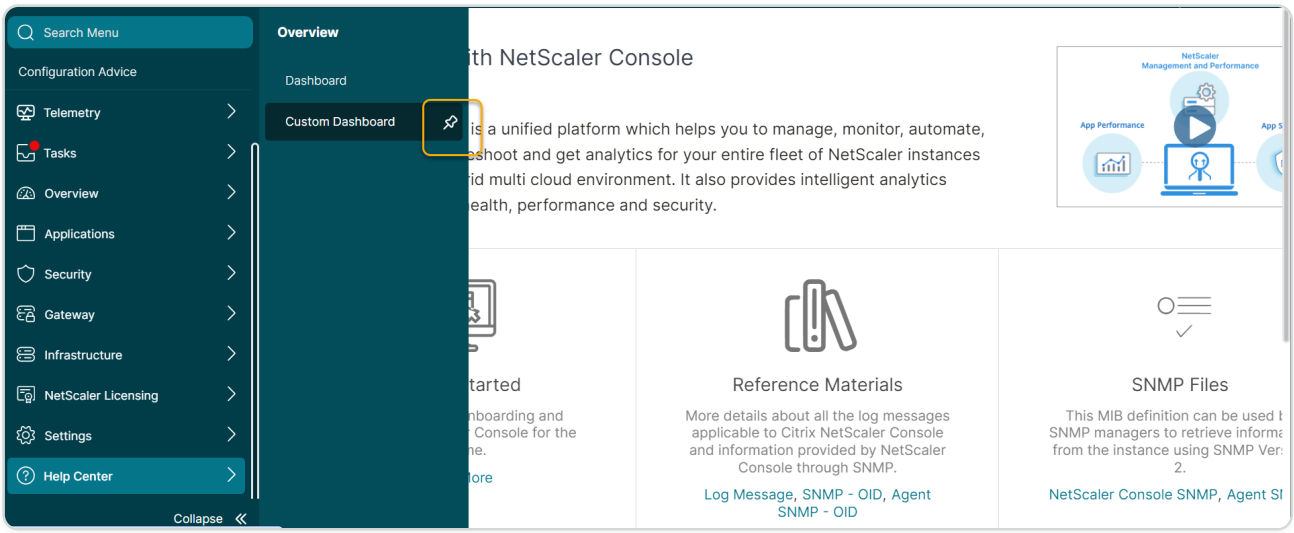
NetScaler Console GUI features an icon next to the name of a submenu that is displayed as a page.The home screen icon allows you to set your landing page. It only appears when you are on that specific page. To remove the page from the home page, simply click the icon again.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

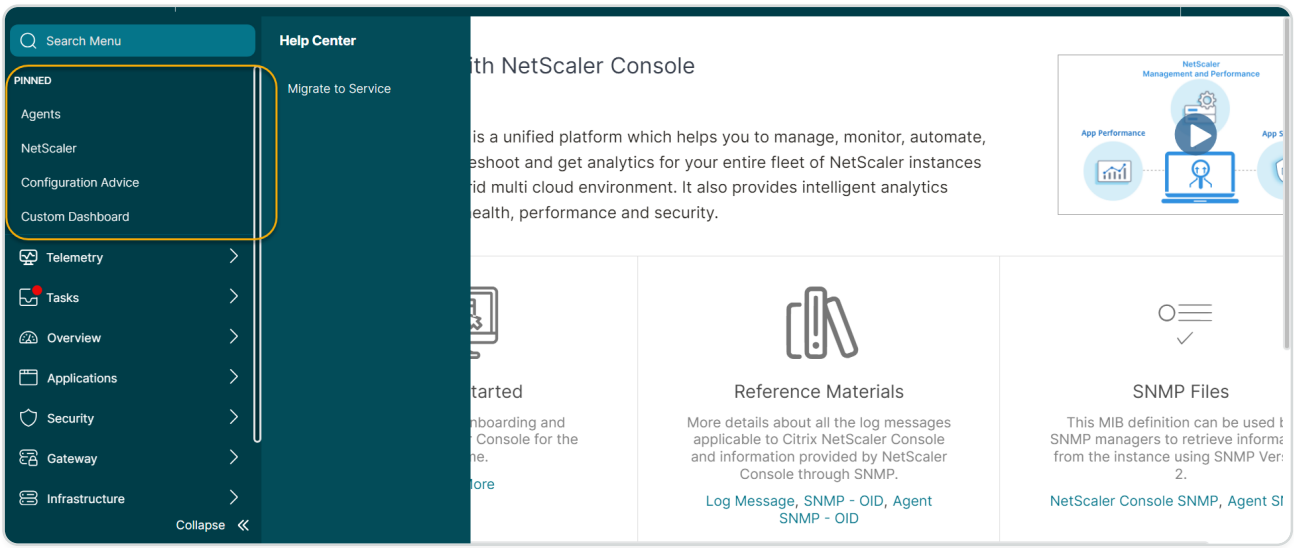


Pin favorite items

The **Pin** feature offers quicker access to your favorite items. To pin a menu or submenu, hover over it and click the pin icon that appears next to its name.



Pinned menus are displayed under **PINNED** in the sidebar, making them easily accessible.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Low-touch onboarding of NetScaler instances using Console Advisory Connect

As your hybrid multi-cloud (HMC) infrastructure grows, the challenges to manage, monitor, analyze, and troubleshoot NetScaler instances become multifold. A centralized controller providing visibility into your complete infrastructure and all the applications running on it becomes the need of the hour.

In today's world, onboarding your instances to a central controller needs to be done in a fast, easy, and low-touch manner. Keeping this need in mind, NetScaler Console launches a new onboarding workflow , which provides you a faster way to get complete visibility into your HMC deployment.

Overview: components of NetScaler Console onboarding workflow

The building blocks of this workflow are two ADC-side components: NetScaler service connect and Call Home.

- **Console Advisory Connect**: it is a new feature in NetScaler that helps enable seamless onboarding of NetScaler instances onto NetScaler Console. This feature lets the NetScaler instance automatically connect with NetScaler Console and send system, usage, and telemetry data to NetScaler Console. Based on this data, the NetScaler Console gives you insights and recommendations on your NetScaler infrastructure. Such as quick identification of performance issues, high resource usage, and critical errors.

  Console Advisory Connect is available on the following NetScaler versions:

  - NetScaler MPX and VPX image version 12.1 57.18 and later and 13.0 61.48 and later. For more information, see Introduction to NetScaler Console connect for NetScaler appliances.
  - NetScaler SDX version image 12.1 58.14 and later and 13.0 61.48 and later. For more information, see Introduction to NetScaler Console connect for NetScaler SDX appliances.

- **Call Home**: it is an existing feature in ADC, which periodically monitors the instances and automatically uploads data to the Citrix technical support server. For more details, see Call

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Home. The data collected by Call Home is also routed to NetScaler Console to enable this new workflow.

All NetScaler instances with internet connectivity or Call Home, or instances enabled with NetScaler Console connect are connected to NetScaler Console. NetScaler Console starts collecting relevant metrics from these NetScaler instances through Call Home route, NetScaler Console connect route, or both. For more information, see Data governance for MPX and VPX instances and Data governance for SDX instances.

Using this data, NetScaler Console creates an inventory of NetScaler instances for every customer (unique org ID), which shows you a consolidated list of your NetScalerinstances. NetScaler Console also uses this data to create insights on your NetScaler and Gateway instances, which give meaningful insights into your HMC deployments, identifies issues, and recommends actions to mitigate the issues. Before you can mitigate the issues, you must onboard the NetScalerinstances to NetScaler Console.

You can check **Select NetScaler and Gateway instances to onboard** and select the NetScaler instances you want to onboard to NetScaler Console. After you start, you are guided to the onboarding process.

The auto-onboarding process uses Console Advisory Connect, which makes the experience automated, seamless, and faster. For NetScaler instances on versions that do not support Console Advisory Connect and auto-onboarding, NetScaler Console provides script-based onboarding, which is a semi-automated process.

NOTES

- The auto and script-based onboarding use a built-in agent. However, this workflow also gives you the flexibility to use an external agent for onboarding. You can use the external agent-based onboarding if you want to use pooled licensing or the complete analytics suite in NetScaler Console. Or if you want both use pooled licensing and the complete analytics suite. The built-in agent supports only management and monitoring.
- The metrics collected by Console Advisory Connect are directly sent to the NetScaler Console service endpoint. Even if the NetScaler is a managed/discovered NetScaler on NetScaler Console and an external agent has been configured for that ADC, the metrics are sent directly from NetScalerto the NetScaler Console service endpoint and are not routed through through the external agent.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

A quick tour of onboarding

Your first touchpoint in the onboarding journey is a product-initiated email. Here's a quick tour of the onboarding journey:

1. A **NetScaler product-initiated email**: You receive an email from NetScaler Console showing some key insights of your NetScaler infrastructure and inviting you to get started with NetScaler Console. Click **Onboard to ADM Service** in the email. The **Citrix Cloud** page appears.
2. In the **Citrix Cloud™** login page:
   - If you are an existing Citrix Cloud customer, sign in to Citrix Cloud using your credentials of **Citrix.com**, **My Citrix**, or **Citrix Cloud**.
   - If you are not an existing Citrix Cloud customer, sign up to Citrix Cloud. For more information, see Signing Up for Citrix Cloud.

   NOTES

   - If you are part of multiple Org IDs and one of the Org IDs is in Citrix Cloud, sign in using your existing credentials. Then, complete the onboarding workflow for the new Org ID.
   - You can enable or disable the email notifications that you receive as part of Console Advisory Connect based low-touch onboarding workflow. For more information, see Email Settings.
3. **NetScaler Console welcome page**: You get an overview of NetScaler Console and its benefits.
4. **Insights on your NetScaler and Gateway instances**: You get detailed insights into your overall NetScaler infrastructure including security advisory (advice on current NetScaler CVEs), upgrade advisory (advice based on EOM/EOL timelines), key metrics, trends, and highlights the issues affecting NetScalerperformance and health and recommends way to mitigate the issues.
5. **Select NetScaler and Gateway instances to onboard**: You get a consolidated view of your NetScalerinventory. You can select which NetScalerinstances you want to onboard to NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. **Onboard NetScaler instances to NetScaler Console**: Based on the NetScalerinstances selected for onboarding, NetScaler Console guides you with the onboarding process. By default, the built-in agent is selected for auto-onboarding.
7. **NetScaler Console GUI dashboard**: After onboarding completes, you are guided to the NetScaler Console instance dashboard.

For more details on each of these onboarding methods, see Onboard NetScaler instances using NetScaler Console connect.

Onboard NetScaler instances using Console Advisory Connect

This document provides a step-by-step guide to help you get started with NetScaler Console. Before you start, read how the NetScaler Console launches a new onboarding workflow, which provides you a faster way to get complete visibility into your hybrid multi-cloud (HMC) deployment. See Low-touch onboarding of NetScaler instances using NetScaler Console connect.

Step 1: Get started

You receive an email from the NetScaler Console showing some key insights of your NetScaler infrastructure and inviting you to get started with the NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Onboard to Citrix ADM Service for Security Advisory



Hello [redacted] Org ID - [redacted]

As a valued Citrix customer, your application delivery infrastructure security is our top concern. To help keep your infrastructure secure, we just launched **security advisory and upgrade advisory** for your Citrix ADCs.

These new features can identify outdated software deployed in your ADC fleet, notify you of known vulnerabilities in these releases, and suggest steps you can take to remediate these issues.

Below, you'll see a preview of these advisories and other key insights customized to your infrastructure. More information and recommended actions are available when you onboard to Citrix ADM service. You can get started with Citrix ADM Service Express account at no additional cost.

Insights on your ADC & Gateway infrastructure

These insights are based on data provided via Call Home and/or Citrix ADM Service Connect.

ADC instances by platforms

30	20	5	5
Total	VPX	SDX	MPX

Security Advisory

5 ADC instances are on versions with known common vulnerability exposures (CVEs).
This advisory is based on ADC build version scan only & more conclusive & exhaustive security advisory insights can be seen after onboarding all your ADCs to ADM Svc

Upgrade Advisory

2 ADC instances are on versions that have reached end of life in last 365 days or earlier.

1 ADC instance is on a version that will reach end of life in next 365 days.

3 ADC instances are on versions that have reached end of maintenance in last 365 days or earlier.

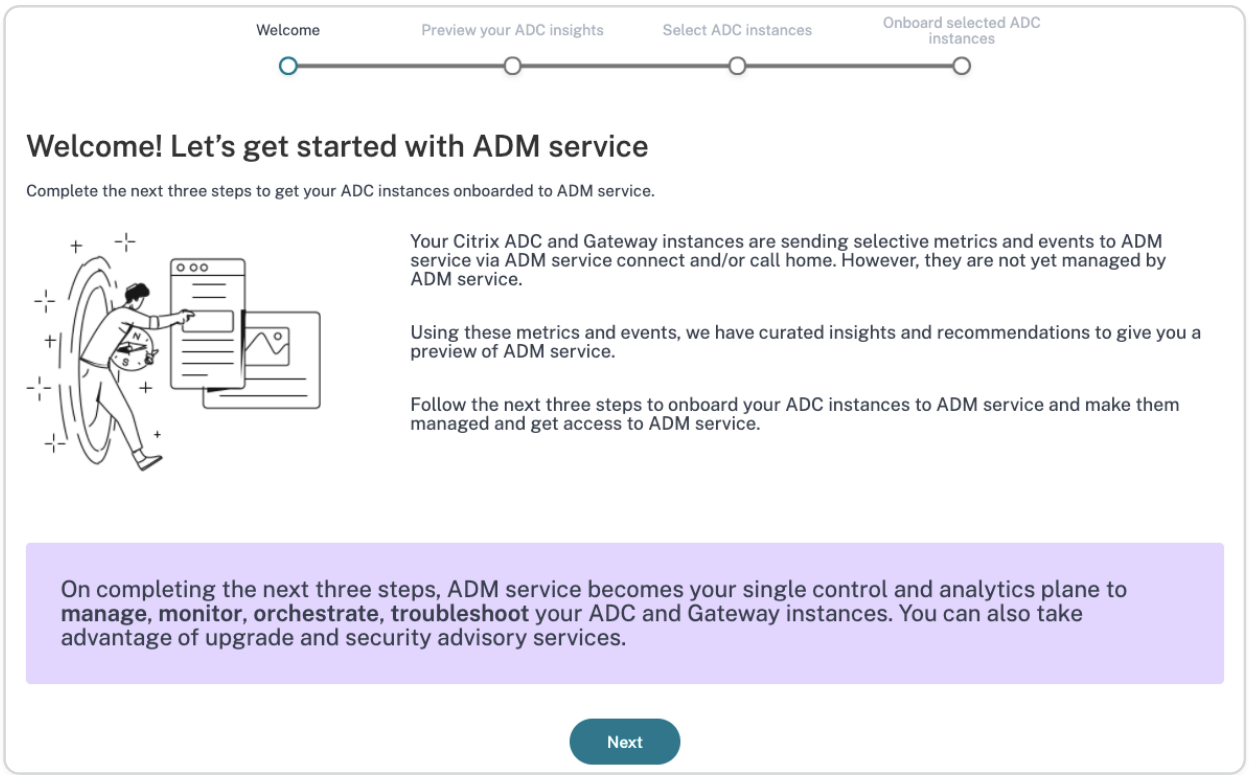
4 ADC instances are on versions that will reach end of maintenance in next 365 days.

1. In the email, click **Onboard to ADM Service**. The **Citrix Cloud™** page appears.
2. In the **Citrix Cloud** login page:
   - If you are an existing Citrix Cloud customer, sign in to Citrix Cloud using your credentials of **Citrix.com**, **My Citrix**, or **Citrix Cloud**.
   - If you are not an existing Citrix Cloud customer, sign up to Citrix Cloud. For more information, see Signing Up for Citrix Cloud.

NOTES

- If you are part of multiple Org IDs and one of the Org IDs is in Citrix Cloud, sign in using your existing credentials. Then, complete the onboarding workflow for the new Org ID.
- You can enable or disable the email notifications that you receive as part of Consolve Advisory Connect based low-touch onboarding workflow. For more information, see Email Settings.

3. In the NetScaler Console landing page, take a moment to read why you are there and the benefits of using NetScaler Console.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

The security advisory insights in the email are based on NetScaler build version scan only. You can see more conclusive and exhaustive security advisory insights after onboarding your NetScaler instances to NetScaler Console.

1. Click **Next**. The **Insights on your NetScaler and Gateway instances** page opens.

The next few steps act as a guided workflow to give you a preview into what NetScaler Console can offer and help you onboard your NetScaler instances onto NetScaler Console seamlessly.

Step 2: Insights on your NetScaler and Gateway instances

This insights page uses the data collected through Call Home or NetScaler Console connect or both Call Home and NetScaler Console connect to provide insights on your NetScaler instances. This page gives you insights into your overall NetScaler infrastructure including security advisory (advice on current NetScaler CVEs), upgrade advisory (advice based on EOM/EOL timelines), key metrics, trends, and highlights the issues affecting NetScaler performance and health and recommends way to mitigate the issues. These insights and recommendations are only a small preview of the plethora of benefits and value-add that NetScaler Console has to offer. To get many more benefits, detailed insights and to be able to run the recommended actions, you must onboard the NetScaler instances onto NetScaler Console.

The insights and recommendations are categorized into the following types:

- **Security advisory**: onboard NetScaler instances to get the CVE impact details on your NetScaler instances and run the recommended remediations or mitigations.
- **Upgrade advisory**: onboard NetScaler instances onto NetScaler Console and upgrade your NetScaler instances that have reached or are reaching EOM/EOL or are on older releases/ builds.
- **Recent events**: onboard NetScaler instances to NetScaler Console to monitor 200+ events regularly, and create rules to get notified over email, PagerDuty, Slack, ServiceNow, take appropriate action.
- **Resource utilization - trends and anomalies**: onboard NetScaler instances to NetScaler Console to get a comprehensive view of NetScaler instance health, performance issues, and recommendations to mitigate those issues. You can also assess predicted CPU and memory usage for your NetScaler instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

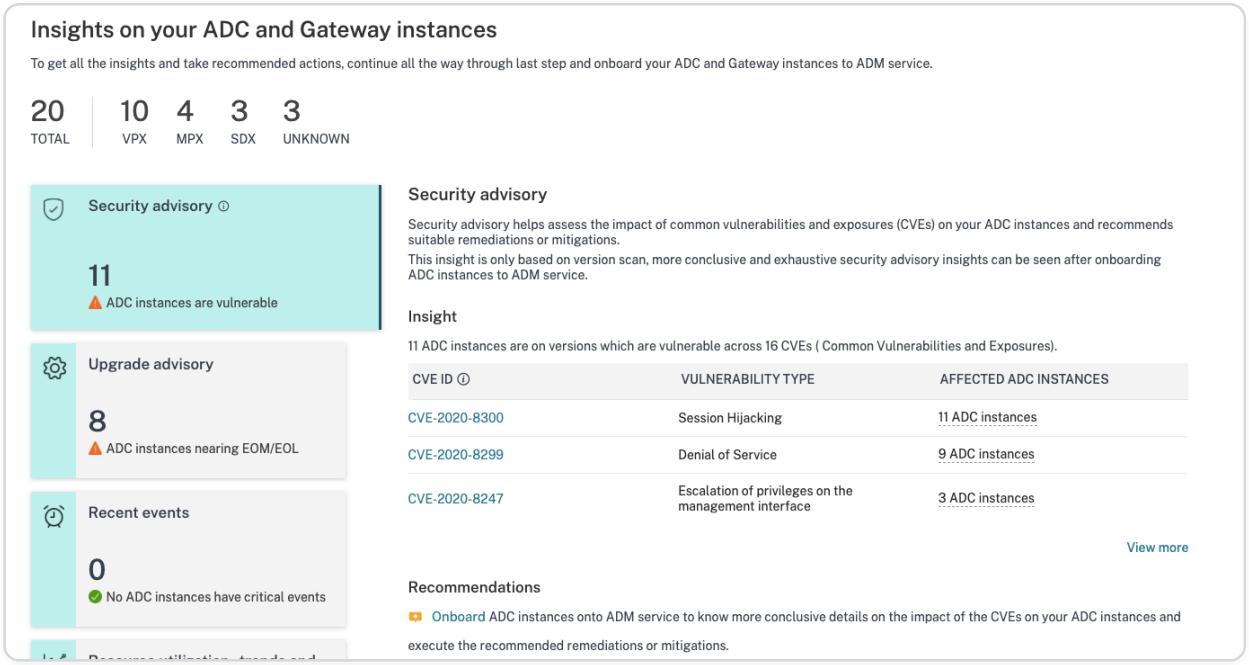
- **NetScaler deployment guidance**: onboard NetScaler instances to NetScaler Console and configure them as HA pair, using configuration jobs on NetScaler Console.

1. **Security advisory**: NetScaler Console Security Advisory alerts you about vulnerabilities putting your NetScaler instances at risk and recommends mitigations and remediations.

   NOTE:

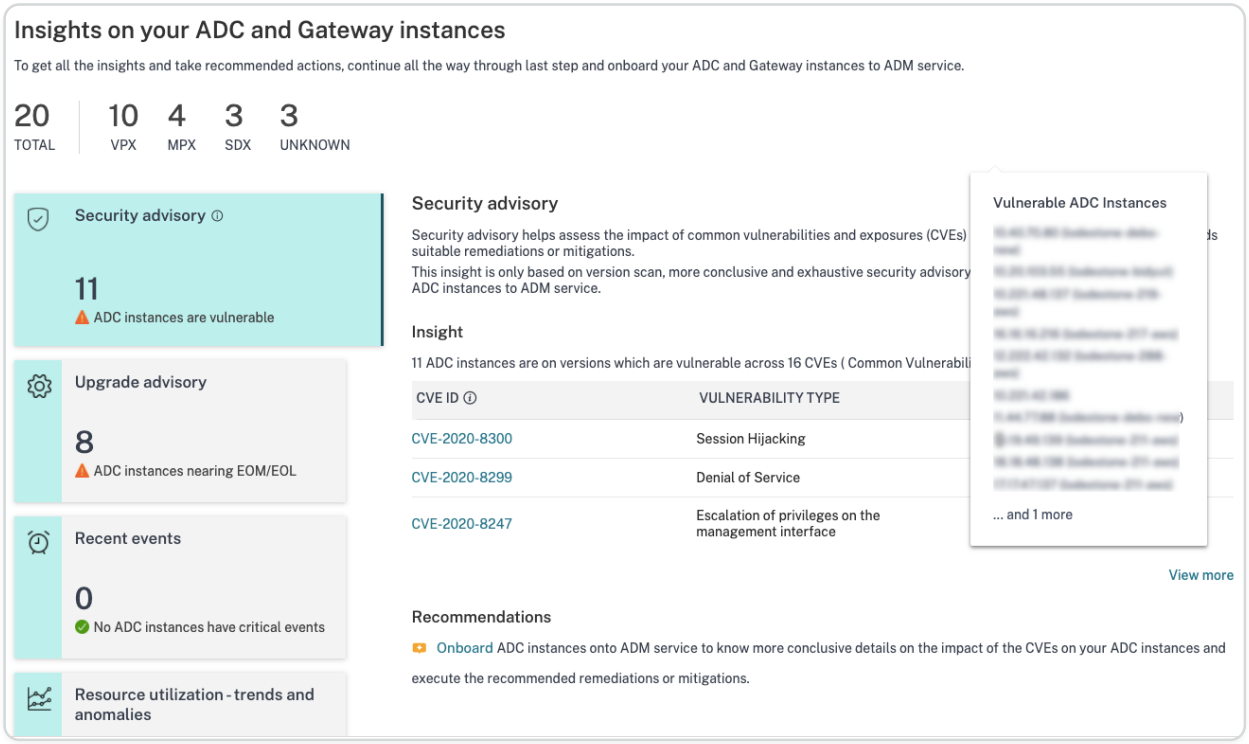
   Security advisory insights in the onboarding email and guided workflow are based on NetScaler build version scan only. You can see conclusive and exhaustive security advisory insights after onboarding your NetScaler instances to NetScaler Console **Example**: If a CVE needs both version scan and config scan for vulnerability assessment, the onboarding email and guided workflow shows the results based on version scan. So, there might be false positives. To know a more conclusive and accurate assessment of the impact, onboard NetScaler to NetScaler Console. After onboarding, NetScaler Console security advisory shows the impact assessment, which vulnerable NetScaler assessment, based on versions scan and config scan.

   You can check the CVE ID, vulnerability type, and affected NetScaler instances. The CVE ID link takes to the security bulletin article.



   The recommendation guides you to onboard your NetScaler instances to NetScaler Console to get more details of the CVE impact on your NetScaler instances and run the recommended mitigation or remediation. Click the affected NetScaler instances to see the IP addresses of the impacted instances.

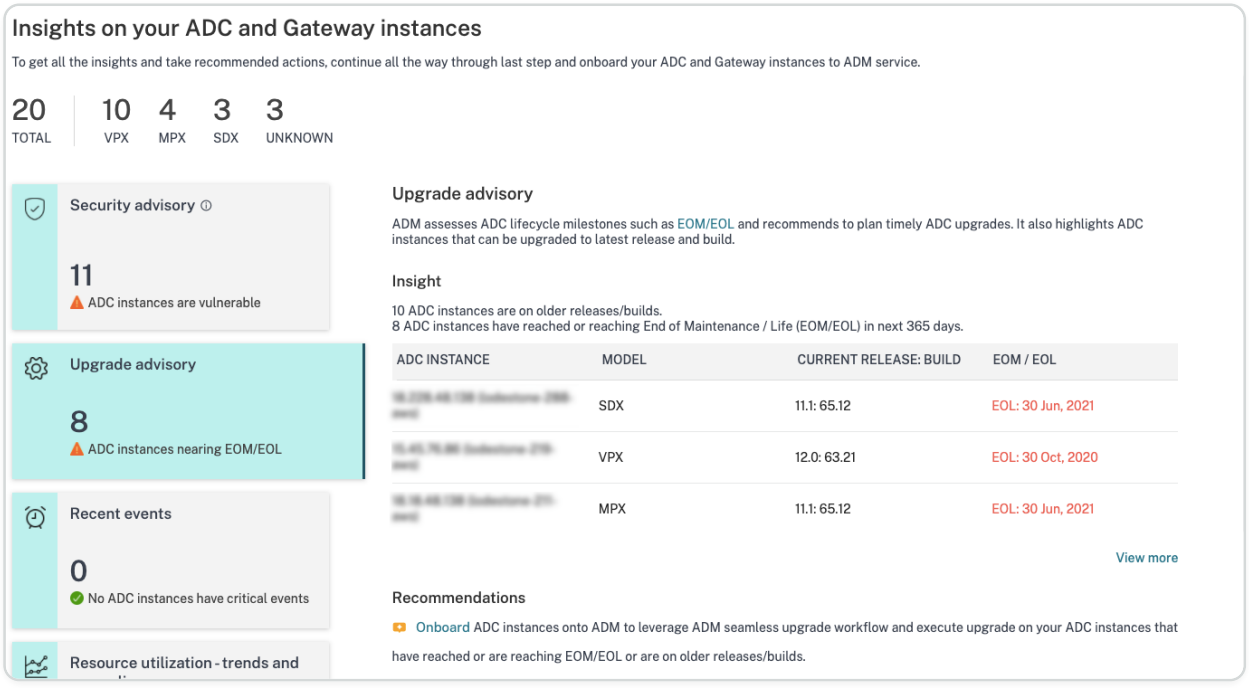
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. **Upgrade advisory**: Use this advisory to check which NetScaler instances are nearing EOM/EOL or are on older builds.

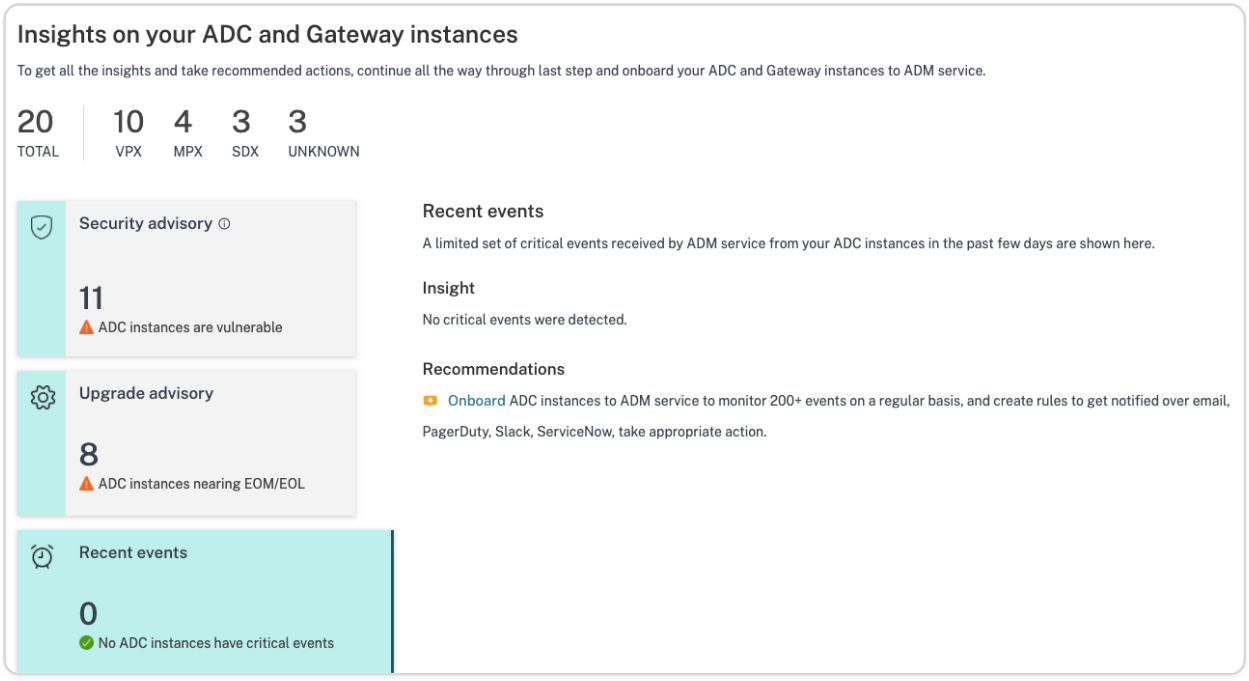
   Based on these insights, NetScaler Console recommends you to plan a timely upgrade before EOM/EOL or to benefit from the latest features and fixes.

   To perform the upgrade, you must onboard your NetScaler instances on to NetScaler Console.



3. **Recent events**: Get details of some critical errors that have happened on the NetScaler instances and a list of NetScaler instances on which the errors have occurred.

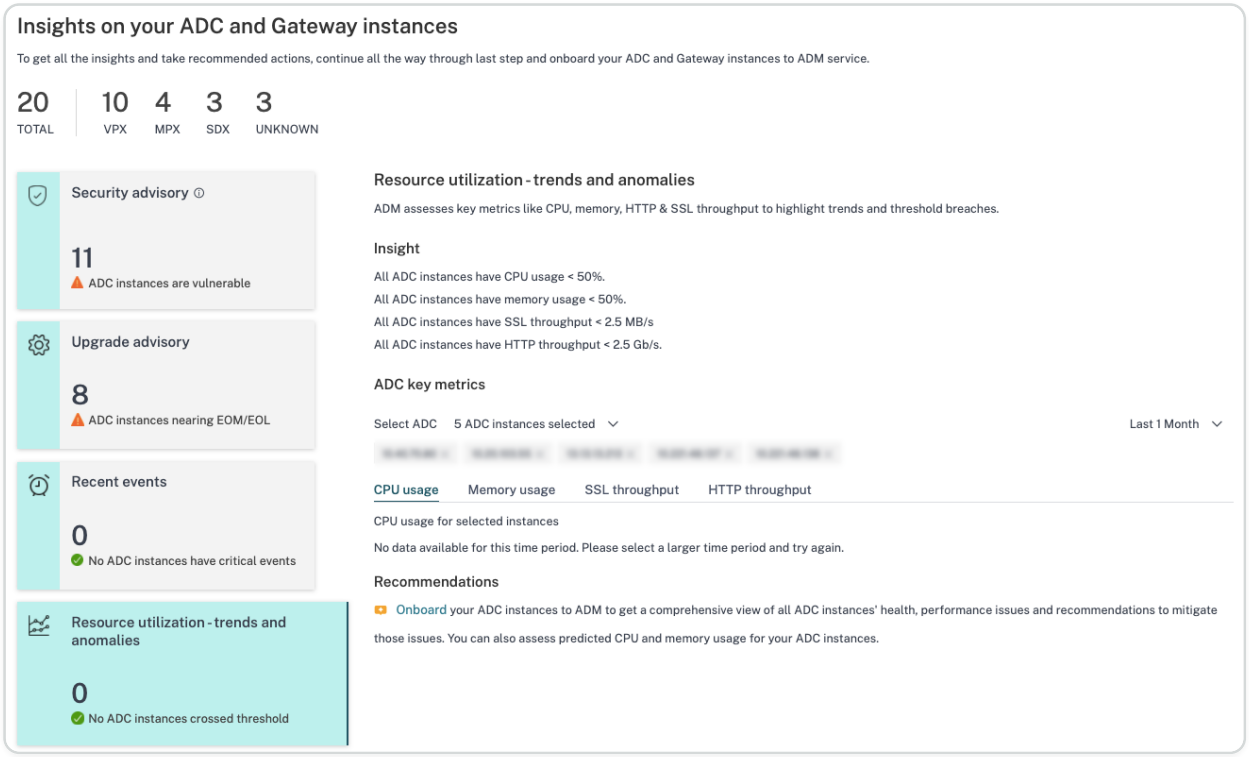
© 1997–2026 Citrix Systems, Inc. All rights reserved.



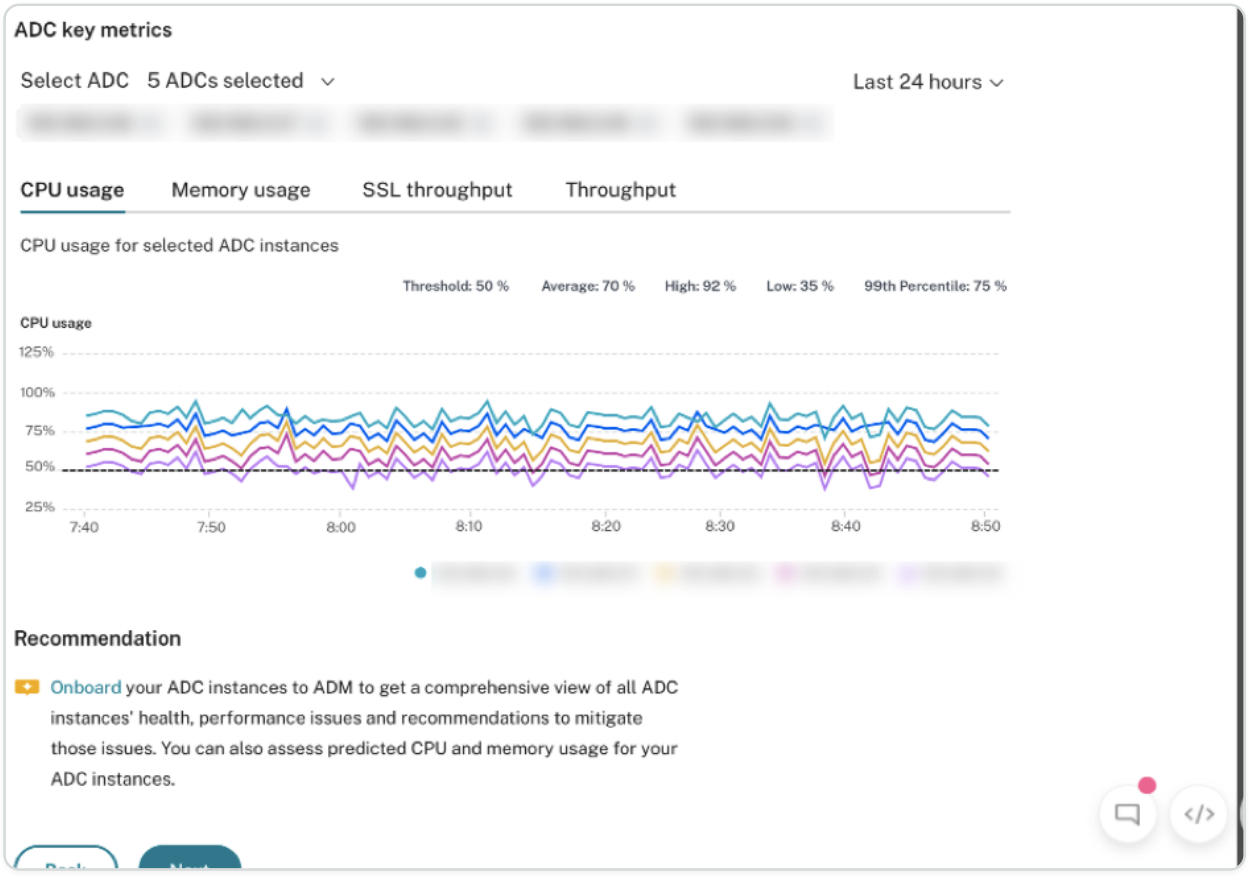
4. **Resource utilization - trends and anomalies**: Find insights about high resource utilization for CPU, memory, HTTP throughput, and SSL throughput. For each insight, NetScaler Console suggests recommended action. To have more visibility into these insights and recommendations, you must onboard your NetScaler instances onto NetScaler Console. Some benefits after onboarding are:

    - CPU: Predict CPU utilization for the next 24 hours on NetScaler Console.
    - Memory: Predict memory utilization for the next 24 hours on NetScaler Console.
    - SSL throughput: View SSL real time optimization with intelligent App Analytics on NetScaler Console.
    - HTTP Throughput: Troubleshoot NetScaler throughput capacity issues with Infrastructure Analytics.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



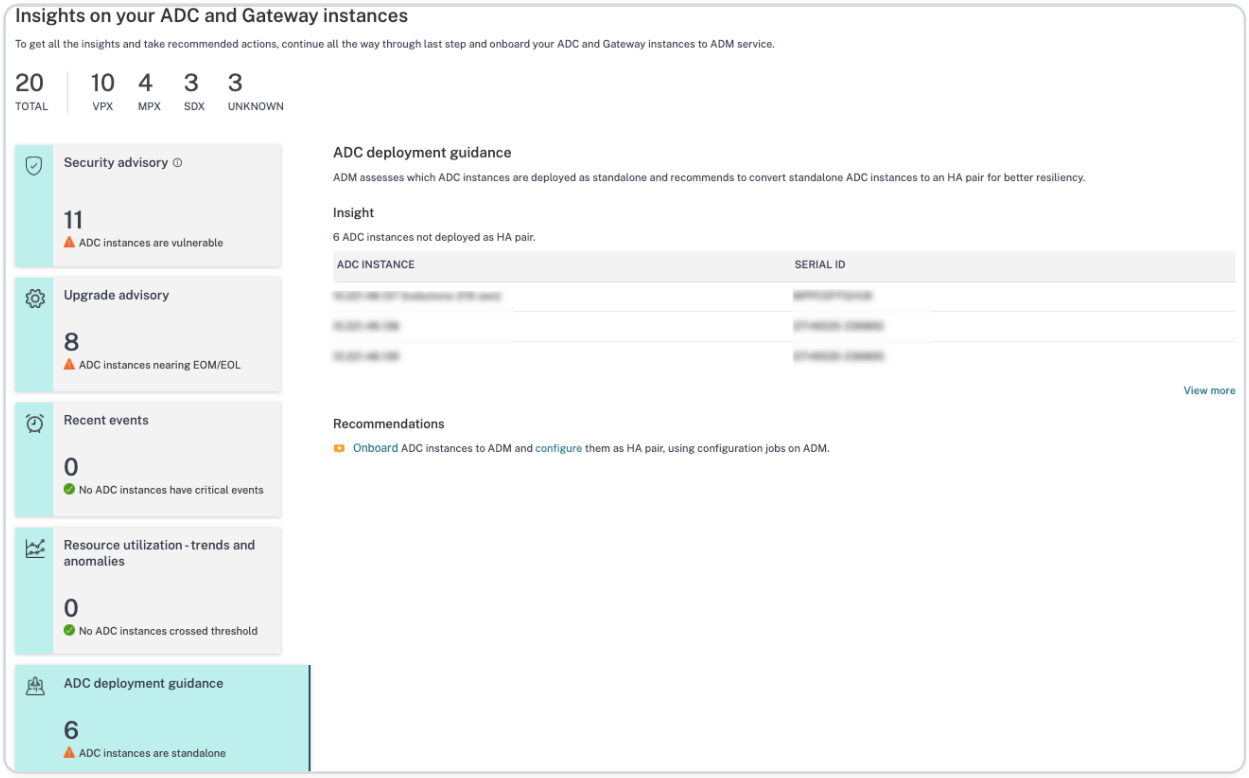
- **Key Metrics**: Get details of key metrics related to CPU, memory, HTTP throughput, SSL throughput, and uncover anomalous trends in metrics.



5. **Deployment guidance**: Have visibility into NetScaler instances that are deployed as a standalone NetScaler. NetScaler Console gives the recommendation to configure these NetScaler instances as an HA pair for better resiliency. This requires you to onboard your

© 1997–2026 Citrix Systems, Inc. All rights reserved.

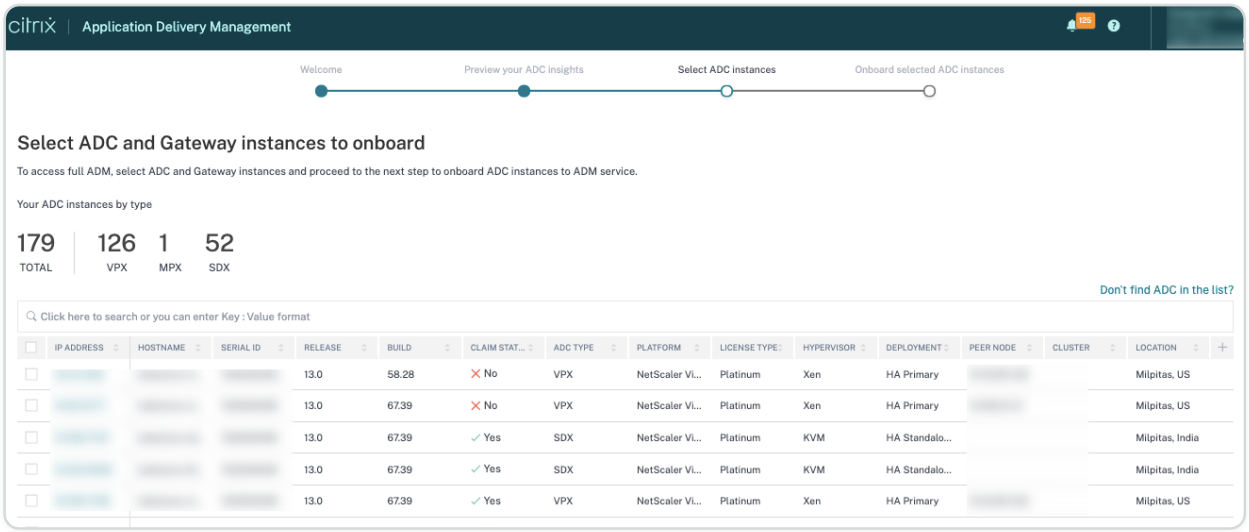
NetScaler instances to NetScaler Console and then use maintenance jobs to configure the instances as an HA pair.



Step 3: Select NetScaler and Gateway instances to onboard

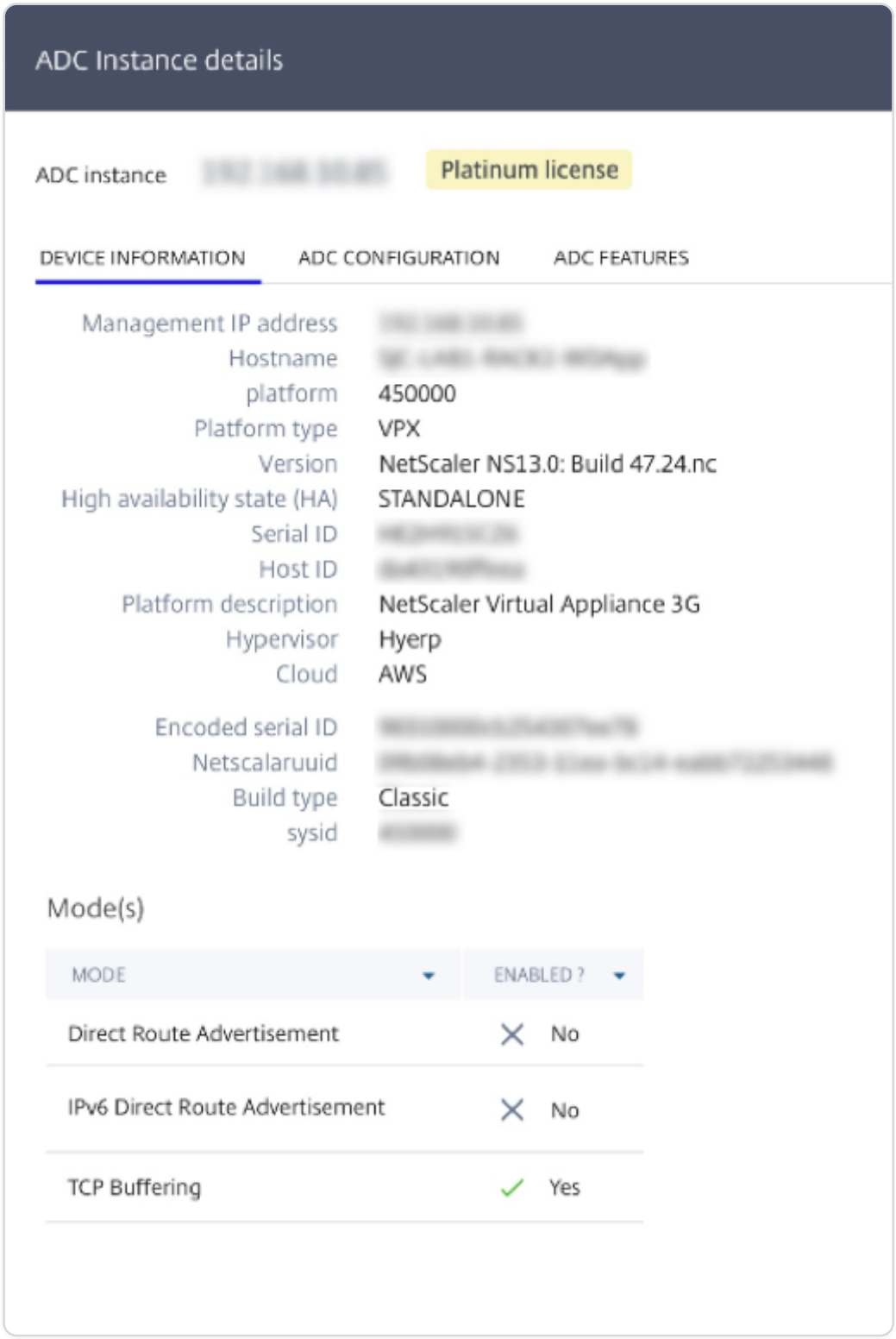
This page displays all the NetScaler and Gateway instances in your environment. View and select the NetScaler and Gateway instances you want to onboard to NetScaler Console and click **Next**.

1. View and select the NetScaler instances you want to onboard to NetScaler Console.



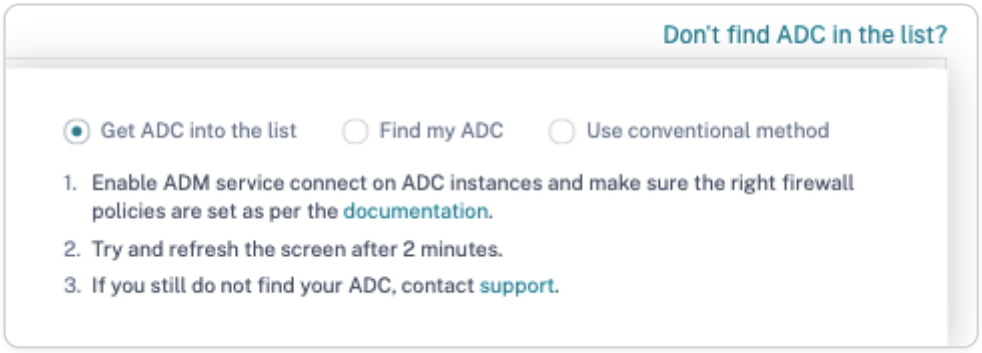
If you need details about any instance such as device information, NetScaler configuration, NetScaler features available, or license information, click the instance IP address under the NetScaler instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



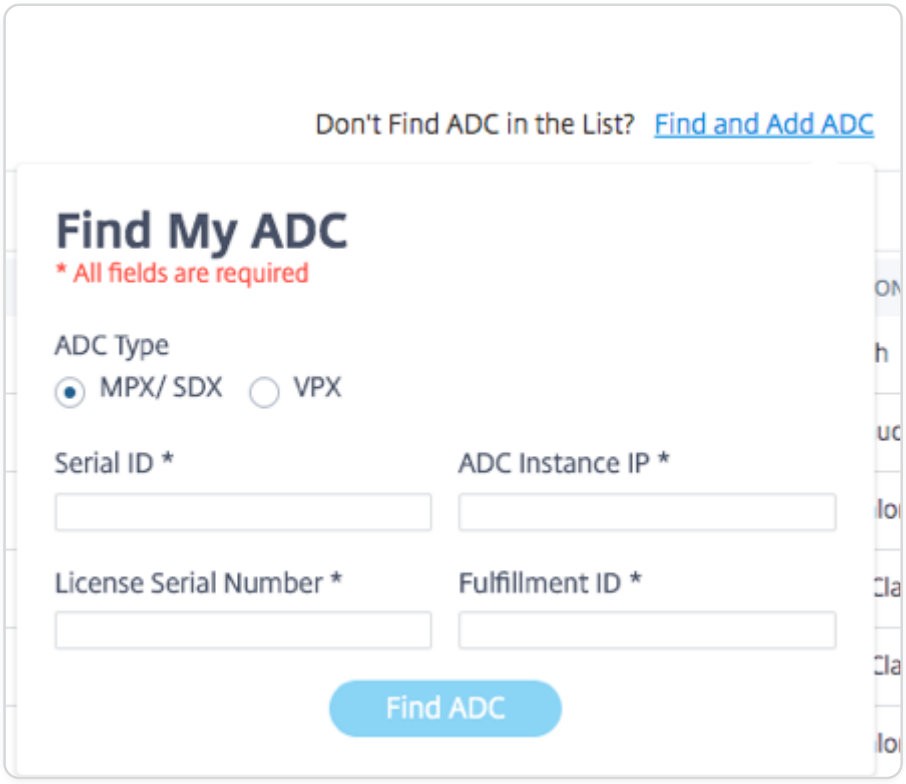
If your instance is not listed, use the **Don't find NetScaler in the list** on the upper-right corner.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can proceed in three ways: follow the steps given under **Get NetScaler into the list** or use the **Find my NetScaler option**. If these two steps do not help, click **Use conventional method** option, which skips the workflow and takes you through the traditional way of onboarding NetScaler instances.

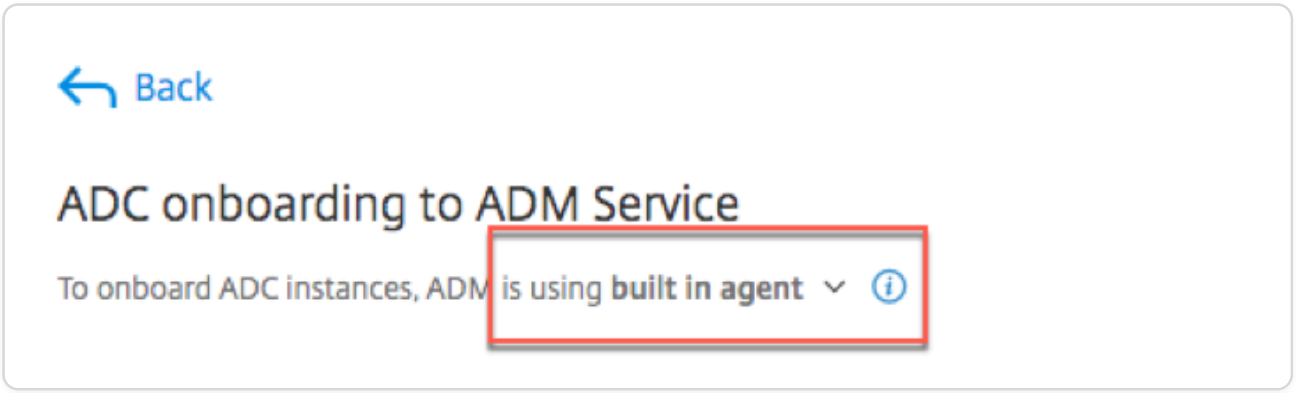
For the **Find my NetScaler option**, enter the details in the mandatory fields (serial ID, NetScaler instance IP address, license serial number, and fulfillment ID) and search.



Step 4: Onboard NetScaler instances to NetScaler Console

You can onboard your instances using the built-agent (default option) or an external agent.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Onboard NetScaler instances using a built-in agent

Auto and script-based onboarding use the built-in agent, which is set by default.

Auto-onboarding: It is supported only on the following NetScaler versions:

- NetScaler MPX and VPX image version 12.1 57.18 and later and 13.0 61.48 and later
- SDX version image 13.0 61.48 and later and 12.1 58.14 and later

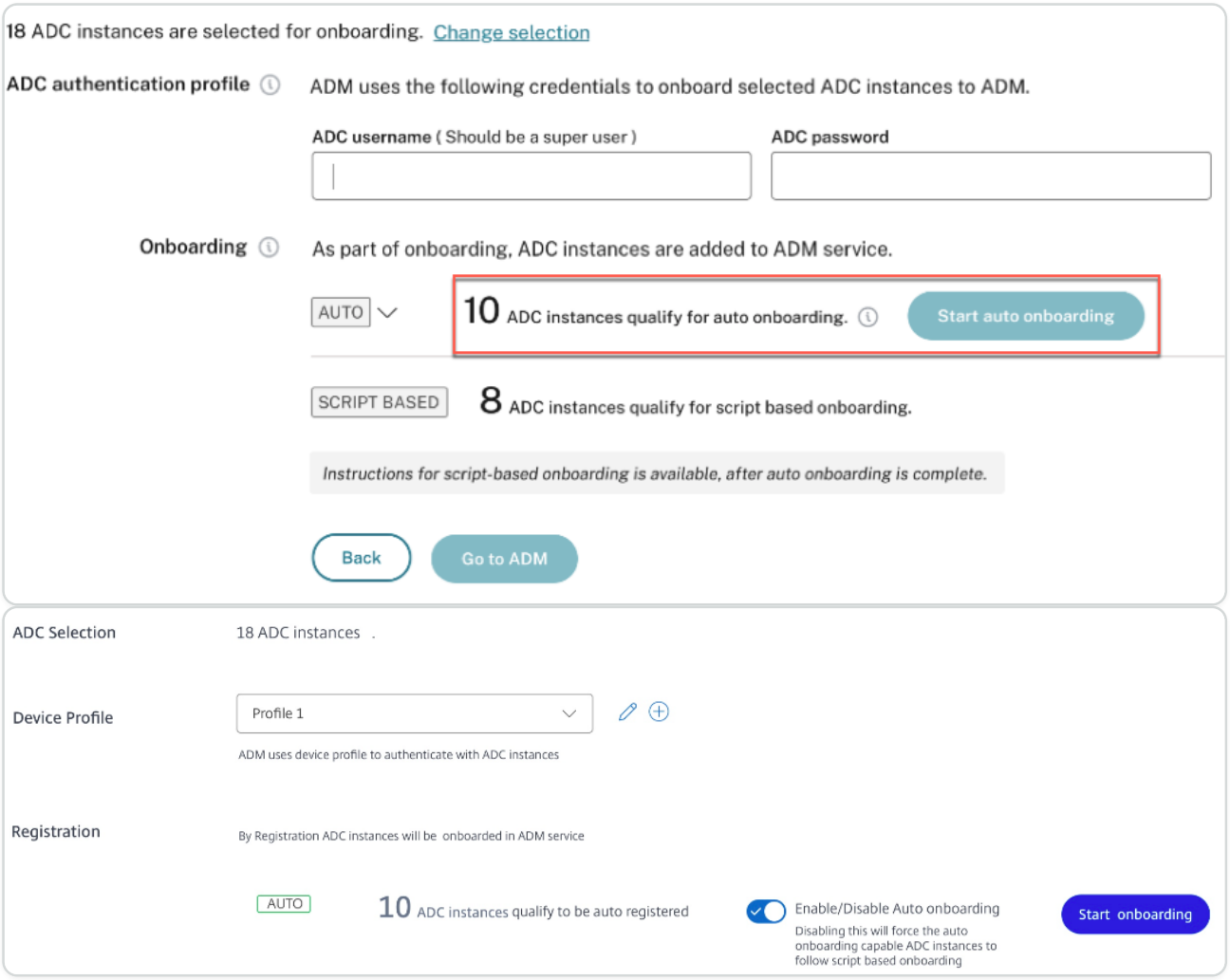
To select a different NetScaler instance, click **Change selection**.

Out of the total selected NetScaler instances, some instances might qualify for auto-onboarding (based on minimum version criteria). You can see the instances that qualify for auto-onboarding.

You can perform a test run of onboarding to ensure that the NetScaler instance is ready to onboard. Click **Test** to start the test run. For more information, see Test onboarding readiness of NetScaler instances.

If you want to onboard without the test run, enter the NetScaler user name and password. The credentials must be NetScaler user admin credentials, and NetScaler Console uses these credentials to onboard NetScaler. Click **Start auto onboarding** to onboard your NetScaler instances on NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

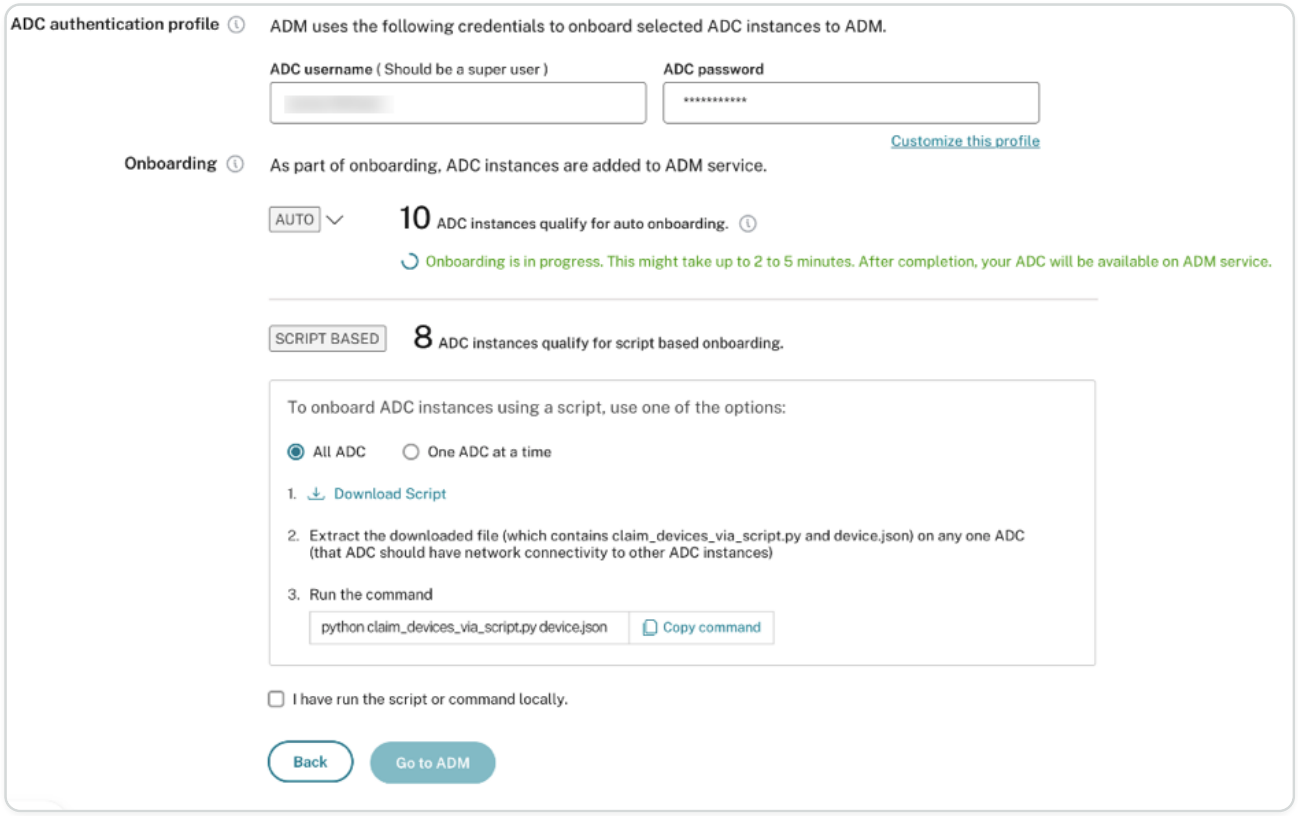


NOTE

After you specify the NetScaler credentials and create the Device Profile, the ADM GUI will not prompt for the Username and Password again for each NetScaler instance. However, you can select the profile from the **Device profile** drop-down to authenticate the NetScaler instances.

Auto-onboarding might take up to 2-5 minutes to complete.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



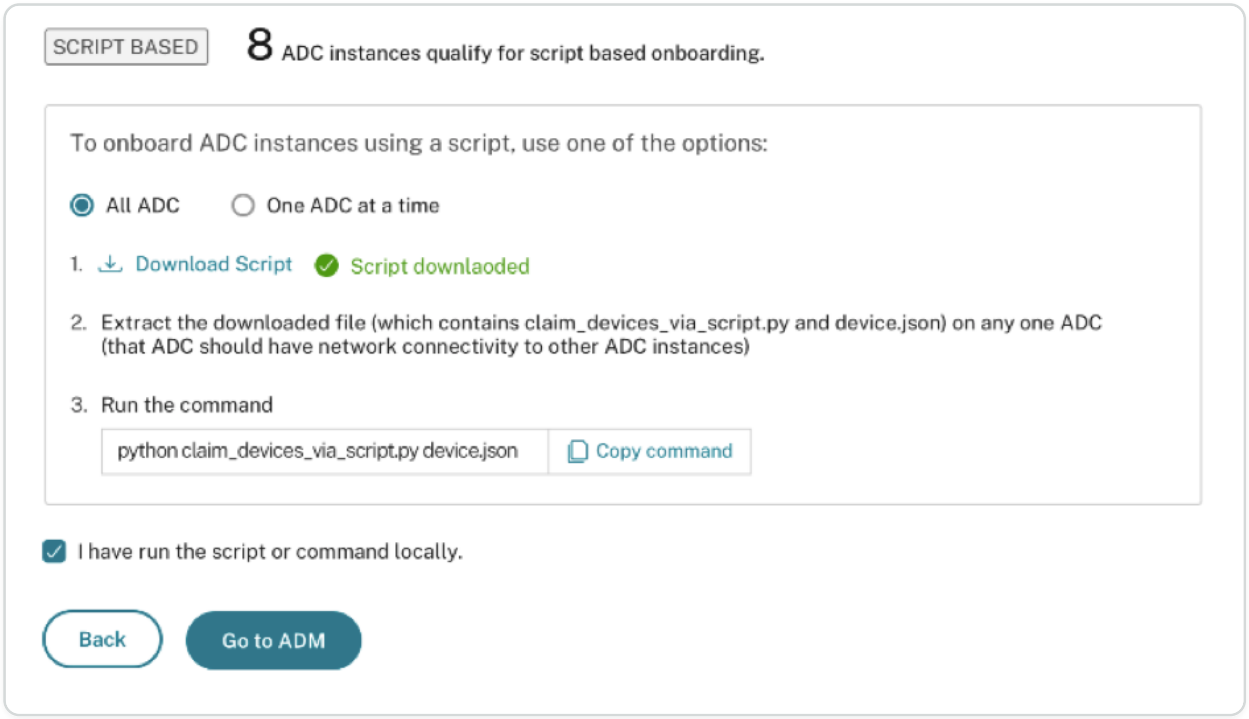
NOTE:

If you don't want the NetScaler instances to auto-onboard to NetScaler Console, you can disable auto-onboarding and you use the script-based option for on onboarding.

Script-based onboarding: after auto-onboarding completes, you can onboard the rest of the instances using the script-based onboarding. Use one of the following options:

- **Option 1**: download the script, extract the tar file, and run it on any one of the NetScaler instances, using the command given on the UI. Ensure that the NetScaler instance on which you run this script has network connectivity to all the other selected NetScaler instances.
- **Option 2**: Log in to the CLI console of each NetScaler instance and run the commands given on the UI. For more details, refer to step 7 in the doc Configure the NetScaler built-in agent to manage instances. Ensure that you generate a new unique activation code for each of the NetScaler instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



After you've onboarded all your instances, click **Go to NetScaler Console** to go to the NetScaler Console instance management UI dashboard and explore the different features.

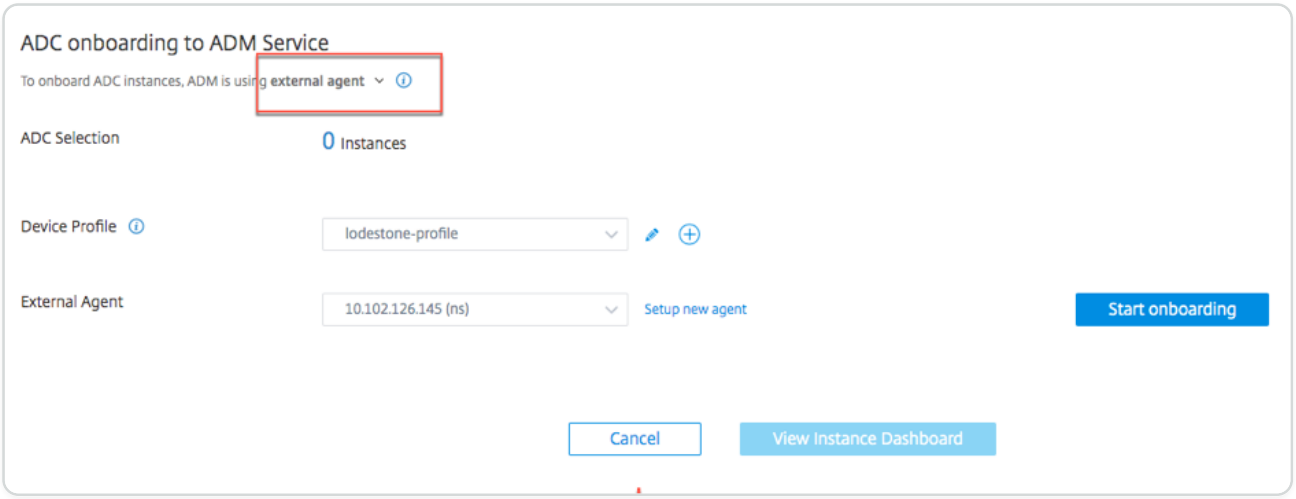
NOTE

If you are a new customer on NetScaler Console without an NetScaler Console license, your Citrix service account by default is an Express account. For more information about the NetScaler Console account entitlement, see Manage NetScaler Console resources using Express account.

Onboard NetScaler instances using an external agent

You can use external agent-based onboarding if you want to use pooled licensing or the complete analytics suite in NetScaler Console or both use pooled licensing and the complete analytics suite.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Complete the following steps:

1. Select a device profile.

   NOTE

   For security reasons, you can't use the default NetScaler credentials (nsroot/nsroot) for onboarding.

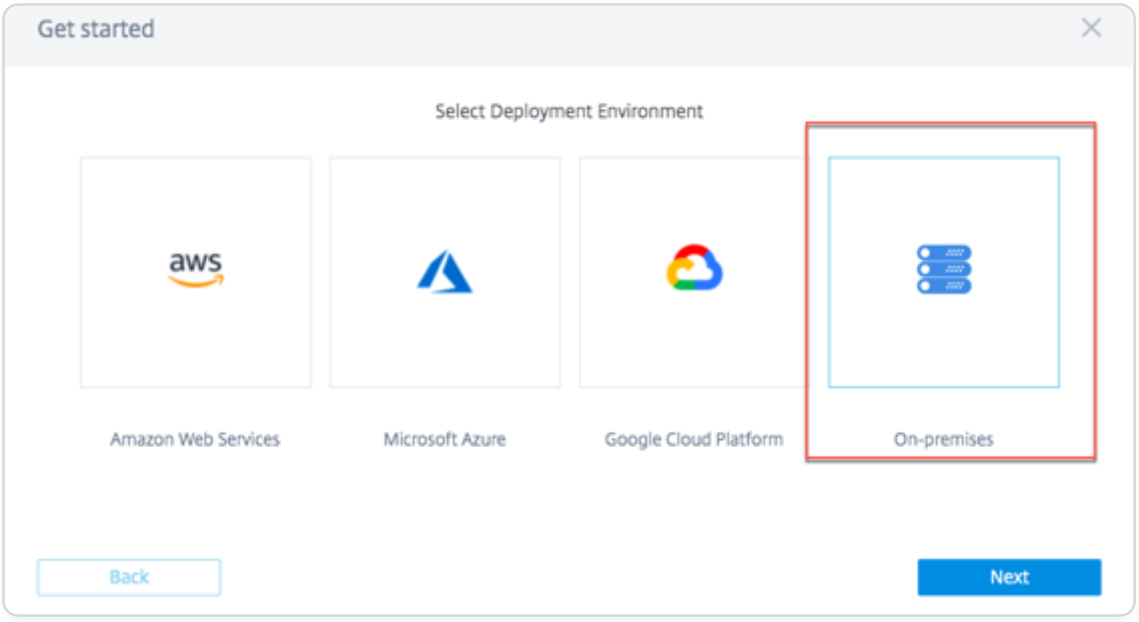
2. Select an external agent and click **Setup new agent**.
3. Select any of the following environments:

   - Amazon Web Services
   - Microsoft Azure
   - Google Cloud Platform
   - On-premises

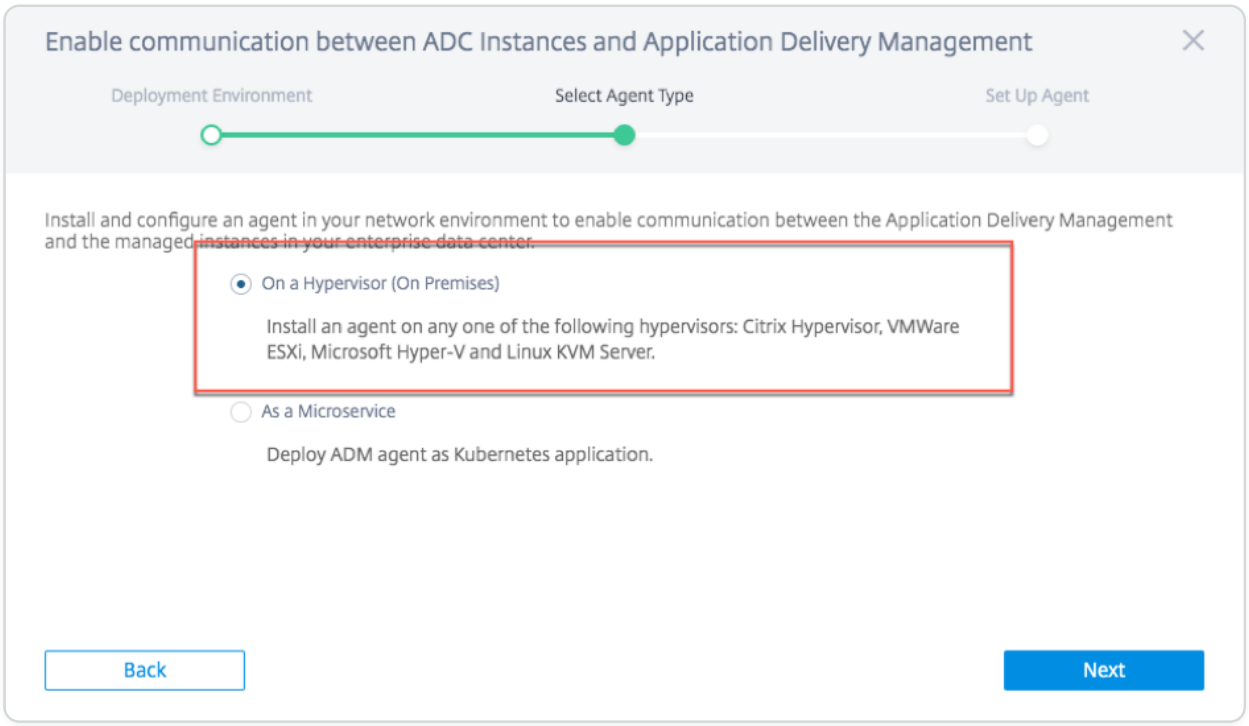
Install an agent on your on-premises hypervisor

If you select **On-premises**, you can install the agent on the following hypervisors: Citrix Hypervisor™, VMware ESXi, Microsoft Hyper-V, Linux KVM Server.

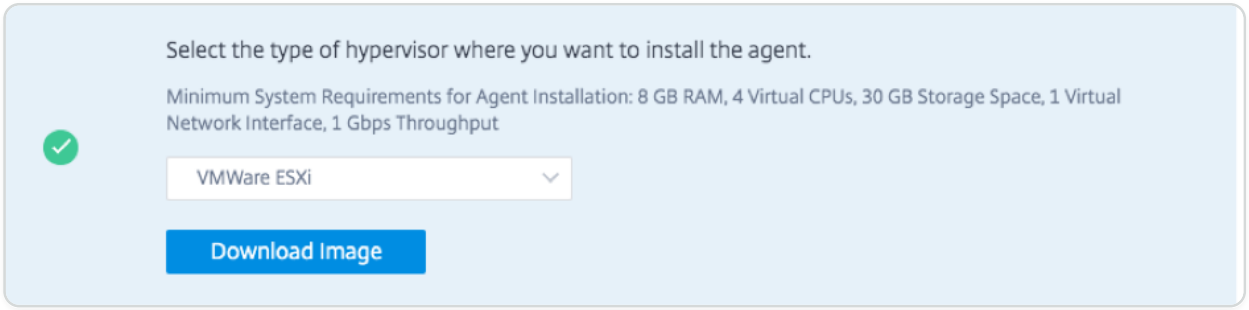
© 1997–2026 Citrix Systems, Inc. All rights reserved.



1. Select **On a Hypervisor (On Premises)** and click **Next**.

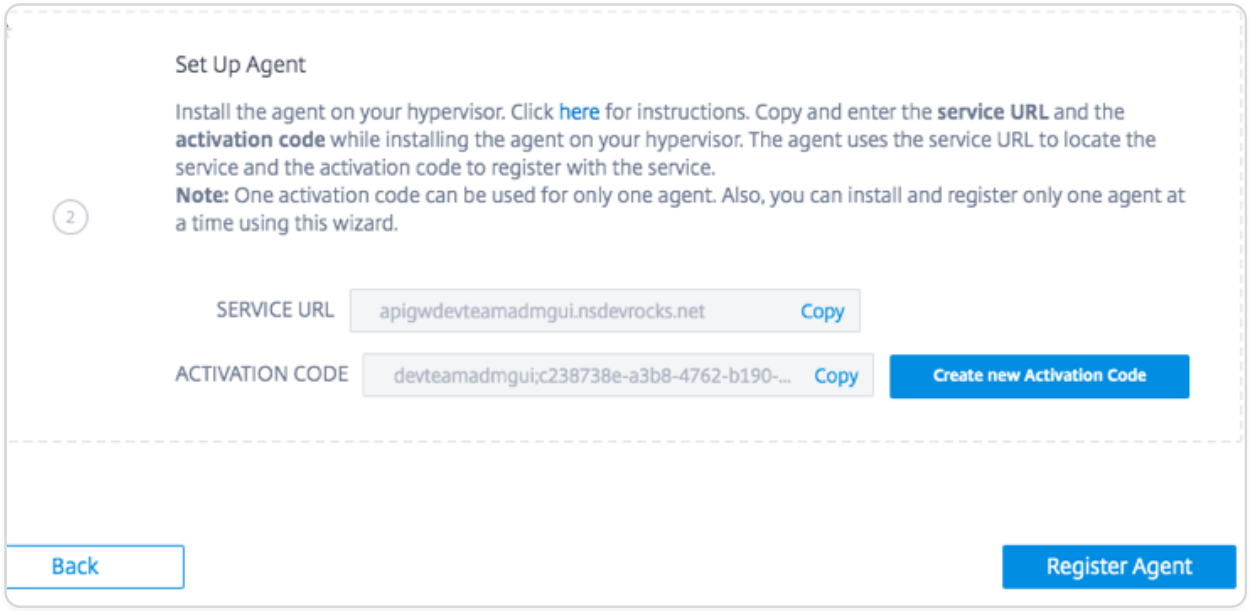


2. Select the hypervisor type and download the image, for example, VMware ESXi.



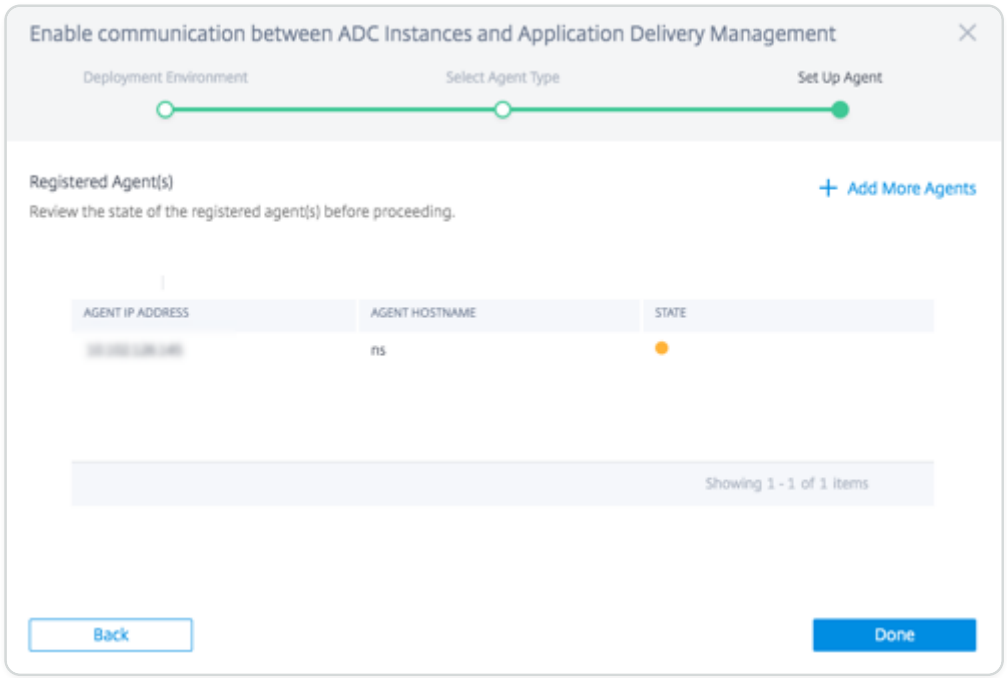
3. Use the service URL and activation code to configure the agent.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



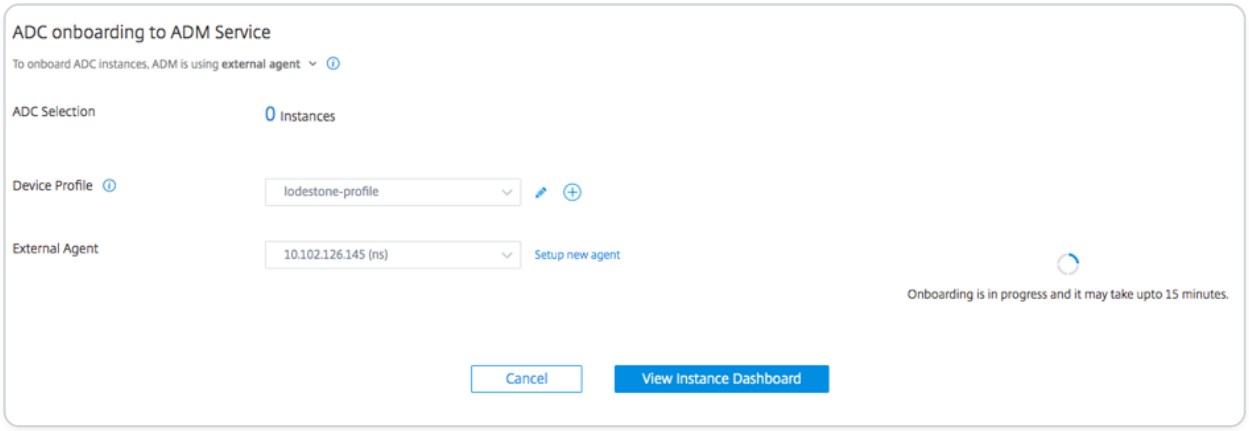
The agent uses the service URL to locate the service and the activation code to register with the service. For detailed instructions about installing an agent on your on-premises hypervisor, see Install a NetScaler agent on-premises

4. Click **Register Agent**. When completed, and click **Done** to return to the NetScaler onboarding NetScaler Console page.



5. Click **Start onboarding**. After you've onboarded all your instances, click **View instance dashboard** to go to the NetScaler Console instance management UI dashboard and explore the different features.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Install an agent on a public cloud

You can install the agent in one of the following cloud environments:

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform

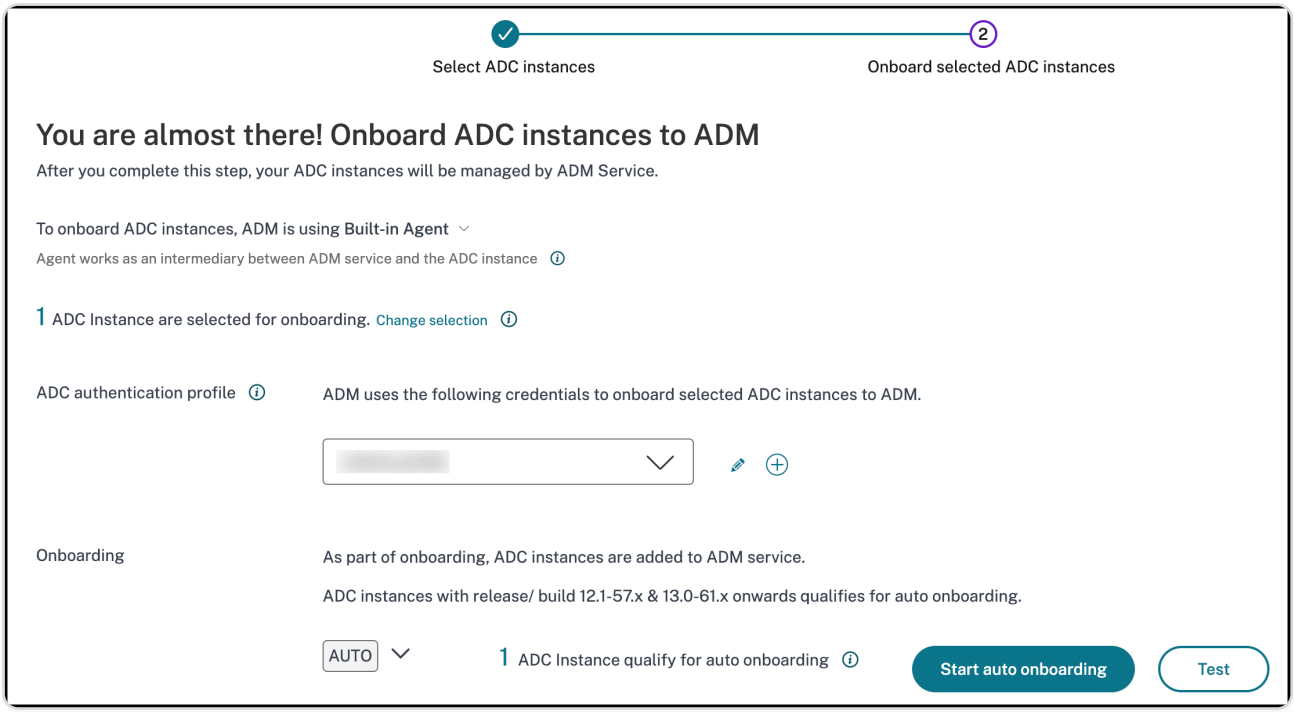
For more information, see the following documents:

- Install an agent on Microsoft Azure cloud
- Install an agent on AWS
- Install an agent on GCP

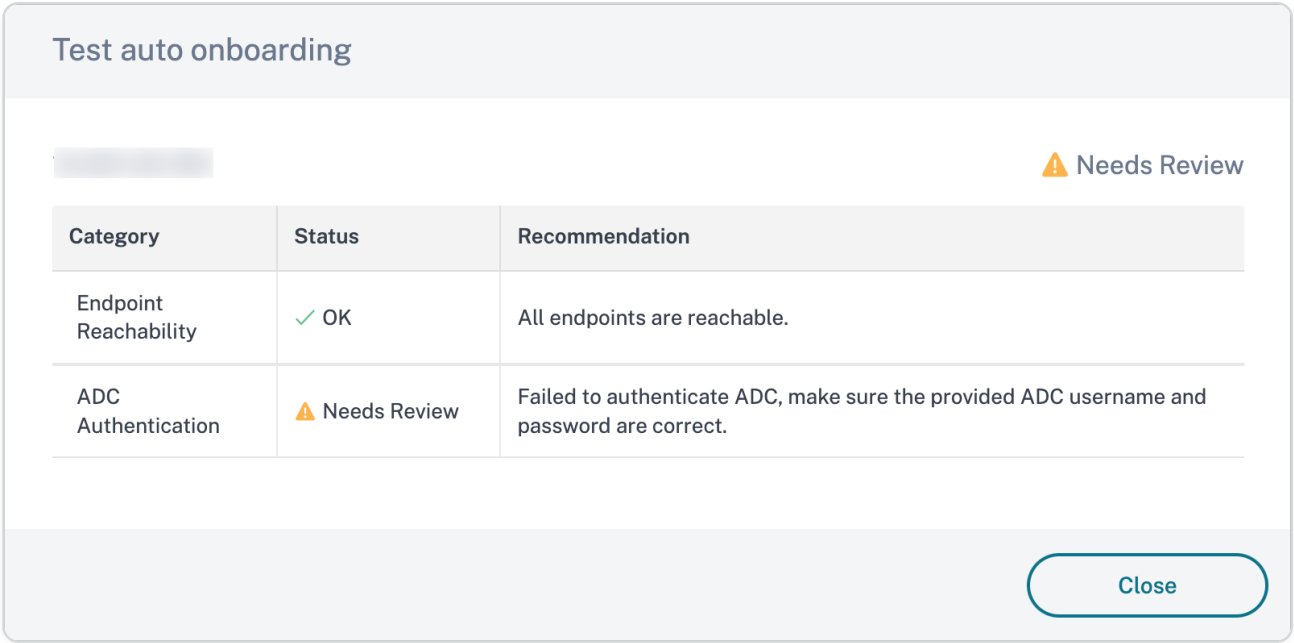
Test onboarding readiness of NetScaler instances

When you want to onboard a NetScaler instance to NetScaler Console, you can test whether the instances are ready for onboarding. The test run status suggests you if the instances are ready or needs review.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Click **Test** to start the diagnostic dry run. The **Test auto onboarding** page displays the issue category, status, and recommendation.



For more information, see View NetScaler diagnostic information in NetScaler Console GUI.

If the NetScaler test run status is in **Needs Review** status, then:

- Review the NetScaler Login credentials in the Device Profile.
- The following endpoints are unreachable:
  - `adm.cloud.com`
  - `agent.adm.cloud.com`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `trust.citrixnetworkapi.net`
- `download.citrixnetworkapi.net`

If you face any issues when you run the test for onboarding readiness, see Troubleshoot for recommendations.

Email Settings

NetScaler Console service allows onboarding of NetScaler instances using the Advisory Concole Connect based low-touch onboarding workflow. As a part of this workflow, customers receive product initiated emails from NetScaler Console service. You can enable or disable the email notifications that you receive as part of the Advisory Console Connect based low-touch onboarding workflow. You can configure and manage the email notifications in the following ways:

- **Enable emails for all admins** - You will be able to enable the emails for all admins in your org. By default, the emails are enabled for all the admins in the Org.
- **Enable / disable emails for selected admins** - You can customize the email settings so that only specific admins in the org receive emails and the other admins do not.
- **Disable emails for all admin**s - You will be able to disable and stop the emails for all admins in your org.

Configure Email Settings

You can configure the Email Settings and enable or disable the emails that you receive as part of the Console Advisory Connect based low-touch onboarding workflow. To configure the **Email Settings**:

1. Click **Onboard to ADM Service** in the product initiated email. The **Citrix Cloud™** page appears.
2. In the **Citrix Cloud** login page:
   - If you are an existing Citrix Cloud customer, sign in to Citrix Cloud using your credentials of Citrix.com, My Citrix, or Citrix Cloud.
   - If you are not an existing Citrix Cloud customer, sign up to Citrix cloud. For more info, see Sign up for Citrix Cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If you are part of multiple Org IDs and one of the Org IDs is in Citrix Cloud, sign in using your existing credentials.

The NetScaler Console landing page appears, providing you with an overview of NetScaler Console and its benefits.

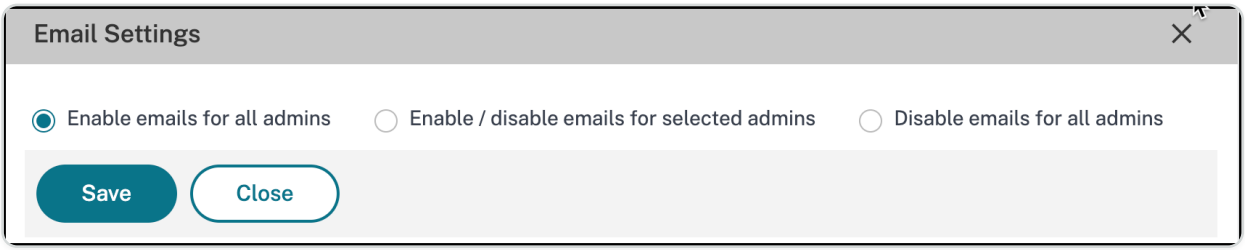
3. In the NetScaler Console landing page, click **Next**.

   The **Insights on your NetScaler and Gateway instances** page appears, where you can get insights into your overall NetScaler infrastructure with recommendations.

4. In the **Insights on your NetScaler and Gateway instances** page, click **Next**.

   The **Select NetScaler and Gateway instances to onboard** page appears, where you can see a list of NetScaler instances to onboard and additional options such as **Email Settings**.

5. Click **Email Settings**. The **Email Settings** pane appears.



You can now configure the email settings to enable or disable emails.

NOTE:

If you have onboarded only one NetScaler instance, then you will not receive these emails.

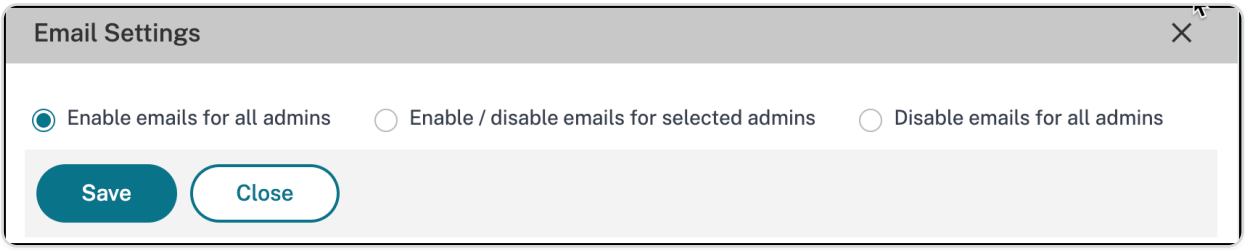
If you are already on the NetScaler Console GUI and you want to configure the email settings:

1. In NetScaler Console GUI, navigate to **Infrastructure > Instances**, and then click **NetScaler**. The **NetScaler** page appears.
2. In the **NetScaler** page, click **Asset Inventory**.

   The **Select NetScaler and Gateway instances to onboard** page appears to show the list of NetScaler instances that are onboarded and additional options such as **Email Settings**.

3. Click **Email Settings**. The **Email Settings** pane appears.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



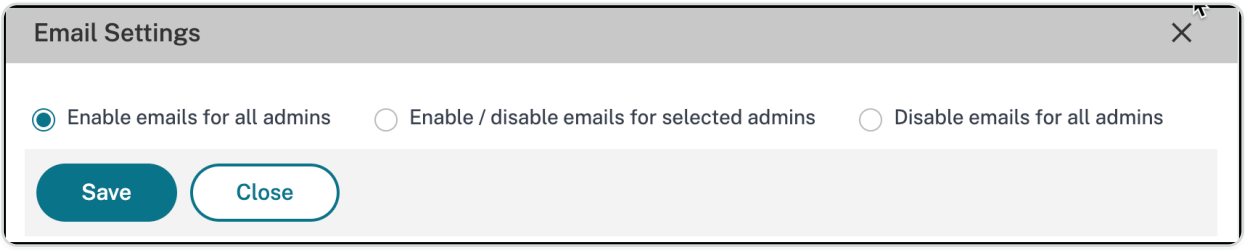
You can now configure the email settings to enable or disable emails.

Enable emails for all admins

By default, the emails are enabled for all the admins in the Org.

To enable or subscribe to the email notifications as part of the Console Advisory Connect based workflow:

1. In the **Email Settings** pane, select **Enable emails** for all admins.



2. Click **Save** and **Close**.

   All the admins in the org are now subscribed and will receive email notifications as part of the Console Advisory Connect based workflow.

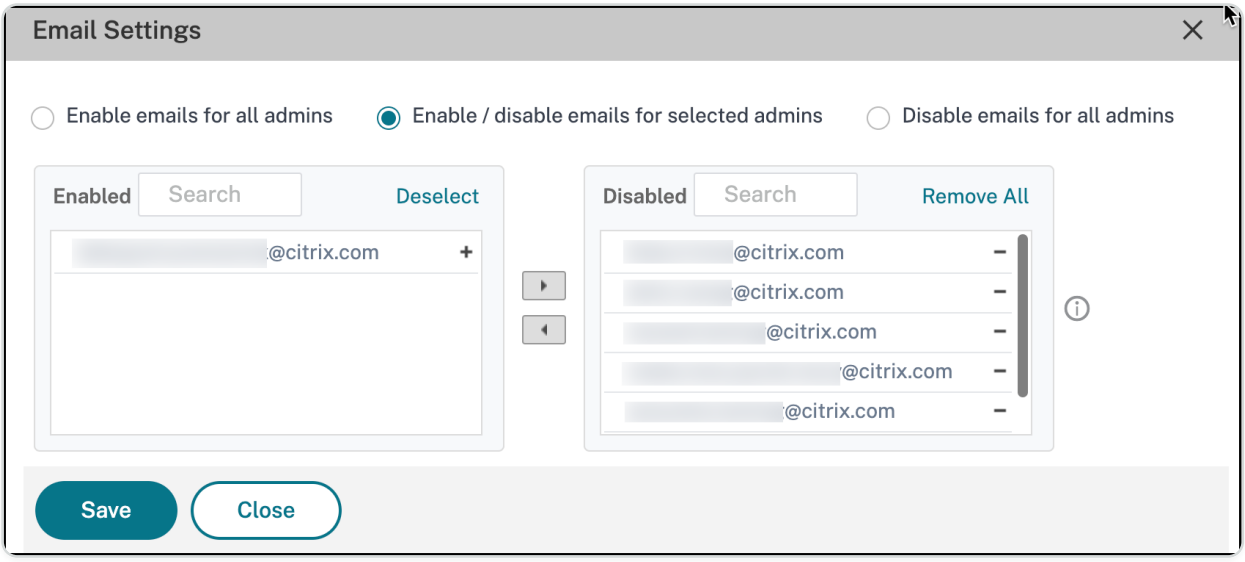
Enable / disable emails for specific admins in the org

You can customize the email settings so that only specific admins in the org receive emails. You will see the list of admins who have the emails enabled on the left and the list of admins who have the emails disabled on the right.

To disable emails for specific admins in the org:

1. Locate the admin email address in the **Enabled** list.
2. Click the add button (**+**).

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You will see the admin email address added to the **Disabled** list.

3. Click **Save** and **Close**.

   The admin is now unsubscribed to not receive email notifications as part of the Console Advisory Connect based workflow.

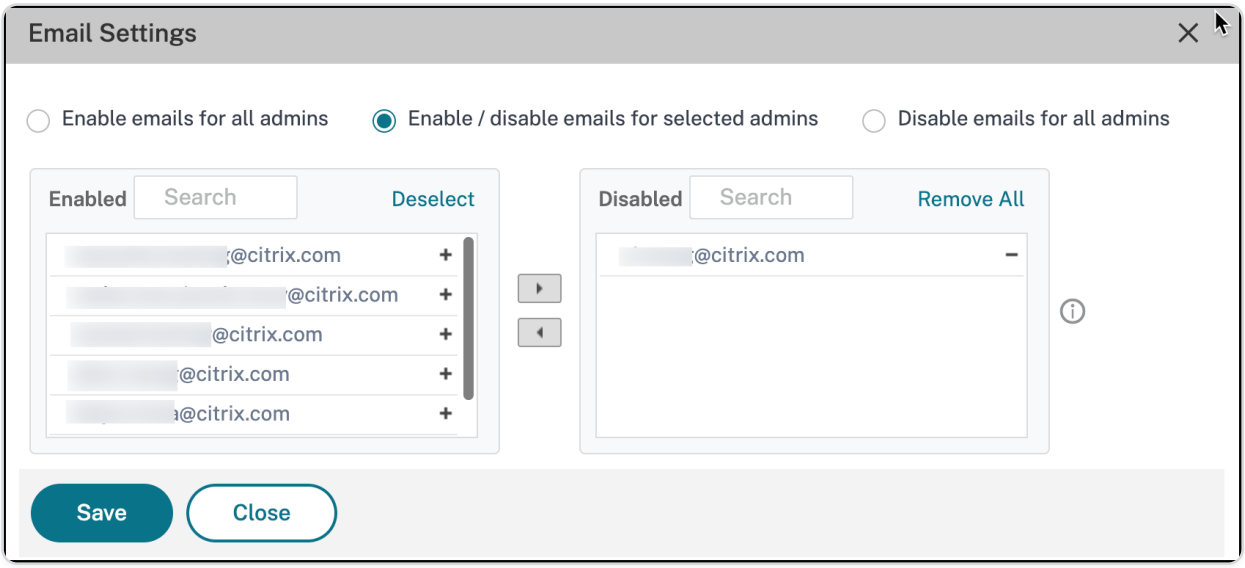
   NOTE:

   If you want to disable emails for multiple admins, select all their email IDs in the **Enabled** email list, and click the add button (**+**) to add the email IDs to the **Disabled** list. Click **Save** and **Close**.

If you have previously disabled emails for specific or all admins in your org, you will be able to enable emails for all the admins. To enable emails for specific admins in the org:

1. Locate the admin email address in the **Disabled** list.
2. Click the remove button (-). You will see the admin email address removed from the **Disabled** list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Click **Save** and **Close**.

   The admin will now start receiving onboarding related emails. The admin is now subscribed to receive email notifications.

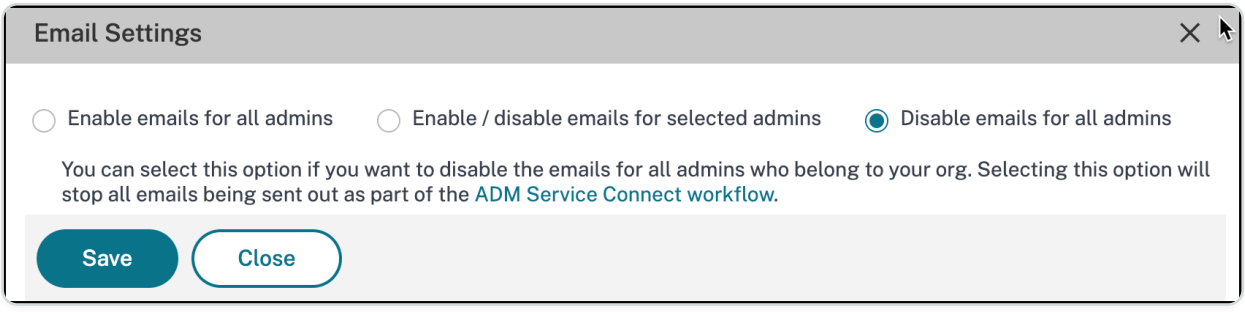
> **NOTE:**
>
> If you want to enable emails for multiple admins, select all their email IDs in the **Disabled** email list, and click the remove button (**-**) to add the email IDs to the **Enabled** list. Click **Save** and **Close**.

Disable emails for all admins

You can select this option if you want to disable or stop the emails for all admins who belong to your org.

To disable or unsubscribe from receiving emails:

1. In the **Email Settings** pane, select **Disable emails for all admins**.



2. Click **Save** and **Close**.

   All the admins in the org are now unsubscribed and will not receive any email notifications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshoot issues using the diagnostic tool or the NetScaler Console GUI

Note

> The diagnostic tool is applicable only for the NetScaler instances onboarded or to be onboarded using the Console Advisory Connect based low-touch onboarding.

For more information, see Low-touch onboarding of NetScaler instances using NetScaler Console connect.

When you onboard a NetScaler instance onto NetScaler Console, you might experience a few issues that prevent the NetScaler instance from successfully onboarding. As an administrator, you must know the reason for the onboarding failure. You can perform diagnostic checks using the diagnostic tool when you:

- Experience any issues during auto-onboarding or script-based onboarding
- Want to ensure if the NetScaler instance is ready to onboard
- Want to analyze issues for the already onboarded NetScaler instances that show "Down" status in the NetScaler Console GUI

If Console Advisory Connect is enabled on the NetScaler instance, the diagnostic details are automatically sent to Citrix and you can view details in the NetScaler Console GUI. If Console Advisory Connect is not enabled, you can manually use the diagnostic tool.

Manually use the diagnostic tool

The diagnostic tool is available as part of the `mastools` upgrade (13.1-2.x or later) and accessible at `/var/mastools/scripts`. You can verify the `mastools` version by running the `cat /var/mastools/version.txt` command in the NetScaler instance.

To run the diagnostic tool:

1. Using an SSH client, log on to the NetScaler instance.
2. Type shell and press Enter to switch to bash mode.
3. Type `cd /var/mastools/scripts`.
4. Type `sh mastools_diag`.

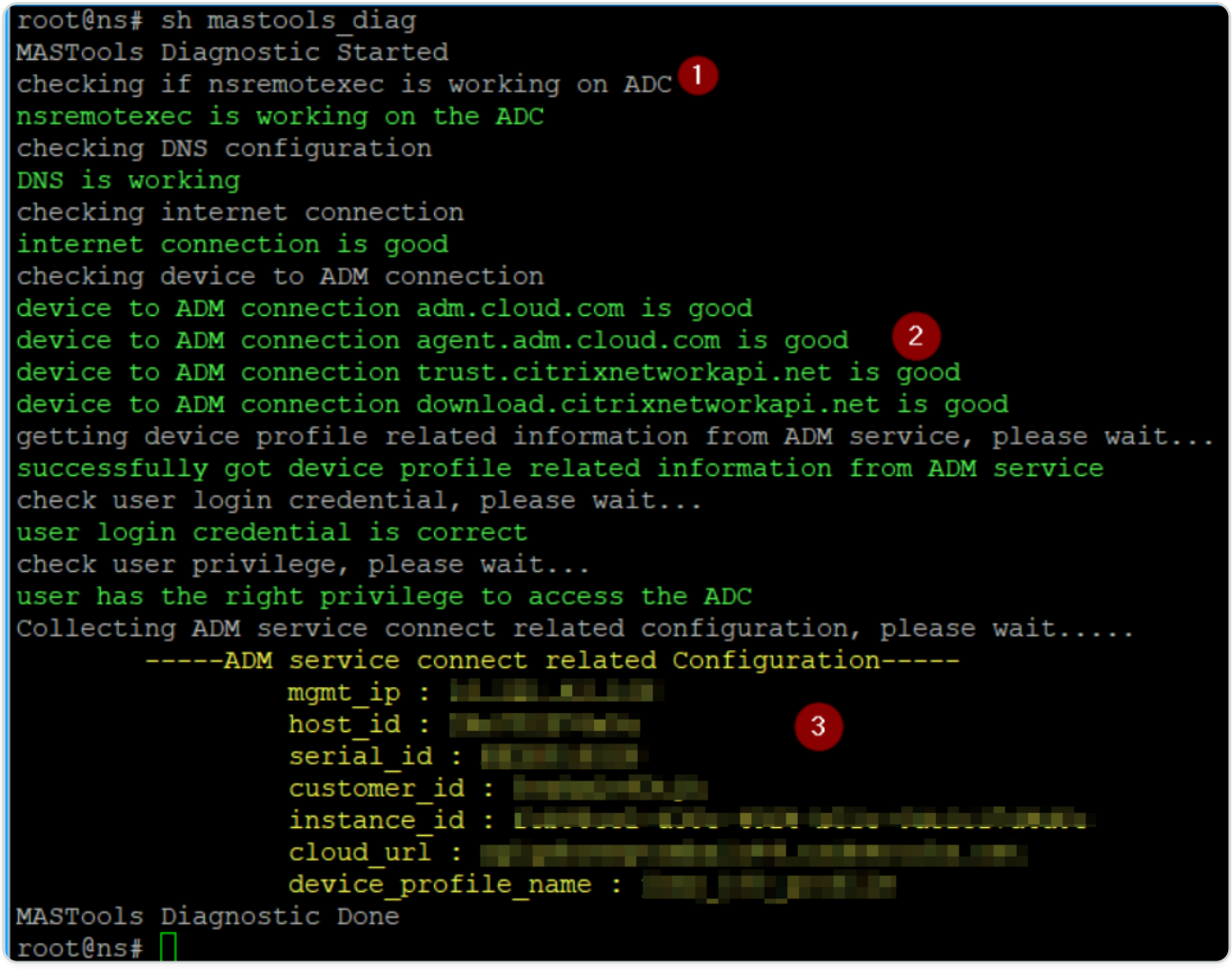
The tool starts and displays the results for the following diagnostic checks:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **nscli**
- **DNS configuration**
- **Internet connection**
- **Instance to ADM connection**
- **User privilege**

If the issues still persist even after troubleshooting, you can contact support. When you contact support, you must provide the configuration information that is displayed after you run the diagnostic tool.

The following is an example of diagnostic results for an NetScaler instance that has no issues:

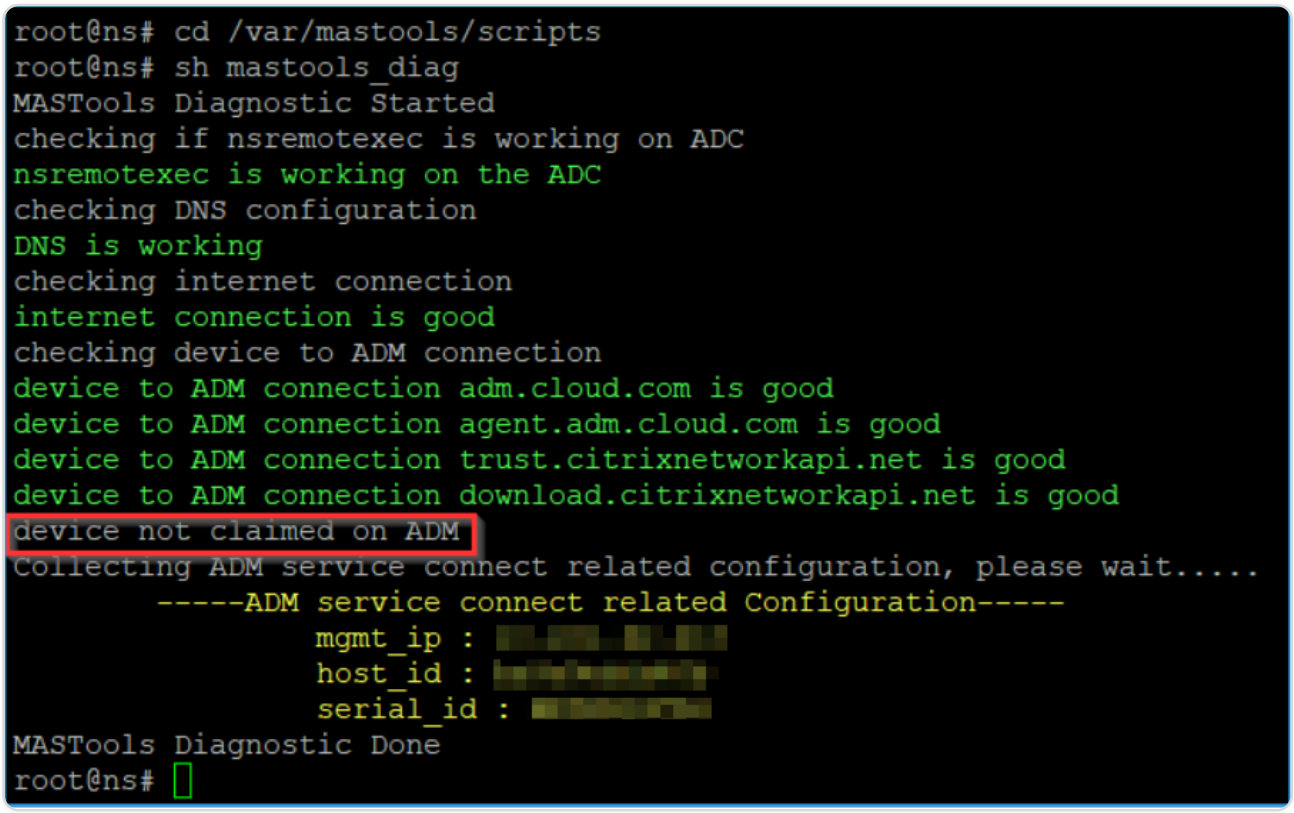


- **1** – Displays the type of diagnostic check
- **2** – Displays the diagnostic check results either in green or in red. Green indicates the result is successful and red indicates the result is not successful.
- **3** – Displays the NetScaler Console configuration information in yellow each time you run the diagnostic tool. If you want to contact NetScaler support, you must provide this information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Validate the NetScaler instance readiness for onboarding using the diagnostic tool

Before you onboard the NetScaler instance to NetScaler Console, you can check the readiness of the NetScaler instance, by running the diagnostic tool on the NetScaler instance. If the NetScaler instance has no issues and ready to onboard, the tool displays the **device not claimed on ADM** message.



View NetScaler diagnostic information in NetScaler Console GUI

Navigate to **Infrastructure > Instances > NetScaler** and click **Asset Inventory** to see the newly added **Onboarding Readiness** option that provides the NetScaler instance onboarding readiness status such as **Needs Review** or **OK**.

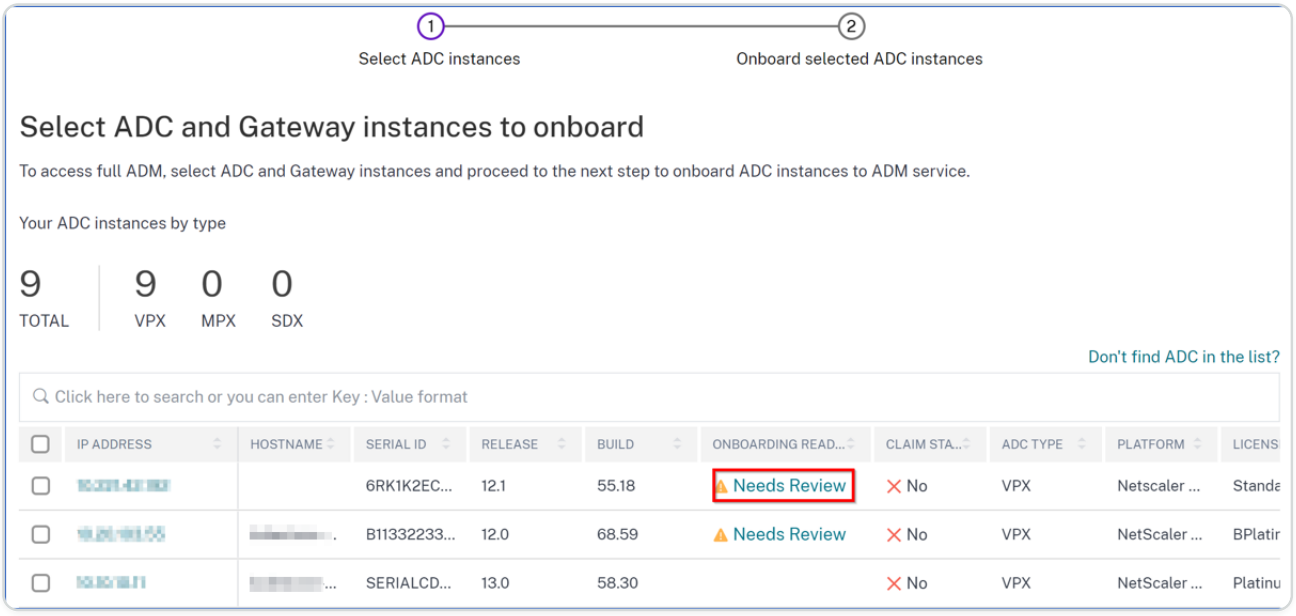
- **Needs Review**. The NetScaler instance has issues that need to be fixed.
- **OK**. The NetScaler instance is ready to onboard.

NOTE:

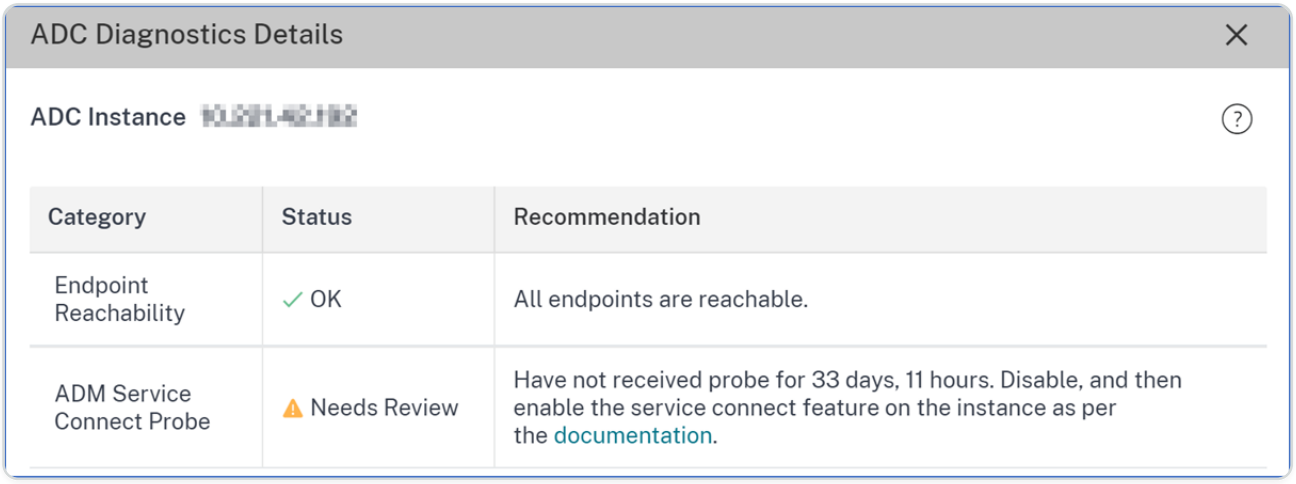
If the **Onboarding Readiness** appears blank, it means the NetScaler instance is not running with the latest image that has diagnostic support.

If the NetScaler instance has any issues, the **Needs Review** option appears, and you can click to view more details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



After you click **Needs Review**, the **NetScaler Diagnostics Details** page displays the issue details.



- **Category**. Provides the issue category.
- **Status**. Provides the issue status such as **Needs Review**, **OK**, or **Not Applicable**.
- **Recommendation**. Provides the required recommendation to troubleshoot the issue.

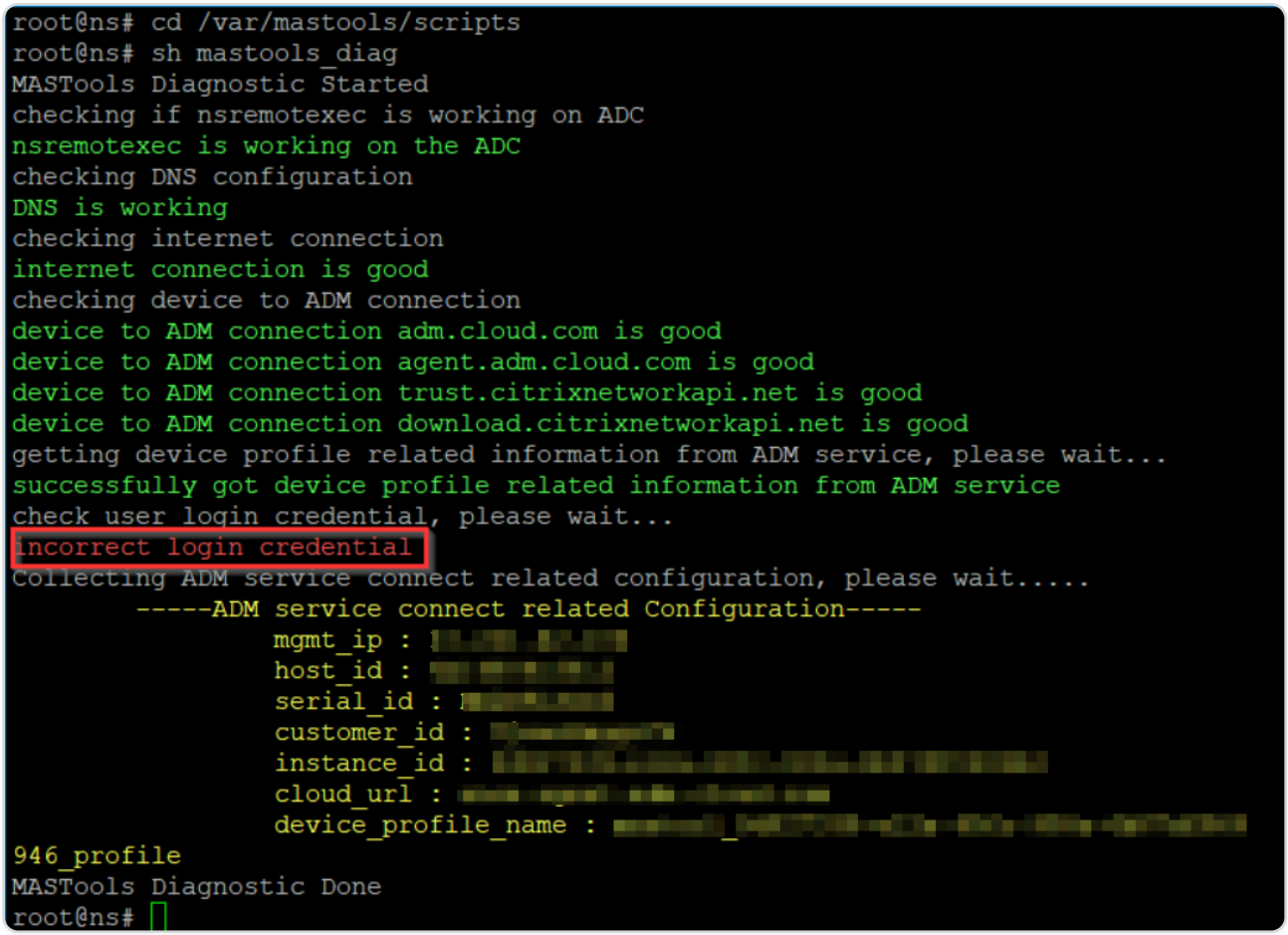
After you fix the issue, the status in the Onboarding Readiness gets changed to **OK**.

Troubleshoot

The following are some of the NetScaler instance issues and their troubleshooting steps:

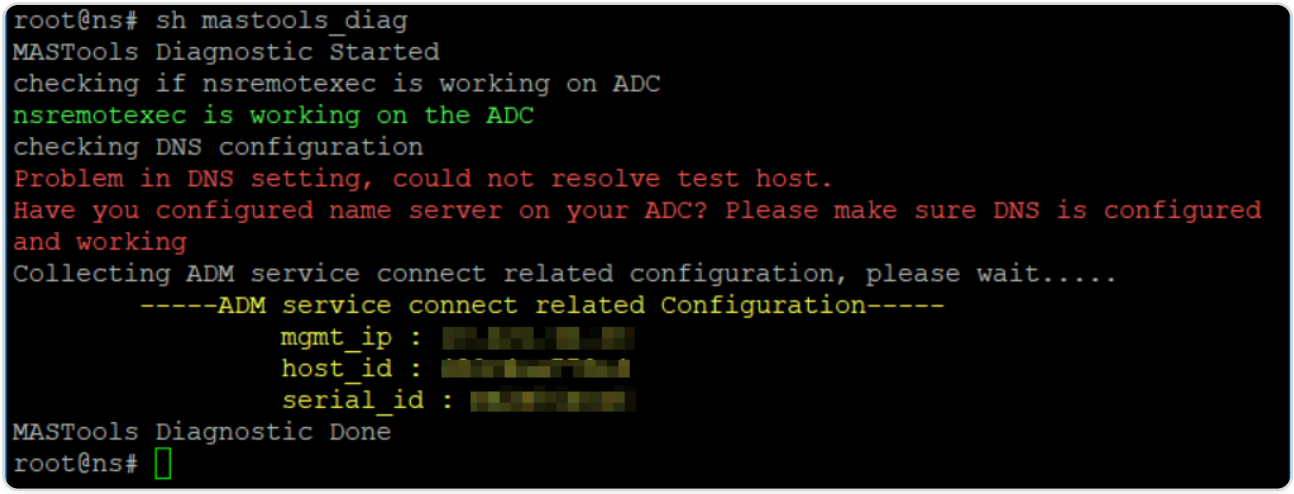
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Invalid user name or password



Workaround: Ensure the user name and password provided in the Admin profile are correct. If you have modified the NetScaler instance password, you must modify the admin profiles of the instances. For more information, see Modify the admin profile.

DNS configuration error



Workaround: Ensure the DNS is configured or the DNS IP address is valid. For more information, see DNS configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

No internet connection

Workaround: Ensure that the firewall setting is not blocking the internet access and the required proxy is configured.

No connection to NetScaler Console endpoint

Workaround: Ensure to check firewall settings and the following NetScaler Console endpoints are not blocked in the firewall:

```
ADM_GRP_EP = "adm.cloud.com"



ADM_AGENT_EP = "agent.adm.cloud.com"



ADM_TRUST_EP = "trust.citrixnetworkapi.net"



ADM_DOWNLOAD_EP = "download.citrixnetworkapi.net"
```

If no issue found in the diagnostic checks and the no connection issue still persists, make a note of the NetScaler Console configuration information (available in yellow) and contact NetScaler support.

When you perform a test run to ensure that the NetScaler instance is ready to onboard, the following issues maybe seen:

Built-in agent dry run timeout

If the results of the dry run are not fetched within 5 minutes, a Timeout message appears.

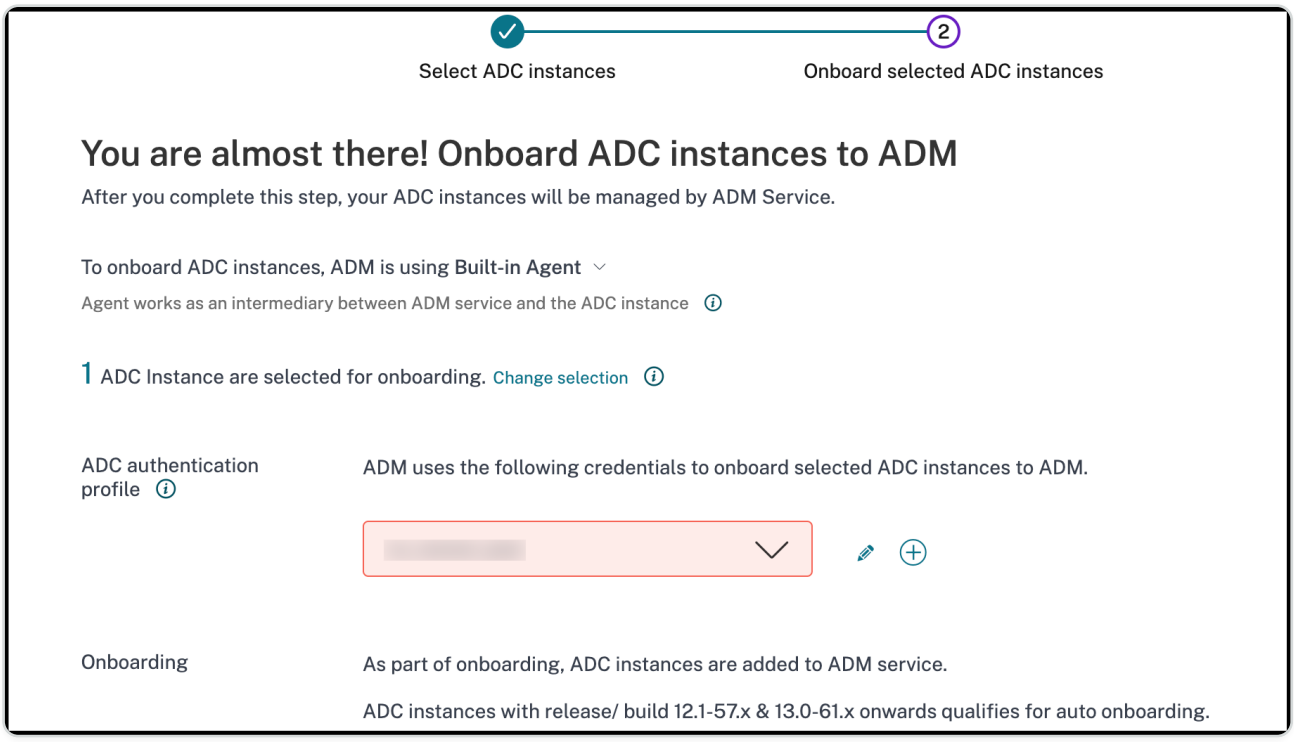
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Recommendation: It is recommended that you verify whether the NetScaler instance is running with the latest image that has diagnostic support. Also, in the Asset Selection table, the Onboarding Readiness column appears blank.

Red outline on the device profile dropdown

NetScaler authentication fails during the dry run and a red outline appears on the device profile dropdown.



Recommendation: Re-enter the NetScaler user admin credentials again, create the device profile and click Test to run the dry run again.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Transition from a built-in agent to an external agent

You might have started with using NetScaler Console for management and monitoring only, and later you might want to use other features such as pooled licensing and analytics. For that, you must transition from the built-in agent to an external agent.

The built-in agent supports only management and monitoring features. For other NetScaler Console features such as pooled licensing and analytics, you need an external agent. This document covers the steps for transitioning from an existing NetScaler Console built-in agent to an external hypervisor-based agent.

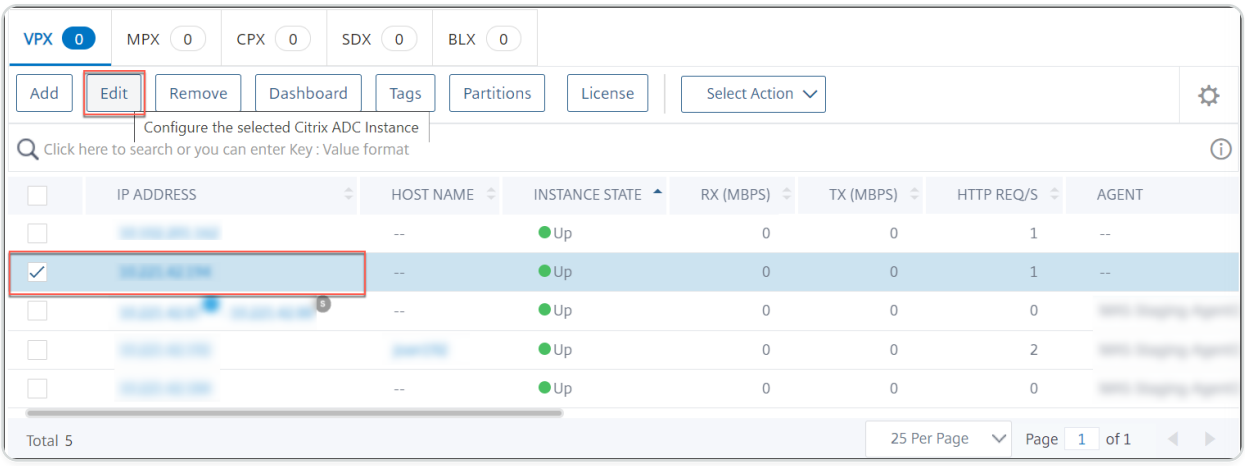
Before you start

Install an external agent before you start transitioning. Follow the procedure given in the topic Install a NetScaler agent on-premises.

Transition from a built-in agent to an external agent

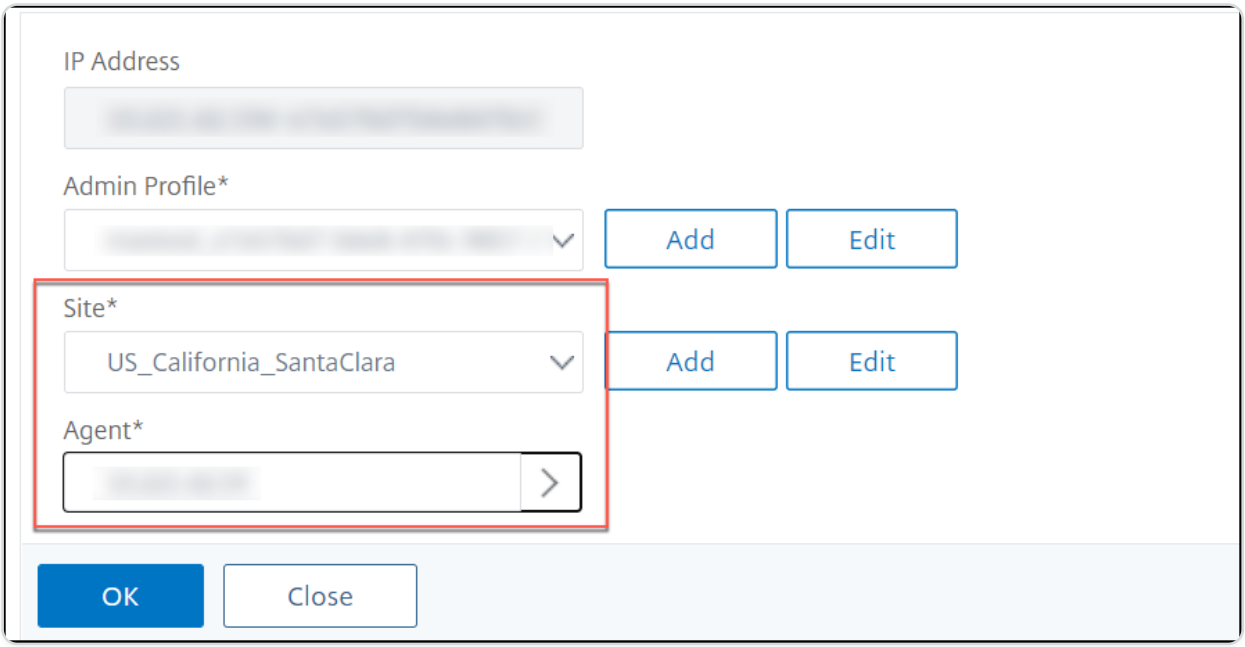
Follow these steps to transition from a built-in agent to an external agent:

1. In the NetScaler Console GUI, under **Infrastructure > Instances Dashboard > NetScaler**, select the NetScaler instance and click **Edit**.



2. Select the site and agent and click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Select the instance again and click **Select Action > Rediscover**.

For information on how to create a site in NetScaler Console and add the agent to the site, see Add Instances

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Connect SAML as an identity provider to NetScaler Console

NetScaler Console supports using SAML (Security Assertion Markup Language) as an identity provider to authenticate administrators and subscribers signing in to their NetScaler Console. You can use the SAML 2.0 provider of your choice with your on-premises Active Directory (AD).

For most SAML providers, use the information in this article to set up SAML authentication. If you want to use SAML authentication with your Azure AD, you have the option to use the Citrix Cloud™ SAML SSO app from the Azure AD app gallery.

Prerequisites

The SAML authentication with NetScaler Console has the following requirements:

- SAML provider that supports SAML 2.0
- On-premises AD domain
- Two Cloud Connectors deployed to a resource location and joined to your on-premises AD domain. The Cloud Connectors are used to ensure Citrix Cloud can communicate with your resource location.
- AD integration with your SAML provider.

Cloud Connectors

You must have at least two (2) servers on which to install the Citrix Cloud Connector™ software. It is recommended to have at least two servers for Cloud Connector high availability. These servers must meet the following requirements:

- Meets the system requirements described in Cloud Connector Technical Details.
- Does not have any other Citrix components installed, is not an AD domain controller, and is not a machine critical to your resource location infrastructure.
- Joined to the domain where your resources reside. If users access resources in multiple domains, you must install at least two Cloud Connectors in each domain.
- Connected to a network that can contact the resources that subscribers access through Citrix Workspace.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Connected to the internet.

Active Directory

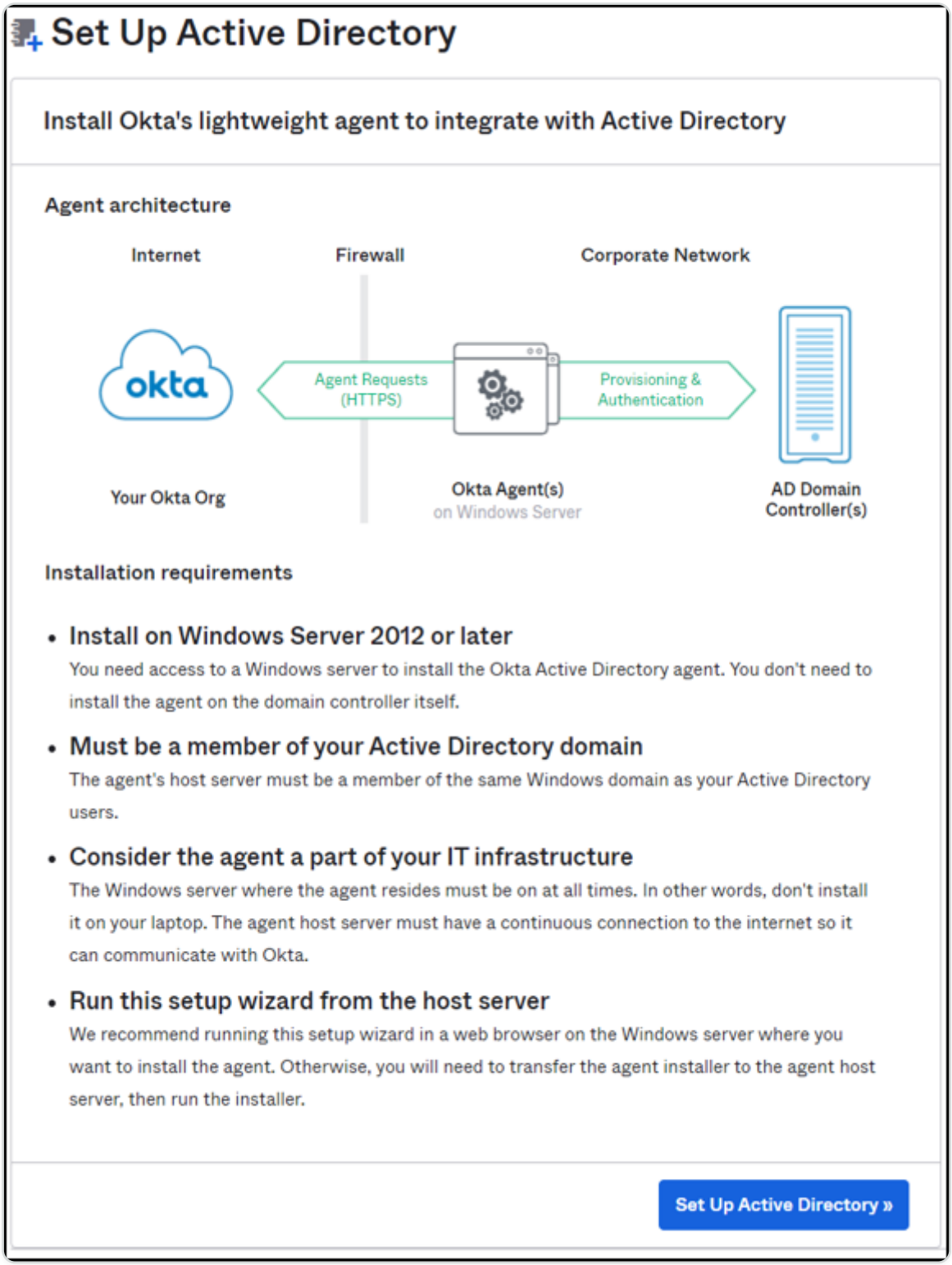
Before configuring SAML authentication, perform the following tasks:

- The First Name, Last Name, and Email fields are mandatory for the users in Active Directory to import users to Okta Instance.
- Verify that your workspace subscribers have user accounts in Active Directory (AD). Subscribers without AD accounts can’t sign in to their workspaces successfully when SAML authentication is configured.
- Ensure that the user properties in your subscribers’ AD accounts are populated. Citrix Cloud requires these properties to establish the user context when subscribers sign in to Citrix Workspace. If these properties aren’t populated, subscribers can’t sign in. These properties include:
  - Email address
  - Display name (optional)
  - Common name
  - SAM account name
  - User Principal Name
  - Object GUID
  - SID
- Connect your Active Directory (AD) to your Citrix Cloud account by deploying Cloud Connectors in your on-premises AD.
- Synchronize your AD users to the SAML provider. Citrix Cloud requires the AD user attributes for your workspace subscribers so they can sign in successfully.

SAML SSO configuration

In an Okta instance, navigate to **Directory integrations > Add Active Directory**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

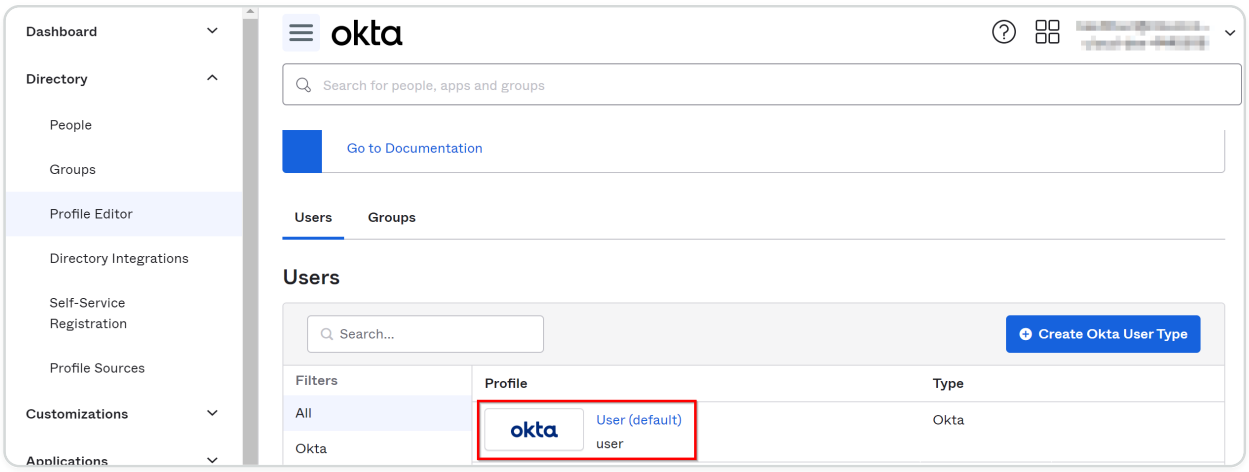


For a successful integration, the SAML identity provider must pass Citrix Cloud certain Active Directory attributes of the user in the SAML assertion. Specifically,

- Security Identifier (SID)
- objectGUID (OID)
- user Principal Name (UPN)
- Mail (Email)

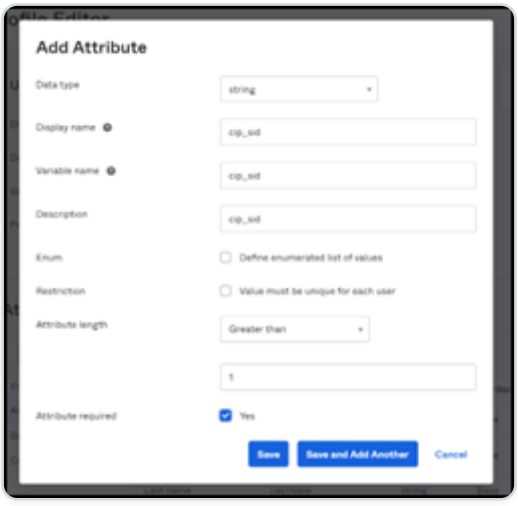
© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Log on to Okta with administrator credentials.
2. Select **Directory > Profile Editor** and select the **Okta User (default)** profile. Okta displays the User profile page.



3. Under **Attributes**, select **Add Attributes** and add the custom fields.

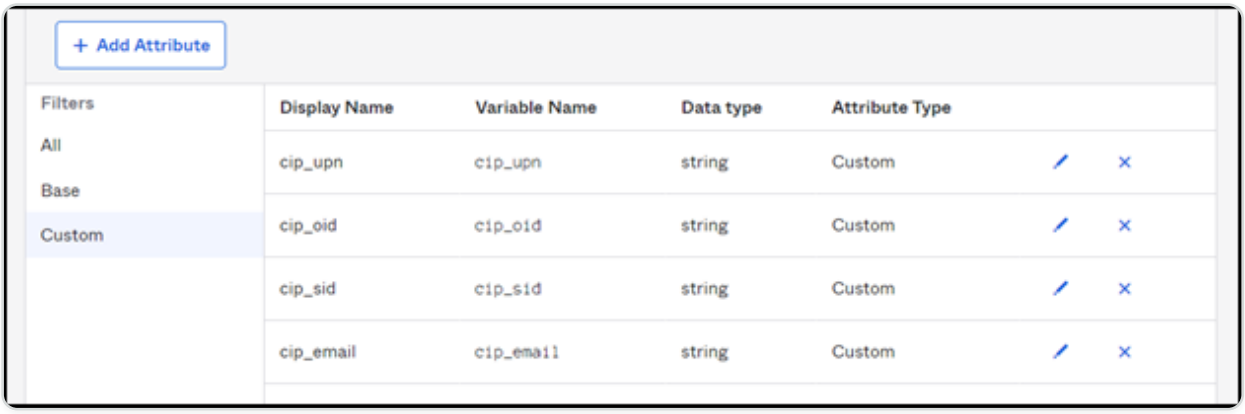
   - `cip_sid`
   - `cip_upn`
   - `cip_oid`
   - `cip_email`



   Click **Save and Add Another** and repeat the process to create 4 custom attributes.

   You can view the following details after creating 4 custom attributes:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

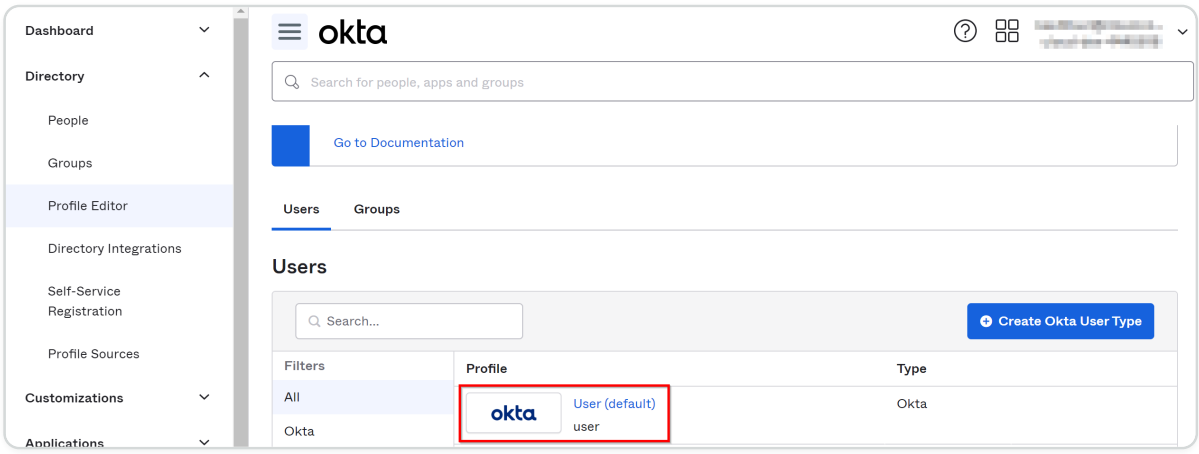


4. Map Active Directory Attributes to the Custom Attributes. Select the Active Directory you are using under **Users > Directories**.
5. Edit the attribute mappings:

    a. From the Okta console, navigate to **Directory > Profile Editor**.

    b. Locate the `active_directory` profile for your AD. This profile might be labeled using the format myDomain User, where myDomain is the name of your integrated AD domain.

    c. Select **Mappings**. The **User Profile Mappings** page for your AD domain appears and the tab for mapping your AD to Okta User is selected.



    d. In the **Okta User User Profile** column, map the Active Directory attributes to the custom attributes you have created:

        i. For `cip_email`, select email from the User Profile column for your domain. When selected, the mapping appears as `appuser.email`.

        ii. For `cip_sid`, select **objectSid** from the User Profile column for your domain. When selected, the mapping appears as `appuser.objectSid`.

        iii. For `cip_upn`, select `userName` from the **User Profile** column for your domain. When selected, the mapping appears as `appuser.userName`.

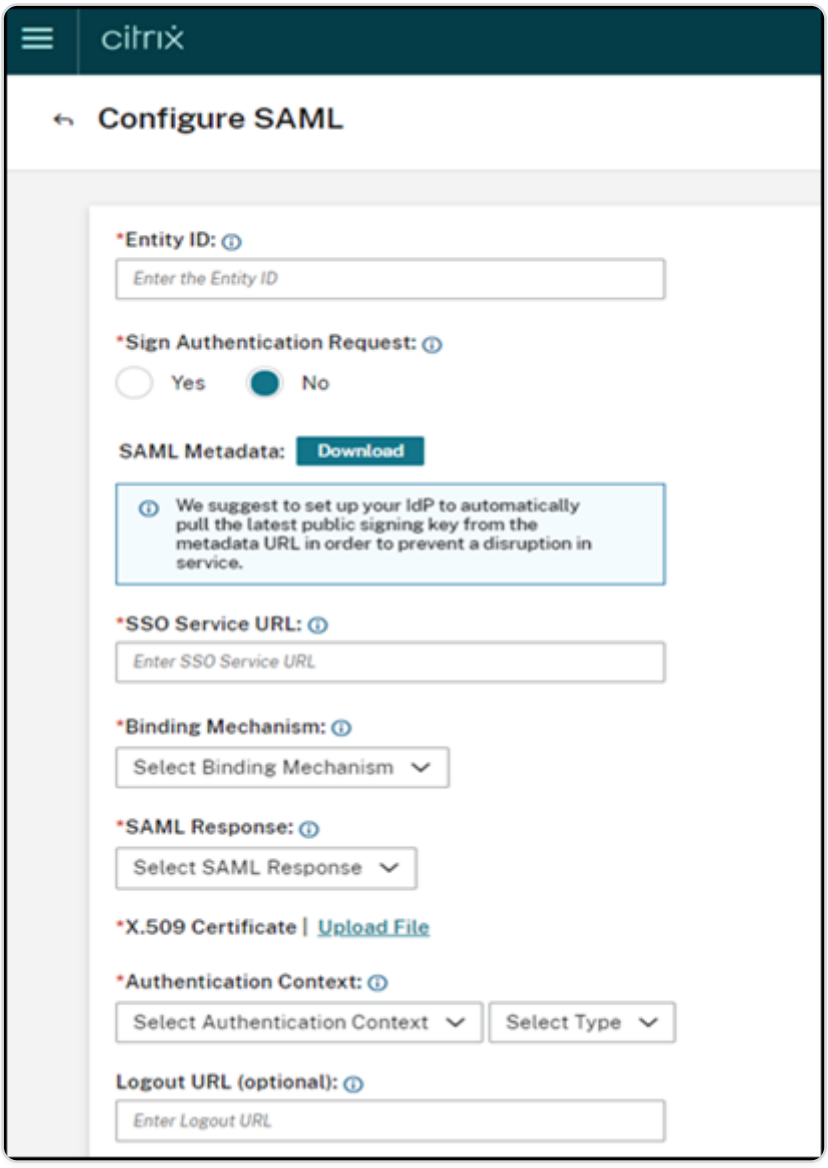
© 1997–2026 Citrix Systems, Inc. All rights reserved.

iv. For `cip_oid`, select `externalId` from the **User Profile** column for your domain. When selected, the mapping appears as `appuser.externalId`.



6. Sign in to Citrix Cloud at `https://citrix.cloud.com`.
7. From the Citrix Cloud menu, select **Identity and Access Management**.
8. Locate **SAML 2.0** and click **Connect**.

   The **Configure SAML** page is displayed.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Download the `xml` file and open the file using any file editor. You must return to this page again after completing further configuration in Okta.

9. In Okta, navigate to **Application > Create App Integration**.
10. In the **Add Application** page, click **Create New App**.
11. In the **Create a New Application Integration** page, select **SAML 2.0** and click **Create**.
12. Provide details such as app name, app logo (optional), set the app visibility, and then click **Next**.
13. In the **Configuration SAML** tab, you must use the details from the downloaded `xml` file:

    a. Provide the URL details for **Single sign-on URL** as `https://saml-internal.cloud.com/saml/acs` and **Audience URI (SP Entity ID)** as `https://saml-internal.cloud.com`.

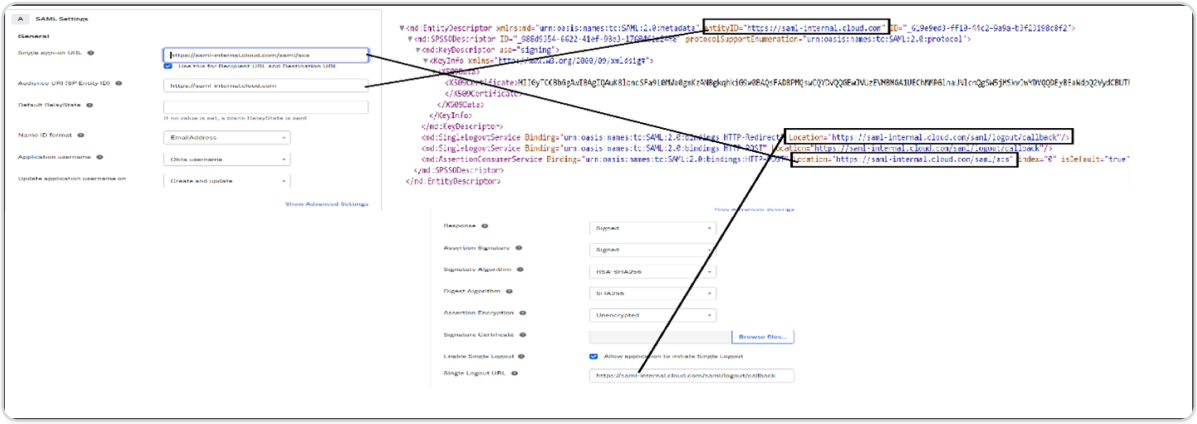
    NOTE:

    If external Citrix Cloud, then the URL must be `https://saml.cloud.com/saml/acs` and `https://saml.cloud.com` instead of `https://saml-internal.cloud.com` domain.

    b. Select **Unspecified** for **Name ID Format**.

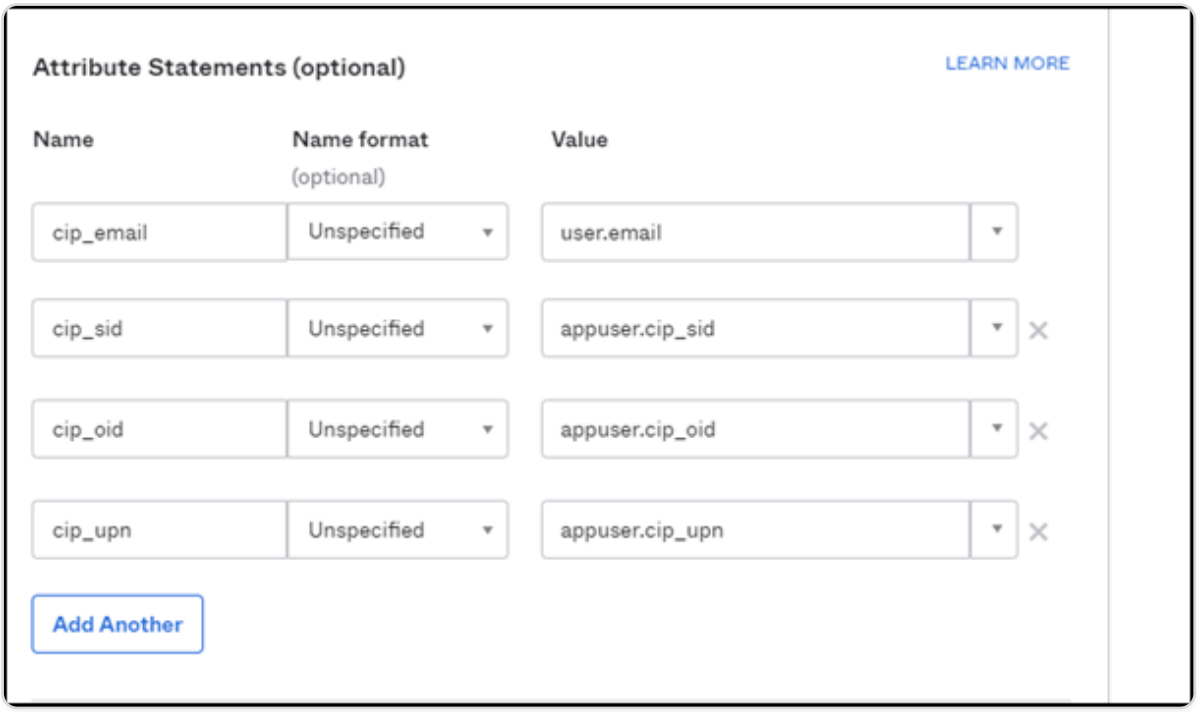
    c. Select **Okta Username** for **Application Username**.

    d. Click **Show Advanced Settings** and ensure that **Response** and **Assertion** are selected with **Signed**.



    e. Add **Attribute Statements** as shown in the following image.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

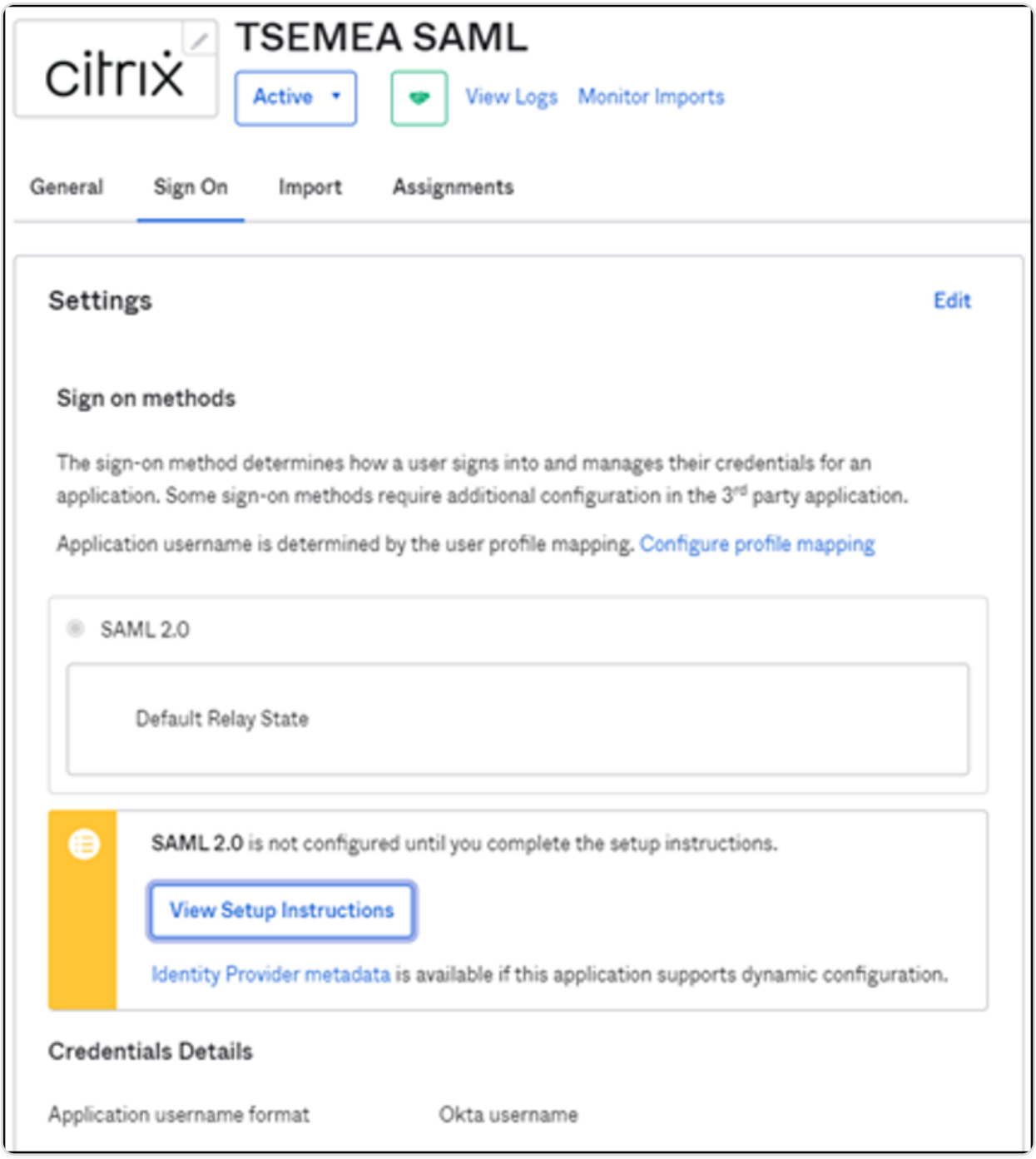


f. You can leave all other options by default and click **Next**.

g. Select **I'm an Okta customer adding an internal app** and then click **Finish**.

14. The Okta application is now created and click **View Setup Instructions**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

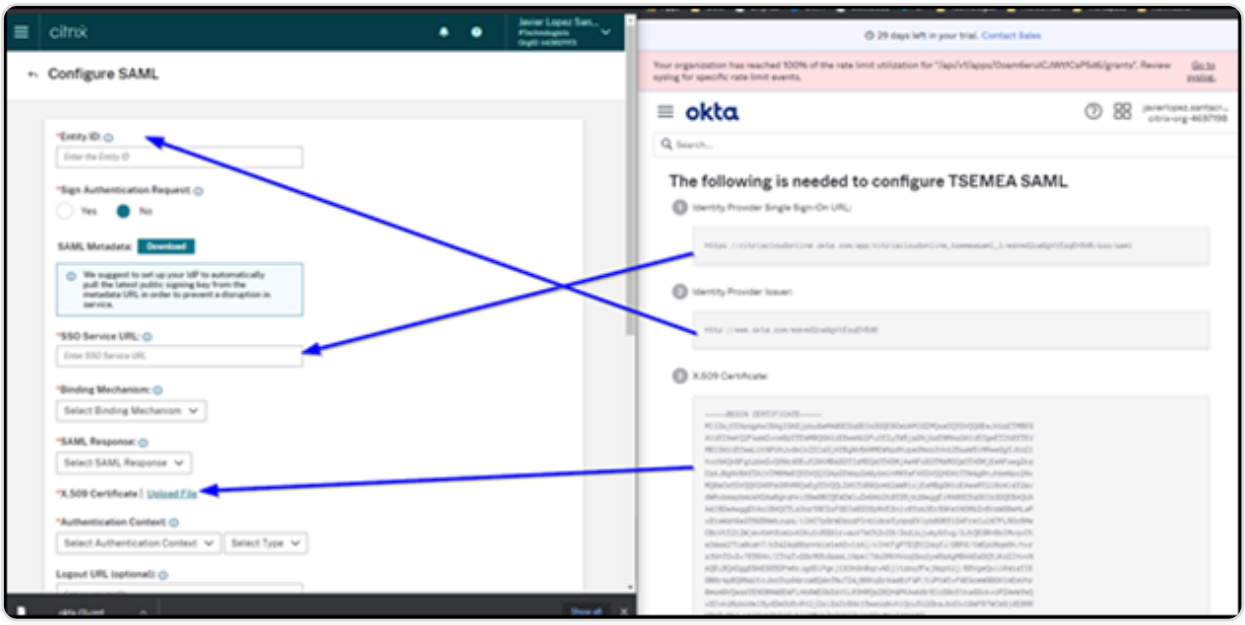


The **How to Configure SAML 2.0 for test Application** page is displayed with details that you must again add it in the Citrix Cloud.

Download the certificate to upload it in Citrix Cloud.

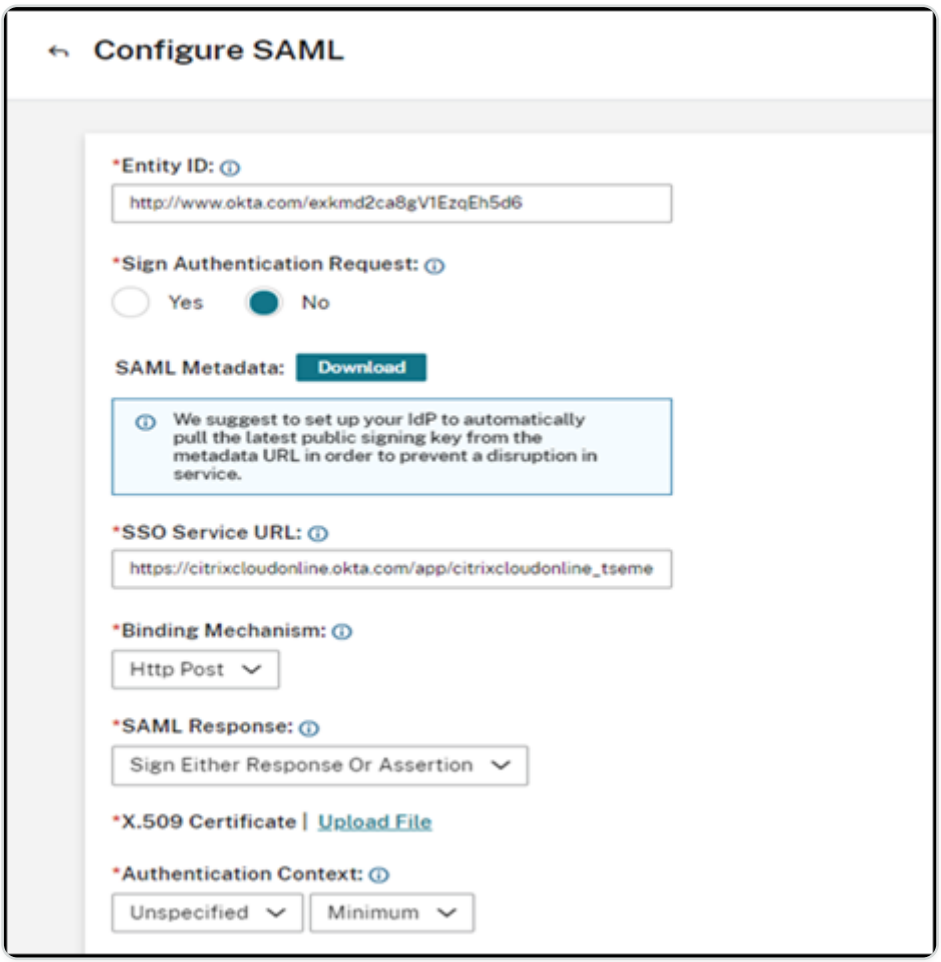
15. You must now return to the **Configure SAML** page in Citrix Cloud and complete the remaining configuration as mentioned in the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



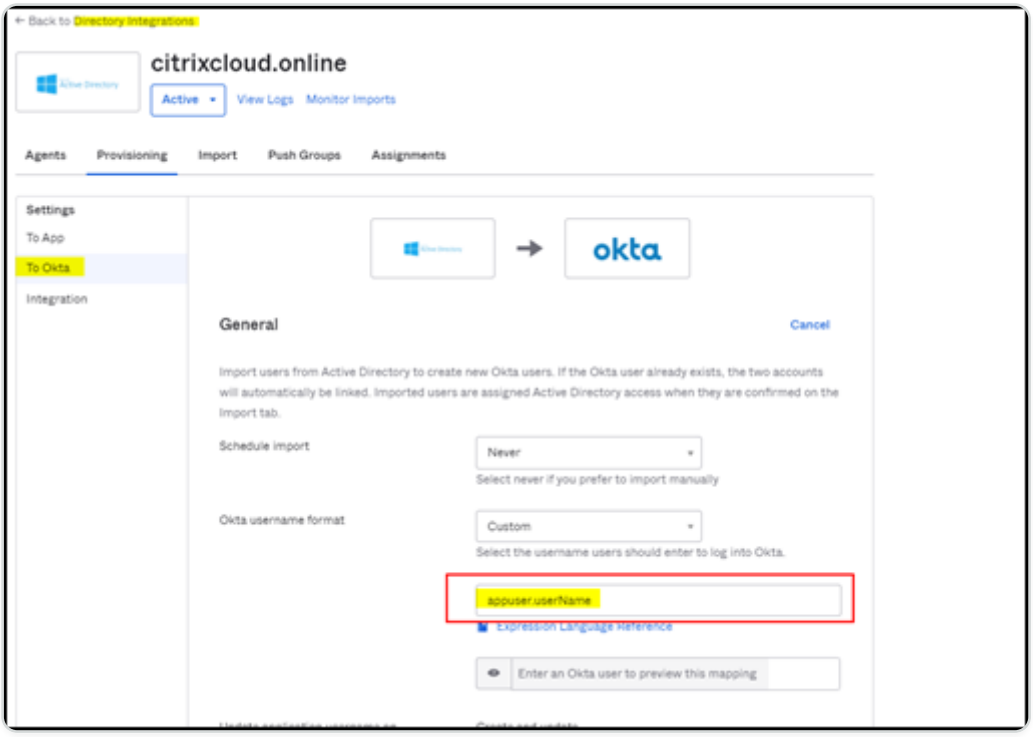
Use the downloaded certificate and rename the file name extension from `.cert` to `.crt` to upload it to Citrix Cloud.

16. After you upload the certificate, use all other options that are by default:



17. Next, you must ensure `appuser.userName` is defined at **Directory-integrations > Active Directory -> Provisiong > To okta**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE:

Sometimes, you must use `user.cip_upn`, instead `appuser.cip_upn`. Ensure to verify the definition of your application in the OKTA integration as shown in this image.

18. You must now try to add users in Okta to this SAML application. You can assign users through multiple ways.

    Method 1:

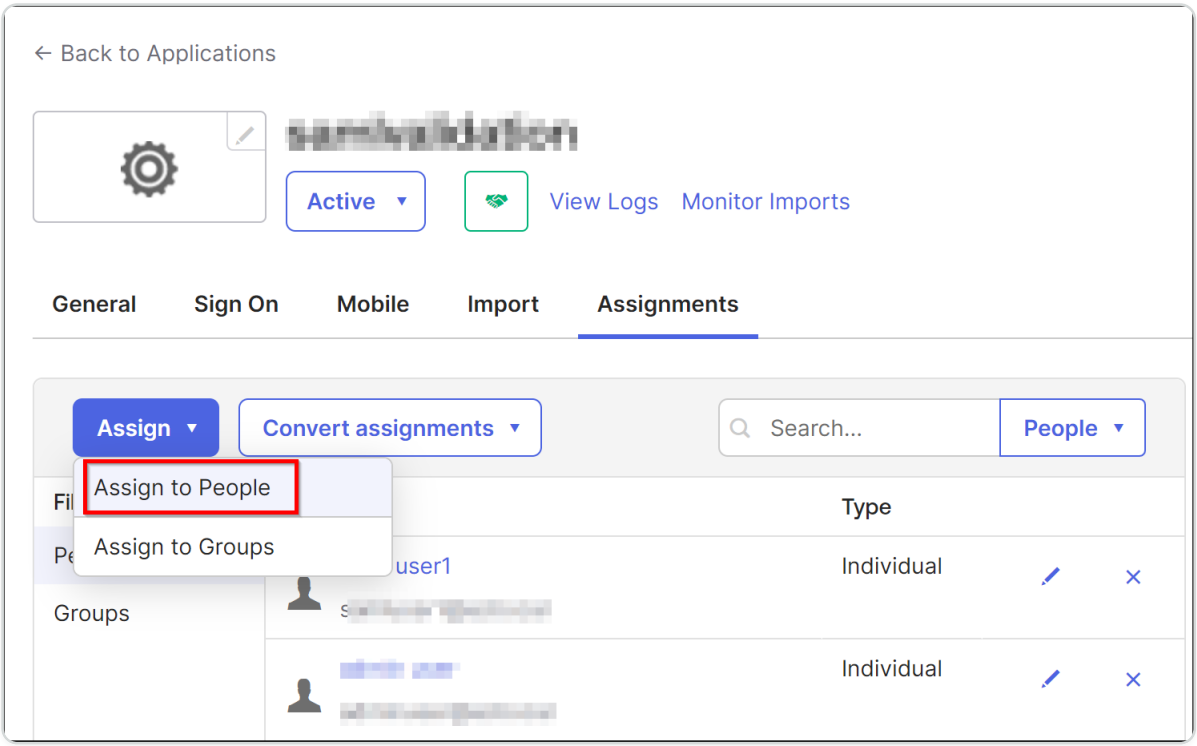
    a. Log on to Okta with administrator credentials

    b. Navigate to **Applications > Applications**

    c. Select the SAML application that you created

    d. Click **Assign > Assign to People**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



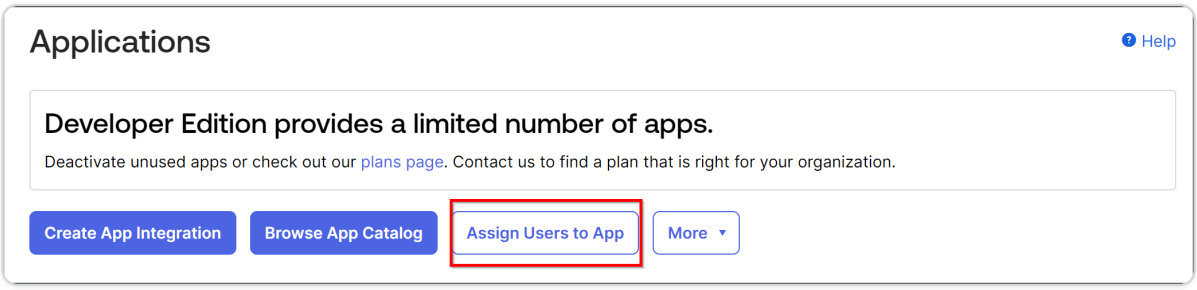
e. Click **Assign** and then select **Save and Go back**.

f. Click **Done**.

Method 2:

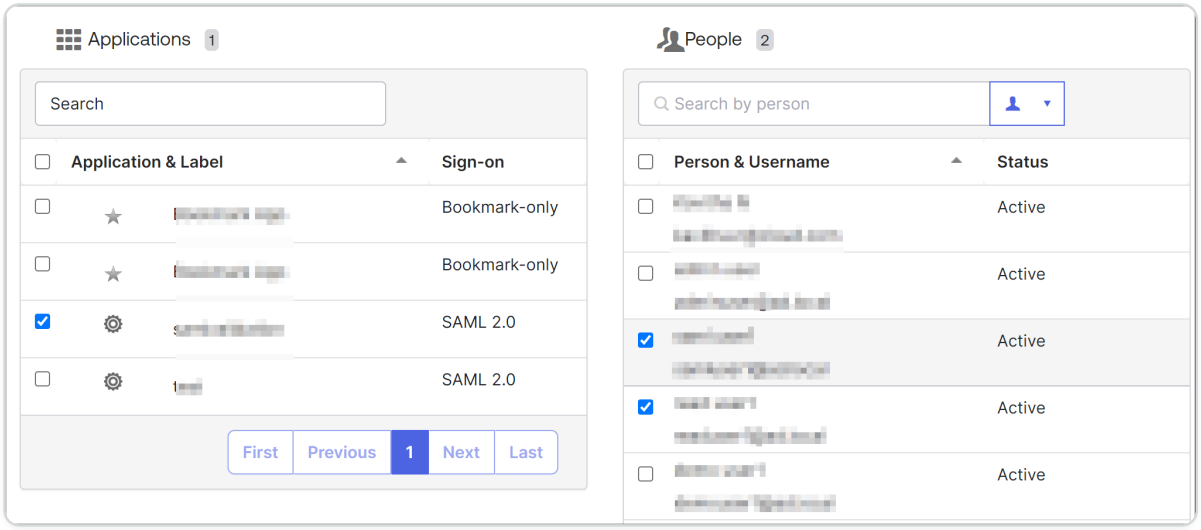
a. Navigate to **Applications > Applications**.

b. Click **Assign Users to App**.



c. Select the application and users, and then click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



d. Click **Confirm Assignments**.

Method 3:

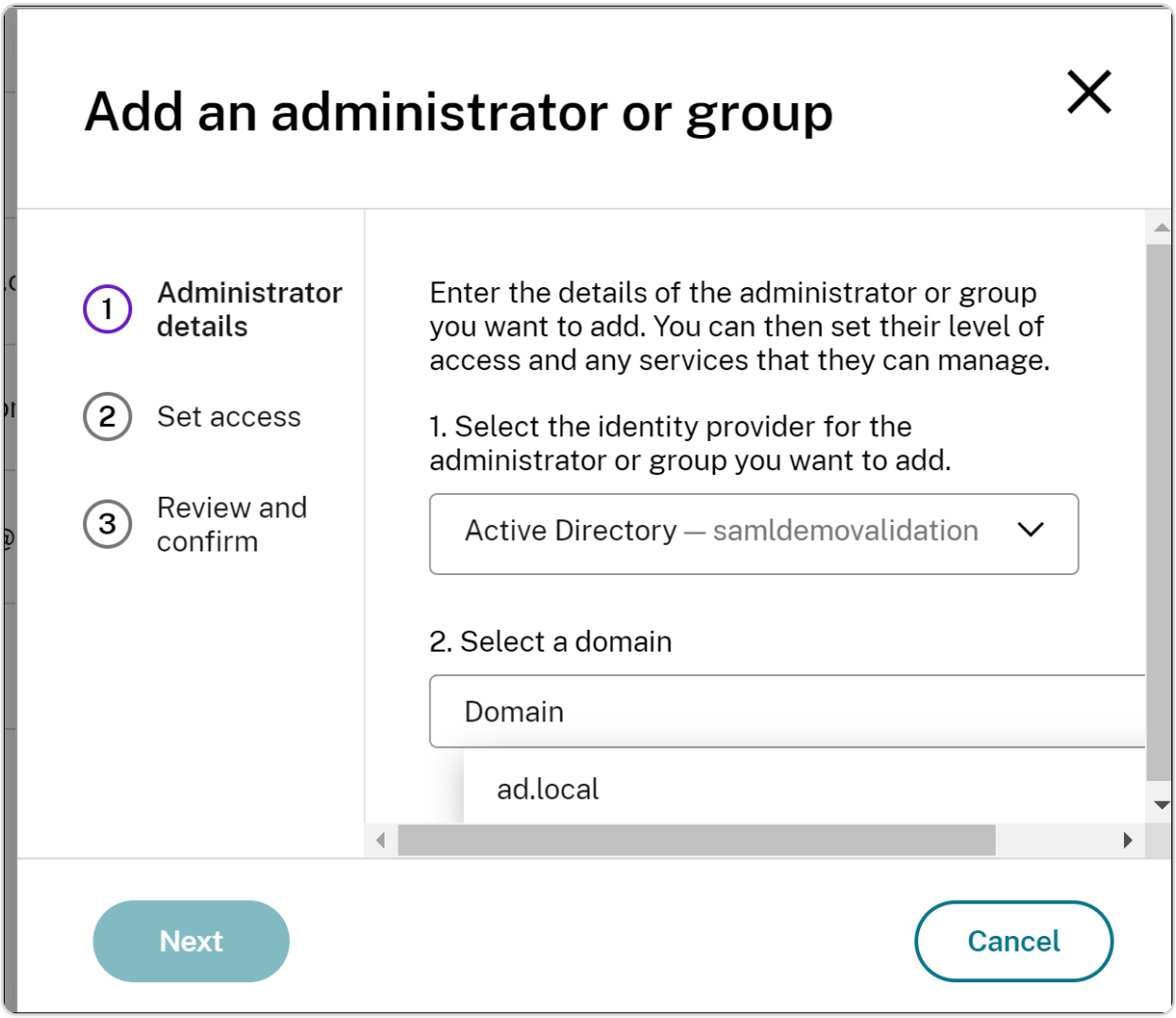
a. Navigate to **Directory > People**.

b. Select any user.

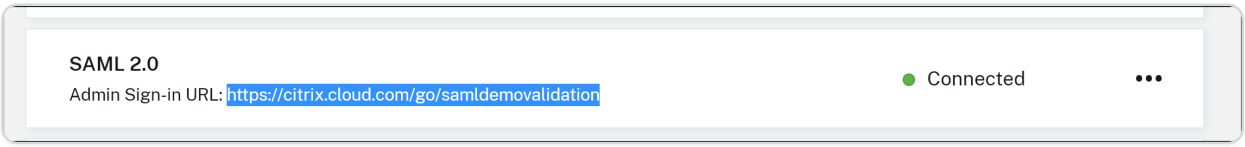
c. Click **Assign Applications** and assign the SAML application to the user.

19. After assigning users, log on to Citrix Cloud.
20. From the Citrix Cloud menu, select **Identity and Access Management**.
21. In the **Administrators** tab, click **Add Administrator/group**.
22. Select **Active Directory -** from the list, select the domain, and then click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



23. Specify the access permissions.
24. Review if everything is correct and click **Send Invitiation**.
25. In **Authentication** tab, you can view the sign-in URL for SAML 2.0. The following is an example:



© 1997–2026 Citrix Systems, Inc. All rights reserved.

System requirements

Before you begin using NetScaler Console, you must review the software requirements, browser requirements, port information, license information, and limitations.

Supported browsers

To access NetScaler Console, your workstation must have a supported web browser.

The following browsers are supported.

WEB BROWSER	VERSION
Microsoft Edge	79 and later
Google Chrome	51 and later
Safari	10 and later
Mozilla Firefox	52 and later

Agent installation requirements

Install and configure an agent in your network environment to enable communication between the NetScaler Console and the managed instances in your data center. In your data center on-premises, you can install an agent on Citrix XenServer, VMware ESXi, Microsoft Hyper-V, and Linux KVM server.

The agent requirements are the virtual computing resources that the hypervisor must provide for each agent. The following table lists the agent requirements to use all NetScaler Console features:

COMPONENT	REQUIREMENT
RAM	32 GB
Virtual CPU	8
Storage Space	30 GB

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COMPONENT	REQUIREMENT
Virtual Network interfaces	1
Throughput	1 Gbps

The agent requirements to use only the pooled or flexed licensing feature, see Lightweight agent for pooled or flexed licensing.

You can also install an agent on Microsoft Azure or AWS or Google Cloud. Citrix recommends you use the following virtual machine types from the respective cloud marketplaces to use all NetScaler Console features:

CLOUD	AGENT REQUIREMENTS	PREFERRED VIRTUAL MACHINE TYPE
AWS	8 virtual CPU, 32 GB RAM, and 30 GB storage space	`m4.2xlarge`
Microsoft Azure	8 virtual CPU, 32 GB RAM, and 30 GB storage space	`Standard_D8s_v3`
Google Cloud	8 virtual CPU, 32 GB RAM, and 30 GB storage space	`e2-standard-8`

NOTES:

Azure will no longer support scaling out for agents with base installer versions 13.0 and 13.1 after July 23, 2024.

For NetScaler agents:

- NetScaler agents with 8 virtual CPUs, 32 GB RAM, and 30 GB storage space remain unaffected. These agents can undergo upgrades without any disruptions.
- Deployments started with version 14.1 also remain unaffected.

For Lightweight agents:

- Lightweight agents with 4 virtual CPUs, 8 GB RAM, and 30 GB storage space, using base installer versions 13.0 or 13.1, cannot scale up (increase CPU or RAM) after the deprecation date.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To scale up the lightweight agents in the future, reprovision a new agent with the latest version.

For instructions about installing an agent, see the following links:

- Install an agent on Microsoft Azure Cloud.
- Install an agent on AWS.
- Install an agent on Google Cloud.

Lightweight agent for pooled or flexed licensing

If you plan to use the NetScaler Console only for pooled or flexed licensing, you can use an agent with lower specifications as listed in the following table:

COMPONENT	REQUIREMENT
RAM	8 GB
Virtual CPU	4
Storage Space	30 GB

Such agents with lower specifications (lightweight) are supported only on NetScaler Console.

Citrix recommends you use the following virtual machine types from the respective cloud marketplaces to use only the pooled licensing feature:

CLOUD	AGENT REQUIREMENTS	PREFERRED VIRTUAL MACHINE TYPE
AWS	4 virtual CPU, 8 GB RAM, and 30 GB storage space	`m4.xlarge`. This instance type provides 4 virtual CPU, 16 GB RAM, and 30 GB storage space. Citrix recommends this instance type since it matches most of the agent requirements among existing instance types.
Microsoft Azure	4 virtual CPU, 8 GB RAM, and 30 GB storage space	`Standard_F4s_v2`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

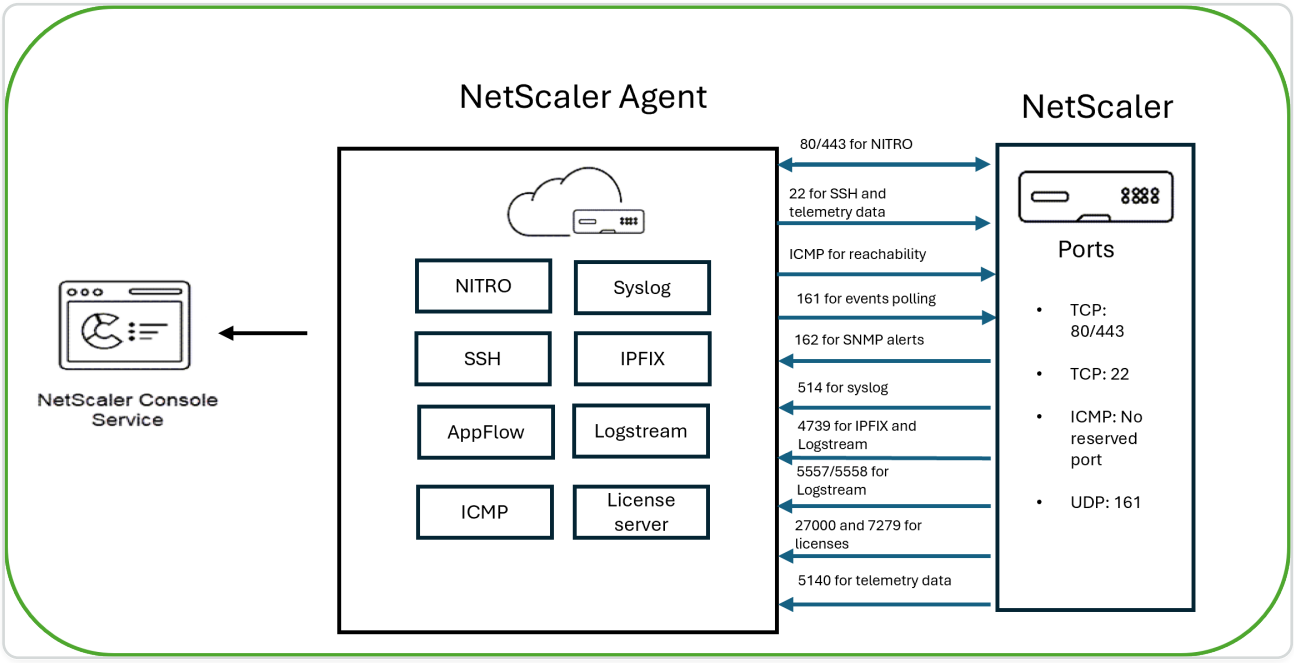
CLOUD	AGENT REQUIREMENTS	PREFERRED VIRTUAL MACHINE TYPE
Google Cloud	4 virtual CPU, 8 GB RAM, and 30 GB storage space	`e2-standard-4`

NOTE

You must disable the default scheduling jobs by navigating to **Settings > Global Settings > Configurable Features**.

Supported ports

For communications between NetScaler instances and agent, open the required ports.



Ports for the NetScaler agent

This table explains the required ports that must be open on the agent.

PORT	TYPE	DETAILS	DIRECTION OF COMMUNICATION
80/443	TCP	For NITRO communication from the NetScaler	NetScaler agent to NetScaler and

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PORT	TYPE	DETAILS	DIRECTION OF COMMUNICATION
		Console service to NetScaler.	NetScaler to NetScaler agent
4739	UDP	For AppFlow communication from NetScaler to the NetScaler Console service.	NetScaler to NetScaler agent
162	UDP	To receive SNMP events from NetScaler instance to the NetScaler Console service.	NetScaler to NetScaler agent
514	UDP	To receive syslog messages from NetScaler instance to the NetScaler Console service.	NetScaler to NetScaler agent
5563	TCP	This port is required for NetScaler Console Collector service to run. To receive NetScaler metrics (counters) from NetScaler instance to NetScaler Console.	NetScaler to NetScaler agent
5557/5558	TCP	For logstream communication (for WAF Security Violations, Web Insight, and HDX Insight) from NetScaler to the NetScaler Console service.	NetScaler to NetScaler agent

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PORT	TYPE	DETAILS	DIRECTION OF COMMUNICATION
27000 and 7279	TCP	License ports for communication between NetScaler agent and NetScaler instance. These ports are also used for NetScaler pooled licenses.	NetScaler to NetScaler agent
5140	UDP	Port to receive NetScaler Gateway telemetry data	NetScaler to NetScaler agent

Ports for NetScaler instances

This table explains the required ports that must be open on NetScaler instances.

PORT	TYPE	DETAILS	DIRECTION OF COMMUNICATION
80/443	TCP	For NITRO communication from NetScaler Console to NetScaler instance.	NetScaler agent to NetScaler and NetScaler to NetScaler agent
22	TCP	For the SSH communication between the agent and NetScaler. **Note:** This port is also used for NetScaler telemetry.	NetScaler agent to NetScaler
No reserved port	ICMP	To detect network reachability between NetScaler agent and NetScaler instances.	NetScaler agent to NetScaler
161	UDP	To poll events from NetScaler instances.	NetScaler agent to NetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ports for NetScaler Built-in agent

This table explains the required ports that must be for NetScaler built-in agent.

PORT	TYPE	DETAILS	DIRECTION OF COMMUNICATION
443	TCP	For NITRO communication from NetScaler Console to NetScaler instance.	NetScaler Console to NetScaler built-in agent and NetScaler built-in agent to NetScaler Console

NOTE:

The endpoint of the NetScaler Console service is the same as the "Service URL" generated while trying to register the agent. The agent uses the Service URL to locate the NetScaler Console.

Ensure that the following endpoint urls are allowed access:

SERVICE	GOVERNMENT CLOUD	JAPAN	OTHER REGIONS (APEC, EU, AND US)
Download service	`download.adm.cloud.us`	`download.citrixnetworkapi.net`	`download.citrixnetworkapi.net`
Trust service	`*.citrixnetworkapi.us`	`*.citrixnetworkapi.jp`	`*.citrixnetworkapi.net`
	`trust.citrixworkspacesapi.us`	`trust.citrixworkspacesapi.jp`	`trust.citrixworkspacesapi.net`
Service URLs	`*.agent.adm.cloud.us`	`*.agent.adm.citrixcloud.jp`	`*.agent.adm.cloud.com`
	`*.adm.cloud.us`	`*.adm.citrixcloud.jp`	`*.adm.cloud.com`
	`adm.cloud.us`	`adm.citrixcloud.jp`	`adm.cloud.com`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SERVICE	GOVERNMENT CLOUD	JAPAN	OTHER REGIONS (APEC, EU, AND US)
Citrix Cloud connectivity	`citrix.cloud.us`	`citrix.citrixcloud.jp`	`citrix.cloud.com`
	`accounts.cloud.us`	`accounts.citrixcloud.jp`	`accounts.cloud.com`

Requirements for NetScaler Console Analytics solution

Minimum Citrix Virtual Apps and Desktops versions required

NETSCALER CONSOLE FEATURE	CITRIX VIRTUAL APPS AND DESKTOPS VERSION
HDX Insight	Citrix Virtual Apps and Desktops 7.0 and later

NOTE

The NetScaler Gateway feature (branded as Access Gateway Enterprise for versions 9.3 and 10.x) must be available on the NetScaler instance. NetScaler Console does not support standalone Access Gateway Standard appliances.

NetScaler Console can generate reports for applications that are published on a Citrix Virtual App or Desktop and accessed through Citrix Workspace. However, this capability depends on the operating system on which the Citrix Workspace is installed. Currently, a NetScaler does not parse ICA traffic for applications or desktops that are accessed through Citrix Workspace running on iOS or Android operating systems.

Thin clients supported for HDX™ Insight

NetScaler Console supports the following thin clients for monitoring NetScaler instances running on software version 11.0 Build 65.31 and later:

- Dell Wyse Windows based Thin Clients
- Dell Wyse Linux-based Thin Clients
- Dell Wyse ThinOS based Thin Clients

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 10ZiG Ubuntu-based Thin Clients

NetScaler instance license required for HDX Insight

The data collected by NetScaler Console for HDX Insight depends on the version and the installed licenses of the NetScaler instances that are monitored. HDX Insight reports are displayed only for NetScaler Premium and Enterprise appliances running on software version 10.5 and later.

NetScaler License/ Duration	5 minutes	1 Hour	1 Day	1 Week	1 Month
Standard	No	No	No	No	No
Advanced	Yes	Yes	No	No	No
Premium	Yes	Yes	Yes	Yes	Yes

Supported operating systems and Citrix Workspace versions

The following table lists the operating systems supported by NetScaler Console, and the Citrix Workspace versions currently supported with each system:

OPERATING SYSTEM	CITRIX WORKSPACE VERSION
Windows	4.0 Standard Edition
Linux	13.0.265571 and later
Mac	11.8, build 238301 and later
HTML5	1.5
Chrome App	1.5

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Licenses

Starting from NetScaler Console service release 14.1-21.x, the concept of licensed VIPs is removed. An unlimited number of VIPs are now available in NetScaler Console service. You no longer have to purchase NetScaler Console virtual server licenses because VIP license SKU will be End of Sale (EOS) and End of Renewal (EOR) shortly.

The changes to NetScaler® Console service storage are as follows:

- NetScaler Console service storage SKU will be End of Sale (EOS) & End of Renewal (EOR) shortly.
- The default NetScaler Console service storage entitlement is now 5GB.
- Any NetScaler Console service storage purchased in the past is honored until the term ends.
- Any NetScaler Console VIP licenses purchased in the past that entitled you to a proportionate entitlement of NetScaler Console service storage are honored until the term ends.
- If you purchase a different package that entitles you to a higher NetScaler Console storage entitlement, the default 5GB is changed to match the entitlement.

NOTE:

If you have purchased a virtual server earlier, 500 MB of storage applies per virtual server until the end of the subscription term.

NetScaler licensing required for NetScaler Console features

The following table lists the NetScaler licenses that are required to use some of the NetScaler Console features.

NETSCALER CONSOLE FEATURE GROUP	NETSCALER CONSOLE FEATURES	NETSCALER AND GATEWAY LICENSE REQUIREMENT
Analytics	HDX Insight	Advanced (reporting < 1 hour) Premium (reporting = Unlimited)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETSCALER CONSOLE FEATURE GROUP	NETSCALER CONSOLE FEATURES	NETSCALER AND GATEWAY LICENSE REQUIREMENT
Analytics	Security Insight	Premium (or) Advanced with App Firewall license
Analytics	Gateway Insight	Advanced (reporting < 1 hour) Premium (reporting = Unlimited)
Applications	Application Statistics (App Dashboard, App Security Dashboard)	NetScaler Web App Firewall related information on App dashboard, and app security dashboard needs Premium (or) Advanced with App Firewall license
Applications	API gateway	Premium (or) Advanced license
Applications	StyleBooks	N/A
Applications	Inventory Management – Infrastructure Dashboard, Instance groups, Instance dashboards and Sites	N/A
Applications	Event Management and Syslog	N/A
Applications	Configuration Jobs, Configuration Audit, and Configuration Advice	N/A
Applications	Network reporting (Instance level)	N/A
Applications	Network reporting (virtual server level)	N/A
Applications	Network Functions (Plain visibility and Management of	N/A

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETSCALER CONSOLE FEATURE GROUP	NETSCALER CONSOLE FEATURES	NETSCALER AND GATEWAY LICENSE REQUIREMENT
	virtual servers, services, service groups, servers)	
Applications	SSL certificate management (Instance level)	N/A
Applications	SSL certificate management (virtual server level)	N/A
System	RBAC and External Authentication (instance level)	N/A
System	RBAC and External Authentication (virtual server level)	N/A

View expiry checks for virtual server subscriptions

You can view the status of installed licenses with the expiry and the allowed storage limit to the licenses in NetScaler Console.

To view the status of the licenses:

1. Navigate to **Settings > Analytics Configuration**.
2. In the **Entitlements** section, you can view the following details:
   - **Entitled Storage:** Storage limit of the license.
   - **Days to Expiry:** Number of days remaining before the license expiry.

View the type of analytics enabled on the virtual servers

After you enable AppFlow® on the selected virtual servers, you can view the type of analytics enabled on the licensed virtual servers or third-party virtual servers from the **Subscriptions** page.

1. Navigate to **Settings > Analytics Configuration**.
2. In the **Virtual Server Analytics Summary** section, select the type of licensed virtual servers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. The licensed virtual servers page displays the list of licensed virtual servers. On this page, the **Analytics Status** column displays the type of analytics enabled on the virtual servers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Upgrade Advisory

As a network administrator, you might manage many NetScaler instances running on different NetScaler releases in NetScaler Console. Monitoring the lifecycle of each NetScaler instance can be a cumbersome task. You must visit NetScaler product Matrix, identify the NetScaler instances that are reaching or reached End of Life (EOL) or End of Maintenance (EOM). Then, plan their upgrade.

To ease this process, NetScaler Console upgrade advisory helps you monitor the lifecycle of your NetScaler instances in the following ways:

- Identifies instances reaching or reached EOL or EOM. So, you can plan NetScaler upgrades ahead of EOL or EOM date.
- Highlights the instances that are not on latest release or build. You can upgrade these instances to latest release or build. With this upgrade, you receive updates on new features and fixed issues.
- Highlights the instances that are not on preferred NetScaler builds. Some organizations might have a preferred NetScaler builds for their instances. In NetScaler Console, you can set the preferred build for your organization depending on build stability, features, and other considerations. Then, review and upgrade the instances that are not on preferred builds. Instances running the preferred builds are indicated with a star icon.
- Highlights instances running on the most popular releases or builds. Instances running the popular builds are indicated with a ribbon icon.

The upgrade advisory provides links to corresponding release notes. With this information, you can review and decide a NetScaler build for upgrade. You can proceed to create a maintenance job to upgrade NetScaler instances from the Upgrade Advisory page.

IMPORTANT

Upgrade advisory only monitors EOL of NetScaler software releases. It doesn’t check the EOL of NetScaler appliances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View upgrade advisory

Navigate **Infrastructure > Instance Advisory > Upgrade Advisory** and view the following information:

- Total count of NetScaler instances.
- Instances reaching the end of life.
- Instances reaching the end of maintenance.
- Instances in older build.
- Instances not in preferred build.
- End of Life and End of Maintenance dates for the various NetScaler releases.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Upgrade Advisory

Settings

MPX & VPX | SDX

12 Total MPX & VPX

3 Instances reaching end of life

0 Instances reaching end of maintenance

12 Instances on older build

12 Instances not on preferred build

Select NetScaler instances grouped by releases / builds and proceed to upgrade.

Release 14.1 — End of Maintenance: 08 Aug, 2029

0 Total NetScaler Instances

Build	MPX	VPX	
12.30	0	0	Release Notes
4.42	0	0	Release Notes

Release 13.1 — End of Maintenance: 15 Sep, 2026

9 Total NetScaler Instances

Build	MPX	VPX	
51.14	0	0	Release Notes
49.15	0	2	Release Notes
48.47	0	0	Release Notes
45.64	0	0	Release Notes

Release 13.0 — End of Life: 15 Jul, 2024

3 Total NetScaler Instances

Build	MPX	VPX	
92.19	0	0	Release Notes
52.24	0	3	Release Notes
47.24	0	0	Release Notes

Release 12.1 — End of Life: 30 May, 2023

0 Total NetScaler Instances

Build	MPX	VPX	
65.37	0	0	Release Notes
56.22	0	0	Release Notes

Release 12.0 — End of Life: 30 Oct, 2020

0 Total NetScaler Instances

Build	MPX	VPX	
63.21	0	0	Release Notes

Release 11.1 — End of Life: 30 Jun, 2021

0 Total NetScaler Instances

Build	MPX	VPX	
65.23	0	0	Release Notes
63.15	0	0	Release Notes

Select instances to upgrade

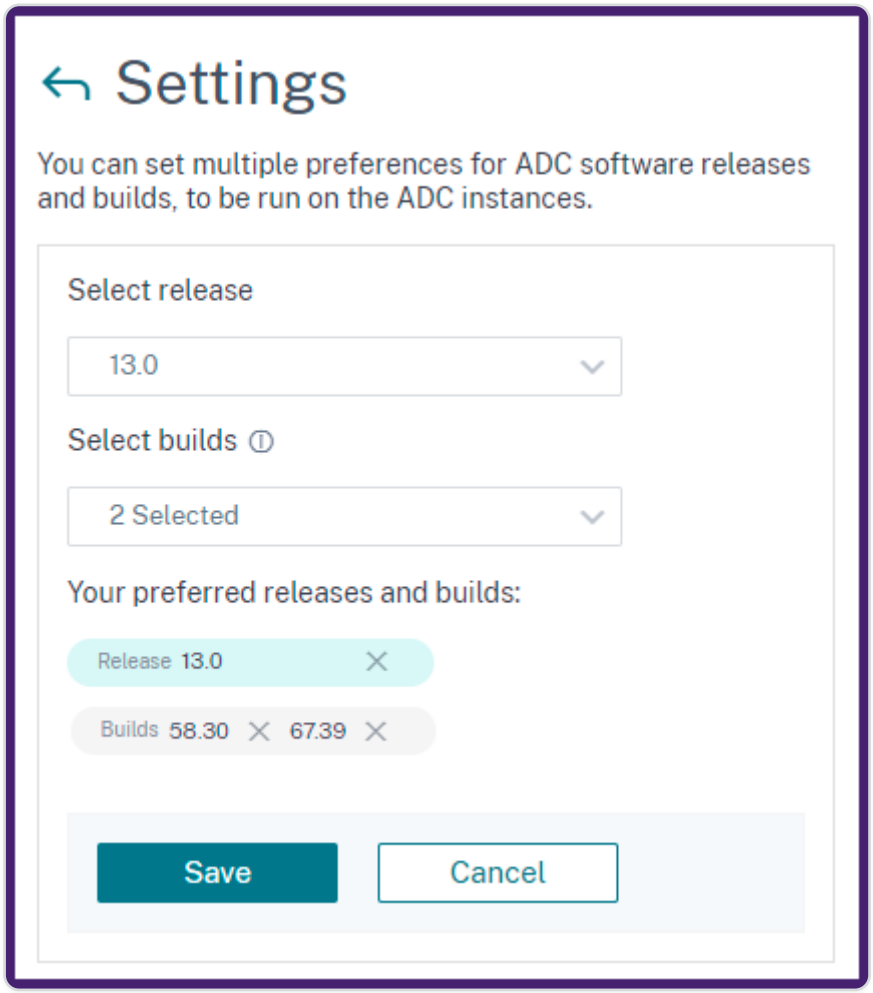
© 1997–2026 Citrix Systems, Inc. All rights reserved.

The **Upgrade Advisory** page groups the NetScaler instances by their releases. The **Release Notes** link guides you to the specific NetScaler release notes. Review new features, fixed, and known issues before deciding to upgrade. You can select multiple NetScaler instances across different releases to upgrade at a time. When you proceed with an upgrade, it creates an upgrade job. See, Upgrade NetScaler instances.

Set the preferred builds

As an administrator, you can define a preferred NetScaler build for organization. Do the following to set the preferred build:

1. In **Infrastructure > Instance Advisory > Upgrade Advisory**, click **Settings**.
2. Select the preferred release and build.



In this example, the preferred builds are `13.0-58.30` and `13.0-67.39`.

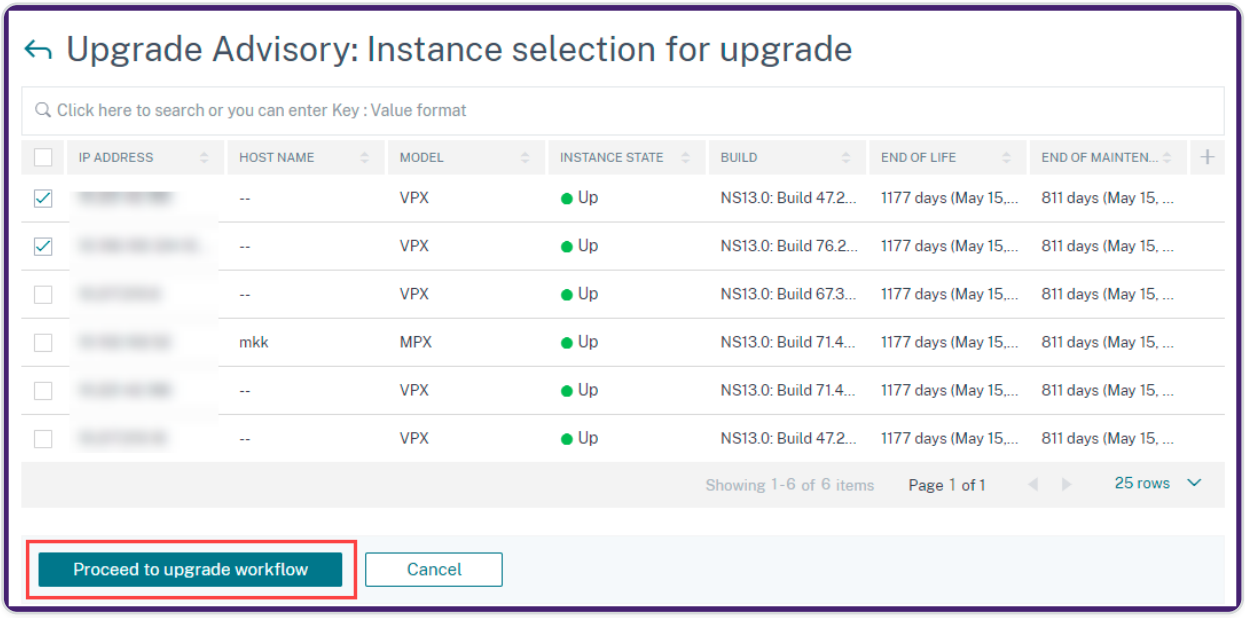
3. Click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Upgrade NetScaler instances

In the **Upgrade Advisory** page, after your review, do the following steps to upgrade the required NetScaler instances:

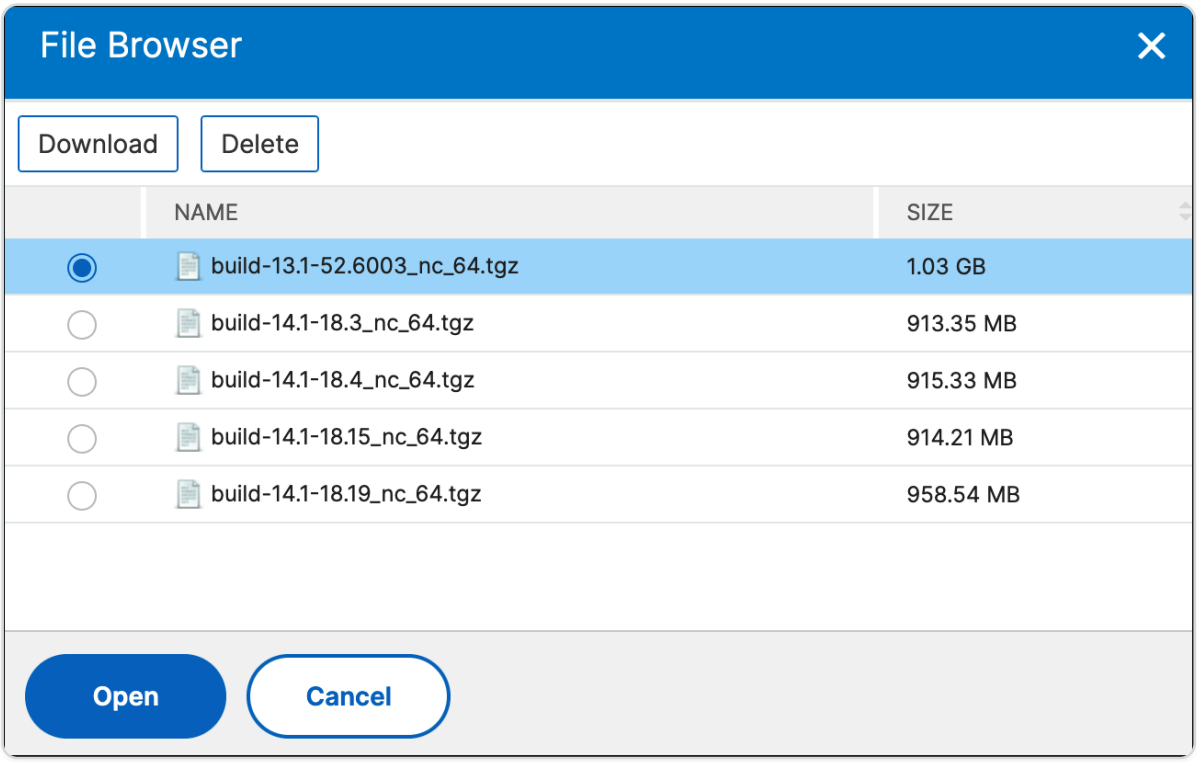
1. Select the instance builds that you want to upgrade and click **Select instances to upgrade**.
2. Select the NetScaler instance that you want to upgrade and click **Proceed to upgrade workflow**.



This workflow creates an upgrade job.

3. In the **Select Instance** tab,
   a. Specify a name to the upgrade job.
   b. (Optional) if you want to add other instances, click **Add Instances**.
   c. Click **Next**.
4. In the **Select Image** tab, select a NetScaler image from the image library or local or appliance.
   - **Select from Image Library**: Select a NetScaler image from the list. This option lists all NetScaler images that are available in the NetScaler downloads website.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The NetScaler software images display the preferred builds with the star icon. And, most downloaded builds with the bookmark icon.

- **Select from local or appliance**: You can upload the image from your local computer or the NetScaler appliance. When you select NetScaler appliance, the NetScaler Console GUI displays the instance files that are present in `/var/mps/mps_images`. Select the image from the NetScaler Console GUI.
- **Skip image uploading to NetScaler if the selected image is already available** - This option checks whether the selected image is available in NetScaler. Upgrade job skips uploading a new image and uses the image available in NetScaler.
- **Clean software image from NetScaler on successful upgrade** - This option clears the uploaded image in the NetScaler instance after the instance upgrade.

Click **Next** to start the pre-upgrade validation on the selected instances.

5. The **Pre-upgrade validation** tab displays the failed instances. you can remove the failed instances and click **Next**.

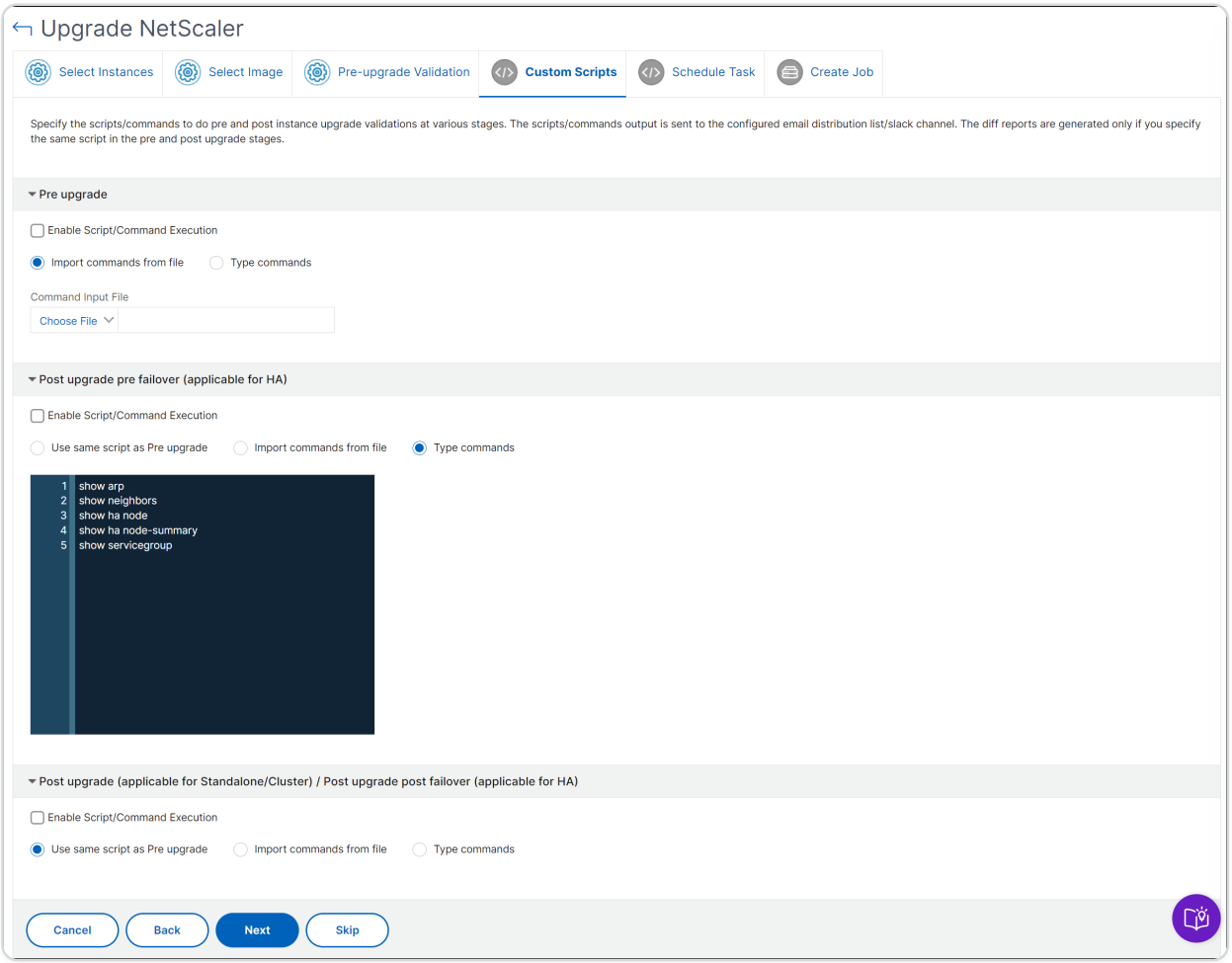
   - **Disk Space Check**: If you face insufficient disk space on an instance, you can check and clean up the disk space. See, Clean up NetScaler disk space.
   - **Policy Check**: If NetScaler Console finds unsupported classic policies, you can remove such policies to create an upgrade job.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If you specify cluster IP address, the NetScaler Console does pre-upgrade validation only on the specified instance not on the other cluster nodes.

6. Optional, in the **Custom scripts** tab, specify the scripts to run before and after an instance upgrade.



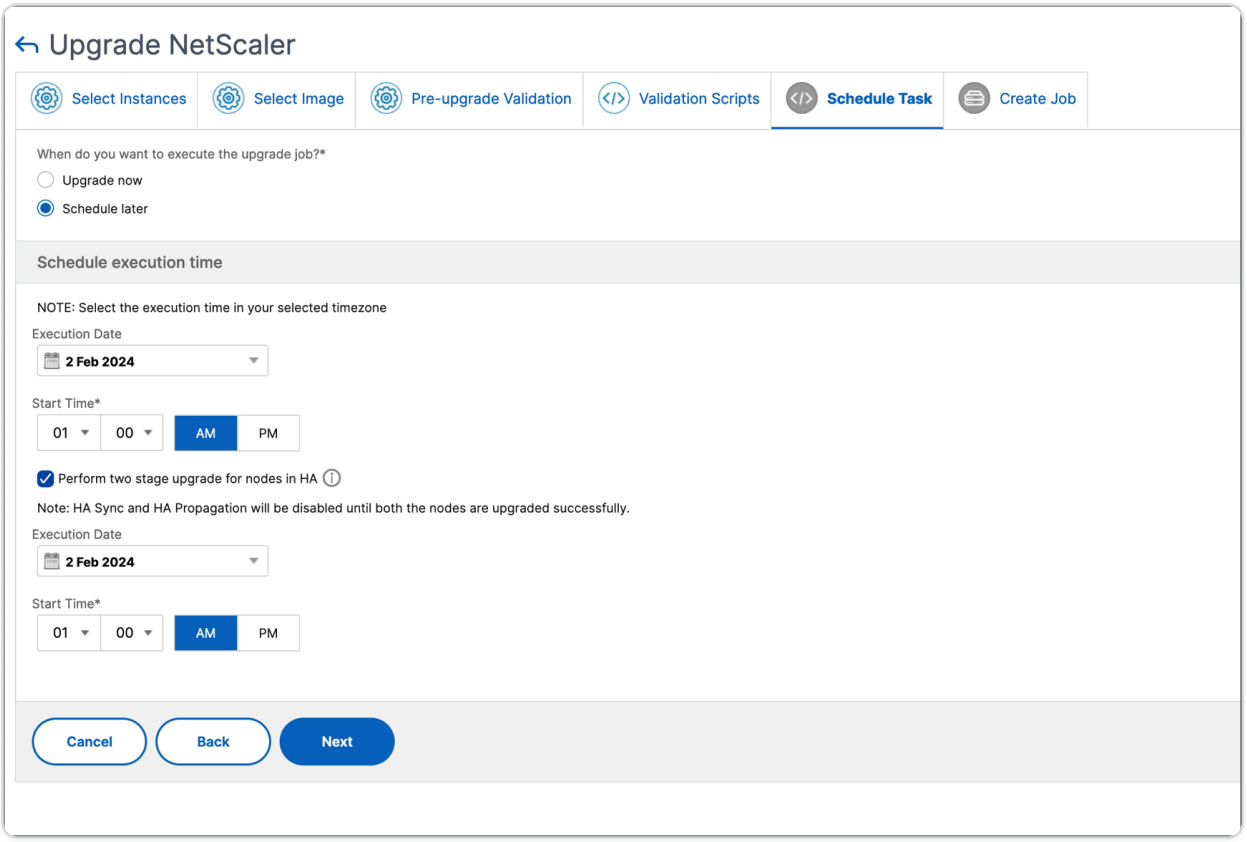
For more information, see Use custom scripts.

7. In the **Schedule Task**, select one of the following options:

   - **Upgrade Now** - The upgrade job runs immediately.
   - **Schedule Later** - Select this option to run this upgrade job later. Specify the **Execution Date** and **Start Time** when you want to upgrade the instances.

   If you want to upgrade a NetScaler high-availability pair in two stages, select Perform two stage upgrade for nodes in HA.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For more information, see Upgrade NetScaler high-availability pair.

8. In the **Create Job** tab, specify the following details:

   If you schedule the upgrade job, you can specify when you want to upload the image to an instance:

   - **Upload now**: Select this option to upload the image immediately. However, the upgrade job runs at the scheduled time.
   - **Upload at the time of execution**: Select this option to upload the image at the time of upgrade job execution.

For more information on the other options, see NetScaler upgrade options.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Security Advisory

A safe, secure, and resilient infrastructure is the lifeline of any organization. Organizations must track new Common Vulnerabilities and Exposures (CVEs), and assess the impact of CVEs on their infrastructure. They must also understand and plan the remediation to resolve the vulnerabilities.

The Security Advisory feature in NetScaler Console enables you to:

- Analyze your NetScaler configuration settings to identify any misconfigurations, weak points, or deviations from best practices that might expose your system to attacks.
- Track any new Common Vulnerabilities and Exposures (CVEs), assess the impact of CVEs, understand the remediation, and resolve the vulnerabilities.
- Examine the integrity of your NetScaler build files.

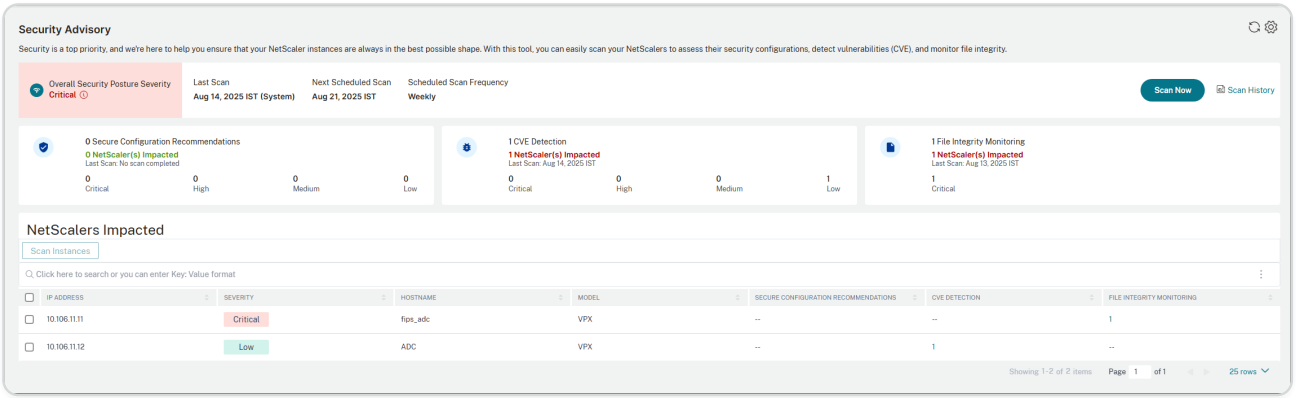
Security advisory landing page

The Security Advisory landing page offers a comprehensive bird's-eye view of your NetScaler deployment's security posture. The interface is enhanced and designed to provide administrators and security professionals with immediate insights into the overall health and vulnerability status of their NetScaler infrastructure.

NetScaler Console provides three types of security advisories:

- **Secure Configuration Recommendations** - Enables you to configure NetScaler instances according to best practices.
- **Common Vulnerabilities and Exposures (CVEs) Detection** - Enables you to identify the CVEs putting your NetScaler instances at risk and recommends remediations.
- **File Integrity Monitoring** - Enables you to identify if any changes or additions have been made to your NetScaler build files.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NetScaler Console security advisory dashboard also includes the following:

- **Overall Security Posture Severity** - Represents the status of security posture and is calculated based on the maximum severity of the three types of advisories. The status can be one of the following:
  - **Critical**: Several critical severity observations are detected that must be addressed with the highest urgency.
  - **High**: Critical vulnerabilities or misconfigurations are detected that must be fixed immediately. While not as urgent as critical findings, these issues pose a significant risk to the security and stability.
  - **Medium**: Important security observations that must be addressed in a timely manner. These issues don't pose an immediate, critical threat, but they might potentially be exploited or lead to more severe problems if left unaddressed.
  - **Low**: Minor security issues or best practice violations that don't pose a significant security risk. While they are not an immediate threat, it's still a good idea to fix these issues to improve the overall security posture.
- **Last Scan** - The date of the last scan. The data provided in the dashboard is based on the results of the last scan.
- **Next Scheduled Scan** - The date of the next scheduled system scan.
- **Scheduled Scan Frequency** - The frequency at which the system scans are run.
- **Scan Now** - Allows on-demand scan that enables you to scan the instances anytime, according to your need, outside the system scan schedule.
- **Scan history** - Provides a historical view of all the scans that have been run on your NetScaler instances.
- **NetScalers impacted** - Lists the NetScaler instances that are impacted.
- **Settings** - Allows you configure system scan settings and set notification for events as per your need.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

With the information available on the dashboard, you can quickly identify critical vulnerabilities, secure configuration recommendations including mitigation steps, and links to relevant documentation.

The landing page allows you to filter issues by criticality and NetScaler IP address. When a specific criticality level is selected, only NetScaler instances at that severity level are shown.

IMPORTANT:

In the **Security Advisory** GUI or report, all CVEs might not appear, and you might only see one CVE. As a workaround, click **Scan Now** and select **CVE** to run an on-demand scan. After the scan is complete, all the CVEs in scope (approximately 15) appear in the UI or report.-->

Secure Configuration Recommendations

The **Secure Configuration Recommendations** tab provides an in-depth, instance-level analysis of configuration observations, designed to empower users with actionable insights. For more information, see Secure configuration recommendations.

CVE Detection

CVE detection primarily focuses on identifying and mitigating security vulnerabilities. For more information, see CVE Detection.

File Integrity Monitoring

File integrity monitoring checks for unauthorized or malicious changes to the core files of a NetScaler instance. It's a key part of the security advisory. For more information, see File Integrity Monitoring.

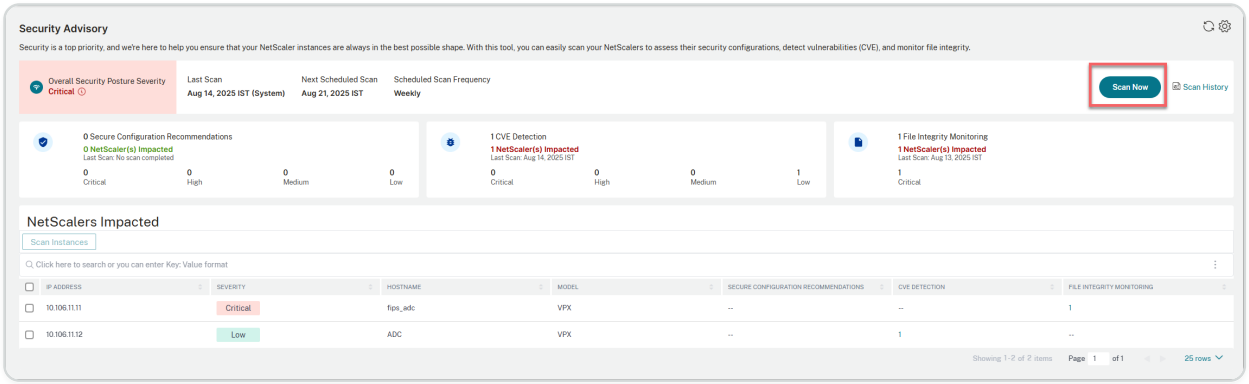
Scan Now

You can scan the instances anytime, according to your need and also choose the types of scans you want to run based on your security requirements.

Perform the following steps to run the scan:

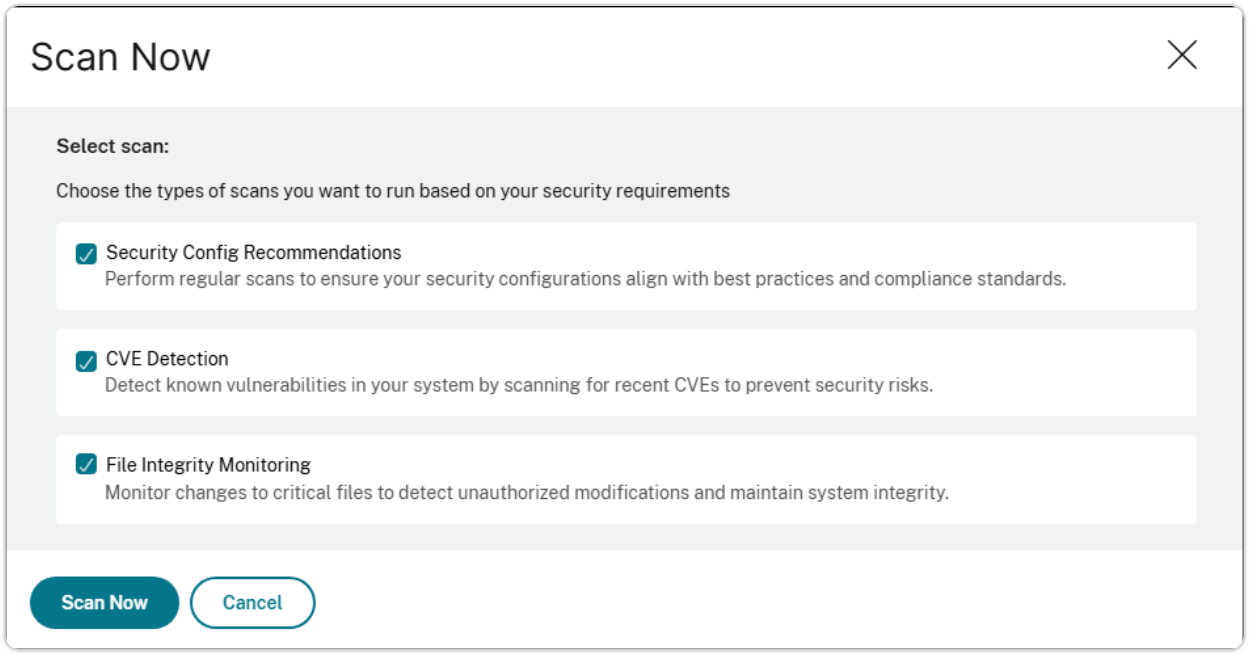
1. Click **Scan Now**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Select the types of scans that you want to run.

   - Security Config Recommendations
   - CVE Detection
   - File Integrity Monitoring

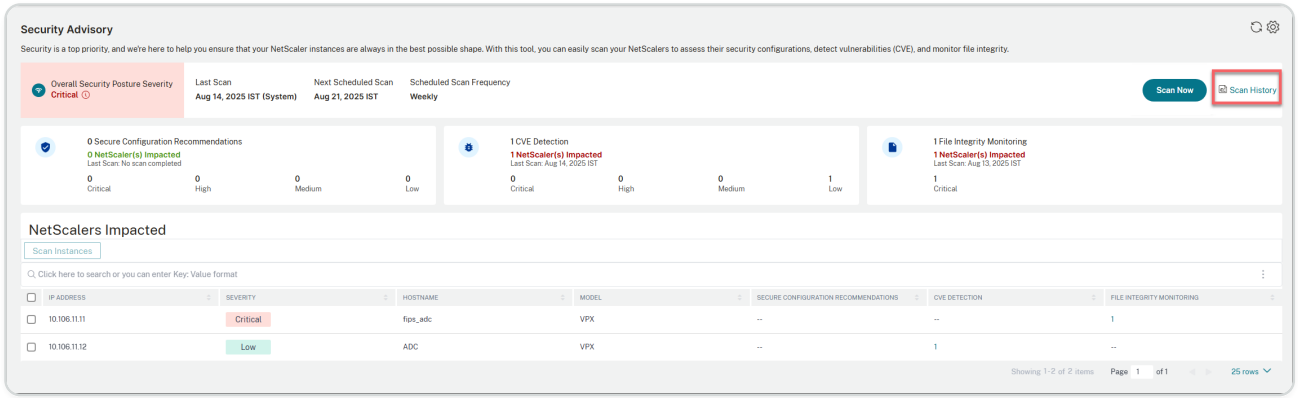


3. Click **Scan Now**. Once the scanning is completed, the revised security details appear in the security advisory dashboard.

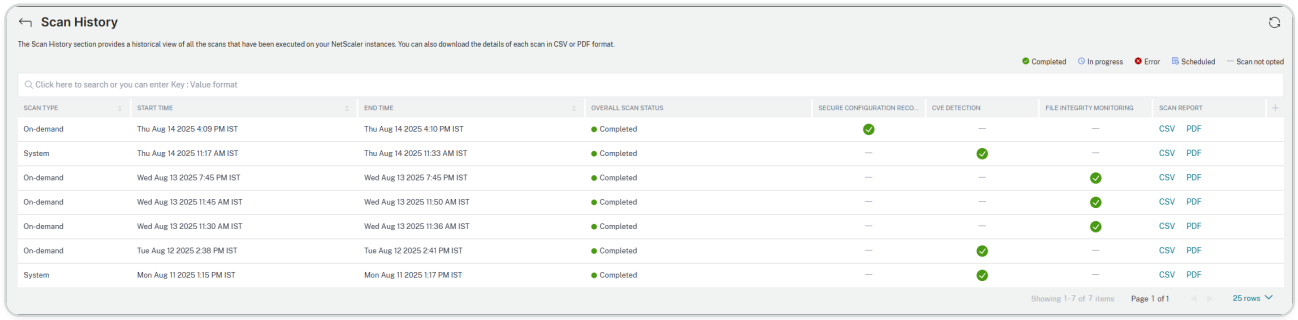
Scan History

Click **Scan History** to view all the historical scans that have been run on your NetScaler instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

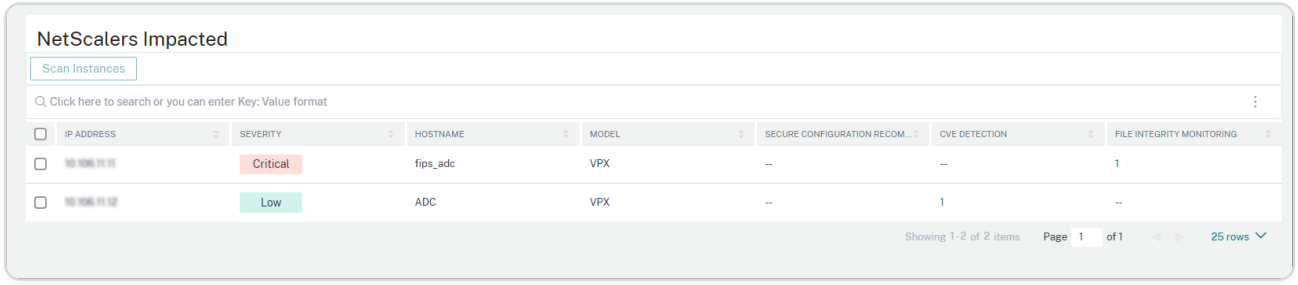


You can view the scan type (On demand scan or system scan), start and end time of the scan, overall scan status, and also download the details of each scan in CSV or PDF format.



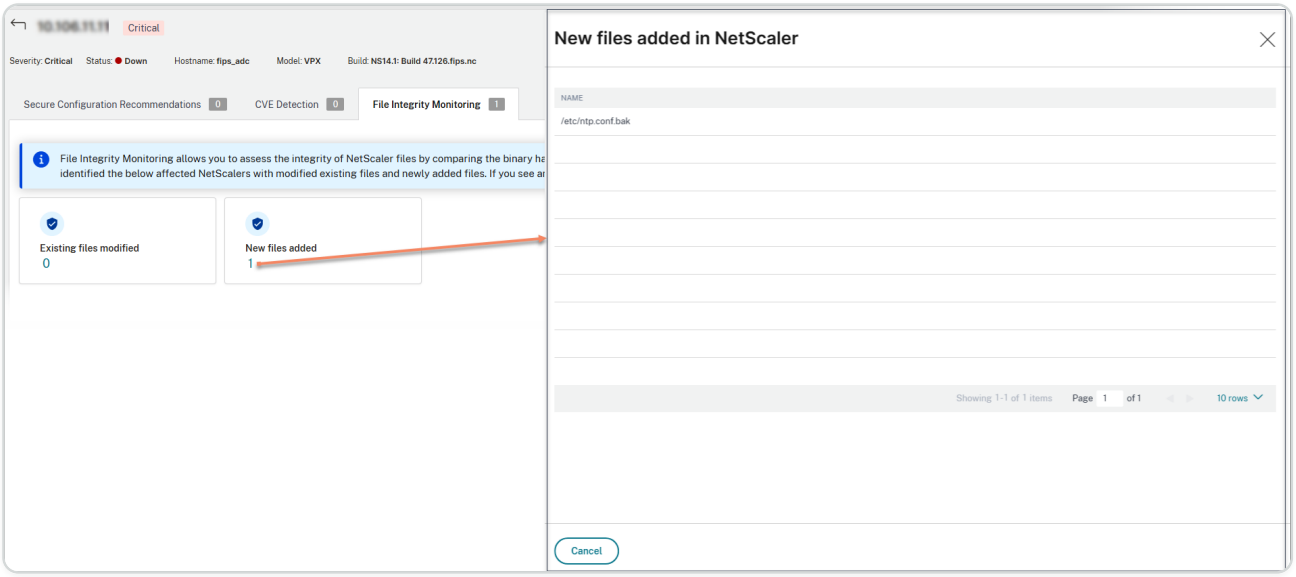
NetScalers impacted

The **NetScalers Impacted** section lists all the NetScaler instances that are impacted by the security configurations, CVEs, and monitor file integrity checks.



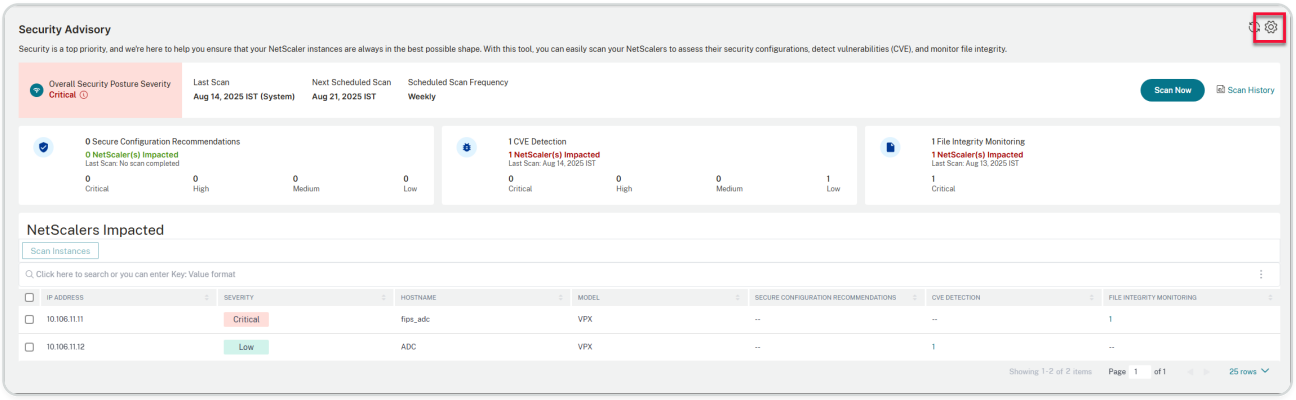
You can also click the number under the **SECURE RECOMMENDATION CONFIGURATION**, **CVE DETECTION**, or **FILE INTEGRITY MONITORING** to view further details. The following is a sample image for your reference.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Settings

As an admin, you can receive Citrix Cloud notifications, which tell how many NetScaler instances are vulnerable with CVEs. To configure when and how you want to receive notifications, click the settings icon on the upper-right corner of the security advisory page.

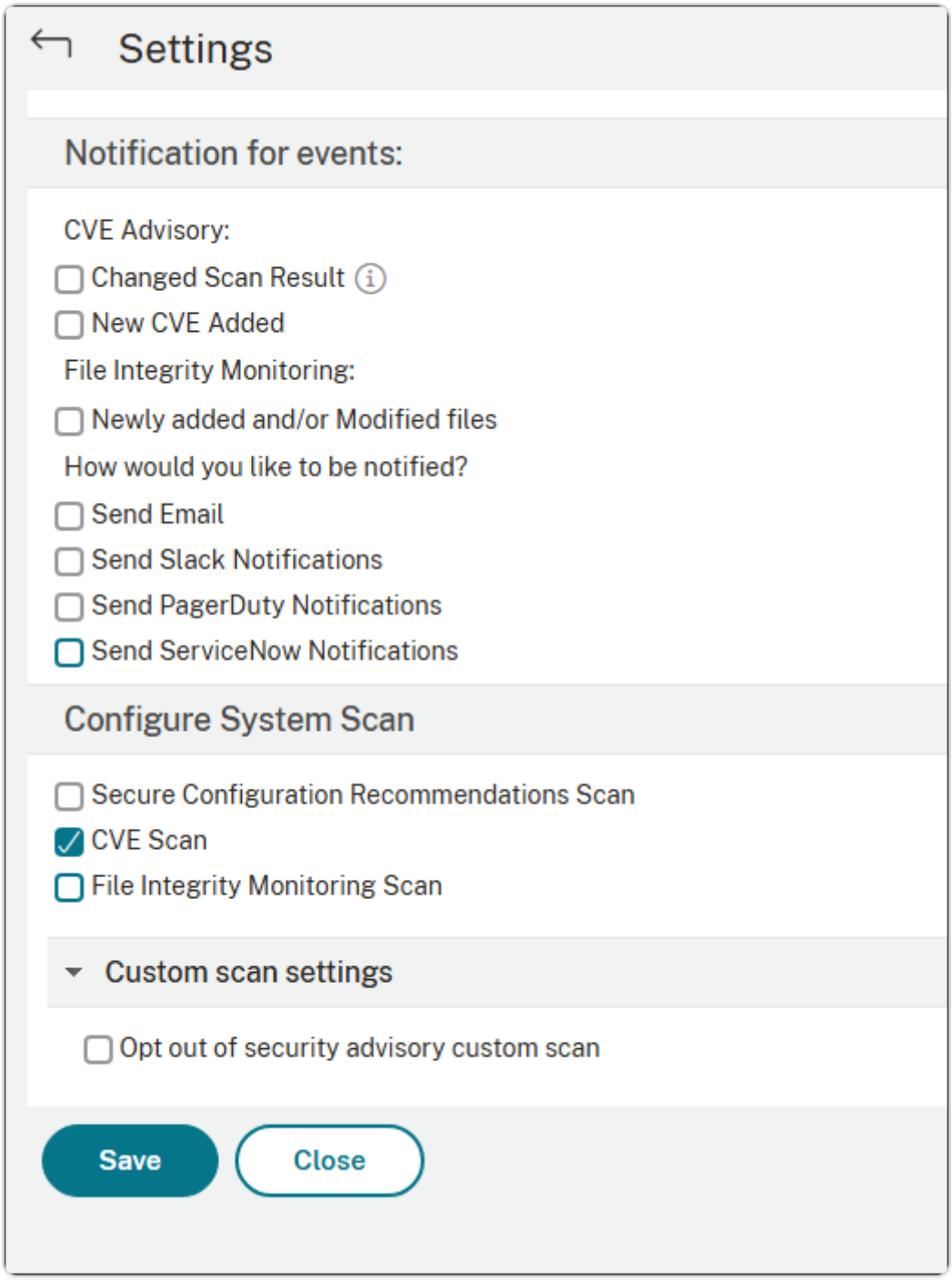


You can perform the following actions:

- Select the type of events for which you must receive the notification.
- Select how you want to be notified. For example, through email, Slack, PagerDuty.
- Select the type of scan that must be included in system scans. By default, only CVE scan is enabled for system scan.
- Opt out of security advisory custom scan.

You can also configure the type of scans that must be included in the system scans.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



DISCLAIMER:

Please note that NetScaler File Integrity Monitoring (“the Feature”) is not capable of detecting all techniques, tactics, or procedures (TTPs) threat actors may use when targeting relevant environments. Threat actors change TTPs and infrastructure frequently, and therefore the Feature may be of limited to no forensic value as to certain threats. You are strongly advised to retain the services of experienced forensic investigators to assess your environment in connection with any possible threat.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This document and the information contained in it is provided as-is. Cloud Software Group, Inc. makes no warranties or representations, whether express or implied, regarding the document or its contents, including, without limitation, that this document or the information contained in it, is error-free or meets any conditions of merchantability or fitness for a particular purpose.

Secure configuration recommendations

NetScaler secure configuration advisory serves as a comprehensive guide offering expert recommendations and specific instructions to enhance the security posture of NetScalerconfigurations. With this feature, you can safeguard your Application Delivery Controller (ADC) infrastructure against potential vulnerabilities and evolving cyber threats. By meticulously following the recommended guidelines, you can proactively mitigate risks, enhance system resilience, and maintain a robust defense against unauthorized access and malicious activities.

This feature not only scans the NetScaler configuration for potential vulnerabilities but also proactively suggests precise commands to remediate those configurations. The network administrators can quickly identify security gaps and implement the necessary changes to strengthen their NetScaler deployment.

The **Secure Configuration Recommendations** tab provides a comprehensive view is meticulously categorized by severity, allowing for a prioritized approach to addressing potential configuration vulnerabilities.

Severity-based prioritization

The categorization by severity enables users to efficiently allocate their efforts. Observations are typically classified into tiers such as:

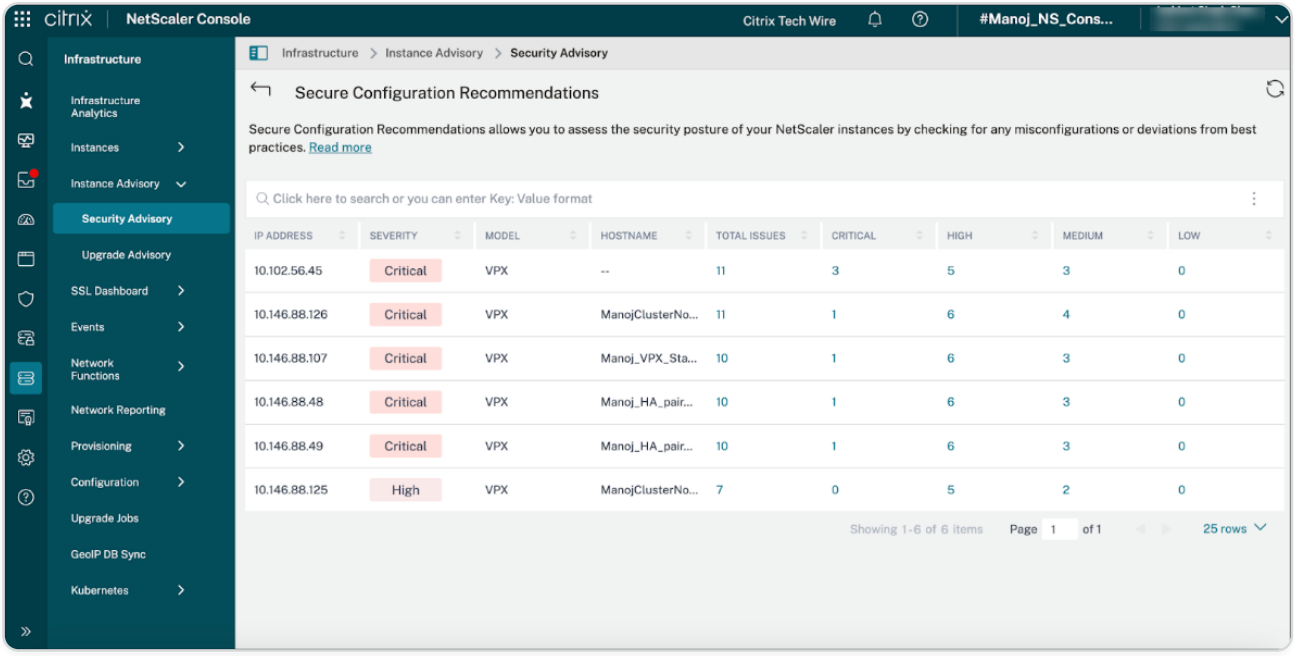
- **Critical**: Issues that pose an immediate and significant risk to the security and integrity of the NetScaler instance. These issues must be addressed with the highest urgency.
- **High**: Configurations that might lead to substantial security breaches if exploited, requiring prompt attention.
- **Medium**: Observations that indicate potential weaknesses or misconfigurations. While these issues are not critical, they might contribute to a larger security incident if left unaddressed.
- **Low**: Minor recommendations or best practices that improve the overall security posture. These issues do not represent an immediate threat.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Benefits of a detailed instance-level view

- **Targeted Remediation**: Instead of generic advice, users receive specific recommendations tailored to each individual NetScaler instance, ensuring precise and effective remediation.
- **Reduced Attack Surface**: By systematically addressing observed misconfigurations, organizations can significantly reduce their attack surface and minimize the likelihood of successful exploits.
- **Compliance Adherence**: The detailed observations can help organizations identify and correct configurations that might violate regulatory compliance standards (for example, GDPR, HIPAA, PCI DSS).
- **Improved Security Posture**: Proactive identification and resolution of configuration weaknesses lead to a stronger overall security posture and enhanced resilience against cyber threats.
- **Operational Efficiency**: By providing clear and actionable insights, the system streamlines the security remediation process, saving time and resources.

You can **pick and choose** which observations to address first, based on your priorities, risk tolerance, and available resources. This flexibility ensures that the most pressing security concerns are tackled without delay, while still providing the necessary information to achieve comprehensive configuration hardening over time. This option empowers security administrators to make informed decisions and take decisive action to safeguard their NetScaler deployments.

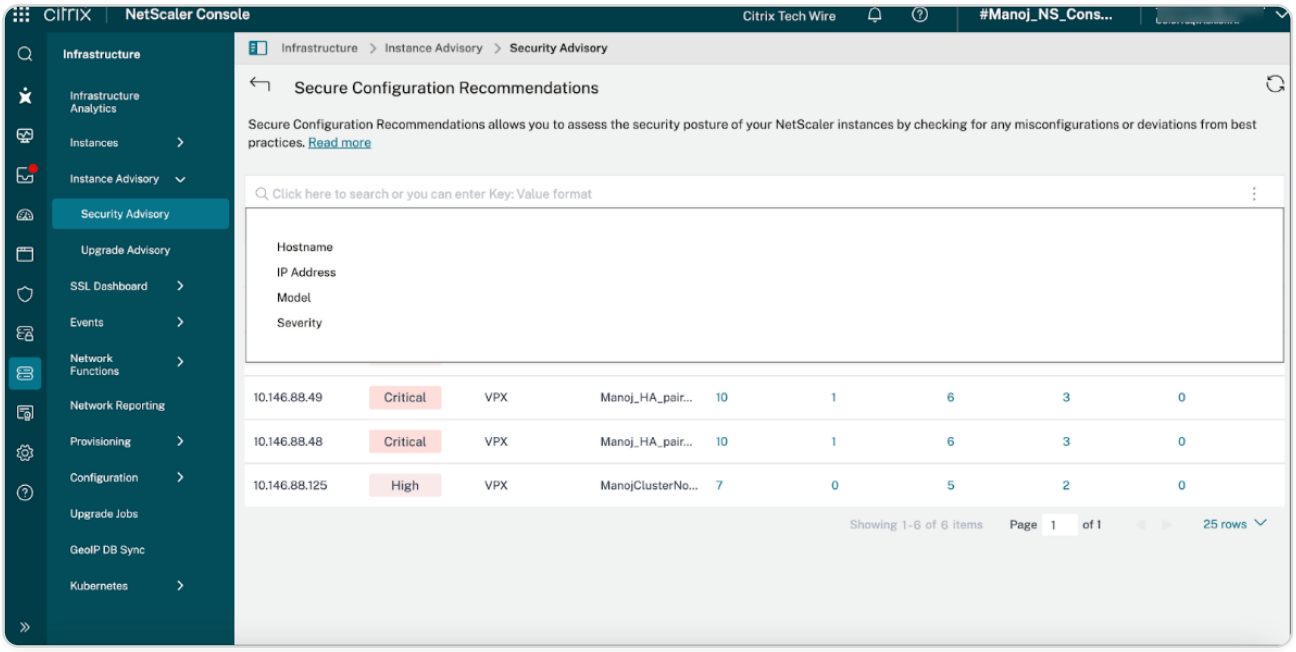


The free-text search functionality enables you to narrow down results based on various key identifiers. For example, you can efficiently search for an instance by its unique host name,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

providing a direct method to pinpoint a particular device. Alternatively, searching by IP address offers another precise way to locate instances, especially useful in network-centric environments.

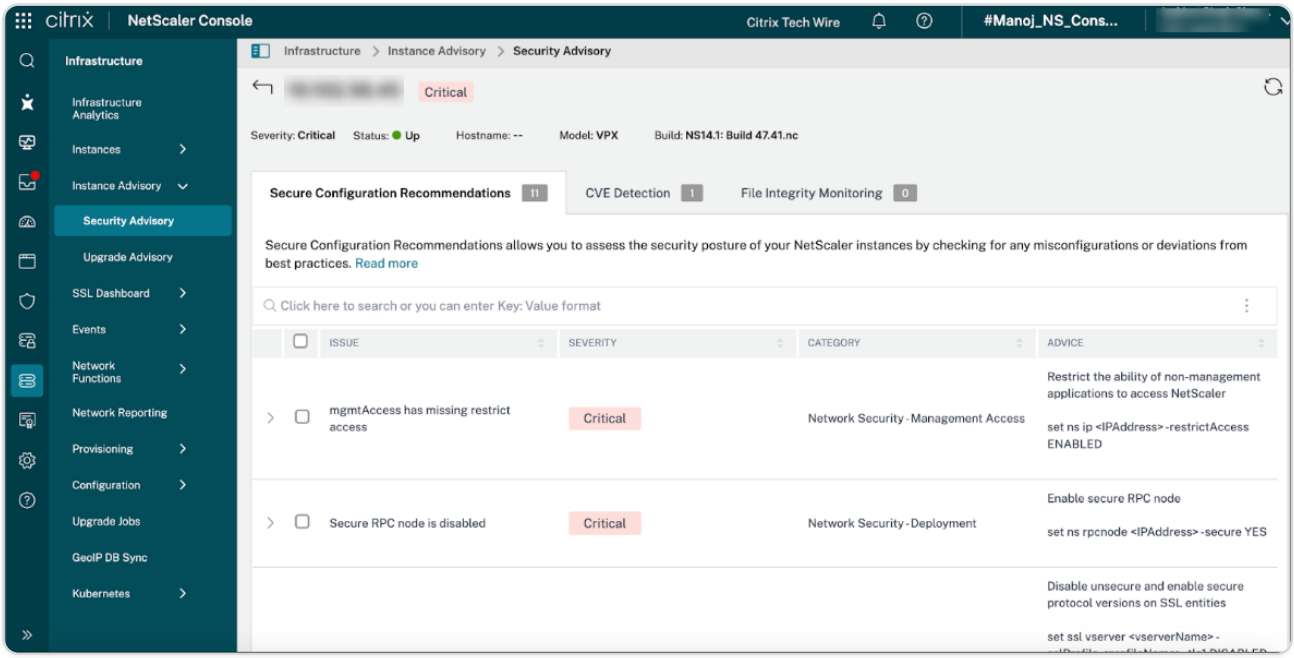
Beyond basic identification, the search also supports filtering by the NetScaler model. This means that you can specify models such as MPX, SDX, or VPX to view only instances belonging to a particular hardware or software category. You can also refine the search by Severity level, allowing you to prioritize instances based on their criticality, from informational alerts to critical warnings.



Remediate configuration recommendations

Once you have evaluated the configuration observations and determined which ones require action, a comprehensive view of recommended configurations is presented. The system then displays a dedicated page, as shown in the following image, displaying the remediation steps tailored to your selections. For instance, if you opt to address only critical severity issues for a specific NetScaler instance (in this particular scenario, the instance with IP address 10.102.56.45), the page dynamically populates with the relevant, high-priority recommendations to guide the remediation process effectively.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Configuration recommendations can be categorized into two types:

- **Recommendations requiring user input**: This category encompasses configuration suggestions that necessitate specific, contextual information or decisions from the NetScaler administrator or security team. These are typically scenarios where a generic default value might not be appropriate, or where the optimal setting depends on the unique operational environment, security policies, or application requirements. The following are a few recommendation examples:
  - **Defining specific IP addresses or IP ranges**: For instance, configuring firewall rules to allow traffic only from trusted internal subnets or specific client IP addresses. The system cannot infer these unique network details.
  - **Setting custom port numbers**: While standard ports exist for many services, applications might be configured to use non-default ports for security or operational reasons. The network admin must specify the port numbers.
  - **Specifying host names or domain names**: When configuring SSL certificates, load balancing virtual servers, or content switching policies, the exact host names or domain names that the NetScaler instance serves or interacts with must be provided by the user.
  - **Providing authentication server details**: Integrating NetScaler with external authentication systems like LDAP, RADIUS, SAML, or OAuth requires the user to input server IP addresses, shared secrets, directory paths, and other protocol-specific details.
  - **Setting up specific URL rewriting or content switching policies**: The precise URLs, patterns, and target destinations for these advanced features are highly specific to the application architecture and must be defined by the user.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **Implications**: These recommendations often involve a deeper understanding of the deployment's specific needs, security policies, and network topology. Errors in user input can lead to service disruptions or security vulnerabilities, emphasizing the need for careful planning and validation. Automated tools or scripts implementing these typically prompt for the necessary parameters, or read them from a configuration file.

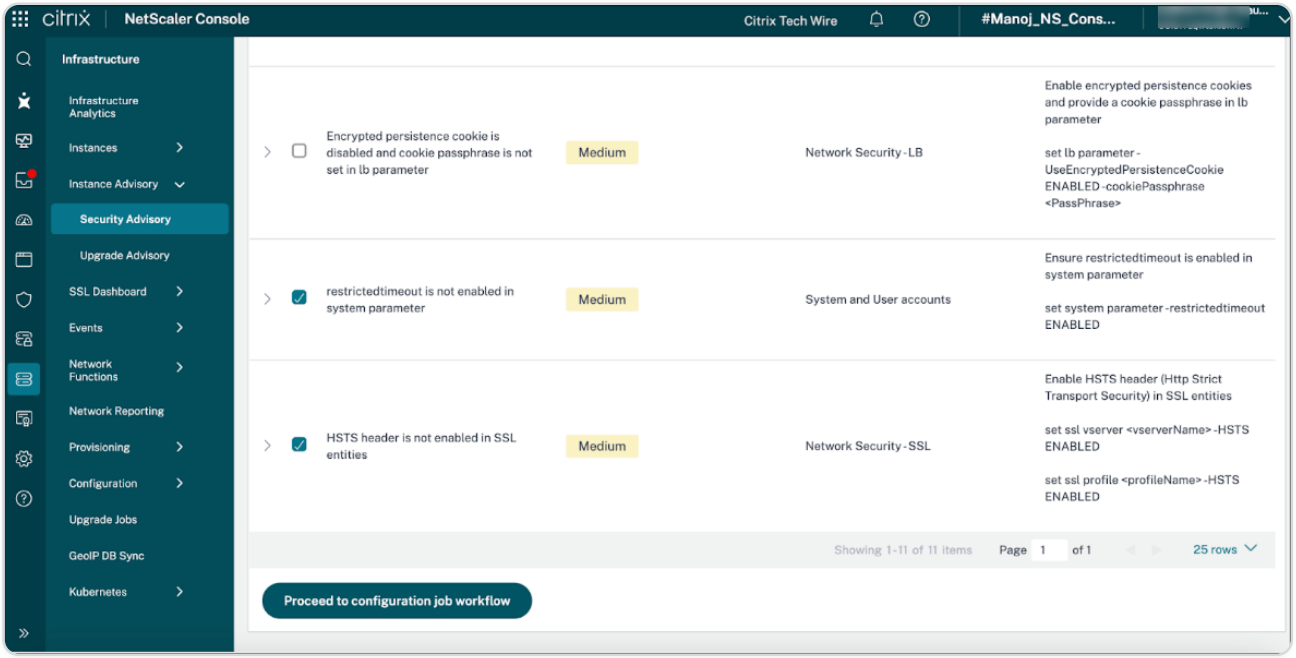
- **Recommendations not requiring user input**: This category includes configuration suggestions that can be applied universally or involve standard best practices that do not depend on unique environmental variables. These are often foundational security enhancements or performance optimizations that are beneficial across most NetScaler deployments. The following are a few recommendation examples:

    - **Disabling weak ciphers or protocols**: Recommend that you disable SSL/TLS versions, such as SSLv3 or TLS 1.0, or specific weak cipher suites (for example, RC4, 3DES), as these are known vulnerabilities and their removal is a universal security best practice. The system does not need specific input to know which ciphers are weak.
    - **Enabling HTTP Strict Transport Security (HSTS)**: This is a policy enforced by web browsers to only interact with a server using secure HTTPS connections. Enabling it is a standard security hardening step.
    - **Setting secure cookie flags (for example, `Secure`, `HttpOnly`)**: These flags enhance the security of session cookies, preventing them from being transmitted over unencrypted channels or accessed through client-side scripts. Their application is a general recommendation.
    - **Enabling common security headers**: Headers like X-Frame-Options, X-Content-Type-Options, and Content-Security-Policy (with a default safe policy) can be recommended without specific user input, as they universally improve client-side security.
    - **Implementing default rate limiting for common attacks**: While custom rate limits might require input, a recommendation to apply a general rate limit to common attack vectors (for example, excessive failed login attempts) might be applicable as a baseline.
    - **Configuring optimal buffer sizes or timeouts**: General performance recommendations related to internal buffer sizes or connection timeouts that are determined by system architecture rather than specific application logic.
    - **Ensuring proper logging levels for security events**: A recommendation to ensure a certain level of logging for security-related events is a general best practice for auditing and incident response.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

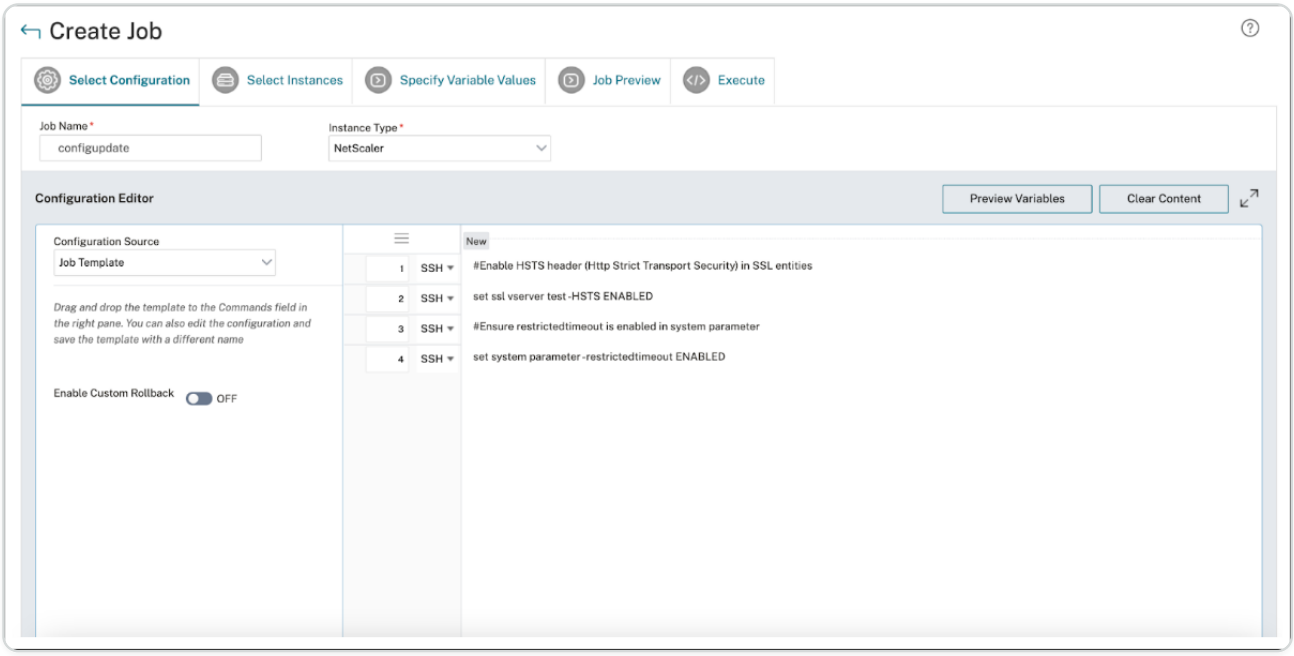
- **Implications**: These recommendations are often excellent candidates for automation or baseline configuration scripts, as they can be applied uniformly across multiple NetScaler instances without requiring manual intervention for specific details. They contribute to a strong security posture by addressing common vulnerabilities and enforcing widely accepted standards.

In summary, classifying configuration recommendations based on user input requirements streamlines the implementation process. Recommendations that require input demand careful data gathering and validation from the user, while those not requiring input can often be applied as standard security baselines or through automated deployment mechanisms.

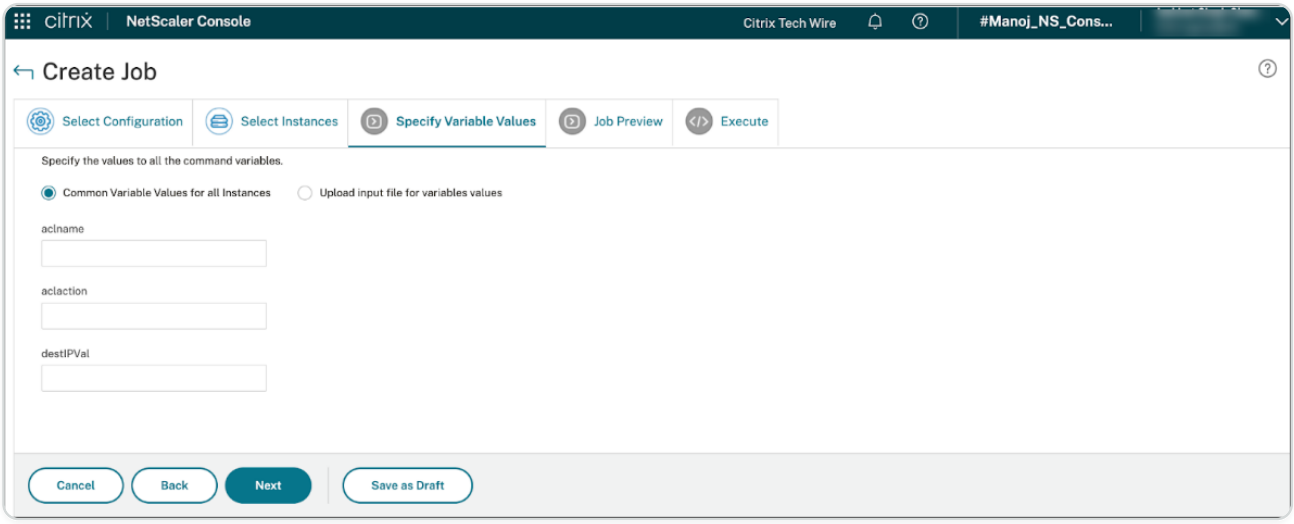


Once a user has decided which configuration to address, the existing configuration job workflow takes over to push the configuration changes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For instance, here's an example of a configuration recommendation that requires user input. One can enter configuration values one by one or choose to upload a file containing the configuration values as shown in the following image.



CVE Detection

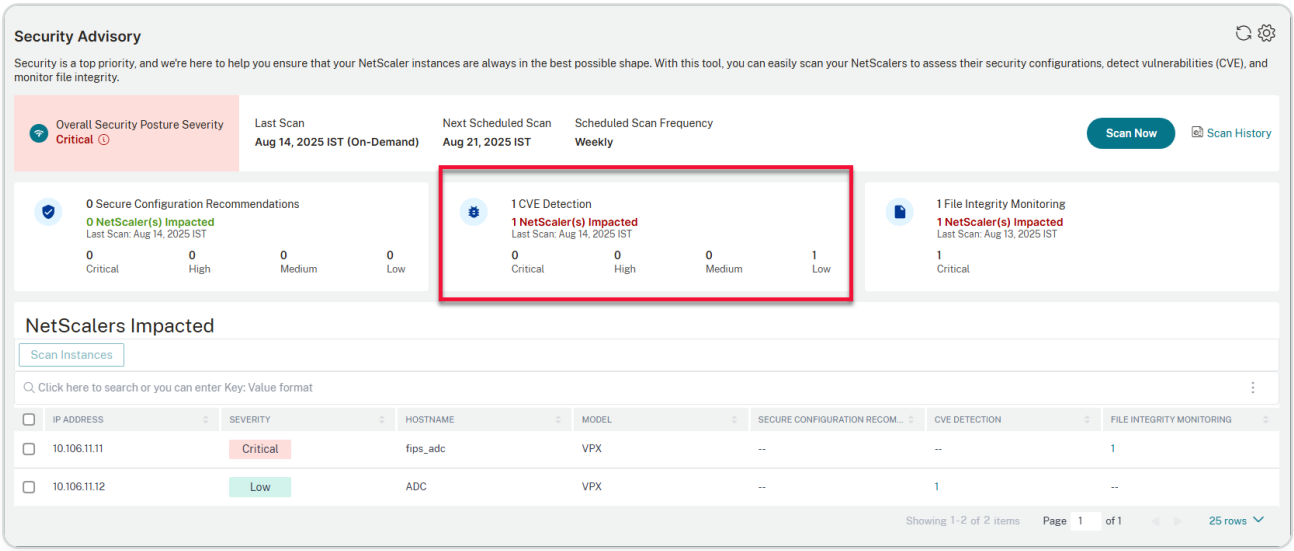
NetScaler detects CVEs by scanning instance versions, configurations, and system files to identify vulnerabilities. It uses an updated CVE repository and provides detailed impact analysis and remediation suggestions.

The **CVE Detection** section in the **Security Advisory** dashboard lists the following:

- Number of CVEs detected
- Number of NetScaler instances impacted
- Date when the last scan was run

© 1997–2026 Citrix Systems, Inc. All rights reserved.

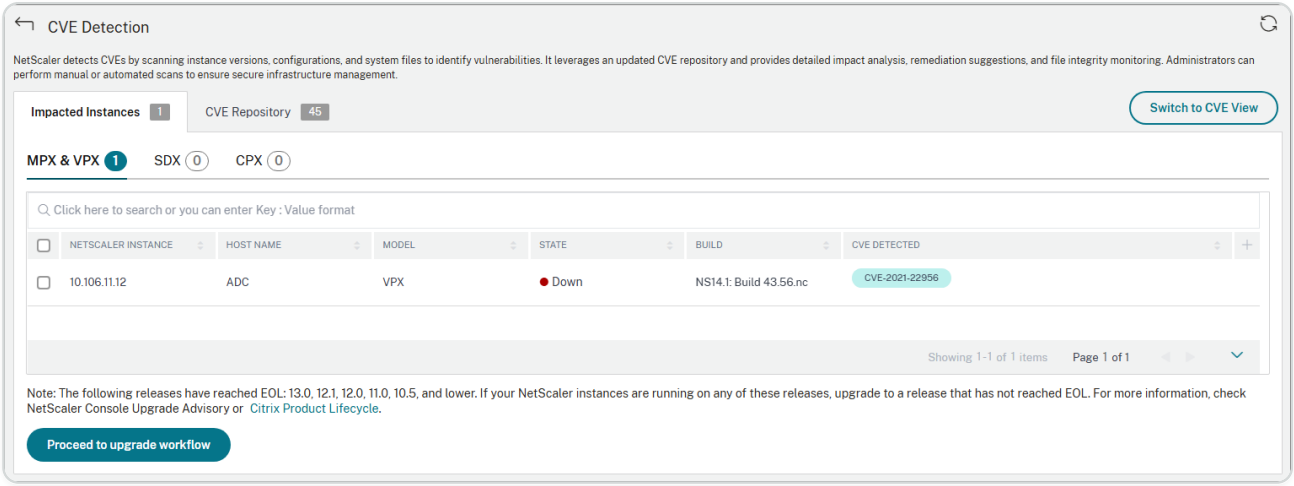
- Impacted NetScaler instances categorized under Critical, High, Medium, and Low severity



As an administrator, you can allow NetScaler to run the system scans that are scheduled periodically or you can choose to run on-demand scans based on your need.

- **System scan** - Scans all managed instances by default. NetScaler Console decides the date and time of system scans, and you cannot change them.
- **On-demand scan** - You can manually scan the instances when required. If the time elapsed after the last system scan is significant, you can run an on-demand scan to assess the current security posture. Or scan after a remediation has been applied, to assess the revised posture. To run the on-demand scan, click **Scan now** on the securty advisory.

You can click the **CVE Detection** section to view detailed information.



The **CVE Detection** section has two views:

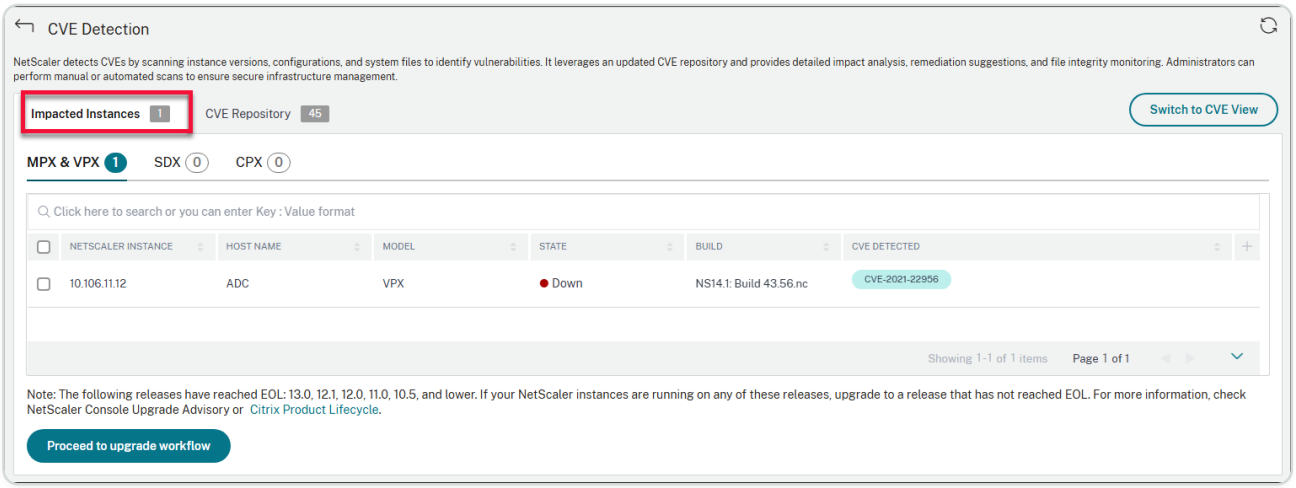
- Instance view
- CVE view

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Instance view

The instance view contains **Impacted Instances** and **CVE Repository** tabs.

The **Impacted Instances** tab displays the list of impacted NetScaler instances.



The impacted instances are categorized based on the following form factors:

- MPX and VPX
- SDX
- CPX
- BLX

You can also search the instances based on the following:

- CVE Detected
- Host Name
- Model
- NetScaler Instance
- State

The table shows the following details:

- NetScaler IP address
- Host name
- NetScaler model number
- State of the NetScaler
- Software version and build
- List of CVEs impacting the NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Most of the CVEs need upgrade as a remediation, while others need upgrade and an additional step as remediation.

- For CVE-2020-8300 remediation, see Remediate vulnerabilities for CVE-2020-8300.
- For CVE-2021-22927 and CVE-2021-22920, see Remediate vulnerabilities for CVE-2021-22927 and CVE-2021-22920.
- For CVE CVE-2021-22956, see Identify and remediate vulnerabilities for CVE-2021-22956
- For CVE CVE-2022-27509, see Remediate vulnerabilities for CVE-2022-27509

NOTE

If your NetScaler instances have customizations, see Upgrade considerations for customized NetScaler configurations before planning NetScaler upgrade.

You can upgrade the vulnerable NetScaler instances to a release and build that has the fix. To upgrade, perform one of the following:

- **Upgrade workflow** - Select an instance and click **Proceed to upgrade workflow**.
- **Configuration job workflow** - Select an instance and click **Configuration job workflow**.

The upgrade workflow starts and the vulnerable NetScaler is auto-populated as the target NetScaler. For more information on how to use NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.

NOTE:

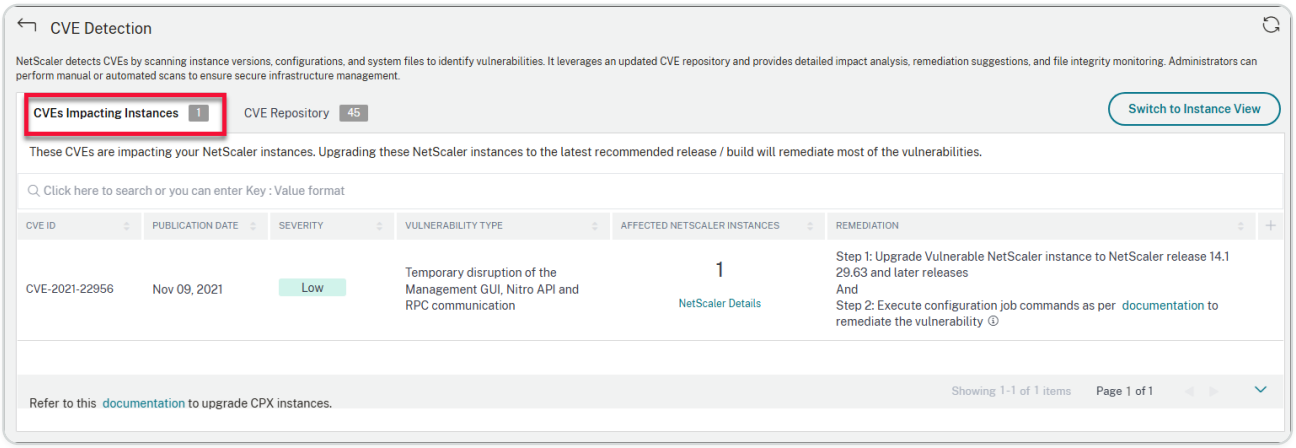
- The releases 13.0, 12.1, 12.0, 11.0, 10.5, and lower are already end of life (EOL). If your NetScaler instances are running on any of these releases, upgrade to a supported release.
- The release and build to which you want to upgrade is at your discretion. See the advice under the remediation column to know which release and builds have the security fix. And accordingly select a supported release and build, which has not reached end of life yet.

To switch to CVE view, click **Switch to CVE View**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CVE view

The CVE view displays the results of all CVEs impacting your infrastructure and all the NetScaler instances getting impacted and suggests remediation. You can use this information to apply remediation to fix security risks.



The table showing the number of CVEs impacting the NetScaler instances has the following details.

- **CVE ID**: The ID of the CVE that impacts the instances.
- **Publication date**: The date the security bulletin was released for that CVE.
- **Severity score**: The severity type (high/medium/critical) and score. To see the score, hover over the severity type.
- **Vulnerability type**: The type of vulnerability for this CVE.
- **Affected NetScaler instances**: The instance count that the CVE ID is impacting. On hover over, the list of NetScaler instances appears.
- **Remediation**: The available remediations, which are upgrading the instance (usually) or applying configuration packs.

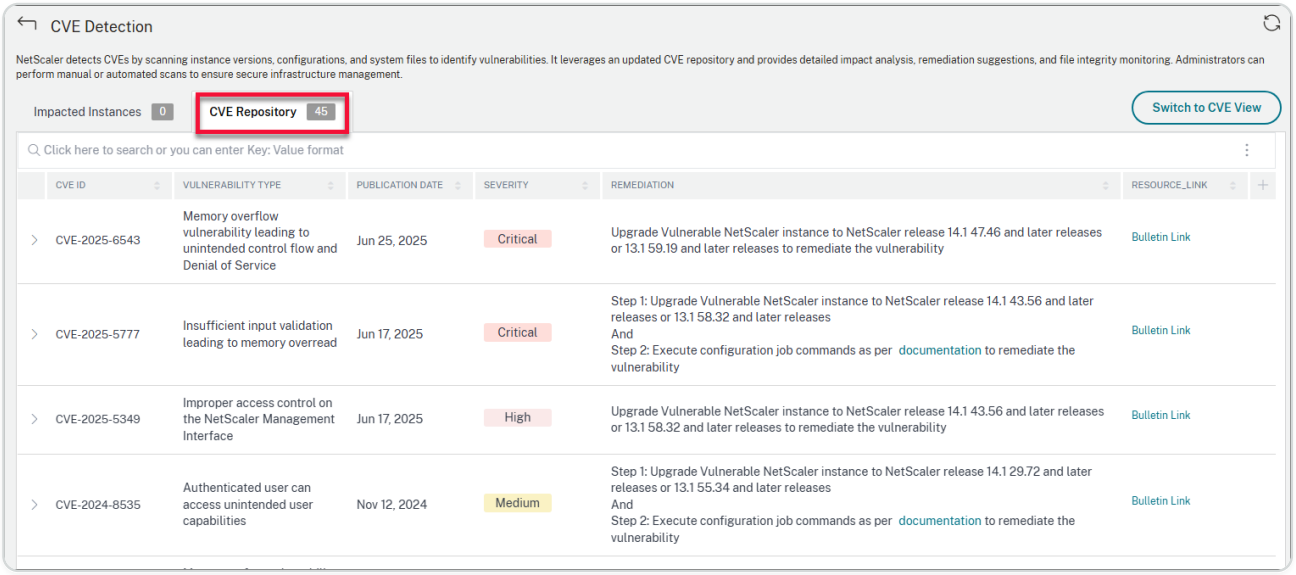
The same instance can be impacted by multiple CVEs. This table helps you see how many instances one particular CVE or multiple selected CVEs are impacting. To check the IP address of the impacted instance, hover over NetScaler Details under **Affected NetScaler Instances**. To check the details of the impacted instance, click **View Affected Instances** at the bottom of the table. You can also add or remove columns in the table by clicking the plus sign.

CVE repository

Both instance view and CVE view contain the **CVE Repository** tab. This tab gives a detailed view of all the NetScaler related CVEs that Citrix has announced since Dec 2019, that might impact your NetScaler infrastructure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- CVE IDs
- Vulnerability type
- Publication date
- Severity level
- Remediation
- Links to security bulletins



You can use this view to understand the CVEs in the security advisory scope and to learn more about the CVE. For information on CVEs that are not supported, see Unsupported CVEs in Security Advisory.

Points to note

- Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.
- Instances supported for CVE detection: all NetScaler (SDX, MPX, VPX) and Gateway.
- Instances supported for File Integrity Monitoring: MPX, VPX instances, and Gateway.
- CVEs supported: All CVEs after Dec 2019.

NOTE:

The detection and remediation of vulnerabilities impacting the NetScaler Gateway plug-in for Windows is not supported by the NetScaler Console Security Advisory. For information on CVEs that are not supported, see Unsupported CVEs in Security Advisory.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler Console security advisory doesn’t account for any kind of feature misconfiguration while identifying the vulnerability.
- NetScaler Console security advisory only supports the identification and remediation of the CVEs. It does not support identification and remediation of the security concerns that are highlighted in the Security article.
- Scope of NetScaler, Gateway releases: The feature is limited to main builds. Security advisory does not include any special build in its scope.
    - Security advisory is not supported in the Admin partition.
- The following types of scan are available for CVEs:
    - **Version scan**: This scan needs NetScaler Console to compare the version of an NetScaler instance with the versions and builds on which the fix is available. This version comparison helps NetScaler Console security advisory identify whether the NetScaler is vulnerable to the CVE. For example, if a CVE is fixed on an NetScaler release and build xx.yy, the security advisory considers all the NetScaler instances on builds lesser than xx.yy as vulnerable. Version scan is supported today in security advisory.
    - **Config scan**: This scan needs NetScaler Console to match a pattern specific to the CVE scan with NetScaler config file (`nsconf`). If the specific config pattern is present in the NetScaler ns.conf file, the instance is considered vulnerable for that CVE. This scan is typically used with version scan. Config scan is supported today in security advisory.
    - **Custom scan**: This scan needs NetScaler Console to connect with the managed NetScaler instance, push a script to it, and run the script. The script output helps NetScaler Console identify whether the NetScaler is vulnerable to the CVE. Examples include specific shell command output, specific CLI command output, certain logs, and the existence or content of certain directories or files. For CVEs that require custom scans, the script runs every time your scheduled or on-demand scan runs. Learn more about the data collected and options for specific custom scans in the Security Advisory documentation for that CVE.
- Scans do not impact production traffic on NetScaler and do not alter any NetScaler configuration on NetScaler.
- NetScaler Console Security Advisory does not support CVE mitigation. If you have applied mitigation (temporary workaround) to the NetScaler instance, the NetScaler Console still identifies the NetScaler as a vulnerable NetScaler until you have completed remediation.
- For the FIPS instances, the CVE scan is not supported.

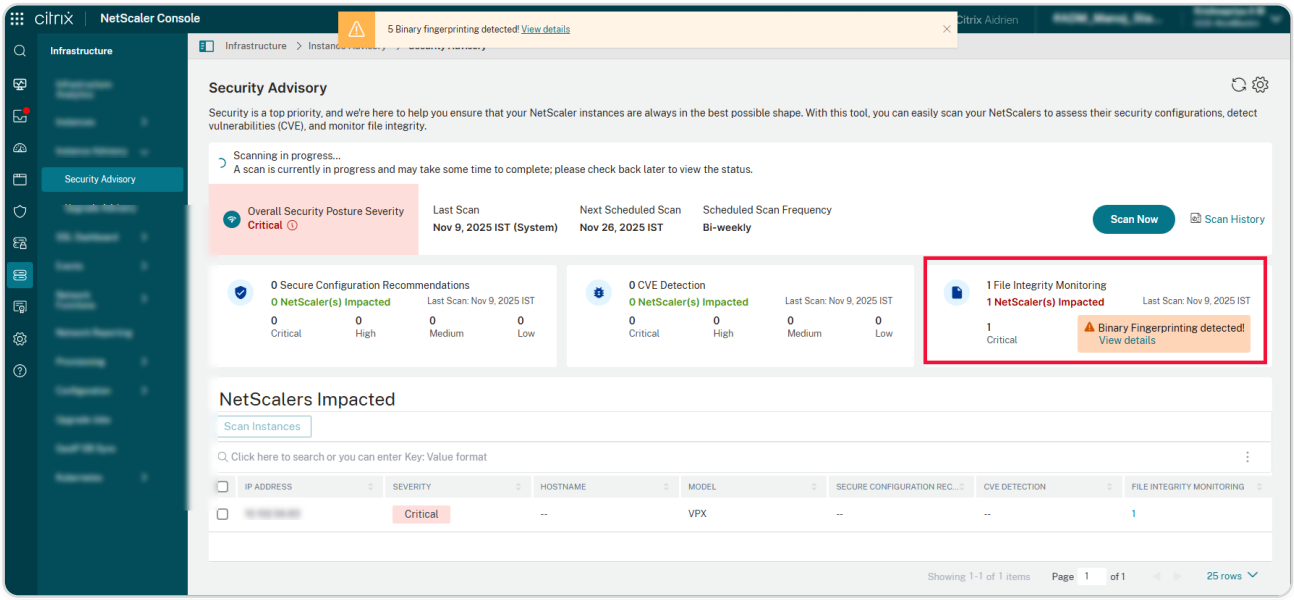
© 1997–2026 Citrix Systems, Inc. All rights reserved.

File integrity monitoring

File integrity monitoring enables you to identify if any changes or additions have been made to your NetScaler file system. This feature assesses the integrity of NetScaler files by comparing the binary hash value of your current NetScaler build with the original binary hash linked to the same NetScaler build.

The **File Integrity Monitoring** section in the **Security Advisory** dashboard lists the following:

- Number of issues detected
- Number of NetScaler instances impacted
- Date when the last scan was run
- Impacted NetScaler instances categorized under Critical, High, Medium, and Low severity
- Impacted NetScaler instances that have reported issues using binary signing and verification



As an administrator, you can allow NetScaler to run the system scans that are scheduled periodically or you can choose to run on-demand scans based on your need.

- **System scan** - Scans all managed instances by default. NetScaler Console decides the date and time of system scans and are disabled by default.
- **On-demand scan** - You can trigger the scan manually when required. To run the on-demand scan, click **Scan now** on the security advisory dashboard.

You can click the **File Integrity Monitoring** section to view detailed information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

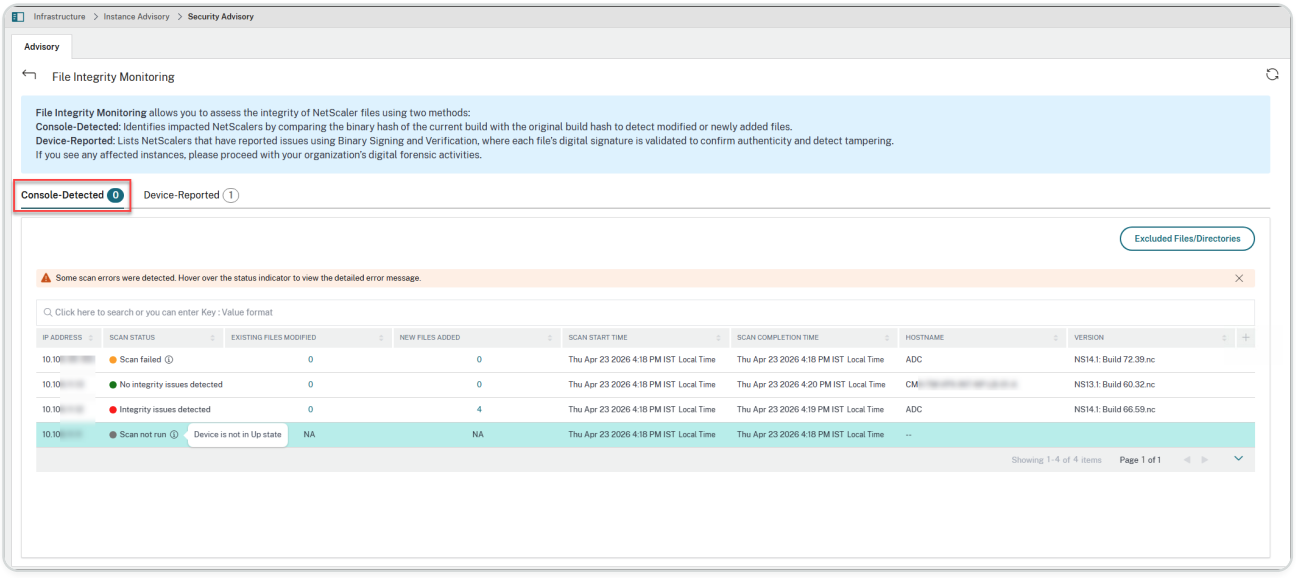
Console-Detected

The **Console-Detected** tab lists the impacted NetScaler instances by comparing the binary hash of the current build with the original build hash to detect modified or newly added files. The table displays the following details:

- IP address - The IP address of the impacted instances.
- Scan status - Displays scan error results.
- Existing file modified -The list of the existing files that are modified.
- New files added - The list of new files added.
- Scan time - The time of the last scan.
- Host name - The host name of the impacted NetScaler.
- Modal - The modal name of the impacted NetScaler.

Scan error results are displayed within the main dashboard view so that you need not click the individual scan results or line items to access error details. Any integrity issues, such as hash mismatches or scan errors, are presented in a clear, accessible format on the dashboard helping you identify and understand problems quickly.

Click the numbers under **Existing files modified** and **New files added** to view details.



You can create a custom allow list and exclude specific files from file integrity monitoring scans. By defining which files to exclude from the scan, you can streamline monitoring and reduce unnecessary alerts for trusted files.

To exclude specific files from file integrity monitoring scans:

1. Click **Exclude Files/Directories**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

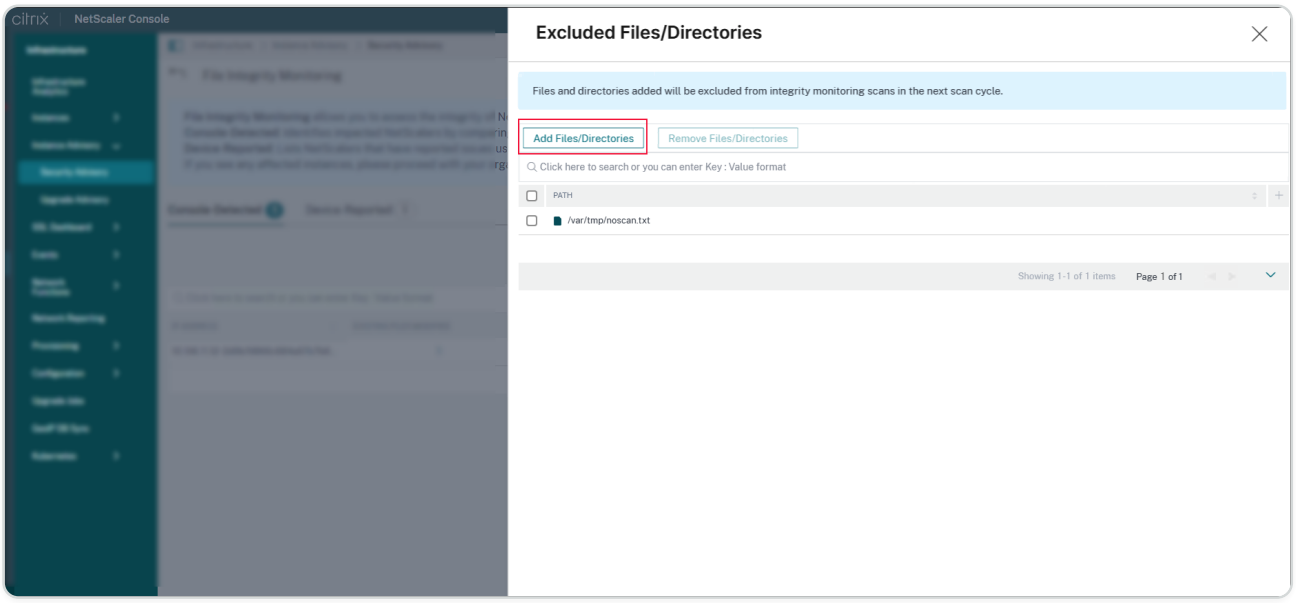
2. Select the required files or directories.

   or

   click **Add Files/Directories** to add new files. You can add standard shell glob patterns and exclude any paths that correspond to the defined criteria. When a directory is added, all its files are excluded from the scan. Click **Add**.

   You can also perform a search to locate particular files or folders. You can also find the exclude list paths by entering a part of a file or folder in the search bar under the `path` option. The search functionality makes managing and reviewing excluded paths easier.

If you do not want to exclude the files from scan, you can select the required files or directories and click **Remove Files/Directories**. The specified files or directories are included in the next scheduled scan.



Points to note

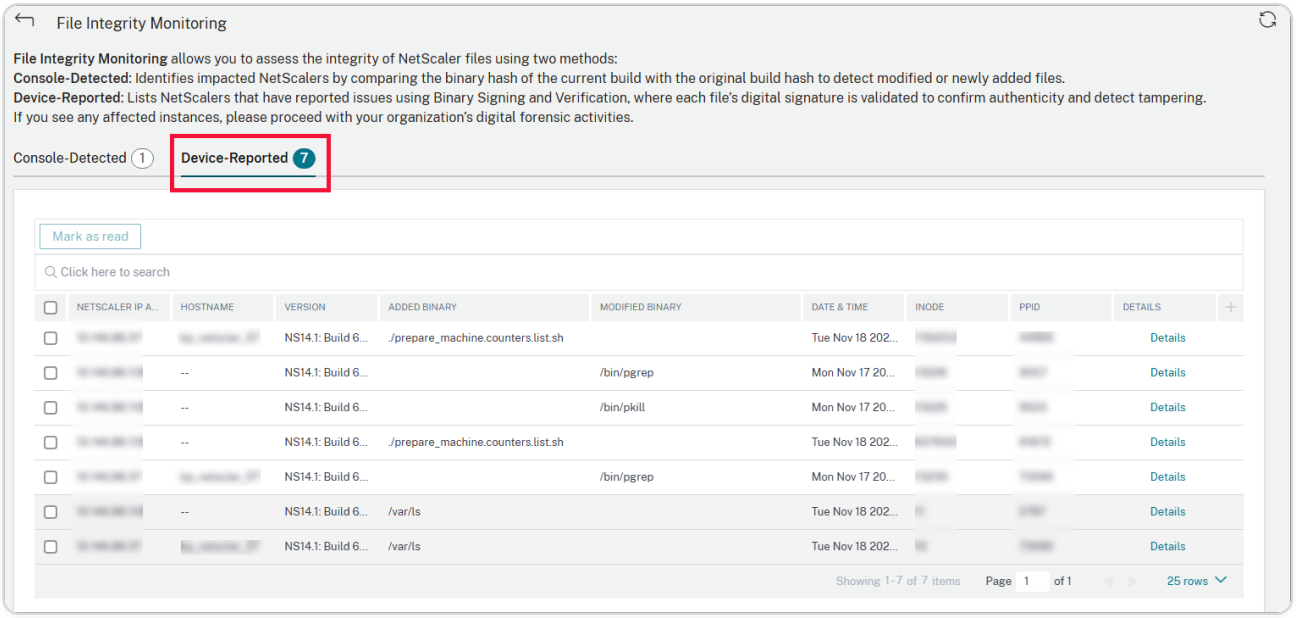
- Instances supported for File Integrity Monitoring: MPX, VPX instances, and Gateway.
- The following scan is available for File Integrity Monitoring:
  - **File Integrity Monitoring scan**: This scan needs the NetScaler Console to connect with the managed NetScaler instance. NetScaler Console does a comparison of the hash values by running a script in NetScaler and collecting the current binary hash values for the NetScaler system files. After the comparison, NetScaler Console provides the result with total number of existing files modified and total number of newly added files. As an administrator, you can contact your organization digital forensics for further investigations on the scan results.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The following is the list of unsupported platforms: BLX

Device-Reported

The **Device-Reported** tab lists the NetScaler instances that have reported issues using binary signing and verification. With this verification, each file's digital signature is validated to confirm authenticity and detect tampering. If you see any affected instances, you can proceed with your organization's digital forensic activities. The table lists the impacted NetScaler instances along with other details such as the host name, added binary, modified binary. You can click **Details** corresponding to the required instance to view detailed information.



Indicators of Compromise detection in NetScaler Console

The Indicators of Compromise (IoC) detection feature in NetScaler Console is designed to detect if your NetScaler appliances have potentially been affected due to a vulnerability.

If there are CVE events, one of the first concerns is that malicious actors have been able to exploit the vulnerability. An exploit causes catastrophic damage to a customer’s business and hence it’s critical to detect such incidents immediately. Indicators of Compromise have been distributed for NetScaler in the past through support channels, which meets the customer need but comes at an additional effort of going through the support process of raising a ticket, speaking with a support professional, which might sometimes not be ideal. The Indicator of Compromise detection feature in NetScaler Console is designed to short-circuit the current support-oriented process and help a customer in making a quick assessment of their NetScaler infrastructure.

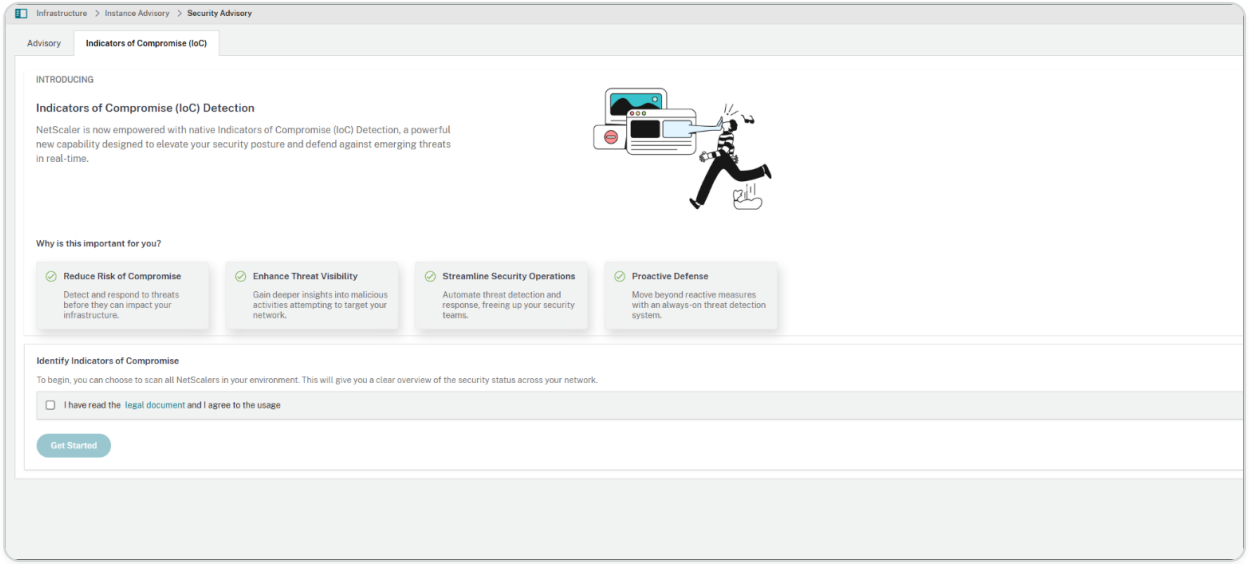
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prerequisites

This feature requires you to send product usage telemetry. For more information on NetScaler telemetry, see `<https://docs.netscaler.com/en-us/netscaler-application-delivery-management-software/current-release/ns-telemetry.html>`.

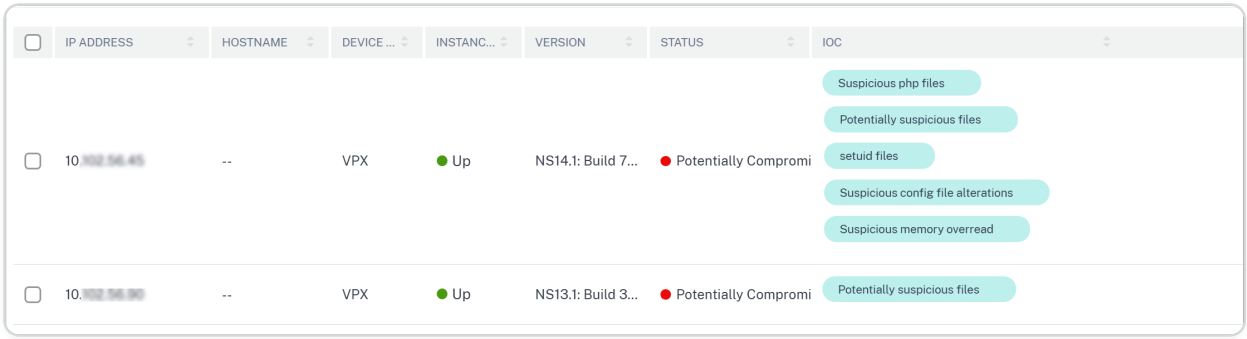
Benefits

- You can run compromise detection scans from the NetScaler Console **Security Advisory** page.

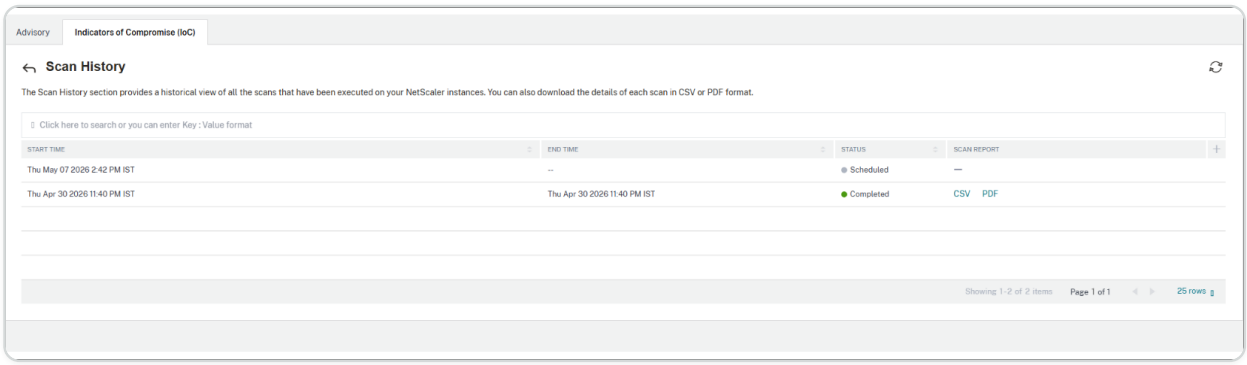


- The scan provides one of the following results:
  - **Potentially Compromised** – If the detection logic has detected a potential compromise for a CVE.
  - **No Compromise Detected** – If the detection logic hasn't detected any compromise.
  - **Skipped** – If the scan has been manually skipped for a particular NetScaler instance.
  - **Failed to Execute** – If the scan did not run successfully.
  - **Execution in Progress** – If the scan is in progress.
- The IoC logic keeps getting updated as more IoC's are discovered. In such a case the home page shows that an update is available.
- Whenever an update is available to the IoC detection logic, you can see it on the landing page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Results of older scans are saved and can be viewed at any point.



- The solution uses a hub-and-spoke architecture where a central cloud service ingests assets from a secure cloud location, and installs them onto the target devices.

NOTE:

The IoC Information does not encompass all techniques, tactics, or procedures (“TTPs”) that threat actors might use when targeting relevant environments. Also, threat actors change TTPs and infrastructure frequently. For these reasons and others, the IoC Information might be of limited forensic value and might fail to identify actual compromises. You are advised to retain the services of experienced forensic investigators to assess your environment.

Remediate vulnerabilities

NetScaler detects CVEs and provides remediation suggestions the same. This topic lists the remediations suggested for the following CVEs:

- Remediate vulnerabilities for CVE-2026-88779
- Remediate vulnerabilities for CVE-2026-88778
- Remediate vulnerabilities for CVE-2026-88777
- Remediate vulnerabilities for CVE-2026-88776
- Remediate vulnerabilities for CVE-2026-88775

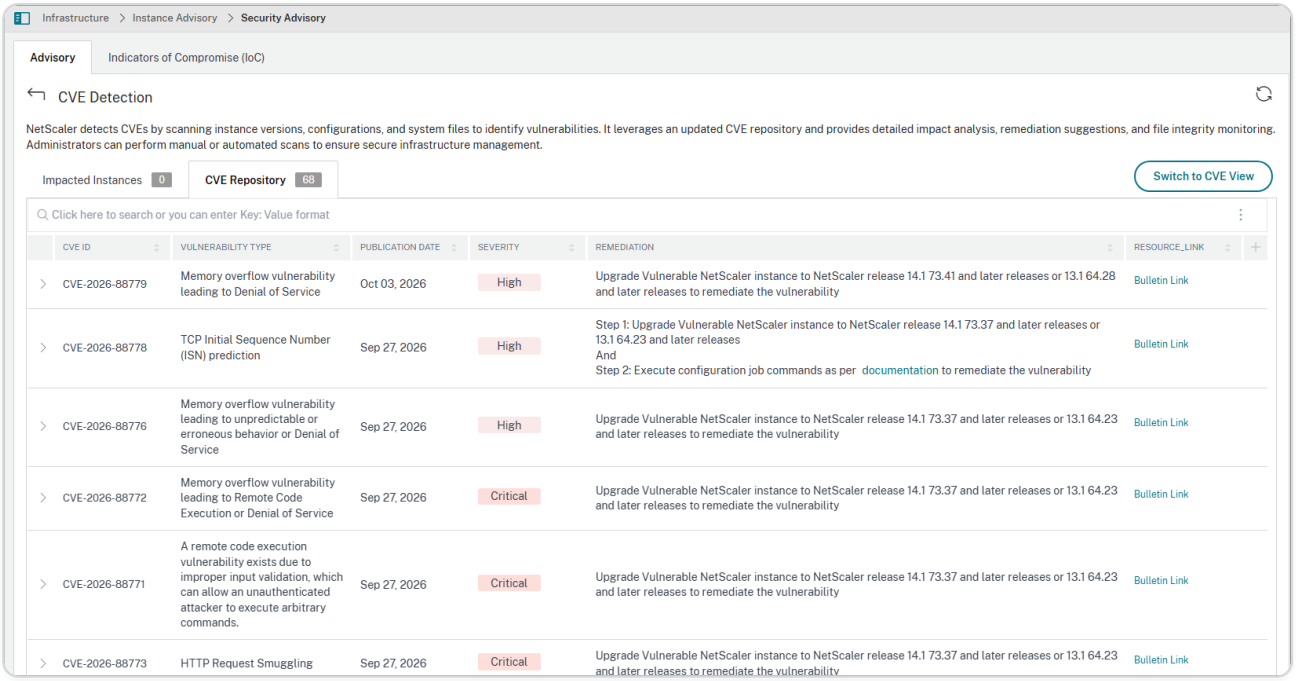
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Remediate vulnerabilities for CVE-2026-88774
- Remediate vulnerabilities for CVE-2026-88773
- Remediate vulnerabilities for CVE-2026-88772
- Remediate vulnerabilities for CVE-2026-88771
- Remediate vulnerabilities for CVE-2026-19490
- Remediate vulnerabilities for CVE-2026-19489
- Remediate vulnerabilities for CVE-2026-13474
- Remediate vulnerabilities for CVE-2026-10817
- Remediate vulnerabilities for CVE-2026-10816
- Remediate vulnerabilities for CVE-2026-8655
- Remediate vulnerabilities for CVE-2026-8452
- Remediate vulnerabilities for CVE-2026-8451
- Remediate vulnerabilities for CVE-2026-4368
- Remediate vulnerabilities for CVE-2026-3055
- Remediate vulnerabilities for CVE-2025-12101
- Remediate vulnerabilities for CVE-2025-8424
- Remediate vulnerabilities for CVE-2025-7776
- Remediate vulnerabilities for CVE-2025-7775
- Remediate vulnerabilities for CVE-2025-6543
- Remediate vulnerabilities for CVE-2025-5349
- Remediate vulnerabilities for CVE-2025-5777
- Remediate vulnerabilities for CVE-2024-8535
- Remediate vulnerabilities for CVE-2020-8300
- Remediate vulnerabilities for CVE-2021-22927 and CVE-2021-22920
- Identify and remediate vulnerabilities for CVE-2021-22956
- Identify and remediate vulnerabilities for CVE-2022-27509

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Identify and remediate vulnerabilities for CVE-2026-88779

In the NetScaler Console® security advisory dashboard, click **CVE Detection**. On the **Impacted Instances** tab, search for CVE-2026-88779. The list of NetScaler instances that are impacted by CVE-2026-88779 is displayed.



For more information about the security advisory dashboard, see Security Advisory.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2026-88779 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2026-88779

For CVE-2026-88779 impacted NetScaler instances, the remediation is a single-step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix.

In the GUI, under **CVE Detection > Impacted Instances**, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

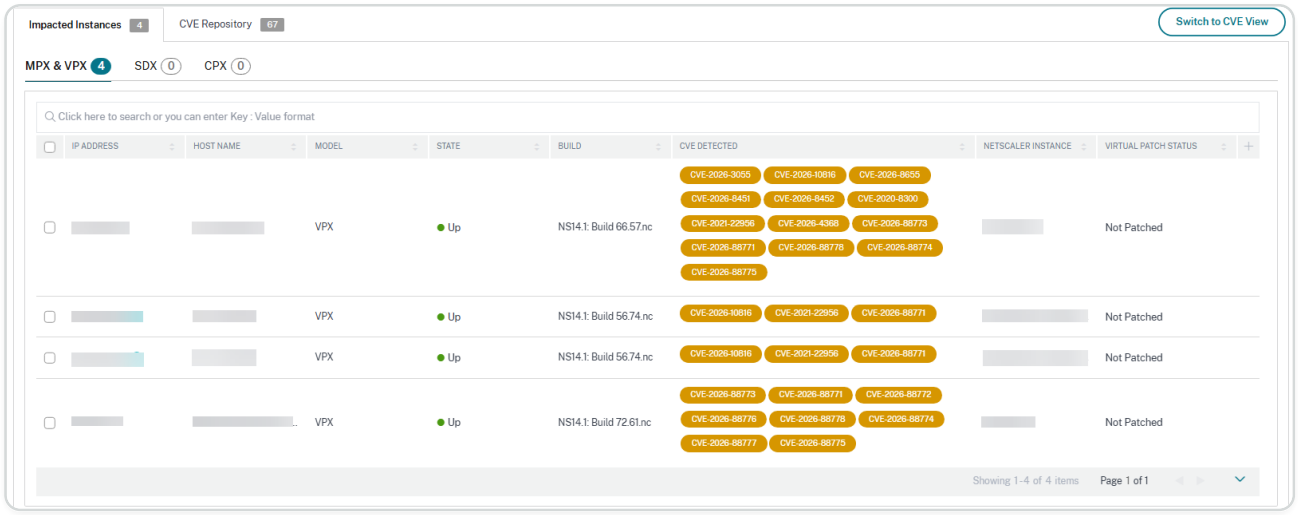
For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This step can be done at once for all the vulnerable NetScaler instances. For more information, see CVE Detection.

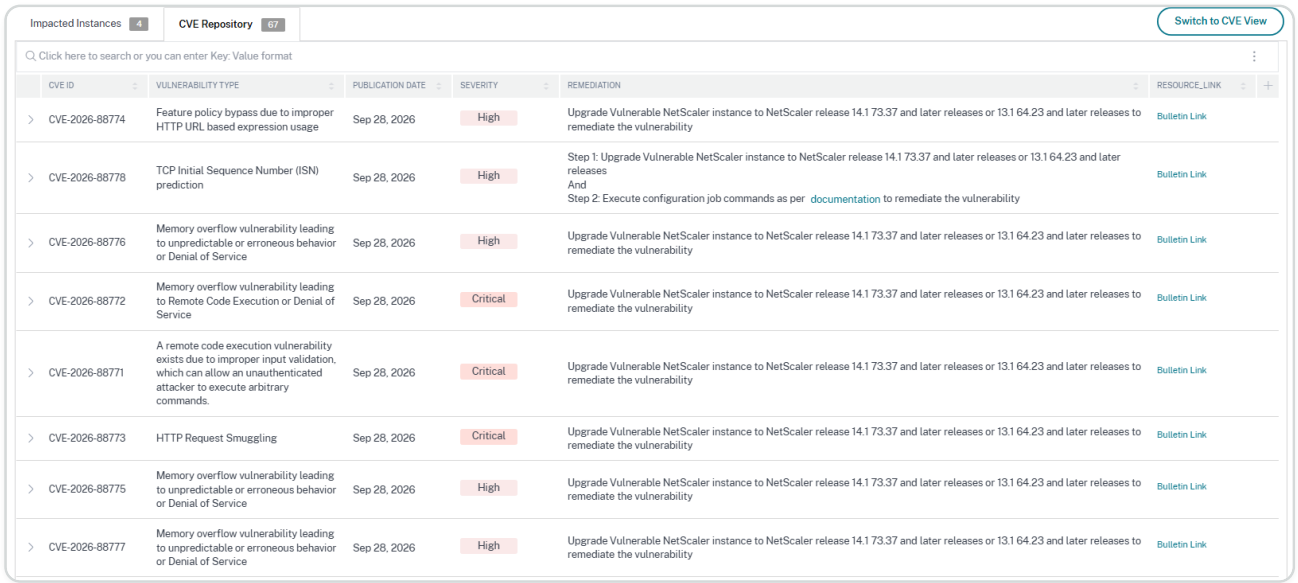
Remediate vulnerabilities for CVE-2026-88778

In the NetScaler Console security advisory dashboard, under **Current CVEs** `<number of>` **NetScaler instances are impacted by CVEs**, you can see all the instances vulnerable due to CVE-2026-88778. To check the details of the instances impacted by the CVEs, select CVE-2026-88778 and click **View Affected Instances**.



Remediate CVE-2026-88778

For CVE-2026-88778-impacted NetScaler instances, the remediation is a two-step process. In the GUI, under **Current CVEs > NetScaler instances are impacted by CVEs**, you can see step 1 and 2.



The two steps include:

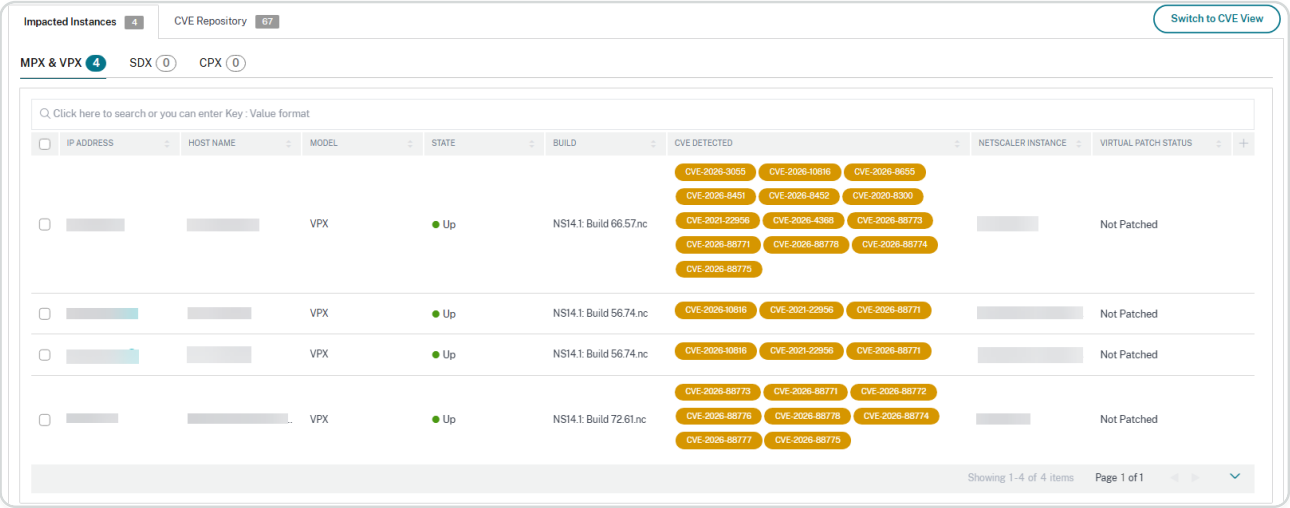
© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Upgrading the vulnerable NetScaler instances to a release and build that has the fix.
2. Applying the required configuration commands using the customizable built-in configuration template in configuration jobs.

Under **Current CVEs> NetScaler instances impacted by CVEs**, you see two separate workflows for this 2-step remediation process: which are **Proceed to upgrade workflow** and **Proceed to configuration job workflow**.

Step 1: Upgrade the vulnerable NetScaler instances

To upgrade the vulnerable instances, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.



For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

NOTE:

This step can be done at once for all the vulnerable NetScaler instances.

Step 2: Apply configuration commands

After you've upgraded the impacted instances, in the **`<number of>` NetScaler instances impacted by CVEs** window, select the instance impacted by CVE-2026-88778 and click **Proceed to configuration job workflow**. The workflow includes the following steps.

1. Customizing the configuration.
2. Reviewing the auto-populated impacted instances.
3. Specifying inputs for variables for the job.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

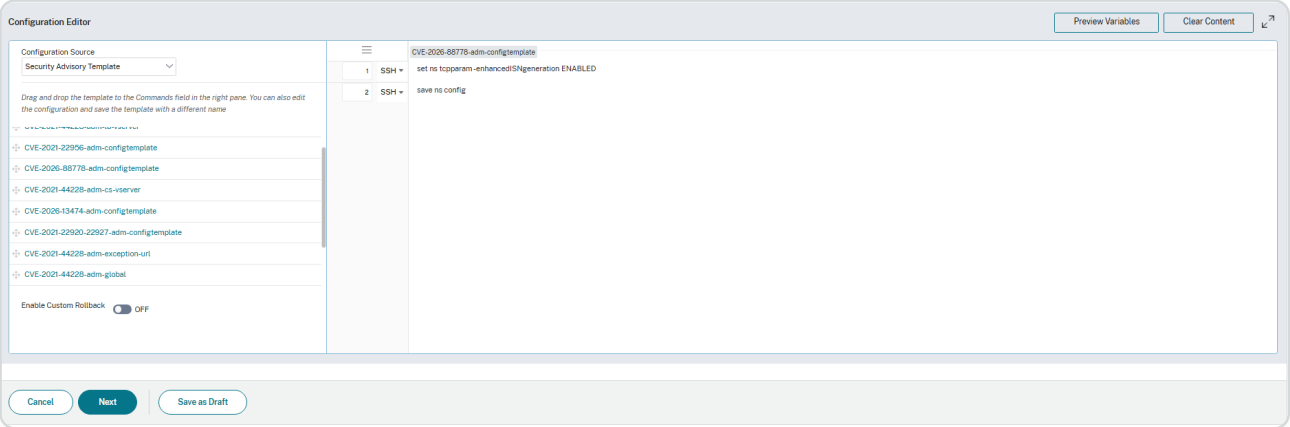
4. Reviewing the final config with variable inputs populated.
5. Running the job.

Keep the following point in mind before you select an instance and click **Proceed to configuration job workflow**:

- For multiple NetScaler instances that are impacted by CVE-2026-88778 only: you can run config jobs on all instances at once. For example, you've NetScaler 1, NetScaler 2, and NetScaler 3, and all of them are impacted only by CVE-2026-88778. Select all these instances and click **Proceed to configuration job workflow**, and the built-in configuration template auto-populates under **Select configuration**.

Step 1: Select configuration

In the configuration job workflow, the built-in configuration base template auto-populates under **Select configuration**.



Step 2: Select the instance

The impacted instance is auto-populated under **Select Instances**. Select the instance. Click **Next**. In the next step preview the configurations. Click **Next**.

NOTE:

For NetScaler instances in cluster mode, using security advisory, NetScaler Console supports running the config job only on the cluster configuration coordinator (CCO) node. Run the commands on non-CCO nodes separately.

Step 3: Run the configuration

Click **Finish** to run the configuration job.

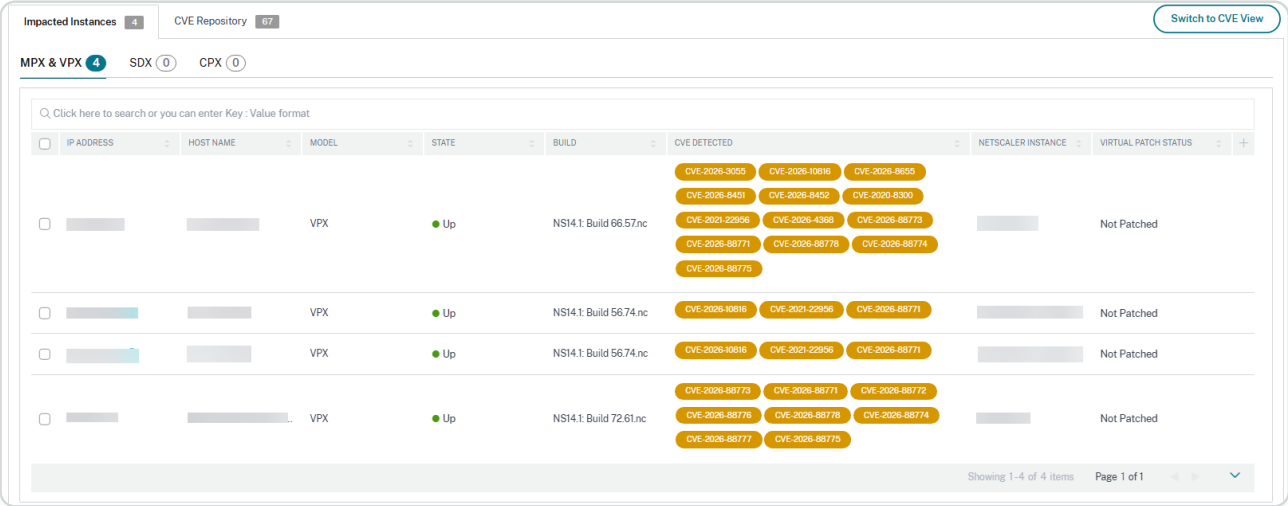
After the job is run, it appears under **Infrastructure > Configuration > Configuration Jobs**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After completing the two remediation steps for all vulnerable NetScaler instances, you can run an on-demand scan to see the revised security posture.

Identify and remediate vulnerabilities for CVE-2026-88777

In the NetScaler Console® security advisory dashboard, click **CVE Detection**. On the **Impacted Instances** tab, search for CVE-2026-88777. The list of NetScaler instances that are impacted by CVE-2026-88777 is displayed.



For more information about the security advisory dashboard, see Security Advisory.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2026-88777 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2026-88777

For CVE-2026-88777 impacted NetScaler instances, the remediation is a single-step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix.

In the GUI, under **CVE Detection > Impacted Instances**, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

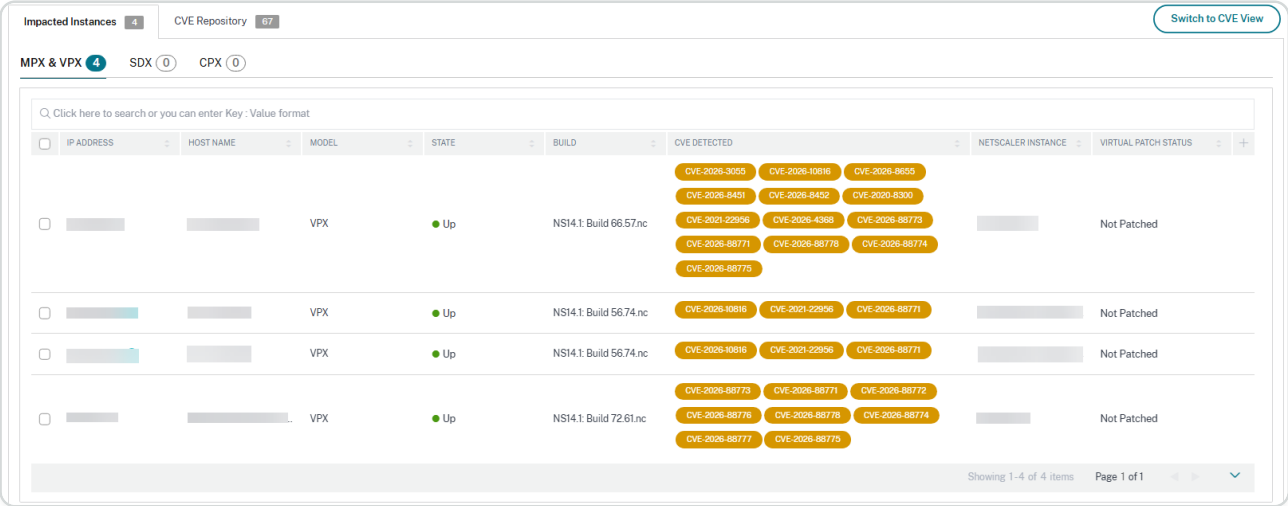
For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This step can be done at once for all the vulnerable NetScaler instances. For more information, see CVE Detection.

Identify and remediate vulnerabilities for CVE-2026-88776

In the NetScaler Console® security advisory dashboard, click **CVE Detection**. On the **Impacted Instances** tab, search for CVE-2026-88776. The list of NetScaler instances that are impacted by CVE-2026-88776 is displayed.



For more information about the security advisory dashboard, see Security Advisory.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2026-88776 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2026-88776

For CVE-2026-88776 impacted NetScaler instances, the remediation is a single-step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix.

In the GUI, under **CVE Detection > Impacted Instances**, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

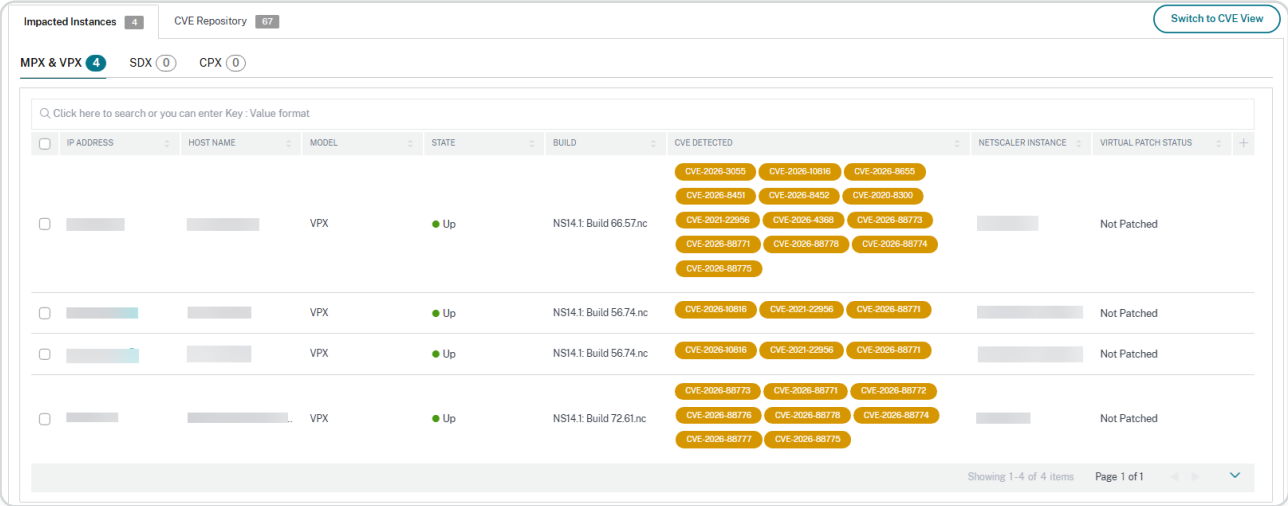
For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This step can be done at once for all the vulnerable NetScaler instances. For more information, see CVE Detection.

Identify and remediate vulnerabilities for CVE-2026-88775

In the NetScaler Console® security advisory dashboard, click **CVE Detection**. On the **Impacted Instances** tab, search for CVE-2026-88775. The list of NetScaler instances that are impacted by CVE-2026-88775 is displayed.



For more information about the security advisory dashboard, see Security Advisory.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2026-88775 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2026-88775

For CVE-2026-88775 impacted NetScaler instances, the remediation is a single-step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix.

In the GUI, under **CVE Detection > Impacted Instances**, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

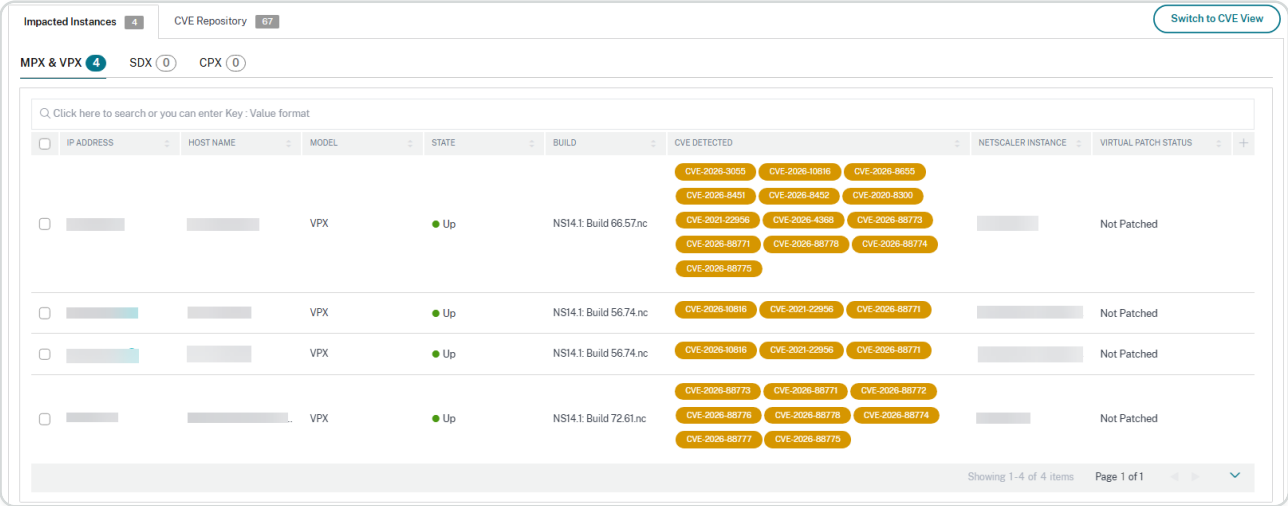
For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This step can be done at once for all the vulnerable NetScaler instances. For more information, see CVE Detection.

Identify and remediate vulnerabilities for CVE-2026-88774

In the NetScaler Console® security advisory dashboard, click **CVE Detection**. On the **Impacted Instances** tab, search for CVE-2026-88774. The list of NetScaler instances that are impacted by CVE-2026-88774 is displayed.



For more information about the security advisory dashboard, see Security Advisory.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2026-88774 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2026-88774

For CVE-2026-88774 impacted NetScaler instances, the remediation is a single-step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix.

In the GUI, under **CVE Detection > Impacted Instances**, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

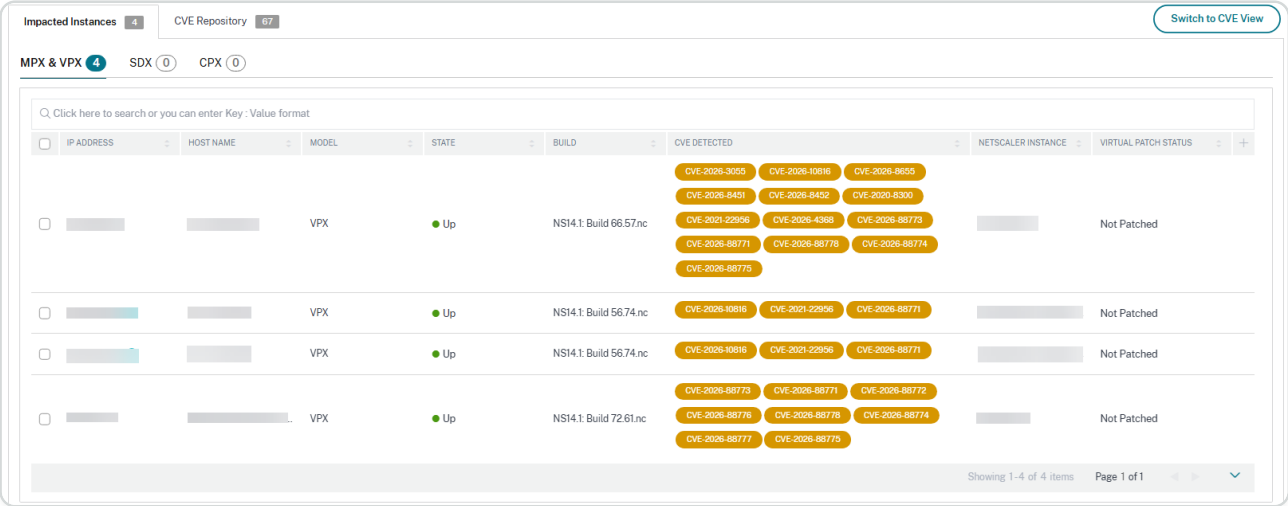
For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This step can be done at once for all the vulnerable NetScaler instances. For more information, see CVE Detection.

Identify and remediate vulnerabilities for CVE-2026-88773

In the NetScaler Console® security advisory dashboard, click **CVE Detection**. On the **Impacted Instances** tab, search for CVE-2026-88773. The list of NetScaler instances that are impacted by CVE-2026-88773 is displayed.



For more information about the security advisory dashboard, see Security Advisory.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2026-88773 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2026-88773

For CVE-2026-88773 impacted NetScaler instances, the remediation is a single-step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix.

In the GUI, under **CVE Detection > Impacted Instances**, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

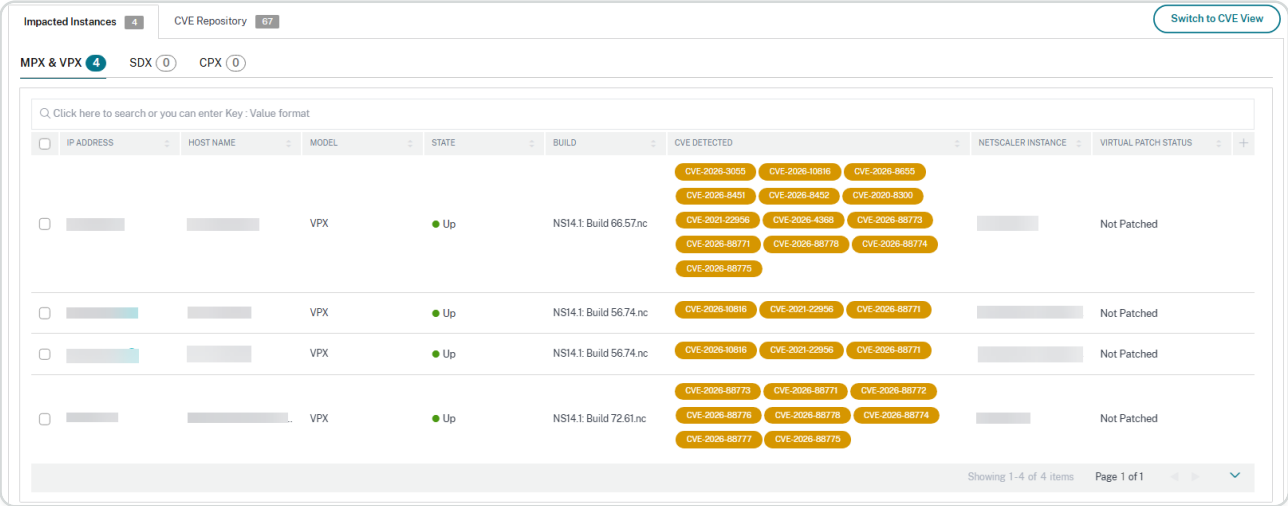
For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This step can be done at once for all the vulnerable NetScaler instances. For more information, see CVE Detection.

Identify and remediate vulnerabilities for CVE-2026-88772

In the NetScaler Console® security advisory dashboard, click **CVE Detection**. On the **Impacted Instances** tab, search for CVE-2026-88772. The list of NetScaler instances that are impacted by CVE-2026-88772 is displayed.



For more information about the security advisory dashboard, see Security Advisory.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2026-88772 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2026-88772

For CVE-2026-88772 impacted NetScaler instances, the remediation is a single-step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix.

In the GUI, under **CVE Detection > Impacted Instances**, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

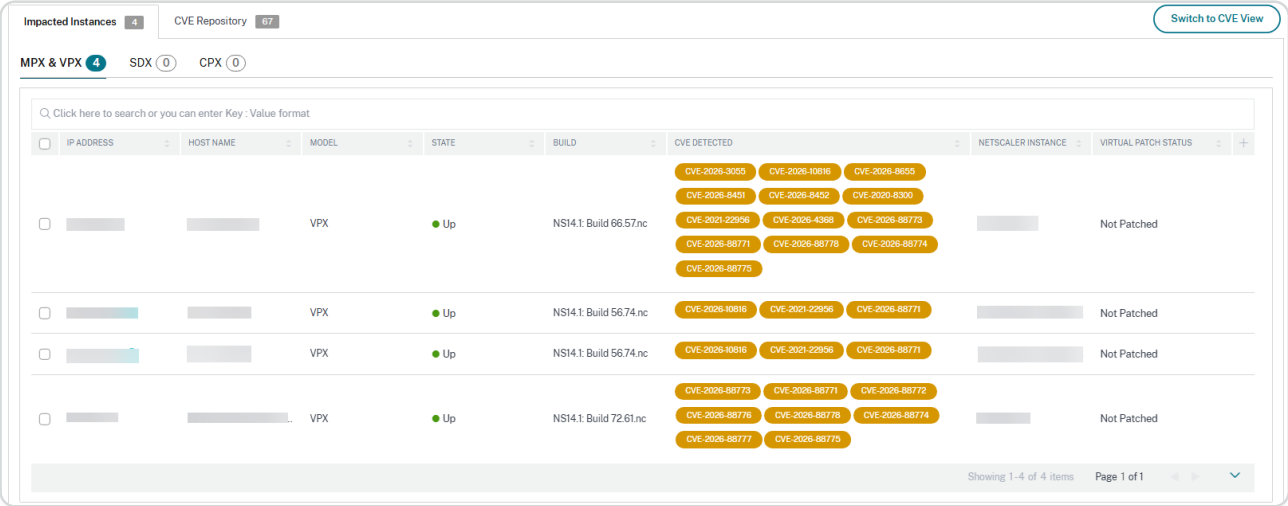
For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This step can be done at once for all the vulnerable NetScaler instances. For more information, see CVE Detection.

Identify and remediate vulnerabilities for CVE-2026-88771

In the NetScaler Console® security advisory dashboard, click **CVE Detection**. On the **Impacted Instances** tab, search for CVE-2026-88771. The list of NetScaler instances that are impacted by CVE-2026-88771 is displayed.



For more information about the security advisory dashboard, see Security Advisory.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2026-88771 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2026-88771

For CVE-2026-88771 impacted NetScaler instances, the remediation is a single-step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix.

In the GUI, under **CVE Detection > Impacted Instances**, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

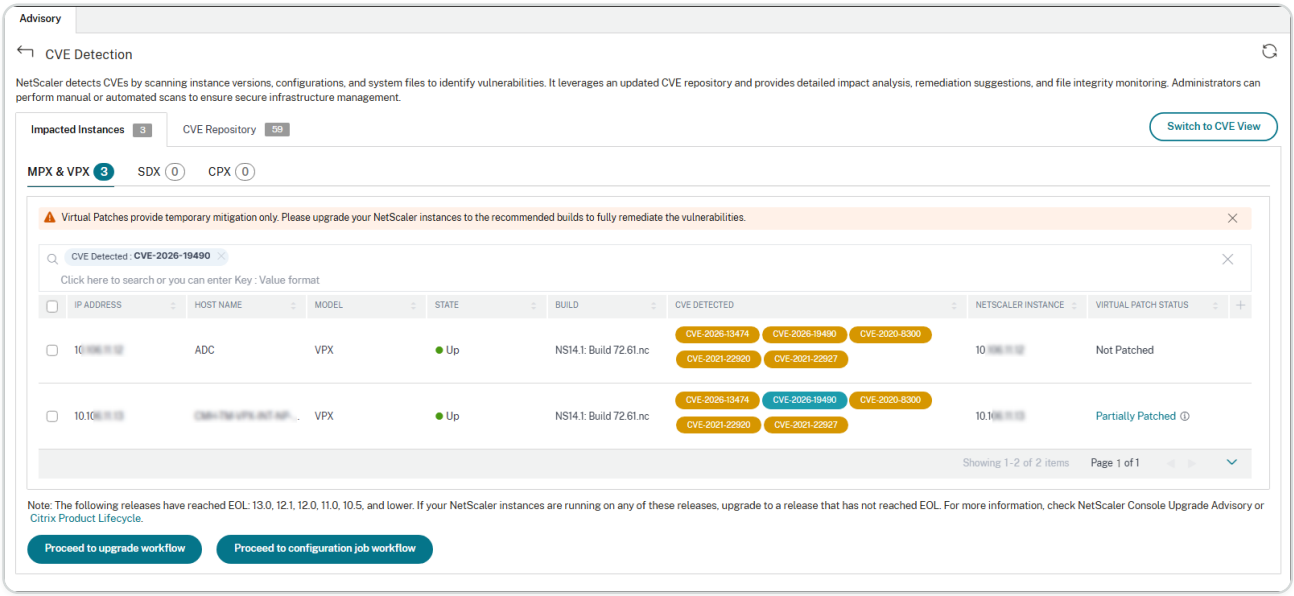
For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This step can be done at once for all the vulnerable NetScaler instances. For more information, see CVE Detection.

Identify and remediate vulnerabilities for CVE-2026-19490

In the NetScaler Console® security advisory dashboard, click **CVE Detection**. On the **Impacted Instances** tab, search for CVE-2026-19490. The list of NetScaler instances that are impacted by CVE-2026-19490 is displayed.



For more information about the security advisory dashboard, see Security Advisory.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2026-19490 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2026-19490

For CVE-2026-19490 impacted NetScaler instances, the remediation is a single-step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix.

In the GUI, under **CVE Detection > Impacted Instances**, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

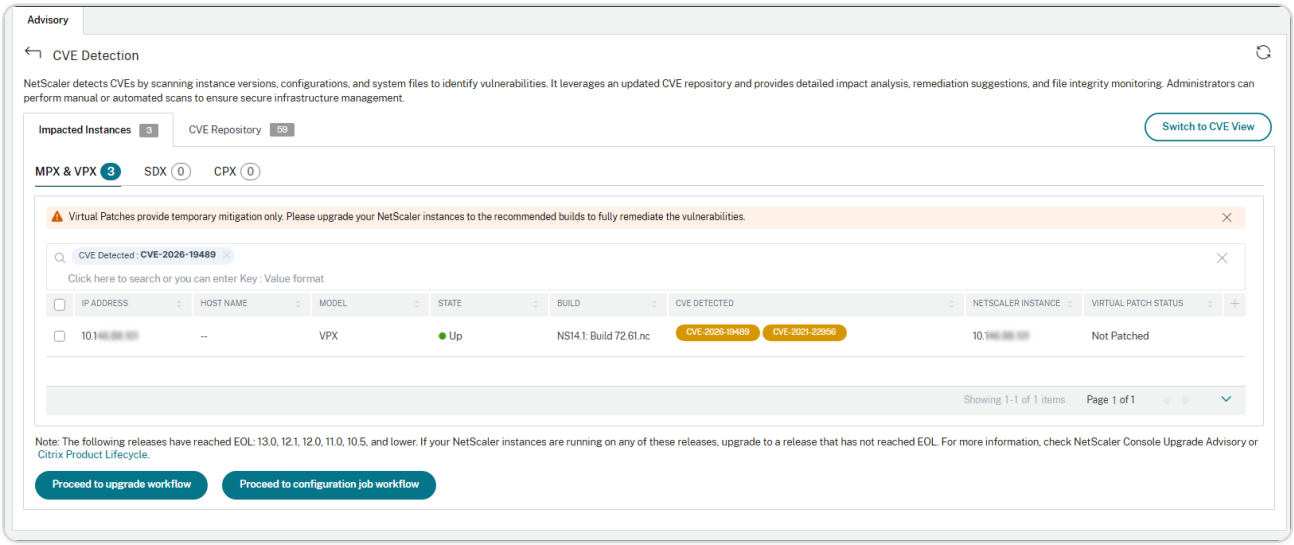
For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This step can be done at once for all the vulnerable NetScaler instances. For more information, see CVE Detection.

Identify and remediate vulnerabilities for CVE-2026-19489

In the NetScaler Console® security advisory dashboard, click **CVE Detection**. On the **Impacted Instances** tab, search for CVE-2026-19489. The list of NetScaler instances that are impacted by CVE-2026-19489 is displayed.



For more information about the security advisory dashboard, see Security Advisory.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2026-19489 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2026-19489

For CVE-2026-19489 impacted NetScaler instances, the remediation is a single-step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix.

In the GUI, under **CVE Detection > Impacted Instances**, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

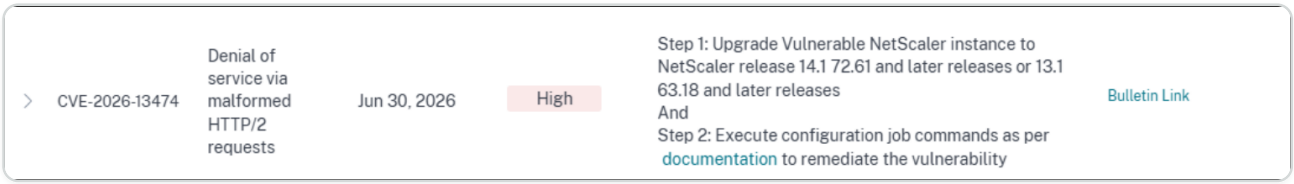
For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

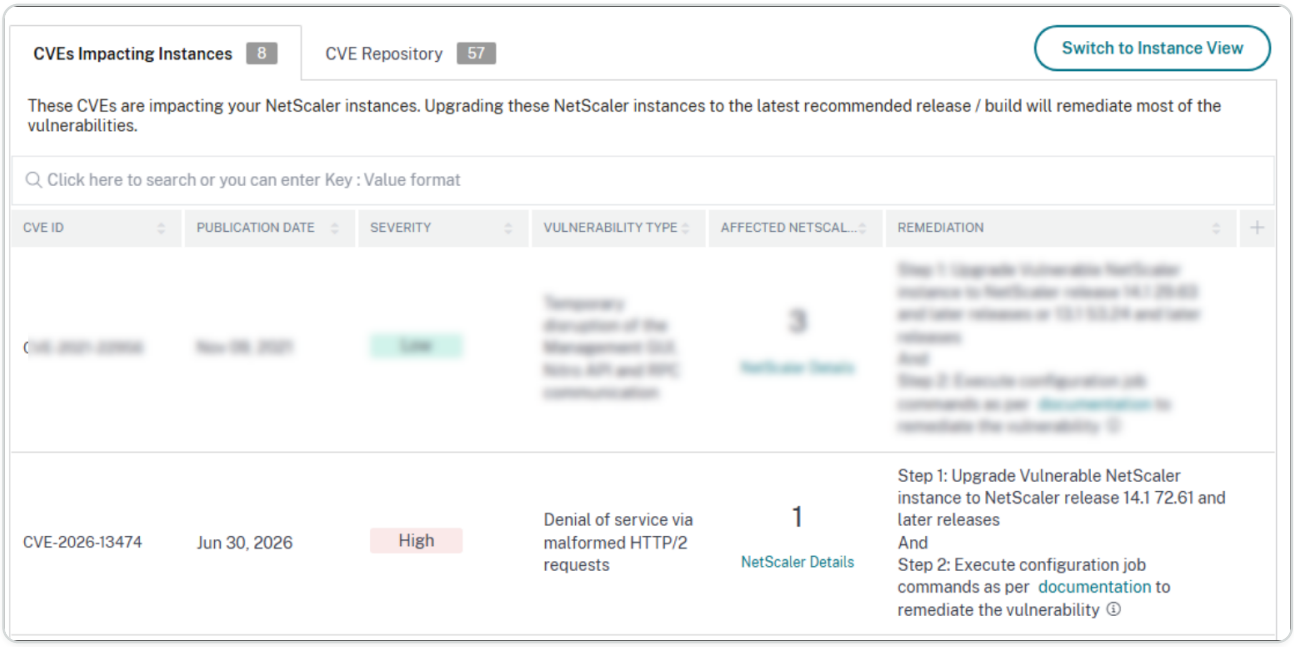
This step can be done at once for all the vulnerable NetScaler instances. For more information, see CVE Detection.

Identify and remediate vulnerabilities for CVE-2026-13474

In the NetScaler Console security advisory dashboard, under **Current CVEs > `<number of>` NetScaler instances are impacted by common vulnerabilities and exposures (CVEs)**, you can see all the instances vulnerable due to this specific CVE. To check the details of the CVE-2026-13474 impacted instances, select **CVE-2026-13474** and click **View Affected Instances**.



The **`<number of>` NetScaler instances impacted by CVEs** window appears. Here you see the count and details of the NetScaler instances impacted by CVE-2026-13474.

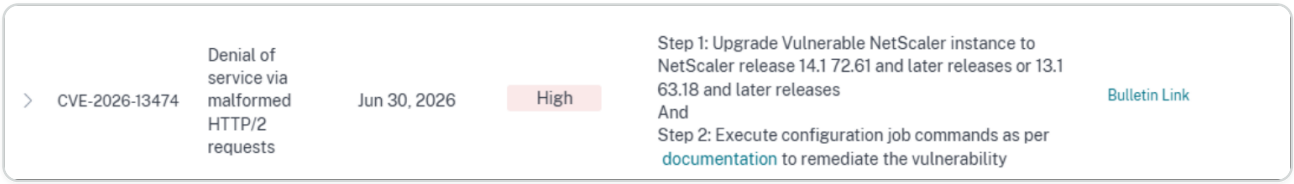


For more information about the security advisory dashboard, see Security Advisory.

Remediate CVE-2026-13474

For CVE-2026-13474 impacted NetScaler instances, the remediation is a two-step process. In the GUI, under **Current CVEs > NetScaler instances are impacted by CVEs**, you can see step 1 and step 2.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



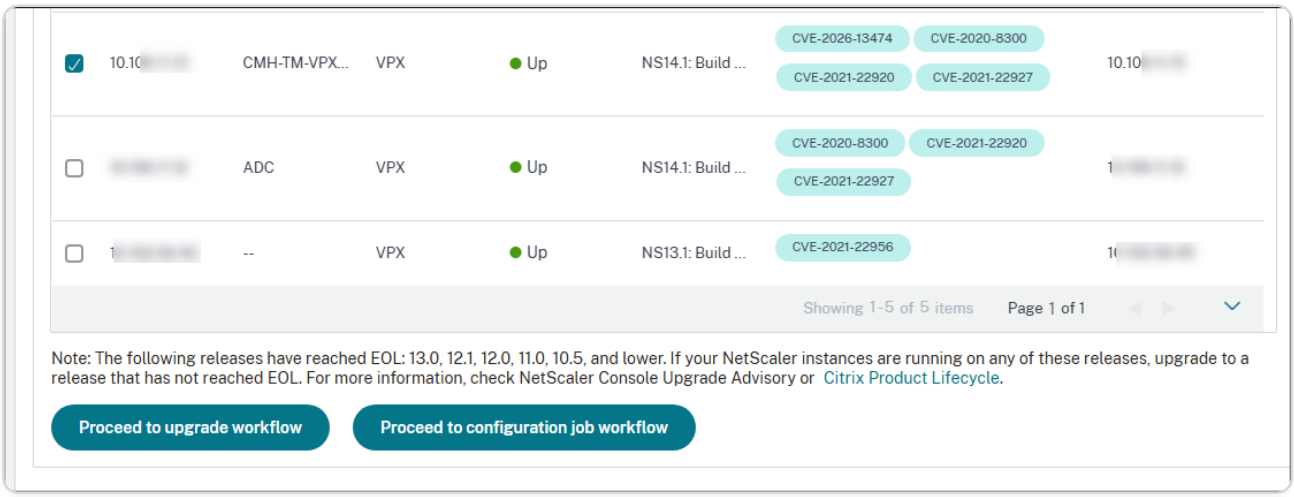
The two steps include:

1. Upgrading the vulnerable NetScaler instances to a release and build that has the fix.
2. Applying the required configuration commands using the customizable built-in configuration template in configuration jobs.

Under **Current CVEs > NetScaler instances impacted by CVEs**, you see two separate workflows for this two-step remediation process: **Proceed to upgrade workflow** and **Proceed to configuration job workflow**.

Step 1: Upgrade the impacted NetScaler instances

To upgrade the vulnerable instances, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.



For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

Step 2: Apply configuration commands

After you upgrade the impacted instances, in the `<number of>` **NetScaler instances impacted by CVEs** window, select the instance impacted by CVE-2026-13474 and click **Proceed to configuration job workflow**. The workflow includes the following steps:

1. Customizing the configuration.
2. Reviewing the auto-populated impacted instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

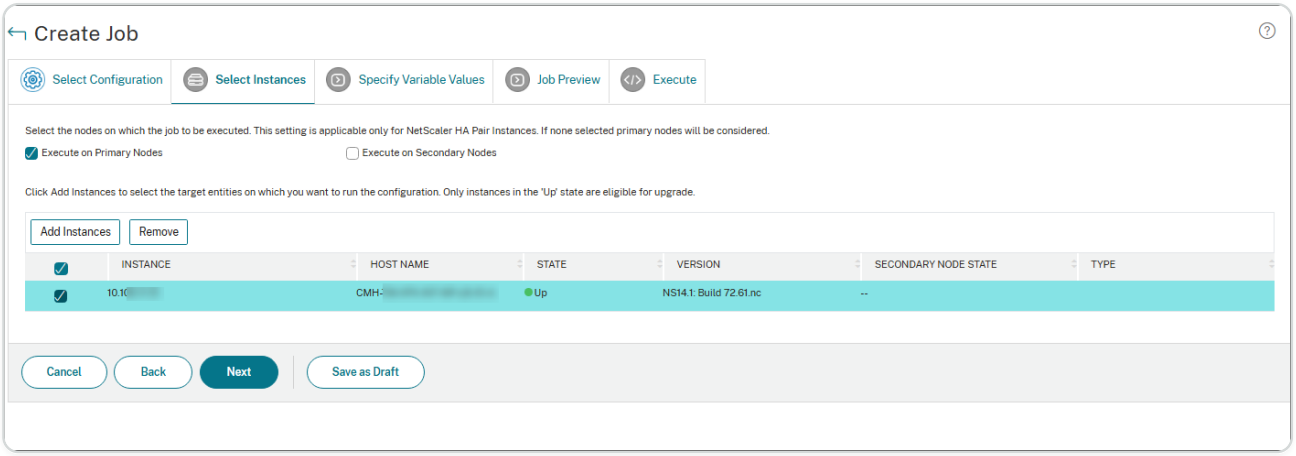
3. Specifying input variables for the job.
4. Reviewing the final configuration with variable inputs populated.
5. Running the job.

Keep the following points in mind before you select an instance and click **Proceed to configuration job workflow**:

- For multiple NetScaler instances that are impacted only by CVE-2026-13474, you can run configuration jobs on all the instances at once. For example, if NetScaler 1, NetScaler 2, and NetScaler 3 are impacted only by CVE-2026-13474, select all these instances and click **Proceed to configuration job workflow**. The built-in configuration template auto-populates under **Select configuration**.

Step 1: Select configuration

In the configuration job workflow, the built-in base configuration template auto-populates under **Select configuration**.



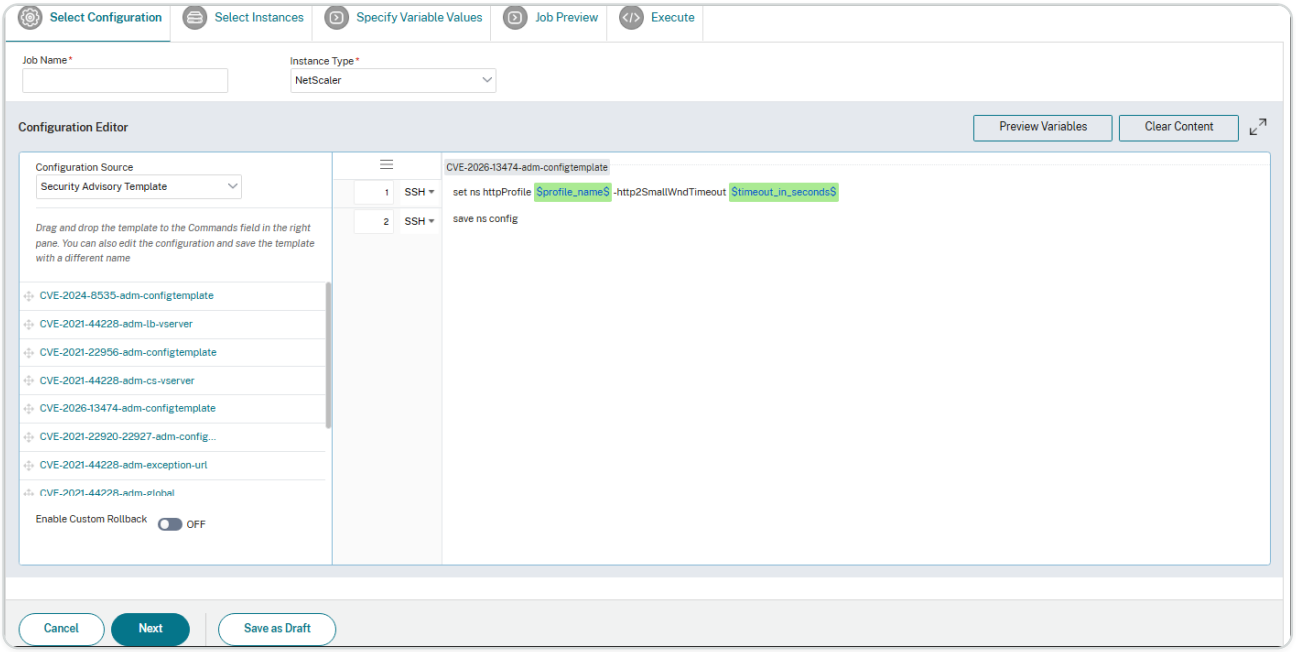
Step 2: Select the instance

The impacted instance is auto-populated under **Select Instances**. Select the instances and click **Next**. In the next step, preview the configurations and click **Next**.

NOTE:

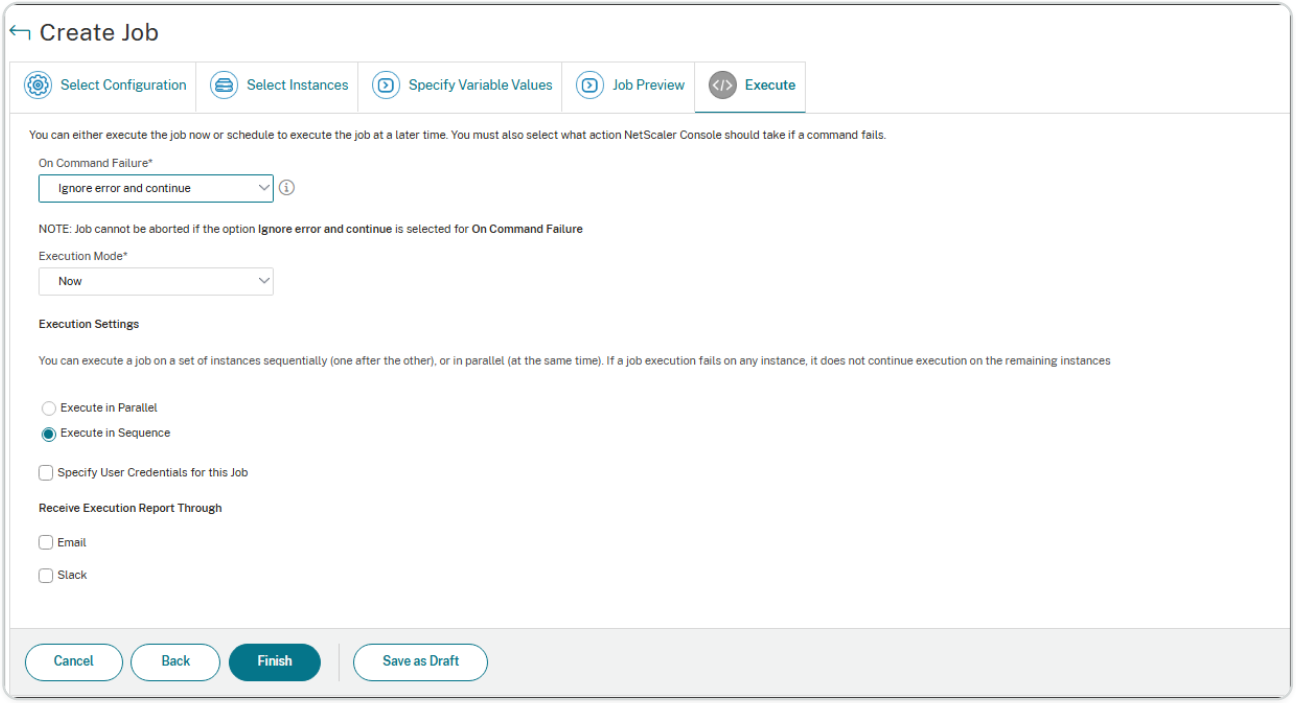
For NetScaler instances in cluster mode, by using security advisory, NetScaler Console supports running the configuration job only on the cluster configuration coordinator (CCO) node. Run the commands on non-CCO nodes separately.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Step 3: Run the configuration

Click **Finish** to run the configuration job.



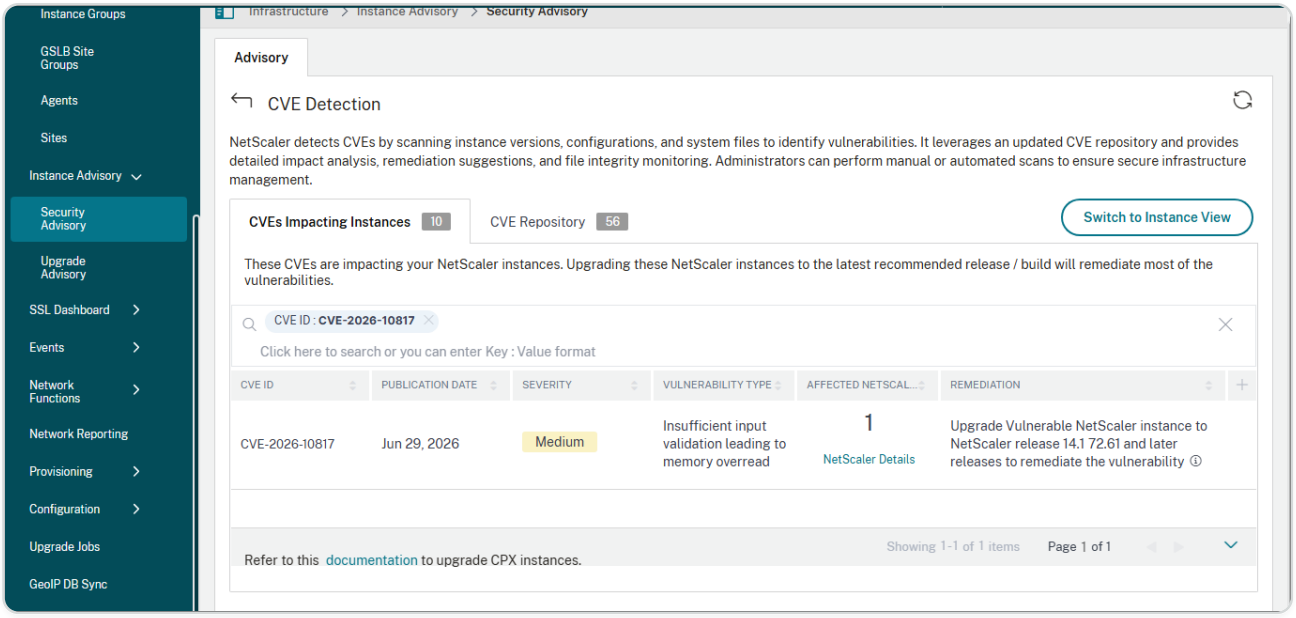
After the job is run, it appears under **Infrastructure > Configuration > Configuration Jobs**.

After you complete the two remediation steps for all vulnerable NetScaler instances, run an on-demand scan to see the revised security posture.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Identify and remediate vulnerabilities for CVE-2026-10817

In the NetScaler Console® security advisory dashboard, click **CVE Detection**. On the **Impacted Instances** tab, search for CVE-2026-10817. The list of NetScaler instances that are impacted by CVE-2026-10817 is displayed.



For more information about the security advisory dashboard, see Security Advisory.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2026-10817 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2026-10817

For CVE-2026-10817 impacted NetScaler instances, the remediation is a single-step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix.

In the GUI, under **CVE Detection > Impacted Instances**, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

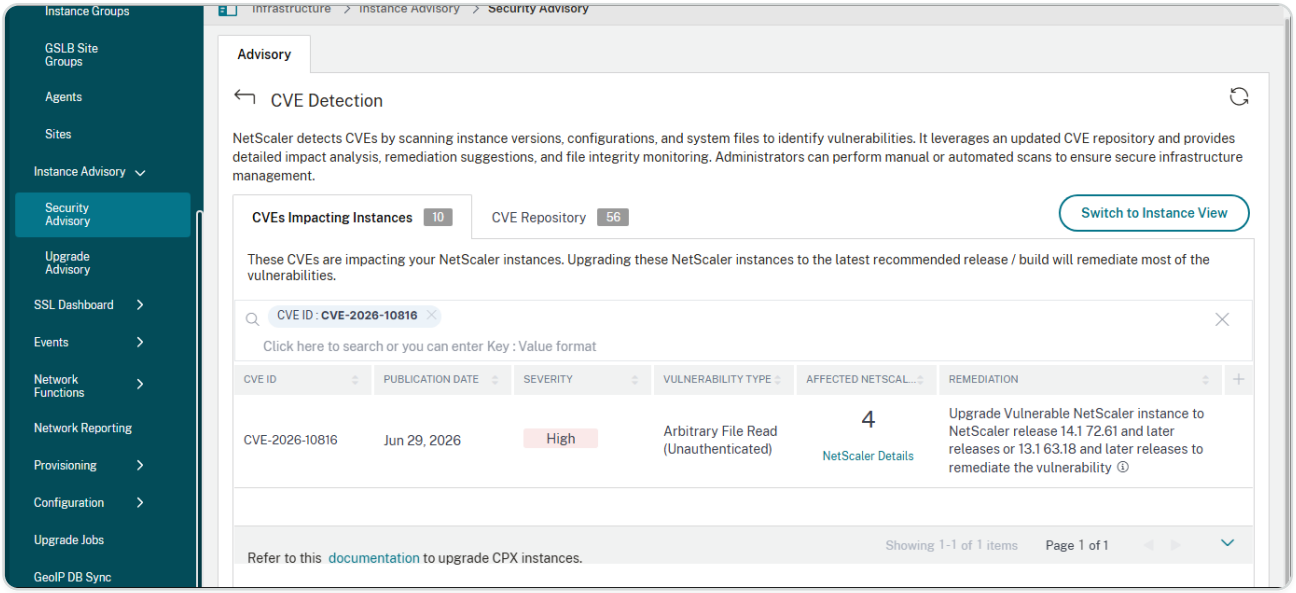
For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

This step can be done at once for all the vulnerable NetScaler instances. For more information, see CVE Detection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Identify and remediate vulnerabilities for CVE-2026-10816

In the NetScaler Console® security advisory dashboard, click **CVE Detection**. On the **Impacted Instances** tab, search for CVE-2026-10816. The list of NetScaler instances that are impacted by CVE-2026-10816 is displayed.



For more information about the security advisory dashboard, see Security Advisory.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2026-10816 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2026-10816

For CVE-2026-10816 impacted NetScaler instances, the remediation is a single-step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix.

In the GUI, under **CVE Detection > Impacted Instances**, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

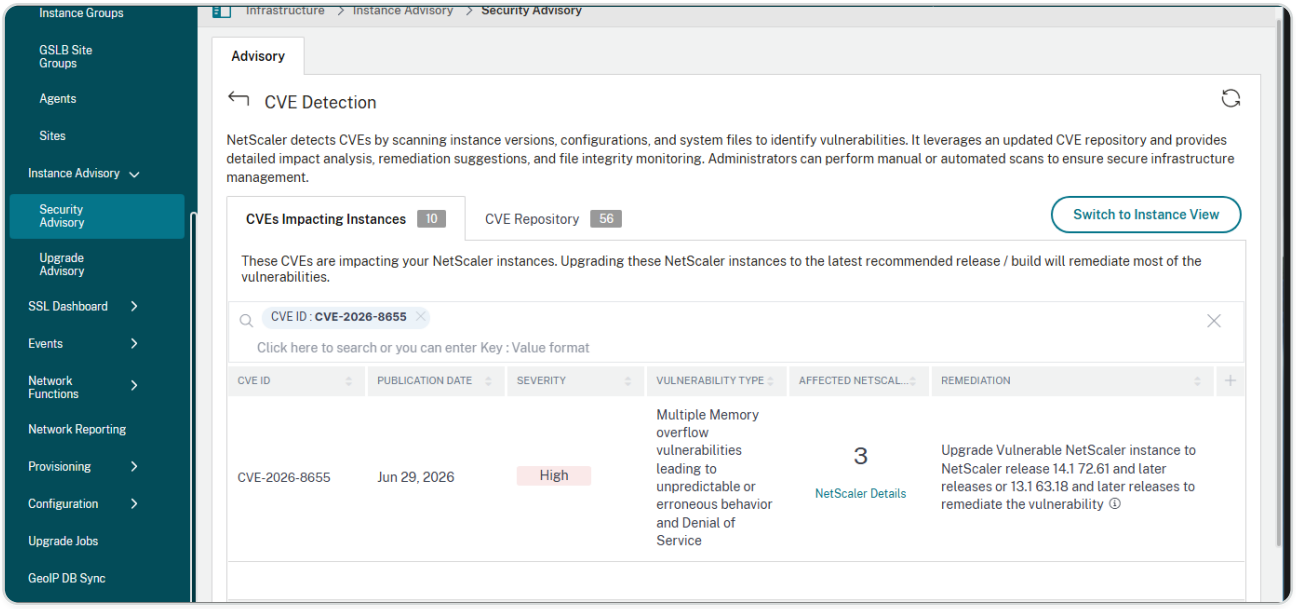
For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

This step can be done at once for all the vulnerable NetScaler instances. For more information, see CVE Detection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Identify and remediate vulnerabilities for CVE-2026-8655

In the NetScaler Console® security advisory dashboard, click **CVE Detection**. On the **Impacted Instances** tab, search for CVE-2026-8655. The list of NetScaler instances that are impacted by CVE-2026-8655 is displayed.



For more information about the security advisory dashboard, see Security Advisory.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2026-8655 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2026-8655

For CVE-2026-8655 impacted NetScaler instances, the remediation is a single-step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix.

In the GUI, under **CVE Detection > Impacted Instances**, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

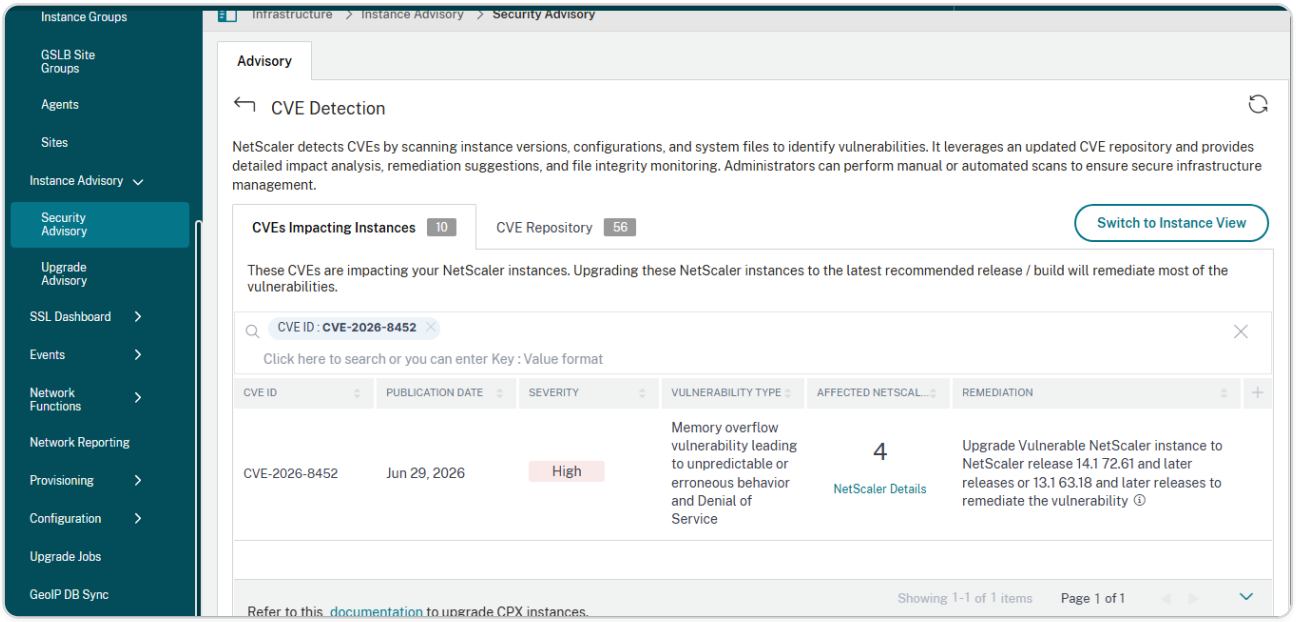
For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

This step can be done at once for all the vulnerable NetScaler instances. For more information, see CVE Detection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Identify and remediate vulnerabilities for CVE-2026-8452

In the NetScaler Console® security advisory dashboard, click **CVE Detection**. On the **Impacted Instances** tab, search for CVE-2026-8452. The list of NetScaler instances that are impacted by CVE-2026-8452 is displayed.



For more information about the security advisory dashboard, see Security Advisory.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2026-8452 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2026-8452

For CVE-2026-8452 impacted NetScaler instances, the remediation is a single-step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix.

In the GUI, under **CVE Detection > Impacted Instances**, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

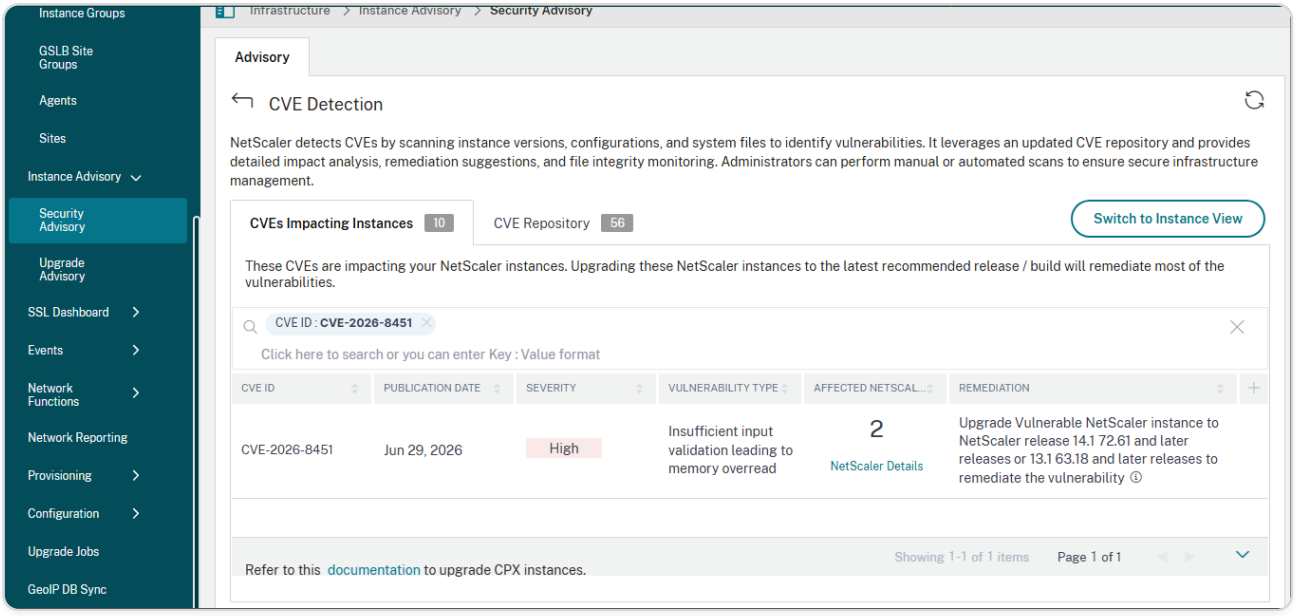
For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

This step can be done at once for all the vulnerable NetScaler instances. For more information, see CVE Detection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Identify and remediate vulnerabilities for CVE-2026-8451

In the NetScaler Console® security advisory dashboard, click **CVE Detection**. On the **Impacted Instances** tab, search for CVE-2026-8451. The list of NetScaler instances that are impacted by CVE-2026-8451 is displayed.



For more information about the security advisory dashboard, see Security Advisory.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2026-8451 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2026-8451

For CVE-2026-8451 impacted NetScaler instances, the remediation is a single-step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix.

In the GUI, under **CVE Detection > Impacted Instances**, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

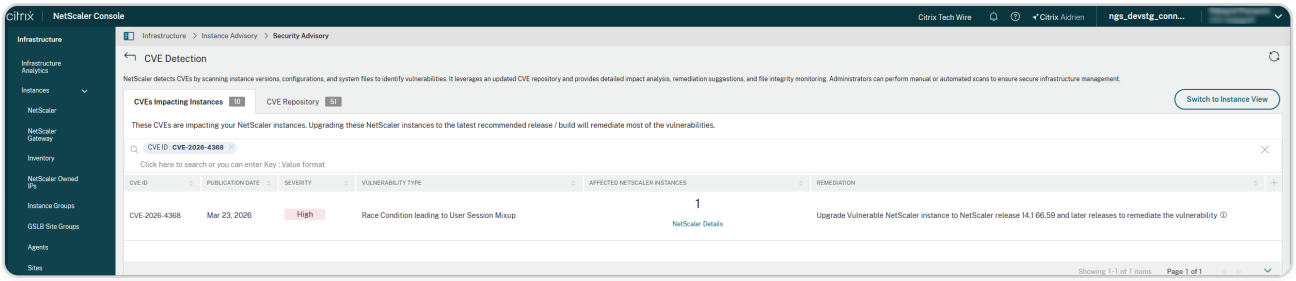
For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

This step can be done at once for all the vulnerable NetScaler instances. For more information, see CVE Detection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Identify and remediate vulnerabilities for CVE-2026-4368

In the NetScaler Console® security advisory dashboard, click **CVE Detection**. On the **Impacted Instances** tab, search for CVE-2026-4368. The list of NetScaler instances that are impacted by CVE-2026-4368 is displayed.



For more information about the security advisory dashboard, see Security Advisory.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2026-4368 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2026-4368

For CVE-2026-4368 impacted NetScaler instances, the remediation is a single-step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix.

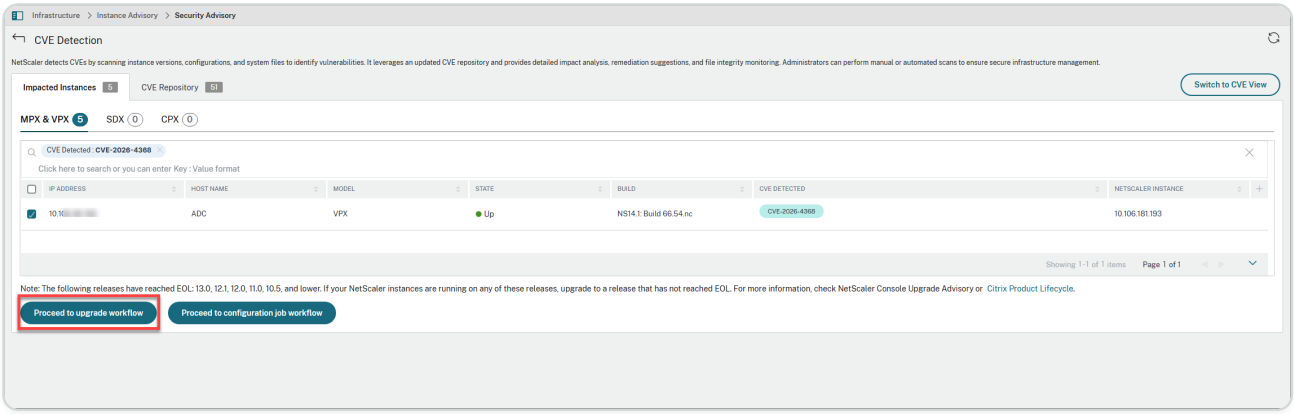
In the GUI, under **CVE Detection > Impacted Instances**, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

IMPORTANT

If your vulnerable NetScaler instances have the /etc/httpd.conf file copied to the /nsconfig directory, see Upgrade considerations for customized NetScaler configurations before planning NetScaler upgrade.

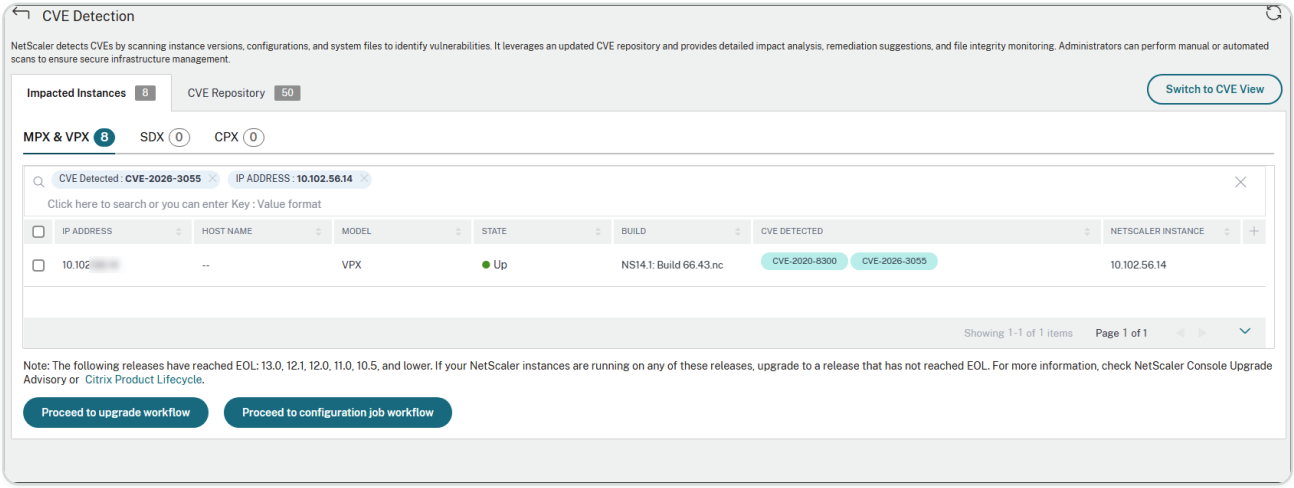
For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Identify and remediate vulnerabilities for CVE-2026-3055

In the NetScaler Console® security advisory dashboard, click **CVE Detection**. On the **Impacted Instances** tab, search for CVE-2026-3055. The list of NetScaler instances that are impacted by CVE-2026-3055 is displayed.



For more information about the security advisory dashboard, see Security Advisory.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2026-3055 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2026-3055

For CVE-2026-3055 impacted NetScaler instances, the remediation is a single-step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix.

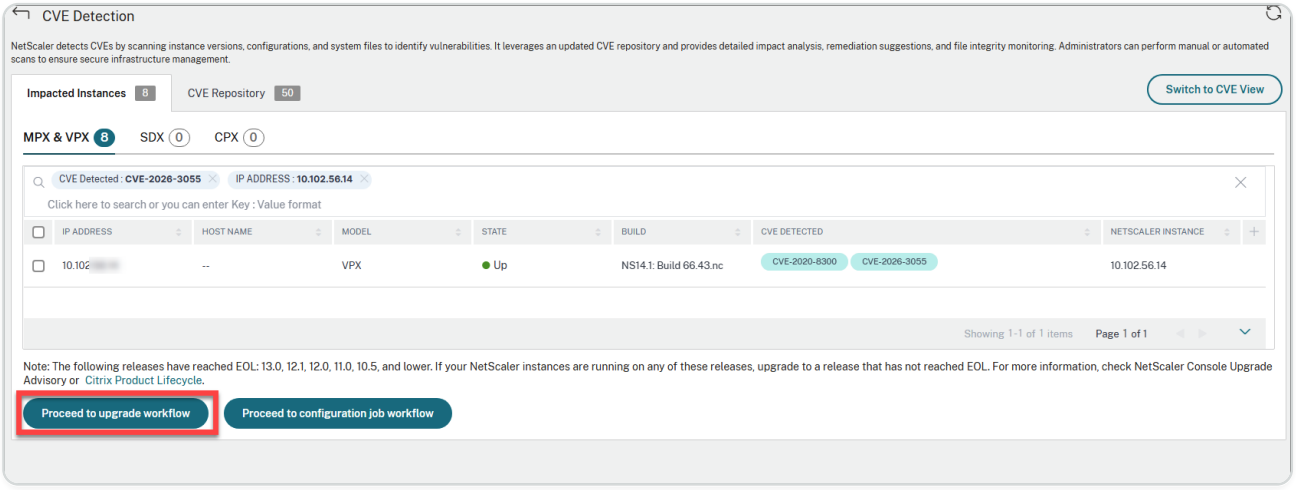
© 1997–2026 Citrix Systems, Inc. All rights reserved.

In the GUI, under **CVE Detection > Impacted Instances**, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

IMPORTANT

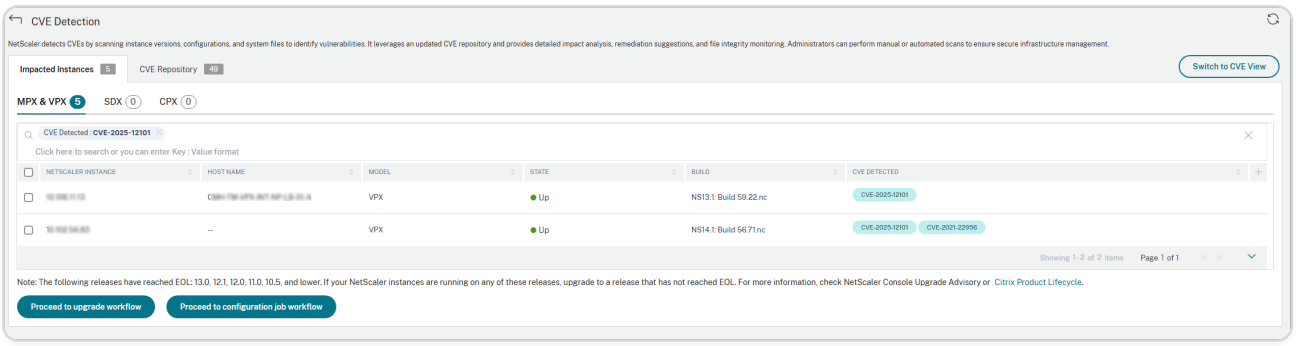
If your vulnerable NetScaler instances have the /etc/httpd.conf file copied to the /nsconfig directory, see Upgrade considerations for customized NetScaler configurations before planning NetScaler upgrade.

For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.



Identify and remediate vulnerabilities for CVE-2025-12101

In the NetScaler Console security advisory dashboard, click **CVE Detection**. On the **Impacted Instances** tab, search for CVE-2025-12101. The list of NetScaler® instances that are impacted by CVE-2025-12101 is displayed.



For more information about the security advisory dashboard see, Security Advisory.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2025-12101 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2025-12101

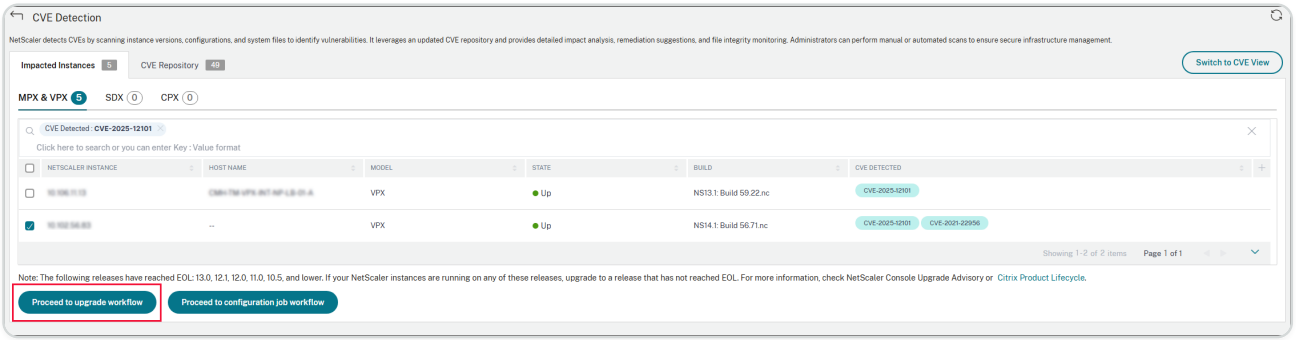
For CVE-2025-12101 impacted NetScaler instances, the remediation is a single-step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix.

In the GUI, under **CVE Detection > Impacted Instances**, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

IMPORTANT

If your vulnerable NetScaler instances have the /etc/httpd.conf file copied to the /nsconfig directory, see Upgrade considerations for customized NetScaler configurations before planning NetScaler upgrade.

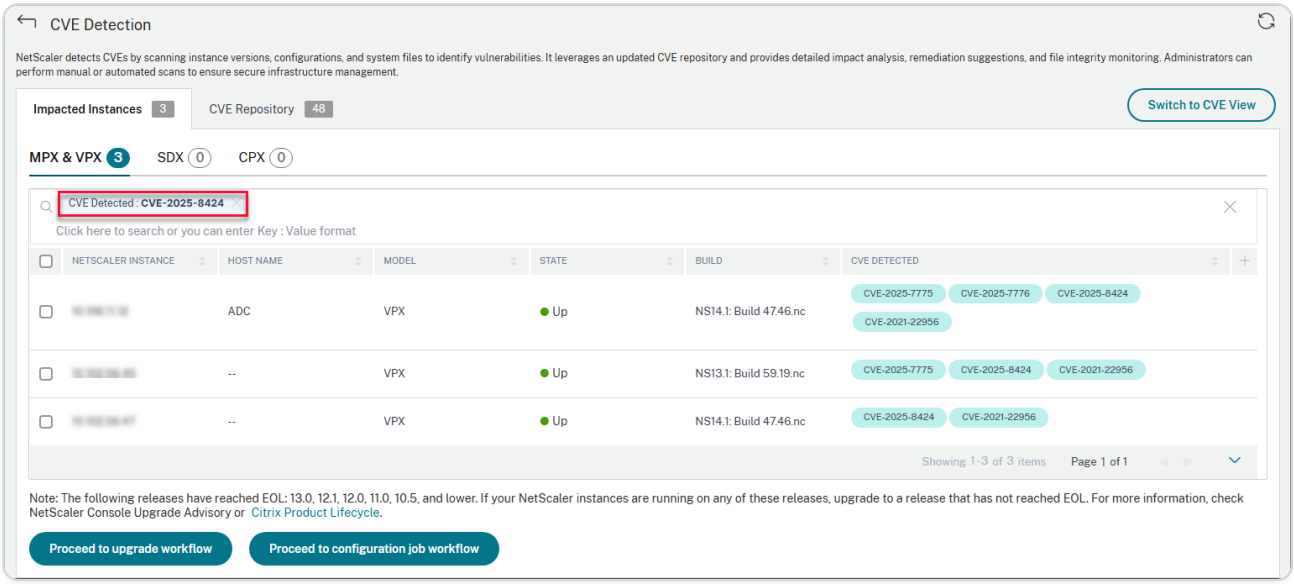
For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.



Identify and remediate vulnerabilities for CVE-2025-8424

In the NetScaler Console security advisory dashboard, click **CVE Detection**. On the **Impacted Instances** tab, search for CVE-2025-8424. The list of NetScaler instances that are impacted by CVE-2025-8424 is displayed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For more information about the security advisory dashboard see, Security Advisory.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2025-8424 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2025-8424

For CVE-2025-8424 impacted NetScaler® instances, the remediation is a single-step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix.

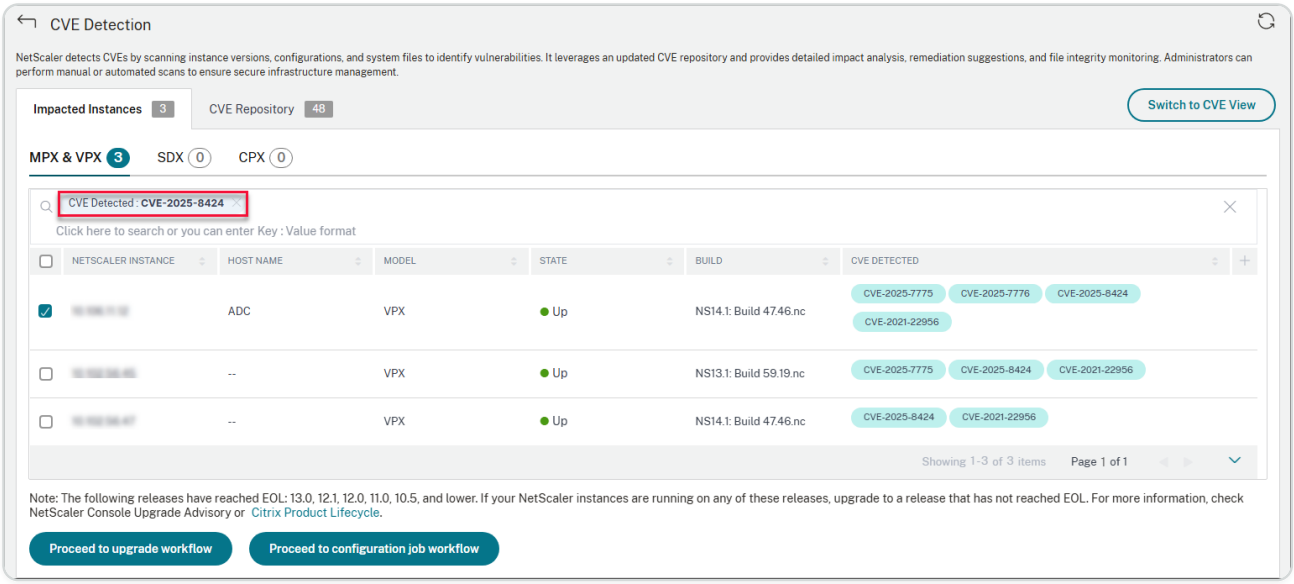
In the GUI, under **CVE Detection > Impacted Instances**, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

IMPORTANT

If your vulnerable NetScaler instances have the /etc/httpd.conf file copied to the /nsconfig directory, see Upgrade considerations for customized NetScaler configurations before planning NetScaler upgrade.

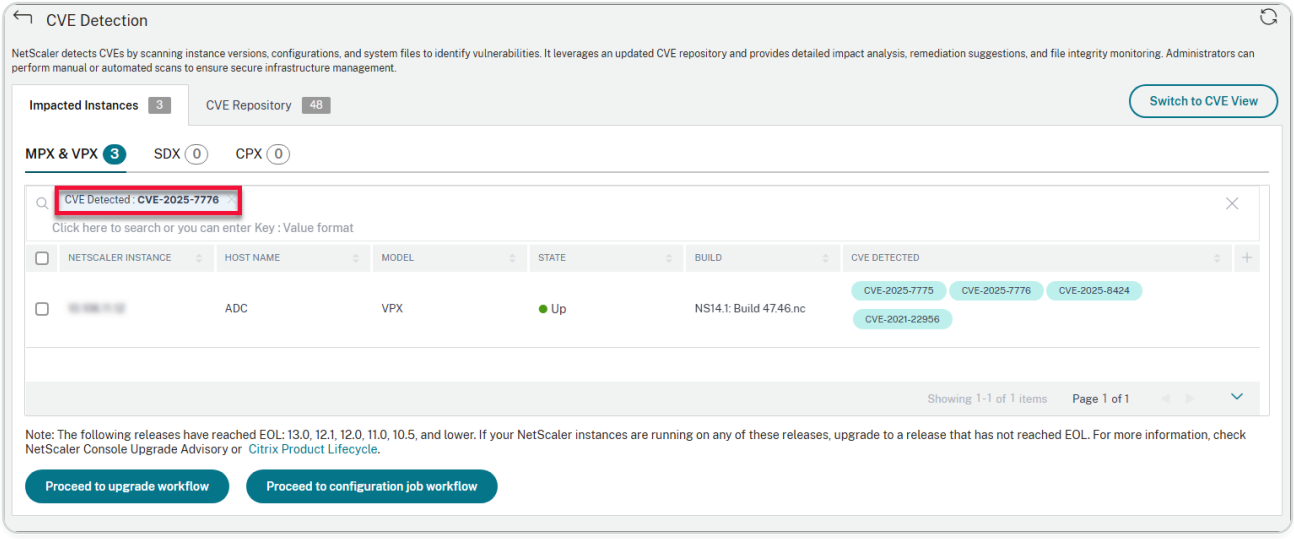
For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Identify and remediate vulnerabilities for CVE-2025-7776

In the NetScaler Console security advisory dashboard, click **CVE Detection**. On the **Impacted Instances** tab, search for CVE-2025-7776. The list of NetScaler instances that are impacted by CVE-2025-7776 is displayed.



For more information about the security advisory dashboard see, Security Advisory.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2025-7776 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Remediate CVE-2025-7776

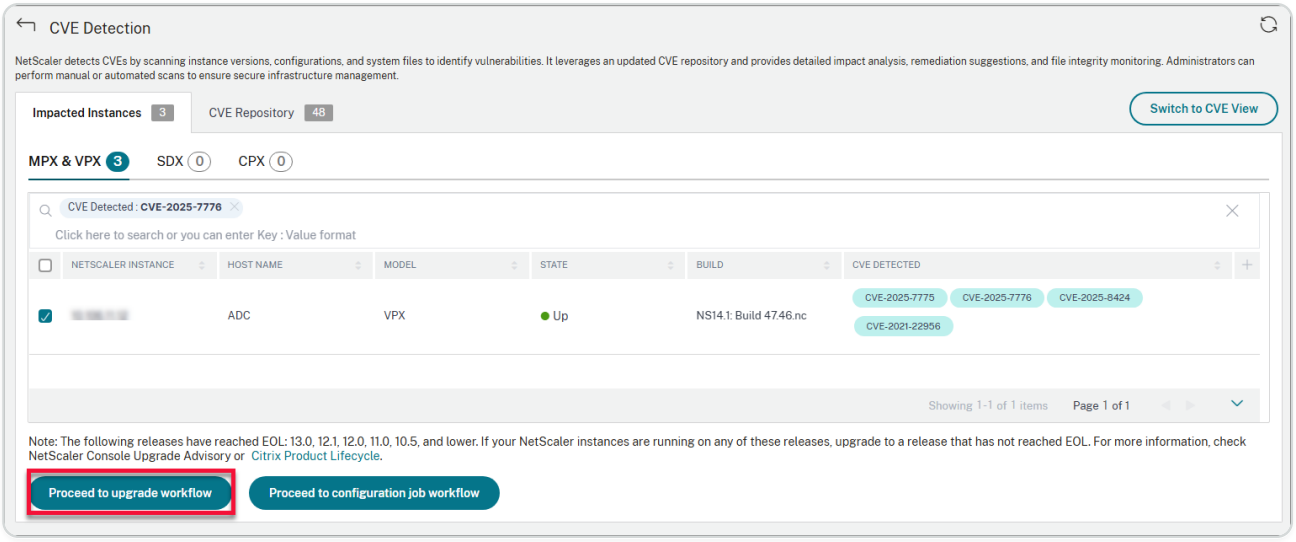
For CVE-2025-7776 impacted NetScaler® instances, the remediation is a single-step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix.

In the GUI, under **CVE Detection > Impacted Instances**, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

IMPORTANT

If your vulnerable NetScaler instances have the /etc/httpd.conf file copied to the /nsconfig directory, see Upgrade considerations for customized NetScaler configurations before planning NetScaler upgrade.

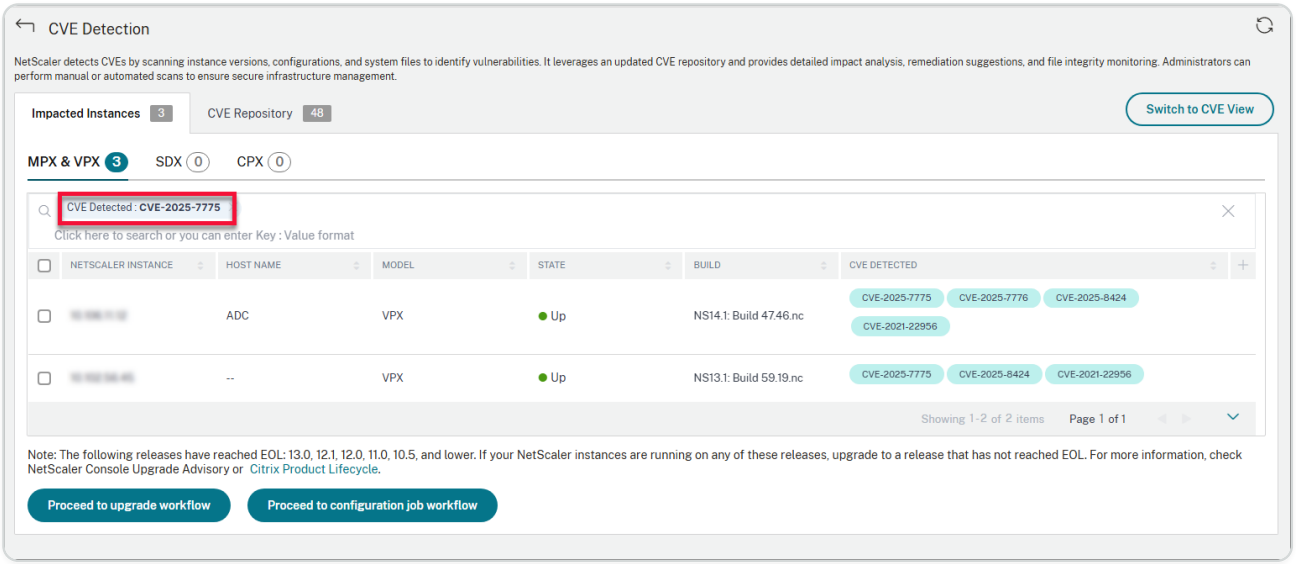
For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.



Identify and remediate vulnerabilities for CVE-2025-7775

In the NetScaler Console security advisory dashboard, click **CVE Detection**. On the **Impacted Instances** tab, search for CVE-2025-7775. The list of NetScaler instances that are impacted by CVE-2025-7775 is displayed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For more information about the security advisory dashboard see, Security Advisory.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2025-7775 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2025-7775

For CVE-2025-7775 impacted NetScaler® instances, the remediation is a single-step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix.

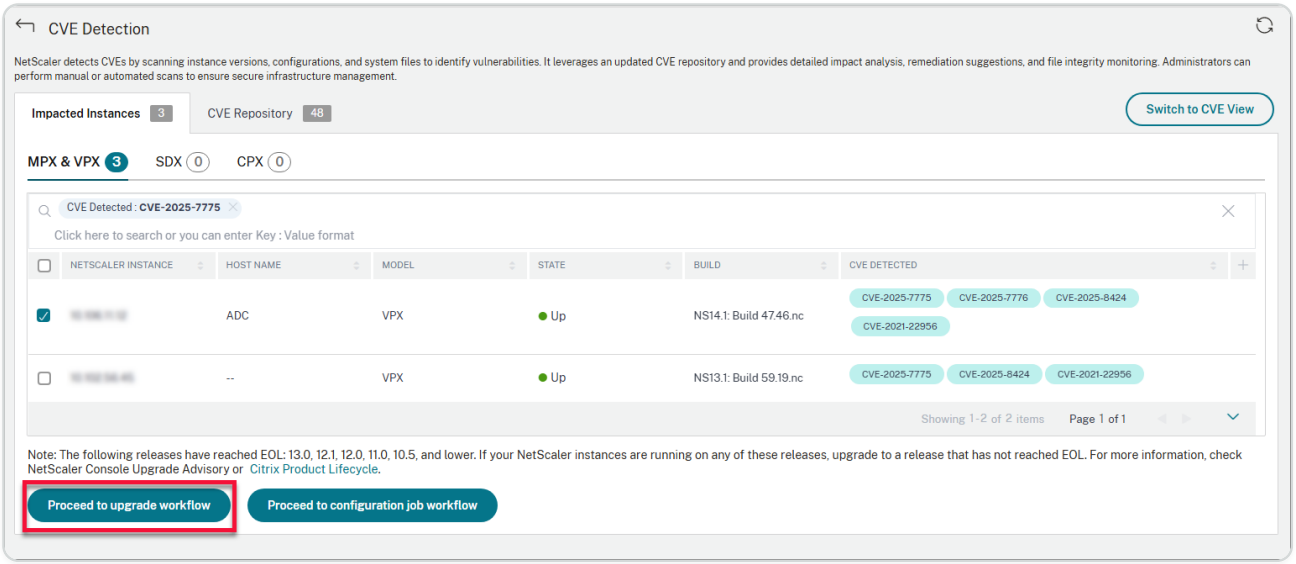
In the GUI, under **CVE Detection > Impacted Instances**, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

IMPORTANT

If your vulnerable NetScaler instances have the /etc/httpd.conf file copied to the /nsconfig directory, see Upgrade considerations for customized NetScaler configurations before planning NetScaler upgrade.

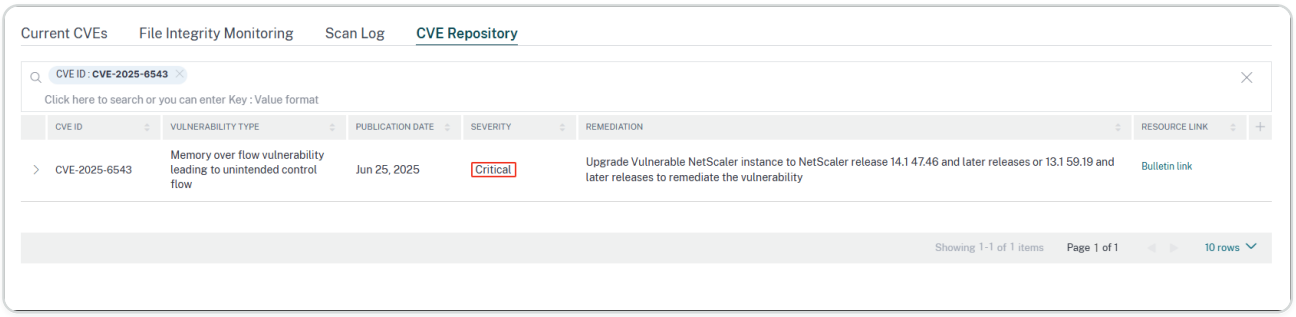
For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Identify and remediate vulnerabilities for CVE-2025-6543

In the NetScaler Console security advisory dashboard, under **Current CVEs** `<number of>` **NetScaler instances are impacted by CVEs**, you can see all the instances vulnerable due to CVE-2025-6543. To check the details of the instances impacted by the CVEs, select CVE-2025-6543 and click **View Affected Instances**.

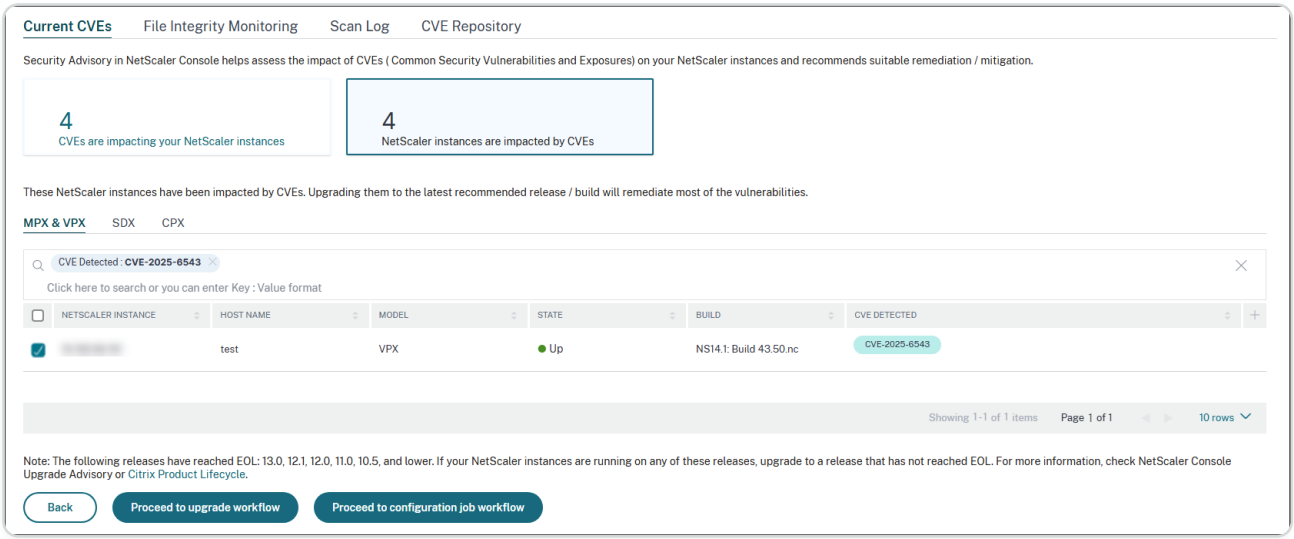


NOTE:

To understand the reason for NetScaler vulnerability, download the CSV report in **Scan logs** tab in Security Advisory.

The `<number of>` **NetScaler instances impacted by CVEs** window appears. In the following screen capture, you can see the count and details of the NetScaler instances impacted by CVE-2025-6543.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For more information about the security advisory dashboard see, Security Advisory.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2025-6543 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2025-6543

For CVE-2025-6543 impacted NetScaler instances, the remediation is a single step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix. In the GUI, under **Current CVEs > NetScaler instances are impacted by CVEs**, you can see the step to remediate.

Under **Current CVEs> NetScaler instances impacted by CVEs**, you see the following workflow for this single step remediation process, which is **Proceed to upgrade workflow**.

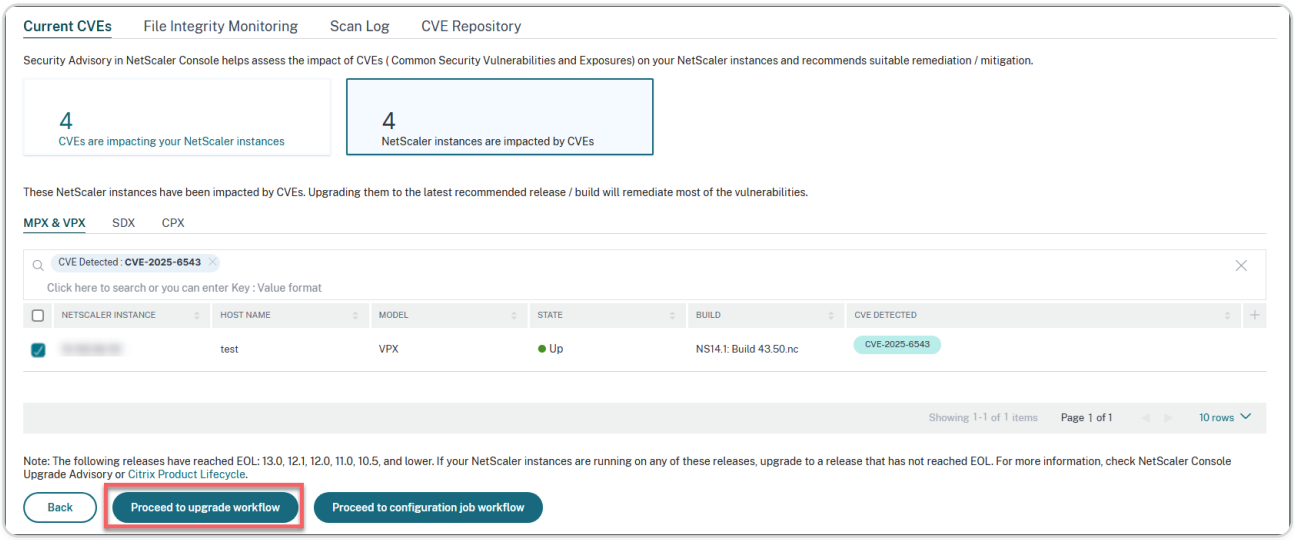
To upgrade the vulnerable instances, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

IMPORTANT

If your vulnerable NetScaler instances have the /etc/httpd.conf file copied to the /nsconfig directory, see Upgrade considerations for customized NetScaler configurations before planning NetScaler upgrade.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.



Identify and remediate vulnerabilities for CVE-2025-5349

In the NetScaler Console security advisory dashboard, under **Current CVEs** `<number of>` **NetScaler instances are impacted by CVEs**, you can see all the instances vulnerable due to CVE-2025-5349. To check the details of the instances impacted by the CVEs, select CVE-2025-5349 and click **View Affected Instances**.

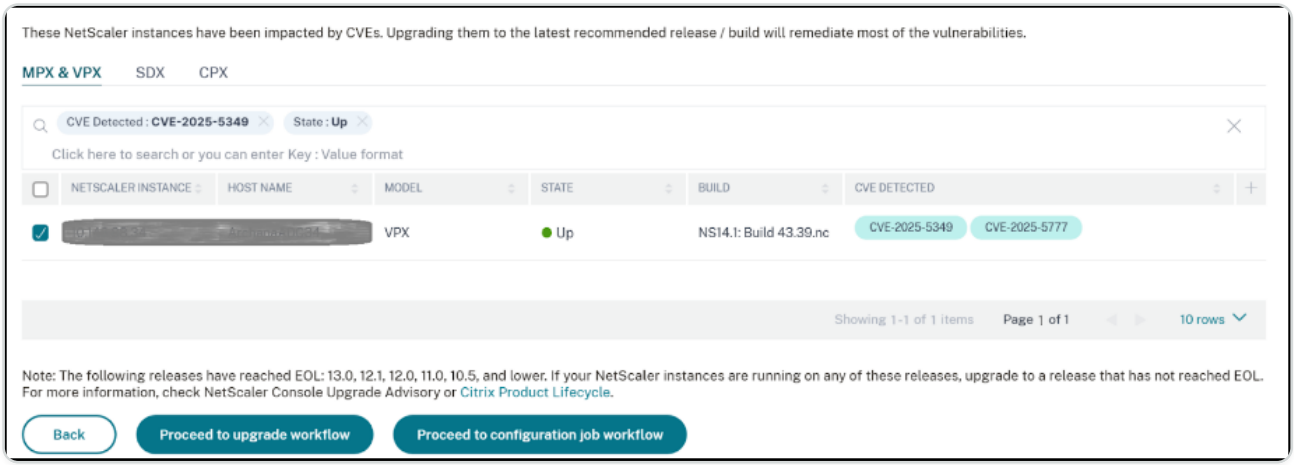


NOTE:

To understand the reason for NetScaler vulnerability, download the CSV report in **Scan logs** tab in Security Advisory.

The `<number of>` **NetScaler instances impacted by CVEs** window appears. In the following screen capture, you can see the count and details of the NetScaler instances impacted by CVE-2025-5349.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For more information about the security advisory dashboard see, Security Advisory.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2025-5349 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2025-5349

For CVE-2025-5349 impacted NetScaler instances, the remediation is a single step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix. In the GUI, under **Current CVEs > NetScaler instances are impacted by CVEs**, you can see the step to remediate.

Under **Current CVEs> NetScaler instances impacted by CVEs**, you see the following workflow for this single step remediation process, which is **Proceed to upgrade workflow**.

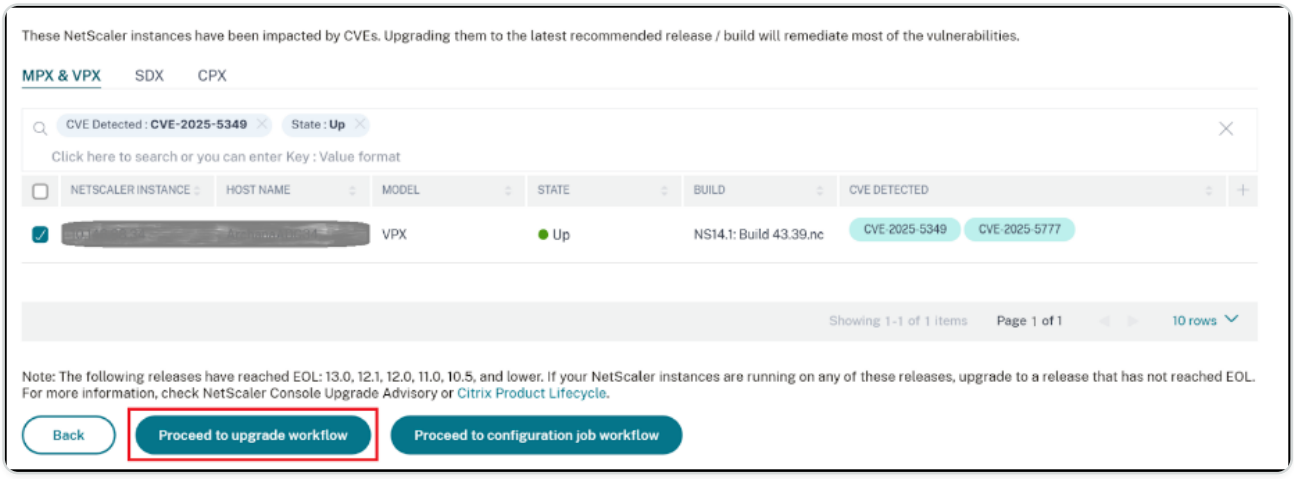
To upgrade the vulnerable instances, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

IMPORTANT

If your vulnerable NetScaler instances have the /etc/httpd.conf file copied to the /nsconfig directory, see Upgrade considerations for customized NetScaler configurations before planning NetScaler upgrade.

For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Remediate vulnerabilities for CVE-2025-5777

In the NetScaler Console security advisory dashboard, under **Current CVEs** `<number of>` **NetScaler instances are impacted by CVEs**, you can see all the instances vulnerable due to CVE-2025-5777. To check the details of the instances impacted by the CVEs, select CVE-2025-5777 and click **View Affected Instances**.

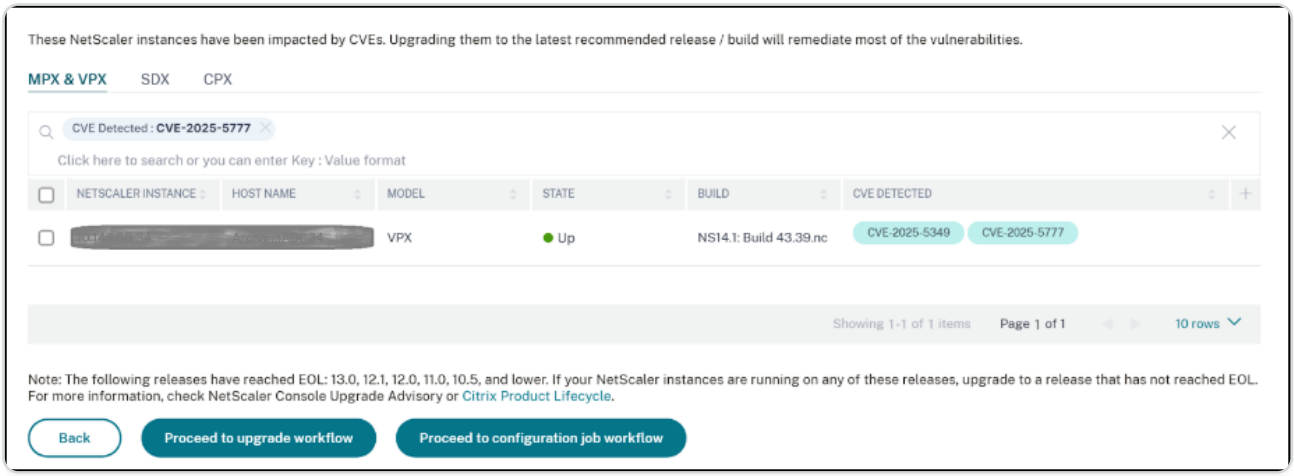


NOTE:

To understand the reason for NetScaler vulnerability, download the CSV report in **Scan logs** tab in Security Advisory.

The `<number of>` **NetScaler instances impacted by CVEs** window appears. In the following screen capture, you can see the count and details of the NetScaler instances impacted by CVE-2025-5777.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For more information about the security advisory dashboard see, Security Advisory.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2025-5777 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2025-5777

For CVE-2025-5777 -impacted NetScaler instances, the remediation is a two-step process. In the GUI, under **Current CVEs > NetScaler instances are impacted by CVEs**, you can see step 1 and 2.



The two steps include:

1. Upgrading the vulnerable NetScaler instances to a release and build that has the fix.
2. Applying the required configuration commands using the customizable built-in configuration template in configuration jobs.

Under **Current CVEs> NetScaler instances impacted by CVEs**, you see two separate workflows for this 2-step remediation process: which are **Proceed to upgrade workflow** and **Proceed to configuration job workflow**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 1: Upgrade the vulnerable NetScaler instances

To upgrade the vulnerable instances, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

NOTE:

This step can be done at once for all the vulnerable NetScaler instances.

Step 2: Apply configuration commands

After you've upgraded the impacted instances, in the **`<number of>` NetScaler instances impacted by CVEs** window, select the instance impacted by CVE-2025-5777 and click **Proceed to configuration job workflow**. The workflow includes the following steps.

1. Customizing the configuration.
2. Reviewing the auto-populated impacted instances.
3. Running the job.

Keep the following points in mind before you select an instance and click **Proceed to configuration job workflow**:

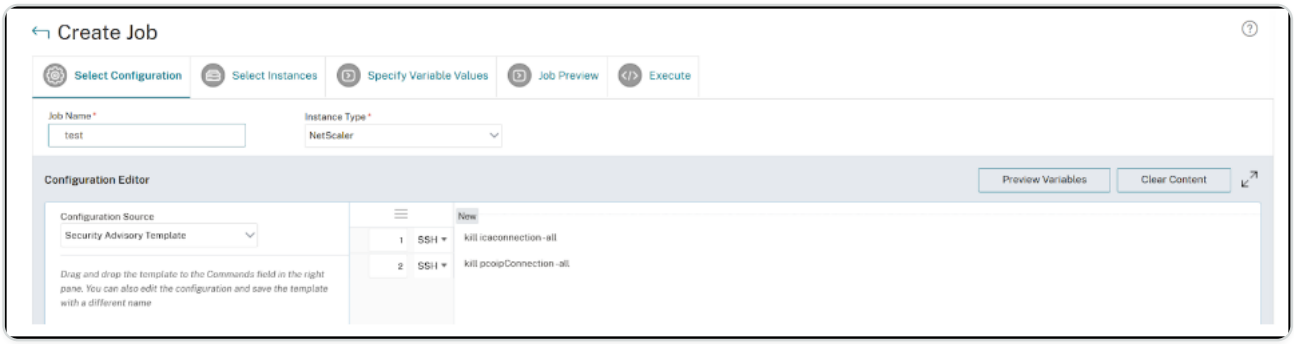
- For a NetScaler instance impacted by multiple CVEs (such as CVE-2020-8300, CVE-2021-22927, CVE-2021-22920, CVE-2021-22956, and CVE-2025-5777): when you select the instance and click **Proceed to configuration job workflow**, the built-in configuration template does not auto-populate under **Select configuration**. You must Drag and drop the appropriate config job template under **Security Advisory Template** manually to the config job pane on the right side.
- For multiple NetScaler instances that are impacted by CVE-2025-5777 only: you can run config jobs on all instances at once. For example, you've NetScaler 1, NetScaler 2, and NetScaler 3, and all of them are impacted only by CVE-2025-5777. Select all these instances and click **Proceed to configuration job workflow**, and the built-in configuration template auto-populates under **Select configuration**.
- For multiple NetScaler instances impacted by CVE-2025-5777 and one or more other CVEs (such as CVE-2020-8300, CVE-2021-22927, and CVE-2021-22920), which require remediation

© 1997–2026 Citrix Systems, Inc. All rights reserved.

to be applied to each NetScaler at a time: when you select these instances and click **Proceed to configuration job workflow**, an error message appears telling you to run the config job on each NetScaler at a time.

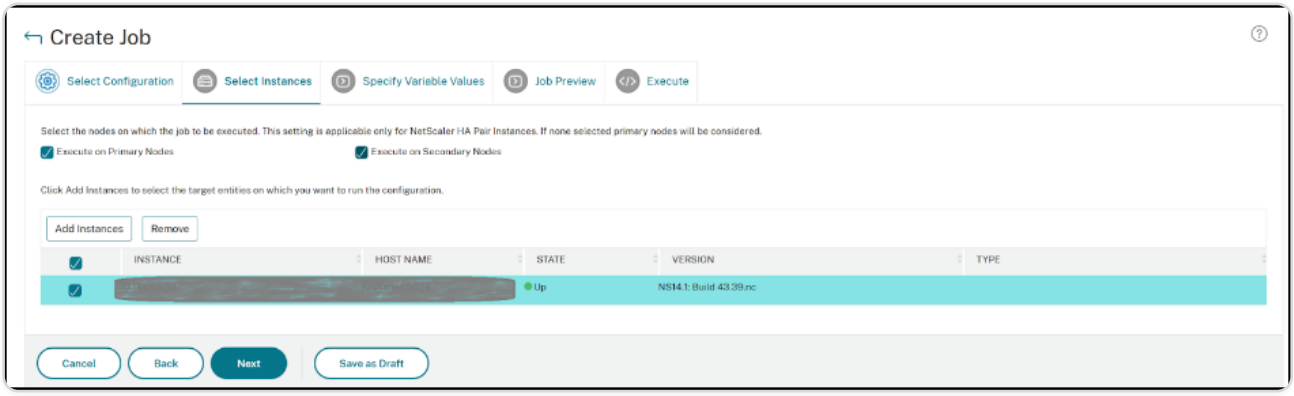
Step 1: Select configuration

In the configuration job workflow, the built-in configuration base template auto-populates under **Select configuration**.



Step 2: Select the instance

The impacted instance is auto-populated under **Select Instances**. Select the instance. If this instance is part of an HA pair, select **Execute on Secondary Nodes**. Click **Next**.



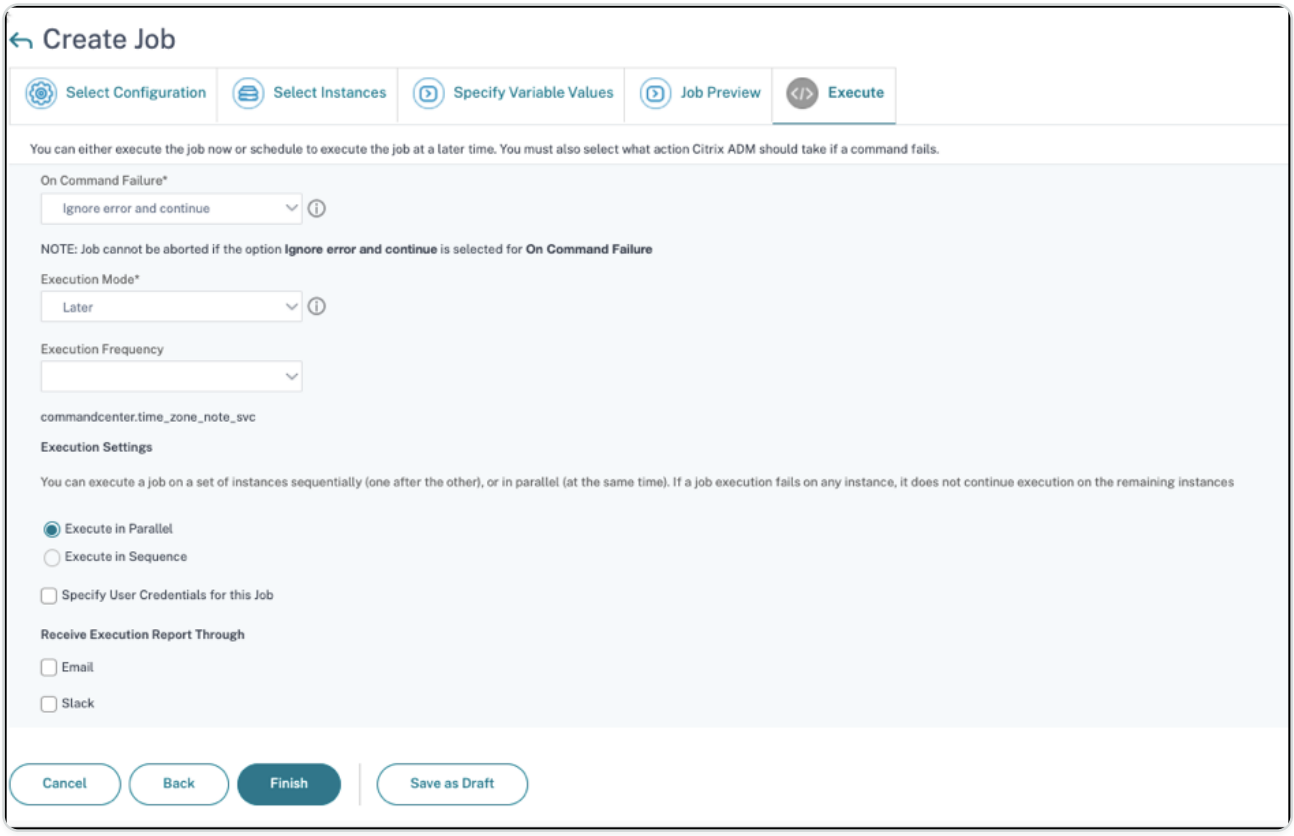
NOTE:

For NetScaler instances in cluster mode, using security advisory, the NetScaler Console supports running the config job only on the cluster configuration coordinator (CCO) node. Run the commands on non-CCO nodes separately.

Step 3: Run the job

Click **Finish** to run the configuration job.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

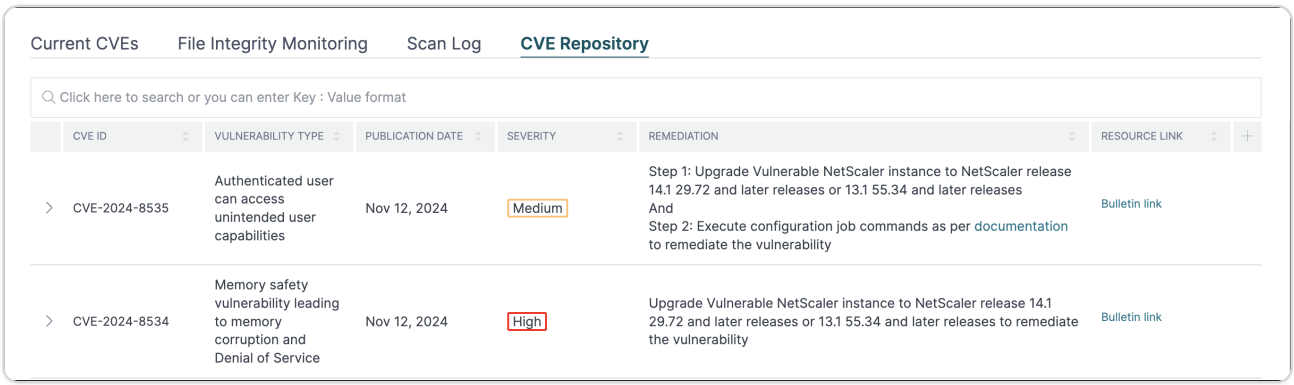


After the job is run, it appears under **Infrastructure > Configuration > Configuration Jobs**.

After completing the two remediation steps for all vulnerable NetScaler instances, you can run an on-demand scan to see the revised security posture.

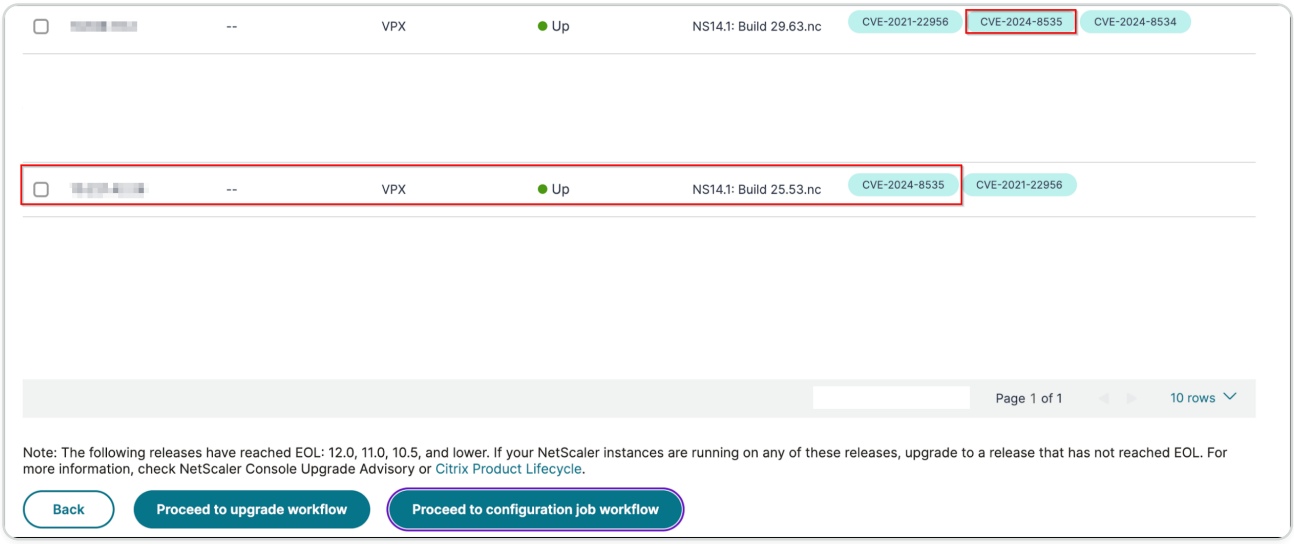
Remediate vulnerabilities for CVE-2024-8535

In the NetScaler Console security advisory dashboard, under **Current CVEs >** `<number of>` NetScaler instances are impacted by common vulnerabilities and exposures (CVEs), you can see all the instances vulnerable due to this specific CVE. To check the details of the CVE-2024-8535 impacted instances, select CVE-2024-8535 and click **View Affected Instances**.



The `<number of>` NetScaler instances impacted by CVEs window appear. Here you see the count and details of the NetScaler instances impacted by CVE-2024-8535.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For more information about the security advisory dashboard see, Security Advisory.

NOTE

It might take some time for security advisory system scan to conclude and reflect the impact of CVE-2024-8535 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2024-8535

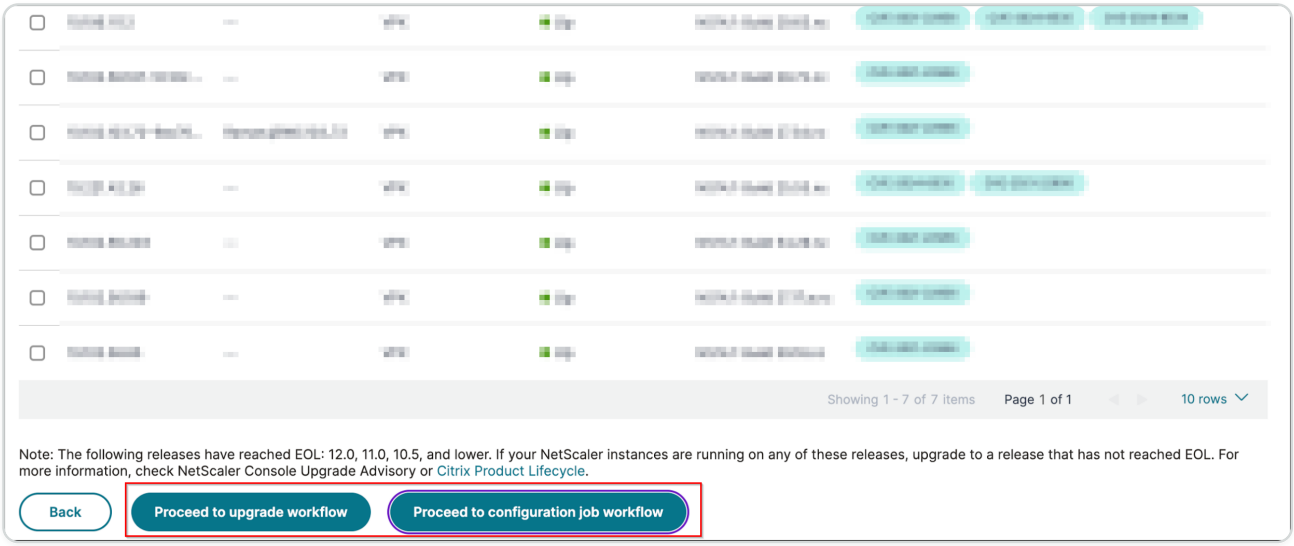
For CVE-2024-8535 -impacted NetScaler instances, the remediation is a two-step process. In the GUI, under **Current CVEs > NetScaler instances are impacted by CVEs**, you can see step 1 and 2.

The two steps include:

1. Upgrading the vulnerable NetScaler instances to a release and build that has the fix.
2. Applying the required configuration commands using the customizable built-in configuration template in configuration jobs.

Under **Current CVEs > NetScaler** instances impacted by CVEs, you see two separate workflows for this 2-step remediation process: which are **Proceed to upgrade workflow** and **Proceed to configuration job workflow**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Step 1: Upgrade the vulnerable NetScaler instances

To upgrade the vulnerable instances, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

NOTE:

This step can be done at once for all the vulnerable NetScaler instances.

Step 2: Apply configuration commands

After you've upgraded the impacted instances, in the **`<number of>` NetScaler instances impacted by CVEs** window, select the instance impacted by CVE-2024-8535 and click **Proceed to configuration job workflow**.

Keep the following points in mind before you select an instance and click **Proceed to configuration job workflow**:

- For a NetScaler instance impacted by multiple CVEs (such as CVE-2020-8300, CVE-2021-22927, CVE-2021-22920, and CVE-2021-22956): when you select the instance and click **Proceed to configuration job workflow**, the built-in configuration template does not auto-populate under **Select configuration**. Drag and drop the appropriate config job template under **Security Advisory Template** manually to the config job pane on the right side.
- For multiple NetScaler instances that are impacted by CVE-2024-8535 only, you can run config jobs on all instances at once. For example, you've NetScaler 1, NetScaler 2, and NetScaler 3,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

and all of them are impacted only by CVE-2024-8535. Select all these instances and click **Proceed to configuration job workflow**, and the built-in configuration template auto-populates under **Select configuration**.

- For multiple NetScaler instances impacted by CVE-2024-8535 and one or more other CVEs (such as CVE-2020-8300, CVE-2021-22927, and CVE-2021-22920), which require remediation to be applied to each NetScaler at a time: when you select these instances and click **Proceed to configuration job workflow**, an error message appears mentioning you to run the config job on each NetScaler at a time.

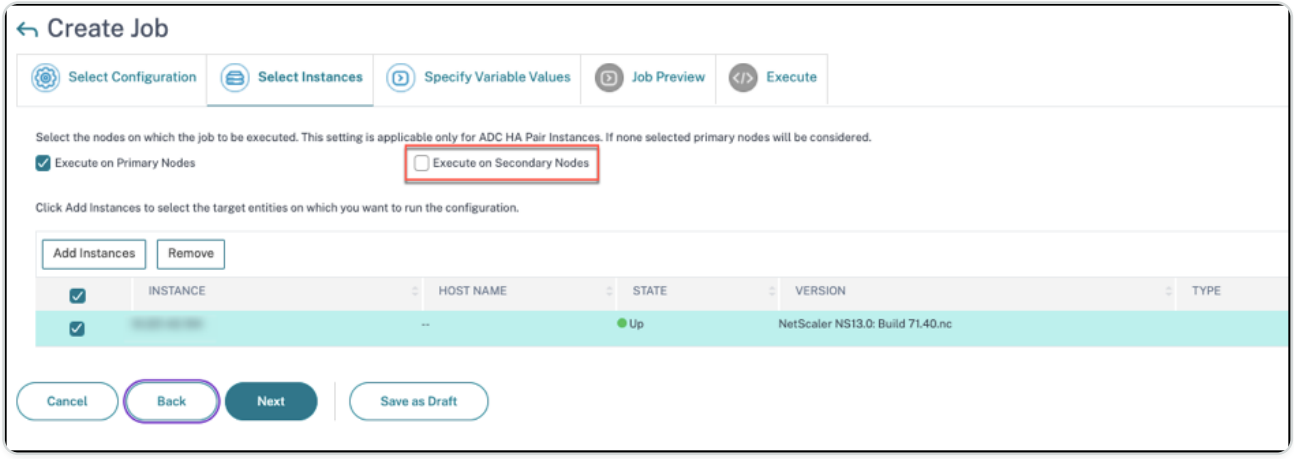
Step 1: Select configuration

In the configuration job workflow, the built-in configuration base template auto-populates under **Select configuration**.



Step 2: Select the instance

The impacted instance is auto-populated under **Select Instances**. Select the instance. If this instance is part of an HA pair, select **Execute on Secondary Nodes**. Click **Next**.



NOTE:

For NetScaler instances in cluster mode, using security advisory, the NetScaler Console supports running the config job only on the cluster configuration coordinator (CCO) node. Run the commands on non-CCO nodes separately.

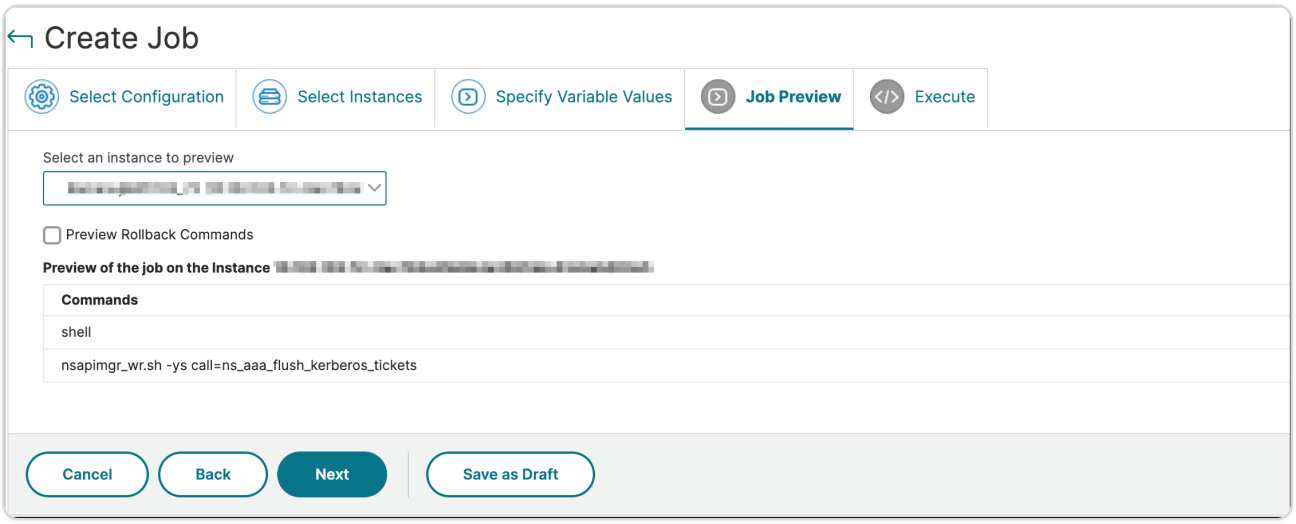
Step 3: Specify variable values

No variable is required to specify in this step. Select **Common Variable Values for all instances** and click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

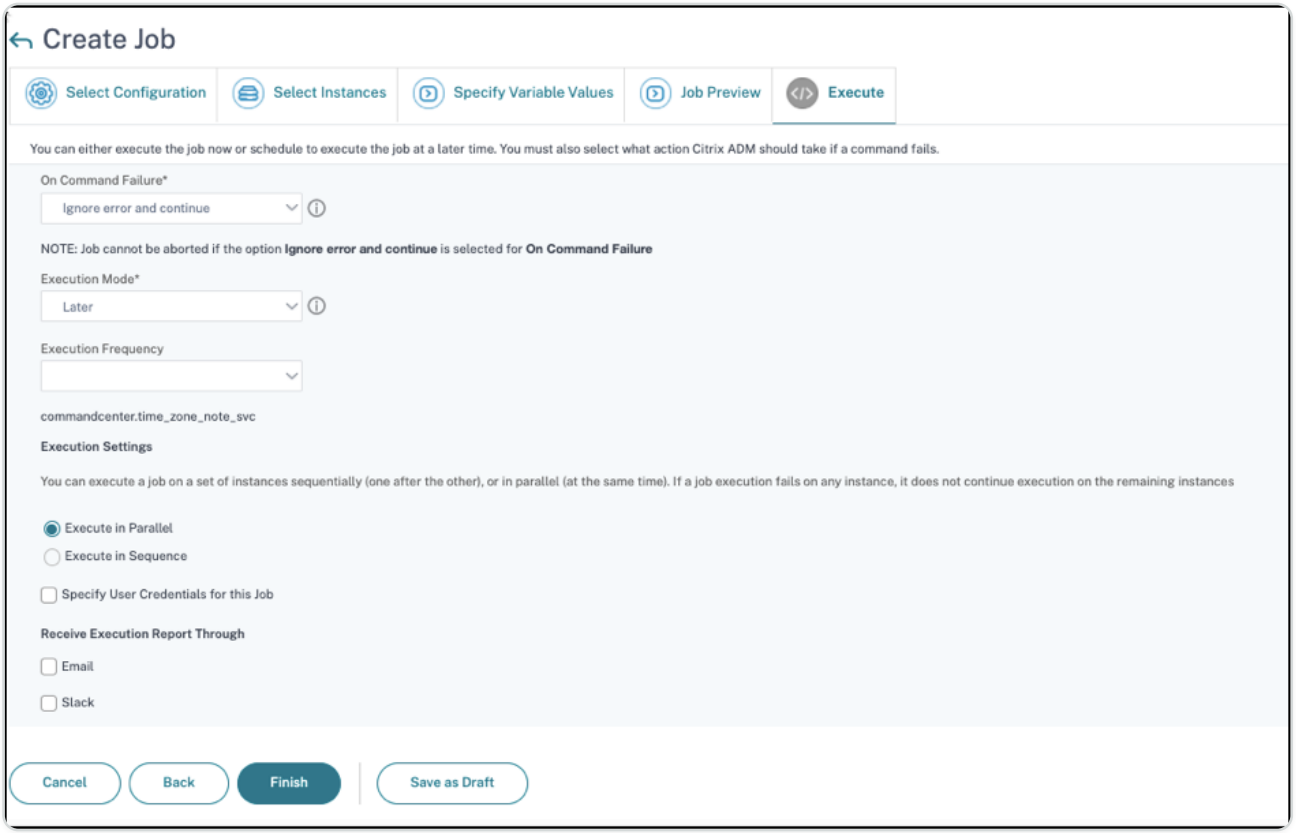
Step 4: Preview the configuration

Previews the variable values having been inserted in the config and click **Next**.



Step 5: Run the job

Click **Finish** to run the configuration job.



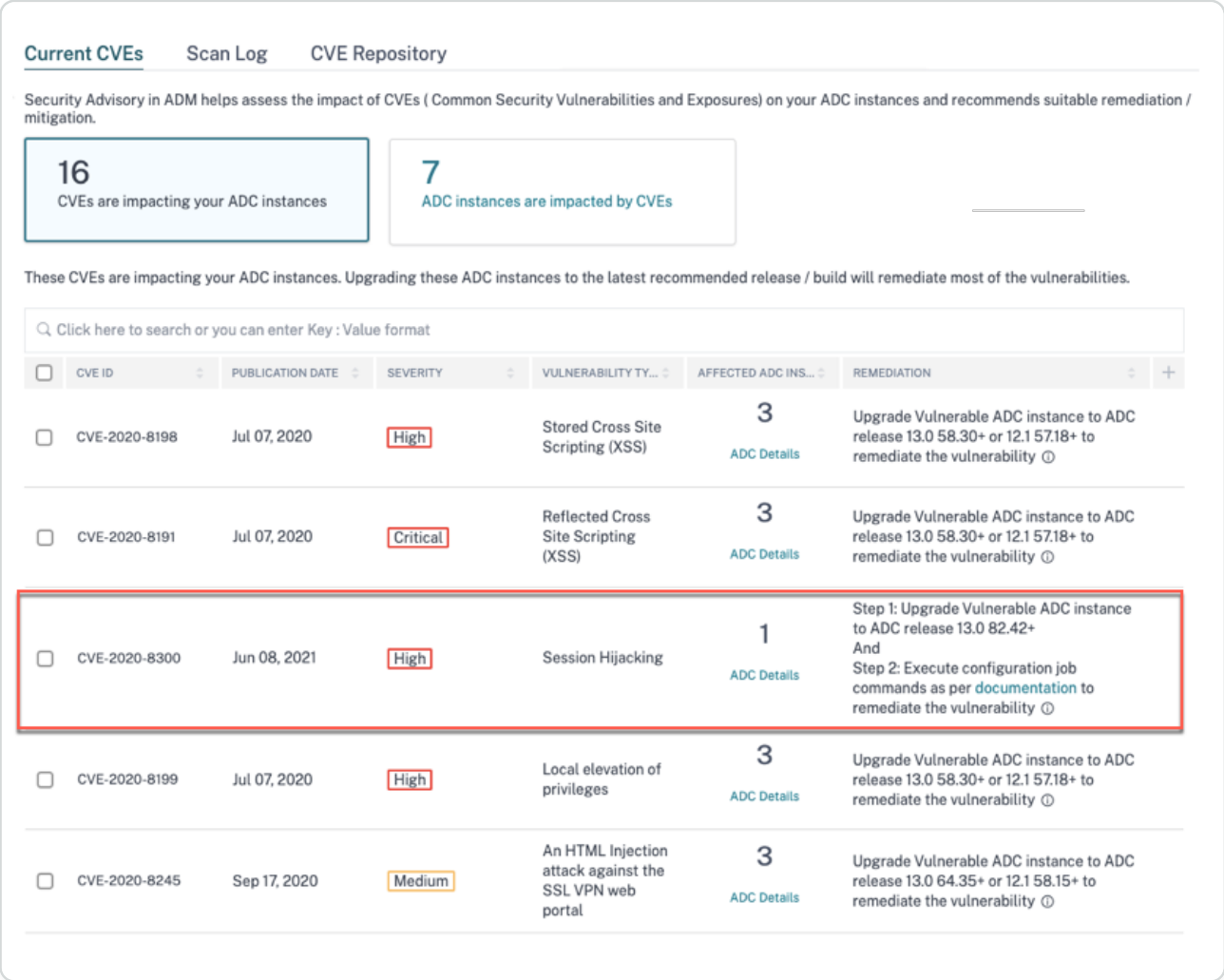
After the job is run, it appears under **Infrastructure > Configuration > Configuration Jobs**.

After completing the two remediation steps for all vulnerable NetScaler instances, you can run an on-demand scan to see the revised security posture.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Remediate vulnerabilities for CVE-2020-8300

In the NetScaler Console security advisory dashboard, under **Current CVEs >** `<number of>` **NetScaler instances are impacted by CVEs**, you can see all the instances vulnerable due to this specific CVE. To check the details of the CVE-2020-8300 impacted instances, select **CVE-2020-8300** and click **View Affected Instances**.

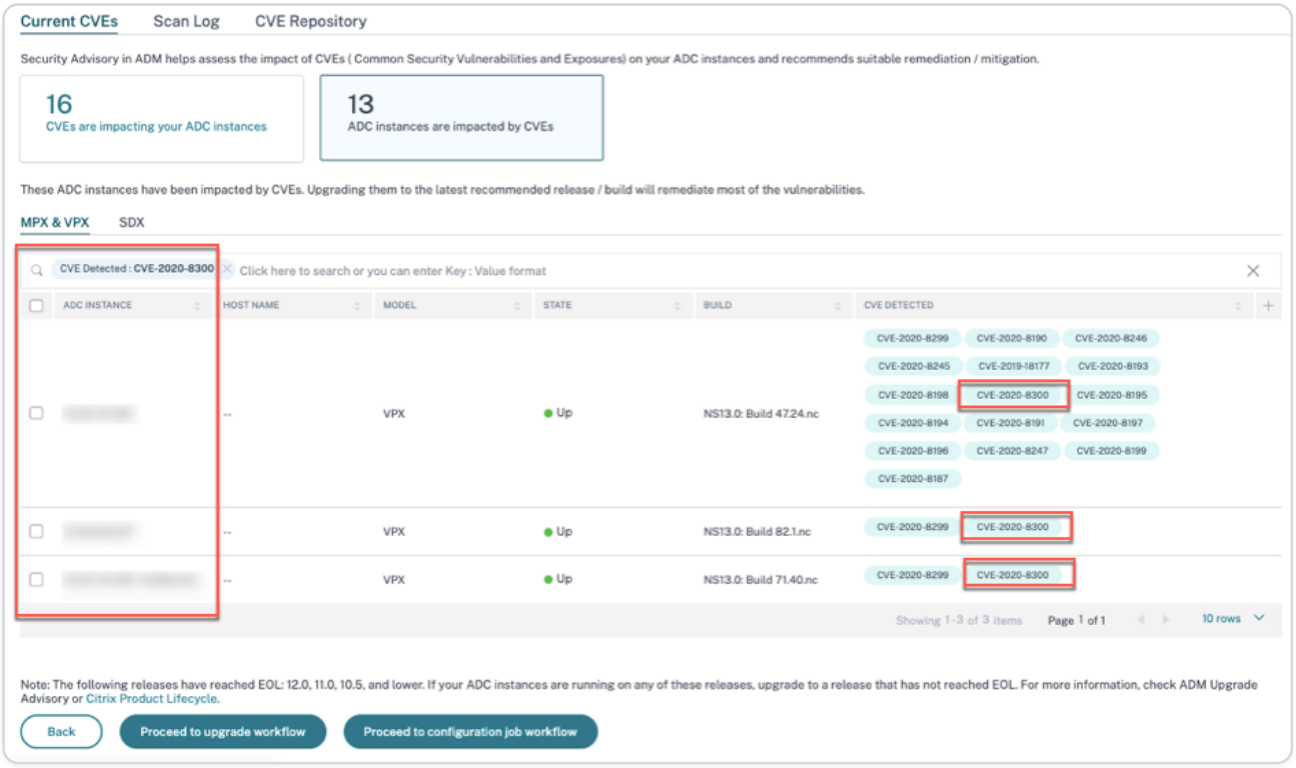


NOTE

For more information about the security advisory dashboard see, Security Advisory.

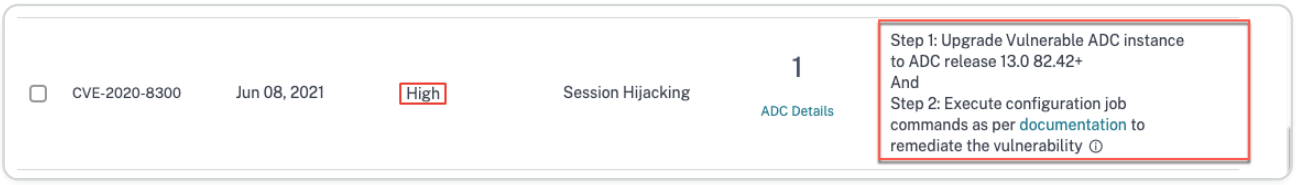
The `<number of>` **NetScaler instances impacted by CVEs** window appears. Here you see the count and details of the NetScaler instances impacted by CVE-2020-8300.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Remediate CVE-2020-8300

For CVE-2020-8300-impacted NetScaler instances, the remediation is a two-step process. In the GUI, under **Current CVEs > NetScaler instances are impacted by CVEs**, you can see step 1 and 2.

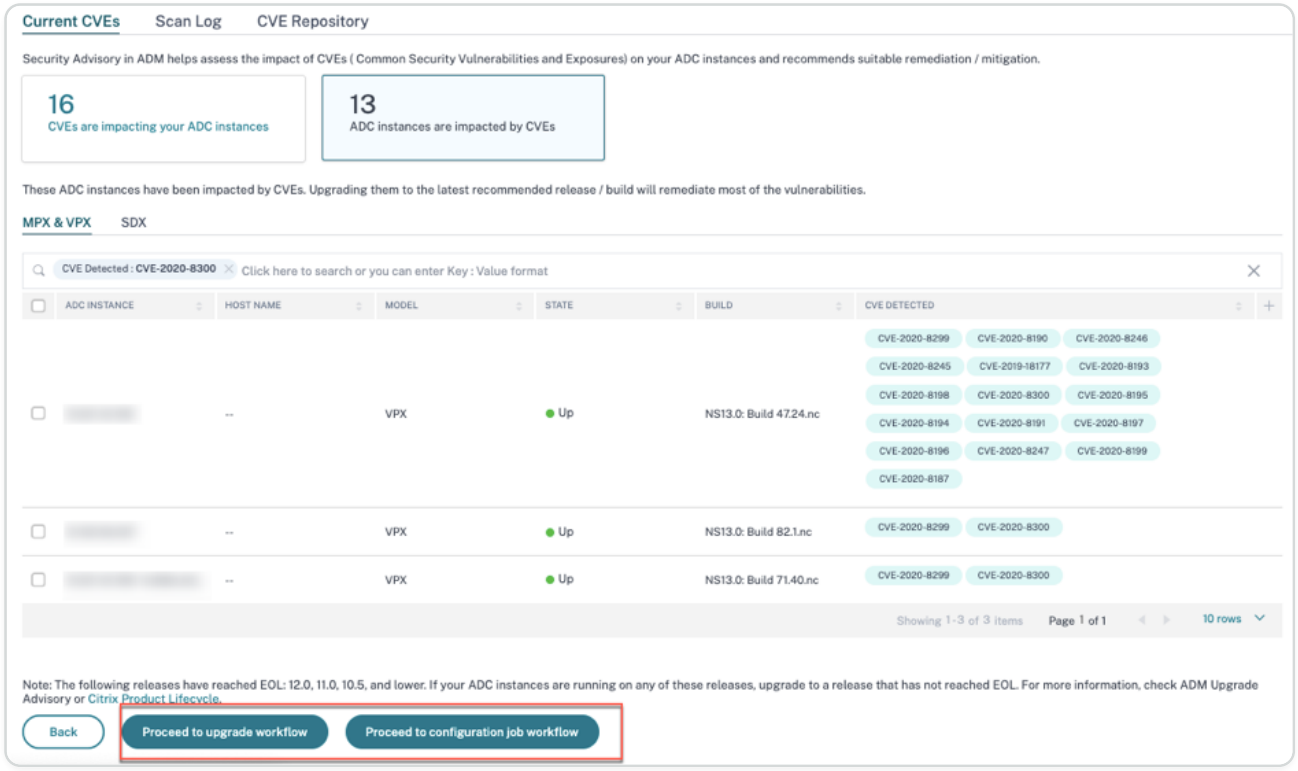


The two steps include:

1. Upgrading the vulnerable NetScaler instances to a release and build that has the fix.
2. Applying the required configuration commands using the customizable built-in configuration template in configuration jobs. Follow this step for each vulnerable NetScaler one at a time and include all SAML actions and SAML profiles for that NetScaler.

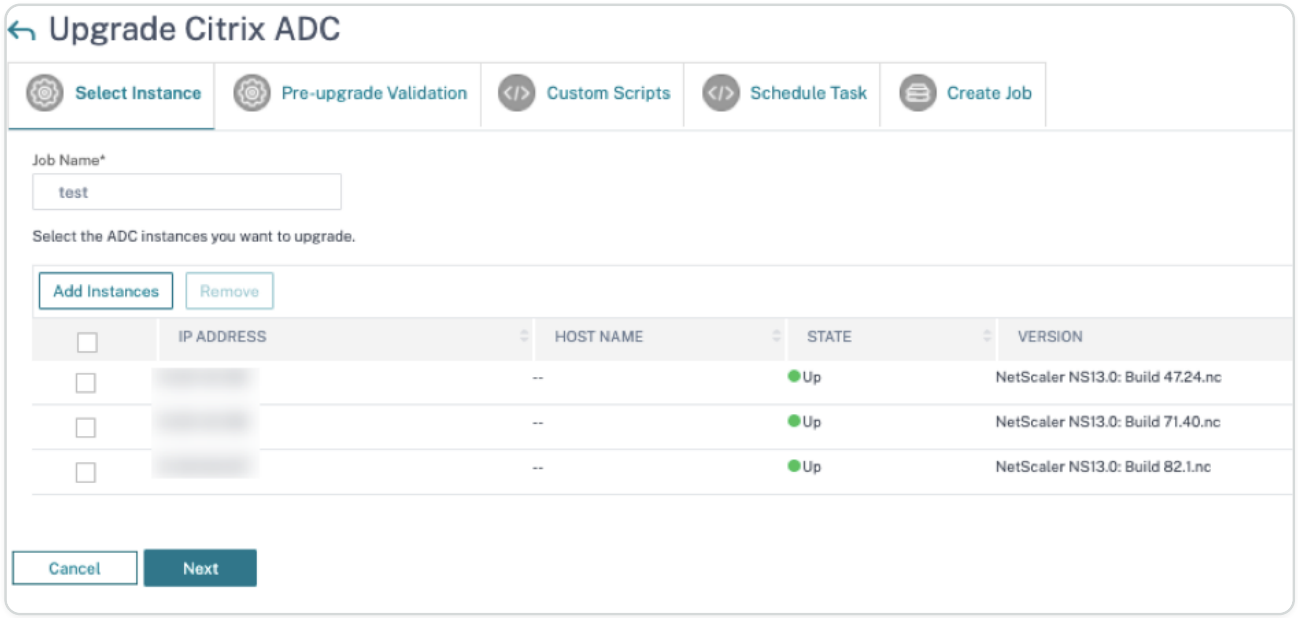
Under **Current CVEs> NetScaler instances impacted by CVEs**, you see two separate workflows for this 2-step remediation process: which are **Proceed to upgrade workflow** and **Proceed to configuration job workflow**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Step 1: Upgrade the vulnerable NetScaler instances

To upgrade the vulnerable instances, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.



For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

This step can be done at once for all the vulnerable NetScaler instances.

Step 2: Apply configuration commands

After you've upgraded the impacted instances, in the `<number of>` **NetScaler instances impacted by CVEs** window, select one instance impacted by CVE-2020-8300 and click **Proceed to configuration job workflow**. The workflow includes the following steps.

1. Customizing the configuration.
2. Reviewing the auto-populated impacted instances.
3. Specifying inputs for variables for the job.
4. Reviewing the final config with variable inputs populated.
5. Running the job.

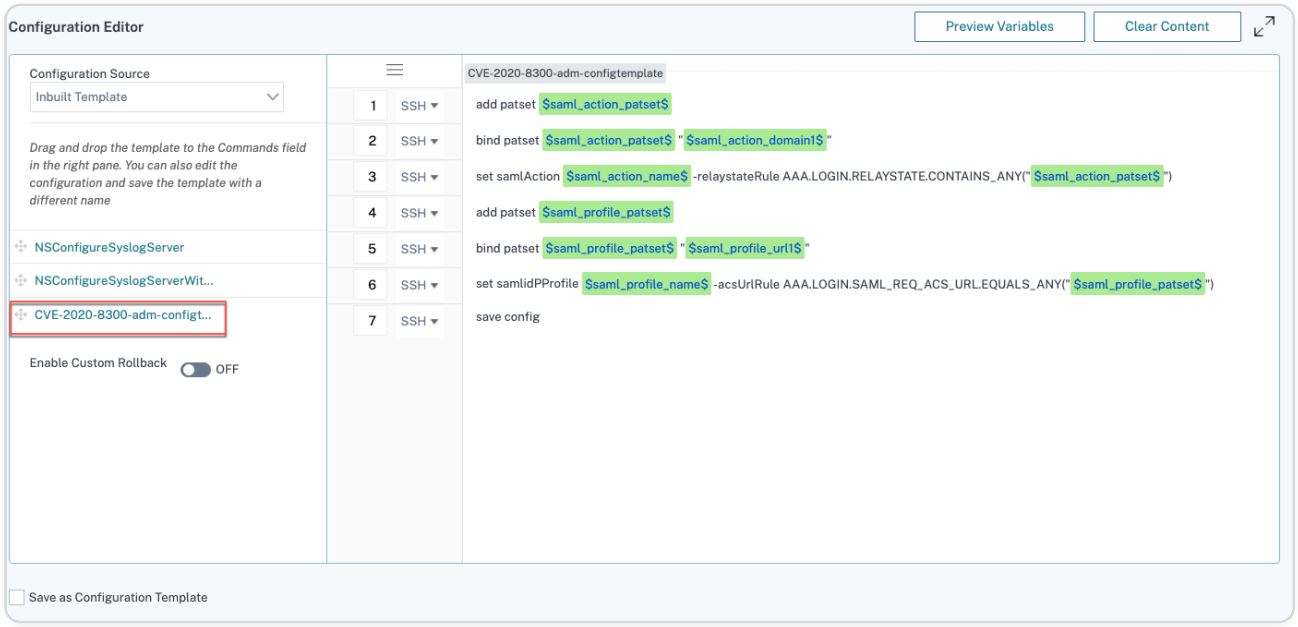
Keep the following points in mind before you select an instance and click **Proceed to configuration job workflow**:

- For a NetScaler instance impacted by multiple CVEs (such as CVE-2020-8300, CVE-2021-22927, CVE-2021-22920, and CVE-2021-22956): when you select the instance and click **Proceed to configuration job workflow**, the built-in configuration template does not auto-populate under Select configuration. Drag and drop the appropriate config job template under **Security Advisory Template** manually to the config job pane on the right side.
- For multiple NetScaler instances that are impacted by CVE-2021-22956 only: you can run config jobs on all instances at once. For example, you've NetScaler 1, NetScaler 2, and NetScaler 3, and all of them are impacted only by CVE-2021-22956. Select all these instances and click **Proceed to configuration job workflow**, and the built-in configuration template auto-populates under **Select configuration**. Refer to the known issue NSADM-80913 in the release notes.
- For multiple NetScaler instances impacted by CVE-2021-22956 and one or more other CVEs (such as CVE-2020-8300, CVE-2021-22927, and CVE-2021-22920), which require remediation to be applied to each NetScaler at a time: when you select these instances and click **Proceed to configuration job workflow**, an error message appears telling you to run the config job on each NetScaler at a time.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 1: Select configuration

In the configuration job workflow, the built-in configuration template auto-populates under **Select configuration**.



Run a separate configuration job for each impacted NetScaler instance, one at a time, and include all SAML actions and SAML profiles for that NetScaler. For example, if you have two vulnerable NetScaler instances each having two SAML actions and two SAML profiles, you must run this configuration job two times. One time per NetScaler covering all its SAML actions and SAML profiles.

NETSCALER 1	NETSCALER2
Job 1: two SAML actions +two SAML profiles	Job 2: two SAML actions +two SAML profiles

Give the job a name and customize the template for the following specifications. The built-in configuration template is only an outline or base template. Customize the template based on your deployment for the following requirements:

a. **SAML actions and their associated domains**

Depending on the number of SAML actions you have in your deployment, you must replicate lines 1–3 and customize the domains for each SAML action.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1	SSH	add patset $saml_action_patset$
2	SSH	bind patset $saml_action_patset$ " $saml_action_domain1$ "
3	SSH	set samlAction $saml_action_name$ -relaystateRule AAA.LOGIN.RELAYSTATE.CONTAINS_ANY(" $saml_action_patset$ ")
4	SSH	add patset $saml_profile_patset$
5	SSH	bind patset $saml_profile_patset$ " $saml_profile_url1$ "
6	SSH	set samlidPProfile $saml_profile_name$ -acsUrlRule AAA.LOGIN.SAML_REQ_ACS_URL.EQUALS_ANY(" $saml_profile_patset$ ")
7	SSH	save config

For example, if you have two SAML actions, repeat lines 1–3 two times and accordingly customize the variable definitions for each SAML action.

And if you have N domains for a SAML action, you must manually type the line `bind patset $saml_action_patset$ “$saml_action_domain1$”` multiple times to ensure that the line appears N times for that SAML action. And change the following variable definition names:

- `saml_action_patset`: is the config template variable, and it represents the value of the name of the pattern set (patset) for the SAML action. You can specify the real value in step 3 of the config job workflow. See the section Step 3: Specify variable values in this doc.
- `saml_action_domain1`: is the config template variable, and it represents the domain name for that specific SAML action. You can specify the real value in step 3, of the config job workflow. See the section Step 3: Specify variable values in this doc.

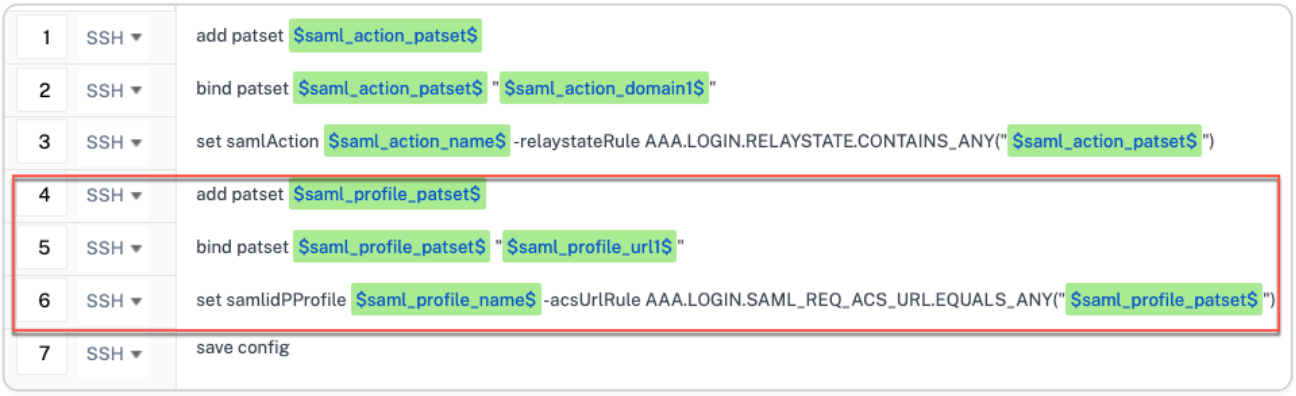
To find all the SAML actions for a device, run the command `show samlaction`.

```
> show samlaction -summary
-------------------------------------------------------------------------------------------------------------------------------------------------------------
     Name            Username field  Decryption key       Encryption key       Url to be redirected to
                    Reject unsigned assertions Issuer name          Two factor Smart Group
-------------------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------
1    SamlSPAct1                      idp_private_public   sp_private_public    https://<IP3>/saml/login
                   ON         http://<IP1>          OFF
2    SamlSPAct2                      idp_private_public   sp_private_public    https://[redacted]/saml/login
                   ON         http://[redacted]     OFF
Done
```

b. **SAML profiles and their associated URLs**

Depending on the number of SAML profiles you have in your deployment, replicate lines 4–6. Customize the URLs for each SAML profile.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For example, if you have two SAML profiles, manually enter lines 4–6 two times and accordingly customize the variable definitions for each SAML action.

And if you have N domains for a SAML action, you must manually type the line `bind patset $saml_profile_patset$ “$saml_profile_url1$”` multiple times to ensure that the line appears N times for that SAML profile. And change the following variable definition names:

- `saml_profile_patset`: is the config template variable, and it represents the value of the name of the pattern set (patset) for the SAML profile. You can specify the real value in step 3, of the config job workflow. See the section Step 3: Specify variable values in this document.
- `saml_profile_url1`: is the config template variable, and it represents the domain name for that specific SAML profile. You can specify the real value in step 3, of the config job workflow. See the section Step 3: Specify variable values in this document.

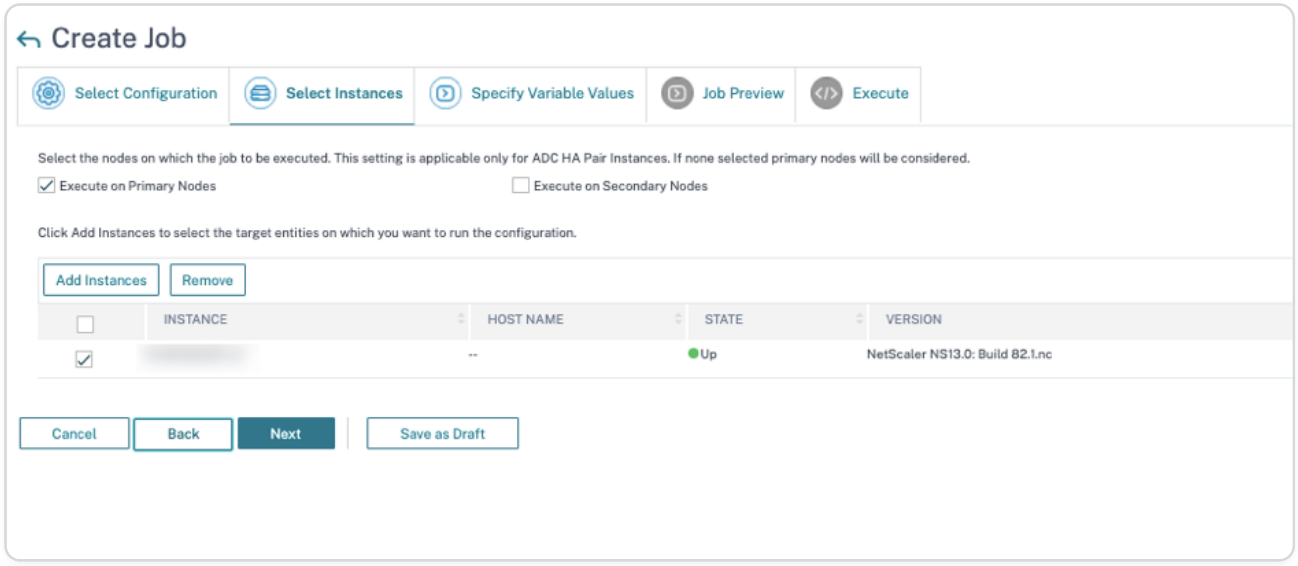
To find all the SAM profiles for a device, run the command `show samlidpProfile`.



Step 2: Select the instance

The impacted instance is auto-populated under **Select Instances**. Select the instance and click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Step 3: Specify variable values

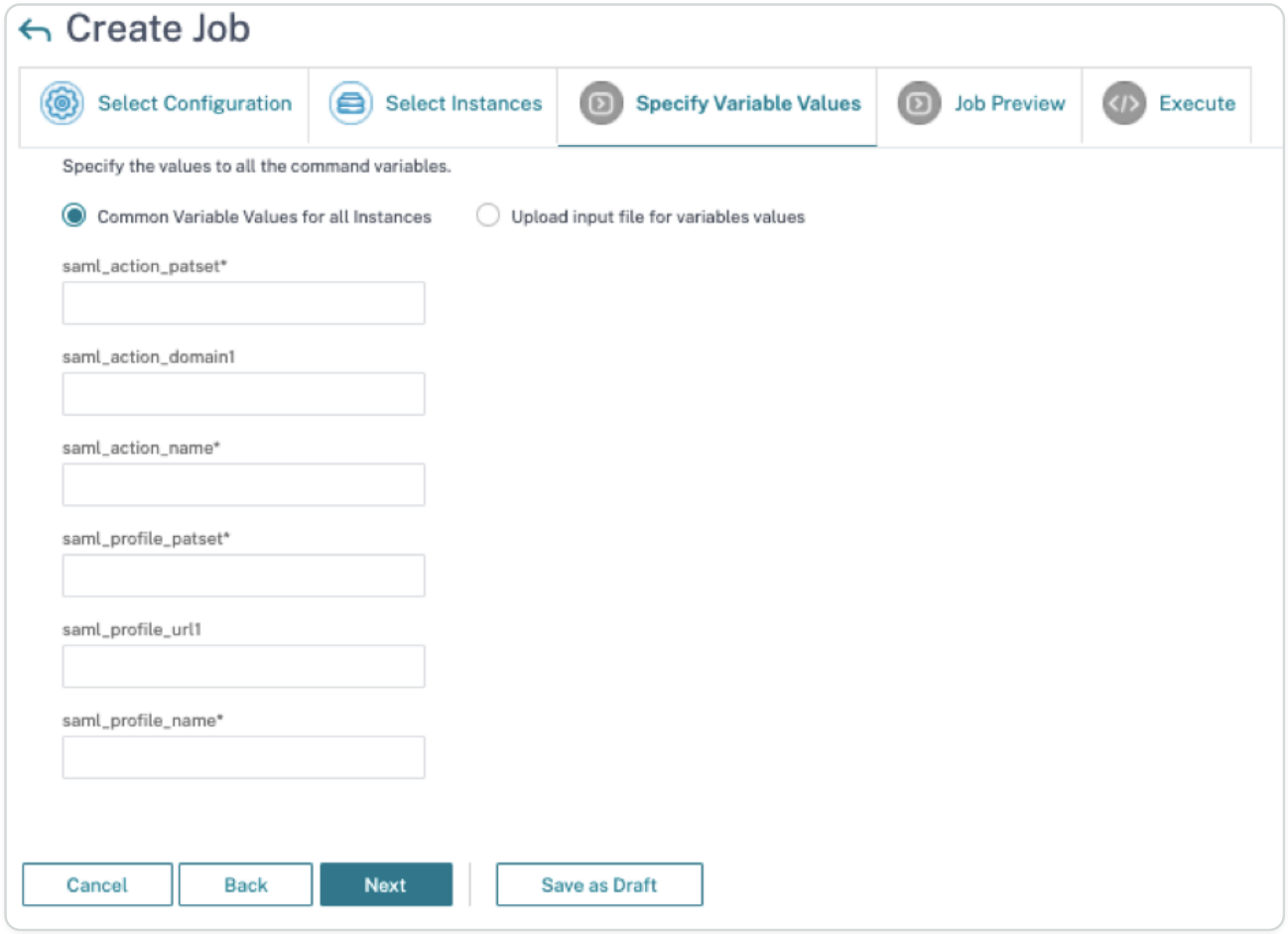
Enter the variable values.

- `saml_action_patset`: add a name for the SAML action
- `saml_action_domain1`: enter a domain in the format `https://<example1.com>/`
- `saml_action_name`: enter the same of the SAML action for which you are configuring the job
- `saml_profile_patset`: add a name for the SAML profile
- `saml_profile_url1`: enter the URL is this format `https://<example2.com>/cgi/samlauth`
- `saml_profile_name`: enter the same of the SAML profile for which you are configuring the job

NOTE

For URLs, the extension is not always `cgi/samlauth`. It depends on what third-party authorization you have, and accordingly you must put the extension.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



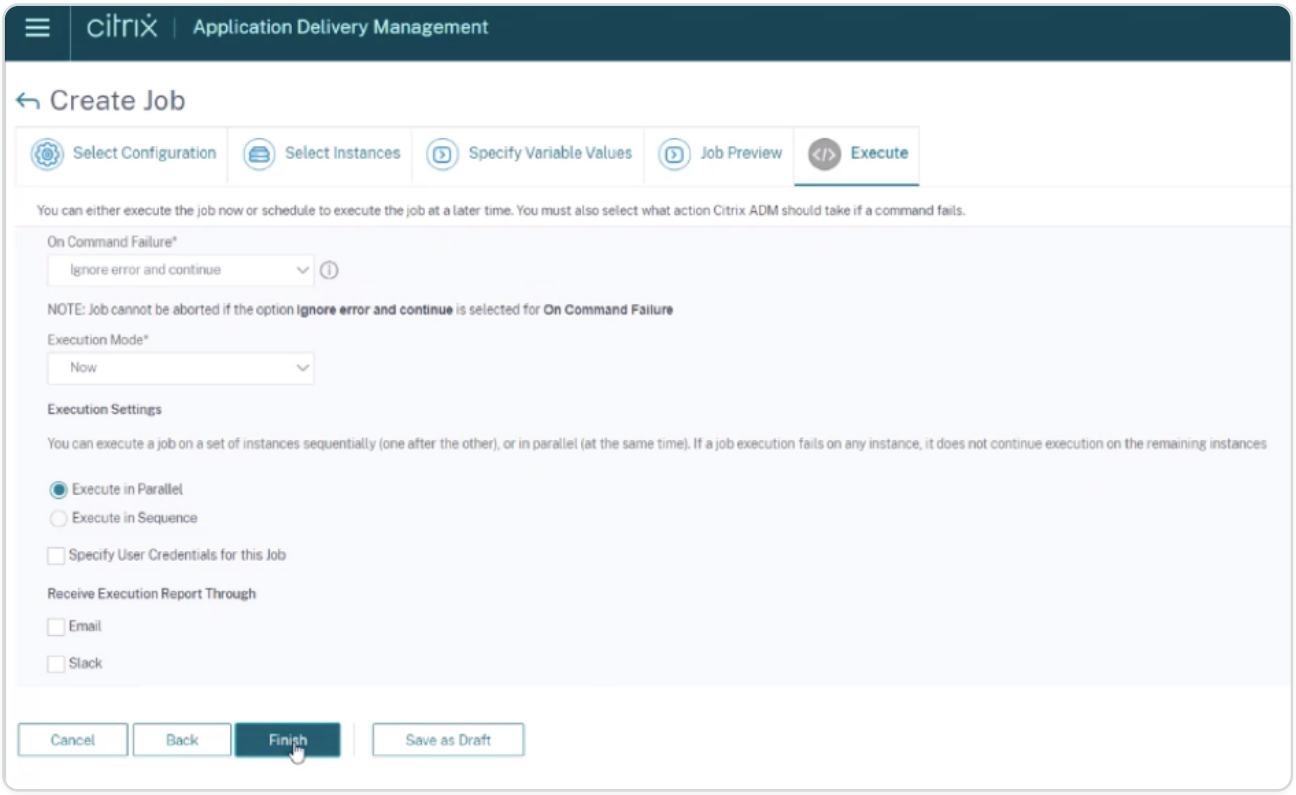
Step 4: Preview the configuration

Previews the variable values having been inserted in the config and click **Next**.

Step 5: Run the job

Click **Finish** to run the configuration job.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



After the job is run, it appears under **Infrastructure > Configuration > Configuration Jobs**.

After completing the two remediation steps for all vulnerable NetScaler instances, you can run an on-demand scan to see the revised security posture.

Points to note for NetScaler Console Express account

The NetScaler Console Express account has limited features, which include limitations of two configuration jobs only. To know more about NetScaler Console Express account, see Manage NetScaler Console resources using Express account. For CVE-2020-8300 remediation, you must run as many configuration jobs as the number of your vulnerable NetScaler instances. So, if you have an Express account and need to run more than two configuration jobs, follow this workaround.

Workaround: Run two configuration jobs for two vulnerable NetScaler instances and then delete both the jobs to continue running the next two jobs for the next two vulnerable NetScaler instances. Continue this until you have covered all vulnerable instances. Before deleting the jobs, you can download the report for future reference. To download the report, under **Network > Jobs**, select the jobs and click **Download** under **Actions**.

Example: If you have six vulnerable NetScaler instances, run two configuration jobs on two vulnerable instances respectively and then delete both the configuration jobs. Repeat this step another two times. At the end, you would have run six config jobs for six NetScaler instances

© 1997–2026 Citrix Systems, Inc. All rights reserved.

respectively. In the NetScaler Console UI under **Infrastructure > Jobs**, you see only the last two configuration jobs.

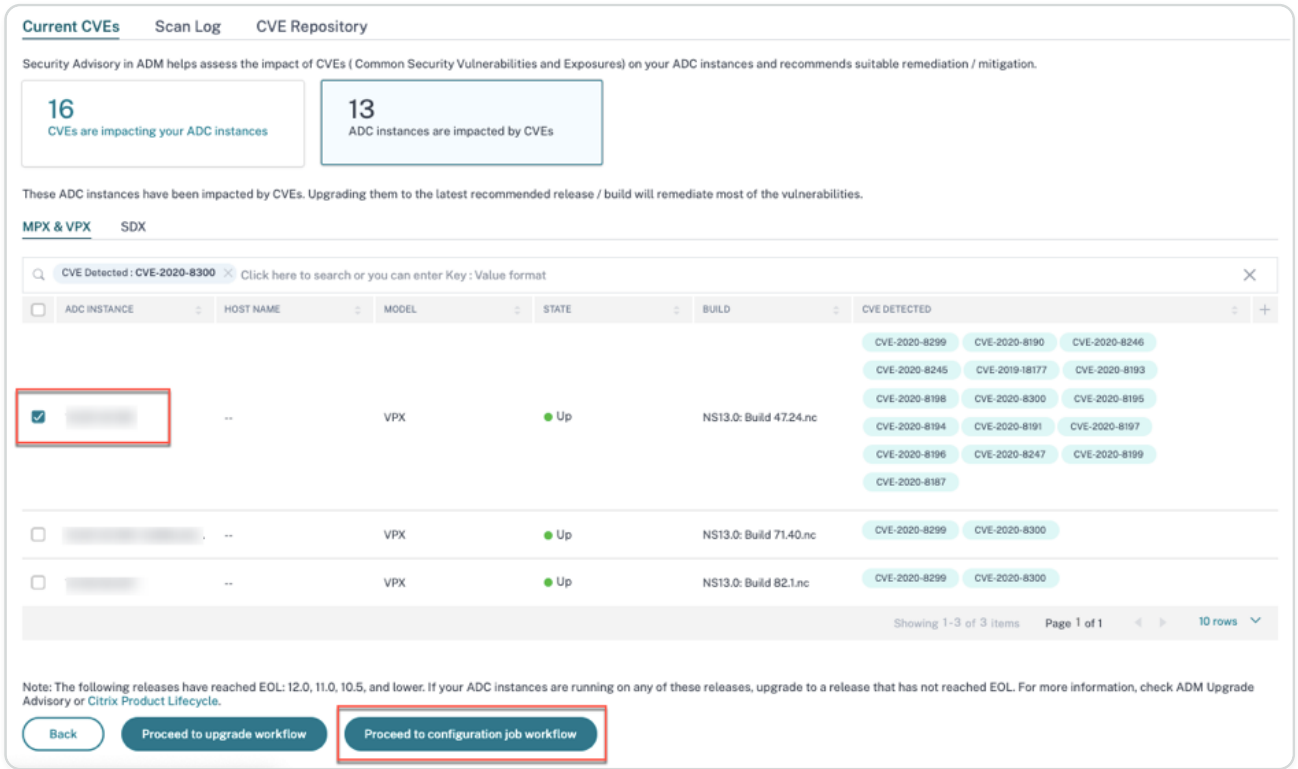
Scenario

In this scenario, three NetScaler instances are vulnerable to CVE-2020-8300 and you need to remediate all the instances. Follow these steps:

1. Upgrade all the three NetScaler instances by following the steps given in the **Upgrade an instance** section in this document.
2. Apply the config patch to one NetScaler at a time, using the configuration job workflow. See the steps given in the **Apply configuration commands** section in this document.

The vulnerable NetScaler 1 has the following configuration:

TWO SAML ACTIONS	TWO SAML PROFILES



Select NetScaler 1 and click **Proceed to configuration job workflow**. The built-in template auto-populates. Next, give a job name and customize the template according to the given configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following tables list the variable definitions for customized parameters.

Table 1. Variable definitions for SAML action

NETSCALER CONFIGURATION	VARIABLE DEFINITION FOR PATSET	VARIABLE DEFINITION FOR SAML ACTION NAME	VARIABLE DEFINITION FOR DOMAIN
SAML action 1 has one domain	saml_action_patset1	saml_action_name1	saml_action_domain 1
SAML action 2 has two domains	saml_action_patset2	saml_action_name2	saml_action_domain 2, saml_action_domain 3

Table 2. Variable definitions for SAML profile

NETSCALER CONFIGURATION	VARIABLE DEFINITION FOR PATSET	VARIABLE DEFINITION FOR SAML PROFILE NAME	VARIABLE DEFINITION FOR URL
SAML profile 1 has one URL	saml_profile_patset1	saml_profile_name1	saml_profile_url1
SAML profile 2 has two URLs	saml_profile_patset2	saml_profile_name2	saml_profile_url2, saml_profile_url3

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Under **Select Instances**, select NetScaler 1 and click **Next**. The **Specify Variable Values** window appears. In this step, you need to provide values for all the variables defined in the previous step.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Specify the values to all the command variables.

(•) Common Variable Values for all Instances ( ) Upload input file for variables values

saml_action_patset1
pat1

saml_action_domain1
https://d1.com/

saml_action_name1
samlSPAct1

saml_action_patset2
pat2

saml_action_domain2
https://d2.com/

saml_action_domain3
https://d3.com/

saml_action_name2
samlSPAct2

saml_profile_patset1
pat3

saml_profile_url1
https://example1.com/cgi/samlautl

saml_profile_name1
samDPProf2

saml_profile_patset2
pat4

saml_profile_url2
hhttps://example2.com/cgi/samlau

saml_profile_url3
hhttps://example3.com/cgi/samlau

saml_profile_name2
samDPProf2

Cancel Back Next | Save as Draft

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Next, review the variables.

Click **Next** and then click **Finish** to run the job.

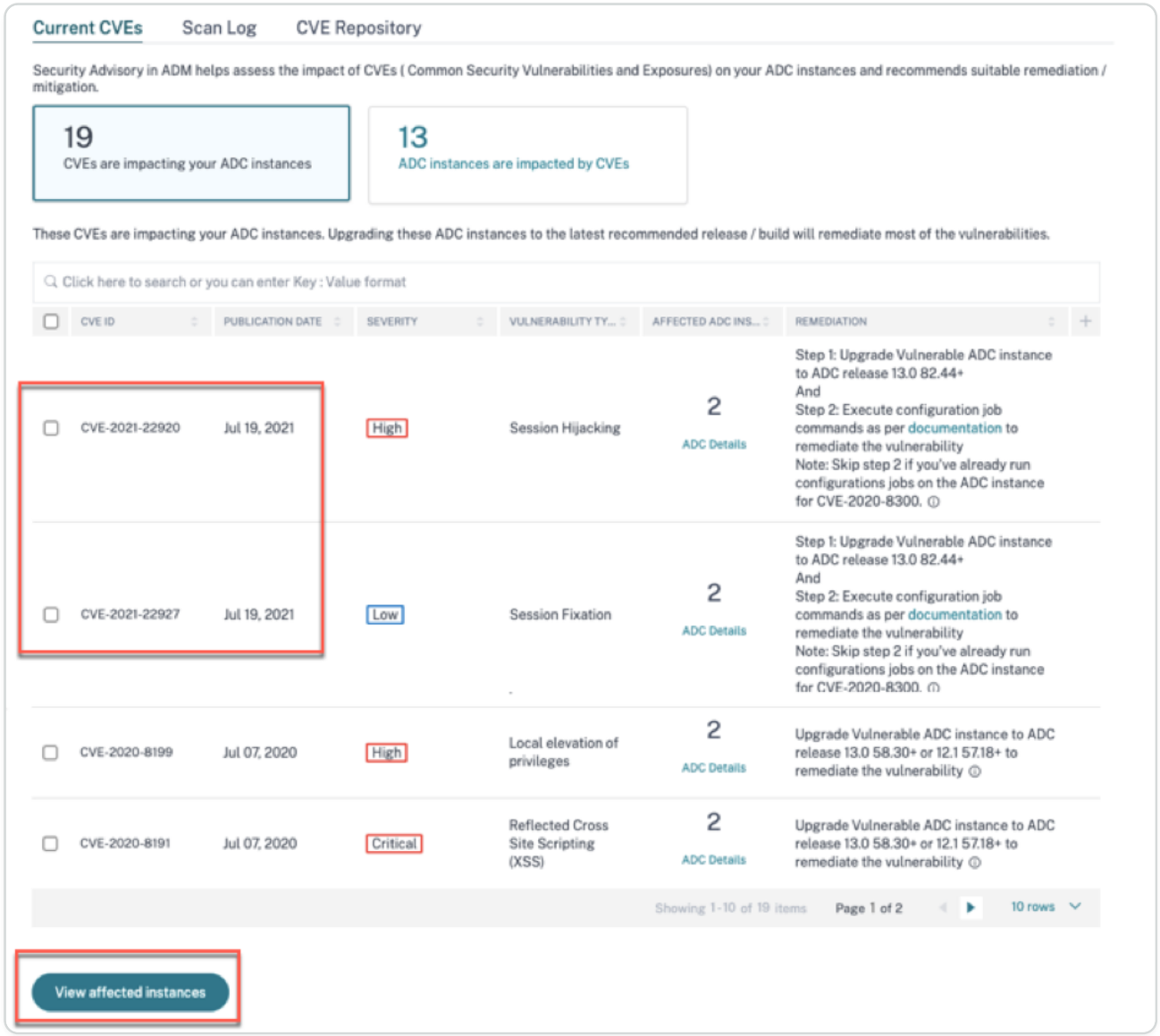
After the job is run, it appears under **Infrastructure > Configuration > Configuration Jobs**.

After completing the two remediation steps for NetScaler 1, follow the same steps to remediate NetScaler 2 and NetScaler 3. After remediation is complete, you can run an on-demand scan to see the revised security posture.

Remediate vulnerabilities for CVE-2021-22927 and CVE-2021-22920

In the NetScaler Console security advisory dashboard, under **Current CVEs > `<number of>` NetScaler instances are impacted by CVEs**, you can see all the instances vulnerable due to CVE-2021-22927 and CVE-2021-22920. To check the details of the instances impacted by these two CVEs, select one or more CVEs and click **View Affected Instances**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

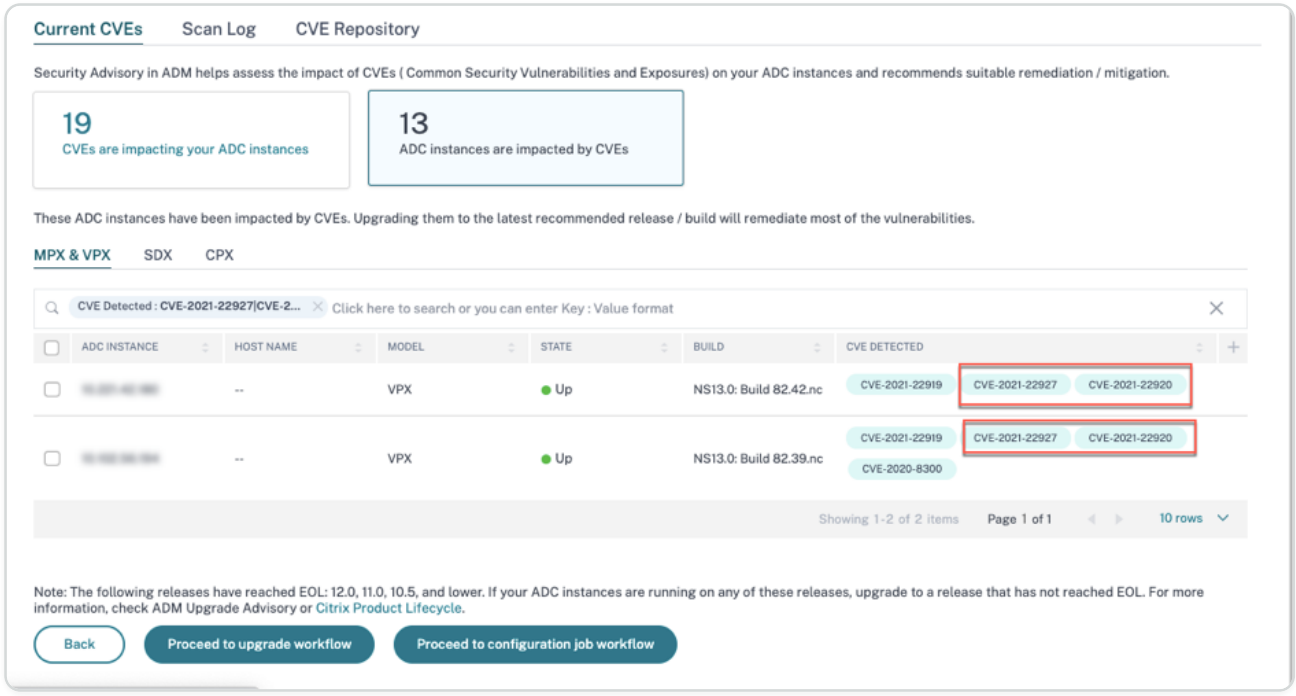


NOTE

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2021-22927 and CVE-2021-22920 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**. For more information about the security advisory dashboard see, Security Advisory.

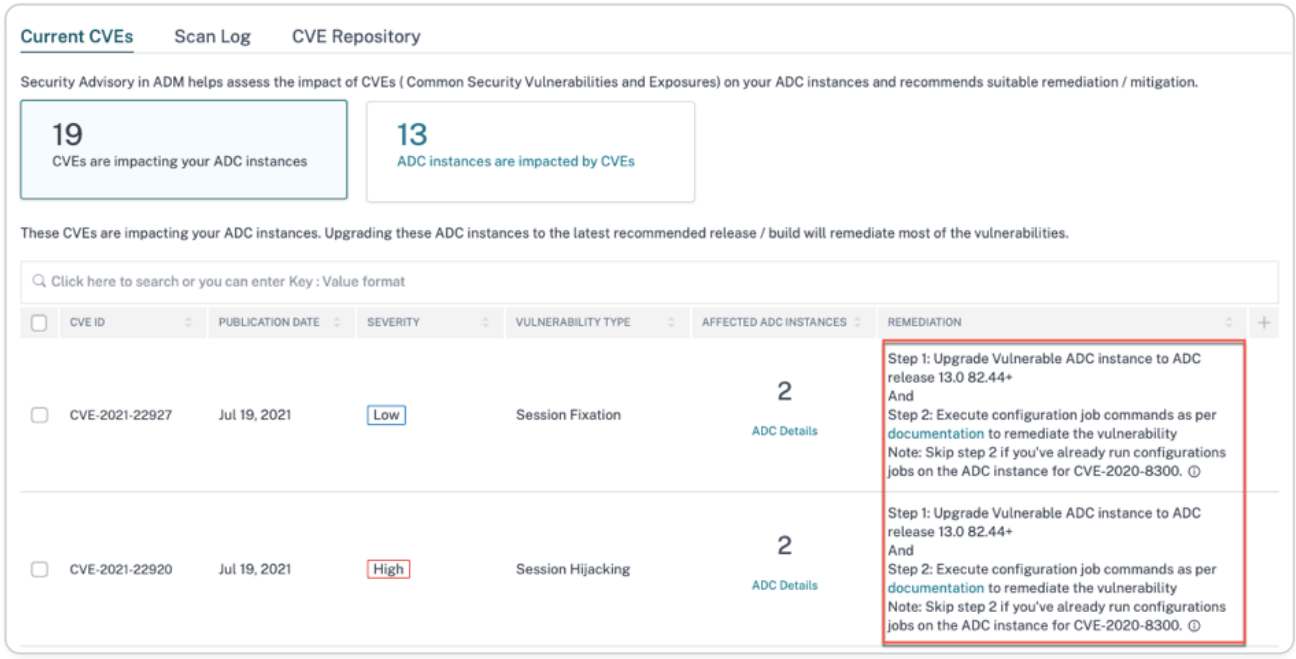
The `<number of>` **NetScaler instances impacted by CVEs** window appears. In the following screen capture, you can see the count and details of the NetScaler instances impacted by CVE-2021-22927 and CVE-2021-22920.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Remediate CVE-2021-22927 and CVE-2021-22920

For CVE-2021-22927 and CVE-2021-22920 impacted NetScaler instances, the remediation is a two-step process. In the GUI, under **Current CVEs > NetScaler instances are impacted by CVEs**, you can see step 1 and 2.



The two steps include:

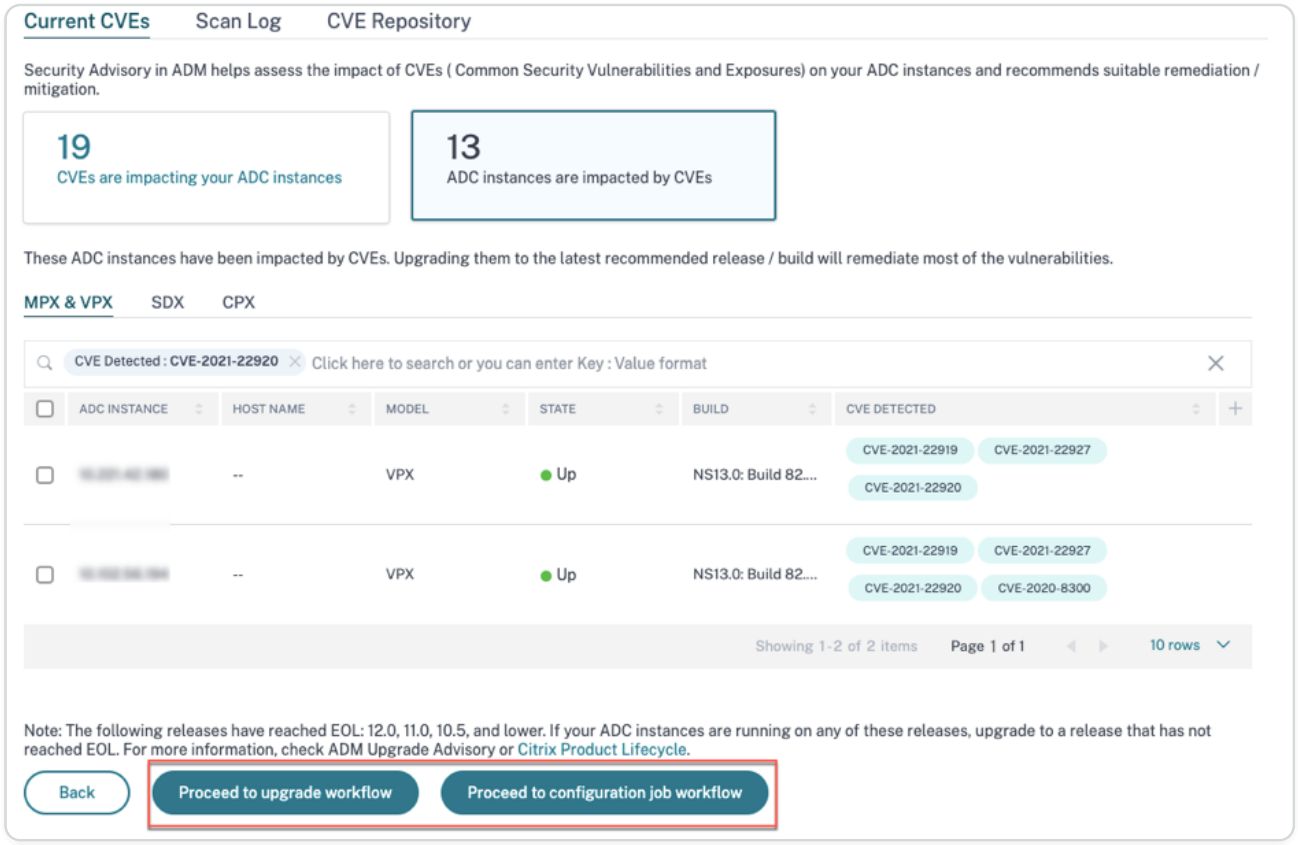
1. Upgrading the vulnerable NetScaler instances to a release and build that has the fix.
2. Applying the required configuration commands using the customizable built-in configuration template in configuration jobs. Follow this step for each vulnerable NetScaler one at a time and include all SAML actions for that NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

Skip step 2 if you've already run configuration jobs on the NetScaler instance for CVE-2020-8300.

Under **Current CVEs> NetScaler instances impacted by CVEs**, you see two separate workflows for this 2-step remediation process: which are **Proceed to upgrade workflow** and **Proceed to configuration job workflow**.



Step 1: Upgrade the vulnerable NetScaler instances

To upgrade the vulnerable instances, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

NOTE

This step can be done at once for all the vulnerable NetScaler instances. **Note**

After you have completed step 1 for all the NetScaler instances vulnerable to CVE-2021-22920 and CVE-2021-22927, do an on-demand scan. The updated security posture under **Current CVEs** helps you understand if the NetScaler instances are still vulnerable to any of these CVEs. From the new posture, you can also check if you need to run configuration jobs. If you've already applied the appropriate configuration jobs to the NetScaler instance for CVE-2020-8300 and now you have upgraded the NetScaler instance, after doing the on-demand scan the instance no longer shows as vulnerable for CVE-2020-8300, CVE-2021-22920, and CVE-2021-22927.

Step 2: Apply configuration commands

After you've upgraded the impacted instances, in the `<number of` **> NetScaler instances impacted by CVEs** window, select one instance impacted by CVE-2021-22927 and CVE-2021-22920 and click **Proceed to configuration job workflow**. The workflow includes the following steps.

1. Customizing the configuration.
2. Reviewing the auto-populated impacted instances.
3. Specifying inputs for variables for the job.
4. Reviewing the final config with variable inputs populated.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

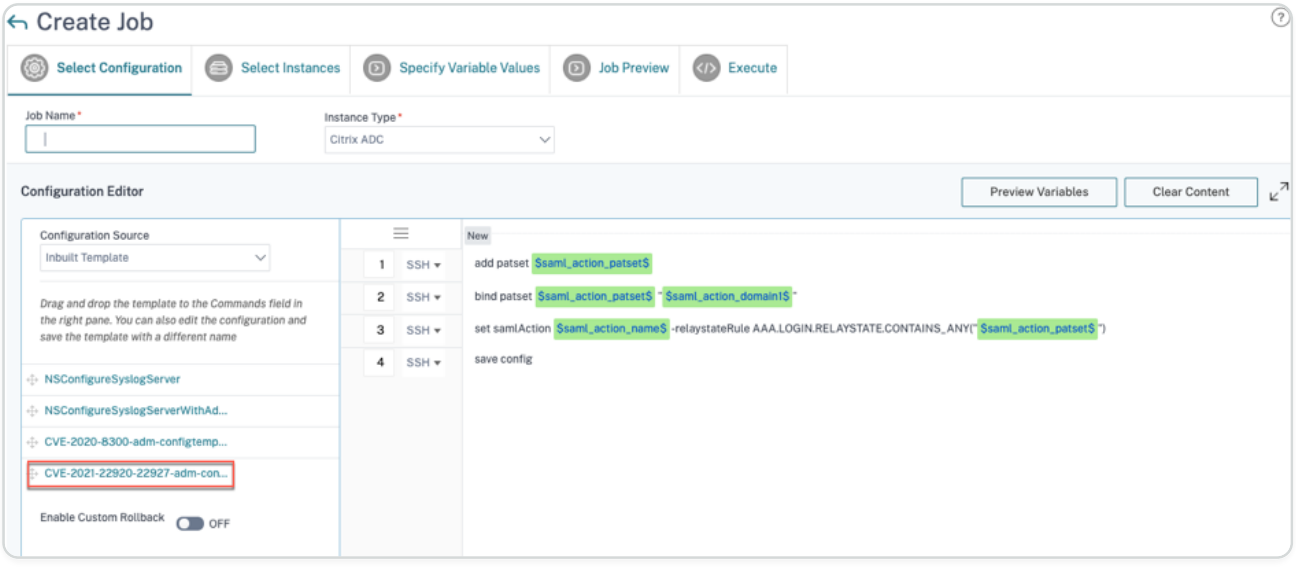
5. Running the job.

Keep the following points in mind before you select an instance and click **Proceed to configuration job workflow**:

- For a NetScaler instance impacted by multiple CVEs (such as CVE-2020-8300, CVE-2021-22927, CVE-2021-22920, and CVE-2021-22956): when you select the instance and click **Proceed to configuration job workflow**, the built-in configuration template does not auto-populate under Select configuration. Drag and drop the appropriate config job template under **Security Advisory Template** manually to the config job pane on the right side.
- For multiple NetScaler instances that are impacted by CVE-2021-22956 only: you can run config jobs on all instances at once. For example, you've NetScaler 1, NetScaler 2, and NetScaler 3, and all of them are impacted only by CVE-2021-22956. Select all these instances and click **Proceed to configuration job workflow**, and the built-in configuration template auto-populates under **Select configuration**. Refer to the known issue NSADM-80913 in the release notes.
- For multiple NetScaler instances impacted by CVE-2021-22956 and one or more other CVEs (such as CVE-2020-8300, CVE-2021-22927, and CVE-2021-22920), which require remediation to be applied to each NetScaler at a time: when you select these instances and click **Proceed to configuration job workflow**, an error message appears telling you to run the config job on each NetScaler at a time.

Step 1: Select configuration

In the configuration job workflow, the built-in configuration base template auto-populates under **Select configuration**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

If the NetScaler instance selected in step 2 for applying configuration commands, is vulnerable to CVE-2021-22927, CVE-2021-22920, and also CVE-2020-8300, the base template for CVE-2020-8300 is auto-populated. The CVE-2020-8300 template is a super set of the config commands required for all the three CVEs. Customize this base template according to your NetScaler instance deployment and requirement.

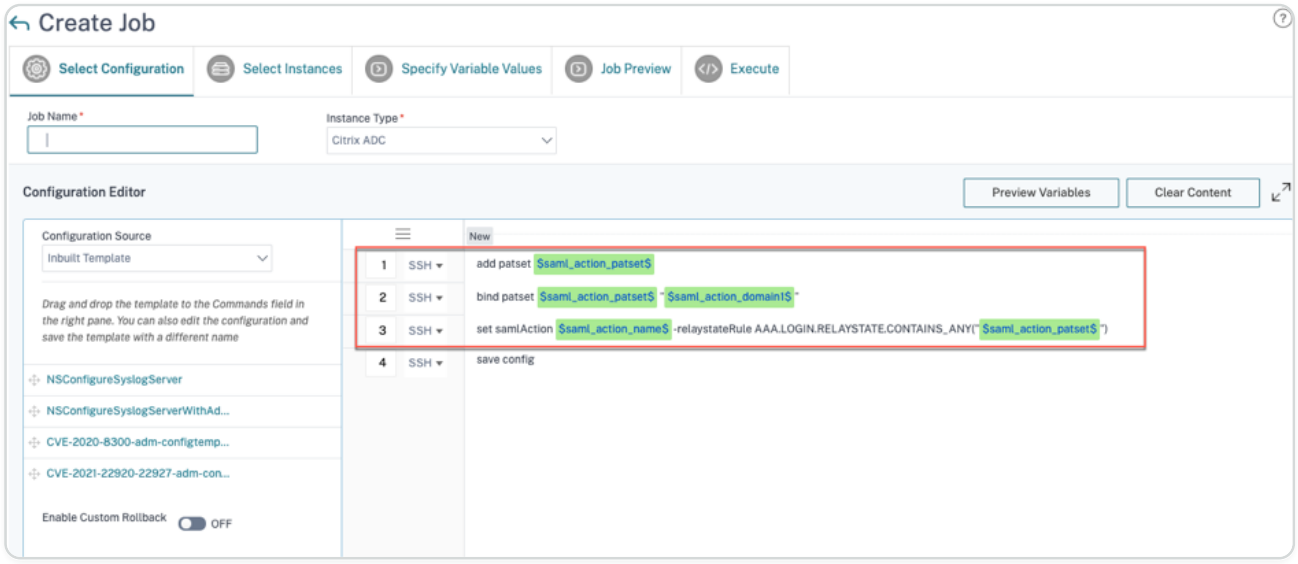
You must run a separate configuration job for each impacted NetScaler instance, one at a time, and include all SAML actions for that NetScaler. For example, if you have two vulnerable NetScaler instances each having two SAML actions, you must run this configuration job two times. One time per NetScaler covering all its SAML actions.

NETSCALER 1	NETSCALER 2
Job 1: two SAML actions	Job 2: two SAML actions

Give the job a name and customize the template for the following specifications. The built-in configuration template is only an outline or base template. Customize the template based on your deployment for the following requirements:

a. **SAML actions and their associated domains**

Depending on the number of SAML actions you have in your deployment, you must replicate lines 1–3 and customize the domains for each SAML action.



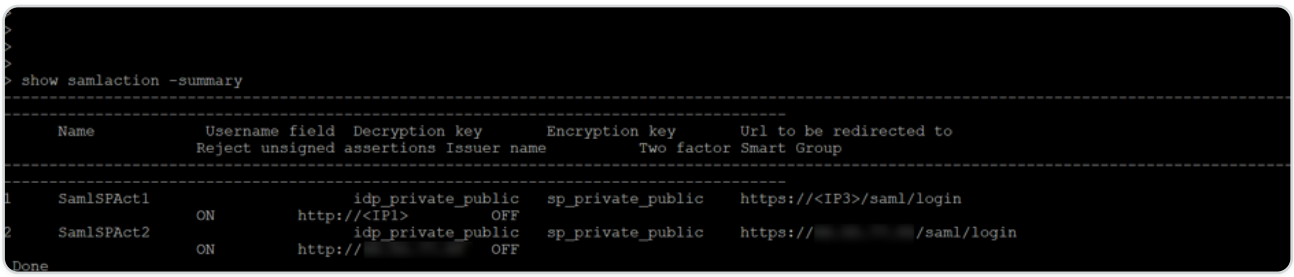
For example, if you have two SAML actions, repeat lines 1–3 two times and accordingly customize the variable definitions for each SAML action.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

And if you have N domains for a SAML action, you must manually type the line `bind patset $saml_action_patset$ “$saml_action_domain1$”` multiple times to ensure that the line appears N times for that SAML action. And change the following variable definition names:

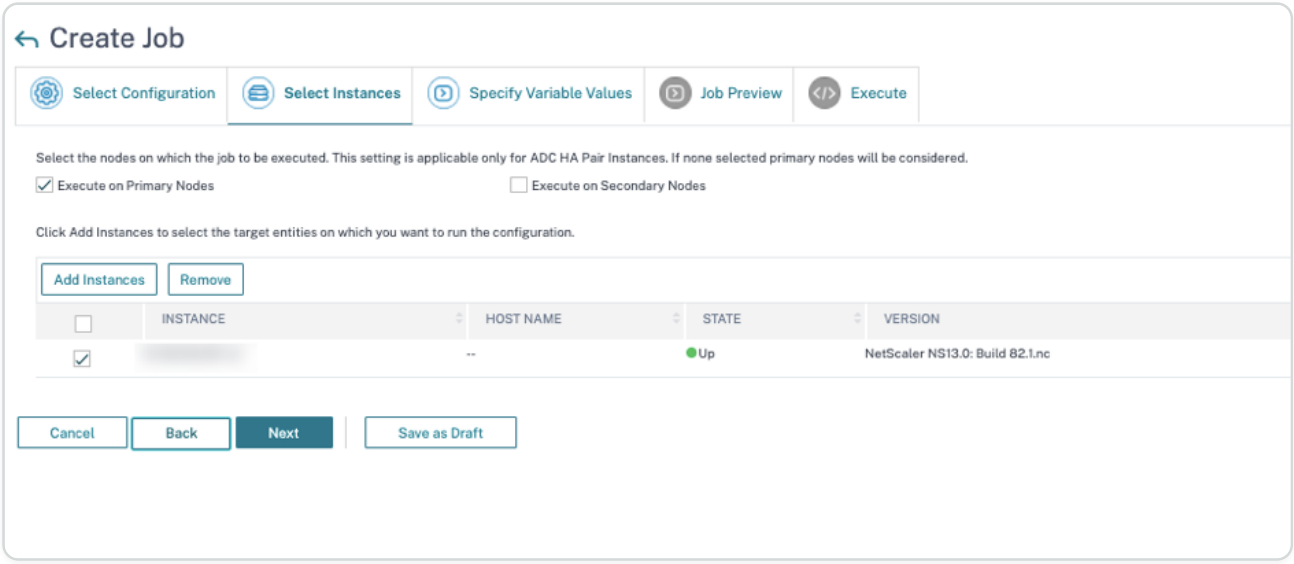
- `saml_action_patset`: is the config template variable, and it represents the value of the name of the pattern set (patset) for the SAML action. You can specify the real value in step 3 of the config job workflow. See the section Step 3: Specify variable values in this doc.
- `saml_action_domain1`: is the config template variable, and it represents the domain name for that specific SAML action. You can specify the real value in step 3, of the config job workflow. See the section Step 3: Specify variable values in this doc.

To find all the SAML actions for a device, run the command `show samlaction`.



Step 2: Select the instance

The impacted instance is auto-populated under **Select Instances**. Select the instance and click **Next**.



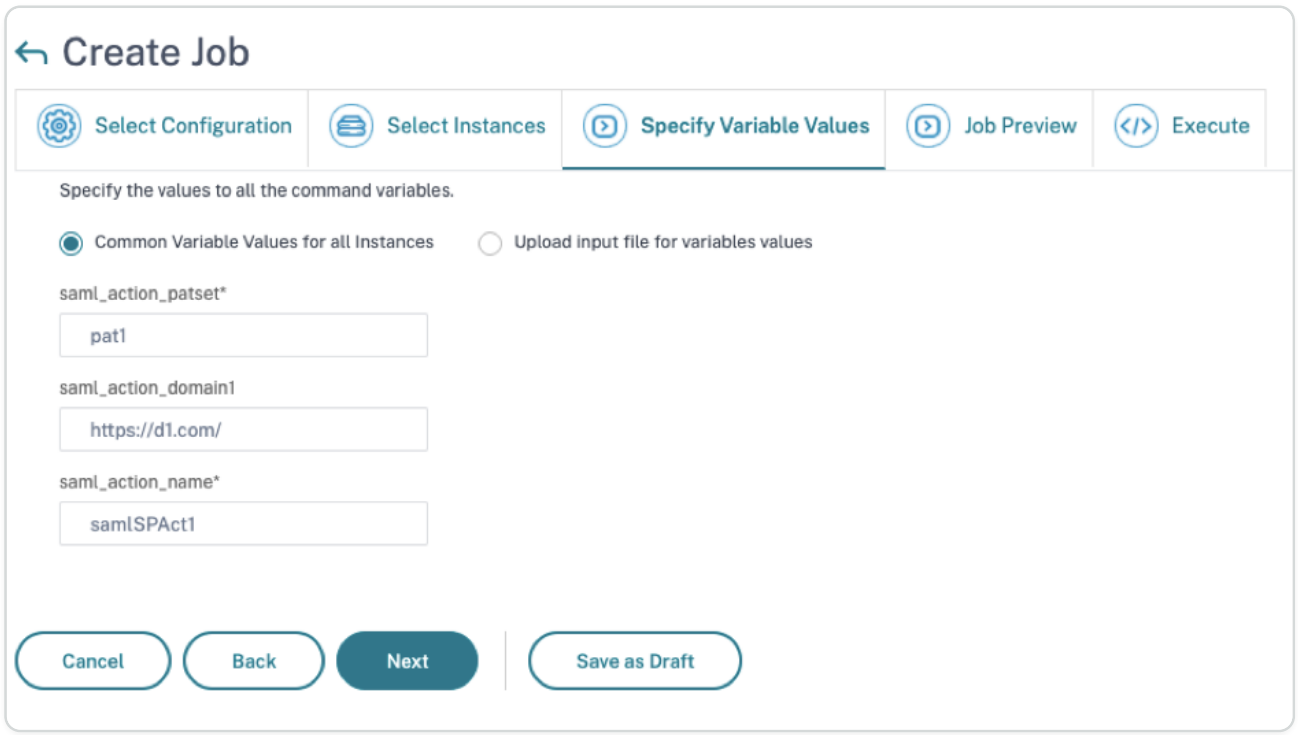
Step 3: Specify variable values

Enter the variable values.

- `saml_action_patset`: add a name for the SAML action

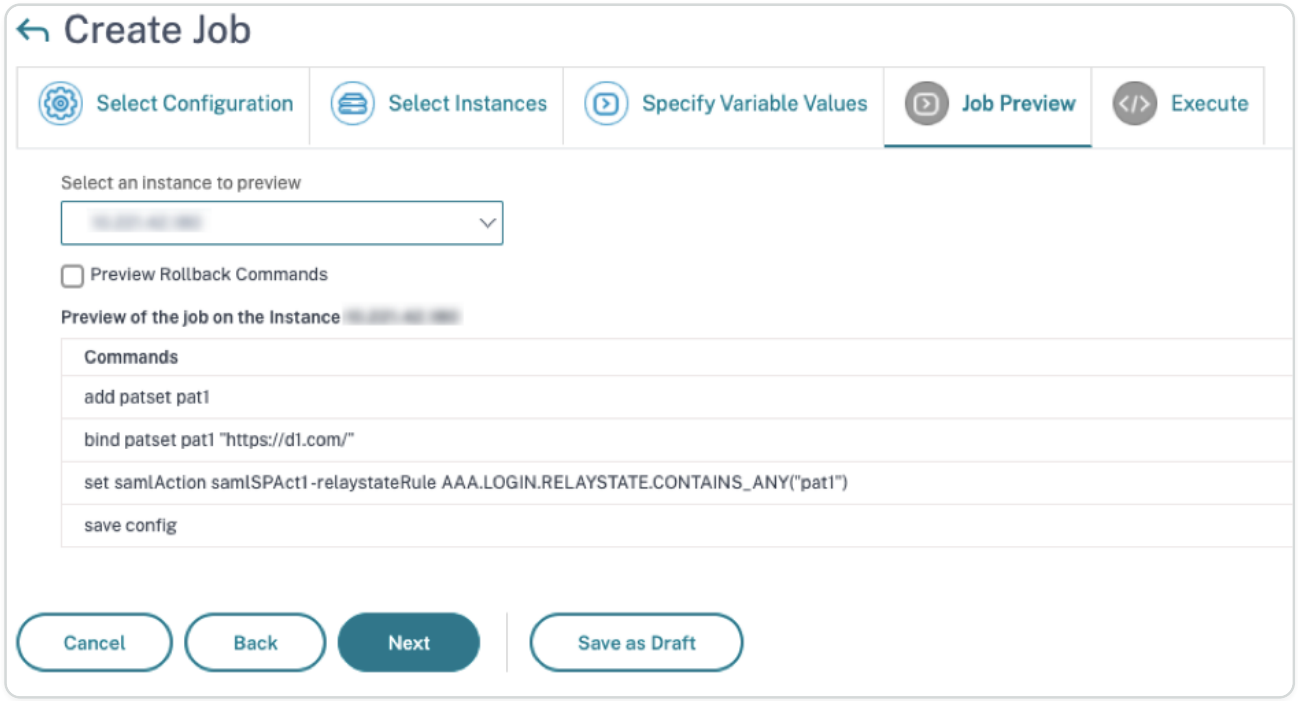
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `saml_action_domain1`: enter a domain in the format `https://<example1.com>/`
- `saml_action_name`: enter the same of the SAML action for which you are configuring the job



Step 4: Preview the configuration

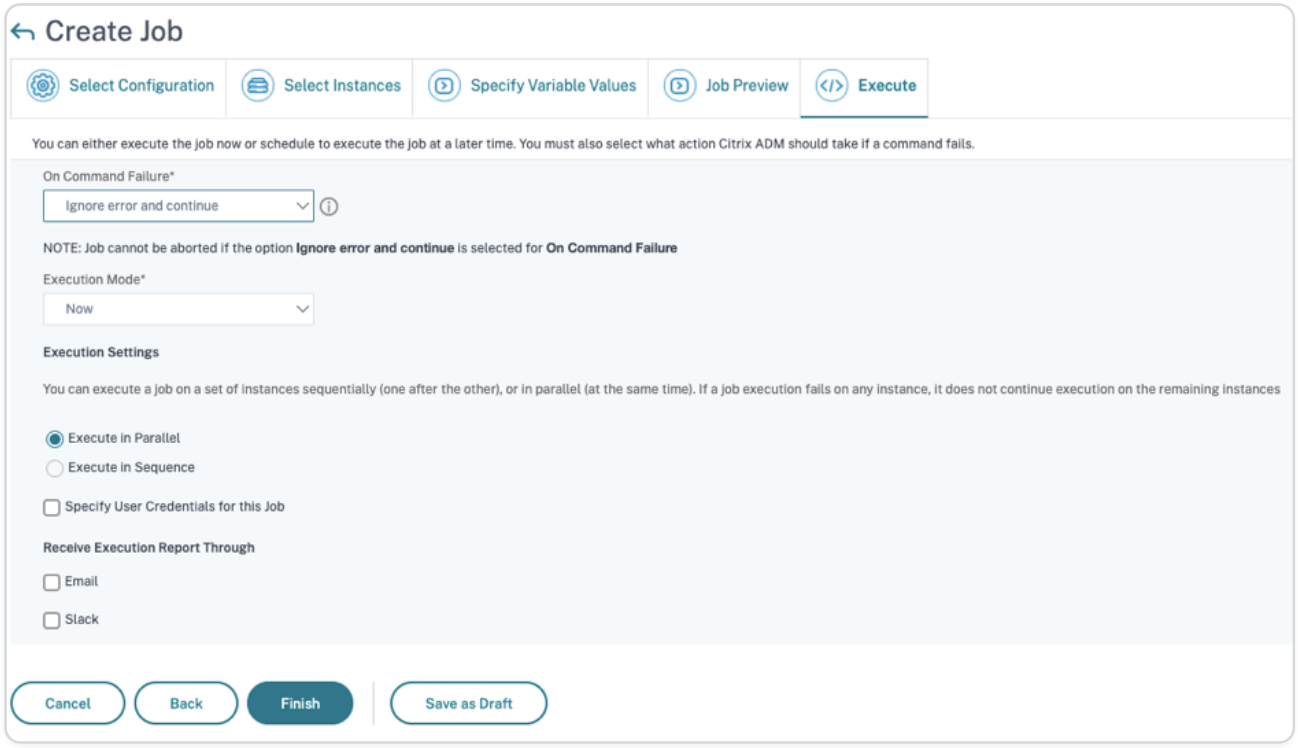
Previews the variable values having been inserted in the config and click **Next**.



Step 5: Run the job

Click **Finish** to run the configuration job.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



After the job is run, it appears under **Infrastructure > Configuration > Configuration Jobs**.

After completing the two remediation steps for all vulnerable NetScaler instances, you can run an on-demand scan to see the revised security posture.

Scenario

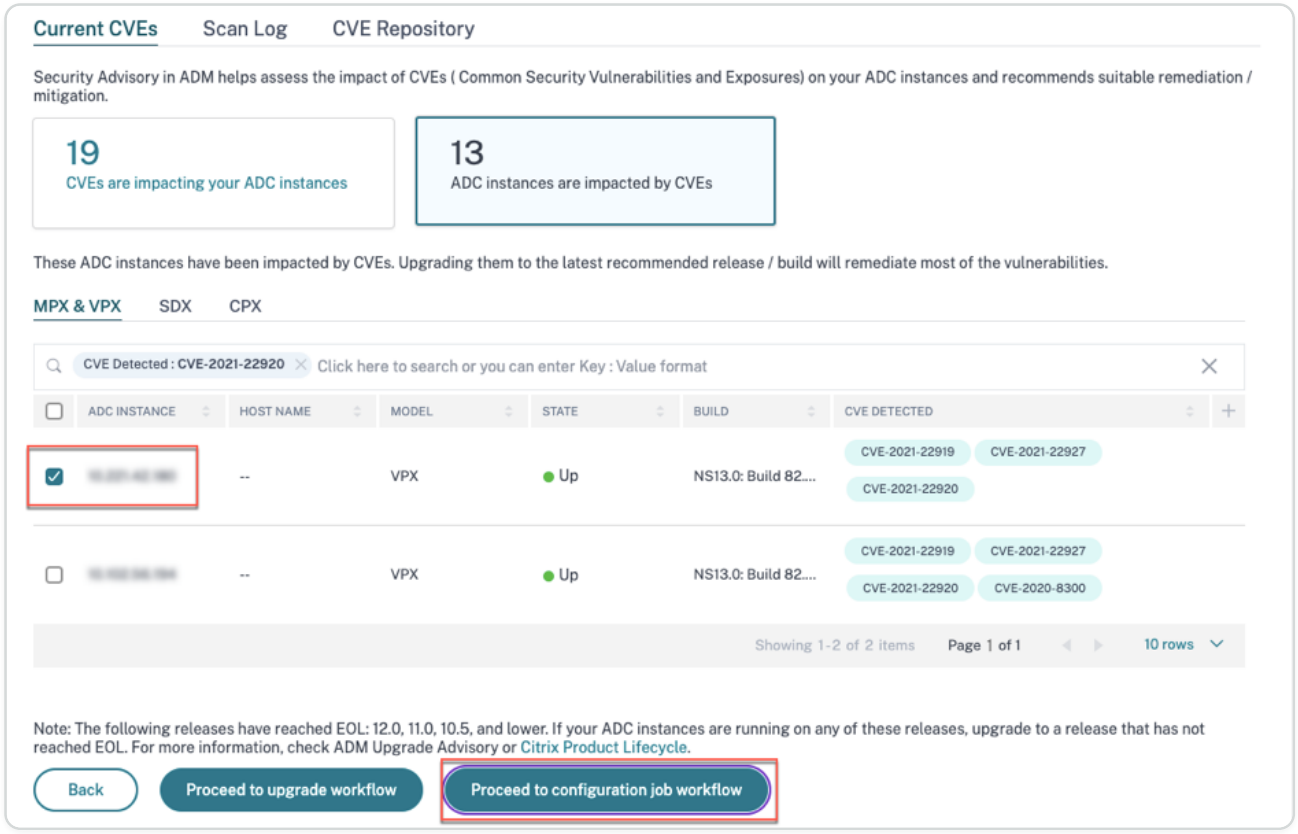
In this scenario, two NetScaler instances are vulnerable to CVE-2021-22920, and you need to remediate all the instances. Follow these steps:

1. Upgrade all the three NetScaler instances by following the steps given in the "Upgrade an instance" section in this document.
2. Apply the config patch to one NetScaler at a time, using the configuration job workflow. See the steps given in the "Apply configuration commands" section in this document.

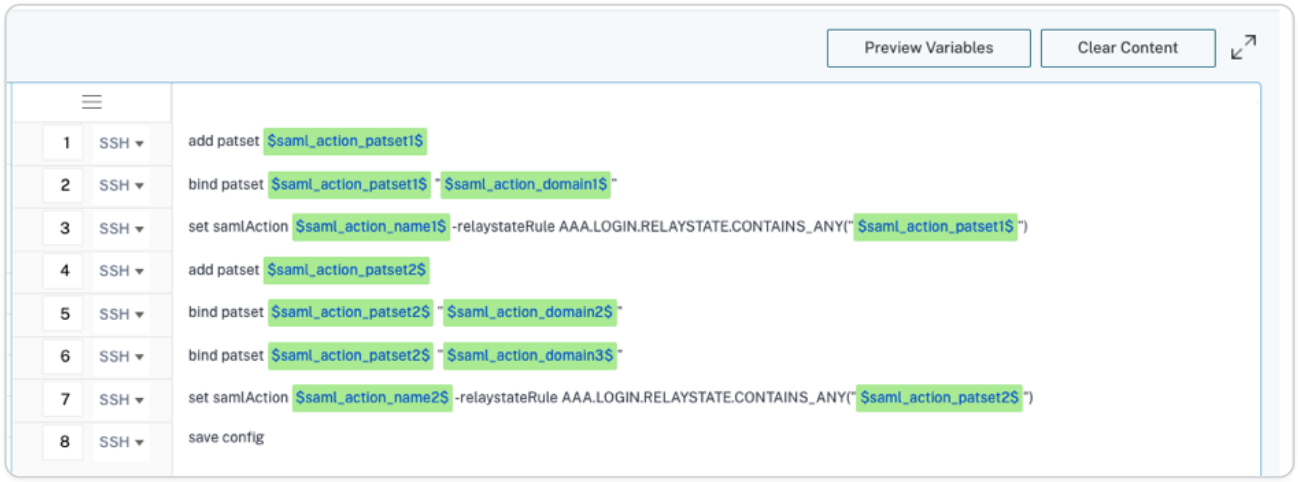
The vulnerable NetScaler 1 has two SAML actions:

- SAML action 1 has one domain
- SAML action 2 has two domains

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Select NetScaler 1 and click **Proceed to configuration job workflow**. The built-in base template auto-populates. Next, give a job name and customize the template according to the given configuration.



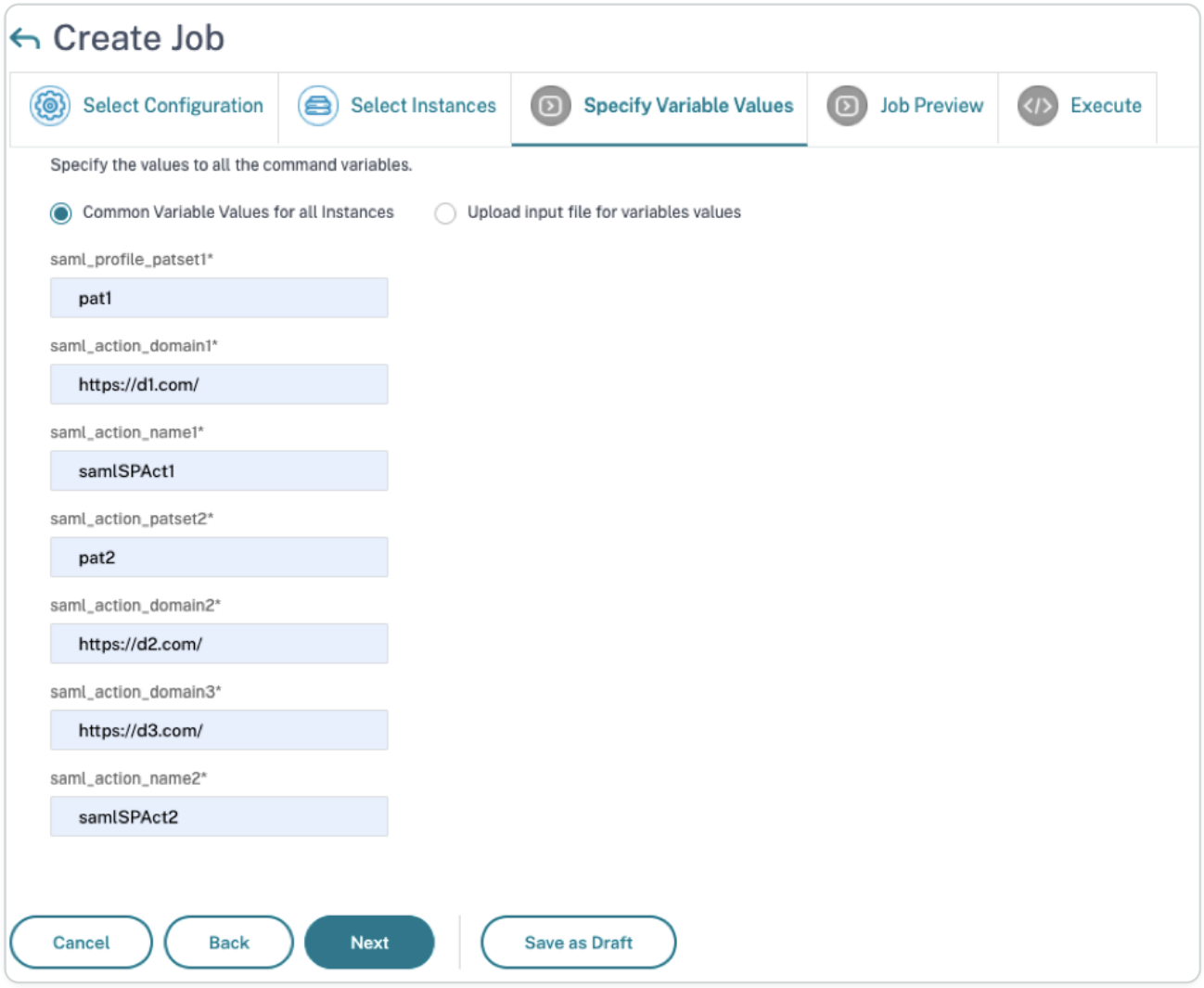
The following table lists the variable definitions for customized parameters.

Table. Variable definitions for SAML action

© 1997–2026 Citrix Systems, Inc. All rights reserved.

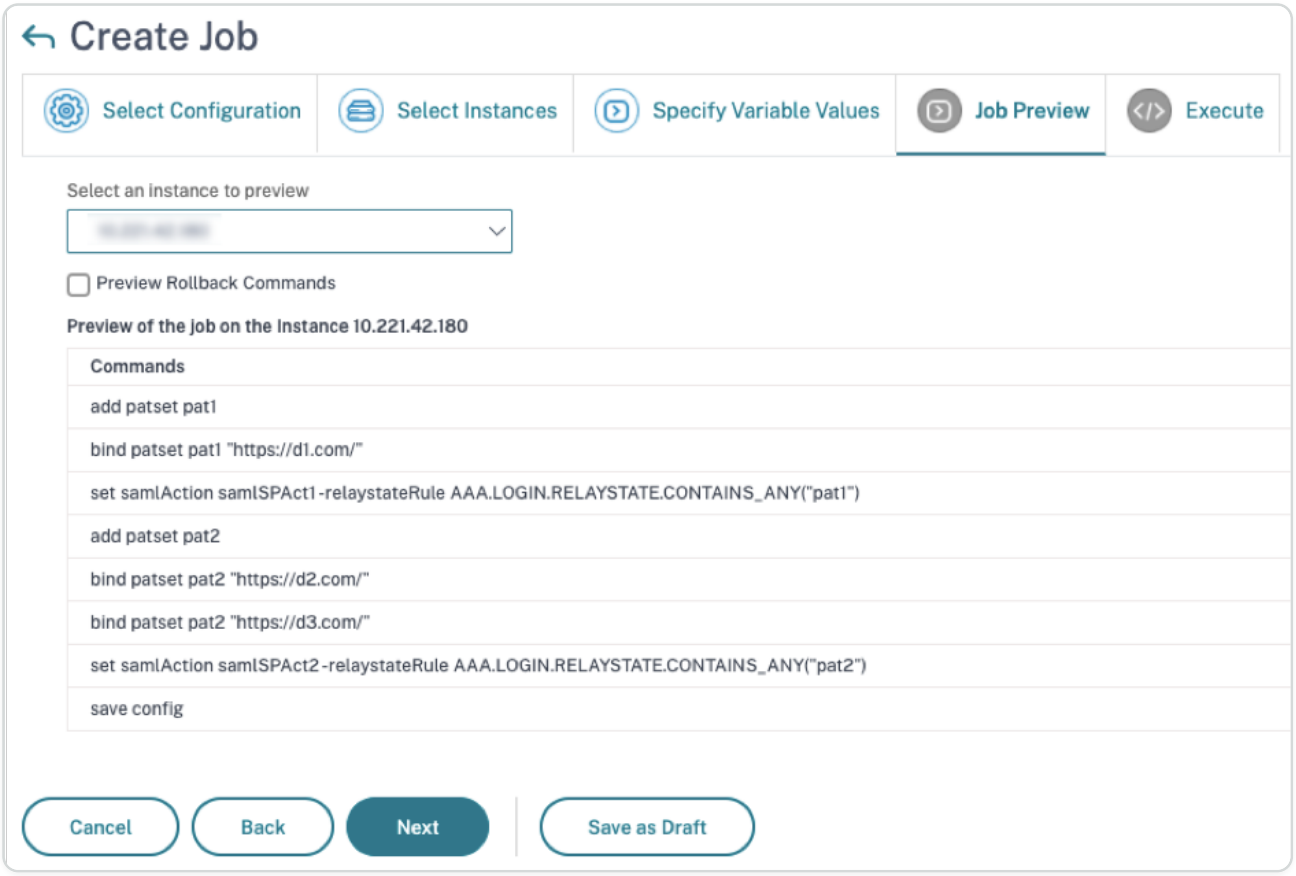
NETSCALER CONFIGURATION	VARIABLE DEFINITION FOR PATSET	VARIABLE DEFINITION FOR SAML ACTION NAME	VARIABLE DEFINITION FOR DOMAIN
SAML action 1 has one domain	saml_action_patset1	saml_action_name1	saml_action_domain 1
SAML action 2 has two domains	saml_action_patset2	saml_action_name2	saml_action_domain 2, saml_action_domain 3

Under **Select Instances**, select NetScaler 1 and click **Next**. The **Specify Variable Values** window appears. In this step, you need to provide values for all the variables defined in the previous step.



Next, review the variables.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Click **Next** and then click **Finish** to run the job.

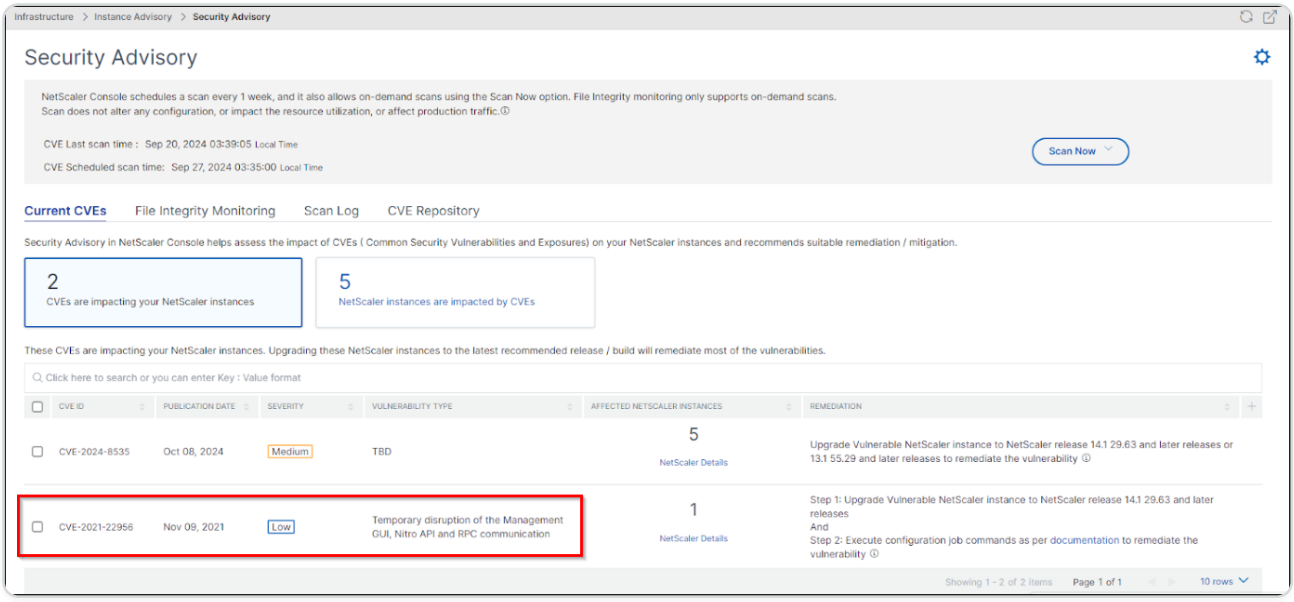
After the job is run, it appears under **Infrastructure > Configuration > Configuration Jobs**.

After completing the two remediation steps for NetScaler 1, follow the same steps to remediate NetScaler 2 and NetScaler 3. After remediation is complete, you can run an on-demand scan to see the revised security posture.

Identify and remediate vulnerabilities for CVE-2021-22956

In the NetScaler Console security advisory dashboard, under **Current CVEs >** `<number of>` NetScaler instances are impacted by common vulnerabilities and exposures (CVEs), you can see all the instances vulnerable due to this specific CVE. To check the details of the CVE-2021-22956 impacted instances, select CVE-2021-22956 and click **View Affected Instances**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The `<number of>` NetScaler instances impacted by CVEs window appear. Here you see the count and details of the NetScaler instances impacted by CVE-2021-22956.



For more information about the security advisory dashboard see, Security Advisory.

NOTE:

It might take some time for security advisory system scan to conclude and reflect the impact of CVE-2021-22956 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Identify CVE-2021-22956 impacted instances

CVE-2021-22956 requires a custom scan, in which the NetScaler Console connects with the managed NetScaler instance and pushes a script to the instance. The script runs on the NetScaler instance and checks the Apache configuration file (`httpd.conf file`) and maximum client connections (`maxclient`) parameters to determine if an instance is vulnerable or not. The information the script shares with NetScaler Console is the vulnerability status in Boolean (true or false). The script also gives back to NetScaler Console a list of counts for max_clients for different network interfaces, for example local host, NSIP, and SNIP with management access. You can see

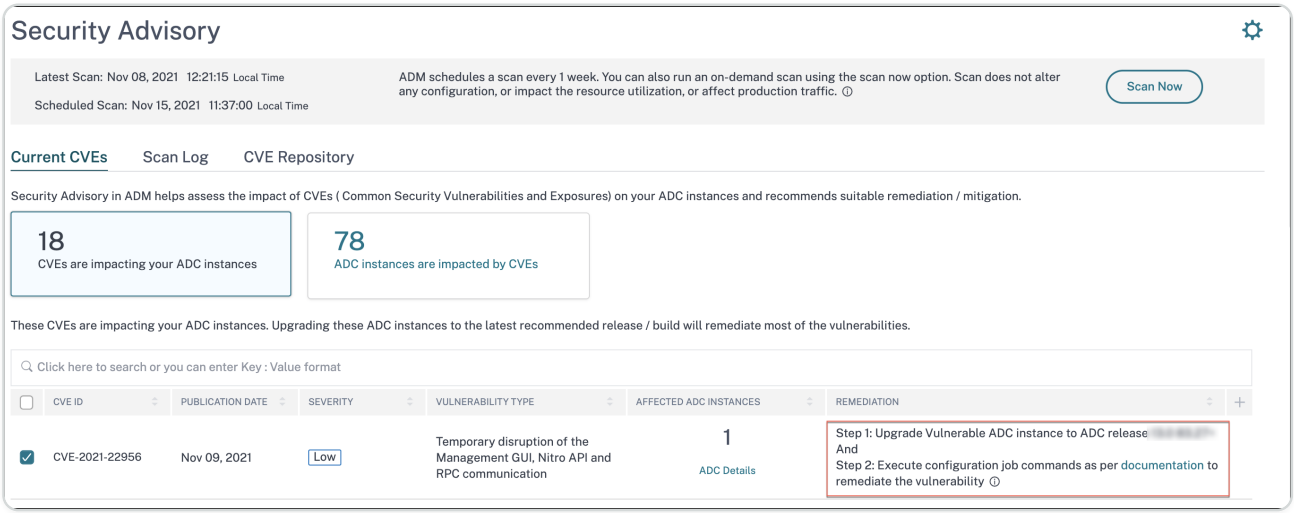
© 1997–2026 Citrix Systems, Inc. All rights reserved.

a detailed report of this list in the CSV file that you can download from the **Scan Logs** tab on **Security Advisory** page.

This script runs every time your scheduled on on-demand scans run. After the scan is completed, the script is deleted from the NetScaler instance.

Remediate CVE-2021-22956

For CVE-2021-22956 -impacted NetScaler instances, the remediation is a two-step process. In the GUI, under **Current CVEs > NetScaler instances are impacted by CVEs**, you can see step 1 and 2.



The two steps include:

1. Upgrading the vulnerable NetScaler instances to a release and build that has the fix.
2. Applying the required configuration commands using the customizable built-in configuration template in configuration jobs.

Under Current CVEs> NetScaler instances impacted by CVEs, you see two separate workflows for this 2-step remediation process: which are Proceed to upgrade workflow and Proceed to configuration job workflow.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 1: Upgrade the vulnerable NetScaler instances

To upgrade the vulnerable instances, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

NOTE:

This step can be done at once for all the vulnerable NetScaler instances.

Step 2: Apply configuration commands

After you've upgraded the impacted instances, in the **<number of> NetScaler instances impacted by CVEs** window, select the instance impacted by CVE-2021-22956 and click **Proceed to configuration job workflow**. The workflow includes the following steps.

1. Customizing the configuration.
2. Reviewing the auto-populated impacted instances.
3. Specifying inputs for variables for the job.
4. Reviewing the final config with variable inputs populated.
5. Running the job.

Keep the following points in mind before you select an instance and click **Proceed to configuration job workflow**:

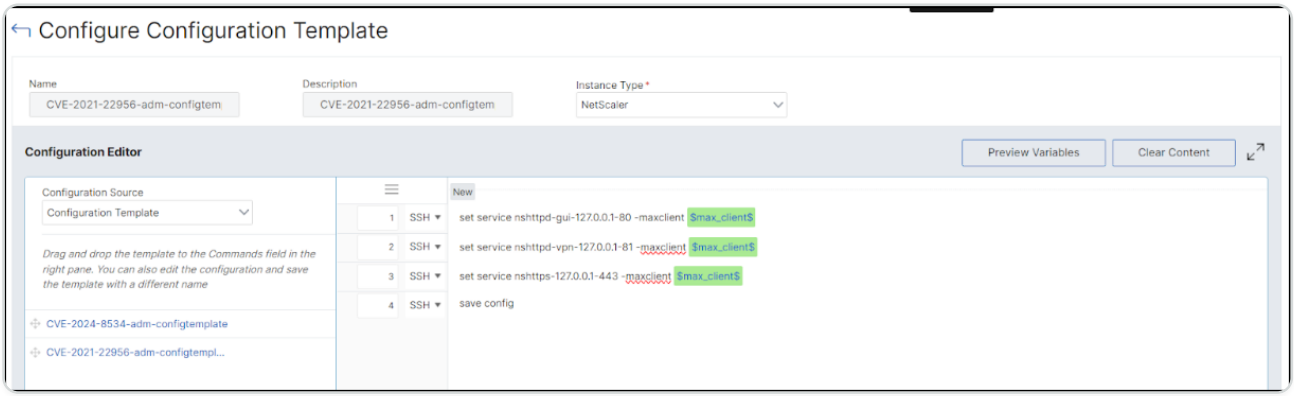
- For a NetScaler instance impacted by multiple CVEs (such as CVE-2020-8300, CVE-2021-22927, CVE-2021-22920, and CVE-2021-22956): when you select the instance and click **Proceed to configuration job workflow**, the built-in configuration template does not auto-populate under Select configuration. Drag and drop the appropriate config job template under **Security Advisory Template** manually to the config job pane on the right side.
- For multiple NetScaler instances that are impacted by CVE-2021-22956 only: you can run config jobs on all instances at once. For example, you've NetScaler 1, NetScaler 2, and NetScaler 3, and all of them are impacted only by CVE-2021-22956. Select all these instances and click **Proceed to configuration job workflow**, and the built-in configuration template auto-populates under **Select configuration**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For multiple NetScaler instances impacted by CVE-2021-22956 and one or more other CVEs (such as CVE-2020-8300, CVE-2021-22927, and CVE-2021-22920), which require remediation to be applied to each NetScaler at a time: when you select these instances and click **Proceed to configuration job workflow**, an error message appears telling you to run the config job on each NetScaler at a time.

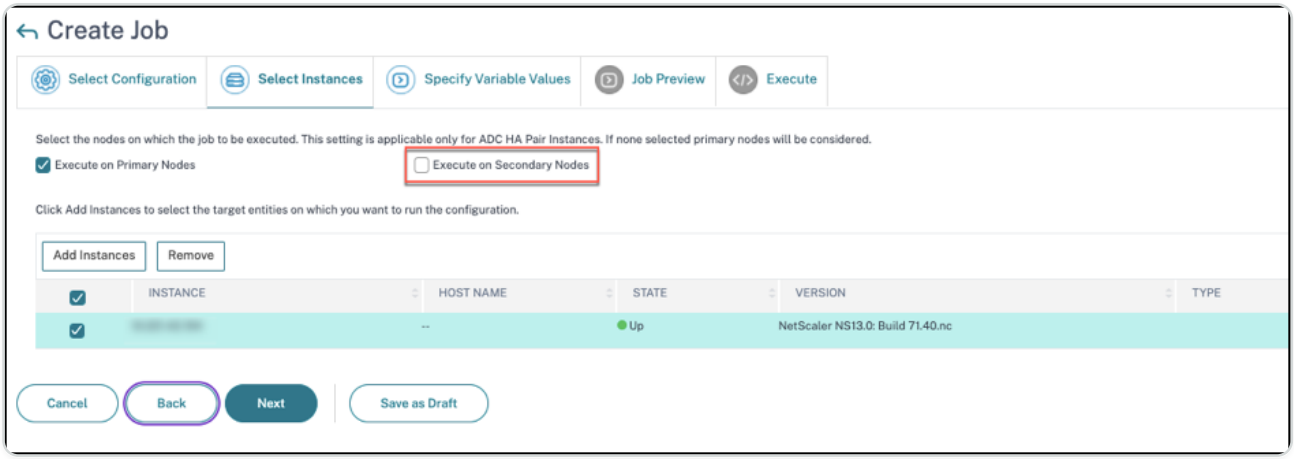
Step 1: Select configuration

In the configuration job workflow, the built-in configuration base template auto-populates under **Select configuration**.



Step 2: Select the instance

The impacted instance is auto-populated under **Select Instances**. Select the instance. If this instance is part of an HA pair, select **Execute on Secondary Nodes**. Click **Next**.



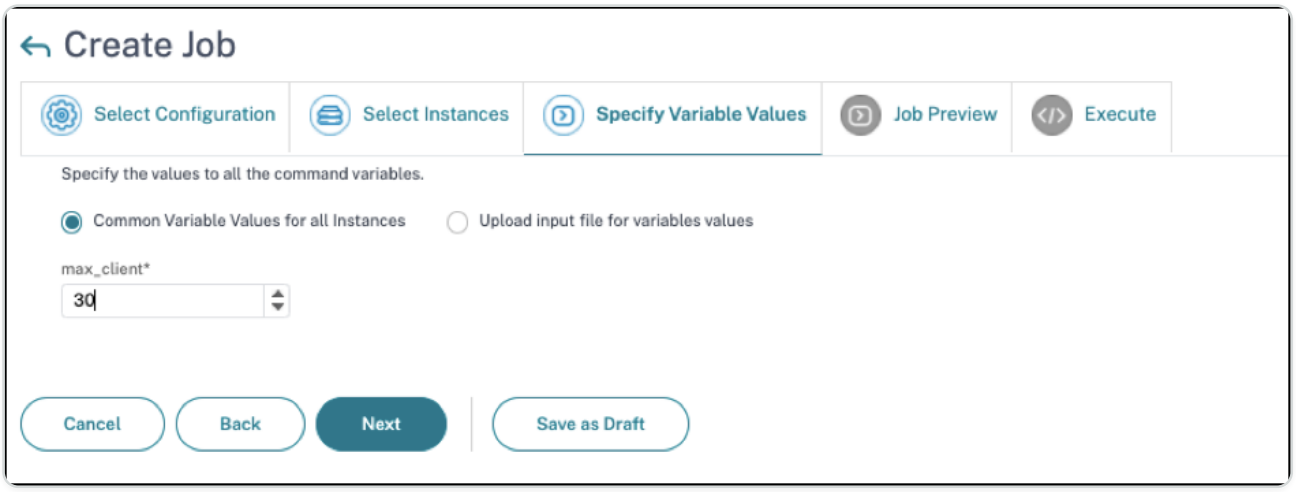
NOTE:

For NetScaler instances in cluster mode, using security advisory, the NetScaler Console supports running the config job only on the cluster configuration coordinator (CCO) node. Run the commands on non-CCO nodes separately.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 3: Specify variable values

Enter the variable values.



Select one of the following options to specify variables for your instances:

Common variable values for all instances: Enter a common value for the variable `max_client`.

Upload input file for variables values: Click **Download Input Key File** to download an input file. In the input file, enter values for the variable `max_client` and then upload the file to the NetScaler Console server.

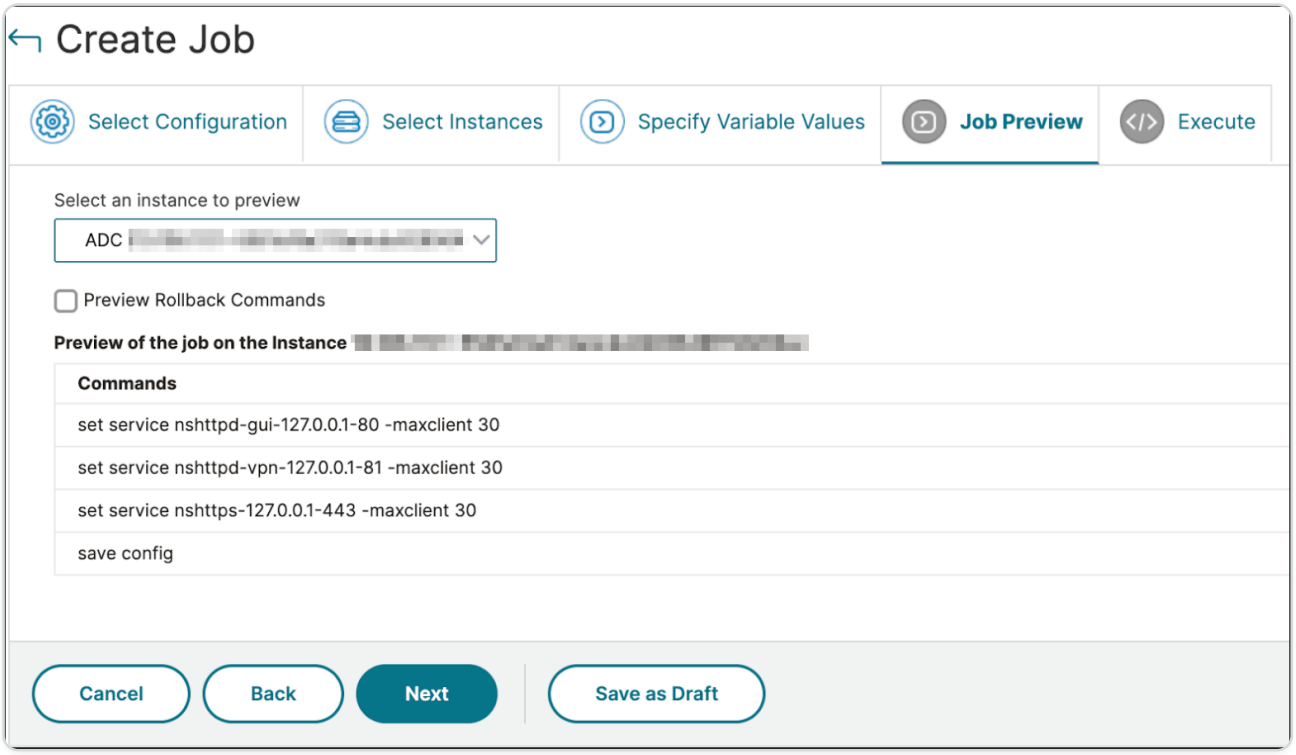
NOTE:

For both options mentioned above, the recommended `max_client` value is 30. You can set the value according to your present value. However, it should not be zero, and it should be less than or equal to the max_client set in the `/etc/httpd.conf` file. You can check the present value set in the Apache HTTP Server configuration file `/etc/httpd.conf` by searching the string `MaxClients`, in the NetScaler instance

Step 4: Preview the configuration

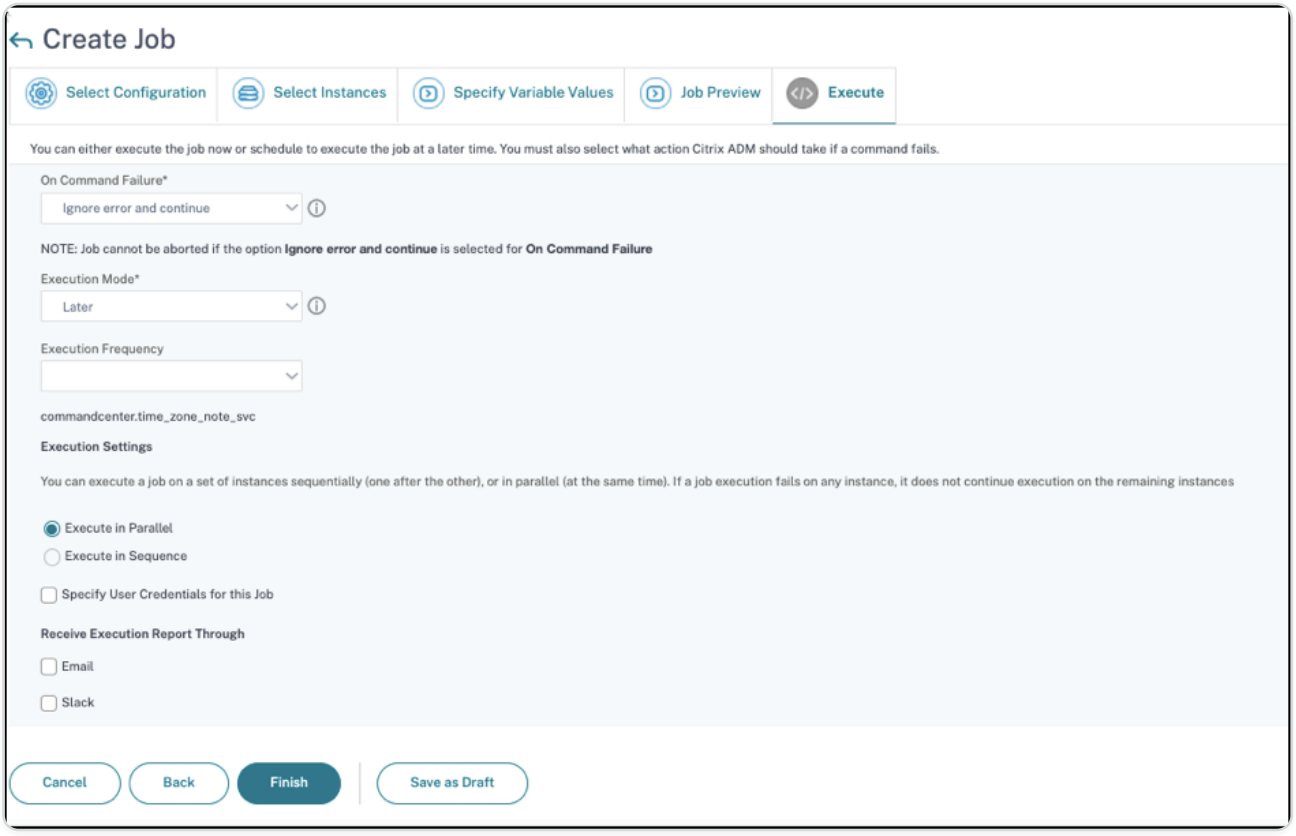
Previews the variable values having been inserted in the config and click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Step 5: Run the job

Click **Finish** to run the configuration job.



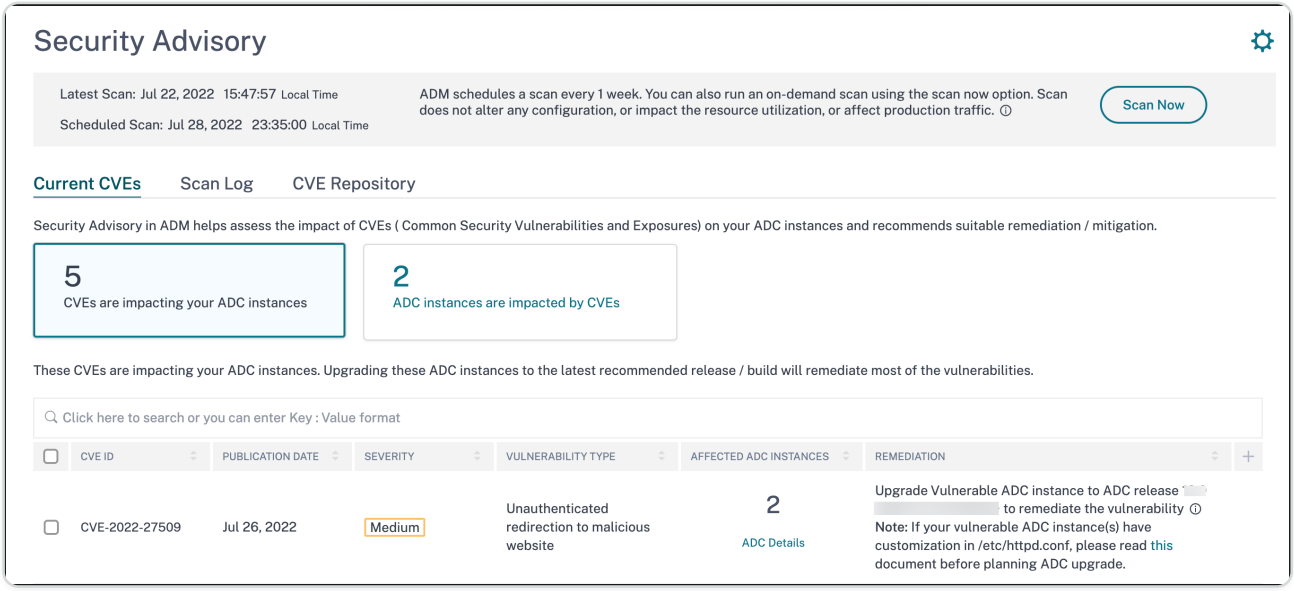
After the job is run, it appears under **Infrastructure > Configuration > Configuration Jobs**.

After completing the two remediation steps for all vulnerable NetScaler instances, you can run an on-demand scan to see the revised security posture.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Identify and remediate vulnerabilities for CVE-2022-27509

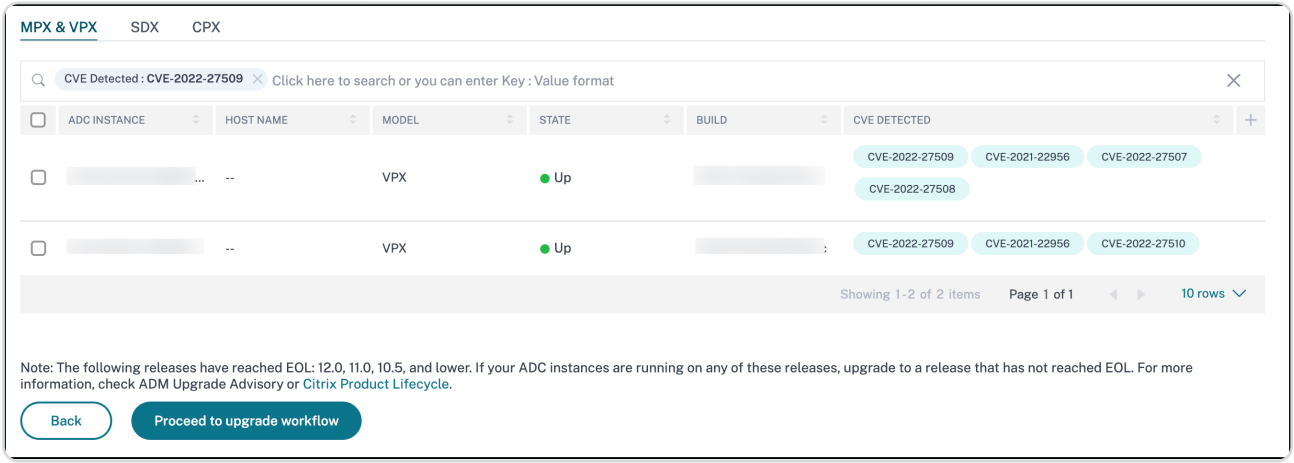
In the NetScaler Console security advisory dashboard, under **Current CVEs** `<number of>` **NetScaler instances are impacted by CVEs**, you can see all the instances vulnerable due to CVE-2022-27509. To check the details of the instances impacted by the CVEs, select CVE-2022-27509 and click **View Affected Instances**.



NOTE

To understand the reason for NetScaler vulnerability, download the CSV report in Scan logs tab in Security Advisory.

The `<number of>` **NetScaler instances impacted by CVEs** window appears. In the following screen capture, you can see the count and details of the NetScaler instances impacted by CVE-2022-27509.



For more information about the security advisory dashboard see, Security Advisory.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2022-27509 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Identify CVE-2022-27509 impacted instances

CVE-2022-27509 requires a combination of custom scan and version scan. As part of the custom scan, the NetScaler Console connects with the managed NetScaler instance and pushes a script to the instance. The script runs on the NetScaler instance and determines if the instance is vulnerable. This script runs every time your scheduled or on-demand scan runs.

After the scan is completed, the script is deleted from the NetScaler instance.

You can also opt out of these Security Advisory Custom scans. For more information on Custom Scan Settings and opting out of custom scans, see the **Configure Custom Scan settings** section on the **Security Advisory** page.

Remediate CVE-2022-27509

For CVE-2022-27509 impacted NetScaler instances, the remediation is a single step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix. In the GUI, under **Current CVEs > NetScaler instances are impacted by CVEs**, you can see the step to remediate.

Under **Current CVEs> NetScaler instances impacted by CVEs**, you see the following workflow for this single step remediation process, which is **Proceed to upgrade workflow**.

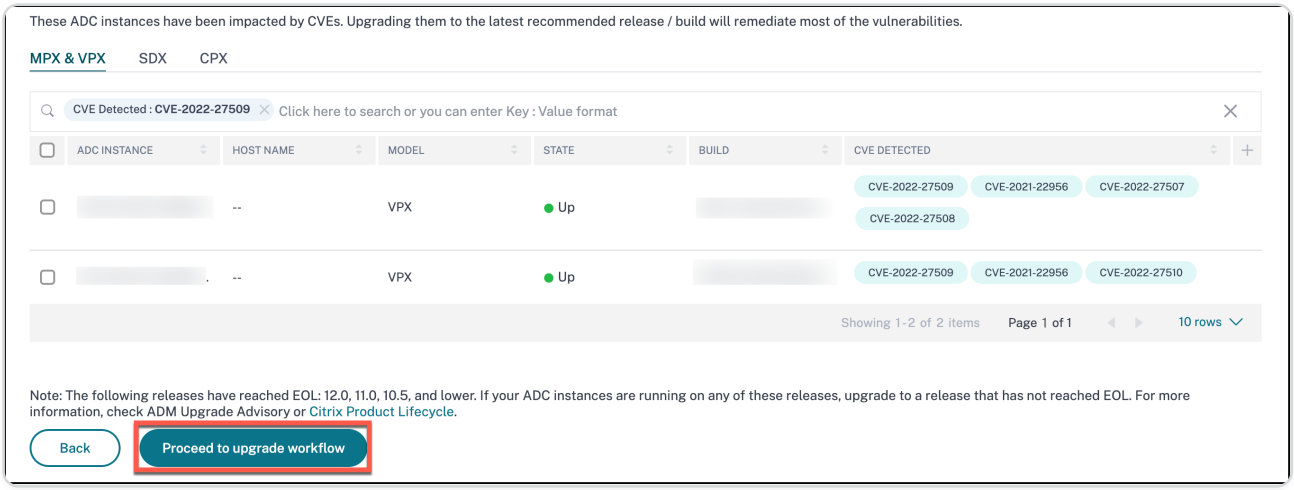
To upgrade the vulnerable instances, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

IMPORTANT

If your vulnerable NetScaler instances have the /etc/httpd.conf file copied to the /nsconfig directory, see Upgrade considerations for customized NetScaler configurations before planning NetScaler upgrade.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.



Unsupported CVEs in Security Advisory

NetScaler Console security advisory tracks all the new Common Vulnerabilities and Exposures (CVEs) and assesses the impact of CVEs on the infrastructure. You can review the recommendations and take appropriate actions. However, there are a few CVEs that are not supported and the detection and remediation of the vulnerabilities are out of NetScaler Console Security Advisory scope.

- **CVE-2022-21827**:

  CVE-2022-21827 impacts NetScaler Gateway plug-in for Windows supported versions prior to 21.9.1.2.

  The detection and remediation of vulnerabilities impacting the NetScaler Gateway plug-in for Windows is not supported by the NetScaler Console. Also, NetScaler Gateway plug-in vulnerabilities cannot be assessed by performing any checks on NetScaler side, verifying the NetScaler version, or by checking the NetScaler configuration. The detection & remediation for this CVE can only be assessed based on the version of the NetScaler Gateway plug-in for Windows deployed on the client.

  As a result, the detection and remediation of this vulnerability is out of NetScaler Console Security Advisory scope.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Setting up

After your initial setup is complete, you have to configure certain settings to start managing your deployment completely.

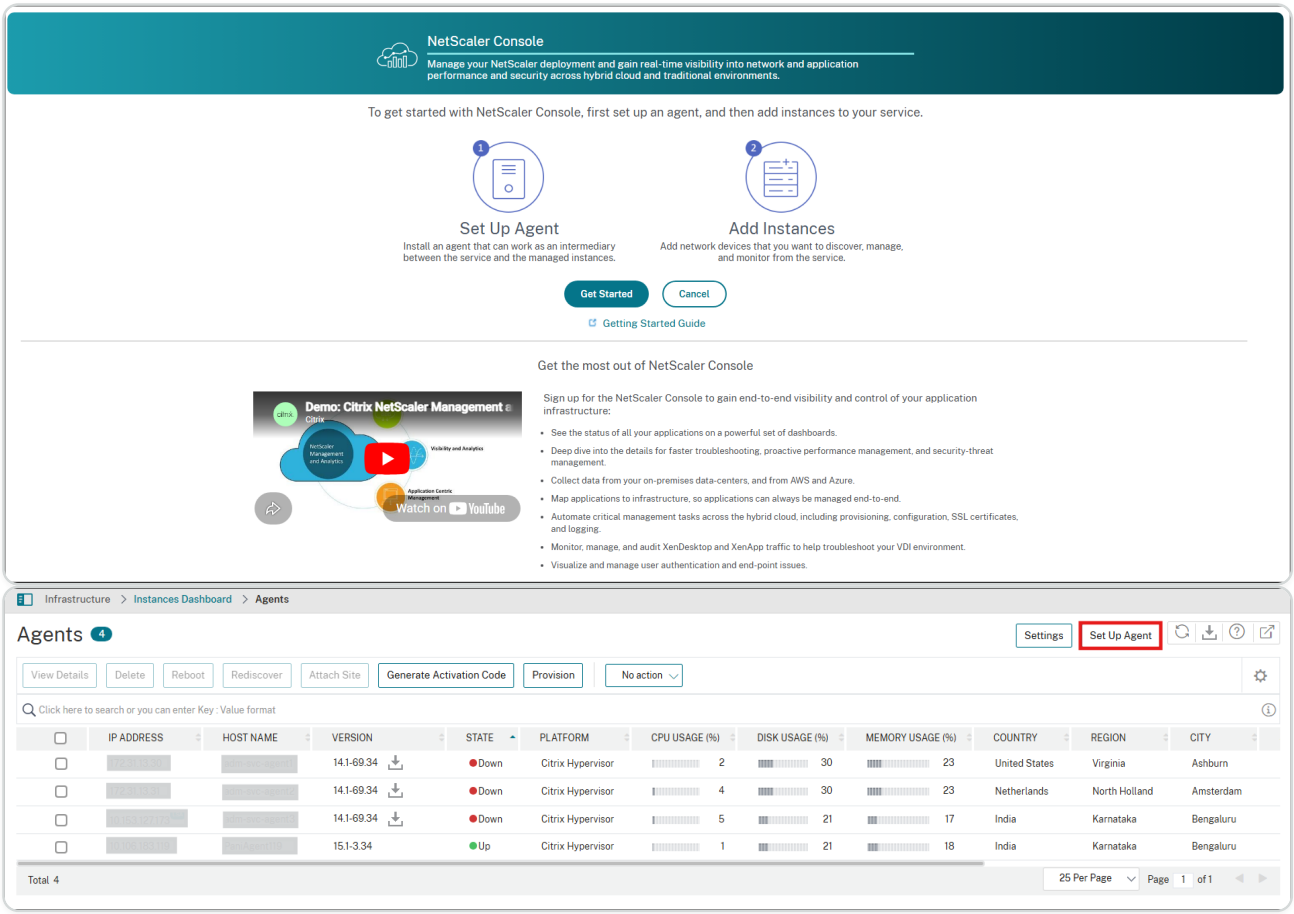
- Adding multiple agents. The number of agents to be installed depends on the number of managed instances in a data center or cloud and the total throughput. Citrix recommends that you install at least one agent for every data center.
- Adding instances. You can add instances either while setting up the NetScaler Console for the first time or at a later time. You have to add instances to the service to start managing and monitoring them. After you install multiple agents, you have to add instances and associate them with the agents.
- Enabling Analytics. To view analytics data for your application traffic flow, you must enable the Analytics feature on the virtual servers that receive traffic for the specific applications.
- Configuring syslog on instances. You can monitor the syslog events generated on your NetScaler instances if you have configured your device to redirect all syslog messages to NetScaler Console. To monitor syslog events, you need to first configure NetScaler Console as the syslog server for your NetScaler instance.
- Configuring role-based access control. NetScaler Console provides fine-grained, role based access control (RBAC) with which you can grant access permissions based on the roles of individual users within your enterprise.
- Configuring Analytics settings. You can configure certain settings to ensure optimal experience with the Analytics feature. For example, you can specify the duration you want to store historical analytics data, and you can also set thresholds and alerts to monitor the desired analytics metrics.

Adding multiple agents

The number of agents to be installed depends on the number of managed instances in a data center and the total throughput. Citrix recommends that you install at least one agent for every data center.

You can install only one agent when you log on to the service for the first time. To add multiple agents, first complete the initial setup, and then navigate to **Infrastructure > Instances > Agents** and click **Set Up Agent.**

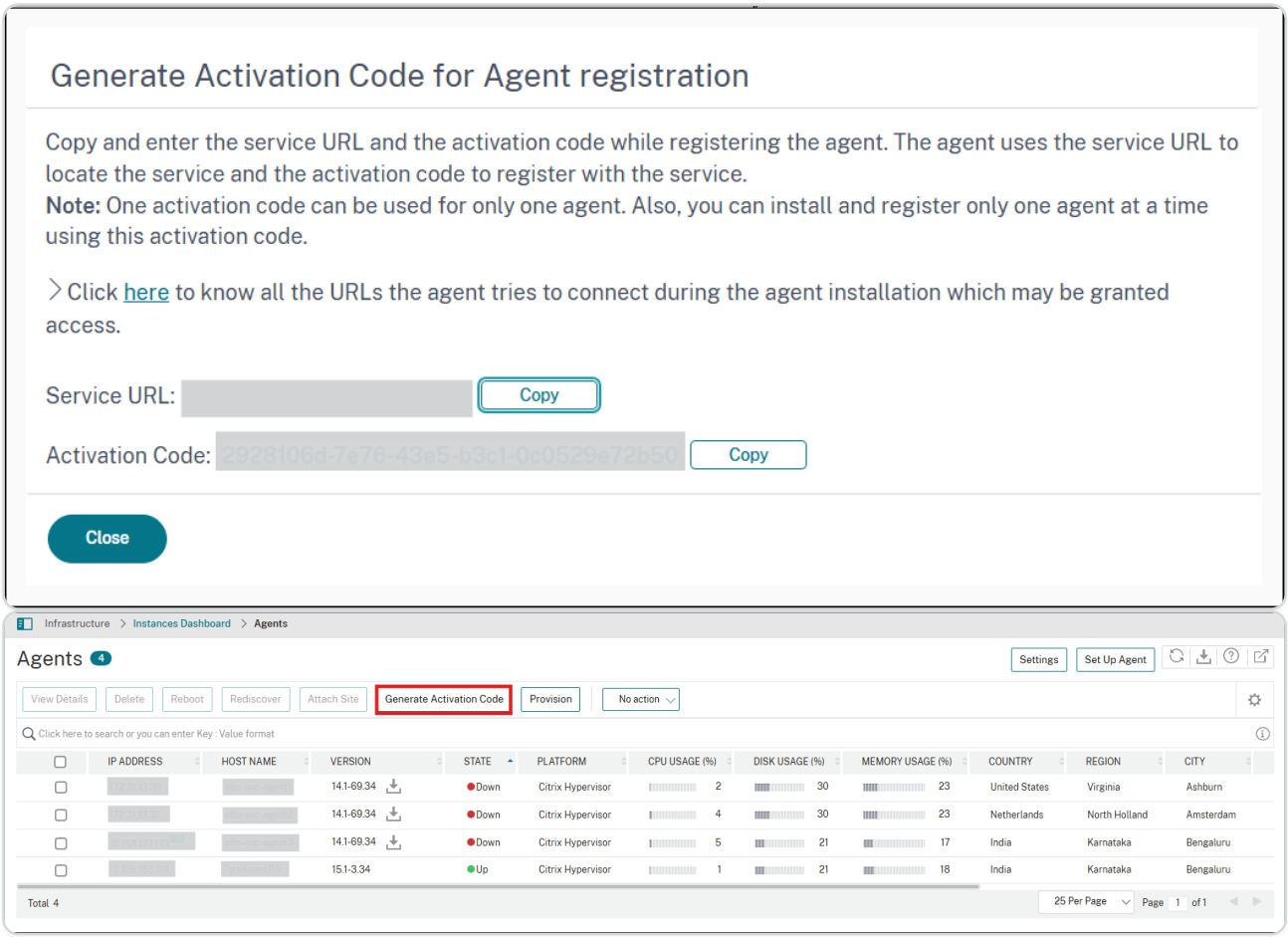
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Download the image for the required hypervisor and install the agent by following the instructions in Getting Started. Make sure you copy the service URL and the activation code displayed on the screen because you have to enter the service URL and the activation code while installing the agent on your hypervisor. The agent uses the service URL to locate the service and the activation code to register with the service.

You can use the same image to install multiple agents in your hypervisor. However, you cannot use the same activation code on multiple agents. After you install one agent, generate the activation code again for the next agent. You can generate a new activation code by navigating to **Infrastructure > Instances > Agents**, click **Generate Activation Code**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



After the agent is successfully installed and registered, verify the agent status on the service GUI and add instances to it.

NOTE

You can also install an agent on Microsoft Azure cloud or AWS cloud. The agent image is available on the respective cloud marketplace.

- For instructions about installing an agent on Microsoft Azure cloud, see Install a NetScaler agent on Microsoft Azure Cloud.
- For instructions about installing an agent on AWS, see Install a NetScaler agent on AWS.

Configure agents for multisite deployment

Agents work as an intermediary between the NetScaler Console and the discovered instances across different data centers and public clouds. NetScaler Console supports agent failover within a data center or a public cloud.

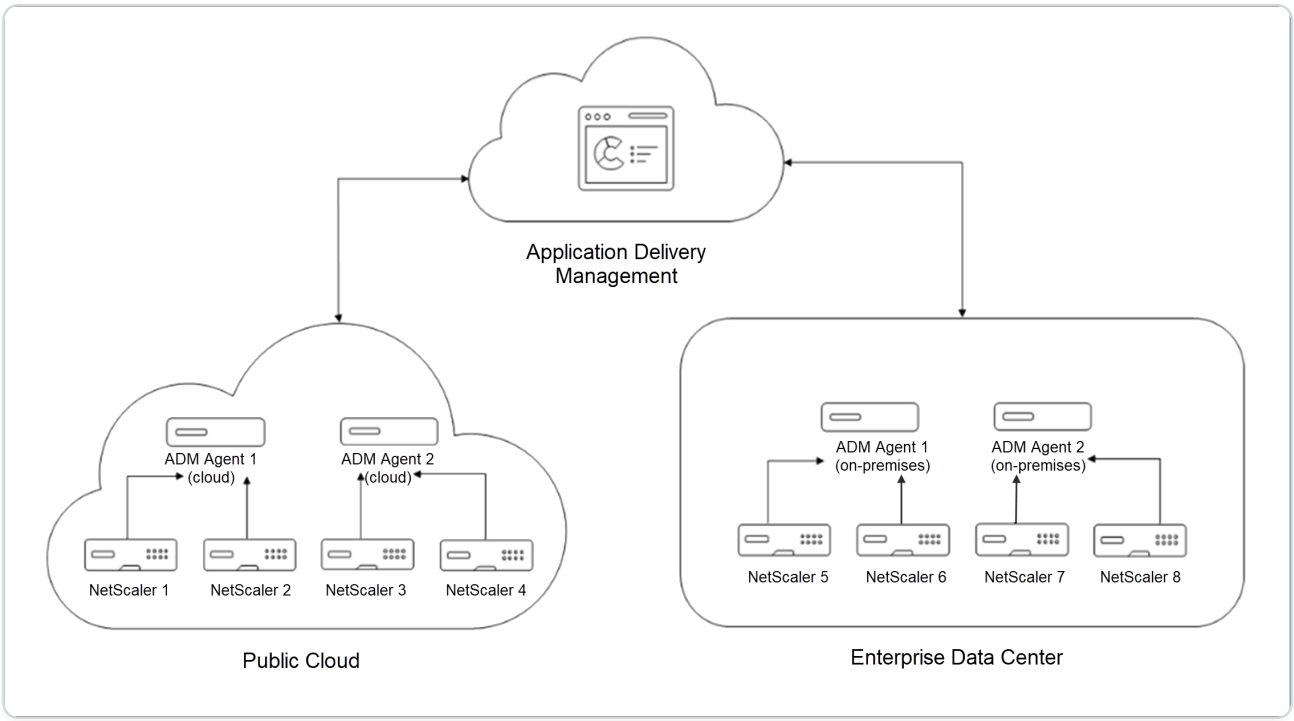
The following are the benefits of installing agents:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The configured instances to an agent send the unprocessed data directly to the agent instead of NetScaler Console. Agent does the first level of data processing and sends the processed data in compressed format to the NetScaler Console for storage.
- Agents and instances are co-located in the same data center or cloud so that the data processing is faster.
- Clustering the agents provides redistribution of NetScaler instances on agent failover. When one agent in a site fails, traffic from NetScaler instances switches to another available agent in the same site.

Architecture

The following figure illustrates NetScaler instances configured on multiple agents in a data center and public cloud to achieve agent failover:



The public cloud has four NetScaler instances and two agents. The enterprise data center also have four NetScaler instances and two agents. Each agent is configured with two NetScaler instances.

The agents receive data directly from the configured instances. After agent receives the data, agent processes the data and sends to the NetScaler Console in a compressed format. Agents communicate with the NetScaler Console server over a secure channel.

On public cloud, when **Agent 1** becomes inactive (DOWN state), agent failover occurs. NetScaler Console redistributes the NetScaler instances of **Agent 1** with **Agent 2**. The instance redistribution occurs on an enterprise data center if one of the agents fails in the data center.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To install an agent, see Install a NetScaler agent.

Agent failover

The agent failover can occur in a site that has two or more registered agents. When an agent becomes inactive (DOWN state) in the site, the NetScaler Console redistributes the NetScaler instances of the inactive agent with other active agents.

IMPORTANT

- Agent failover does not consider CPX instances.
- Ensure Agent Failover feature is enabled on your account. To enable this feature, see Enable or disable NetScaler Console features.
- If an agent is running a script, ensure that script is present on all the agents in the site. Therefore, the changed agent can run the script after agent failover.

To attach a site to an agent in the NetScaler Console GUI:

1. Navigate to **Infrastructure > Instances > Agents**.
2. Select an agent that you want to attach to a site.
3. Specify the site from the list. If you want to add a new site, click **Add**.
4. Click **Save**.

To achieve an agent failover, select the agents one by one and attach to the same site.

For example, two agents 10.106.1xx.2x and 10.106.1xx.7x are attached and operational in the Bangalore site. If one agent becomes inactive, NetScaler Console detects it and displays the state as down.

When an agent becomes inactive (Down state) in a site, NetScaler Console waits for few minutes for the agent to become active (Up state). If the agent remains inactive, NetScaler Console automatically redistributes the instances among available agents in the same site. This redistribution may take approximately 10-15 minutes.

NetScaler Console triggers instance redistribution every 30 minutes to balance the load among active agents in the site.

The instances attached and automatically reconfigured to agents in the same site for trap destination, syslog server, and analytics.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuring agent upgrade settings

In NetScaler Console, agents running on software version 12.0 build 507.110 and later are automatically upgraded to newer and recommended versions by NetScaler Console. The agent is upgraded either when a new version is available or at a time specified by you.

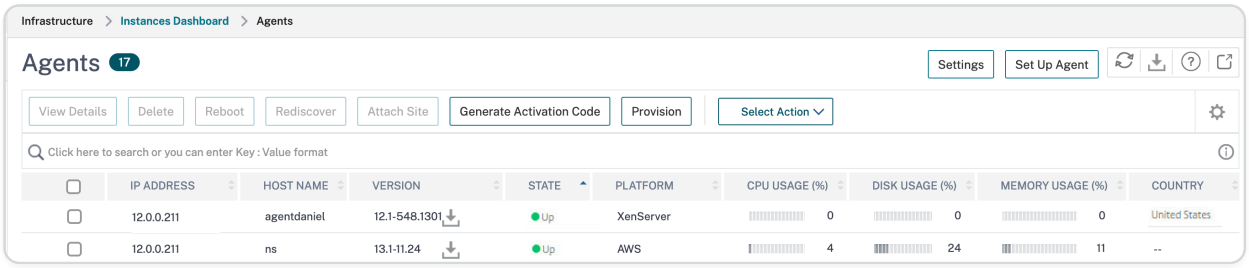
You can view the current version and the recommended version of your agents by navigating to **Infrastructure > Instances > Agents**.

By default, an agent is upgraded automatically when a newer version is available. However, you can schedule an upgrade for each of the agents.

During the upgrade, there might be a downtime of approximately five minutes.

To configure agent upgrade settings:

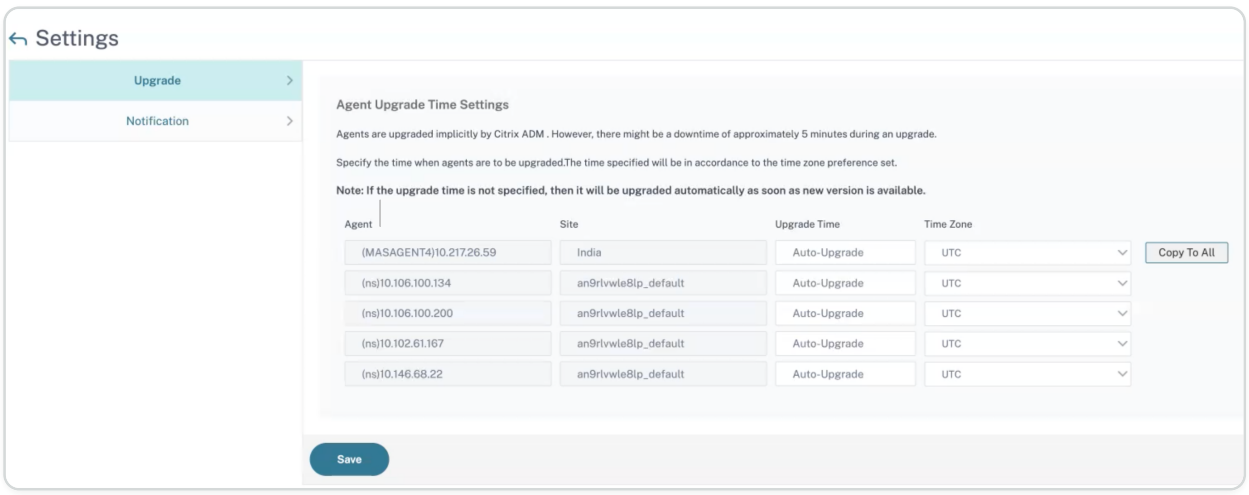
1. Navigate to **Infrastructure > Instances > Agents**, click **Settings**.



2. Specify when you want the upgrade to start for each of the agent.

   You can use one of the following options to upgrade the agent:

   - Automated upgrade - Choose **Auto-Upgrade** for the agent to be upgraded when a new agent image is available. If you do not enter a value, **Auto-Upgrade** is selected by default.
   - Set a specific time: Enter the time (in hh:mm format) and select the time zone when you want NetScaler Console to automatically upgrade the agent.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

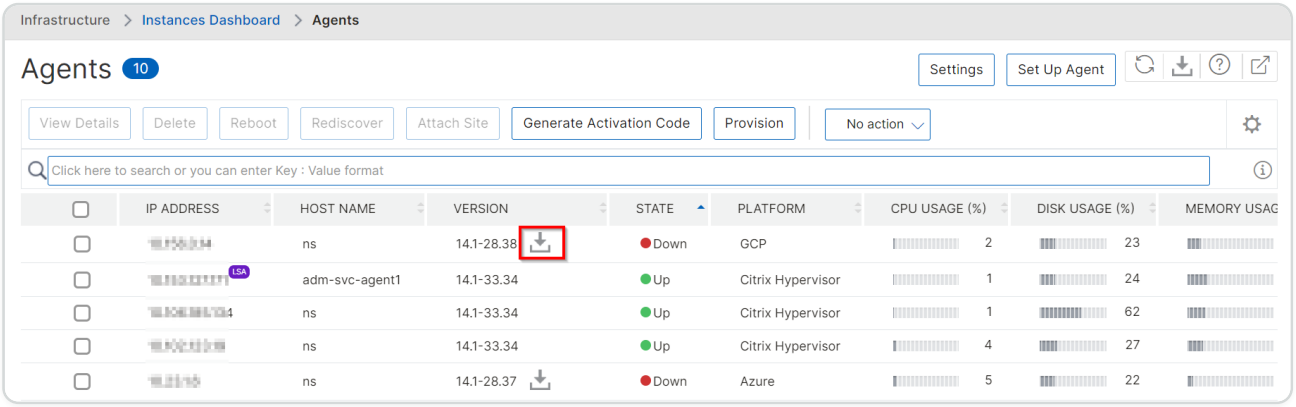
You can click **Copy to All** to apply the same upgrade time to all the agents.

3. Click **Save**.

These settings persist for future agent upgrades until you change the settings.

Upgrade agent manually

In some scenarios, the agents might not be automatically upgraded and still running on an older version. In such scenarios, you must manually upgrade the agent. You can validate if the agent is running on the latest version by navigating to **Infrastructure > Instances > Agents** and checking the build under **Version**. If you see a download icon, the agent is running on an older version.



To manually upgrade the external agent:

1. In **Infrastructure > Instances > Agents**, download the latest build by clicking the download icon that is available in the version.
2. Using an FTP client, copy the agent package (`build-masagent.tgz`) to the agent `/var/mps/mps_agent_images/latest` location.
3. Log on to NetScaler agent by using an SSH client.
4. Untar the agent package.

   ```
   cd /var/mps/mps_agent_images/latest
   ```

   ```
   tar -xzvf build-masagent.tgz
   ```

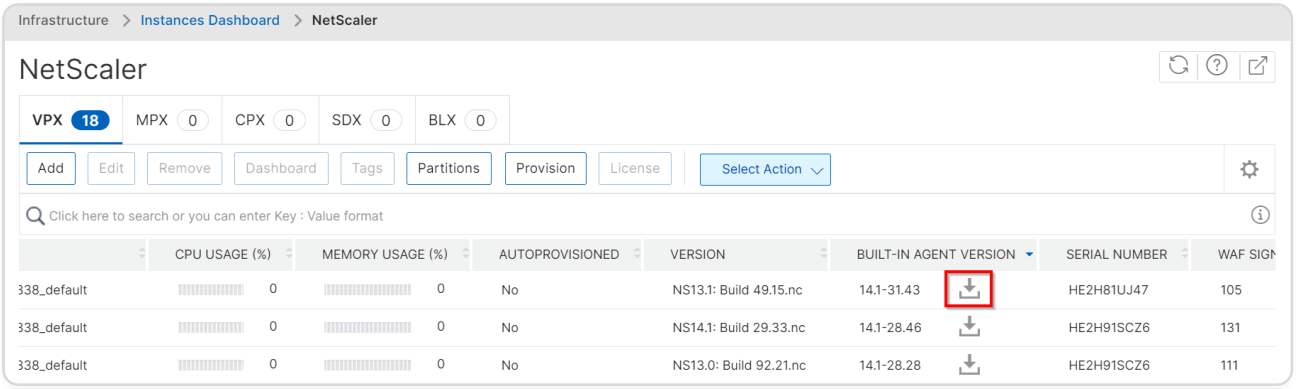
5. Run `./installmasagent`

The installation process starts and the agent reboots after the upgrade is complete.

To manually upgrade the built-in agent:

Navigate to **Infrastructure > Instances > NetScaler** and scroll right to view the **Build-in agent version**. If you see a download icon, the agent is running at an older version.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1. In **Infrastructure > Instances > NetScaler**, download the latest build by clicking the download icon that is available in the version.
2. Using an FTP client, copy the mastools package to the `/var/mastools directory` location.
3. Log on to NetScaler by using an SSH client.
4. Run `/var/mastools/scripts/mastoolsd stop`.
5. Run `tar xvzf <package_name_with_path> -C /var/mastools`.

   NOTE:

   You must replace `package_name_with_path` with the exact path of your package location.

6. Run `/bin/sh /var/mastools/scripts/admautoreg/admautoregd_ctl restart_if_running`.
7. Run `/var/mastools/scripts/mastoolsd restart`.

Dual NIC support on NetScaler Console

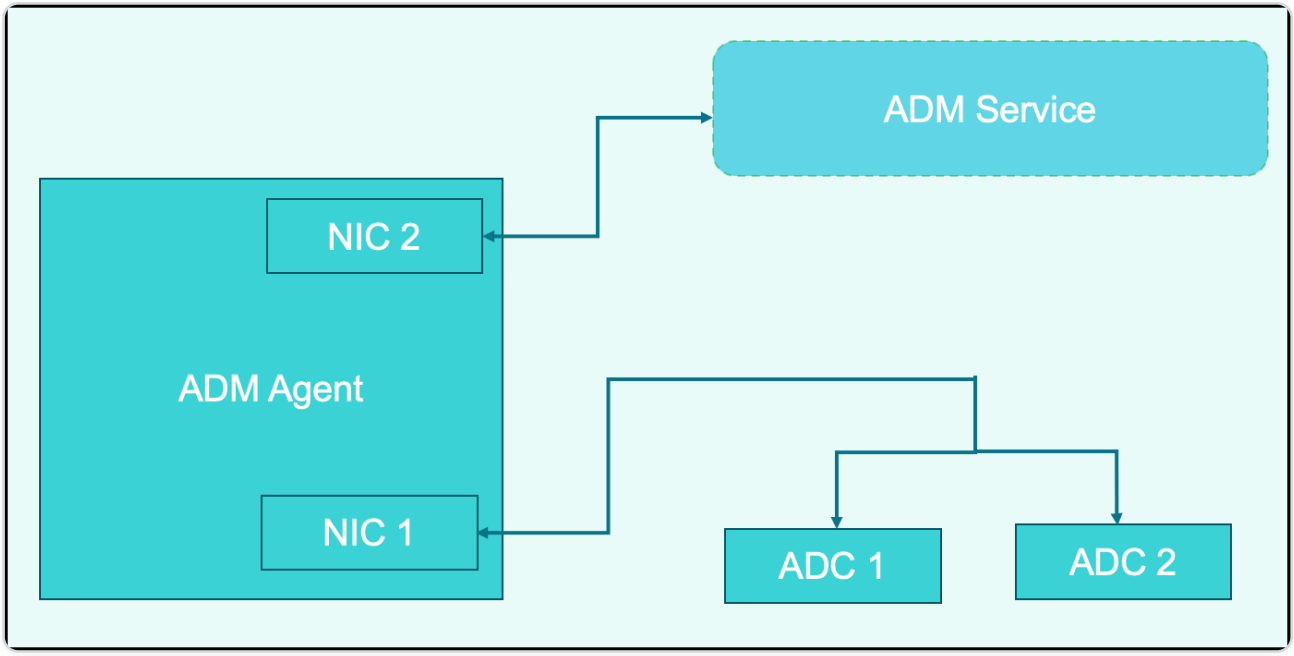
You can configure two NICs on an agent. Using the Dual NIC architecture, agent will be able to:

- Establish communication between the agent and NetScaler instances - You can use the first NIC to isolate the traffic that is received and sent through the NetScaler Console and also to communicate between NetScaler Console and its managed NetScaler instances in another network.
- Establish communication between the agent and the NetScaler Console - You can use the second NIC to manage the NetScaler Console that is on a network and perform administrative tasks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

You cannot interchange the functionality and configuration of both the NICS.



In this scenario, as an administrator, you can:

- Configure IP address for the traffic between NetScaler Console and its managed NetScaler instances.
- Configure IP address for managing the NetScaler Console software to perform all administrative tasks in the software.

NOTE

It is not mandatory to configure Dual NICs for an agent. It is optional and is required only when traffic between agent, NetScaler Console service, and NetScaler instances need to be separated.

Prerequisites

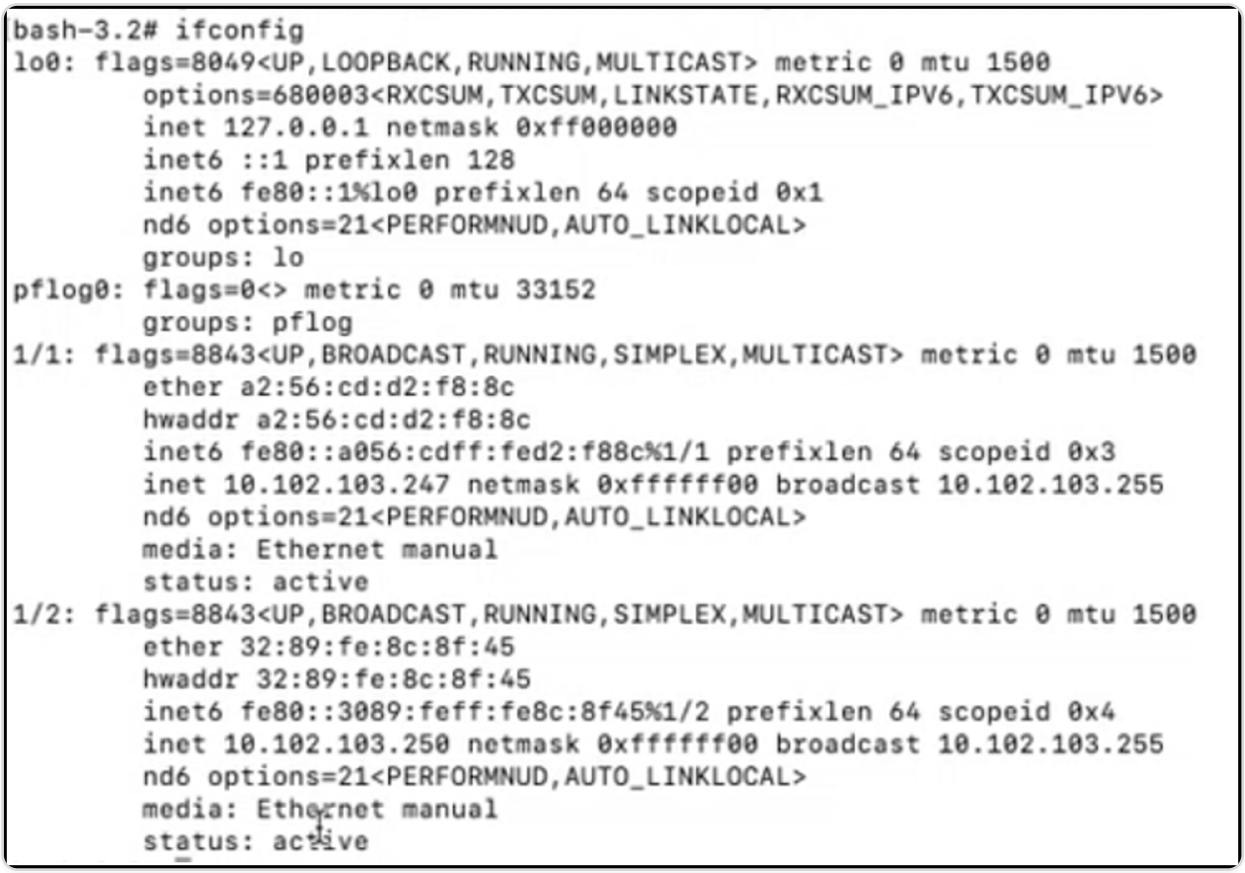
- Ensure you have deployed and configured NetScaler agent on the hypervisor (Citrix Hypervisor, Microsoft Hyper-V, Linux KVM, or VMware ESXi).
- Ensure you have added the second NIC on the hypervisor (Citrix Hypervisor™, Microsoft Hyper-V, Linux KVM, or VMware ESXi).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To assign an IP address to a NIC on a Citrix Hypervisor and create a secondary interface, see Assign an IP Address to a NIC.

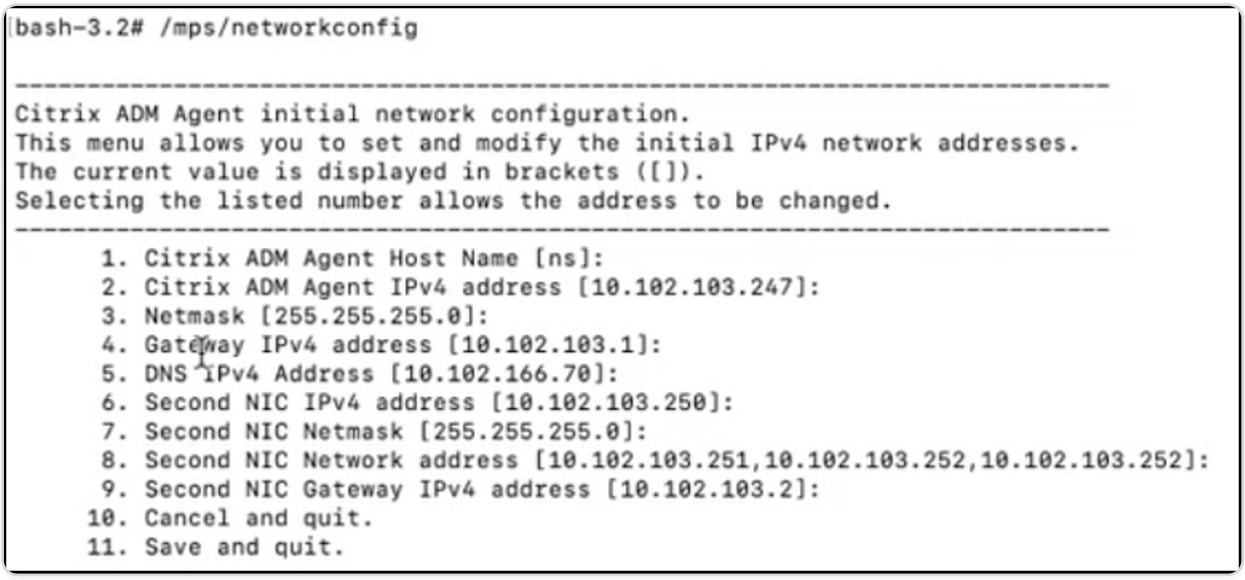
Modify the IPV4 NIC network addresses

1. Open an SSHconnection to the NetScaler agent console by using an SSH client, such as PuTTY.
2. Log in using the **nsrecover/nsroot** credentials and switch to the shell prompt.
3. Run the command **ifconfig**. You can see the details of the two NICs that you have configured -
   - NIC 1 – For communication between agent and NetScaler Communication
   - NIC 2 – For communication between agent and NetScaler Console



4. Run the command **networkconfig**. A menu appears which allows you to set or modify the IPV4 network addresses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE:

\>

Second NIC Network address can take multiple IP values.

5. Select a menu item to modify. Save and quit the settings.

Adding instances

You can add instances either while setting up the NetScaler Console for the first time or later.

Instances are NetScaler appliances or virtual appliances that you want to discover, manage, and monitor from NetScaler Console. You can add the following NetScaler appliances and virtual appliances to NetScaler Console:

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler BLX
- NetScaler Gateway
- Citrix Secure Web Gateway™

To add instances, you must specify either the host name or IP address of each NetScaler instance, or a range of IP addresses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Specify an instance profile that NetScaler Console can use to access the instance. This instance profile contains the user name and password of the instances that you want to add to the service. For each instance type, a default profile is available. For example, the ns-root-profile is the default profile for NetScaler instances. The default NetScaler administrator credentials define this profile. If you have changed the default admin credentials of your instances, you can define custom instance profiles for those instances. If you change the credentials of an instance after the instance is discovered, you must edit the instance profile or create a profile, and then rediscover the instance.

You can access the GUIs of NetScaler instances from the NetScaler Console after adding the instances in the NetScaler Console. To access the NetScaler instances from the NetScaler Console, you must be connected to the Citrix network.

NOTE

- To add NetScaler instances configured in a cluster, you must specify either the cluster IP address or any one of the individual nodes in the cluster setup. However, on NetScaler Console, the cluster IP address represents the cluster.
- For the NetScaler instances set up as an HA pair, when you add one instance, the other instance in the pair is automatically added.
- To make sure that the NetScaler user has all the privileges, assign superuser permissions to the user in NetScaler. For more information, see User, user groups, and command policies

How to create a NetScaler® profile

NetScaler profile contains the user name, password, communication ports, and authentication types of the instances that you want to add to NetScaler Console. For each instance type, a default profile is available. For example, the `nsroot` is the default profile for NetScaler instances. The default profile is defined by using the default NetScaler administrator credentials. If you have changed the default admin credentials of your instances, you can define custom instance profiles for those instances. If you change the credentials of an instance after the instance is discovered, you must edit the instance profile or create a profile, and then rediscover the instance.

You can create a NetScaler profile from the **Instance** page or while adding or changing an instance.

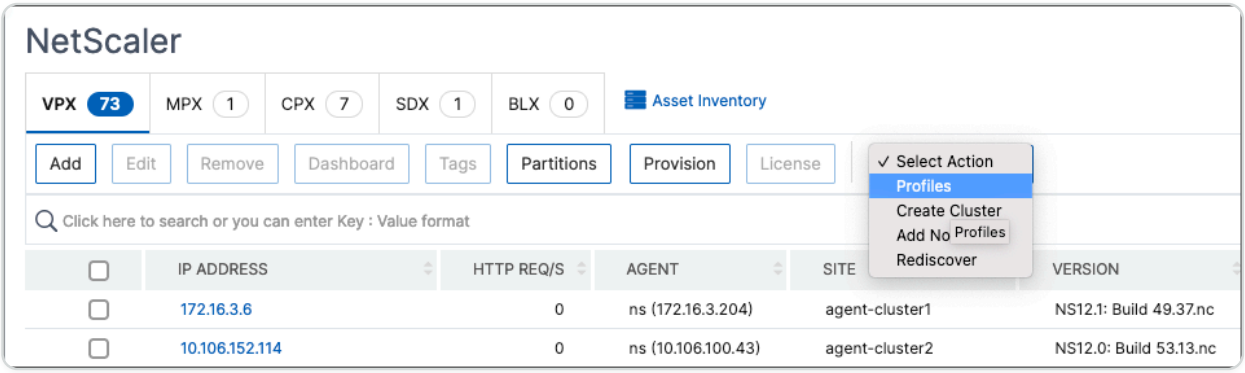
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Ensure to use the super administrator account to create an instance profile.

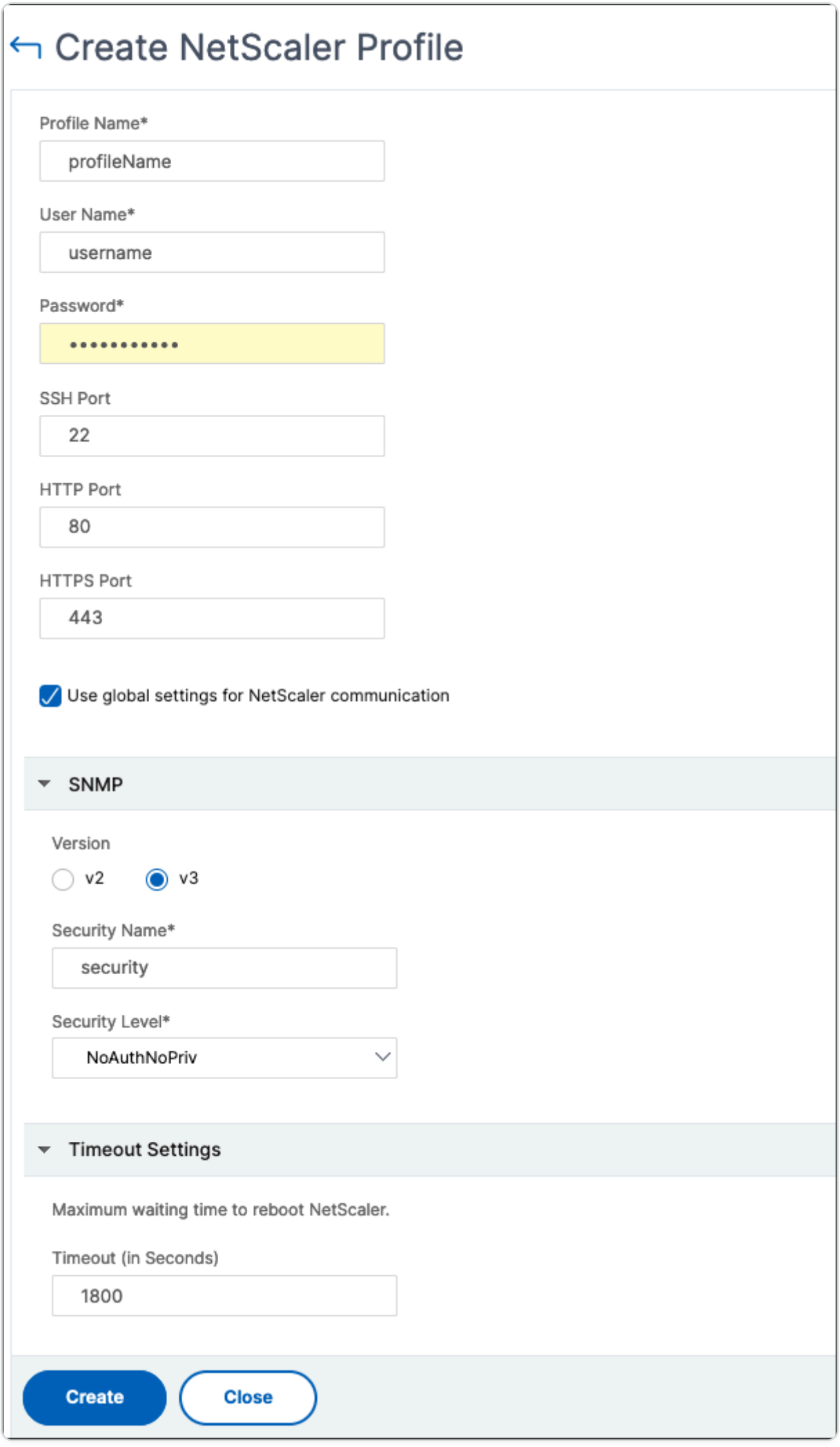
To create a NetScaler profile from the Instance page:

1. Navigate to **Infrastructure > Instances**.
2. Select an Instance. For example, NetScaler.
3. On the NetScaler page, under **Select Action** select **Profiles**.



4. On the **Admin Profiles** page, select **Add**.
5. On the **Create NetScaler Profile** page, do the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.


Create NetScaler Profile
Profile Name*
profileName
User Name*
username
Password*
SSH Port
22
HTTP Port
80
HTTPS Port
443
Use global settings for NetScaler communication
SNMP
Version
v2
v3
Security Name*
security
Security Level*
NoAuthNoPriv
Timeout Settings
Maximum waiting time to reboot NetScaler.
Timeout (in Seconds)
1800
Create
Close

a. **Profile Name**: Specify a profile name for the NetScaler instance.

b. **User Name**: Specify a user name to log on to the NetScaler instance.

c. **Password**: Specify a password to log on to the NetScaler instance.

d. **SSH Port**: Specify the port for SSH communication between NetScaler Console and the NetScaler instance.

e. **HTTP Port**: Specify the port for HTTP communication between NetScaler Console and the NetScaler instance.

> **NOTE:**
>
> The default HTTP port is 80. You can also specify the non-default or customized HTTP port that you might have configured in your NetScaler CPX instance. The customized HTTP port can be used for communication only between NetScaler Console and NetScaler CPX.

f. **HTTPS Port**: Specify the port for HTTPS communication between NetScaler Console and the NetScaler instance.

> **NOTE:**
>
> The default HTTPS port is 443. You can also specify the non-default or customized HTTPS port that you might have configured in your NetScaler CPX instance. The customized HTTPS port can be used for communication only between NetScaler Console and NetScaler CPX.

g. **Use global settings for NetScaler communication**: Select this option if you want to use the system settings for communication between NetScaler Console and NetScaler instance, otherwise select either HTTP or https.

h. **SNMP Version**: Select either **SNMPv2** or **SNMPv3** and do the following:

   i. If you select SNMPv2, specify the **Community** name for authentication.

   ii. If you select SNMPv3, specify the **Security Name** and **Security Level**. Based on the security level, select the **Authentication Type** and **Privacy Type**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **NOTE:**
>
> For NetScaler SDX, only **SNMPv2** is supported.

i. **Timeout Settings**: Specify the time that NetScaler Console must wait before sending a connection request to the NetScaler instance after a restart.

j. Select **Create**.

To add a NetScaler instance to NetScaler Console

> **NOTE**
>
> Perform this task to add all other NetScaler instances except the NetScaler CPX instance.

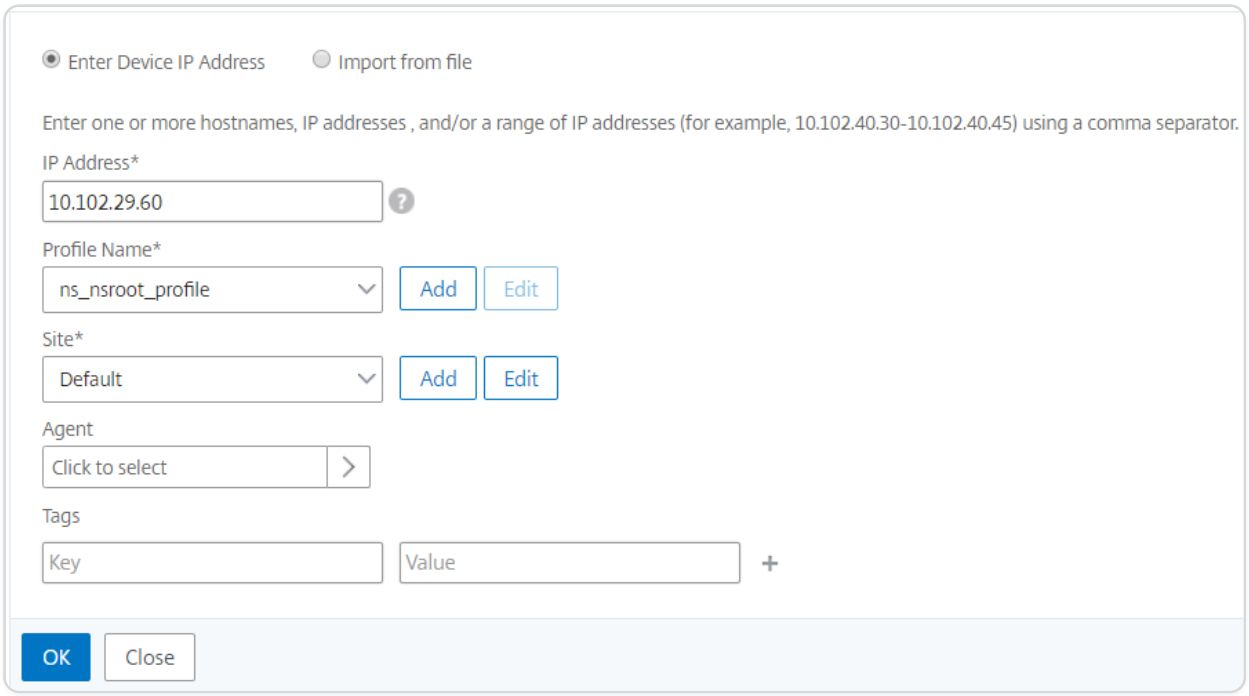
1. Navigate to **Infrastructure > Instances > NetScaler**. Under **Instances**, select the type of instance you want to add (for example, NetScaler VPX) and click **Add**.
2. Select one of the following options:
   - **Enter Device IP address** - For NetScaler instances, specify any one of the following:
     - Host name
     - IP address or NAT IP of each NetScaler instance
     - Range of IP addresses

     For example, enter one or more host names, IP addresses or NAT IP, and/or a range of IP addresses (for example, 10.10.20.10-10.10.20.45) using a comma separator. Input format for the discovery of NAT HA instances is 10.10.20.10#10.10.20.32 (NAT IP address of both NetScaler HA instances).
   - **Import from file** - From your local system, upload a text file that contains the IP addresses of all the instances you want to add.
3. (Optional) Select **Enable Device addition on first time login failure**. With this option, you can add the instance even without valid credentials.
4. From **Profile** Name, select the appropriate instance profile, or create a profile by clicking the **+** icon.
5. From **Site**, select the site where you want the instance to be added.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. From **Agent**, select the agent with which you want to associate the instances, and then click **OK**.

   If there is only one agent configured on your NetScaler Console, that agent is selected by default.



To add NetScaler CPX instance in NetScaler Console

1. Navigate to **Infrastructure > Instances**. Under **Instances**, select **NetScaler** and select the CPX tab.
2. Click **Add**.
3. Select one of the following options:

   - **Enter Device IP address**. Specify either the host name or IP address of each instance, or a range of IP addresses.
   - **Import from file**. From your local system, upload a text file that contains the IP addresses of all the instances you want to add.

4. (Optional) Select **Enable Device addition on first time login failure**. With this option, you can add the instance even without valid credentials.
5. In the **Routable IP/Docker IP** field, enter the IP address. The IP address can be either the NetScaler CPX instance (if it is reachable) or the Docker host.
6. In the **Profile Name** field, select the appropriate instance profile, or create a profile by clicking the + icon.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

When you are creating a profile, ensure to specify the HTTP, HTTPS, SSH, and SNMP port details of the host. You can also specify the range of ports that are published by the host in the Start Port and Number of ports field.

7. As an option, select the site where you want to deploy the CPX instance. You can create a site also by clicking **Add**.
8. If available, select the agent from the list of agents.
9. Click **OK** to initiate the process of adding instances to NetScaler Console.

NOTE

If you want to rediscover an instance, perform the following steps:

a. Navigate to **Infrastructure > Instances > NetScaler** > **CPX**.
b. Select the instance you want to rediscover.
c. From the **Select Action** list, click **Rediscover**.

To add a standalone NetScaler BLX instance in NetScaler Console

A standalone NetScaler BLX instance is a single instance that is running on the dedicated host Linux server.

1. Navigate to **Infrastructure > Instances > NetScaler**.
2. In the **BLX** tab, click **Add**.
3. (Optional) Select **Enable Device addition on first time login failure**. With this option, you can add the instance even without valid credentials.
4. Select the **Standalone** option from the **Instance Type** list.
5. In the **IP address** field, specify the IP address of the BLX instance.
6. In the **Host IP address** field, specify the IP address of the Linux server where the BLX instance is hosted.
7. In the **Profile Name** list, select the appropriate profile for a BLX instance, or create a profile.

   To create a profile, click **Add**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT

Ensure you have specified the correct host user name and password of the Linux server in the profile.

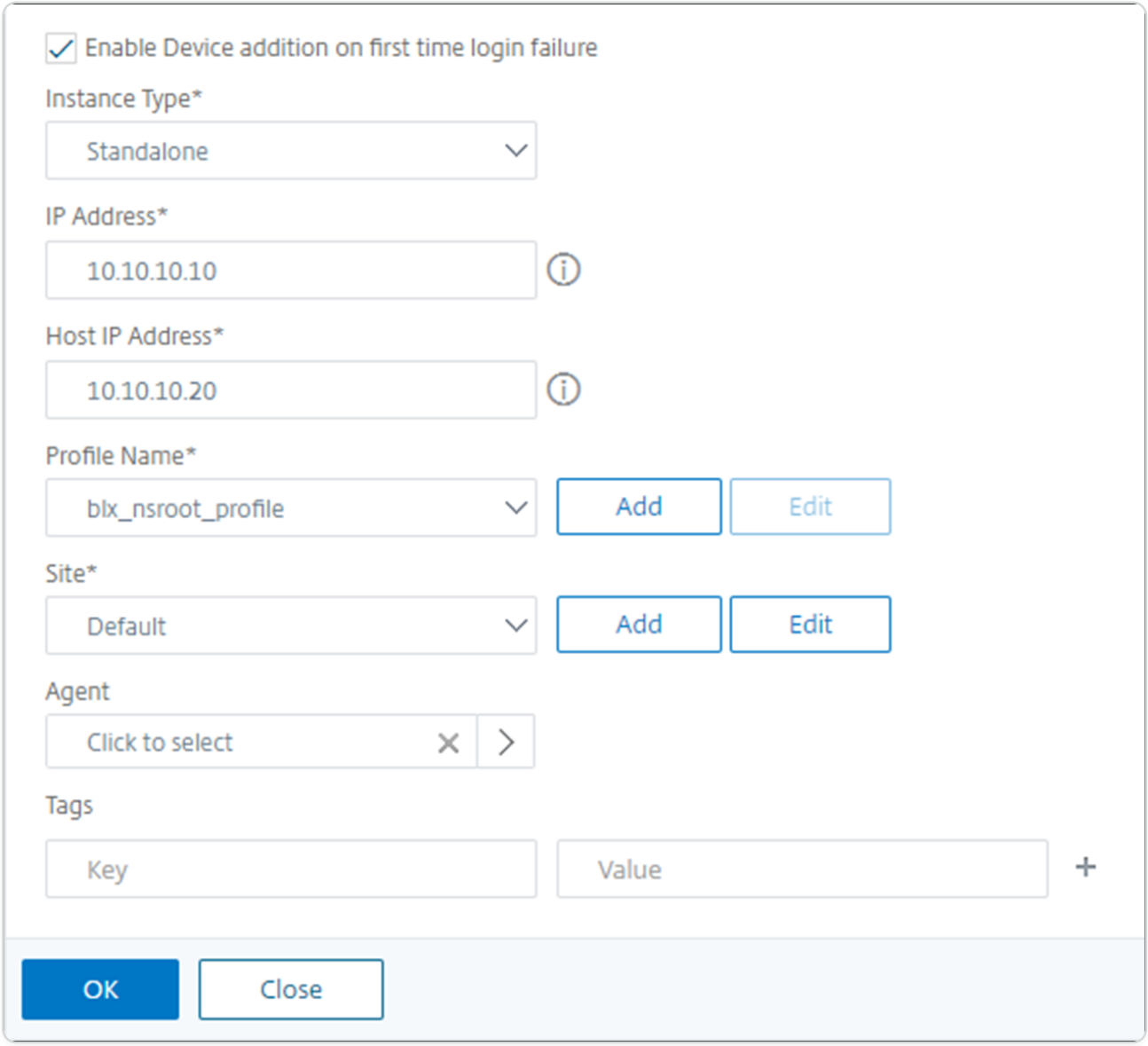
8. In the **Site** list, select the site where you want to add an instance.

   If you want to add a site, click **Add**.

9. In the **Agent** list, select the agent to which you want to associate the instance.

   If there is only one agent configured on your NetScaler Console, that agent is selected by default.

10. Click **OK**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

To add high-availability NetScaler BLX instances in NetScaler Console

The high-availability NetScaler BLX instances that run on different host Linux servers. A Linux server cannot host more than one BLX instances.

1. In the **BLX** tab, click **Add**.
2. (Optional) Select **Enable Device addition on first time login failure**. With this option, you can add the instance even without valid credentials.
3. Select the **High Availability** option from the **Instance Type** list.
4. In the **IP address** field, specify the IP address of the BLX instance.
5. In the **Host IP address** field, specify the IP address of the Linux server where the BLX instance is hosted.
6. In the **Peer IP address** field, specify the IP address of the peer BLX instance.
7. In the **Peer Host IP address** field, specify the IP address of the Linux server where the peer BLX instance is hosted.
8. In the **Profile Name** list, select the appropriate profile for a BLX instance, or create a profile.

   To create a profile, click **Add**.

   IMPORTANT

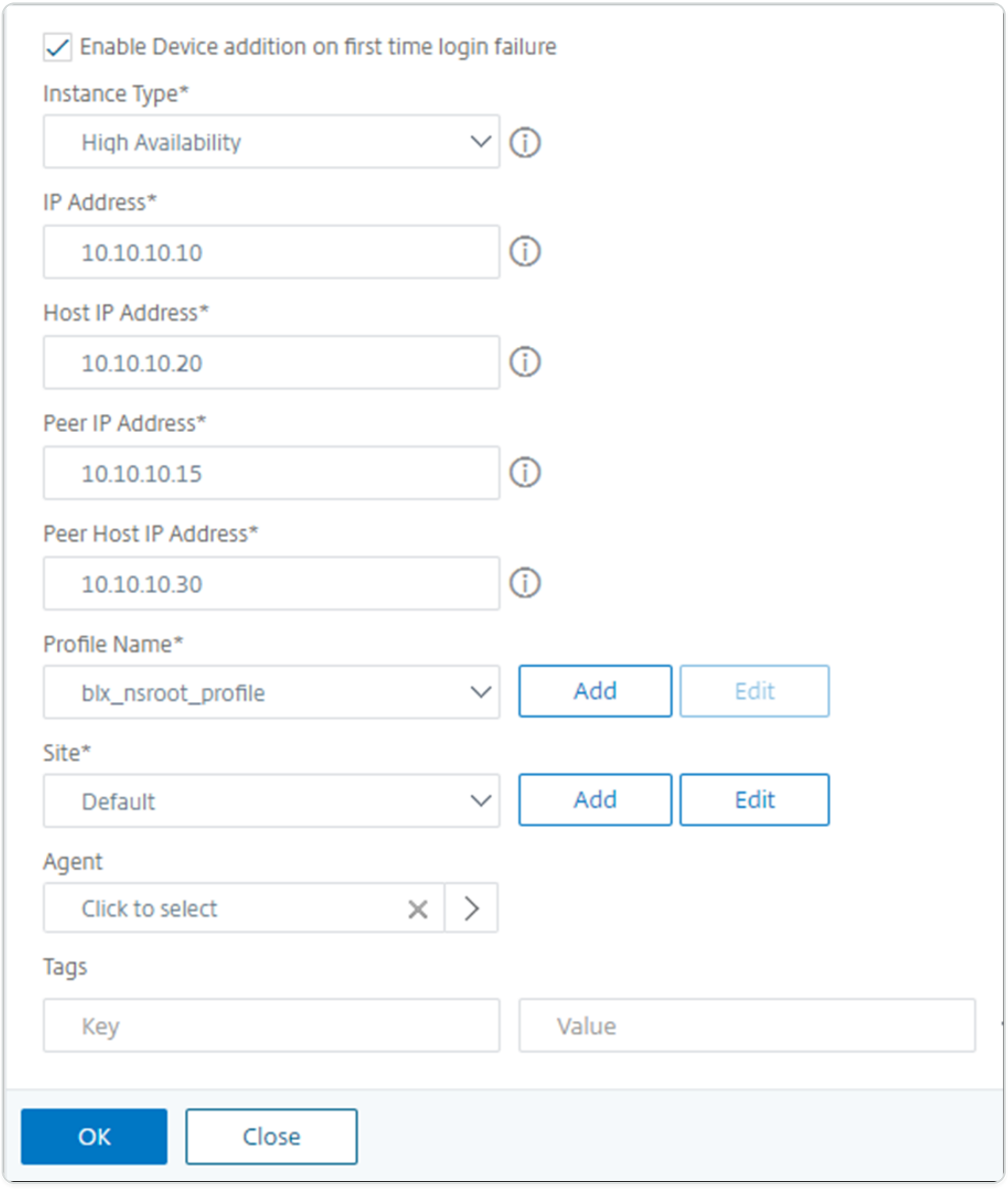
   Ensure you have specified the correct host user name and password of the Linux server in the profile.

9. In the **Site** list, select the site where you want to add an instance.

   If you want to add a site, click **Add**.
10. In the **Agent** list, select the agent to which you want to associate the instance.

    If there is only one agent configured on your NetScaler Console, that agent is selected by default.
11. Click **OK**.

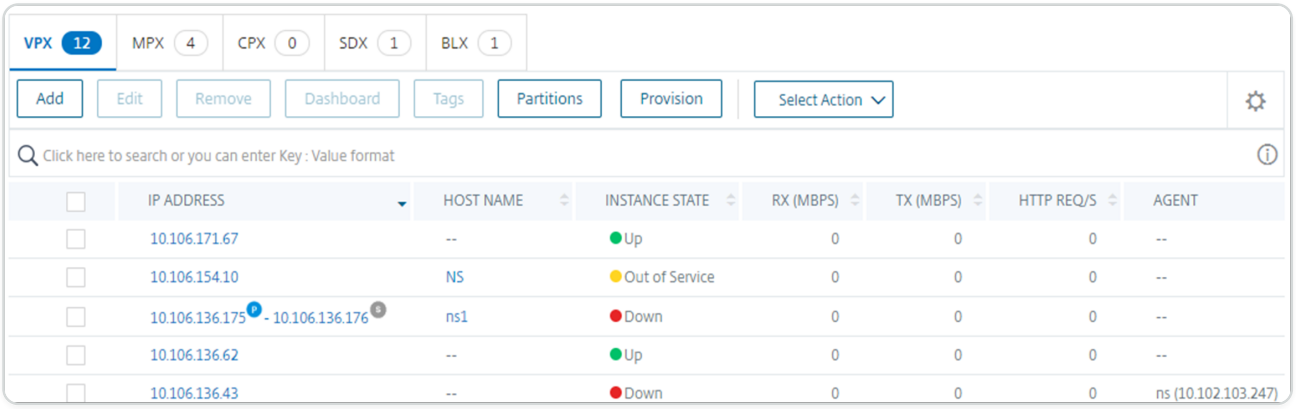
© 1997–2026 Citrix Systems, Inc. All rights reserved.



To access an instance GUI from the NetScaler Console

1. Navigate to **Infrastructure > Instances** > **NetScaler**.
2. Select the type of instance you want to access (for example, VPX, MPX, CPX, SDX, or BLX).
3. Click the required NetScaler IP address or host name.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The instance IP addresses indicate the deployment type with the following notations:

- In high-availability pair, **P** – Primary server and **S** – Secondary server.
- **C**-Cluster
- **A**-Autoscale™ Group

If an Instance has no notation, it indicates the standalone deployment.

The GUI of the selected instance appears in a pop-up window.

Resolve instance warnings

A warning sign appears on the instance for the following reasons:

- **Login failed** - When you add an instance without valid credentials, it appears in DOWN state, with a Login failed warning. Specify the correct credentials to manage the instance in NetScaler Console.

  If the instance is unlicensed, the **License** option appears when you select the instance. Click **License** to apply the license to an instance from the license pool.
- **Unlicensed instance with HTTPS profile** - If an unlicensed instance uses only HTTPS connection, apply license to an instance from the NetScaler GUI.

Configuring syslog on instances

The syslog protocol provides a transport to allow the NetScaler instances to send event notification messages to NetScaler Console, which is configured as a collector or the syslog server for these messages.

You can monitor the syslog events generated on your NetScaler instances if you have configured your device to redirect all syslog messages to NetScaler Console. To monitor syslog events, you need to first configure NetScaler Console as the syslog server for your NetScaler instance. After

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the instance is configured, all the syslog messages are redirected to NetScaler Console, so that these logs can be displayed to the user in a structured manner.

Syslog uses the User Datagram Protocol (UDP), port 514, for communication, and because UDP is a connectionless protocol it does not provide any acknowledgment back to the instances. The syslog packet size is limited to 1024 bytes and carries the following information:

- Facility
- Severity
- Host name
- Timestamp
- Message

In NetScaler Console, you must configure facility and log severity levels on the instances.

- **Facility** - Syslog messages are broadly categorized on the basis of the sources that generate them. These sources can be the operating system, the process, or an application. These categories are called facilities and are represented by integers. For example, 0 is used by kernel messages, 1 is used by user-level messages, 2 is used by the mail system, and so on. The local use facilities (from local0 to local7) are not reserved and are available for general use. Hence, the processes and applications that do not have pre-assigned facility values can be directed to any of the eight local use facilities.
- **Severity** - The source or facility that generates the syslog message also specifies the severity of the message using a single-digit integer, as shown below:

```
1 - Emergency: System is unusable.


2 - Alert: Action must be taken immediately.


3 - Critical: Critical conditions.


4 - Error: Error conditions.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
5 - Warning: Warning conditions.


6 - Notice: Normal but significant condition.


7 - Informational: Informational messages.


8 - Debug: Debug-level messages.
```

To configure syslog on NetScaler instances:

1. In NetScaler Console, navigate to **Infrastructure > Instances**.
2. Select the NetScaler instance from which you want the syslog messages to be collected and displayed in NetScaler Console.
3. In the **Action** drop-down list, select **Configure Syslog**.
4. Click **Enable**.
5. In the **Facility** drop-down list, select a local or user-level facility.
6. Select the required log level for the syslog messages.
7. Click **OK**.

This configures all the syslog commands in the NetScaler instance, and NetScaler Console starts receiving the syslog messages. You can view the messages by navigating to **Infrastructure > Events > Syslog Messages**.

Logstream overview

NetScaler instances generate AppFlow records and are a central point of control for all application traffic in the data center. **IPFIX** and **Logstream** are the protocols that transport these AppFlow records from NetScaler instances to NetScaler Console. For more information, see AppFlow.

- **IPFIX** is an open Internet Engineering Task Force (IETF) standard defined in RFC 5101. **IPFIX** uses UDP protocol which is unreliable transport protocol used for data flow in one direction.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Since IPFIX uses UDP protocol, adhering to IPFIX standard results in processing more resources in NetScaler Console.

- **Logstream** is a Citrix-owned protocol that is used as one of the transport modes to efficiently transfer the analytics log data from NetScaler instances to NetScaler Console. **Logstream** uses reliable TCP protocol and requires lesser resources in processing the data.

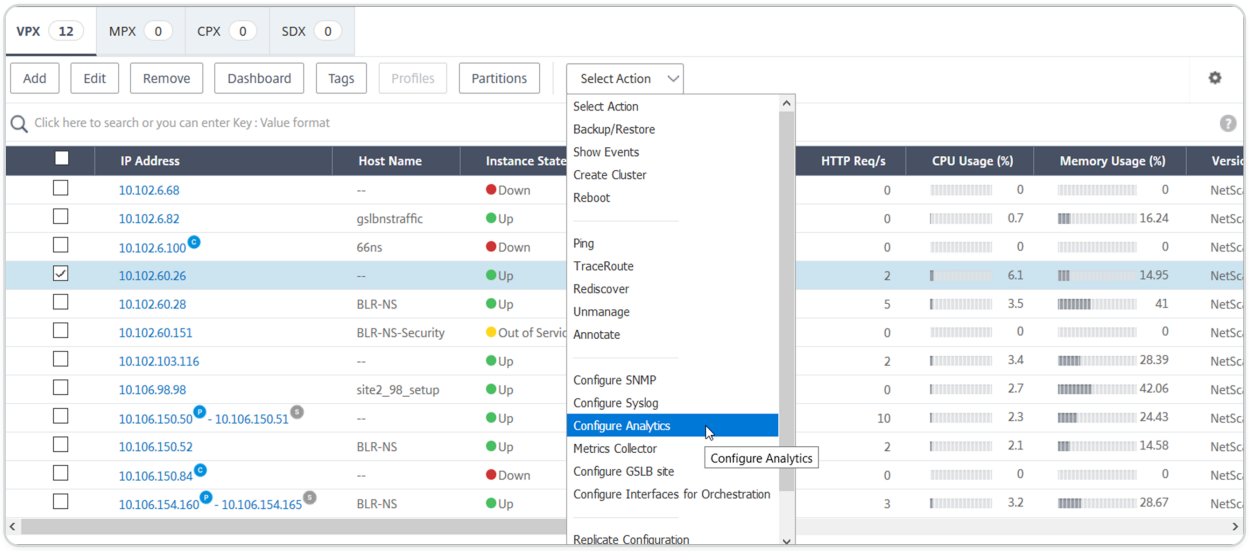
For NetScaler between **11.1 Build 47.14 and 11.1 Build 62.8**, **Logstream** is the default transport mode for enabling Web Insight (HTTP) and IPFIX is the only transport mode for enabling other insights. For NetScaler version starting from **12.0 to latest version**, you can select either **Logstream** or **IPFIX** as the transport mode.

NOTE

The NetScaler Console version and build must be **equal to or higher** than your NetScaler version and build. For example, if you have installed NetScaler 12.1 Build 50.28/50.31, then ensure you have installed NetScaler Console 12.1 Build 50.39 or later.

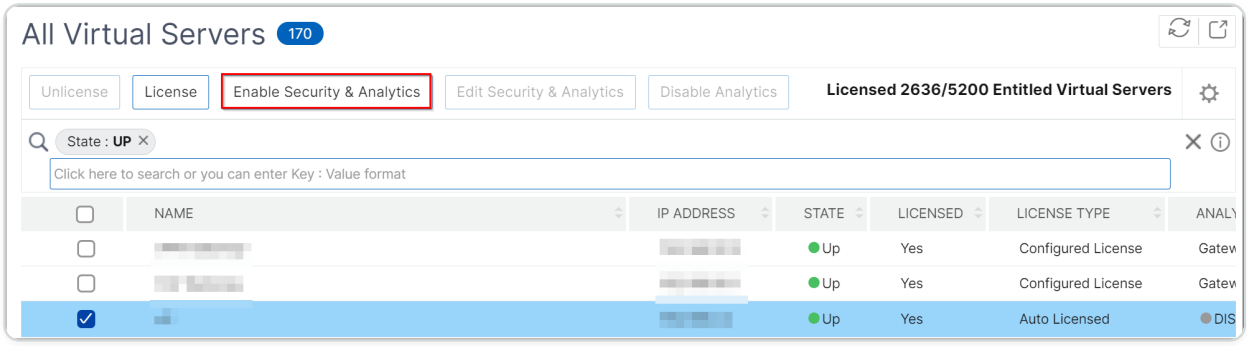
Enable Logstream as Transport Mode

1. Navigate to **Infrastructure > Instances**, and select the NetScaler instance you want to enable analytics.
2. From the **Select Action** list, select **Configure Analytics**.



3. Select the virtual servers and then click **Enable Security & Analytics**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. On the **Enable Security & Analytics** window:

   a. Select the insight types (Web Insight or WAF Security Violations or Bot Security Violations)

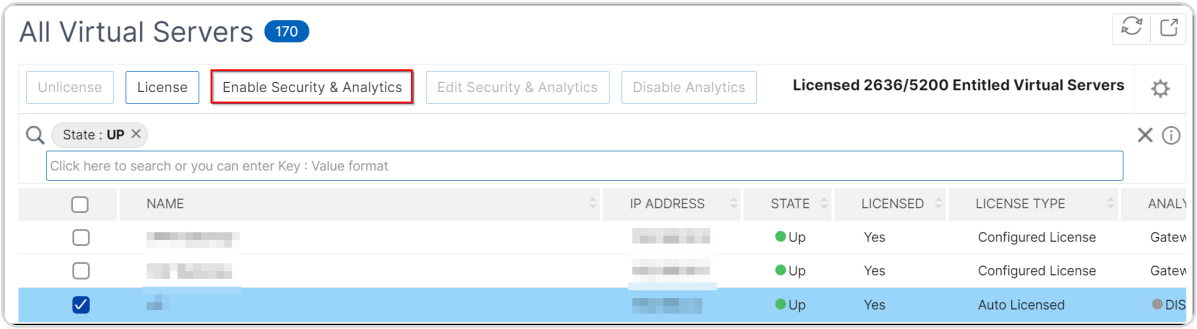
   b. Select **Logstream** as Transport Mode

   NOTE

   For NetScaler between **11.1 Build 47.14 and 11.1 Build 62.8**, **Logstream** is the default transport mode for enabling Web Insight (HTTP) and IPFIX is the only transport mode for enabling other insights. For NetScaler version starting from **12.0 to latest version**, you can select either **Logstream** or **IPFIX** as the transport mode.

   c. The Expression is true by default

   d. Click **Save Analytics**



NOTE

- For admin partitions, only **Web Insight** is supported
- For virtual servers such as Cache Redirection, Authentication, and GSLB, you cannot enable analytics. An error message is displayed.

The following table describes the features of NetScaler Console that supports **Logstream** as the transport mode:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE	IPFIX	LOGSTREAM
Web Insight	•	•
Bot Security Violations	Not supported	•
WAF Security Violations	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	Not supported	•
CR Insight	•	•
IP Reputation	•	•
AppFirewall	•	•
Client Side Measurement	•	•
Syslog/Auditlog	•	•

How to assign more permissions to delegated admin users

When the first user of your organization signs up and logs on to NetScaler Console, this user is assigned the super admin privileges. Every subsequent user that logs on is assigned a delegated admin role by default. A delegated admin does not have the permission to view and perform any tasks related to user administration or RBAC settings.

However, you can assign super admin privileges or specific non-super admin roles to a delegated admin so that the admin is able to perform tasks related to user administration.

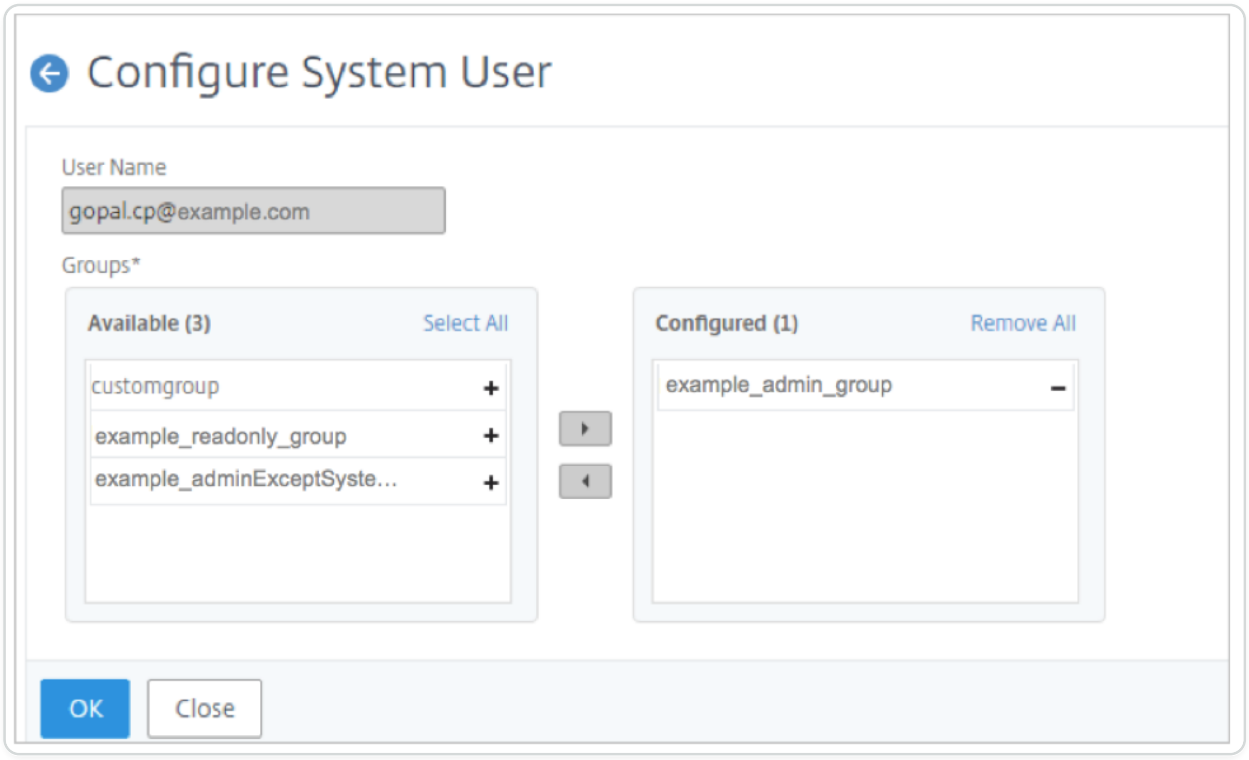
For detailed information about role-based access control see Configuring Role-Based Access Control.

Assigning Super Admin Permissions to a Delegated Admin

To assign super admin permissions to a delegated admin, a super admin has to assign the default admin group to a delegated admin user. Perform the following tasks:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Log on to NetScaler Console as the super admin.
2. Navigate to **Account** > **User Administration** > **Users**.
3. Select the user name of the delegated admin and click **Edit**.
4. Assign the group **\<*tenant*_*name*\>_admin_group** to the delegated admin and click **OK**. For example, in the following image, "example_admin_group" is assigned to a delegated admin user.

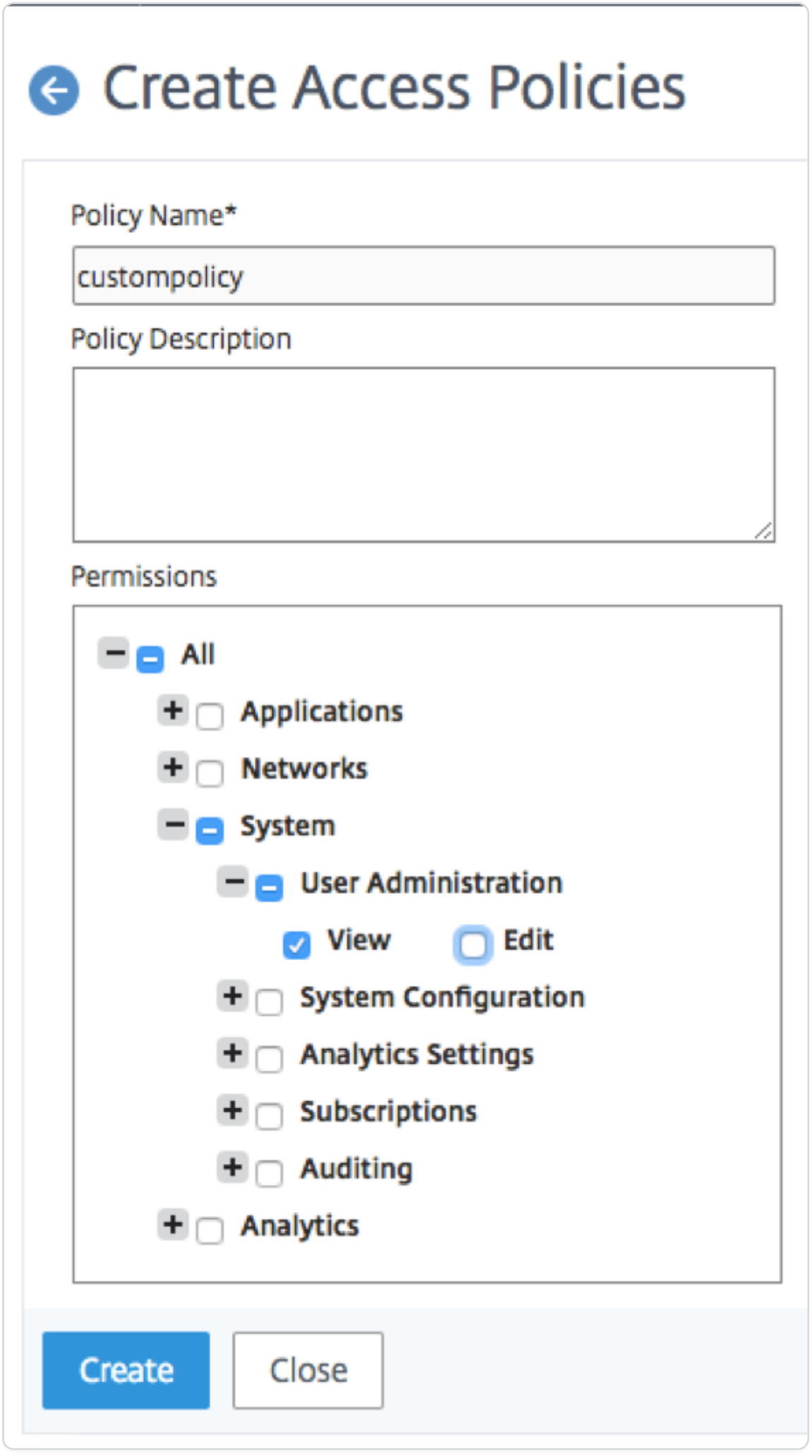


Assigning Custom Role to a Delegated Admin

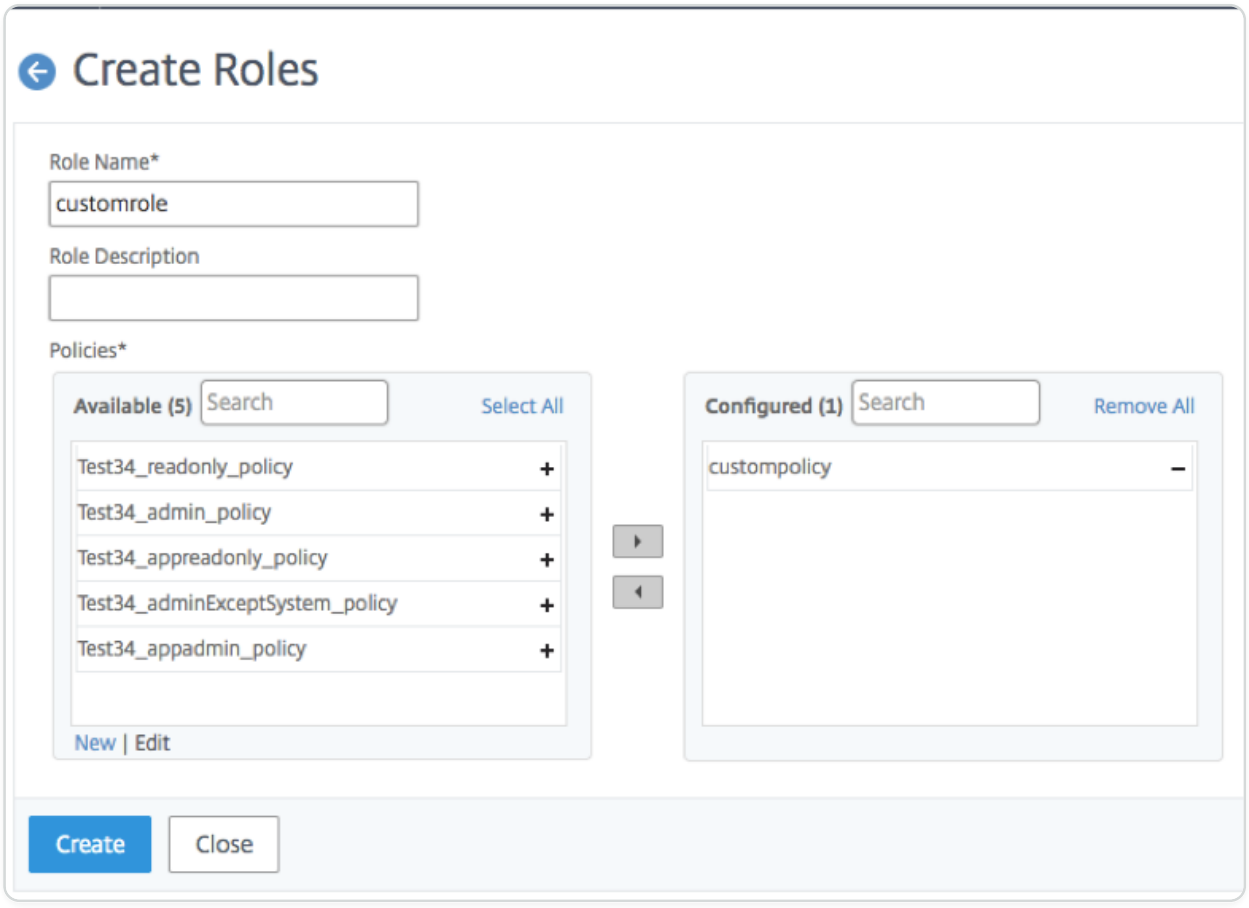
To assign any custom role to a delegated admin, the super admin has to create a group, role, and policy and assign to the delegated admin user. This ensures that the delegated admin has only the required permissions. Perform the following tasks:

1. Log on to NetScaler Console as the super admin.
2. Navigate to **Account** > **User Administration** > **Access Policies**. Select **Add** to create an access policy with the required permissions for the delegated admin. In this example, an access policy `custompolicy` is created that allows view access to User Administration settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

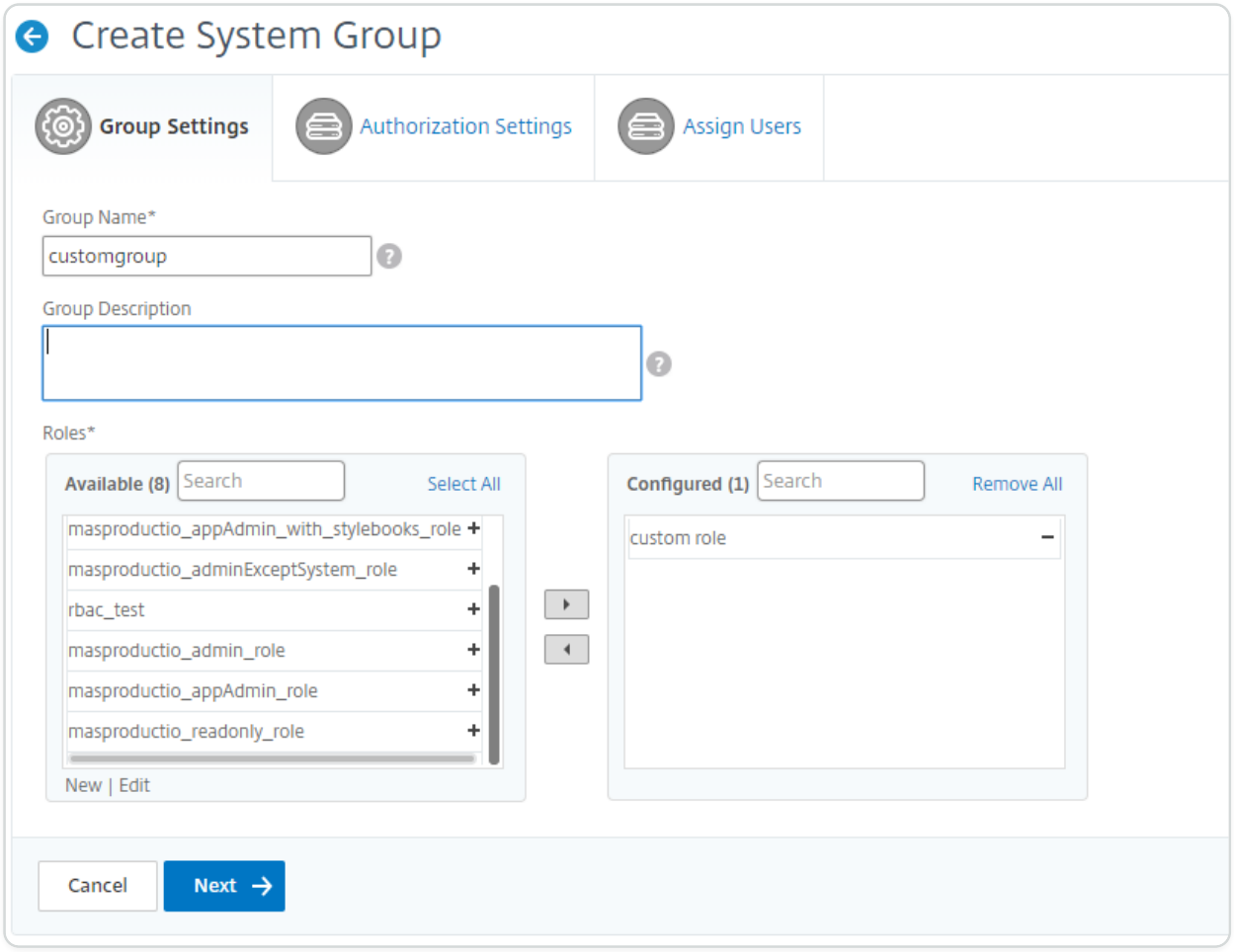

Create Access Policies
Policy Name*
custompolicy
Policy Description
Permissions
All
Applications
Networks
System
User Administration
View
Edit
System Configuration
Analytics Settings
Subscriptions
Auditing
Analytics
Create
Close

3. Navigate to **Account** > **User Administration** > **Roles**. Select **Add** to create a role and bind this role to the access policy that you created in the previous step. In this example, a role `customrole` is created and bound to the `custompolicy` access policy.



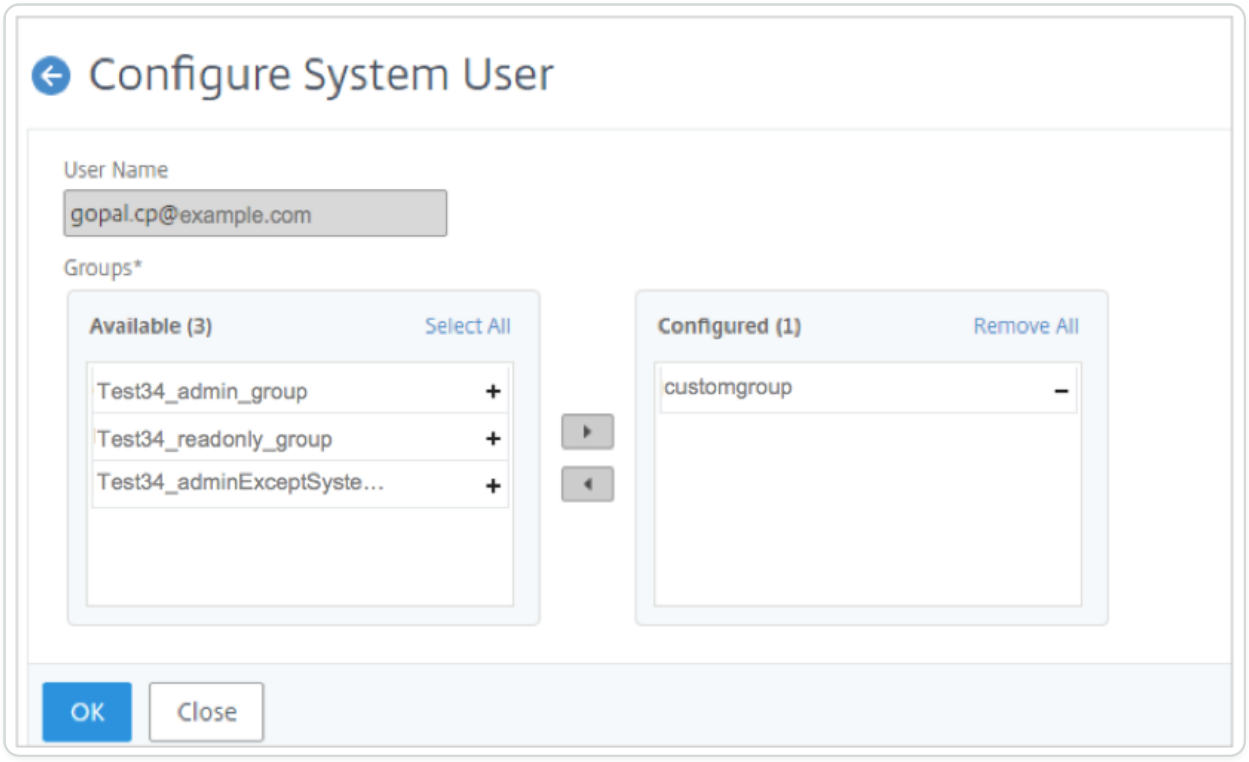
4. Navigate to **Account** > **User Administration** > **Groups**. Select **Add** to create a group and bind this group to the role you created in the previous step. In this example, the group "custom group" is created and bound to the role "custom role."

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Navigate to **Account** > **User Administration** > **Users**
6. Select the user name of the delegated admin and click **Edit**.
7. Assign the group you created in the previous step to the delegated admin user. In this example, the delegated admin user is assigned the group `customgroup`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Integration with the ServiceNow instance

As a NetScaler administrator, you might use ServiceNow as the primary IT request and support system. You need to raise tickets or incidents for the critical NetScaler events to investigate, track, and troubleshoot them.

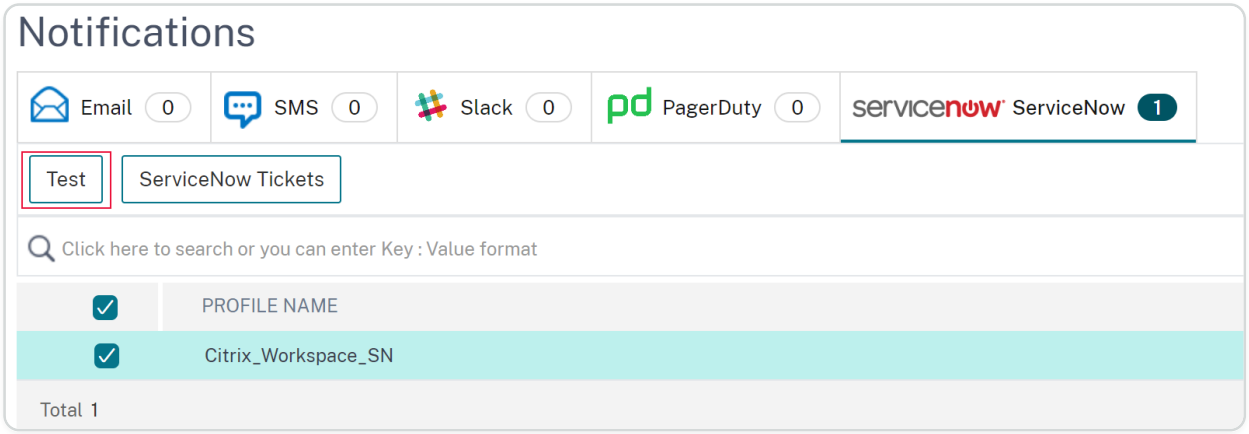
You can automate the ticket creation in ServiceNow using NetScaler Console and Citrix ITSM connector for ServiceNow. To start this automation, onboard Citrix ITSM adapter service to receive events and create relevant incidents in ServiceNow. For more information about preparation and integration steps, see Get started in Citrix ITSM Adapter Service.

After the successful integration, configure auto-generate ServiceNow incidents in NetScaler Console. Follow the steps to verify whether ServiceNow tickets are getting auto generated.

1. Log in to NetScaler Console.
2. Navigate to **Settings > Notifications** and select **ServiceNow**.
3. Select the ServiceNow profile from the list.
4. Click **Test** to auto-generate a ServiceNow ticket and verify the configuration.

   if you want to view ServiceNow tickets in the NetScaler Console GUI, select **ServiceNow Tickets**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



When you integrate NetScaler Console with ServiceNow, you can automate the generation of ServiceNow incidents for the following:

- Any NetScaler events
- SSL Certificates that are about to expire
- The NetScaler Console license expiry events

And, you can also customize the NetScaler Console event policies.

Generate ServiceNow incidents for any NetScaler events

In NetScaler Console, you can configure rules to automatically raise a ticket in ServiceNow for specific events. NetScaler Console auto generates a ServiceNow ticket for events like:

- Virtual servers go down or out of service.
- Resource consumption crosses the threshold value.
- License expires on a NetScaler instance.

The auto generated ticket in ServiceNow has the required details to track and troubleshoot the issue. You can manage the notifications across one or more network devices from a single ServiceNow console. Then, assign to the administrator for further analysis.

You can create an event rule on the NetScaler Console by navigating to **Infrastructure > Events > Rules**. For more information, see Send ServiceNow notifications.

Generate ServiceNow incidents for SSL certificates that are about to expire

When an SSL certificate on NetScaler instances is about to expire, NetScaler Console auto generates a ServiceNow ticket. This way you can check the upcoming SSL certificate expiry tickets in advance on your ServiceNow dashboard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To send ServiceNow notifications for an SSL certificate expiry, see SSL certificate expiry.

Generate ServiceNow incidents for NetScaler Console license expiry

In NetScaler Console, you can configure the rules to automatically raise a ticket in ServiceNow for specific NetScaler Console license expiry events.

To send ServiceNow notifications for the NetScaler Console license expiry, see NetScaler Console license expiry.

Customize NetScaler Console event policies

You can define policies to control how ServiceNow processes the NetScaler Console events based on event attributes. Set the NetScaler Console event policies in the Citrix ITSM connector. You can decide how an incident must be generated, processed, and reported in ADM. Then, do the following actions through ITSM:

- Ignore incidents
- Display incidents on the dashboard
- Create incidents

For more information, see Customize NetScaler Console event policies.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Actionable tasks and recommendations

NOTE:

- The **To Do** tab is renamed as **Recommendations**. In **Recommendations**, you can continue to review the existing tasks and click **Guide Me** to complete the task.
- The **Archive** tab is no longer available. Instead, you can choose to **Dismiss** a recommendation from the list.

You might have hundreds of discovered NetScaler instances and configured multiple virtual servers (applications) from each instance. As an administrator, you must ensure that all the NetScaler instances and your applications are efficiently managed to get insights for better prioritizing and troubleshooting.

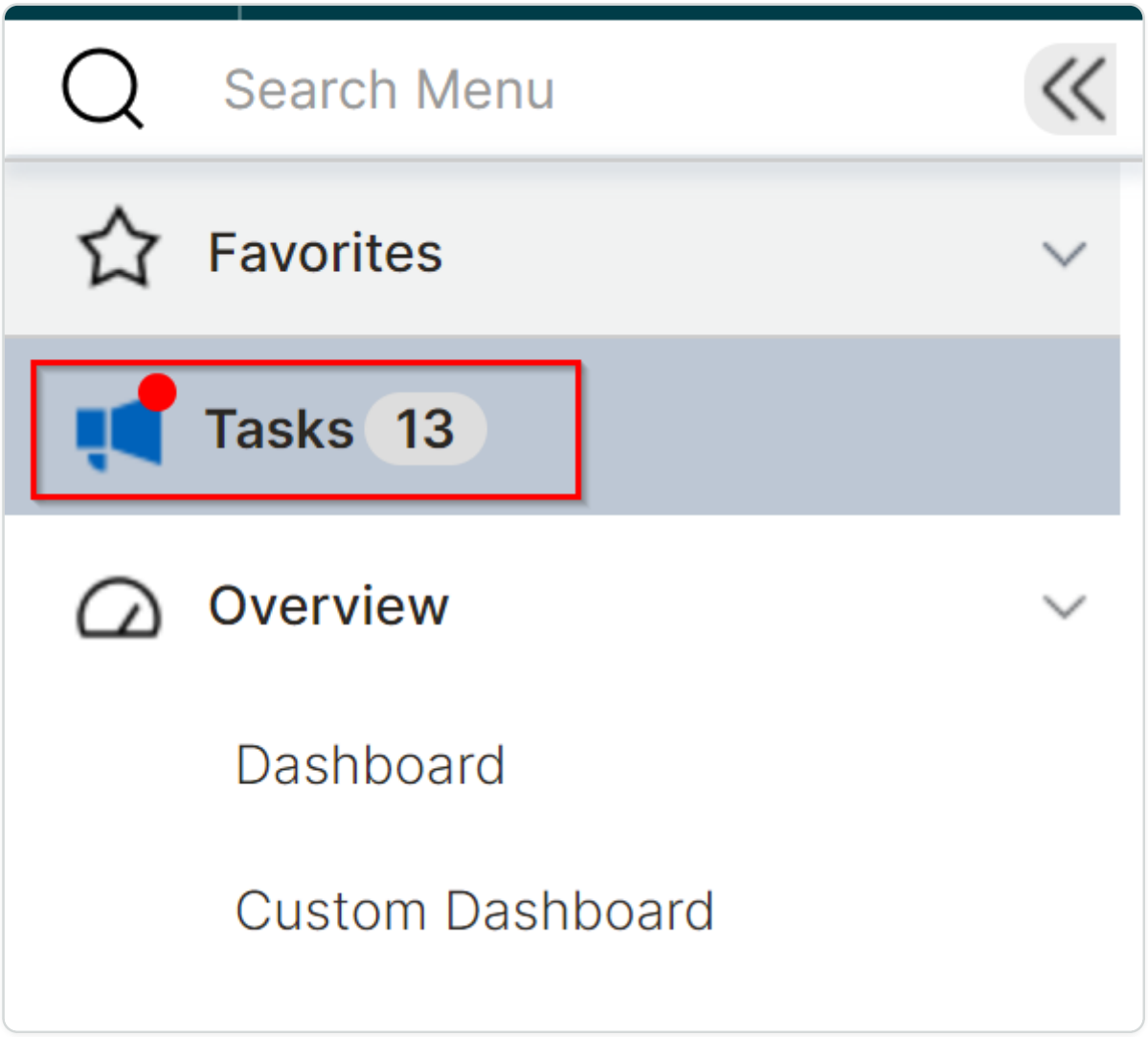
As you scale-up your infrastructure more, you might also need to focus on the critical issues impacting your instances and applications that need your immediate attention. You must also ensure that your NetScaler Console deployment is efficient, secure, and compliant. Based on your current utilization and subscription, the **Tasks** feature in NetScaler Console enables you to view both actionable **Tasks** that you must take immediate action and **Recommendations** to ensure efficient deployment.

As an administrator, by using these actionable **Tasks** and **Recommendations**, you can:

- Get instant visibility on any observations or issues that require your immediate action.
- Configure notifications to receive notification whenever NetScaler Console detects any tasks and proactively take action.
- Achieve an efficient deployment of NetScaler Console and NetScaler instances.
- Reduce the crucial time and effort in identifying the critical issues.
- Ensure that you are using all the capabilities of NetScaler Console, enable product discovery and functionalities recommended by the product for efficient administration of the deployment.

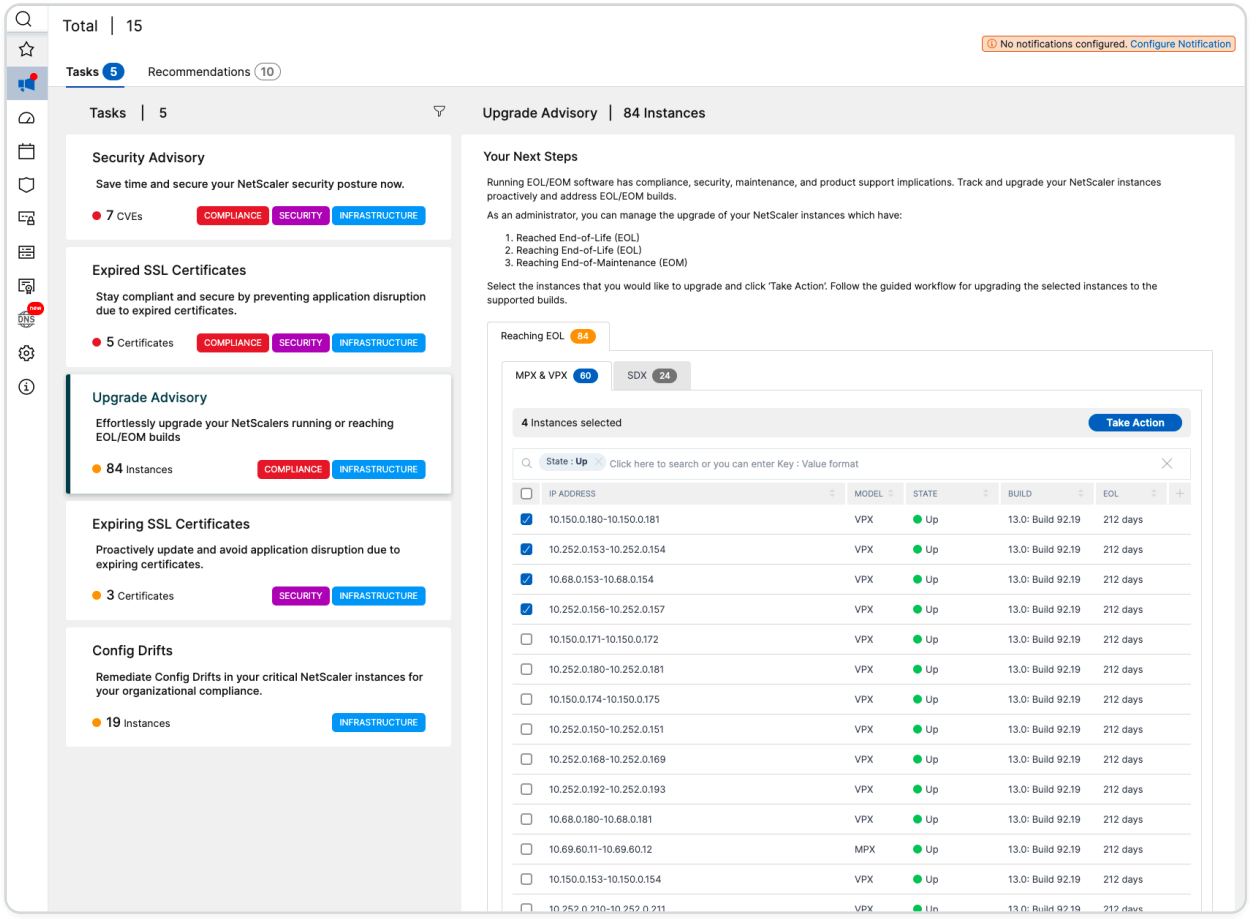
From the NetScaler Console GUI, click **Tasks** to view both **Tasks** and **Recommendations**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Tasks** - Enables you to view a list of tasks that need your immediate attention and action. As you scale-up your infrastructure, some critical issues might go unnoticed that result in security breach. For example, NetScaler instances with CVEs require immediate attention and you must take immediate action to ensure that the instances are running in the recommended build and version. In **Tasks**, you can immediately get those insights. Based on your current utilization, you can view a total of 5 tasks. The tasks are displayed based on the severity (Critical and Medium).

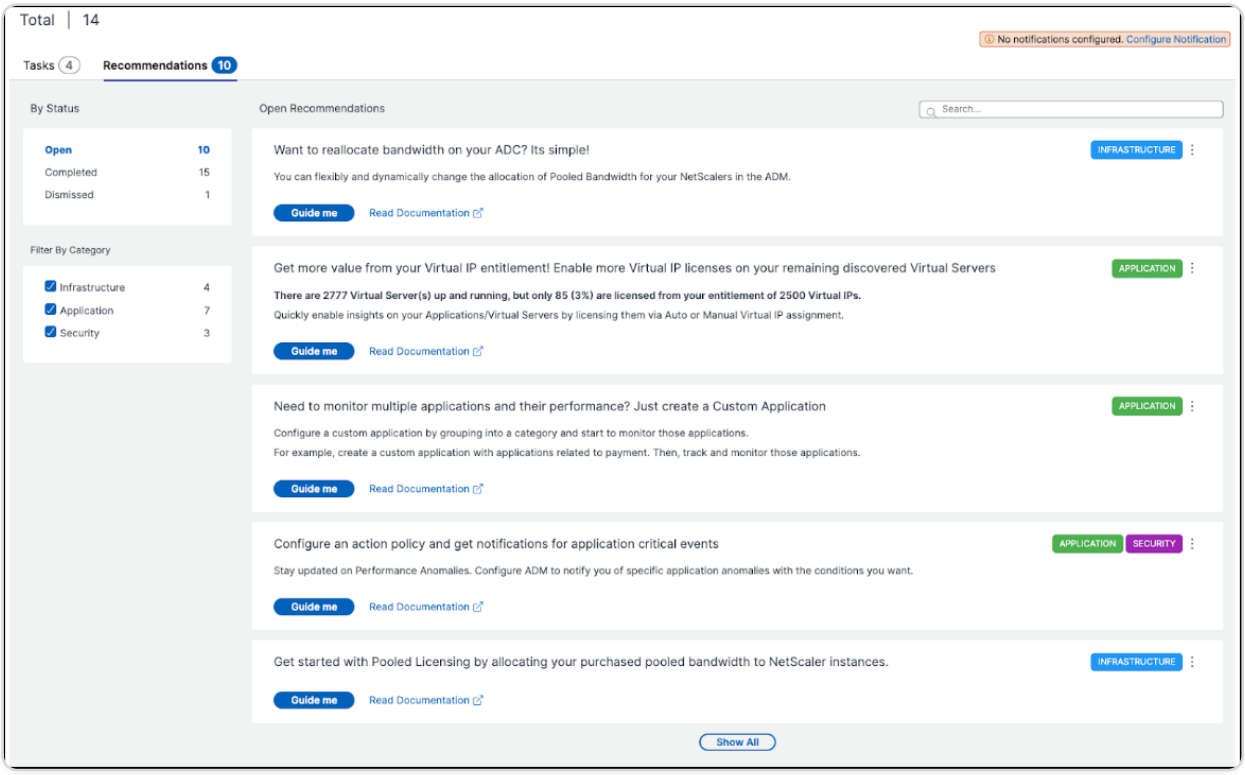
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Recommendations** - Provides certain recommendations based on your current utilization to improve your NetScaler Console deployment. You can use the **Guide Me** option to complete any recommendation. Any recommendation that you complete using the **Guide Me** option is moved to Completed. You can also dismiss any recommendations and they are moved under **Dismissed** category. To view your dismissed recommendations, use the filter **By Status** and select **Dismissed** to view those dismissed recommendations.

  You can also use the **Filter By Category** to filter specific recommendations based on the categories (Infrastructure, Application, and Security). Alternatively, you can also use the **Search** bar, type in the first few characters to drill down to the task.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Tasks

Under **Tasks**, you can view the following 4 tasks depending upon your current NetScaler Console deployment.

- **Expired SSL Certificates** – Provides information about the expired SSL certificates installed in your NetScaler Console. Select this task to view the following tabs:
  - **Delete unused certificates**: Displays the certificates that are not used in any NetScaler instances. To complete the task, review the unused certificates, select the certificate, click **View and Delete**.

    Recommended Action: You are redirected to **Infrastructure > SSL Dashboard > SSL Certificates - Expired**. To delete a certificate, click **Delete**. If you want to update the certificate, select the certificate and click **Update**. For more information, see How to update an installed certificate.
  - **Update certificates**: Displays the certificates that are already expired. To complete the task, review the certificates, select the certificate, and click **View and Update**.

    Recommended Action: You are redirected to **Infrastructure > SSL Dashboard > SSL Certificates - Expired**. Select the certificate and click **Update** or **Delete**. For more information, see How to update an installed certificate.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Expiring SSL Certificates** – Provides information about the SSL certificates that are about to expire.

  Recommended Action: Select this task to view tabs based on the total number of days before the expiry date. To complete the task, select the certificate from the tab, click **View and Update**. You are redirected to the relevant page in **Infrastructure > SSL Dashboard**. Select the certificate and click **Update**. For more information, see How to update an installed certificate.

- **Config Drifts** – Provides information about the configuration deviations (saved vs running diff and template vs running diff) in the NetScaler instances. Select this task to view the following tabs:

  - **Instances with unsaved configuration**: You can view instances that have the unsaved configuration. To complete the task, select the instance, click **View and Save configuration**.

    Recommended Action: You are redirected to **Infrastructure > Configuration > Configuration Audit > Audit Reports** and you can view the instances that have unsaved configurations. Click **Save Configuration** to complete this task. For more information, see the documentation.

  - **Instances with drifts from template**: You can view instances that have template deviations. To complete the task, select the instance, click **View and Run correct commands**.

    Recommended Action: You are redirected to **Infrastructure > Configuration > Configuration Audit > Audit Reports** and you can view the instances that have template deviations. Follow the documentation to complete the task.

- **Security Advisory** – Provides information about the CVEs that are impacting your NetScaler instances. Select this task to view the following tabs:

  - **Detected CVEs**: Displays the CVEs detected and the NetScaler instances impacting the CVEs. To complete this task, select a CVE, click **View and Remediate**.

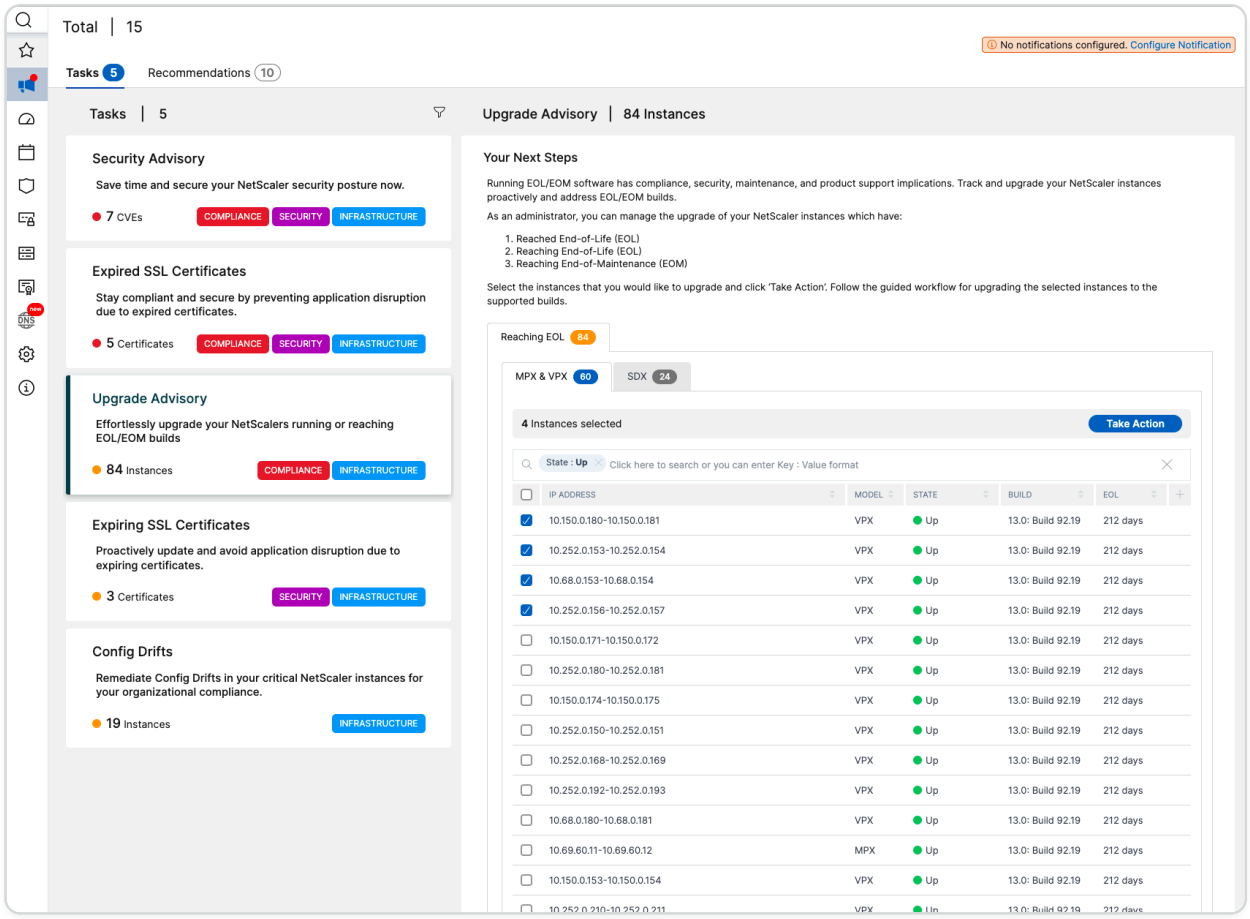
    Recommended Action: You are redirected to the **Security Advisory** page in **Infrastructure > Instance Advisory > Security Advisory**. Follow the documentation to complete the task.

  - **Affected Instances**: Displays the NetScaler instances that are affected with CVEs. To complete the task, select the instance, click **View and Remediate**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Recommended Action: You are redirected to the **Security Advisory** page in **Infrastructure > Instance Advisory > Security Advisory**. Follow the documentation to complete the task.

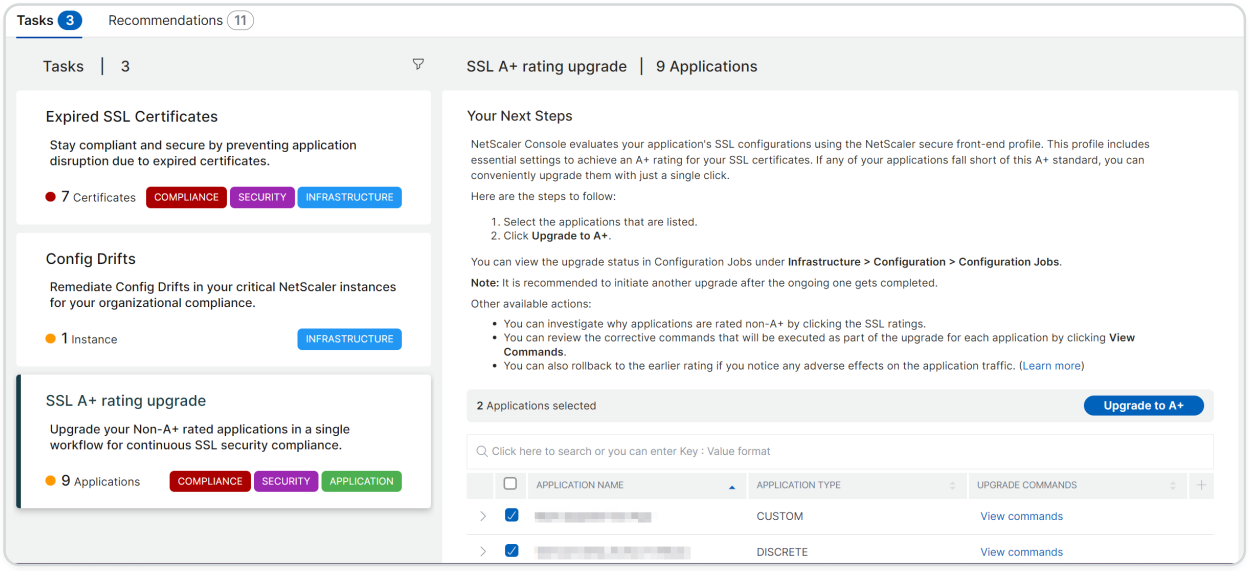
- **Upgrade Advisory**: Provides information about your NetScaler® instances that have already reached or about to reach End of Life (EOL) or End of Maintenance (EOM) within 90 days.



Recommended Action: Click **Take Action** and upgrade the instances to a recommended build.

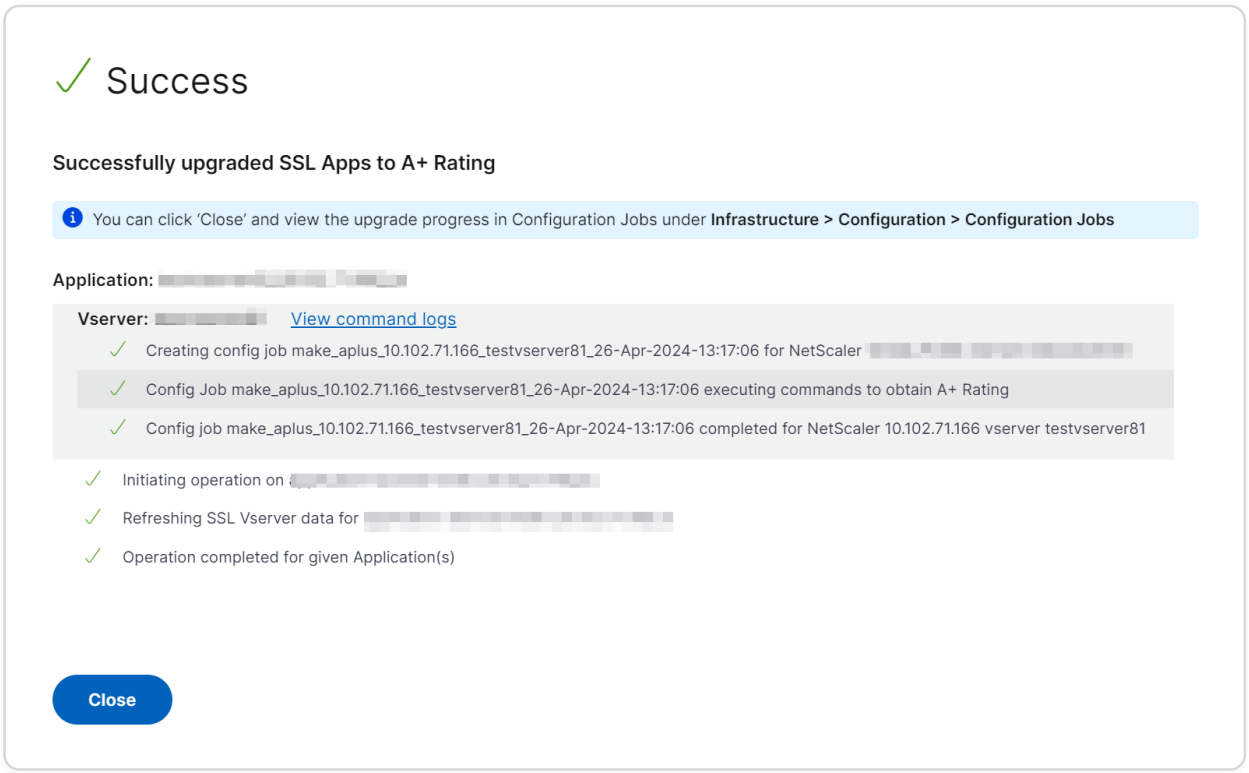
- **SSL A+ rating upgrade**: Provides information about your applications that are not compliant with an A+ rating.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Recommended Action: Select the applications from the list and click **Upgrade to A+**.

After the upgrade is successful, you can the following success message:



After the upgrade is completed, the application details are removed from the task.

Points to note:

- Depending upon the number of applications selected, the duration for the upgrade completion process might vary.
- After you initiate an upgrade process, it is recommended to initiate another upgrade process after the ongoing one gets completed.

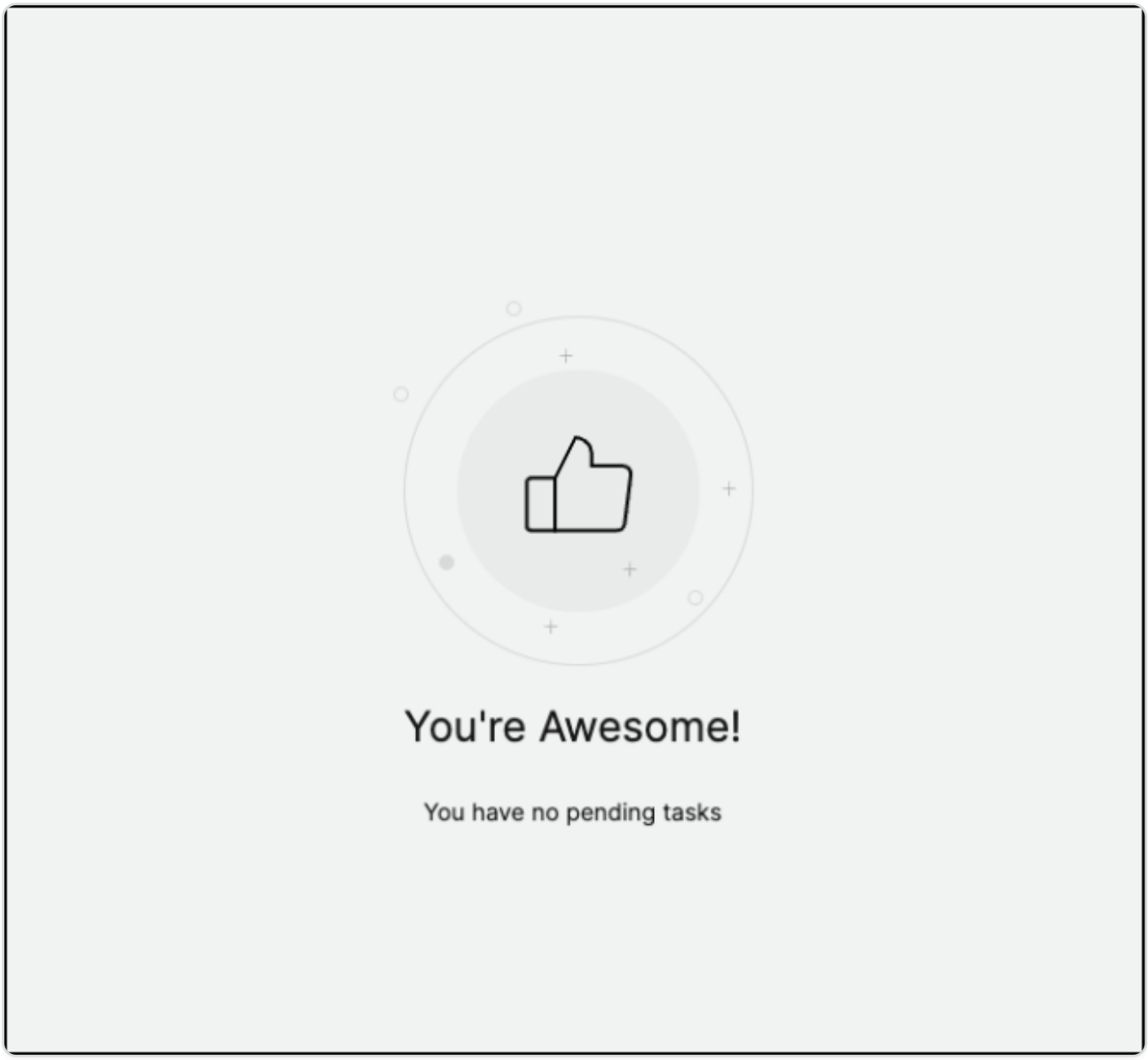
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You can also view the status for the upgrade process in **Infrastructure > Configuration > Configuration Jobs**.
- If the upgrade process is not successful, you can view the status in **Infrastructure > Configuration > Configuration Jobs**. You can again initiate the upgrade process from the task.
- If you do a bulk upgrade and if one or more applications fail to upgrade, you can view only those failed application details in the task. You can again initiate the upgrade process to complete.

NOTE:

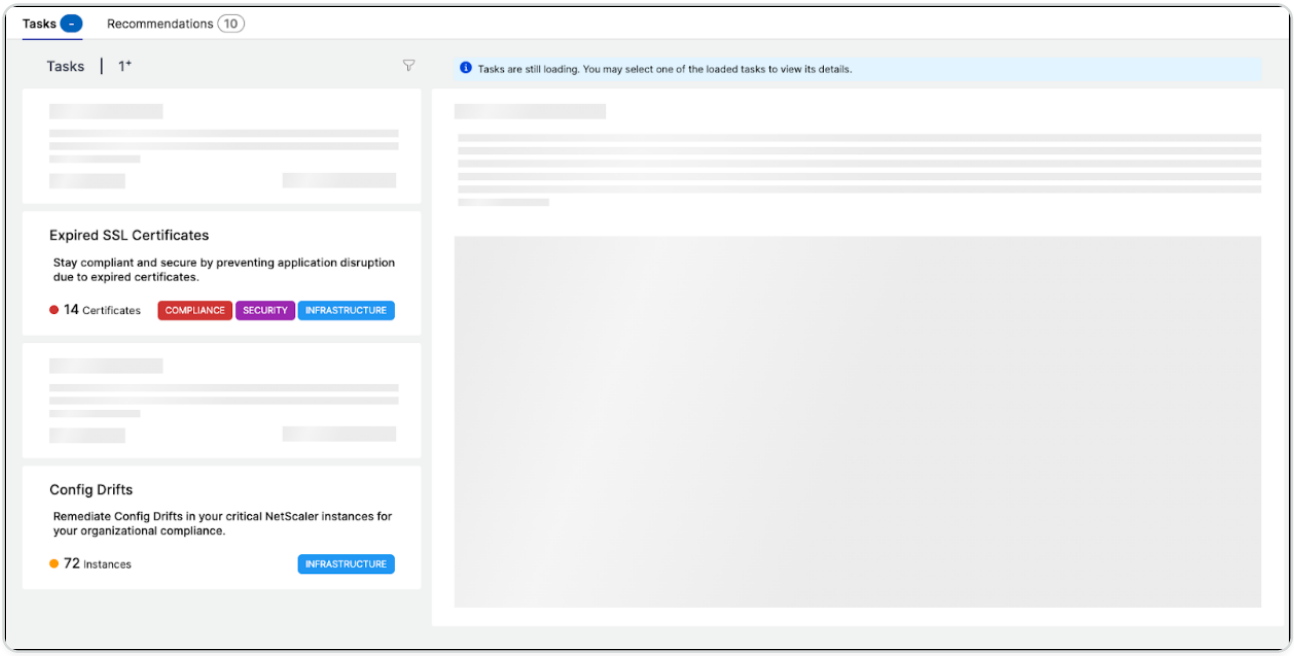
- You can view the following page if your NetScaler Console does not have any pending tasks:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- In some scenarios, the checks happen at all the instances and it might take additional time to load all the tasks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Recommendations

The following table describes the recommendations that you can view in the NetScaler Console GUI:

NOTE

For pooled licensing, you get recommendations based on your existing pooled licensing entitlements.

RECOMMENDATION NAME	WHEN THE TASK IS VISIBLE IN THE GUI?
Add a NetScaler instance	After you onboard to NetScaler Console and if no NetScaler instance is discovered.
Add an external agent to utilize the maximum features in NetScaler Console	If an external agent is not configured. You can get started with a built-in agent. However, an external agent is required to use all features such as analytics, pooled licensing, and so on.
Register a NetScaler from a built-in agent to an external agent	After you onboard to NetScaler Console using the Service Connect workflow, the NetScaler instances are onboarded using the built-in agent. You can register those NetScaler instances to an external agent to use all

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION NAME	WHEN THE TASK IS VISIBLE IN THE GUI?
	features such as analytics, pooled licensing, and so on.
Want to reallocate bandwidth on your NetScaler? It’s simple!	If the pooled licenses are allocated in the NetScaler GUI and those NetScaler instances are discovered in NetScaler Console, you can make the reallocation using NetScaler Console.
Enable Granular Role based access for your key enterprise users	If role-based access control (RBAC) is not yet configured in NetScaler Console.
Configure rules and never miss any critical events on your NetScaler instances	If a custom event rule is not configured yet.
Need to monitor multiple applications and their performance? Just create a Custom Application	If the custom app is not configured yet.
Notify and never miss critical events in your applications	If action policy is not configured for app score deviation, server processing time, client network latency, server network latency, or response time.
Avoid application outages and never miss expiring SSL certificates in an application	If no alerts or notifications configured for the expiring SSL certificates.
Security Advisory - Keep your NetScaler instances up-to-date with CVEs and mitigations	If the NetScaler instances have any CVE impact.
Configure an enterprise policy and monitor for any deviations	If the SSL enterprise settings are not changed or still in default.
Repeating tasks manually? Create Configuration Jobs and apply them to multiple NetScaler instances	If **Config Job** task is not configured yet.
Manage and monitor your instance score by selecting custom indicators of your choice.	If the default settings and thresholds in **Instance Score Settings** are not modified.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

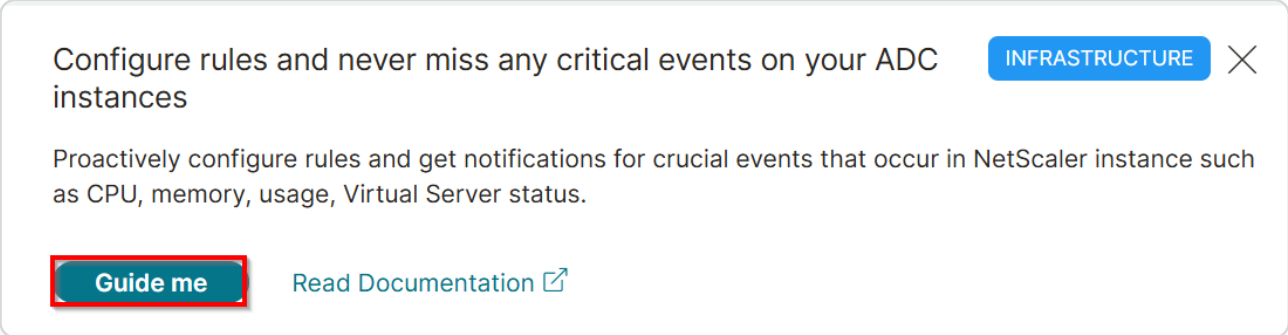
RECOMMENDATION NAME	WHEN THE TASK IS VISIBLE IN THE GUI?
Track your application score by selecting custom indicators of your choice	If the App Score components in the App Dashboard are used in default and no customization is made.
Add private IP blocks to visualize client requests in the Geo Map	If IP blocks are not configured. You can create IP Blocks for mapping and visualizing client requests on a Geo Map based on their private IPs/range.
Subscribe and export your AppSec violations to Splunk in realtime	If Splunk integration in NetScaler Console is not yet configured.
Customize the default threshold or create a new threshold for your Kubernetes services	If only default thresholds are used in service graph and no single or double threshold is applied to the services.
Proactively configure notification profiles and get notifications in your communication destinations	If a notification profile is not yet configured.
Schedule recurring exports and get notifications on the infrastructure details	If no export schedules configured yet in **Infrastructure > Instances**.
Having ServiceNow and looking to integrate with ADM?	If ServiceNow integration in NetScaler Console is not yet configured.
Automate SSL Certificate management using Venafi and ADM	If the Venafi server is not yet configured in NetScaler Console.
Renew your Pooled license before it expires.	If your existing license is about to expire in 30 days.
Get started with Pooled Licensing by allocating your purchased pooled bandwidth to NetScaler instances.	If you have not yet started allocating your pooled license entitlements.
Consider purchasing more pooled bandwidth capacity.	If you have utilized 90% or more of your pooled bandwidth entitlement.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RECOMMENDATION NAME	WHEN THE TASK IS VISIBLE IN THE GUI?
Your current pooled bandwidth entitlement is underutilized. Review and consider allocating more	If your pooled license allocation utilization is less than 70%.

How to use the Guide me workflow and complete the recommendation?

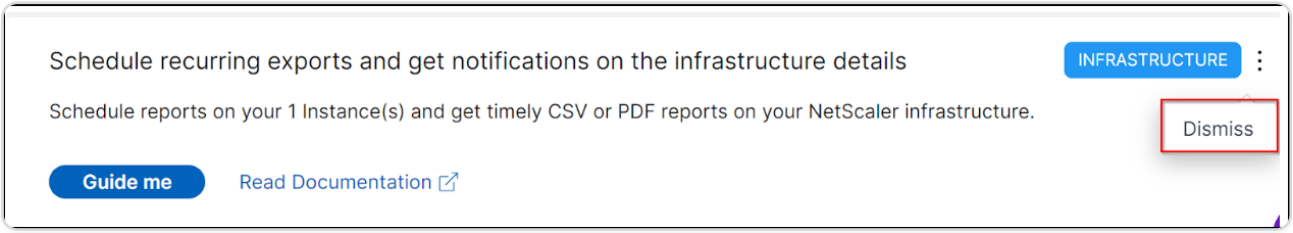
Consider that you want to configure rules for any event. Click **Guide me** for the following task:



After you click **Guide me**, you are redirected to **Infrastructure > Events > Rules**. Click **Add** to create a rule. For more information, see Create event rules.

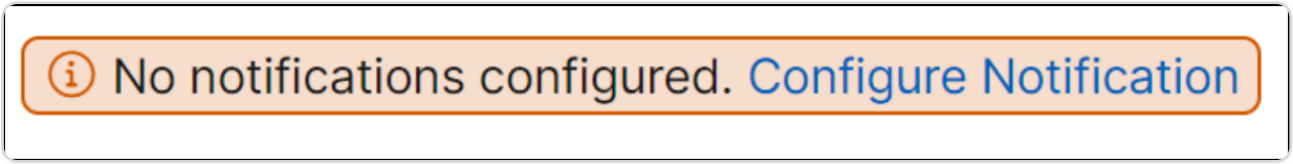
After you complete creating a rule, the recommendation is complete and it is moved to **Completed**.

Similarly, if you want to complete any recommendation later, you can select **Dismiss** from the list and it is moved to **Dismissed**.



Configure notifications

You can configure and get notifications whenever NetScaler Console identifies any open tasks that require your immediate action. If you have not configured notifications, you can click **Configure Notification** from the top-right corner.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

In the **Notifications** page, you can configure profiles for **Email** and **Slack**, and then click **Save** to receive notifications. For each notification type, the NetScaler Console GUI displays the configured distribution list or profile. The NetScaler Console sends notifications to the selected distribution list or profile.

FAQs

1. **Guide me** does not show tool-tip and only does redirection of UI? What should I do to fix this?

   This issue can happen if your firewall is blocking Pendo FQDN. Refer to Enable Pendo for your enterprise and ensure that the FQDN is allowed in the firewall. Allowing Pendo FQDN enables the **Guide me** to show tool tips. You can experience the **Guide me** workflow at its best only when Pendo is available.

2. Why type of recommendations is present for the administrators?

   Currently, the recommendations are specific to deployments that help the admins more on configurations and setup tasks for making the deployment efficient. It also enables better product discovery and admins can know what a task does and how it can help without any prior knowledge or knowing if the feature exists in NetScaler Console or not.

3. What happens if I dismiss any recommendation?

   The recommendations that you dismiss are moved to **Dismissed**. You can complete these recommendations later.

4. Does the recommendation go to **Completed** if I start a guide me and leave it in the middle?

   No, the recommendation is not completed unless the action is saved or completed.

5. Can I perform search or filtering?

   Yes! You can use the search bar or narrow down to specific tasks by selecting the category from the list.

6. Will I get tasks to take actions on dynamic events?

   Yes! Currently you can view a total of 4 actionable tasks. For more information, see Tasks.

7. Will all the actionable tasks and 20+ recommendations show up even if I do not have NetScaler instances added in NetScaler Console?

   No. You must have both NetScaler instance and virtual servers available in NetScaler Console to show all the tasks and recommendations.

8. How often will the tasks refresh?

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When you click **Tasks** from the left navigation pane, they are refreshed and available at the latest status. The details are fetched and updated.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

A unified dashboard to view instance key metric details

In NetScaler Console, you can view various insights about the usage and performance of applications, NetScaler infrastructure, security (Bot and WAF) violations, and so on. As an administrator, you might have to navigate to various options in the NetScaler Console GUI to view multiple insights. For example, to check the virtual servers (applications) and NetScaler instance insights:

- You must first navigate to **Applications > Dashboard** to view insights for applications.
- Then you must navigate to **Infrastructure > Infrastructure Analytics** to view insights for NetScaler instances.

For a better monitoring experience, it is necessary for you to have a privilege that contains an overview of all the required insights. Navigate to **Overview > Dashboard** to visualize a single-pane dashboard with an overview of the key metrics details based on the following categories:

- Applications
- NetScaler Infrastructure
- Application security
- Gateway
- API analytics

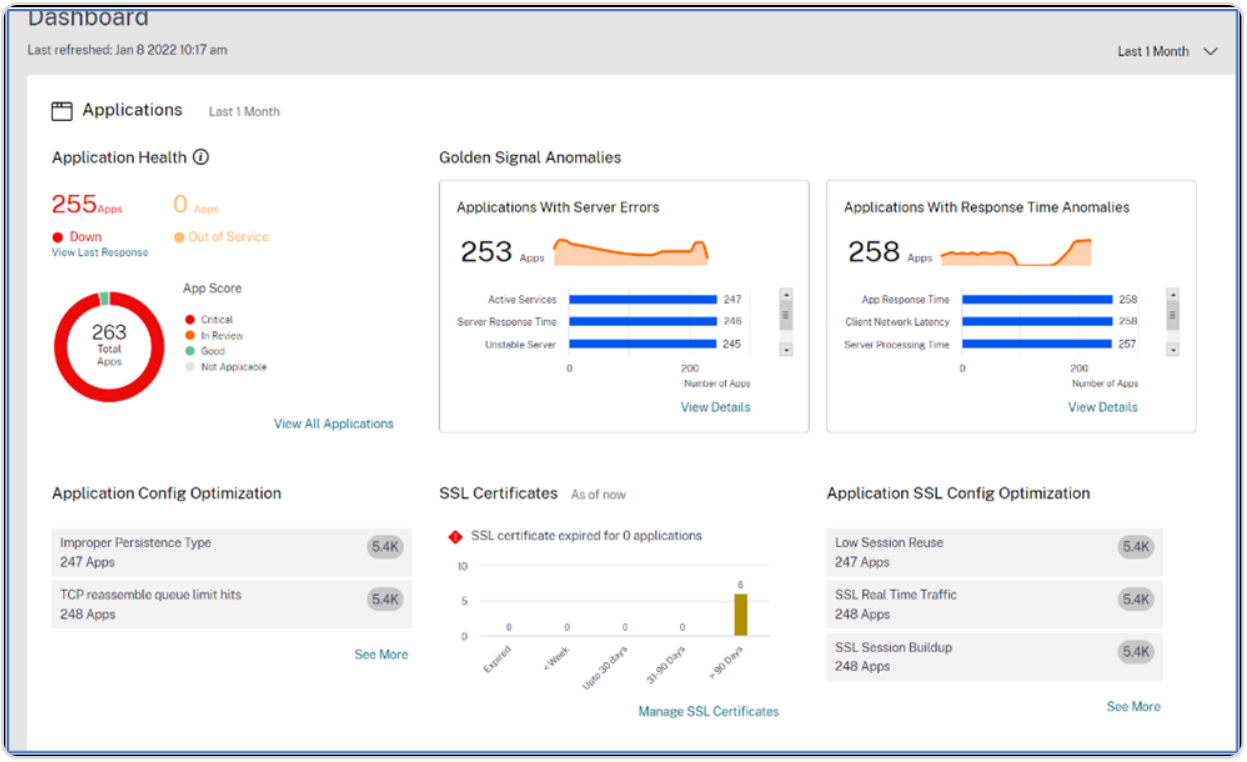
Applications

Under **Applications**, you can view:

- **Application Health** – Provides an overview of applications that are in **Down** and **Out-of-Service**, and based on their status such as **Critical**, **In Review**, **Good**, and **Not Applicable**. Click **View All Applications** to view details in App Dashboard.
- **Golden Signal Anomalies** – Provides an overview of applications that have server errors and response time anomalies. Click **View Details** for more information.
- **Application Config Optimization** – Provides an overview of total applications that have performance issues. Click **See More** to view issue details in app dashboard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **SSL Certificates** – Provides an overview of SSL certificates along with their validity. Click **Manage SSL Certificates** to view more information in SSL dashboard.
- **Application SSL Config Optimization** – Provides an overview of total applications that have SSL related issues. Click **See More** to view issue details.



NetScaler Infrastructure

Under **NetScaler Infrastructure**, you can view the following NetScaler instance related key metrics:

- **NetScaler Instance Health** – Provides an overview of total NetScaler instances based on the instance score.
- **NetScaler Instances impacted by CVEs** – Provides an overview of total NetScaler instances that are impacted with Common Vulnerabilities and Exposures (CVEs). For more information, see Security Advisory.
- **NetScaler Instance Issues** – Provides an overview of NetScaler instance issues depending upon the issue category. For more information, see Infrastructure Analytics.
- **NetScaler Instance Upgrade Summary** – Provides an overview of total NetScaler instances that are not on the latest build. Click **View NetScaler Instances Dashboard** for more information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Application Security

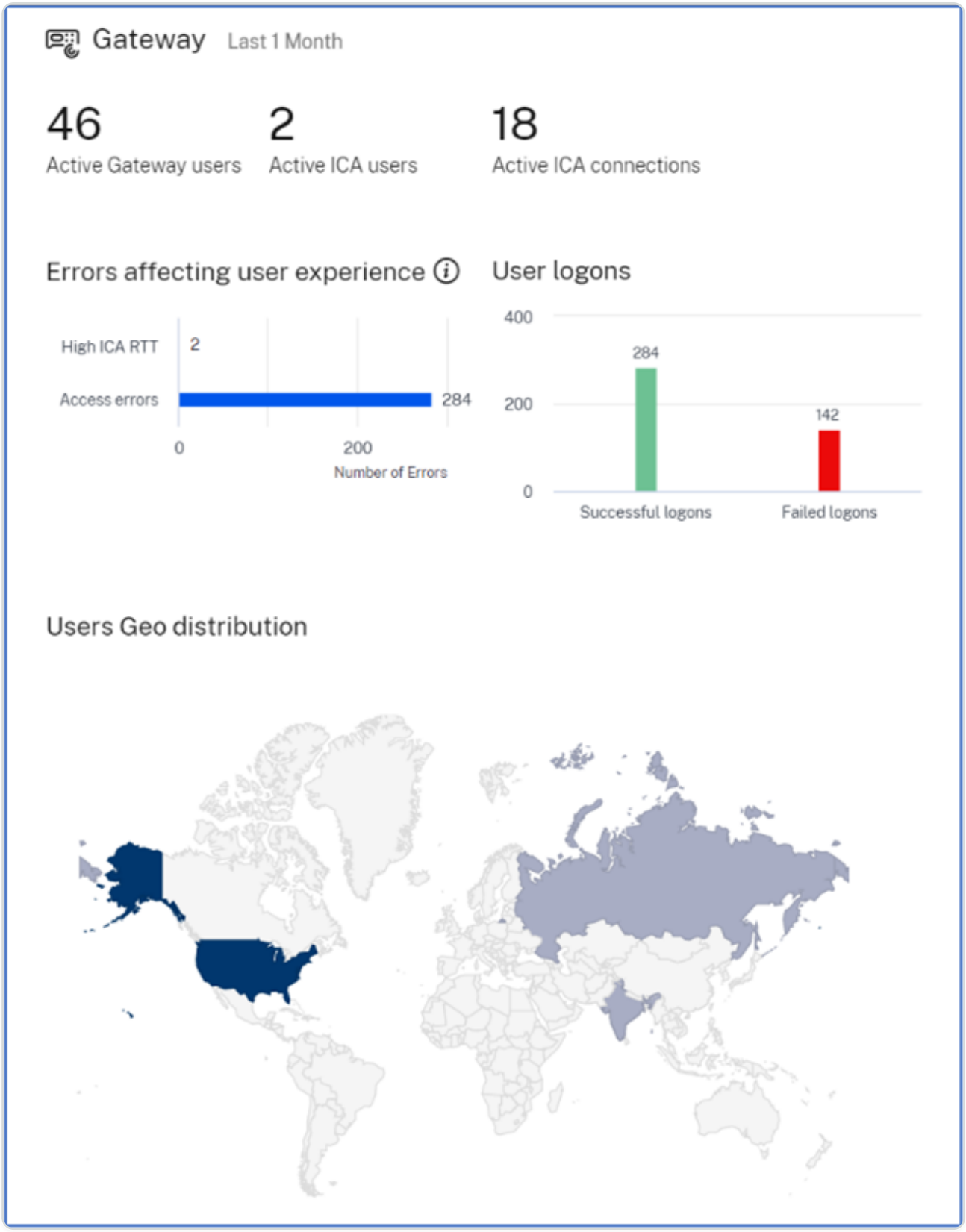
Provides an overview of total affected applications and total violations (Bot and WAF) reported for the selected duration. Click **View Security Dashboard** to view the security and bot violation details.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gateway

Provides an overview of total active gateway users, total active ICA® users, and total active ICA connections. You can also view errors, user logon details, and a geo map that provides details on the user locations.

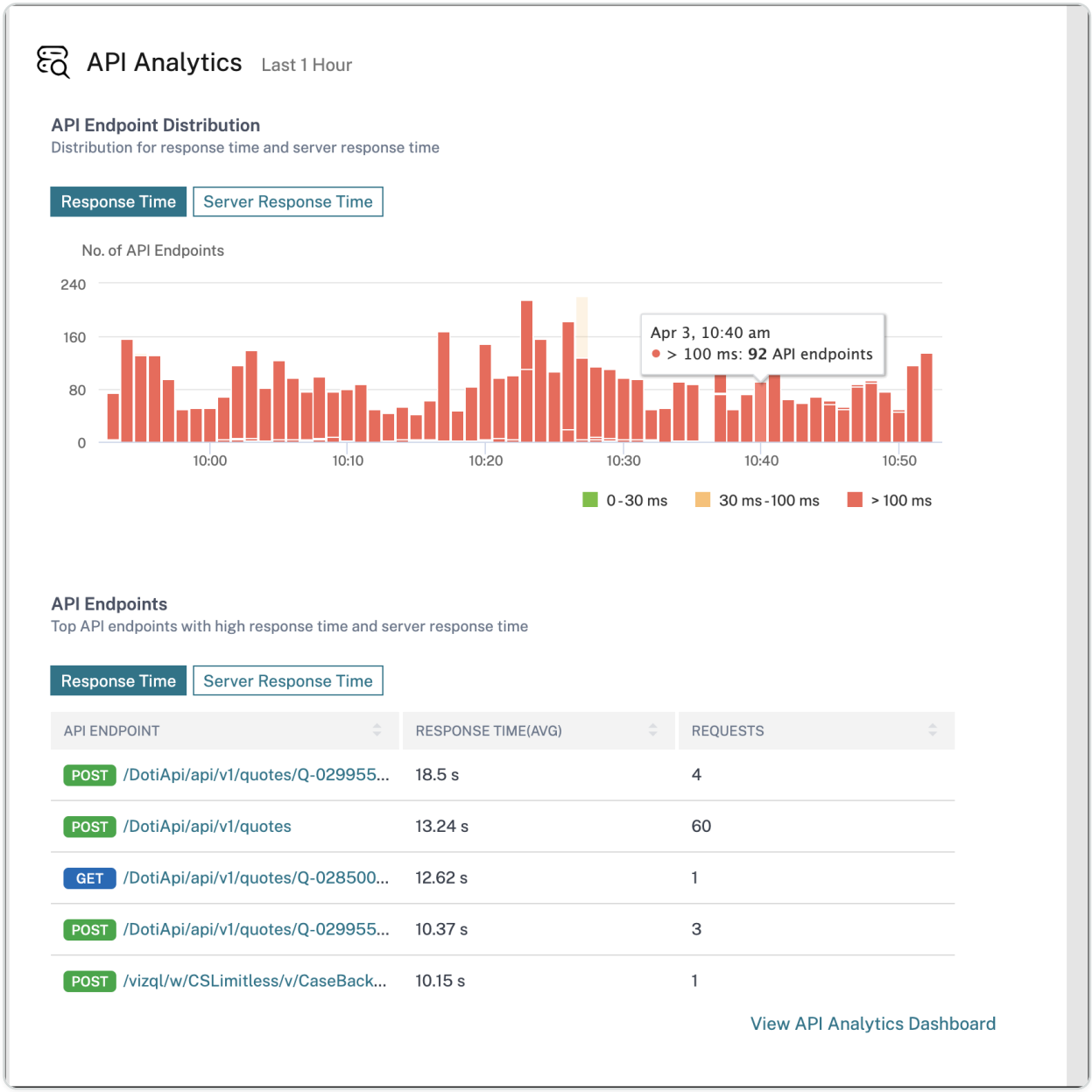


© 1997–2026 Citrix Systems, Inc. All rights reserved.

API Analytics

Provides an overview of the performance and usage of the API endpoints configured through NetScaler Console. You can view the:

- Distribution of application and server response time for API endpoints.
- Endpoints with high application and server response time.



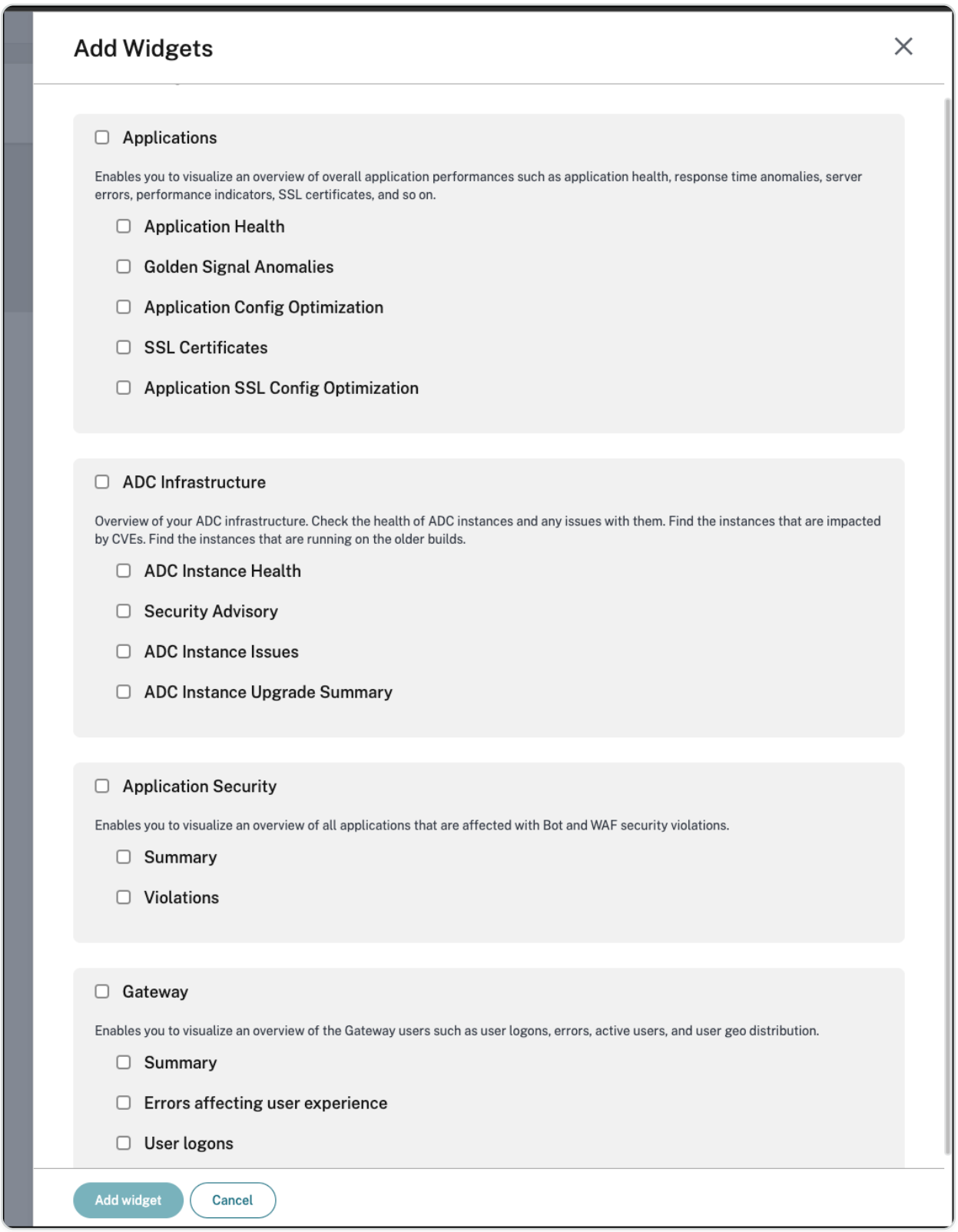
Customize dashboard

You can use the **Edit dashboard** option and customize the dashboard view based on your choice. Using the **Edit dashboard** option, you can:

- Drag widgets

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Remove the whole widget (Applications, NetScaler Infrastructure, Gateway, or Application Security).
- Remove the smaller widgets present under each widget.
- Click **Add widget** and select the required key metrics that you want to view under each widget.



- Reset to default

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Reset to last saved

After making changes, click **Save**.

NOTE

- By default, all widgets are displayed. If you customize the dashboard, save the changes, and again use the **Reset to default** option, all widgets get added to the dashboard.
- The **Reset to last saved** option loads the previously saved configuration.

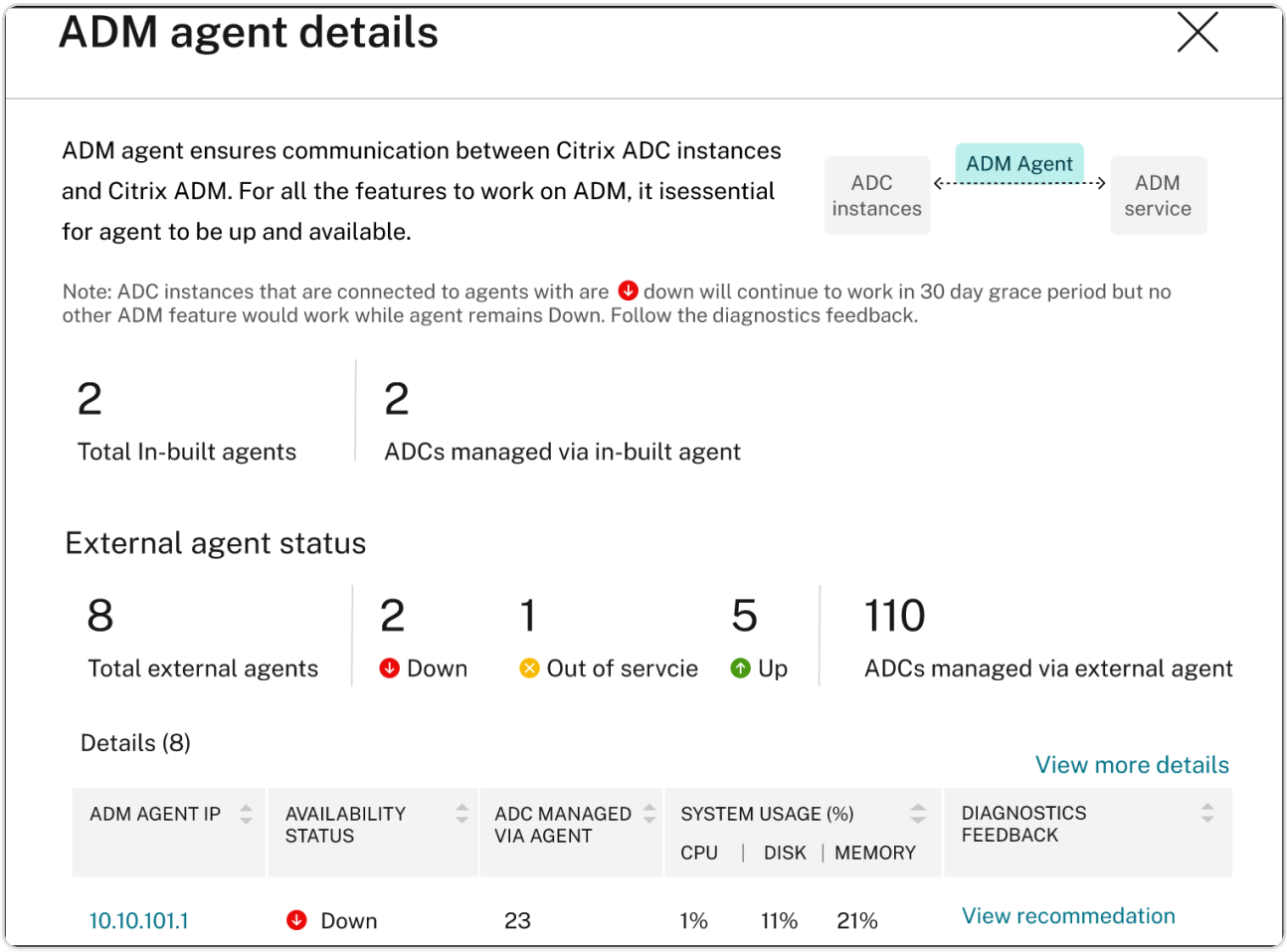
View agent details

In the unified dashboard, you can visualize an overview of agent details. In **Overview > Dashboard**, next to the **Agent Status**, you can view the following status that enables you to analyze the overall agent availability:

- **All available**. Indicates all agents are up and running.
- **All unavailable**. Indicates all agents are down and not accessible.
- **unavailable**. Indicates a few agents are down and not accessible.
- **All out of service**. Indicates all agents are in out of service.
- **out of service**. Indicates a few agents are in out of service.
- **External agent not found**. Indicates no agent (through any hypervisors) is configured.

Click **View Details** to visualize an overview of agent details such as total in-built agents, total external agents, agent IP, status, system usage, diagnostic checks, and so on.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Create and apply filters

You can apply filters and view insights only for the selected instances or applications in the following:

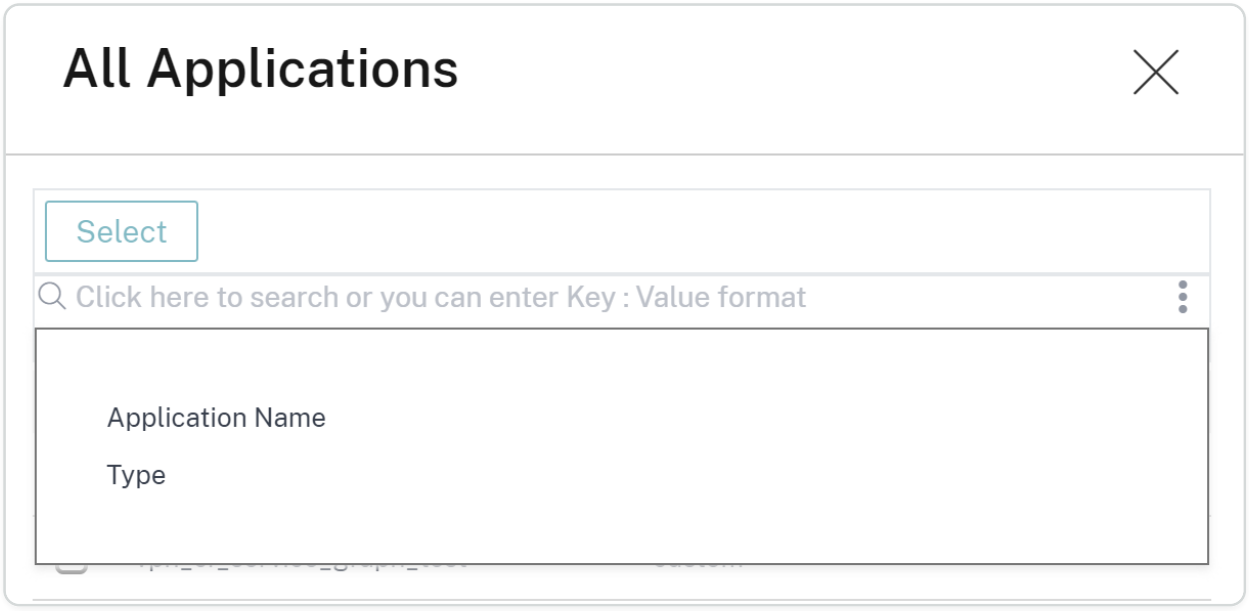
- Applications
- NetScaler Infrastructure
- Application Security

By default, all applications are selected. You can create a customized filer from the dashboard by clicking the filters icon available in the tile.

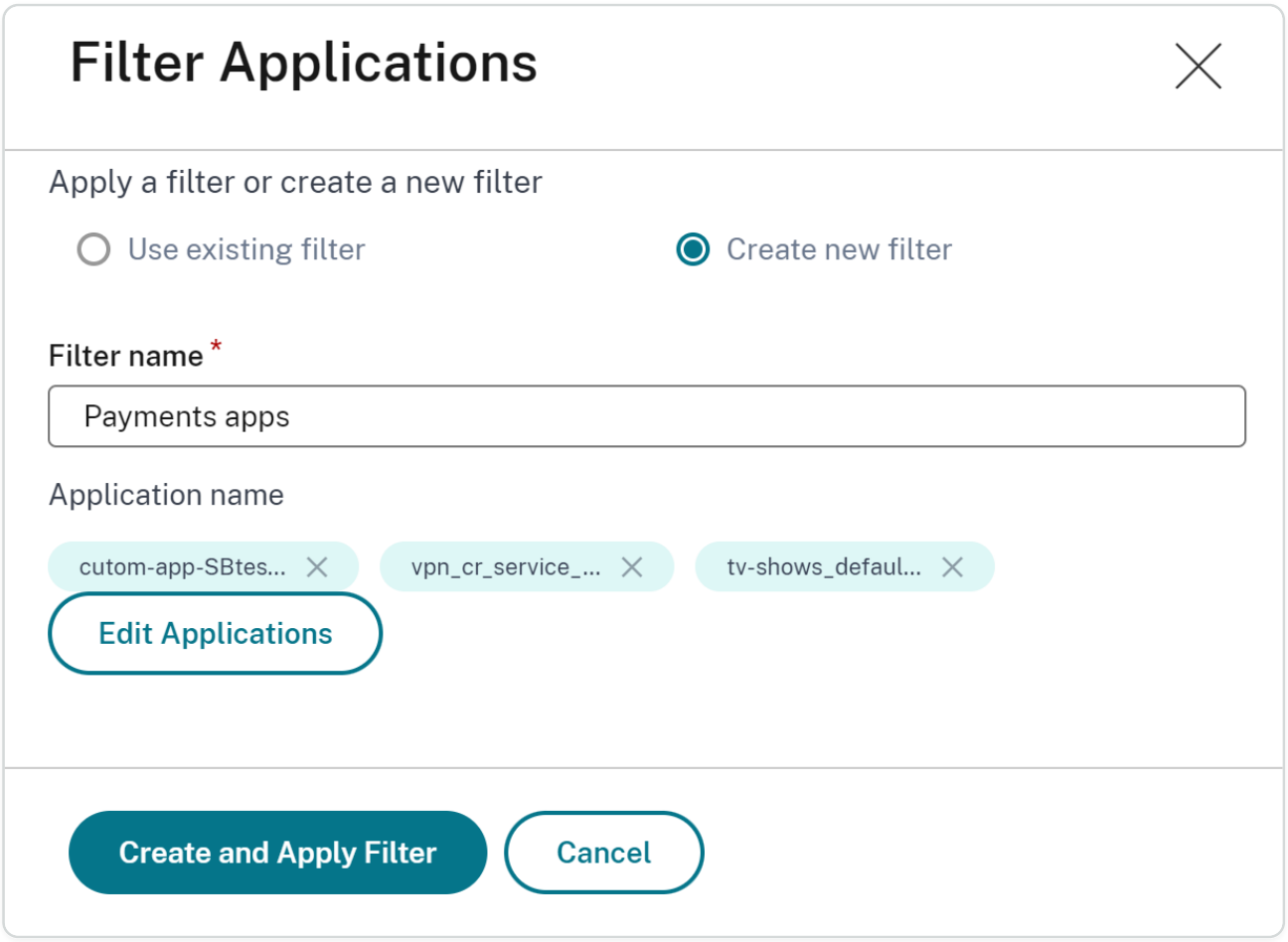
In the **Filter Applications** window:

1. Select **Create new filter**.
2. Provide a filter name based on your choice.
3. Click **Select Applications** and add all the required applications for the filter. When you select applications, you can also use the filters (**Application Name** and **Type**) and then select applications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

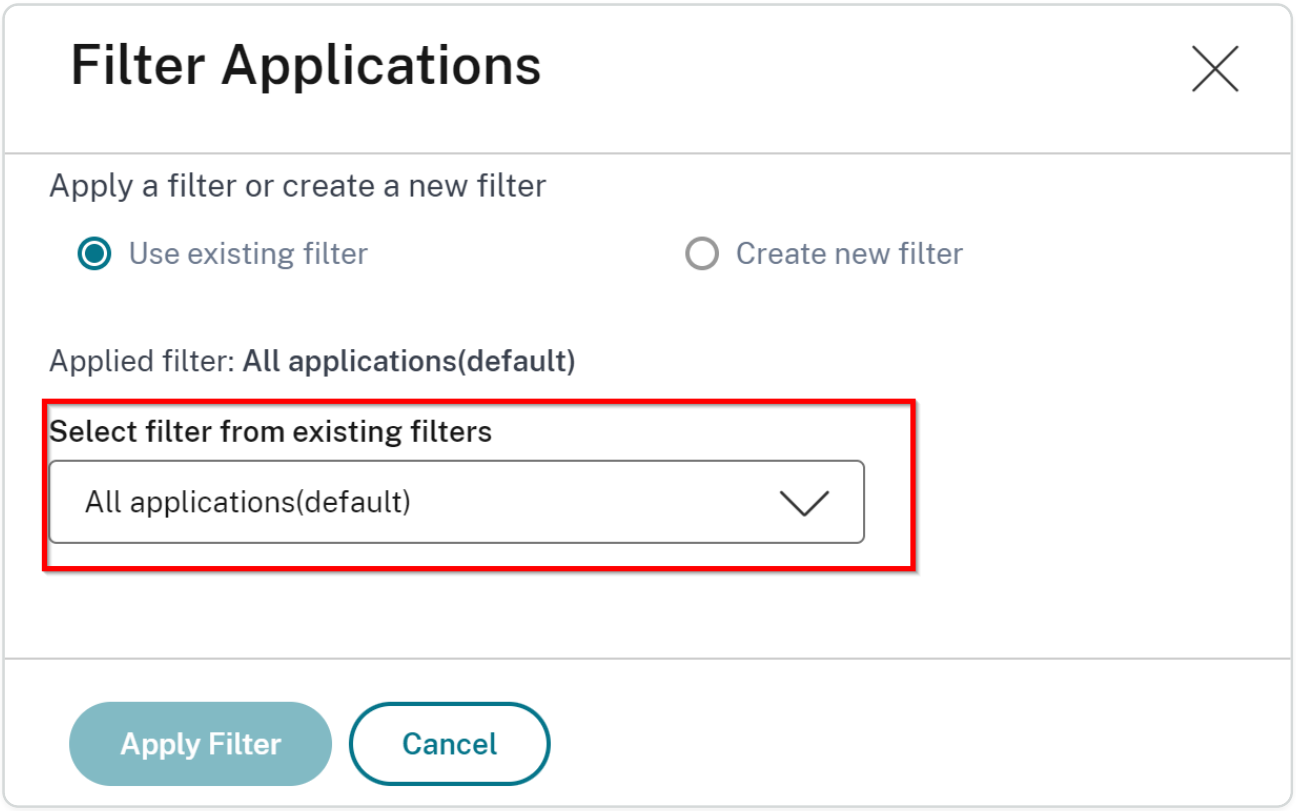


4. Click **Create and Apply filter**.



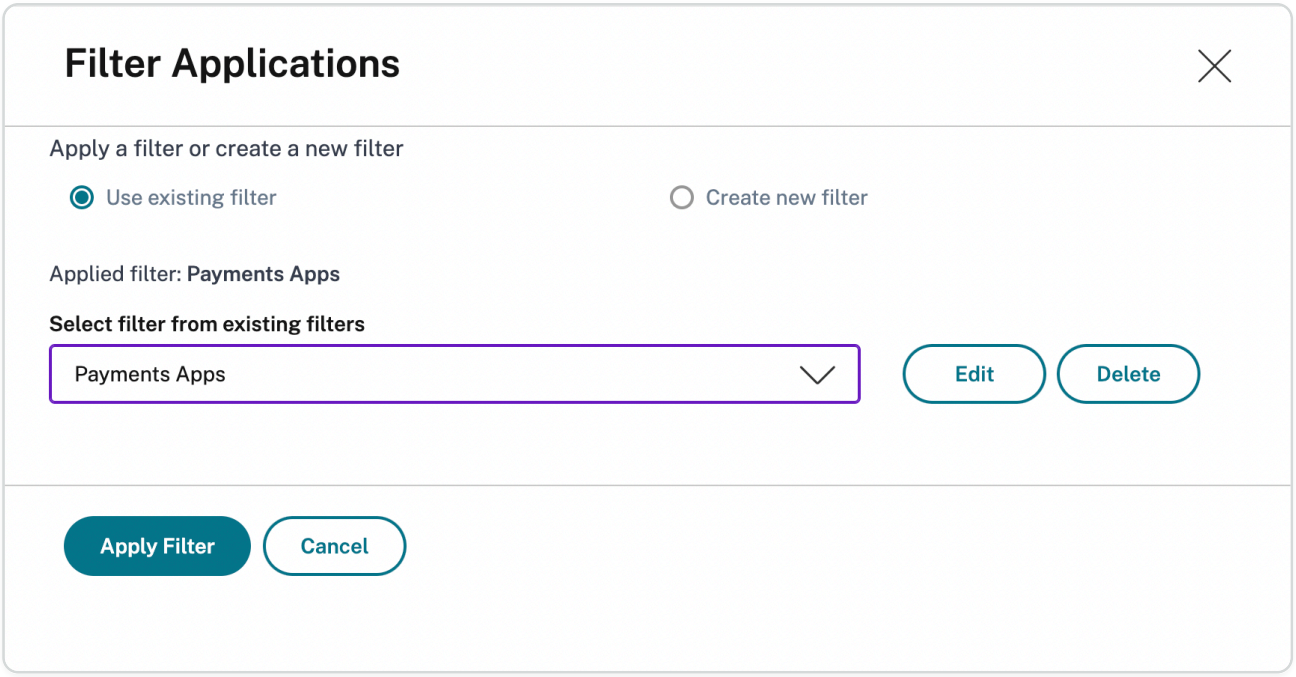
The filter is now created and applied. You can create more filters by following the same procedure. After you create filters, you can select and apply filters through the **Select filter from existing filters** list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Edit filters

You can edit a filter by selecting the filter from the list and clicking **Edit**. Using the edit option, you can add or remove applications and then update the filter.



To delete a filter, select the filter from the list and click **Delete**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

When you create a filter with applications and if one of the applications is deleted in the app dashboard, the application details are removed immediately from the unified dashboard.

Create custom dashboards to view instance key metric details

Similar to the unified dashboard (**Overview > Dashboard**), you can view instance metric details based on your choice by creating custom dashboards. You can create up to 30 dashboards by using a unique name for each dashboard. As an administrator, this enhancement enables you to create multiple dashboards and monitor only the required instance insights.

To get started, consider that you want to monitor the key metrics for **Applications** and **Application Security**:

1. Navigate to **Overview > Custom Dashboard**.
2. Click **+** to create a new dashboard.

   In the **Create Custom Dashboard** page:

   a. **Custom Dashboard Name** - Specify a unique name for the dashboard.

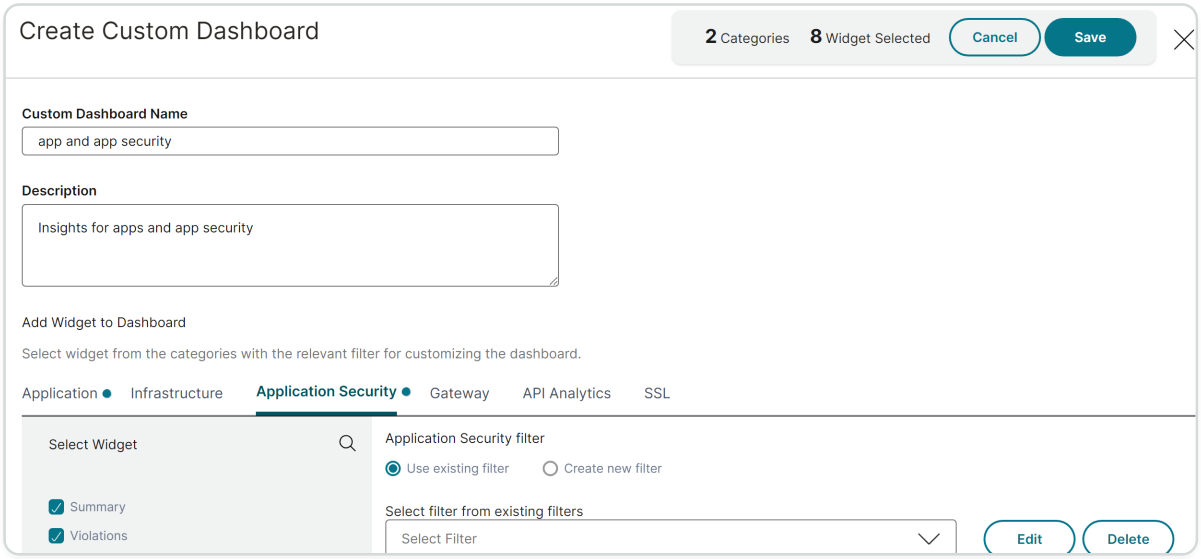
   b. **Description** - Provide a brief description to have additional details.

   c. **Add Widget to Dashboard** - In this example, the requirement is to add widgets for applications and application security. Select the widgets that you want to monitor from **Application** and **Application Security** categories.

   d. **Application filter** - By default, the filter is applied to all applications. You can also create a filter and select only specific applications. For more information, see Create and apply filters.

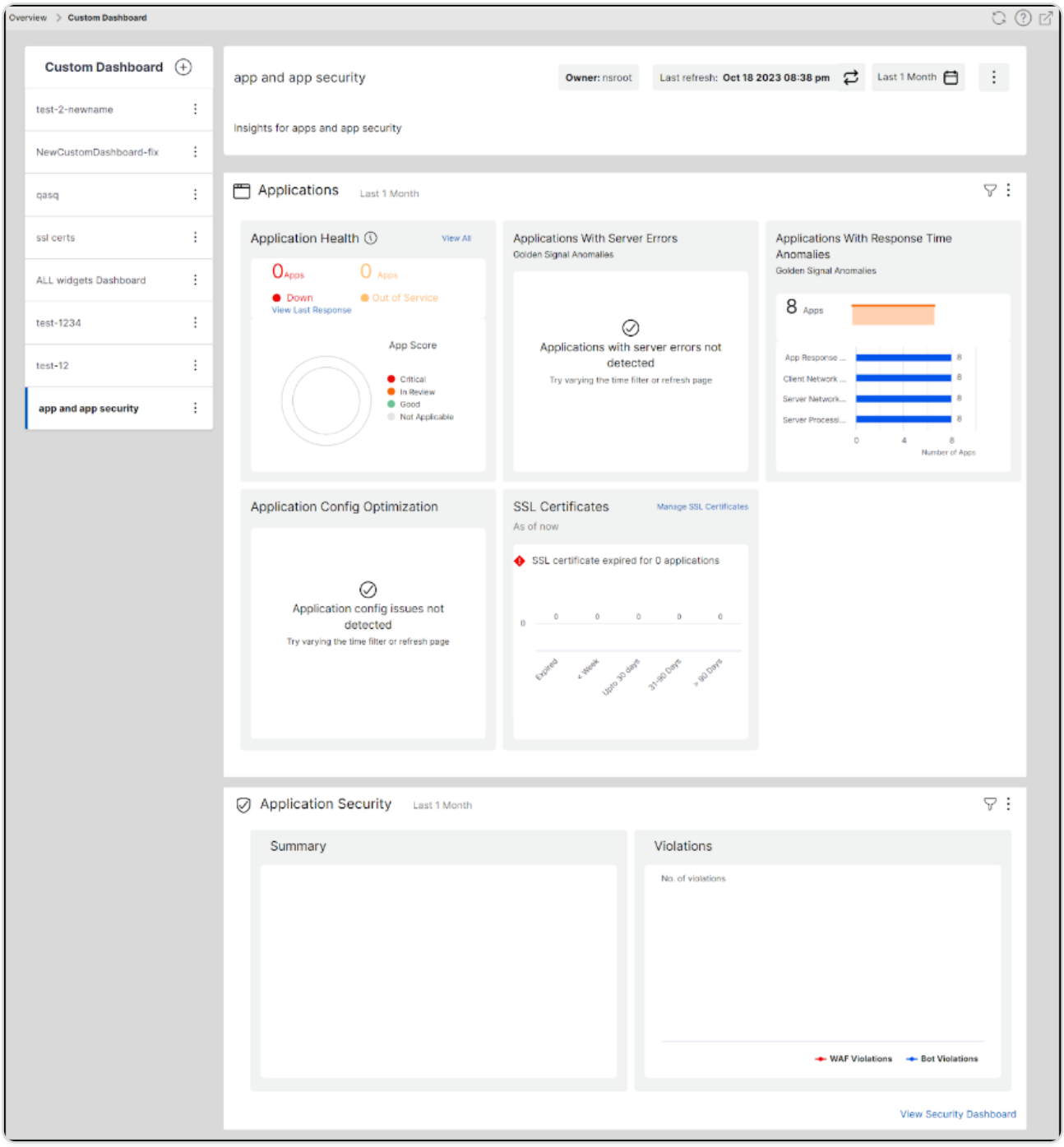
   e. Click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The dashboard is successfully created. Similarly, you can create up to 20 dashboards and select categories based on your choice by specifying a unique name for each dashboard.

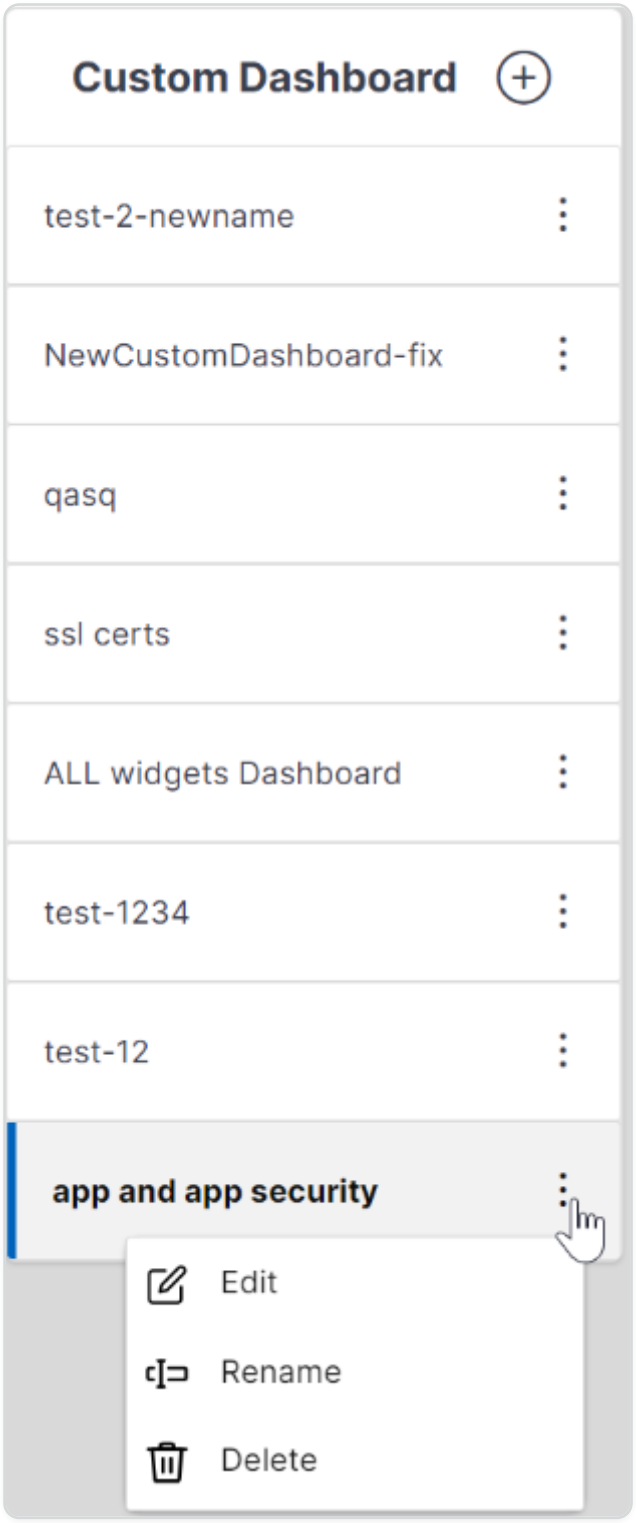
© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can use the following options after you create a custom dashboard:

- **Edit**: You can edit the dashboard by adding more widgets or removing widgets, applying filters, and so on.
- **Rename**: You can change the dashboard name.
- **Delete**: You can delete the dashboard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



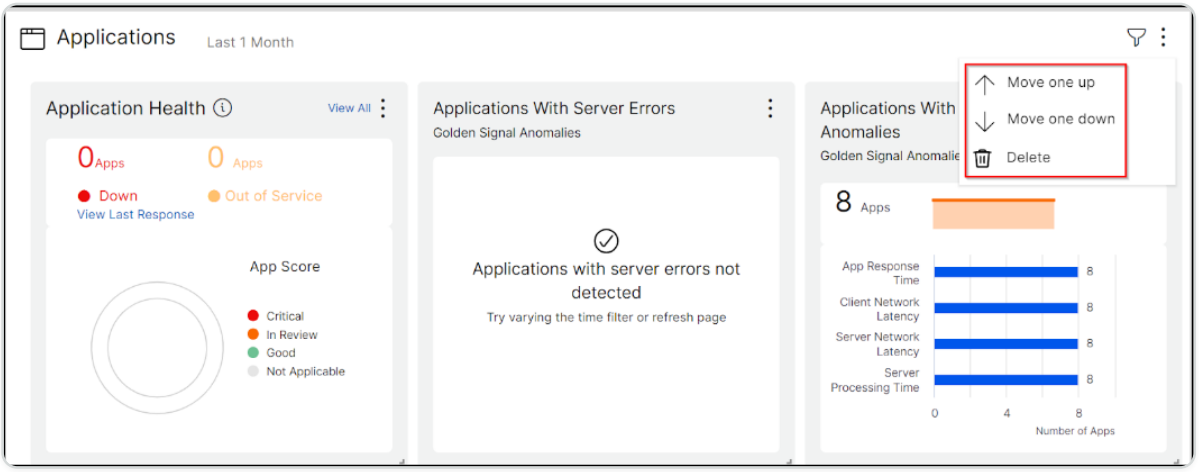
More options in the dashboard

In the custom dashboard that you have created, you can use the following options:

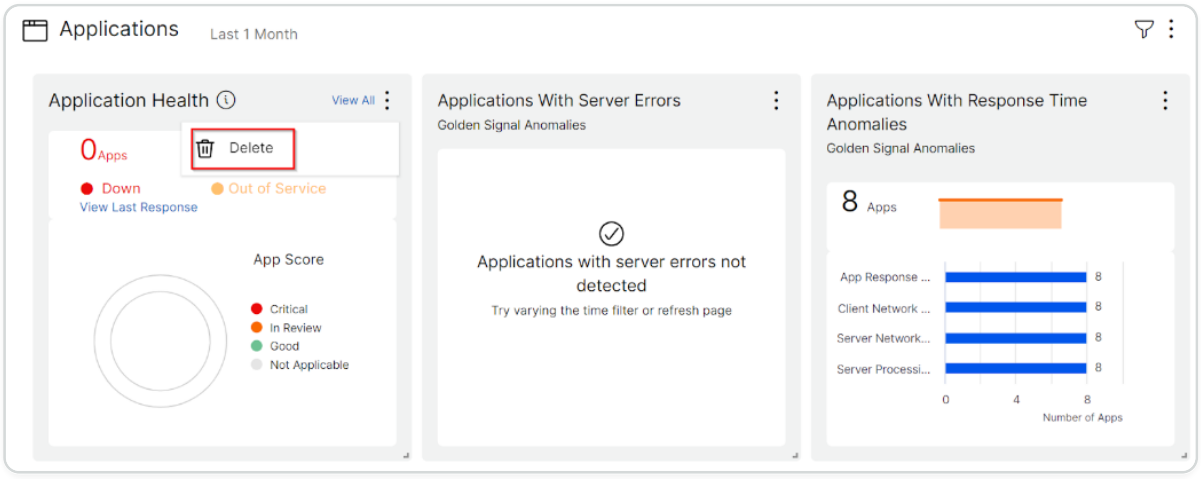


© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Edit Configuration**: You can also use this option to edit the dashboard by adding more widgets or removing widgets, applying filters, and so on.
- **Edit Layout**: You can use this option to have additional customization to the dashboard.
  - You can select to move up, down, or delete.

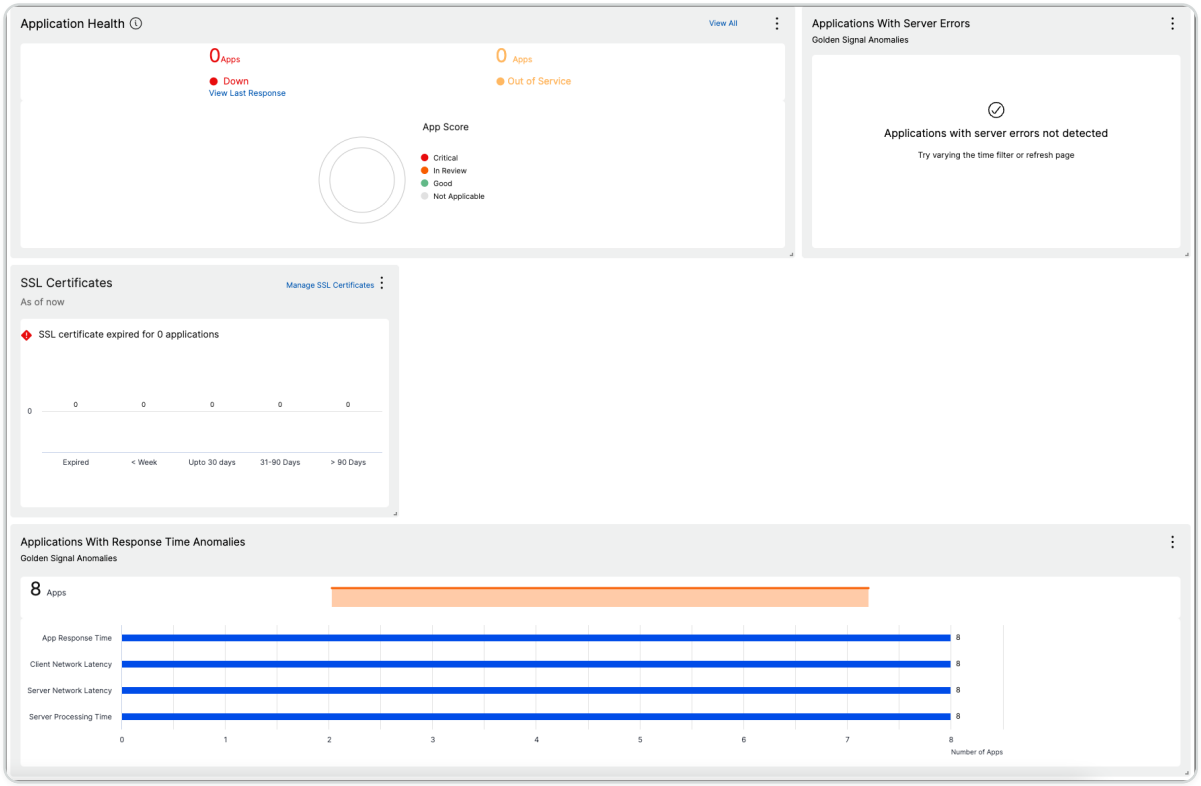


  - In the Widgets, you can delete any widget by selecting the Delete option.



  - Drag to place the widgets wherever you want.
  - Increase or decrease the widget size to have a better visibility for certain insights.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



After you make changes, click **Save** to see the updated dashboard.

Share dashboard to other users

You can share the dashboard to other users. Select an existing dashboard and click **Share**. Type the user name and click **Invite** to share the dashboard. The assigned user can view the dashboard in read-only mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

API Security

APIs, or Application Programming Interfaces, are sets of rules, protocols, and tools that allow different software applications or systems to communicate with each other. APIs play an important role in protecting sensitive data by enforcing access controls, authentication, and encryption, ensuring that only authorized entities can access and transmit confidential information securely.

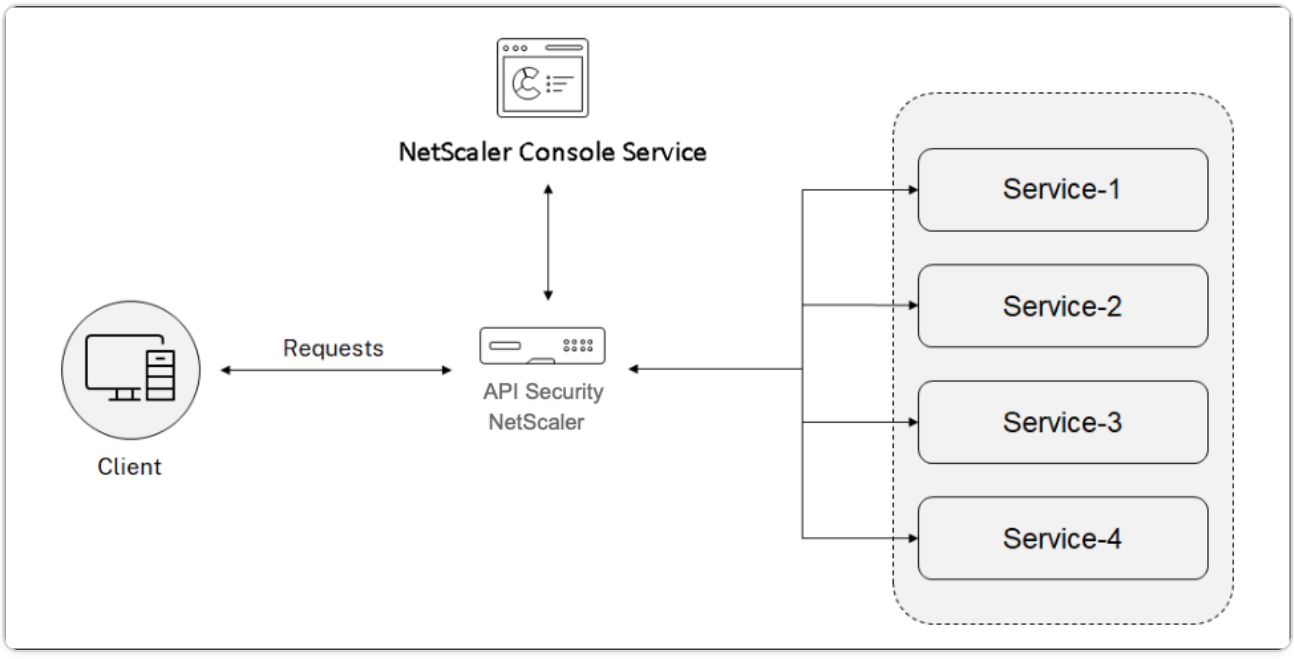
APIs work as the backend framework for mobile and web applications. Therefore, it is critical to protect the sensitive data they transfer. API security refers to the practice of preventing or mitigating attacks on APIs.

In API security, a gateway acts as the entry point for all requests to your API endpoints. And, ensures secure and reliable access to all API endpoints and microservices in your system.

To secure your APIs, do the following steps:

- Create or upload an API definition
- Deploy an API instance
- Add policies to an API deployment

The following image describes how the API Security in NetScaler Console receives the client request and sends the response from the back-end API services:



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

In NetScaler Console, this feature is available for the users who have Premium licenses.

Benefits of API Security

The API Security provides you the following benefits:

- **Secures your API endpoints**: The API Security adds a security layer and it protects your API endpoints and back-end API servers from the attacks such as:
  - Buffer Overflow
  - SQL injection
  - Cross-site scripting
  - Denial of Service (Dos)
- **Monitors and improves the API performance**: The API Security provides services such as SSL offloading, Authentication, Authorization, Rate limiting, and more. These services increase the API performance and its availability.

  The API analytics provide you the visibility to your API performance metrics and threats to your API endpoints. For more information, see View API analytics.
- **Manages the API traffic**: The API Security abstracts the complexity of your back-end API infrastructure.
- **Discovers API endpoints**: The API Security discovers the API endpoints that are in your organization and adds to the **API Discovery** page.

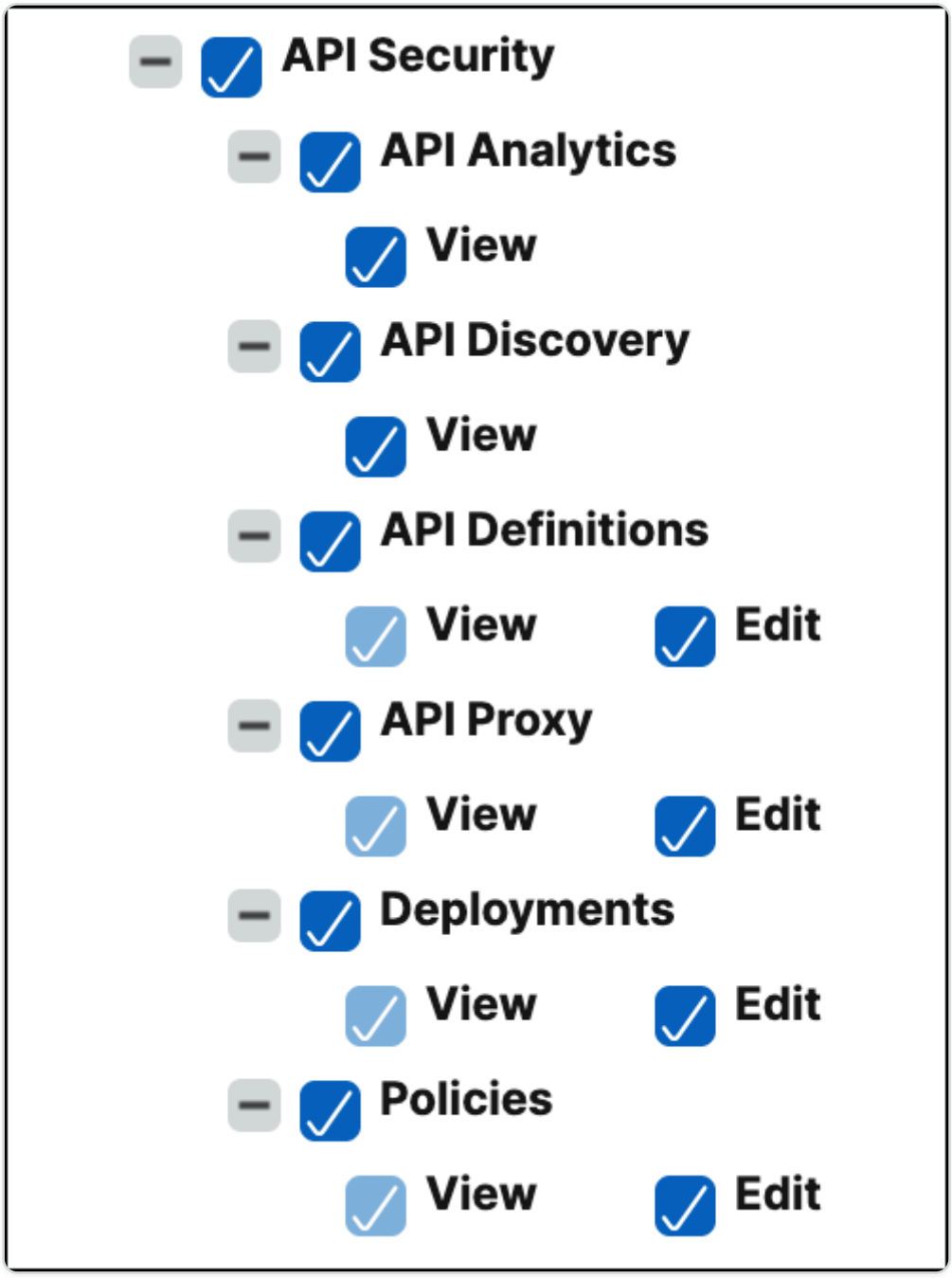
Grant API Security configuration and management permissions

As an administrator, you can create an access policy to grant user permissions for API Security configuration and management. The user permissions can be view, add, edit, and delete. Do the following to grant permissions:

1. Navigate to **Settings > User & Roles > Access policies**.
2. Click **Add**.
3. In **Create Access Policies**, specify a policy Name and the description.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. In the **Permissions** field, expand **Applications** and then **API Security**.
5. Select the required **API Security** pages. Then, select the permissions that you want to grant.



IMPORTANT:

Ensure to grant permissions for the features that are necessary to use an API Security. For example, if you grant user access to the **Deployments** page, the following features also require user access:

- StyleBooks

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- IPAM
- Load Balancing (Under **Network Functions**)
- Content Switching (Under **Network Functions**)
- Device API Proxy (Under **API**)

For more information about access policies, see Configure access policies on NetScaler Console.

Create or upload an API definition

An API definition is a document that describes an API using OpenAPI Specification standards. This definition can contain API resource paths and methods to operate them. You can add API definitions to NetScaler Console then deploy them to an API gateway (NetScaler).

You can create API definitions in one of the following ways:

- Upload Swagger OAS specification file
- Create your own API definition

NOTE:

Currently, NetScaler Console supports parsing OAS specification files that use **Swagger 2.0** or **openapi 3.0.1**.

Upload the OAS specification

You can upload the OAS specification to the NetScaler Console GUI.

1. Navigate to **Security > API Security > API Definitions**.
2. Click **Add**.
3. Select **Upload OAS Specification**.

   NOTE:

   Ensure that the OAS Specification file is in YAML or JSON format. And, this file must not contain external references.

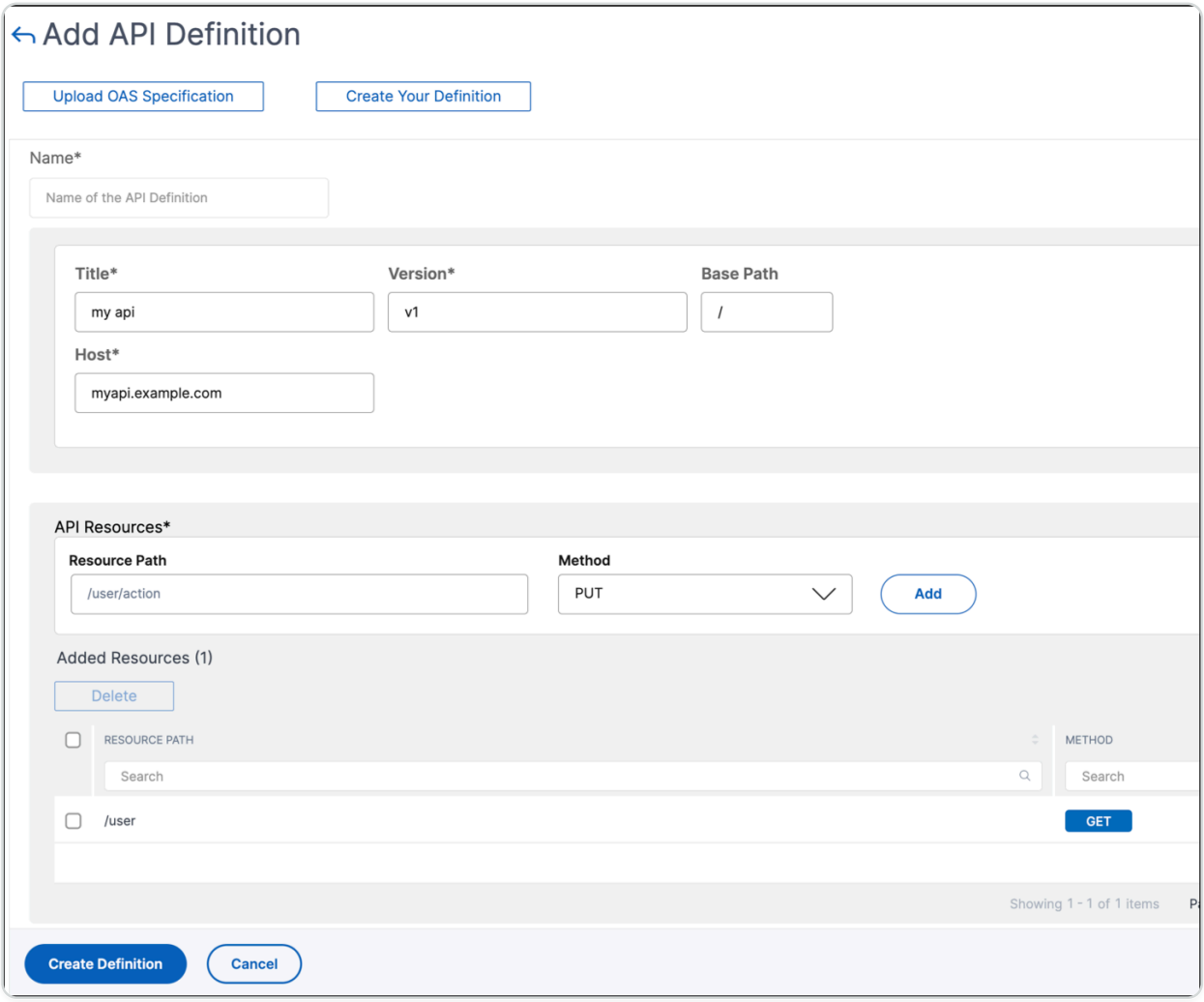
4. Browse an OAS specification from your local computer and upload to NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create an API definition

You can create your own API definition in the NetScaler Console GUI.

1. Navigate to **Security > API Security > API Definitions**.
2. Click **Add**.
3. Select **Create Your Definition** and specify the following:
   - **Name** - A name for the API definition.
   - **API Definition** - A definition must include title, version, base path, and host. You can specify a domain name or IP address in the **Host** field.
   - **API Resources** - Add multiple API resources to your definition. Each resource has a path and supported method. Click **Add**. The resource is added to the **Added Resources** table. Click **Delete** to delete an API resource.



4. Click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View API definitions

The **API Definitions** page lists the uploaded definition. Click **View** to see the following API definition details:

- **Name** – Displays the name of an API definition.
- **API Definition** – Displays title, version, base path, and host of a definition.
- **API resources** – Lists the API resources in an API definition and their methods to operate them.

Deploy an API instance

To deploy an API instance, you require an API proxy. An API proxy is a front-end virtual server where the API Security (NetScaler instance) receives the API traffic from API clients. The API clients can be browsers, mobile applications, and so on.

You can share an API proxy with different API deployments. In an organization where you have many API services, you can create a separate API proxy for each API service. Or, you can create and share an API proxy with API instances for different API services.

For example, the two API services `app1` and `app2` are deployed on the same API Security and using the same front-end virtual server. You want to provide the same virtual IP address and SSL certificate information to both API services. In this case, you can add an API proxy with the required information and share with separate deployments. So, API services on different deployments can receive requests using the shared API proxy.

As an administrator, do the following to deploy an API instance:

1. Add an API proxy.
2. Deploy an API instance using the API proxy.

Add an API proxy

Follow the steps to add an API proxy:

1. Go to **Security > API Security > API Proxy > Add**.
2. Specify the following:
    - **Proxy Name** – A name for an API proxy.
    - **Target NetScaler Instance** - Select an NetScaler instance that acts as an API gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **IP address** – An IP address of the virtual server that is hosting API services.
- **Port** – A port number of the virtual server that is hosting API services.
- **Protocol** – Set a protocol depending on the type of traffic that you want to receive on the API proxy (HTTP or HTTPS).
- **TLS Security Profile** – Select High or Medium from the list. If you select High, it maps to the A+ rating SSL profile on a NetScaler instance.
- **Certificate Store** - Select the SSL certificate for the API Security. NetScaler agent certificate store helps you to store and manage your SSL certificates in one location.

  In the NetScaler agent certificate store, you can store SSL certificates in NetScaler agent and reuse them during NetScaler configuration.

  NOTE:

  If your existing deployments use the SSL certificate or key that are not in the NetScaler agent certificate store, you must add the certificate and key to the store with the same name.

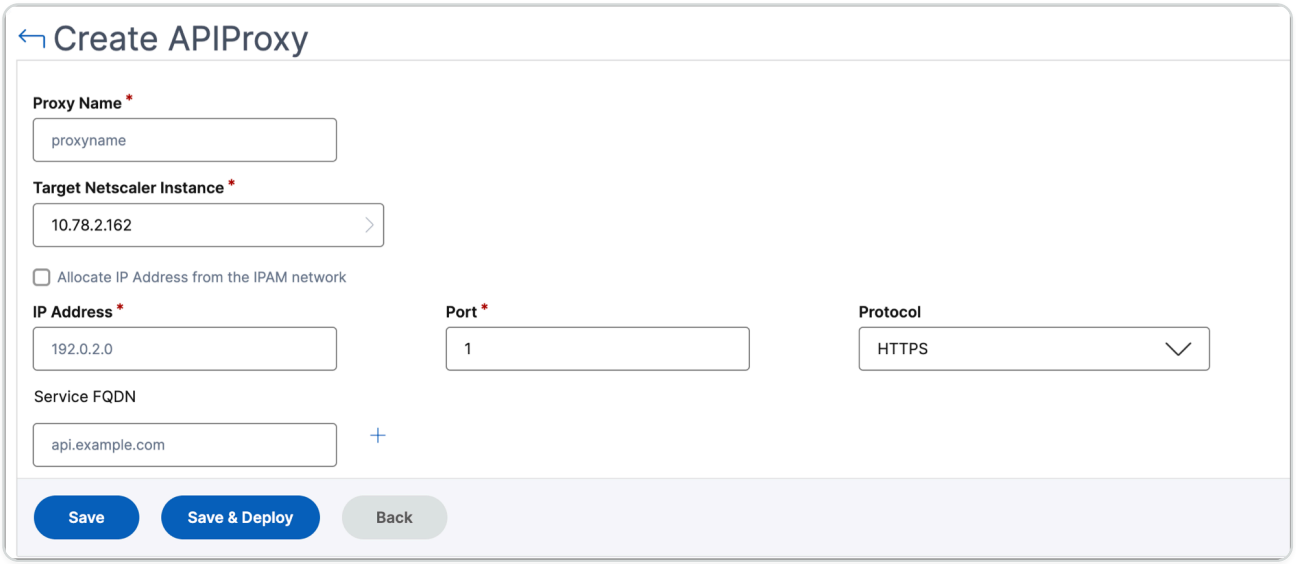
- **Service FQDN** – A fully qualified domain name where your API services are hosted. For example: `api.example.com`

Alternatively, you can select an IPAM network to allocate the IP address. To view the allocated IP address from the IPAM network, navigate to **Settings > IPAM**. For more information on IPAM, see Configure IPAM.

3. Click **Save** to save the deployment configuration.

   If you want to deploy this API proxy on the API Security, click **Save and Deploy**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



After adding an API proxy, deploy an API instance.

Deploy an API instance using the API proxy

Follow the steps to deploy an API instance:

1. Navigate to **Security > API Security > Deployments**.
2. Click **Add**.
3. In **Deployment Basic** Info,
    a. Specify the **Deployment Name**.
    b. In **API Definitions**, select the required API definition.
    c. Select the **API Proxy** that you want to use with this deployment.
4. In **Upstream Services**, click **Add** to add back-end (origin) API servers where you want to egress the API traffic. You can configure an upstream service with its domain name or IP address.

    You can specify SNIP address and netmask details while deploying an API instance. The NetScaler instance uses the specified SNIP address to communicate with the upstream services (back end). The specified SNIP address becomes the source IP address for the egress traffic sent to upstream services. You can also use IPAM to configure SNIP address and netmask. If you don't configure the SNIP address, the default SNIP address of the NetScaler instance becomes the source IP address for the upstream services.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

By default, the SNIP address and netmask options are optional. However, if you specify one of these options, you must specify another option too.

a. Specify a name to an upstream service.

b. Specify the domain.

c. In **Services**, specify an IP address and port value. To add more IP addresses, click **Add a new row**.

d. Click **Add**.

5. In **Routing**, specify the following details to route incoming API traffic based on the resource path prefix:

   a. Specify the route name.

   b. Select an **API Resource** to receive an API request.

      NOTE:

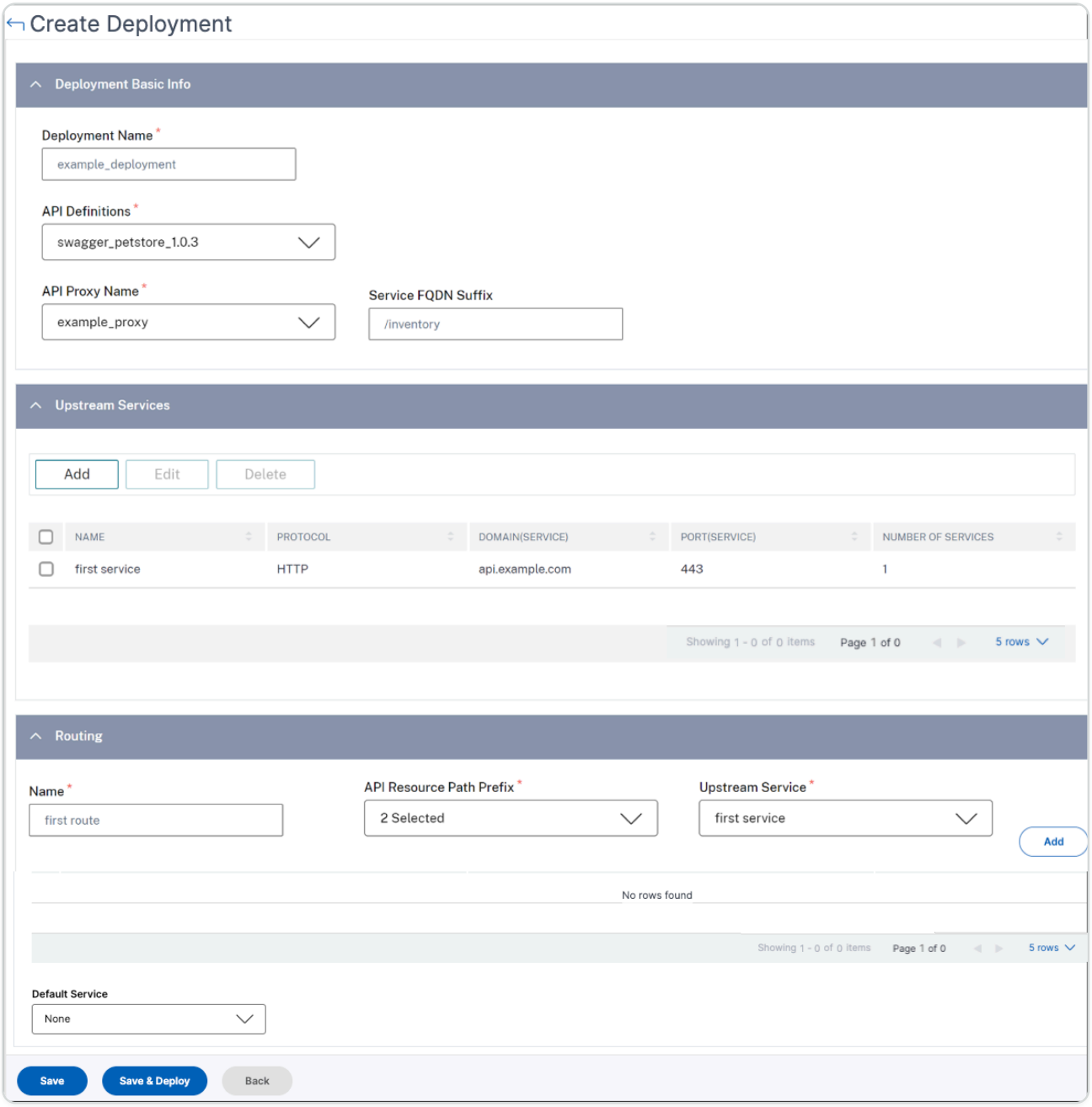
      You can also specify the custom path or path prefix.

   c. Select an **Upstream Service** from the list where you want to transfer the API traffic.

6. Click **Save** to save the deployment configuration.

   If you want to deploy the configuration to the API Security, click **Save and Deploy**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Enable the API analytics

The following are the prerequisites to enable analytics for a deployment:

- Ensure that virtual servers are **licensed**
- Ensure that analytics status is **Disabled**
- Ensure that virtual servers are in **UP** status

To enable the API analytics for a deployment, do the following:

1. In **Security > API Security > Deployments**, select the deployment to which you want to enable the API analytics.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Click **Enable Analytics**.
3. In the **Configure Analytics for deployment** page, select the virtual server, and click **Enable Analytics**.
4. On the **Enable Analytics** window:

    a. Select the insight type (Web Insight, Security Insight, Bot Insight)

    b. Select **Logstream** or **IPFIX** as Transport Mode.

    For more information about IPFIX and Logstream, see Logstream overview.

    The Expression is true by default.

    c. Click **OK**.

NetScaler Console enables analytics on the selected virtual servers.

Add policies to an API deployment

You can configure various security policies for your API traffic. This configuration requires you to specify the traffic selection criteria and the parameters required for a policy. Do the following steps to add a policy to an API definition:

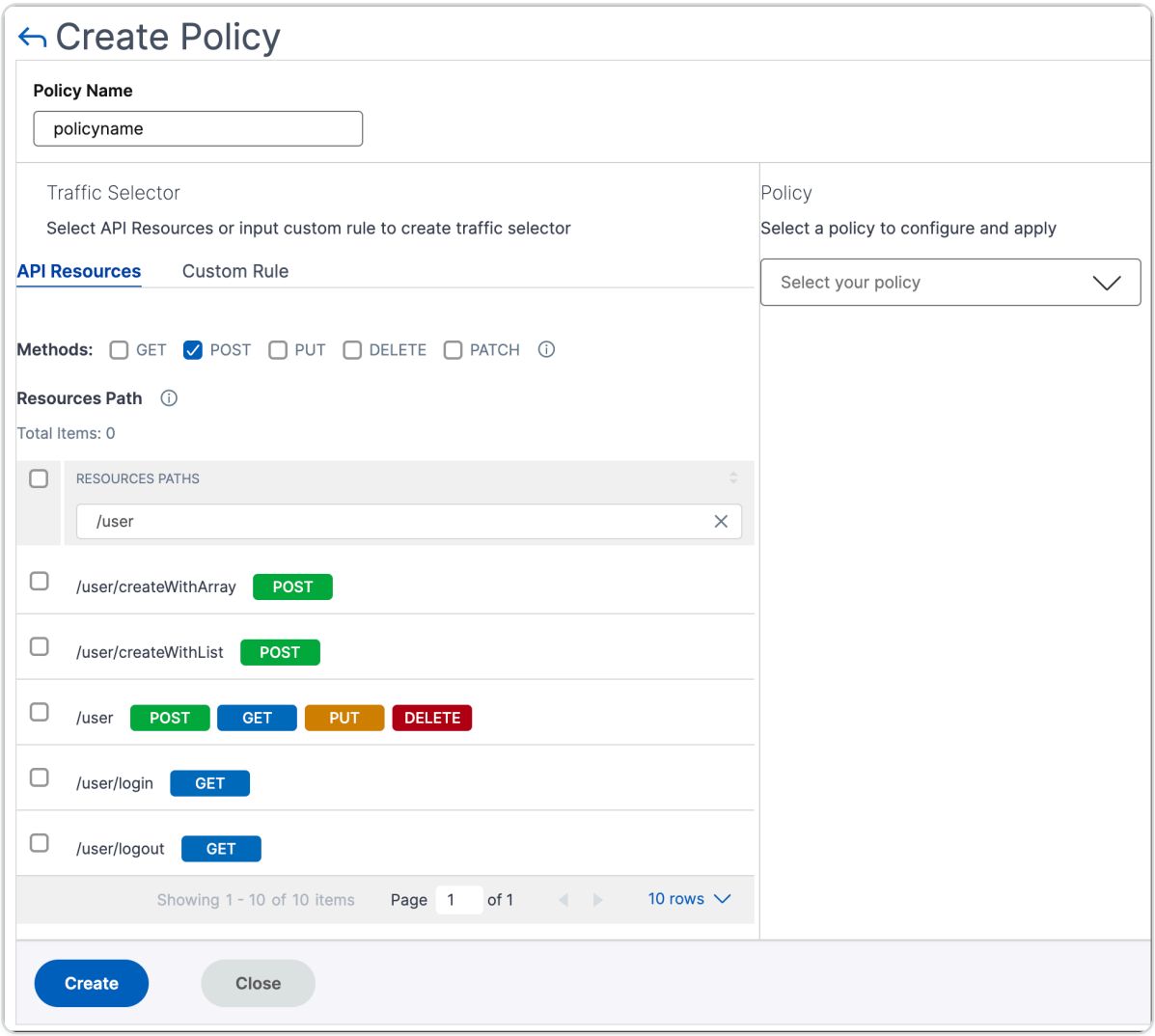
1. Navigate to **Security > API Security > Policies**.
2. Click **Add**.
3. Specify the name for a policy group.
4. Select a **Deployment** from the list.
5. Select an **Upstream Service** from the list for which you want to configure policies.
6. Click **Add** to select traffic selectors and a policy type.

    Traffic selector - The traffic selection criteria includes API resource paths or path prefixes, methods, and policy.

    You can use any of the following options to specify traffic selection criteria:

    - **API Resources** – Select an API resource and its methods for which you want to apply a policy. You can search API resources and methods with a key word.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

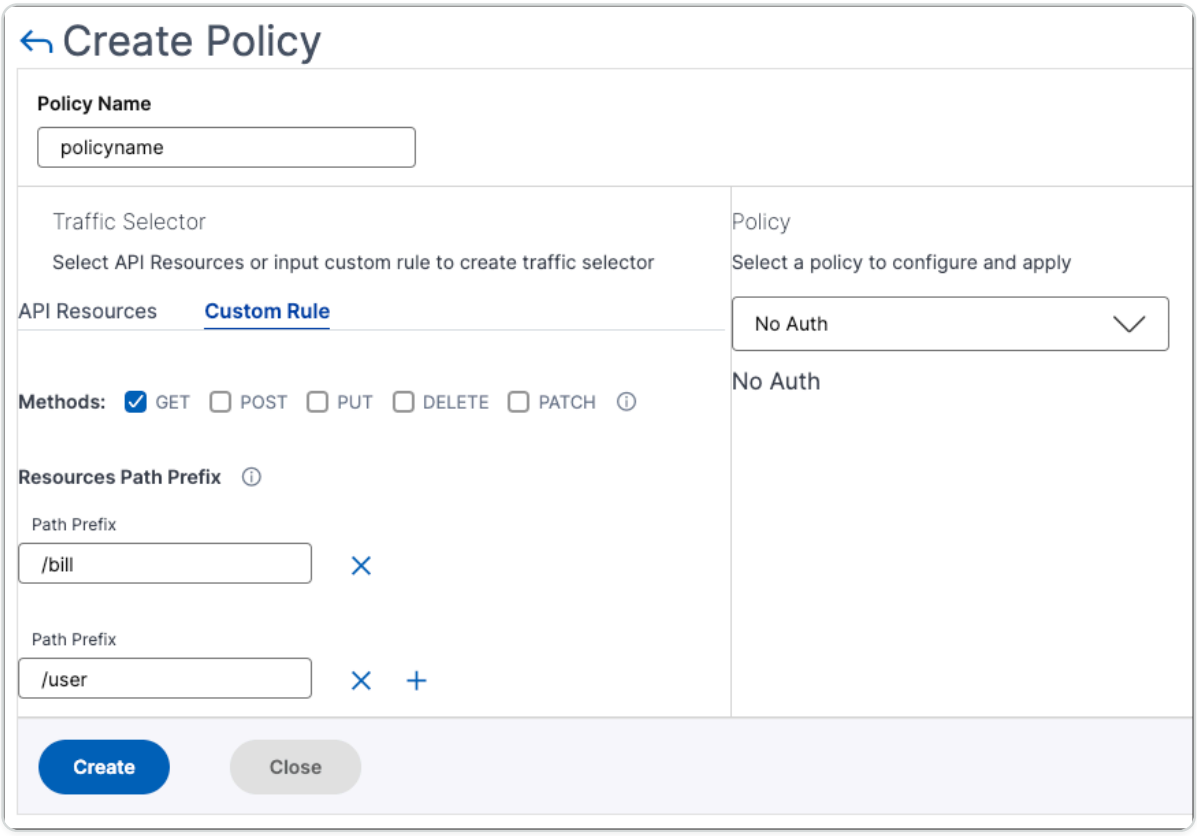


In this example, the API resources with `/user` that have the `POST` method are listed.

- **Custom Rule** – In this tab, you can specify custom path prefixes and multiple methods.

  The configured policy applies to an incoming API request that matches the custom rule for API traffic selection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



In this example, the **No-Auth** policy applies to the API resources that have the `/bill` prefix and the `GET` method.

In **Policy**, select a policy from the list that you want to apply to the selected API resource and method. For more information about each policy, see Policy types.

7. Optional, you can move policy types to set a priority. The policy types with higher priority apply first.
8. Click **Save** to add a policy. If you want to apply the policy immediately, click **Save & Apply**.

Policy types

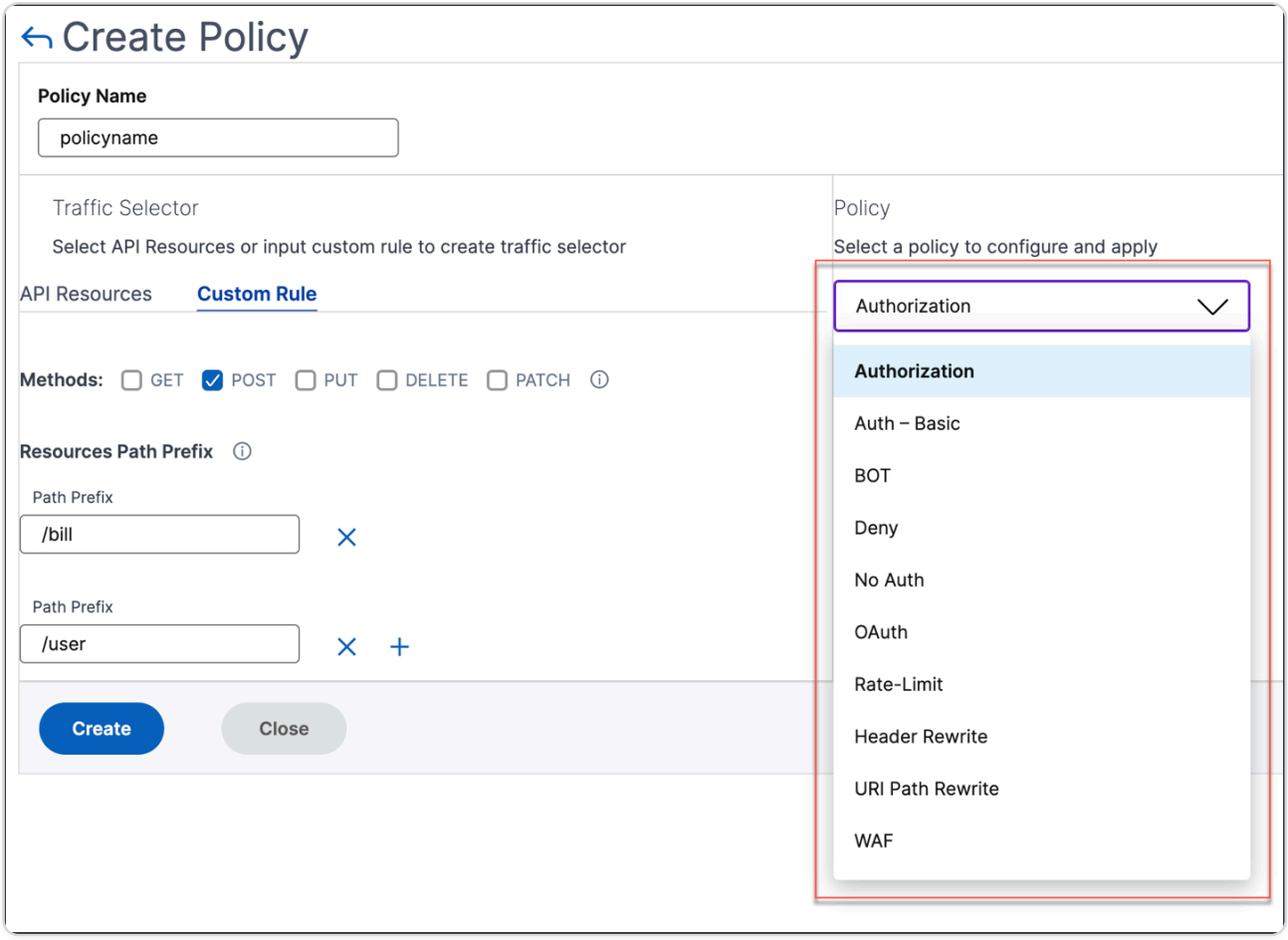
When you are configuring an API policy, you can select the following policies that you want to apply to the API resource and method:

- **Authentication and Authorization**
- **Rate limit**
- **WAF**
- **BOT**
- **Header Rewrite**
- **URI Path Rewrite**
- **Deny**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

To manage the API Security using APIs, see Use APIs to manage API Security.



Authentication and Authorization

API resources are hosted on an application or API server. When you want to enforce access restrictions on such API resources, you can use the authentication and authorization policies. These policies verify whether the incoming API request has a necessary permission to access the resource.

Use the following policies to define authentication and authorization for the selected API resources:

`No-Auth`

Use this policy to skip authentication on the selected traffic.

`Auth-Basic`

This policy specifies that local authentication to be used with the HTTP basic authentication scheme. To use local authentication, you must create user accounts on the NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`OAuth`

OAuth requires an external identity provider to authenticate a client using oAuth2 and issue an access token. When the client provides this token as an access credential to an API gateway, the token is validated based on the configured values.

- **JWKS URI** - The URL of an endpoint that has JWKs (JSON Web Key) for JWT (JSON Web Token) verification
- **Issuer** - The identity (usually a URL) of the authentication server.
- **Audience** - The identity of the service or application for which the token is applicable.
- **Claims to save** - The access permissions are represented as a set of claims and expected values. Specify the claim values in the CSV format.
- **Introspect URI** - An introspection endpoint URL of the authentication server. This URL is used to verify opaque access tokens. For more information about these tokens, see OAuth configuration for opaque access tokens.

  After you specify **Introspect URI**, specify the **Client Id** and **Client Secret** to access the authentication server.
- **Allowed algorithms** - This option allows you to restrict certain algorithms in the incoming tokens. By default, all the supported methods are allowed. However, you can check the required algorithms for the selected traffic.

On successful validation, API Security grants access to the client.

IMPORTANT:

When you configure an OAuth or **Auth-Basic** policy for the selected API resources, configure the **No Auth** policy for the remaining API resources. This configuration explicitly indicates that you want to skip authentication for the remaining resources.

Authorization

This policy verifies the required permissions to access an API resource. The access permissions are represented as a set of claims and expected values. To configure this policy, select **Add a new Claim** and specify the following:

- Claim Name
- Claim Values

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT:

API Security requires both authentication and authorization policies for API traffic. Therefore, you must configure an authorization policy with an authentication policy. The authentication policy can be OAuth or `Auth-Basic`.

Even if you do not have any authorization checks, you must create an authorization policy with empty claims. Otherwise, the request is denied with a 403 error.

Rate limit

Specify the maximum load given to the selected API resource. With this policy, you can monitor the API traffic rate and take preventive actions. To configure this policy, specify the following:

- **HTTP Header Name** - It is a traffic selector key that filters the traffic to identify the API requests. And, the Rate limit policy applies and monitors only to such API requests.
- **Header Values** - These header values are separated by commas for the mentioned header name.
- **Threshold** - The maximum number of requests that can be allowed in the specified interval. If you have specified **Header Values**, this threshold applies for each header value.

  Example-1:

  When you specify header values (`"key1","key2","key3"`) for the header name `x-api-key` and you set the threshold to `80`, the set threshold applies for each header value.

  Example-2:

  If you want to specify different thresholds for each header value, create separate rate limit policies using the same HTTP header name.

  - **Policy-1**: Specify header values (`"key1","key2"`) for the header name `x-api-key` and you set the threshold to `80`.
  - **Policy-2**: Specify header values (`"key3"`) for the header name `x-api-key` and you set the threshold to `30`.

  If you don't specify a header value, the threshold applies for the specified HTTP header name.
- **Time slice** - The interval specified in microseconds. During this interval, the requests are monitored against the configured limits. By default, it is set to 1000 microseconds (1 millisecond).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Limit type** - The mode how you want to apply the rate limit policy. You can select **Burst** or **Smooth** limit type.
- **Action** - Defines an action that you want to take on the traffic that breaches the threshold. You can specify one of the following actions:
  - **DROP**: Drops the requests above the configured traffic limits.
  - **RESET**: Resets the connection for the requests.
  - **REDIRECT**: Redirects the traffic to the configured redirect_url.
  - **RESPOND**: Responds with the standard response (`429 Too many requests`).

WAF

This policy prevents security breaches, data loss, and possible unauthorized modifications to websites that access sensitive business or customer information.

Before you configure a WAF policy, create a WAF profile in NetScaler Console using StyleBooks.

In **WAF Profile Name**, select or specify the WAF profile that you have created.

Bot

This policy identifies bad bots and protects your appliance from advanced security attacks.

Before you configure a BOT policy, create a BOT profile in NetScaler Console using StyleBooks.

In **Bot Profile Name**, specify the BOT profile that you have created.

Header Rewrite

This policy helps you modify the header of API requests and responses. If you want to replace the value in the HTTP header, specify the following:

- **HTTP Header Name**: The filed name that you want to modify in the request header.

  Example: `Host`
- **Header value**: Optional, the value string that you want to modify in the specified header name.

  Example: `sample.com`
- **Header new value**: The new value to replace the specified header value.

  If no **Header value** is specified, it replaces any received value with the specified value to the **HTTP Header Name**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example: `example.com`

In this example, the header rewrite policy replaces `sample.com` to `example.com` in the `Host` field of an API request.

URI Path Rewrite

This policy helps you modify the URI path of API requests and responses. If you want to replace a segment in the URI path, add a rule to do one of the following:

- **Replace a path segment** – When you select this action type, specify the following:
  - **Current path segment** – The path segment that you want to replace.
  - **New path segment** – New path segment that replaces only the current path segment.

  For example, to change a locale in the URI path from English to Chinese, specify `/en-us/` in **Current Path Segment**. And, specify `/zh-zh` in **New Path Segment**. It replaces only the path segment and retains the remaining URI path.
- **Replace the full path** – This action type completely replaces the URI path of API requests and responses with the specified path. If you specify `/example.html` in **New Path Segment**, the URI path of an API request or response is changed to the specified path.
- **Remove the path segment** – This action removes the specified segment from the URI. For example, to remove English locale from the URI path, specify `/en-us/` in **Current Path Segment**.
- **Insert a path segment** – This action inserts the specified segment in the URI path. To apply this rule, specify the position where you want to insert the segment. And, what segment you want to insert.

  For example, when you want to insert a segment right after some text, do the following:

  a. Specify the position where you want to insert a new segment.
  b. In **Current Path Segment**, specify the text after which a new segment to be added.
  c. In **New Path Segment**, specify the segment that you want to add.

Deny

This policy helps you deny API requests from reaching your API resources.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View API analytics

API analytics enables visibility into API traffic. This analytics allows IT administrators to monitor API instances and endpoints served by an API gateway. It provides integrated periodic monitoring of API requests.

Before you monitor API analytics, ensure to complete the following:

1. Add an API definition
2. Deploy an API definition
3. Add a policy to an API definition
4. Apply license to API instances
5. Enable Web Insight on API instances

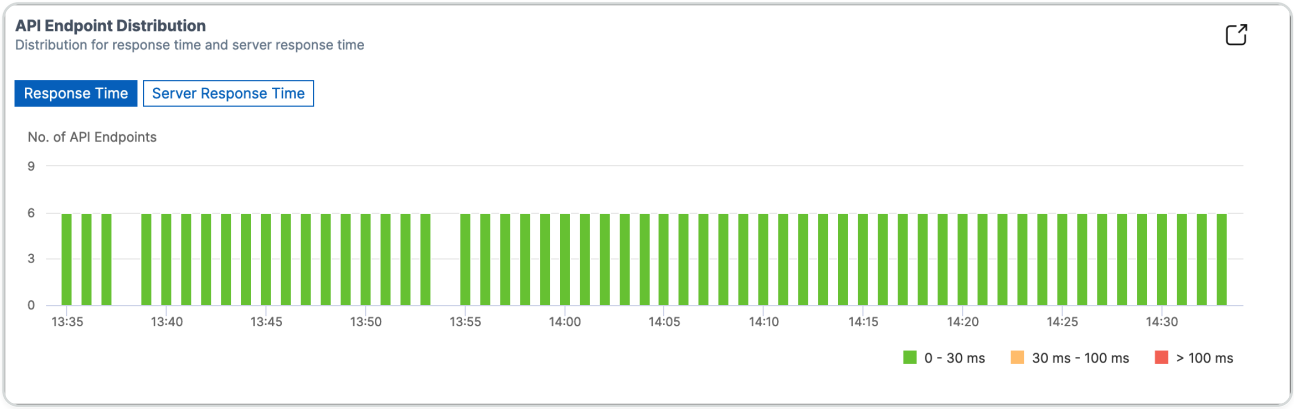
In **API Analytics**, you can monitor the response time of API instances and endpoints that are added as part of API definitions. It also displays the bandwidth consumed by API instances and endpoints.



By default, the dashboard displays API analytics for the last one hour. You can select a duration to view API analytics for that interval. Click **See more** on each tile to view the entire list. In this view, you can search API instances and endpoints by their partial names except the **Geo Locations** tile.

API endpoint distribution

This graph displays the distribution of application and server response time for API endpoints. You can identify an API endpoint that has a huge response time and take the necessary actions.



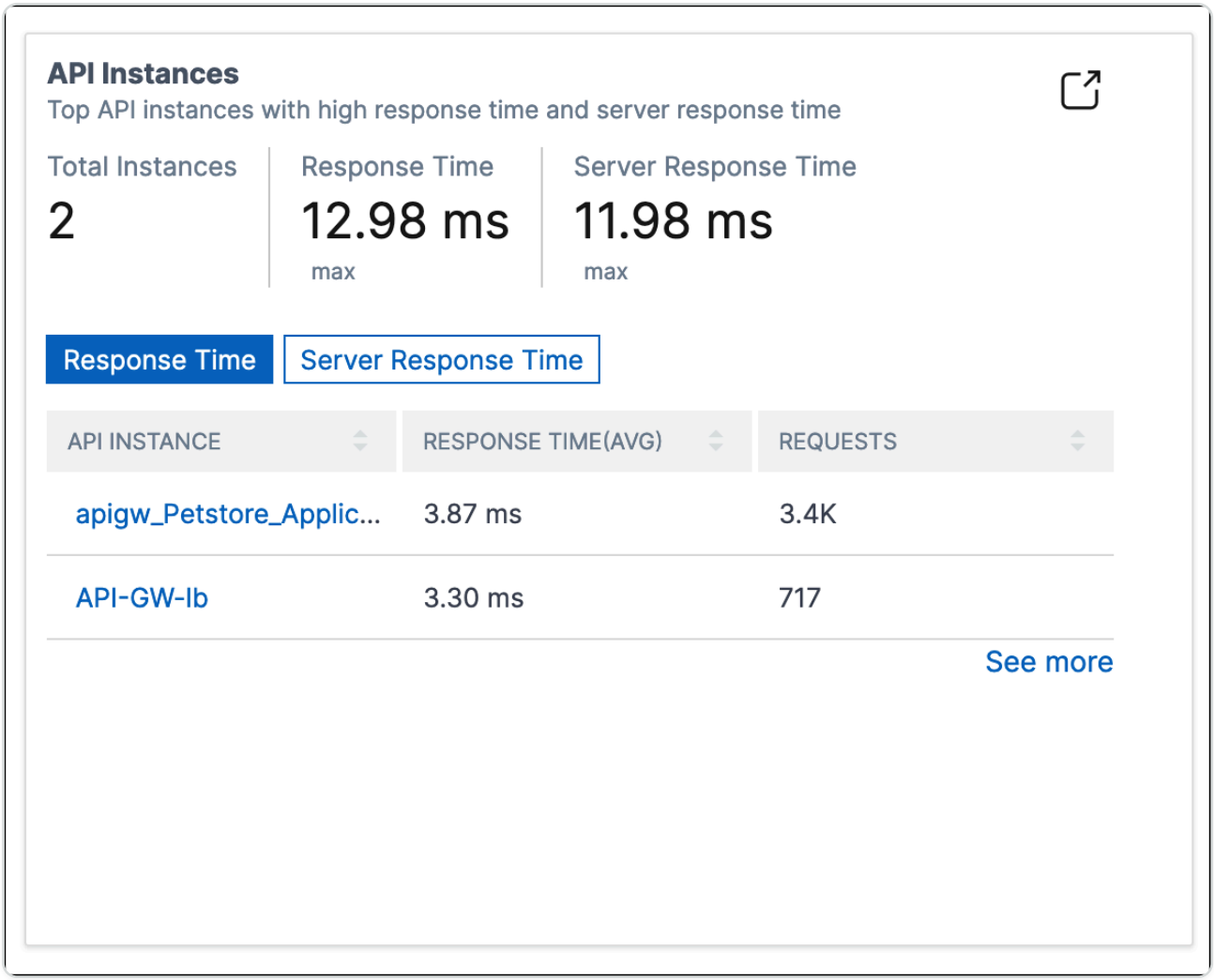
The API endpoints appear in one of the following colors depending on their response time limits:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Green** – If the response time is less than 30 milliseconds.
- **Orange** – If the response time is between 30–100 milliseconds.
- **Red** – If the response time is more than 100 milliseconds.

API instances

The **API Instances** tile displays the top API instances with high application and server response time.



Select an API instance to view its performance, usage, and security details. The selected API instance displays the following information:

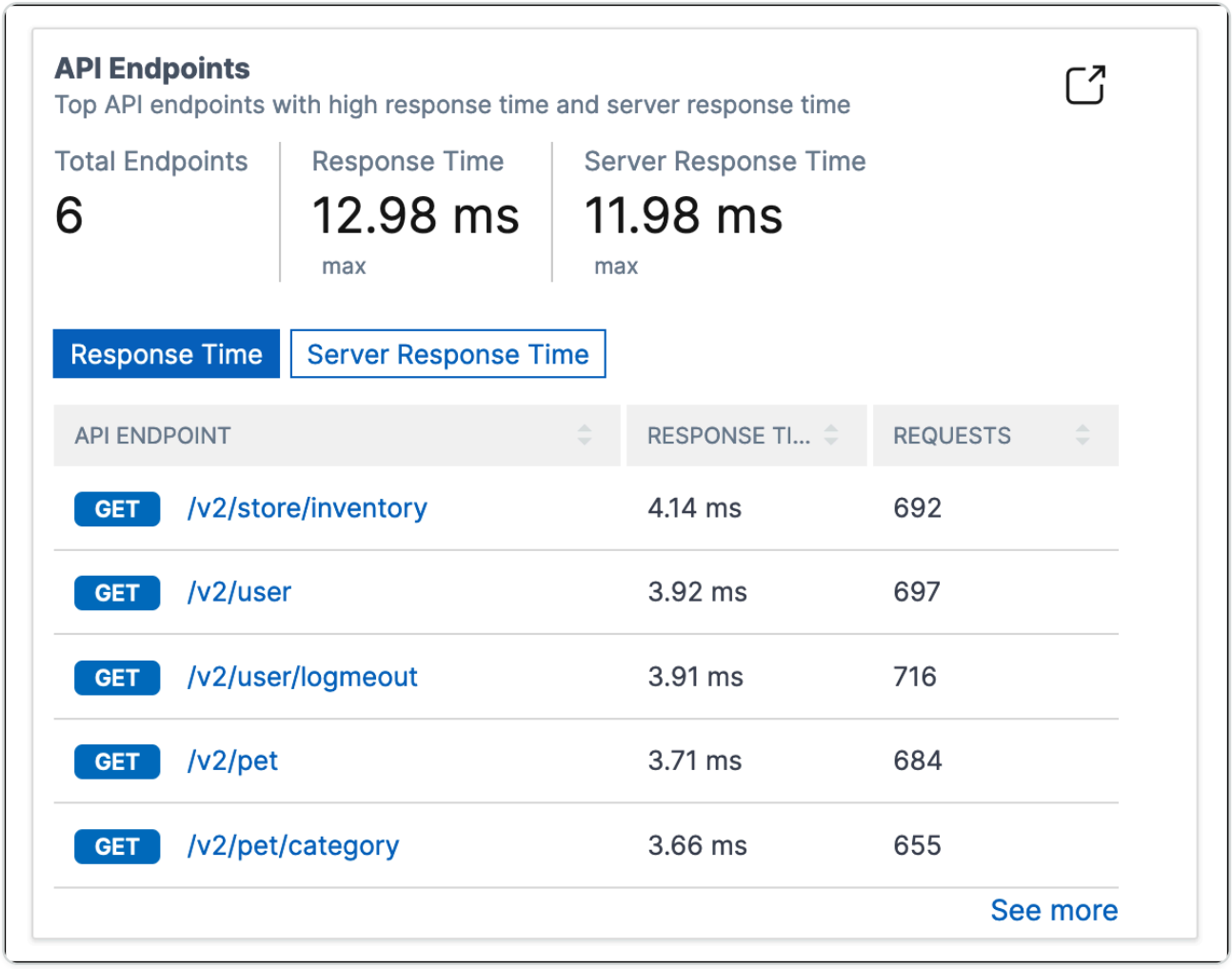
- API endpoints count
- Requests count
- Application and server response time
- Consumed bandwidth
- Authentication failures

© 1997–2026 Citrix Systems, Inc. All rights reserved.

API Endpoints	Requests	Response Time	Server Response Time	Bandwidth	Auth Failures
5	3.5K	3.88 ms	1.98 ms	3.04 MB	0

API endpoints

The **API Endpoints** tile displays the top endpoints with high application and server response time.

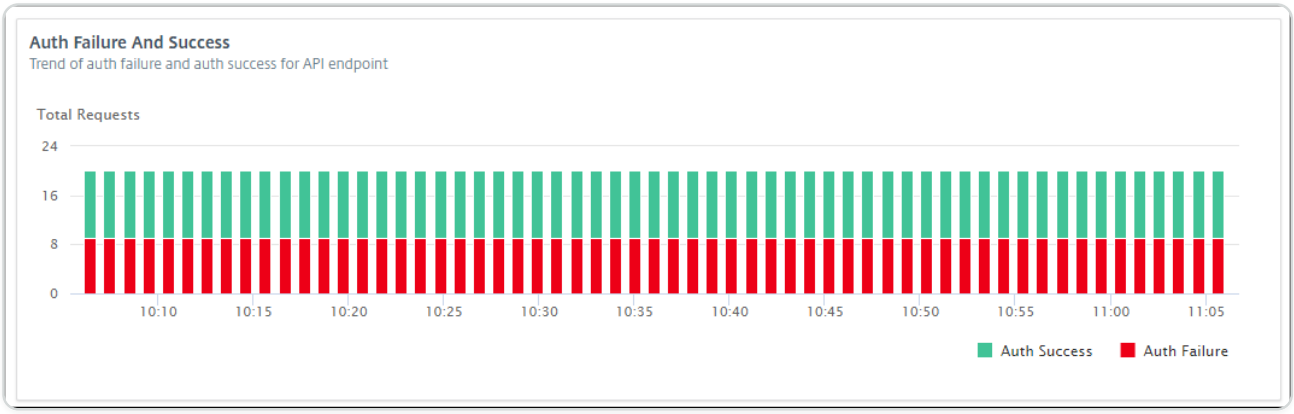


Select an API endpoint to view performance, usage, and security details.

Authentication failures

The **Auth Failures** tile displays top API endpoints that have more authentication failures. The authentication failure or success happens based on the policy added to an API definition.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



If you want to view authentication failure and success rate in an API endpoint, do the following:

1. Select an endpoint from **API Endpoints**.
2. Select the **Security** tab. This tab displays the authentication failures and successes in the selected endpoint.



If you want to view the authentication failure and success rate in the API endpoints of an instance, do the following:

1. Select an instance from **API Instance**.
2. Select the **Security** tab. This tab displays the authentication failures and successes in the endpoints of the selected instance.

View different API insights

Navigate across API Analytics to view a specific information on the following:

- View API analytics
  - API endpoint distribution

© 1997–2026 Citrix Systems, Inc. All rights reserved.

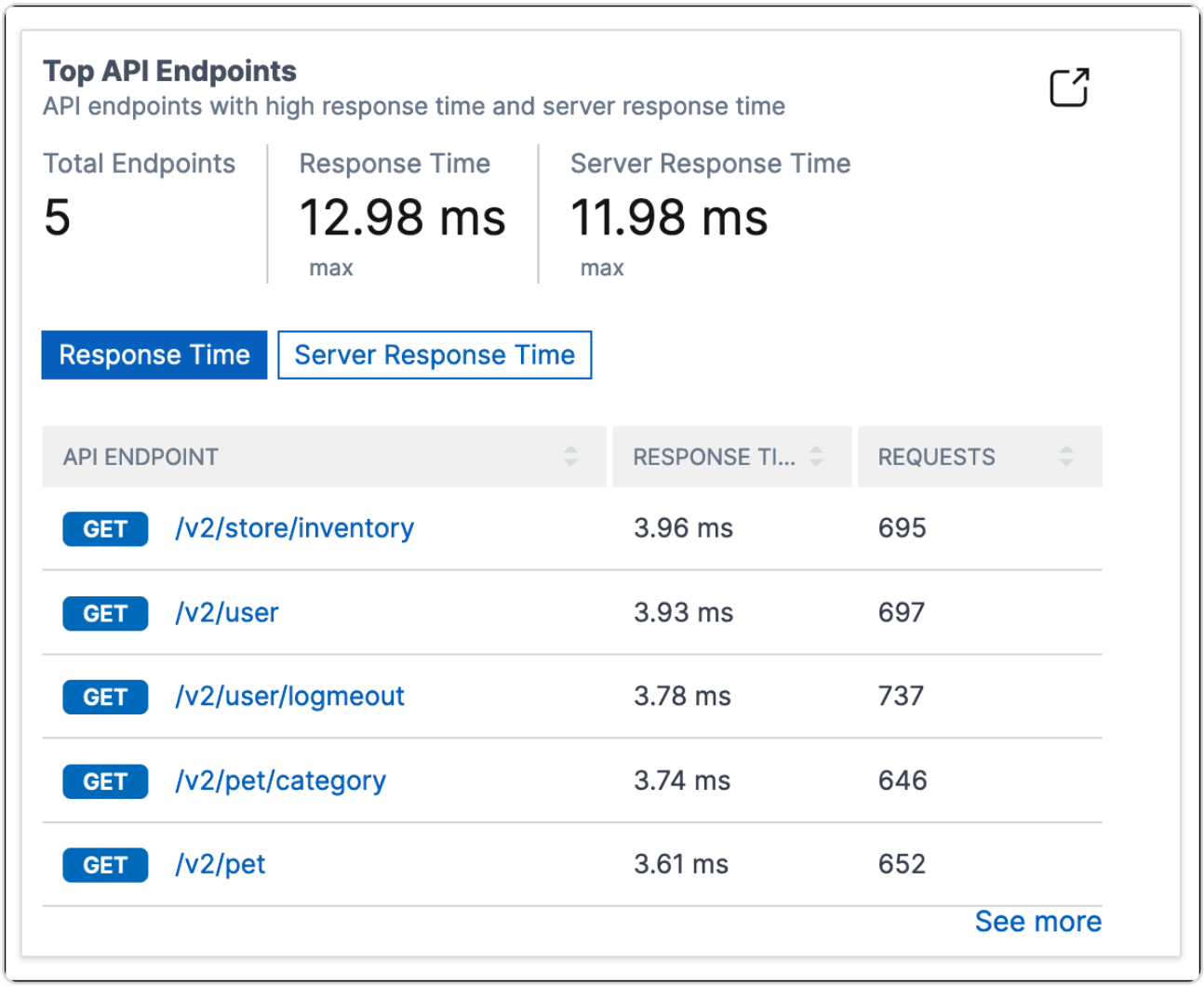
- API instances
- API endpoints
- Authentication failures
- View different API insights
  - View top API endpoints in an instance
  - View most accessed APIs
  - View geo-location of an endpoint
  - View HTTPS response status
  - View API requests trend
  - View bandwidth consumption of an endpoint
  - View SSL errors and usage

View top API endpoints in an instance

The **API Analytics** page displays the top endpoints that have high response time. If you want to view similar endpoints of an instance, select an instance from **API Instances**.

The **Top API Endpoints** tile displays the endpoints that have high application and server response time.

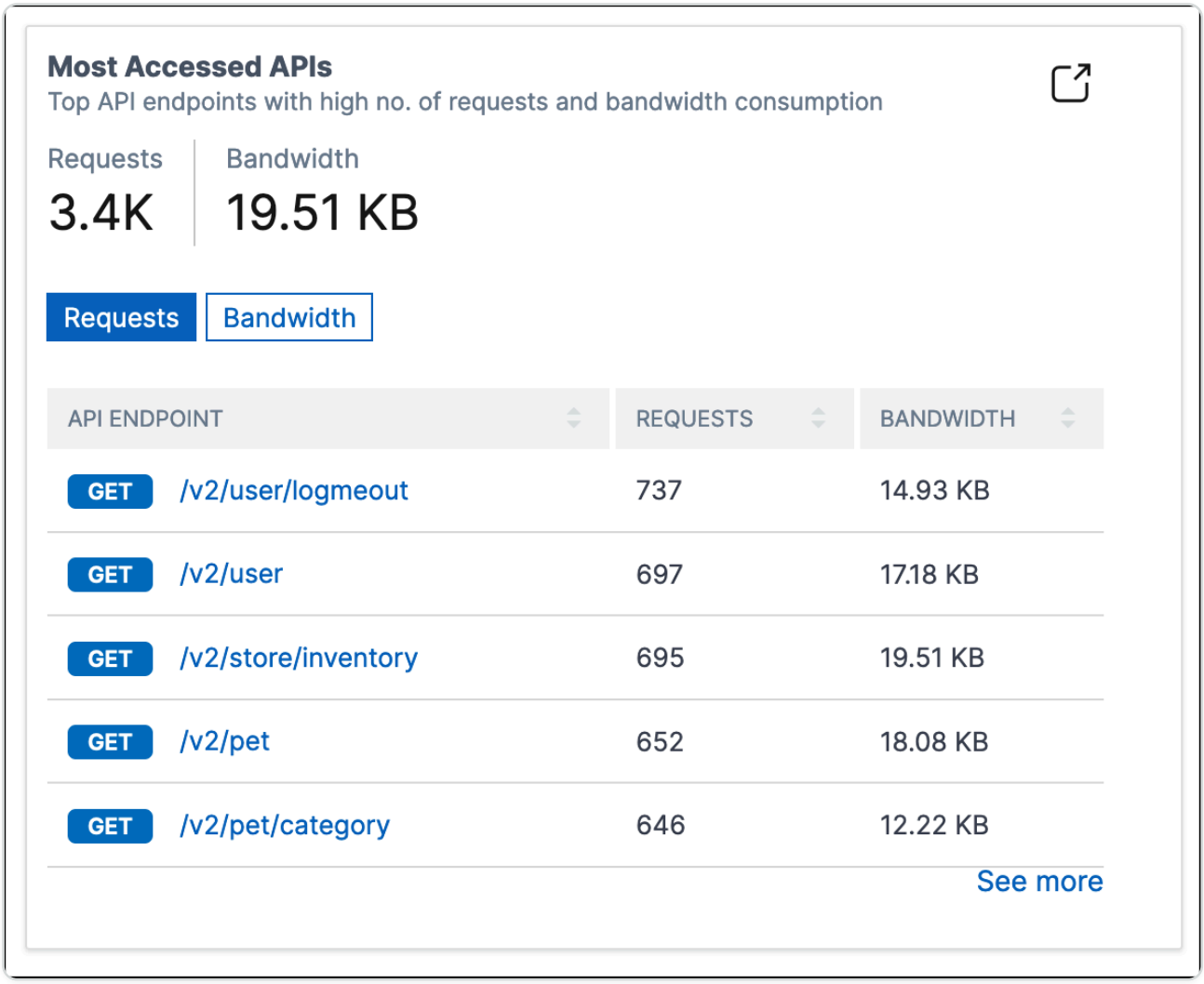
© 1997–2026 Citrix Systems, Inc. All rights reserved.



View most accessed APIs

In **API Analytics**, select an API instance from API instances. The **Most Accessed APIs** tile displays the top endpoints that have more requests and bandwidth.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

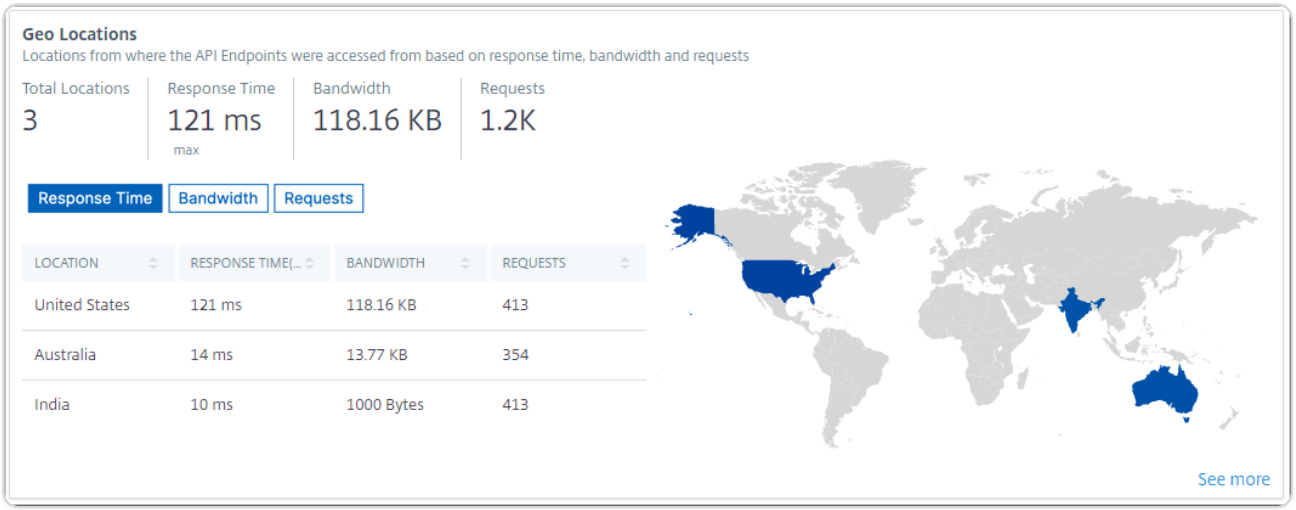


View geo-location of an endpoint

1. In **API Analytics**, select any of the following:
   - Select an instance from **API Instances** to view the locations from where the endpoints of the selected instance received requests.
   - Select an endpoint from **API Endpoints** to view locations from where the endpoint received requests.
2. In **Performance and Usage**, the **Geo Locations** tile appears.

   You can sort locations based on response time, bandwidth, and requests.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

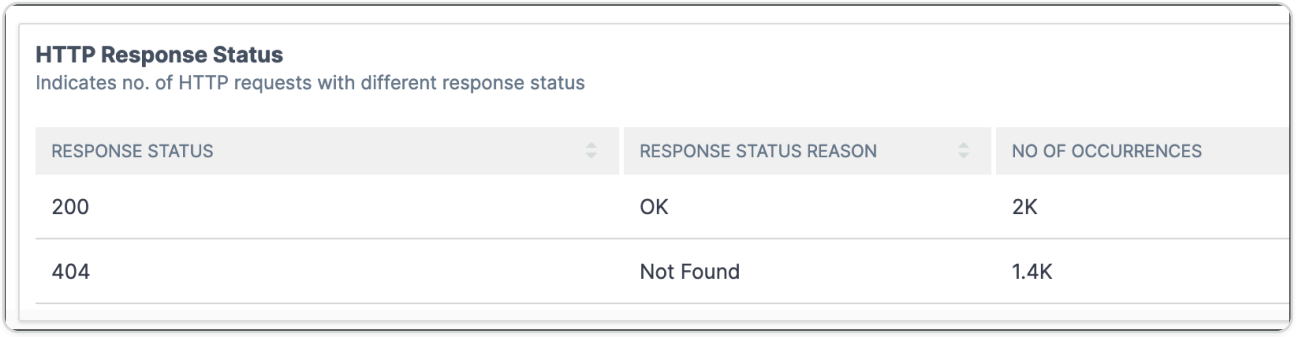


View HTTPS response status

The **HTTPS Response Status** tile displays the response status with its reasons and occurrences. You can view HTTPS response status in one of the following ways:

- Select an instance from **API Instances**.
- Select an endpoint from **API Endpoints**.

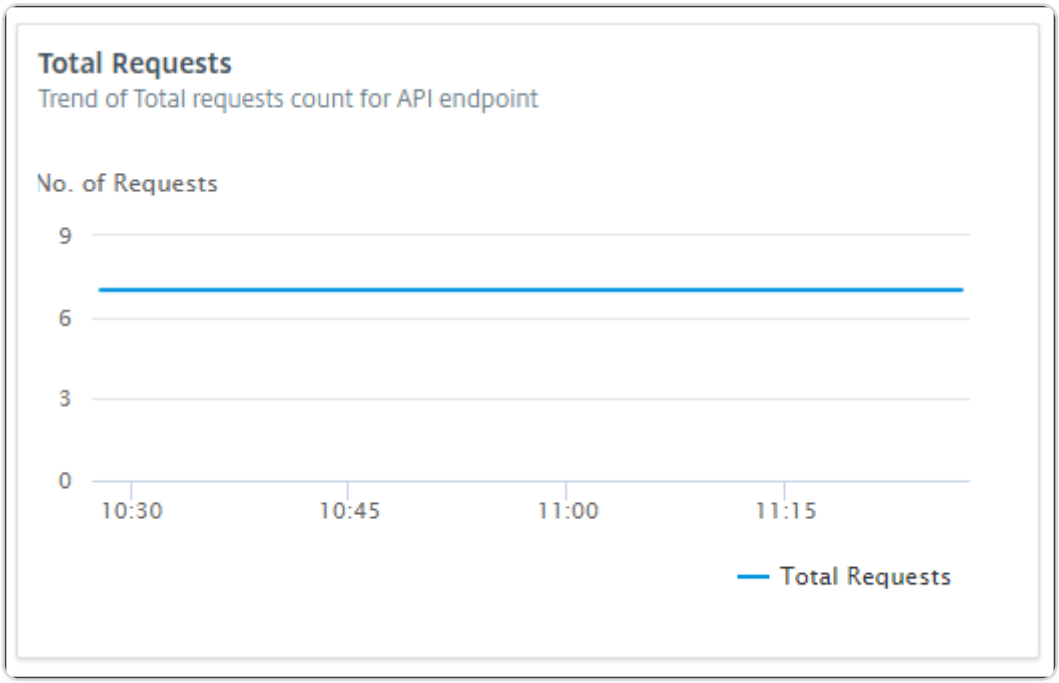
This tile appears in the **Performance and Usage** tab.



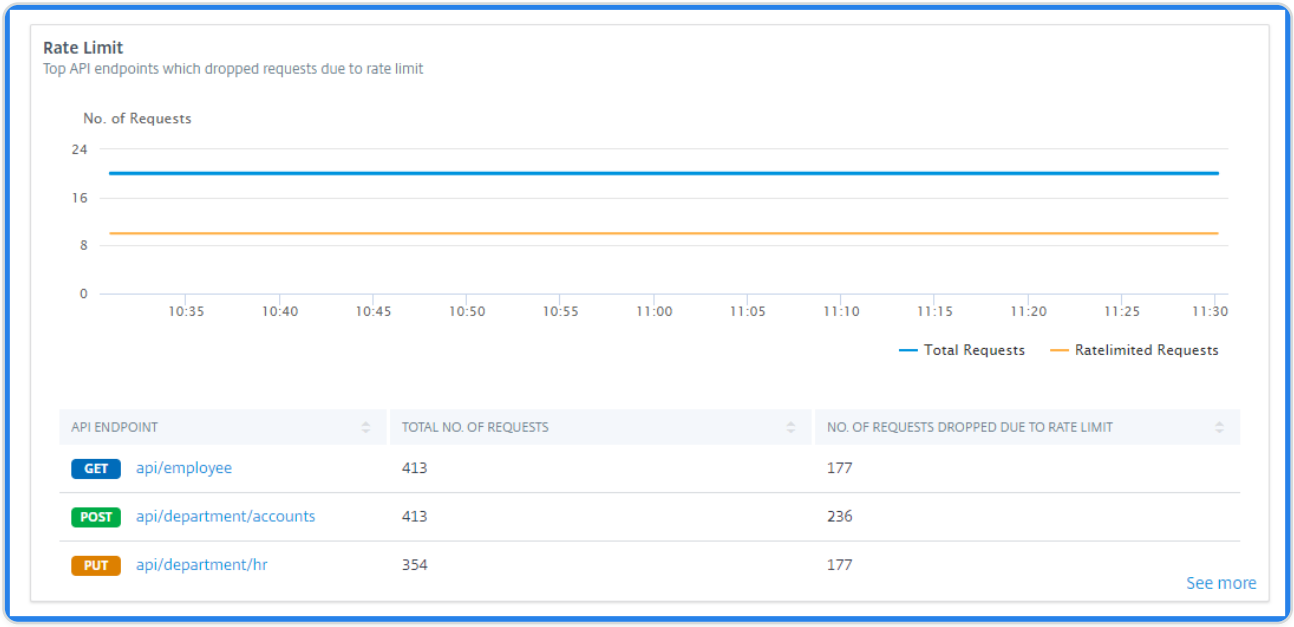
View API requests trend

Select an endpoint from **API Endpoints**. In **Performance and Usage**, the **Total Requests** tile displays the trend of total requests count received by an endpoint.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



If you want to view the trend of dropped requests because of a rate limit, select an instance from **API Instances**. In **Security**, the **Rate Limit** tile displays the trend of dropped requests. It also displays the trend of total requests received by an endpoint.

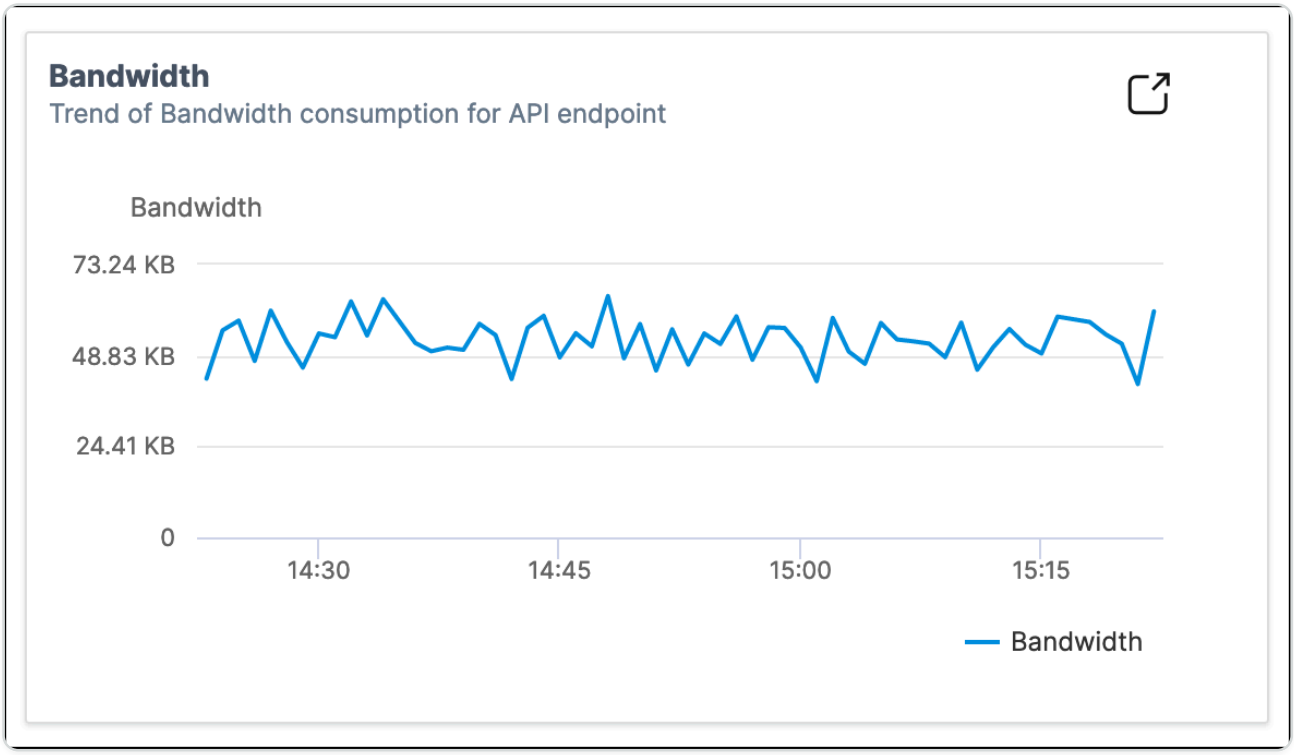


With this comparison, you can determine how many requests are dropped because of a rate limit among total requests.

View bandwidth consumption of an endpoint

To view the bandwidth consumption trend by an endpoint, select an endpoint from the API endpoints. The **Bandwidth** tile displays a bandwidth consumption graph.

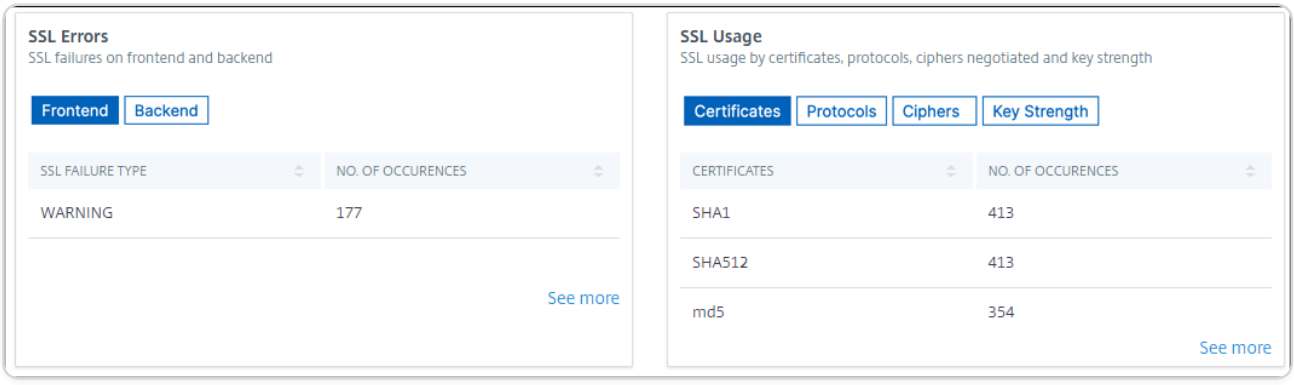
© 1997–2026 Citrix Systems, Inc. All rights reserved.



View SSL errors and usage

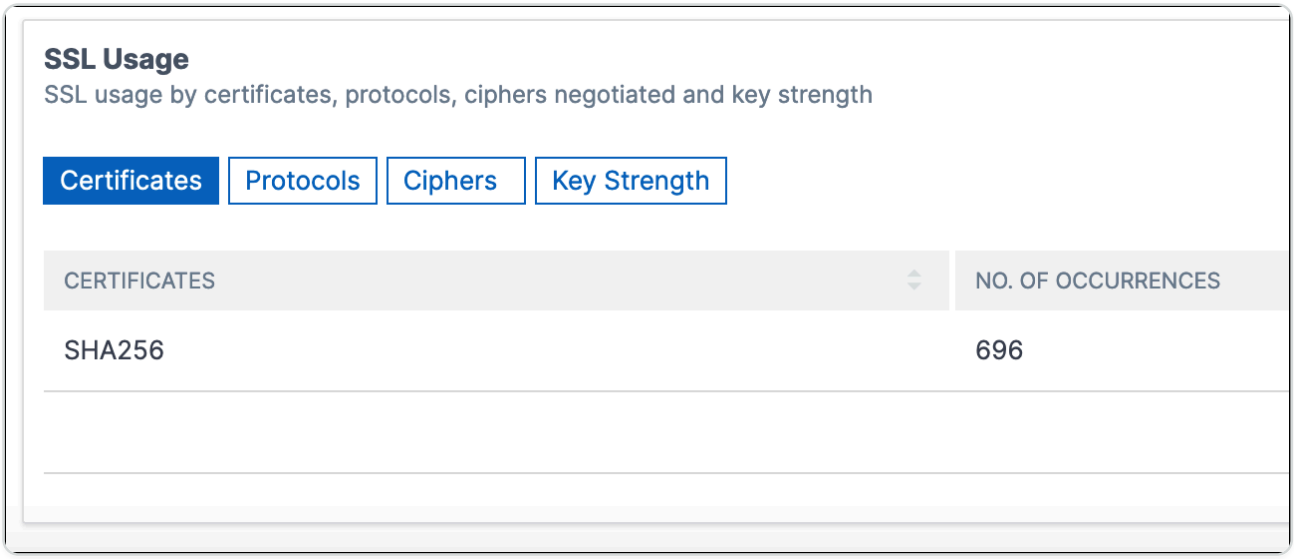
Select an instance from **API Instances**. In **Security**, the following tiles appear:

- **SSL Errors** – Displays SSL failures occurred on clients and applications servers.
- **SSL Usage** – Displays SSL certificates, protocols, cipher, and key strengths with their occurrences.



To view the SSL usage in an endpoint, select an endpoint from the API endpoints. The **SSL Usage** tile appears in the **Security** tab.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Discover API endpoints

You can view the discovered API endpoints that are in your organization using API Security. NetScaler Console discovers the API endpoints based on the API traffic received on NetScaler instances and API deployments.

In NetScaler Console, the **Security > API Security > API Discovery** page displays the discovered API endpoints.

- **Virtual servers** - The **VServer** tab displays the virtual servers from your NetScaler instances. The virtual servers appear in this tab when they receive the API requests for the specified period.
- **API deployments** - This tab displays the API deployments that are deployed from NetScaler Console using an API definition. This tab discovers the API endpoints when API deployments receive the API requests for the specified period. To add and deploy an API definition, see Add an API definition and Deploy API definitions.

NOTE:

- Ensure to configure analytics and enable Web Insights on virtual servers. See, Enable Web Insight on API instances.
- You can only add policies to the API endpoints that are discovered under the **API deployments** tab.

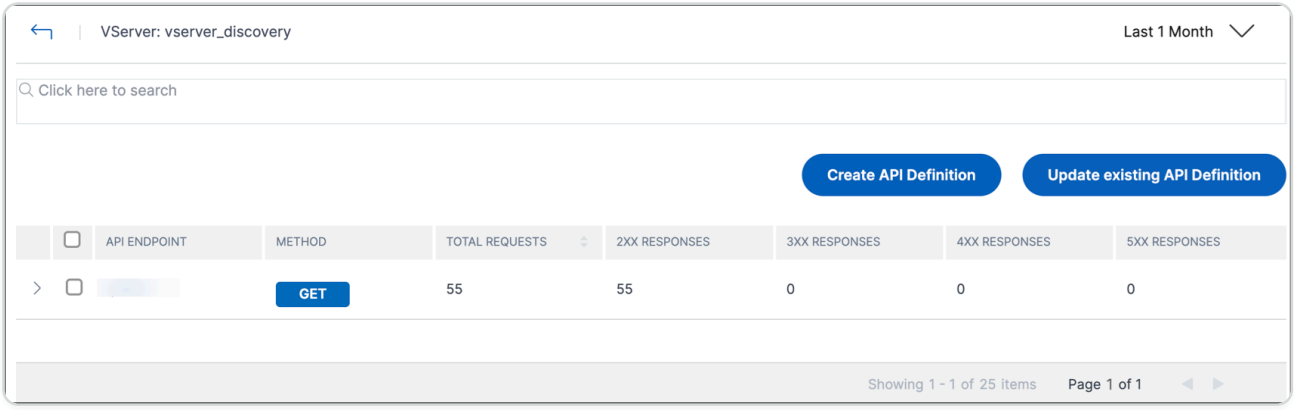
© 1997–2026 Citrix Systems, Inc. All rights reserved.

View API endpoints

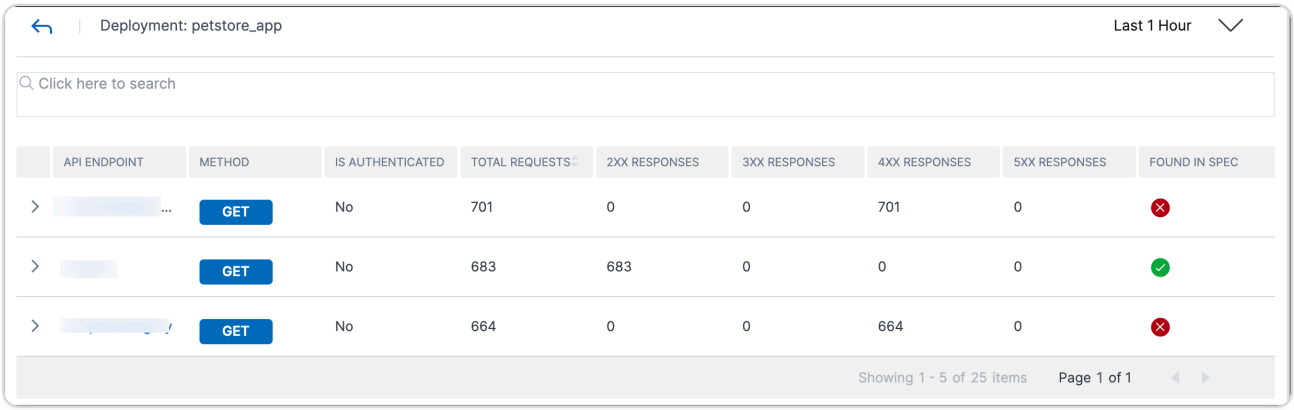
In **API Discovery**, when you select a virtual server or API deployment, the NetScaler Console GUI displays the API endpoints and their details such as:

- **Method** - It displays the method used in an API endpoint. For example, `GET` and `POST` methods.
- **Total requests** - It displays the count of API requests on the API endpoint.
- **Response statuses** - It displays the count for each response status. For example, `2xx`, `3xx`, `4xx`, and `5xx`.
- **Found in Spec** - This column appears only for API deployments. Sometimes, the internal APIs that 's not part of the API definition might receive traffic from outside. This column helps you identify whether the API endpoint and observed method are part of the API definition.

The API endpoints in a virtual server are available as follows:

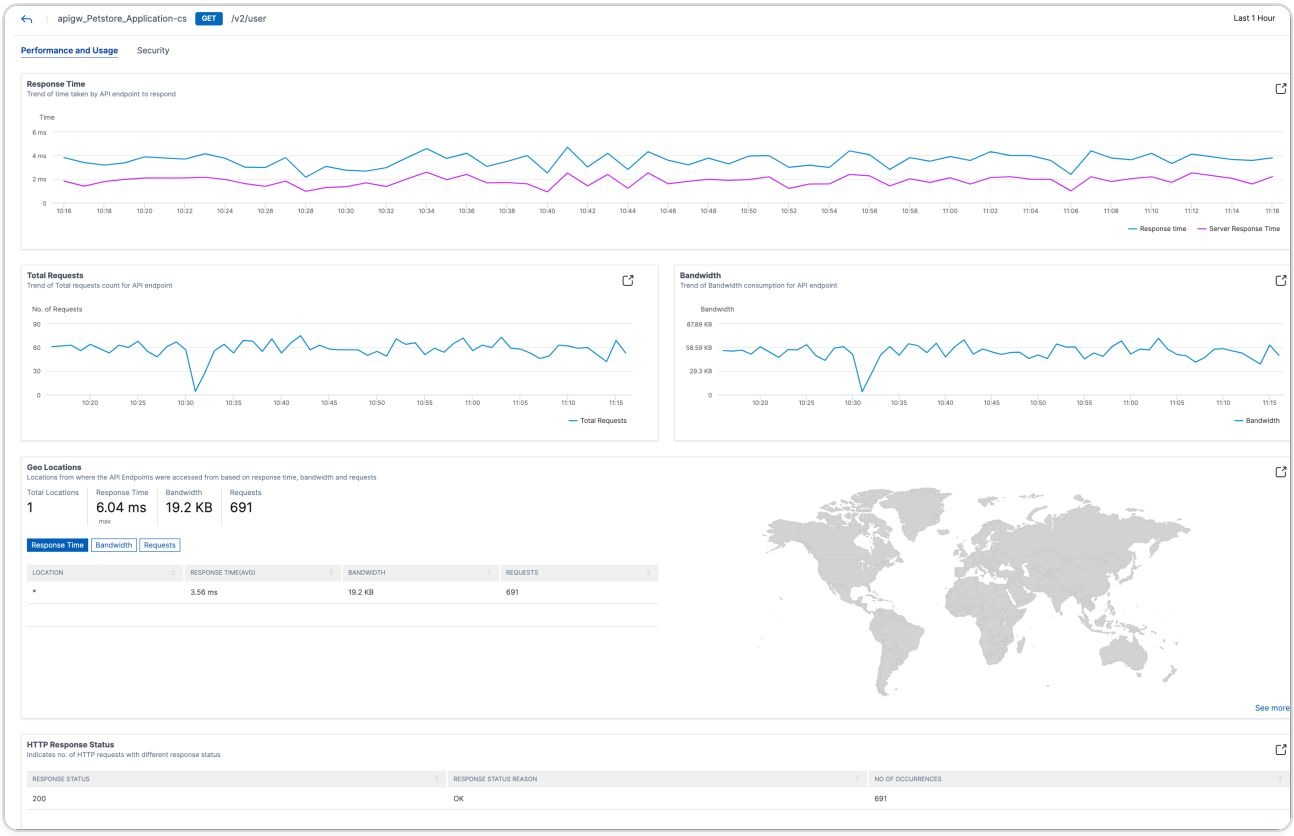


The API endpoints in API deployments are available as follows:



You can also select the required API endpoint to view its detailed analytics report.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

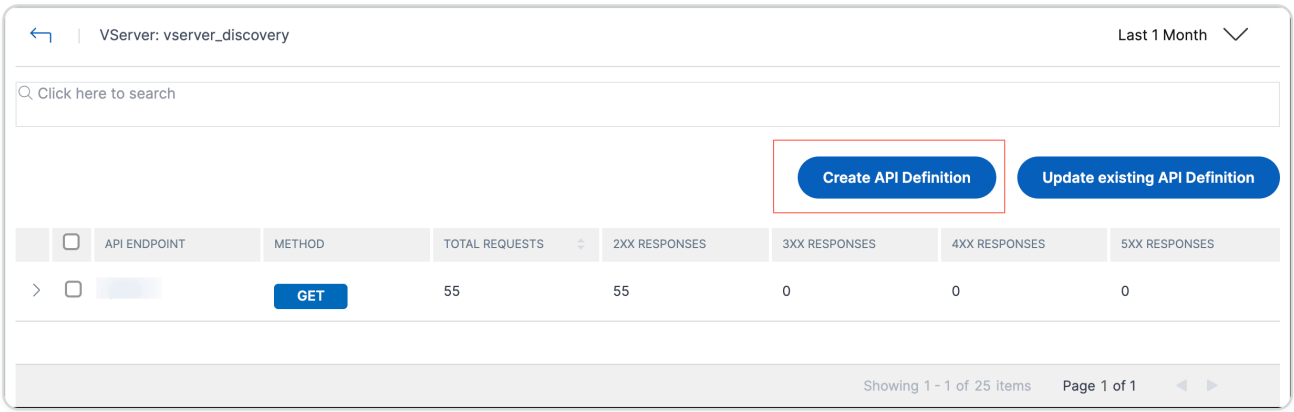


For more information about each section, see View API analytics.

Create API definitions from discovered API endpoints

To create API definitions from discovered API endpoints (API resources and methods):

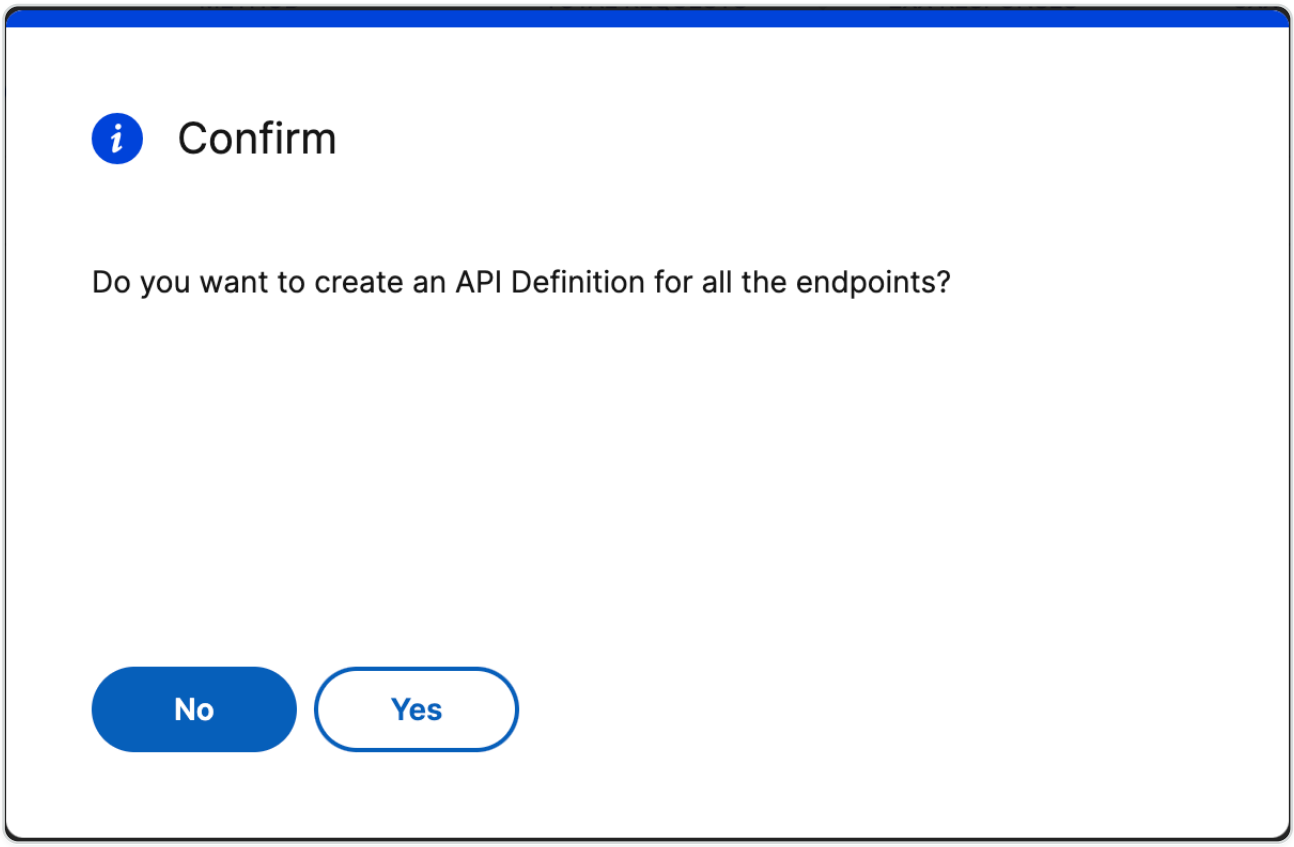
1. Navigate to **Security > API Security > API Discovery** to view the list of virtual servers and API deployments.
2. Click any virtual server in the **VServers** tab.
3. The virtual server page displays the list of discovered endpoints. Select any endpoint and click **Create API Definition**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If you do not select any endpoint and click **Create API Definition**, a pop-up window appears for you to confirm whether you want to create an API definition for all the endpoints. Click **Yes** to create the API definition with all the endpoints, else click **No**.



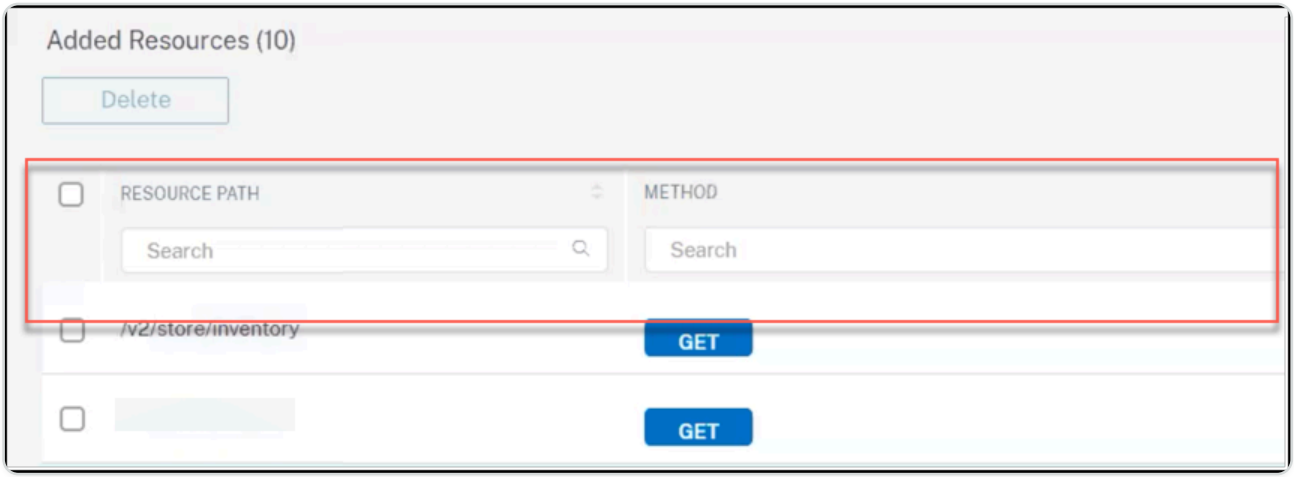
1. In **Create API Definition**, specify the following:
    - **Name** - A name for the API definition.
    - **API Definition** - A definition must include title, version, base path, and host. You can specify a domain name or IP address in the **Host** field.
    - **API Resources** - Add multiple API resources to your definition. Each resource has a path and supported method.
2. Click **Create Definition** to create the API definition.

NOTE:

If you want to edit an API resource path before adding it to the API definition, use the sort or search functionality for the API resources on the API definition screen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

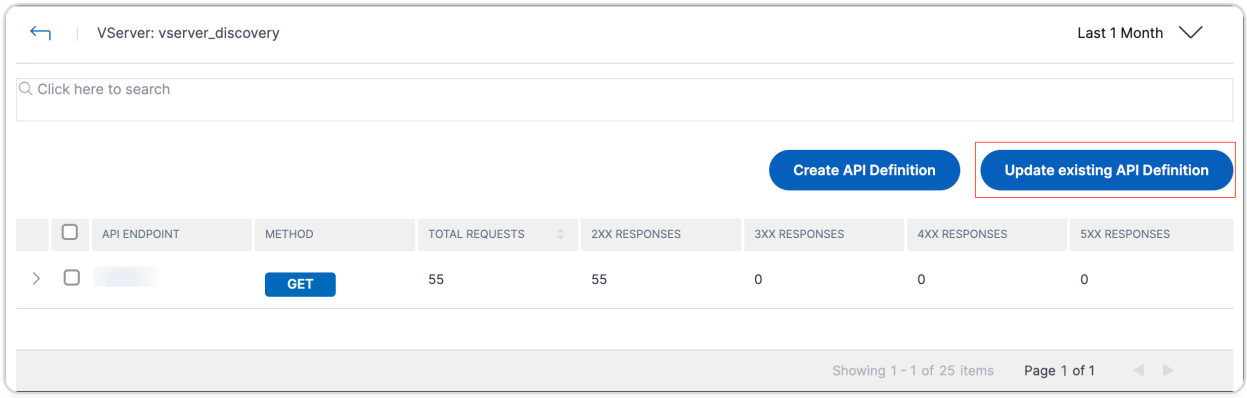
For example, consider an API resource named "/api/products/123-3243-2344334/reviews" where the path segment "123-3243-2344334" is a variable product id. You can now sort the API resources, add the resource path as "/api/products/{id}/reviews", and delete all the API endpoints with IDs such as "/api/products/123-3243-2344334/reviews".



Update an existing API definition with discovered API endpoints

To update an existing API definition with API endpoints (API resources and methods):

1. Navigate to **Security > API Security > API Discovery** to view the list of virtual servers and API deployments.
2. Click any virtual server in the **VServers** tab.
3. The virtual server page displays the list of discovered endpoints. Select the endpoint which you want to add to an existing API definition. Click **Update existing API Definition**.



4. From the **Select existing API Definition** drop-down list, select the API definition you want to update. Click **Update Definition**.
5. The **Update existing API definition** page appears. The **API Resources** section displays the following tables:

    - **Added Resources** - The API endpoints you selected

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Existing Resources** - The API endpoints already available in the API definition

> **NOTE:**
>
> If the same API endpoint is available in **Added Resources** and **Existing Resources**, the endpoint is added only once to the API definition.

6. Click **Update Definition**.

Undeploy an API instance

You can use the Undeploy option when you want to remove the API instance configuration from a NetScaler instance but keep the API instance objects in NetScaler Console as draft. This action sets the deployment status to In Draft. And, it can be applied only to the deployed API instance configurations.

> **IMPORTANT:**
>
> - Before you undeploy an API deployment, make sure all the associated API policies are undeployed or deleted. See, Undeploy an API policy.
> - Before you undeploy an API proxy, make sure all the associated API deployments are undeployed or deleted. See, Undeploy an API Deployment.

Undeploy an API policy

Follow the steps to undeploy an API policy:

1. In **Security > API Security > Policies**, select the policy that you want to undeploy.
2. Click **Undeploy**.

This action sets the **Policy Status** to In Draft.

Undeploy an API deployment

Follow the steps to undeploy an API deployment:

1. In **Security > API Security > API Deployments**, select the API deployment that you want to undeploy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Ensure all the associated policies of the selected deployment are undeployed or deleted.

2. Click **Undeploy**.

This action sets the **Deployment Status** to In Draft.

Undeploy an API proxy

Follow the steps to undeploy an API proxy:

1. In **Security > API Security > API Proxies**, select the API proxy that you want to undeploy.

NOTE:

You can share an API proxy with different API deployments. So, ensure all the associated deployments of the selected proxy are undeployed or deleted.

2. Click **Undeploy**.

This action sets the **Proxy Status** to In Draft.

Use APIs to manage API Security

You can access the APIs to create, configure, and deploy an API Security.

NOTE:

To understand how to use API Security APIs to configure the feature, see the Nitro API documentation.

	STEPS	RESOURCE URL
1	Create an API Definition	`https://adm.cloud.com/{customerid}/apisec/nitro/v1/config/apidefs`
2	Add an API proxy	`https://adm.cloud.com/apiproxies`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	STEPS	RESOURCE URL
3	Deploy an API instance using the API Proxy	`https://adm.cloud.com/apiproxies/{customerid}/deployments`
4	Add API policies	`https://adm.cloud.com/{customerid}/apisec/nitro/v1/config/policies/{id}`

Each API policy has a different `config_spec` object. It is an opaque object that contains a JSON dictionary to configure a `policytype` with specific values.

In this object, you can select an API resource and its methods using the following options:

- `api-resource-paths` - Specify the API resource paths and methods that are defined in an API definition.

  Example:

  ```
  {
  "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],
     "get": true,
     "post": false,
     "put": false,
     "delete": false
  }
  ```

- `custom-rules` - Specify the custom API resource paths and methods that might not exist in an API definition.

  Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{

"endpoints": ["/pet/categories", "/pet/findByName"],

   "get": true,

   "post": false,

   "put": false,

   "delete": false

}
```

With this configuration, the policy filters the incoming traffic requests that match the specified API resource paths.

For information about `config_spec` of each policy type, see API examples for policy types.

API examples for policy types

This section describes the supported API policy types and their configuration:

- Rate limit
- OAuth
- Basic authentication
- No authentication
- Bot
- WAF
- Header Rewrite
- URI Path Rewrite
- Authorization
- Deny

Rate limit

The following is an example configuration for the `Ratelimit` policy type. Specify the following configuration in the `config_spec` object:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{
    "policytype": "Ratelimit",
    "config_spec": {
        "api-resource-paths": {
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],
            "get": true,
            "post": false,
            "put": false,
            "delete": false
        },
        "custom-rules": {},
        "threshold": "10",
        "timeslice": "20000",
        "limittype": "BURSTY",
        "api-respondertype": "DROP",
        "header_name": "x-api-key",
        "per_client_ip": true
    },
    "order_index": 1,
    "policy_name": "ratelimit_policy"
}
```

For more information on each attribute, see Rate limit policy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OAuth

The following is an example API configuration for the `JWT Auth validation` policy type. Specify the following configuration in the `config_spec` object:

```
{

    "policytype": "JWT Auth Validation",

    "config_spec": {

        "api-resource-paths": {

            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],

            "get": true,

            "post": true,

            "put": false,

            "delete": false

        },

        "custom-rules": {},

        "jwks-uri": "https://uri.petstore.com",

        "issuer": "https://issuer.petstore.com",

        "audience": "petstore",

        "introspect-uri": "https://introspect.uri.com",

        "clientid": "client",

        "clientsecret": "clientsecret",

        "claims-to-save": ["scope", "scope2"],

        "allowed-algorithms": {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "hs256": true,
            "rs256": true,
            "rs512": true
        }
    },
    "order_index": 2,
    "policy_name": "Jwt_auth_policy"
}
```

For more information on each attribute, see OAuth policy

Basic authentication

The following is an example API configuration for the `BasicAuth` policy type:

```
{
    "config_spec": {
        "api-resource-paths": {
            "delete": false,
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],
            "get": true,
            "post": true,
            "put": false
        },
        "custom-rules": {}
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    },
    "order_index": 3,
    "policy_name": "Auth_BaSIC",
    "policytype": "BasicAuth"
}
```

For more information on each attribute, see Basic authentication policy.

No authentication

The following is an example API configuration for the `NoAuth` policy type:

```
{
    "config_spec": {
        "api-resource-paths": {
            "delete": false,
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],
            "get": true,
            "post": false,
            "put": false
        },
        "custom-rules": {}
    },
    "order_index": 4,
    "policy_name": "no_auth_policy",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "policytype": "NoAuth"

}
```

Bot

The following is an example API configuration for the `Bot` policy type:

```
{

    "config_spec": {

        "api-resource-paths": {

            "delete": false,

            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],

            "get": false,

            "post": false,

            "put": false

        },

        "bot-prof-name": "apisec_test_profile",

        "custom-rules": {}

    },

    "order_index": 5,

    "policy_name": "bot_policy",

    "policytype": "Bot"

}
```

For more information on each attribute, see Bot policy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WAF

The following is an example API configuration for the WAF policy type:

```
{
    "config_spec": {
        "api-resource-paths": {
            "delete": false,
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],
            "get": false,
            "post": false,
            "put": false
        },
        "waf-prof-name": "apisec_waf_profile",
        "custom-rules": {}
    },
    "order_index": 6,
    "policy_name": "waf_policy",
    "policytype": "WAF"
}
```

For more information on each attribute, see WAF policy.

Header Rewrite

The following is an example API configuration for the Header Rewrite policy type, specify this configuration in the `config_spec` object:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{

    "policytype": "Header Rewrite",

    "config_spec": {

        "api-resource-paths": {

            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],

            "get": true,

            "post": true,

            "put": false,

            "delete": false

        },

        "custom-rules": {},

        "rewrite-policy-header-field-name": "org",

        "rewrite-policy-header-field-val": "Citrix",

        "rewrite-policy-header-field-new-val": "Citrite"

    },

    "order_index": 7,

    "policy_name": "header_rewrite_pol"

}
```

For more information about each attribute, see Header Rewrite policy.

URI Path Rewrite

The following is an example API configuration for the URI Path Rewrite policy type:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{
    "config_spec": {
        "api-resource-paths": {
            "endpoints": ["/store/order", "/store/inventory"],
            "delete": false,
            "get": true,
            "post": true,
            "patch": false,
            "put": false
        },
        "custom-rules": {
            "delete": false,
            "endpoints": [],
            "get": false,
            "post": false,
            "patch": false,
            "put": true
        },
        "path-rewrite-params": [
        {
            "insert-segment-position": "beginning",
            "new-path-value": "v3",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "old-path-value": "v2",
            "action-type": "replace path segment"
        },
        {
            "insert-segment-position": "beginning",
            "new-path-value": "begin",
            "action-type": "insert path segment"
        },
        {
            "insert-segment-position": "end",
            "new-path-value": "end",
            "action-type": "insert path segment"
        },
        {
            "insert-segment-position": "before",
            "new-path-value": "before",
            "old-path-value": "store",
            "action-type": "insert path segment"
        },
        {
            "insert-segment-position": "after",
            "new-path-value": "after",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "old-path-value": "store",
            "action-type": "insert path segment"
        }
        ]
    },
        "order_index": 24,
        "policy_name": "eats_uripathrewrite",
        "policytype": "URI Path Rewrite”
}
```

For more information about each attribute, see URI Path Rewrite policy.

Authorization

The following is an example API configuration for the `Authorization` policy type. Specify the following configuration in the `config_spec` object:

```
{
    "policytype": "Authorization",
    "config_spec": {
        "api-resource-paths": {
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],
            "get": true,
            "post": true,
            "put": false,
            "delete": false
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        },
        "custom-rules": {},
        "claims": [{
            "name": "scope",
            "values": ["value1", "value2"]
        }]
    },
    "order_index": 8,
    "policy_name": "authorization"
}
```

For more information about each attribute, see Authorization policy.

Deny

The following is an example API configuration for the `Deny` policy type. Specify the following configuration in the `config_spec` object:

```
{
    "policytype": "Deny",
    "config_spec": {
        "api-resource-paths": {
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],
            "get": true,
            "post": true,
            "put": false,
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "delete": false

        },

        "custom-rules": {},

        "api-denytype": "RESPONDWITH"

    },

    "order_index": 9,

    "policy_name": "deny_policy"

}
```

In `api-denytype`, you can specify one of the following values:

- RESPONDWITH
- RESET

For more information about each attribute, see Deny rule.

Create WAF and BOT profiles using StyleBooks

When you can select a policy to an API resource in **API Gateway**, it allows you to define the traffic selection criteria to authenticate an API request. Also, it allows you to configure API security policies to the API traffic. For more information, see API Security.

You can configure WAF and BOT policies to an API resource. Before you configure a policy, ensure to create its profile in NetScaler Console. Use the following default StyleBooks to create a profile:

- API WAF Detection StyleBook
- API BOT Detection StyleBook

Create a WAF profile using StyleBooks

Perform the following to create a WAF profile:

1. In NetScaler Console, navigate to **Applications** > **Configurations** > **StyleBooks**. Search for the StyleBook by typing the name as `api-waf-profile`. Click **Create Configuration**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The StyleBook opens as a user interface page on which you can enter the values for all the parameters defined in this StyleBook.

2. Specify values for the following parameters:
   - **API WAF profile name** - A name to identify a WAF profile.
   - **Application Type** - Add application types to the profile. The WAF profile supports JSON and XML application types.
3. Optional, enable **Security Settings** to specify HTTP, JSON, or XML protection checks. You can also specify an Error URL to the NetScaler Web App Firewall. For more information, see Creating Web App Firewall profile.
4. Select the target NetScaler instance or instance group on which you want to deploy this configuration.
5. Click **Create**.

To configure a WAF policy, see Add policies to an API deployment.

Create a BOT profile using the StyleBook

Perform the following to create a BOT profile:

1. In NetScaler Console, navigate to **Applications** > **Configurations** > **StyleBooks**. Search for the StyleBook by typing the name as `api-bot-profile`. Click **Create Configuration**.

   The StyleBook opens as a user interface page on which you can enter the values for all the parameters defined in this StyleBook.
2. In **BOT Profile Name**, specify a name to identify a BOT profile.
3. Optional, enable the following options based on your requirements:
   - **Enable IP reputation check** - This option identifies the IP address that is sending unwanted requests. You can use the IP reputation list to preemptively reject requests that are coming from the IP with the bad reputation.
   - **Enable BOT Signatures** - Specify the BOT signature name. It blocks the requests from the specified signature.
   - **Allow List** - Specify IPv4 or subnet (CIDR) address. This option enables the BOT profile to bypass requests from the specified IPv4 or subnet address.
   - **Deny List** - Specify IPv4 or subnet (CIDR) address. This option enables the BOT profile to block requests from the specified IPv4 or subnet address.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Select the target NetScaler instance or instance group on which you want to deploy this configuration.
5. Click **Create**.

To configure a BOT policy, see Add policies to an API deployment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Applications

The application analytics and management feature of NetScaler Console enables you to monitor the applications through an application-centric approach. This approach helps you to:

- Check the score and analyze the overall performance of the applications
- Check for any issues that persist with the server or client
- Detect anomalies in the application traffic flows and take corrective actions

> **NOTE**
>
> Applications refer to one or more virtual servers that are configured on the instances (NetScaler).

You can monitor the applications for the time duration such as 1 hour, 1 day, 1 week, and 1 month.

Prerequisites

- Ensure you have added NetScaler instances in NetScaler Console.
- Ensure you have a valid license for your NetScaler instances. For more information, see Licensing.

Application overview

Applications can be:

- Discrete applications
- Custom applications
- Microservices applications (k8s_discrete)

Discrete applications

All virtual servers that are discovered in NetScaler® Console are referred to as discrete applications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Custom applications

The virtual servers under one category are referred to as custom applications. As an administrator, you must add custom applications based on a category. You can then manage and monitor the applications through the dashboard. You get an ease of monitoring specific applications that are grouped under one category.

For example, you can create a category for your data center1 and add its NetScaler instances. After you define a category and add the instance for your data center1, the application dashboard is displayed with a separate category, comprising all the applications related to your data center1.

Points to note

- The discrete applications that are added to the custom applications are removed from the discrete applications.
- All applications that are not added to any category are available as **"others"**.

Microservices applications

In a Kubernetes cluster, NetScaler provides an Ingress Controller for NetScaler MPX (hardware), NetScaler VPX (virtualized), and NetScaler CPX (containerized). For more information, see NetScaler Ingress Controller.

The discrete applications that are configured using the NetScaler CPX instances are referred to as microservices applications.

Application management and application dashboard

NetScaler Console enables you to manage applications and view application details from **Dashboard** page.

Manage applications

From the application dashboard, click **Manage Apps** to view all custom and discrete applications.

From the **Manage Applications** page, as an administrator, you can:

- Add applications
- View application details such as app name, app type, app category, associated virtual servers, associated services, and so on.
- Edit or delete custom applications

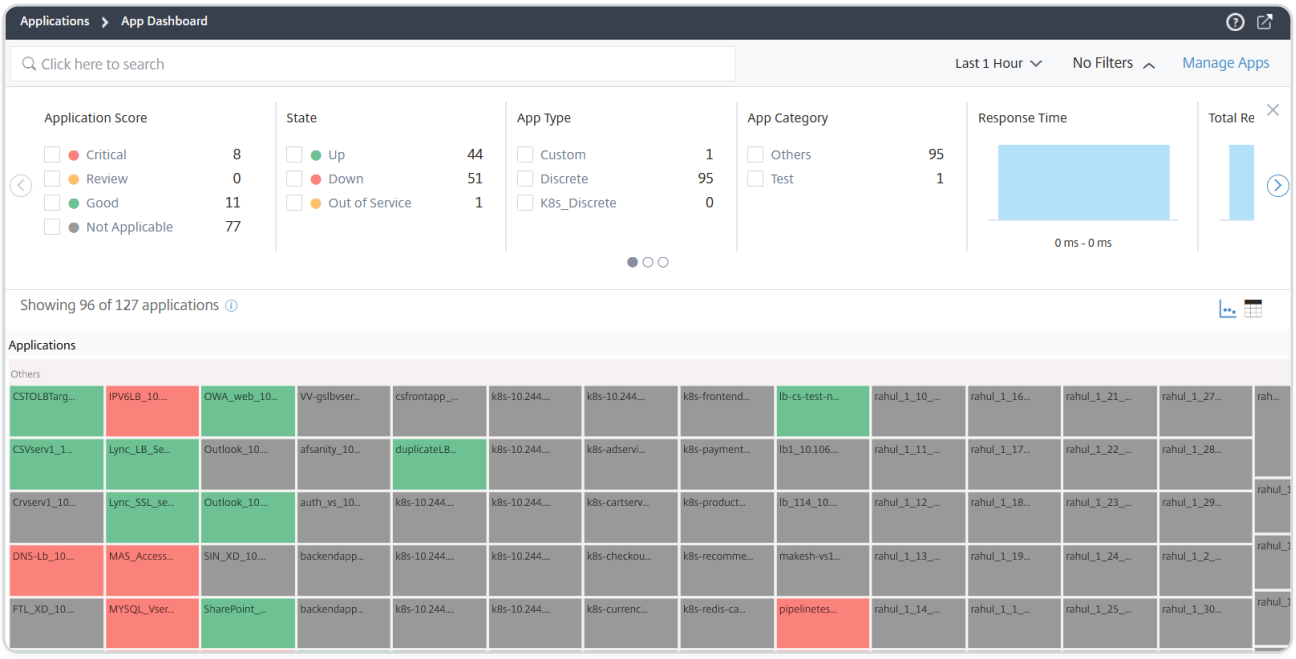
© 1997–2026 Citrix Systems, Inc. All rights reserved.

After you add, edit, or delete applications, the details are immediately reflected in the Applications page.

For more information, see Manage applications.

Application dashboard

Navigate to **Applications** > **Dashboard** to view the list of applications either in tabular view or in graph view.



All applications get displayed in the dashboard only after the applications start to populate data. From the dashboard, click an application to view detailed information of the application performance. For more information, see Application details.

If the application analytics is not displayed even after approximately 10–15 minutes duration, perform the troubleshooting steps at Troubleshoot App Dashboard.

Sort data on dashboard columns

In app dashboard, from the tabular view, you can sort data on the following columns:

- **App score**
- **App name**
- **Response time**
- **Total requests**
- **Throughput**
- **Data volume**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Client connection**
- **Server connection**

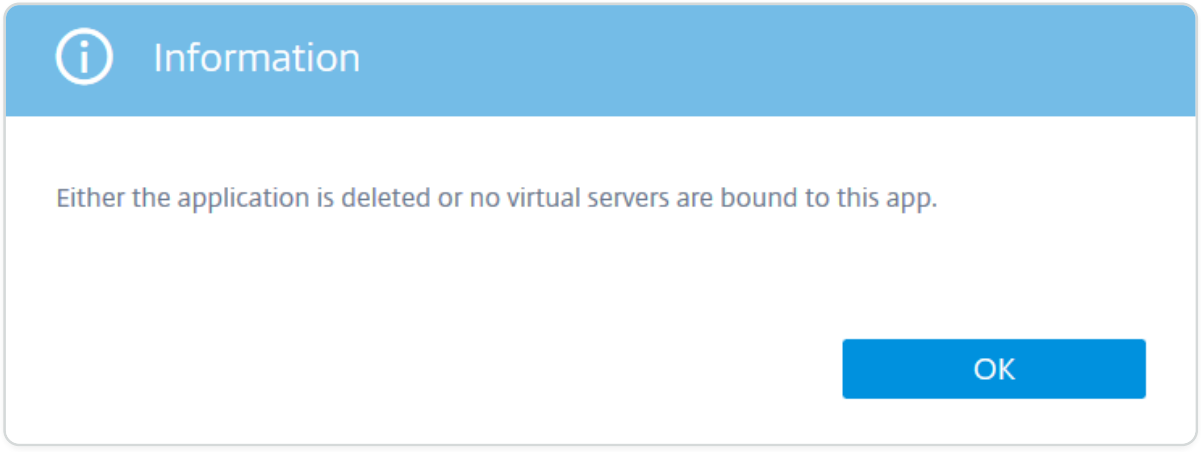
When you apply a sort, the dashboard gets organized with applications that are available across all pages. For example, if the dashboard comprises 5 pages, sort happens across all those 5 pages and the results displayed accordingly.

Updates in the new dashboard behavior compared to the earlier dashboard

- After you add or edit a custom application, it may take a few minutes to reflect the application in the dashboard.
- If you delete a custom application, the dashboard still displays the deleted application, until NetScaler Console has its analytics data (maximum of 1-month duration).

  Consider a scenario that you have created an application on Jan 2, 2020 and you have deleted the application on Jan 4, 2020. In this scenario:

  - The dashboard can still display the deleted application on Jan 4, 2020, when you select the time duration for the last 1-day, 1-week and 1-month.
  - The dashboard can still display the deleted application on Jan 5, 2020, when you select the time duration for the last 1 week and 1 month.
  - When the duration exceeds the app deletion date, the application is not displayed in the dashboard. That is, the dashboard is not displayed with the deleted application on Jan 6, 2020 (for the last 1 day), Jan 12, 2020 (for the last 1 week), and after February 5, 2020 (for the last 1 month).
  - When you click the deleted application from the dashboard, the following message is displayed.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

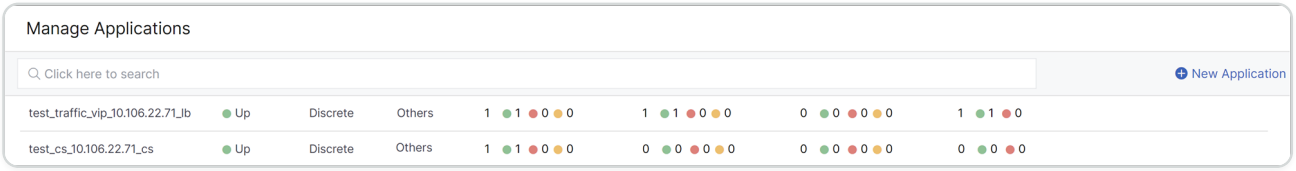
After you add an application, if the associated NetScaler instance is Down, out of service, or not reachable because of a temporary network glitch:

-The applications associated with the NetScaler instance are only visible in **Applications** page, but not in the dashboard.
-The applications are displayed in the dashboard after the NetScaler instance is up and running.

Manage applications

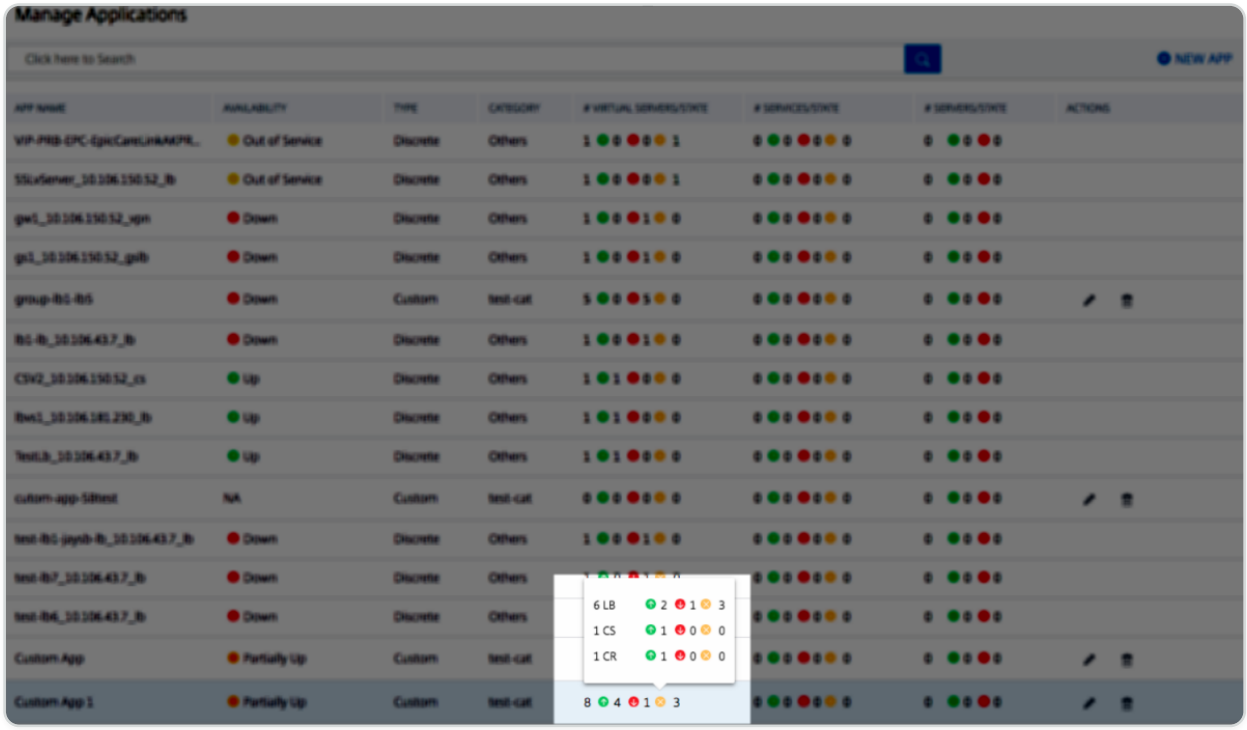
From the dashboard, click **Manage Apps** to view application details and add, edit, or delete custom applications.

View application details



- **App name** – Denotes the application name
- **State** – Denotes the current application status, such as **Up**, **Down**, **Partially Up**, **Out of Service**, and **NA**
  - **Up** – All virtual servers associated with the application are Up.
  - **Down** – All virtual servers associated with the application are Down
  - **Partially Up** – Either one virtual associated with the application is Down or out of service
  - **Out of Service** – All virtual servers associated with the applications are out of service
  - **NA** – No virtual servers is configured for the application
- **Type** – Denotes if the application belongs to Custom or Discrete
- **Category** – Denotes the application category that is grouped
- **Virtual server/state** – Denotes the total virtual servers configured and status of all virtual servers. Hover the mouse pointer to see the details such as total virtual servers, virtual server type, and virtual server status

© 1997–2026 Citrix Systems, Inc. All rights reserved.



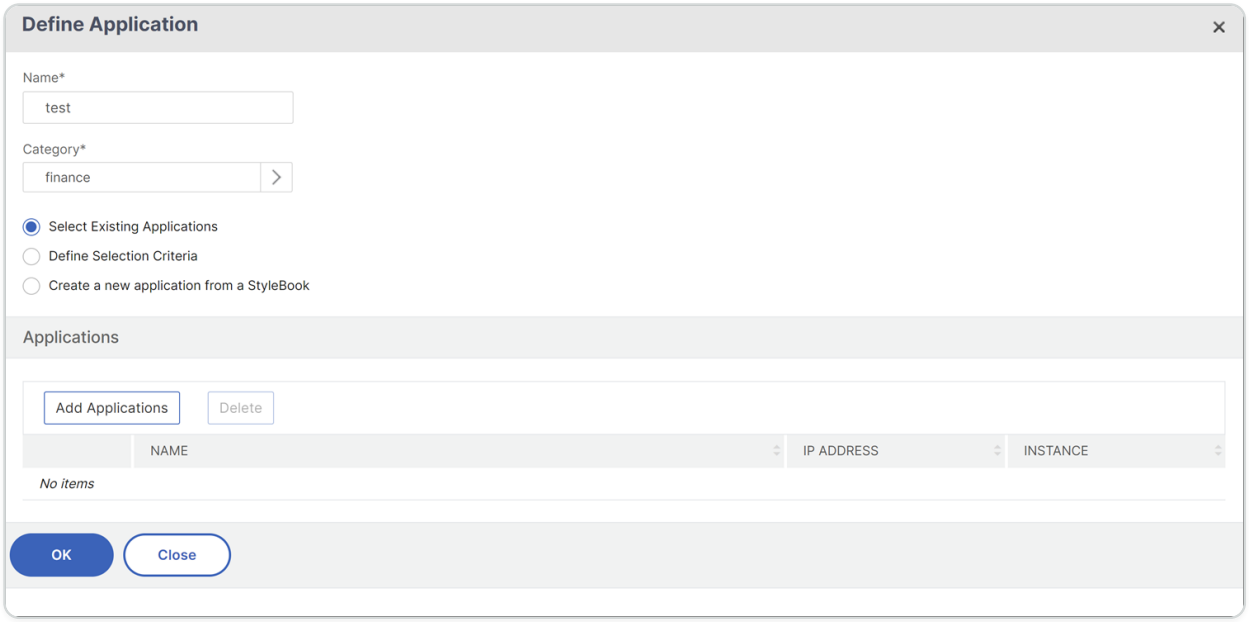
- **Services/state** – Denotes the total services configured and status of all services
- **Service Goups/state** – Denotes the total service groups configured and status of all service groups
- **Servers/state** – Denotes the total servers configured for the application and the status of all servers
- **Actions** – Enables you to either edit or delete the custom applications

Add an application

1. Click **New Application** to create an application

   The **Define Application** page is displayed

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Set the following parameters:

FIELD	DESCRIPTION
Name	The name of the custom application. For example, LB_TEST.
Category	The category that you can group the applications. Click to get the Application Category page. Select the category and click **Select**. To add a category:
	1. Click **Add**
	2. Enter a name of your choice.
	3. Click **Create**
Select Existing Applications	Enables you to select the existing applications added to the NetScaler instances.
Add Application	Displays all the virtual servers that are configured on the instances. Select the applications from the list and click **OK**.
Define Selection Criteria	Option to define application by virtual server range, or by origin server/service IP address range.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FIELD	DESCRIPTION
	- **Server.** Specify the server or service IP address, server name, or the port of the back-end server on which the applications are running. You can enter one IP address, a range of IP addresses, or a combination of both separated by commas. For example, you can enter 10.102.29.20, 10.102.43.10-60, 10.216.43.45.
	- **Virtual Servers.** You can specify either one of the following: the virtual server IP address, virtual server name, or the port of the back-end server on which the applications are running. You can enter one IP address or a range of IP addresses or a combination of both separated by commas. For example, you can enter 10.102.29.20, 10.102.43.10-60, 10.216.43.45.
Create an application from a StyleBook	Enables you to create an application using the StyleBook. For more information, see Create an application using the StyleBook.

3. Click **OK**.

NOTE:

Currently, Application Dashboard supports only load balancing and content switching virtual servers.

The application dashboard is now displayed with the category and all the applications are grouped underneath.

When you create an application using StyleBooks, confirm the required licenses consumption during the application deployment.

Click **Yes** to the confirmation message. The NetScaler Console allocates the required licenses to an application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create an application using the StyleBook

To create an application using the StyleBook:

1. In NetScaler Console, navigate to **Applications** > **Dashboard** and click **Manage Apps**.
2. Select the application category from the **Category** section. NetScaler Console allows you to define categories to group the user-defined applications. You can also add more categories if necessary.
3. Click to select **Create a new application from a StyleBook** and click **OK**.

   The Choose StyleBook page is displayed. This page contains all the default StyleBooks available in NetScaler Console.
4. Select the StyleBook. The **Configuration Details** page is displayed.
5. Type the values for all parameters in the StyleBook. You can also click View Definition to view the construct of the StyleBook before using it.

   For more information, see Use Default StyleBooks.
6. Click **Create**.

   A confirmation message appears to consume required licenses and deploy an application.
7. Click **Yes**.

You can also click **Dry Run** to check the configurations that NetScaler Console attempts to create on the selected NetScaler instance. This option is just for your test purpose to see the final check on the configurations. Even if Dry Run option is successful, the actual configuration on the selected NetScaler might still fail due to various reasons (IP conflict, instance not reachable, and so on.)

Edit or delete an application

From the **Manage Applications** page, you can either edit or delete the custom applications. Click the edit button to edit an application and click the delete button to remove the application.

Export reports of app dashboard and security dashboard

NetScaler Console allows you to take a snapshot of the current App Dashboard and export them as reports. At a frequent interval of time, the App administrators might need to use these reports to update on app usage and performance penalties.

With this feature, the administrators are able to extract this data as .png, .jpeg, or .pdf reports.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

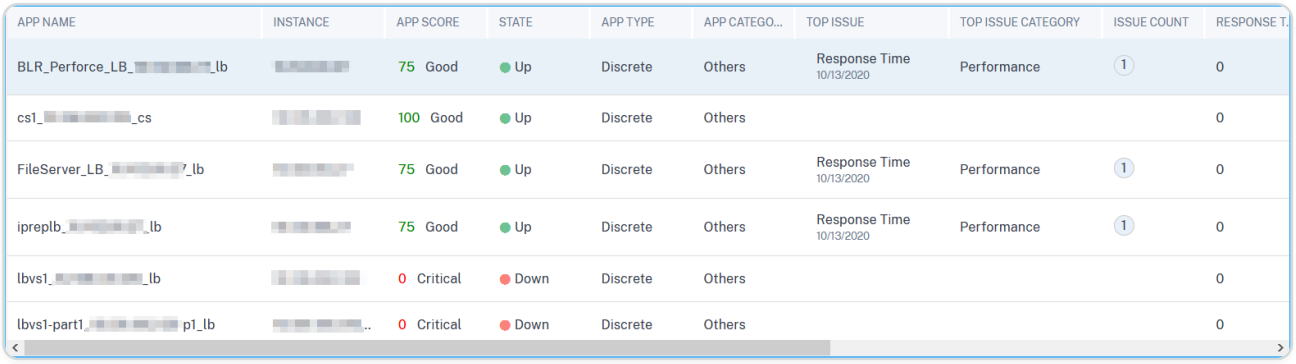
NOTE

Unlike other report export options in NetScaler Console, you can export the App Dashboard and Security Dashboard reports only as .pdf or .png files. The .csv format is not supported currently.

The report downloads onto your system. From the App Dashboard and App Security Dashboard pages, you can also navigate to second-level pages and export them as reports. Currently, you can download reports of only one application at a time.

View applications

By default, the application dashboard displays all applications. Depending upon your requirement, you can use the filter option to view applications.



APP NAME	INSTANCE	APP SCORE	STATE	APP TYPE	APP CATEGO...	TOP ISSUE	TOP ISSUE CATEGORY	ISSUE COUNT	RESPONSE T...
BLR_Perforce_LB_[redacted]_lb	[redacted]	75 Good	Up	Discrete	Others	Response Time 10/13/2020	Performance	1	0
cs1_[redacted]_cs	[redacted]	100 Good	Up	Discrete	Others				0
FileServer_LB_[redacted]?_lb	[redacted]	75 Good	Up	Discrete	Others	Response Time 10/13/2020	Performance	1	0
ipreplb_[redacted]_lb	[redacted]	75 Good	Up	Discrete	Others	Response Time 10/13/2020	Performance	1	0
lbvs1_[redacted]_lb	[redacted]	0 Critical	Down	Discrete	Others				0
lbvs1-part1_[redacted] p1_lb	[redacted]	0 Critical	Down	Discrete	Others				0

NOTE:

Starting from **14.1 20.x** build, you can view metrics details for applications that are created from the NetScaler admin partitions.

The dashboard displays the following application details:

- **App name** – Denotes the application name.
- **Instance** – Denotes the NetScaler instance.
- **App Score** – Denotes the application score and the status such as **Critical**, **Good**, **Fair**, and **Not Applicable**.
- **State** – Denotes the current availability of the application, such as **Up**, **Down**, **Partially Up**, **Out of Service**, and **NA**.
    - **Up** – All virtual servers associated with the application are Up.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - **Down** – All virtual servers associated with the application are Down.
  - **Partially Up** – Either one virtual associated with the application is Down or Out of Service.
  - **Out of Service** – All virtual servers associated with the applications are out of service.
  - **NA** – No virtual servers is configured for the application.

- **App Type** – Denotes the application type such as **Custom**, **Discrete**, or **Kubernetes services**.
- **App Category** – Denotes the category that is assigned to the application.
- **Top issue** – Denotes the issue that has the maximum error counts on the application.
- **Top issue category** – Denotes the category of the issue.
- **Issue count** – Denotes the total issue counts for the application.
- **Response time** – Denotes the average response time to respond from the application.
- **Total requests** – Denotes the total requests received by the application.
- **Throughput** – Denotes the total network throughput for the application. Throughput is calculated by the Req Bytes / Sec + Res Bytes / Sec for the virtual servers.
- **Data volume** – Denotes the total data processed by the application.
- **Client connections** – Denotes the average client connections established by the application.
- **Server connections** – Denotes the average server connections established by the application.

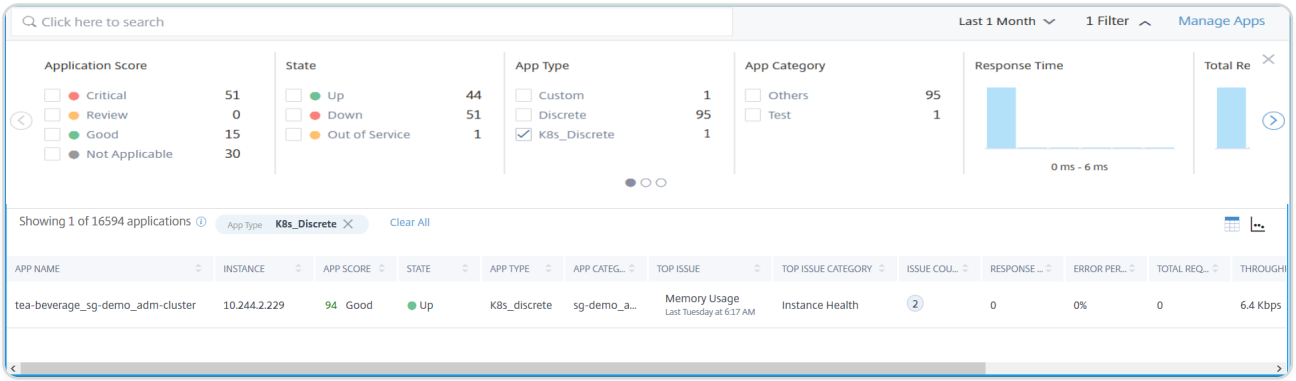
View microservices applications

To view the microservices applications, select the **K8s_Discrete** option under **App Type** filter.

You can view the microservice applications in **App Dashboard** as the following name format:

`<k8s service>_<k8s namespace>_<k8s cluster_name>`

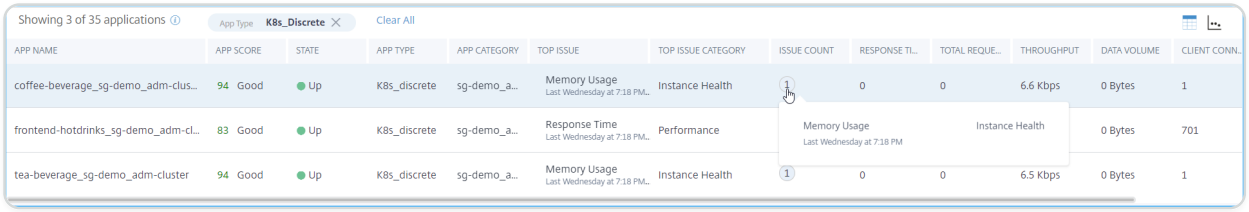
For example, `tea-beverage_sg-demo_adm-cluster` refers to a service named "tea-beverage" with the namespace of `sg-demo` in the cluster `adm-cluster`.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

The following metrics are displayed in dashboard for the selected time duration:

- **App Name** – Denotes the application name.
- **Instance** – Denotes the NetScaler CPX instance IP address.
- **App Score** – Denotes the application score.
  - **Critical** – App score is between 0 and < 40
  - **Review** – App score is between 40 and < 75
  - **Good** – App score is greater than 75
- **State** – Denotes the current application status.
- **App Category** – Denotes the cluster name where the application is hosted.
- **Top Issue** – Denotes the top issues that affects the current application score.
- **Top Issue Category** – Denotes the issue category affecting the application.
- **Issue Count** – Denotes the total issues affecting the application. Hover the mouse pointer on the issue count to see the overview of the issues.



- **Response Time** – Denotes the average response time received by the application.
- **Error Percentage** – Denotes the average error percentage of 5xx errors for the application.
- **Total Requests** – Denotes the total number of requests received by the application.
- **Throughput** – Denotes the total network throughput processed by the application.
- **Data volume** – Denotes the total data processed by the application. Data volume is calculated as the total request bytes and response bytes for the application.
- **Client connections** – Denotes the average client connections established by the application. This can also refer to the associated outgoing services connected with the selected service.
- **Server connections** – Denotes the average server connections established by the application. This can also refer to the associated incoming services connected with the selected service.

Click the **+** option to add or remove the options to be displayed in the dashboard.

Click an application to view the application details. For more information, Microservices application details

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure and associate an application to multiple custom applications

In **Application Dashboard**, you can configure an application and associate it to multiple custom applications. Using this feature, you can reuse the same application for multiple custom applications, rather than creating a separate application for each custom app.

Consider that you manage two e-commerce portals with the names **ComABC** and **ComCDE** respectively, and you wanted to use a payment gateway server with the name **PaymentApp** for both portals. In this scenario, you must:

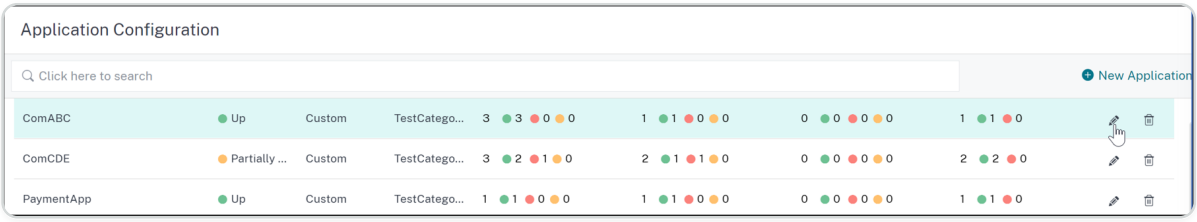
- Create two custom apps with the name **ComABC** and **ComCDE**.
- Create an application with the name **PaymentApp** and associate it to **ComABC** and **ComCDE**.

To implement this scenario, you must:

- Create the **Custom Apps (ComABC and ComCDE)**:
    a. Navigate to **Applications > Dashboard**, and click **Manage Apps**.
    b. Click **New Application**.
    c. Specify a name and category.
    d. Select the type for choosing the application. In this example, **Select Existing Applications** option is selected. For more information, see Add an application.
    e. Under **Applications**, click **Add Applications**.
    f. Select the applications from the list and click **OK** to create the custom app.
- Create the **PaymentApp**. For this, you must convert a discrete app to custom app:
    a. Navigate to **Applications > Dashboard**, and click **Manage Apps**.
    b. Click **New Application**.
    c. Specify a name and category.
    d. Select the type for choosing the application. In this example, Select Existing Applications option is selected. For more information, see Add an application.
    e. Under **Applications**, click **Add Applications**.
    f. Select the applications from the list and click **OK** to create the custom app.
- Next, you can use the **PaymentApp** and associate to **ComABC** and **ComCDE**.
    a. Navigate to **Applications > Dasboard**, and **click Manage Apps**.

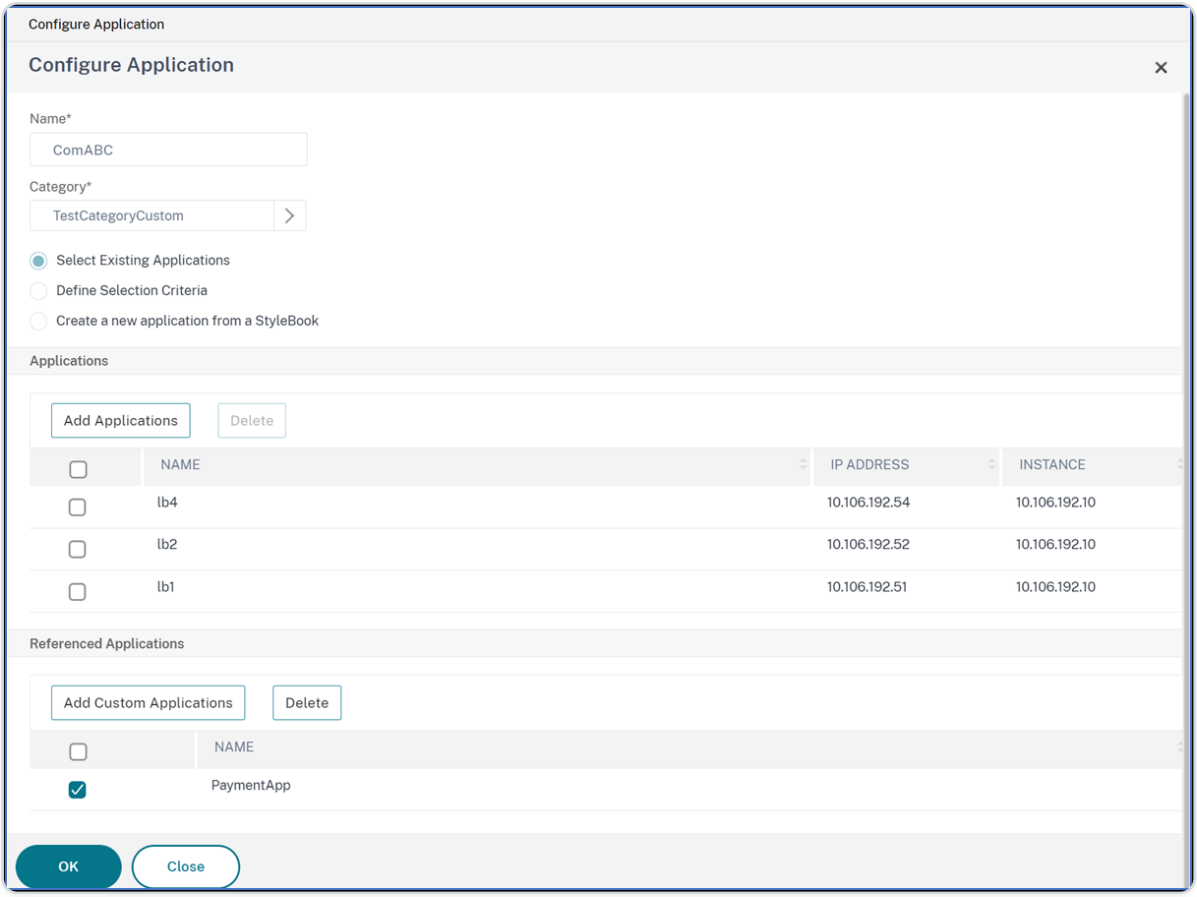
© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Locate the **ComABC** app and click **Edit**.



c. Under **Referenced Applications**, click **Add Custom Applications**, and select the **PaymentApp**.

d. The **PaymentApp** is now available under **Referenced Applications**. Click **OK** to associate the **PaymentApp** to **ComABC** custom app.



e. Repeat the same procedure for **ComCDE** custom app.

NOTE:

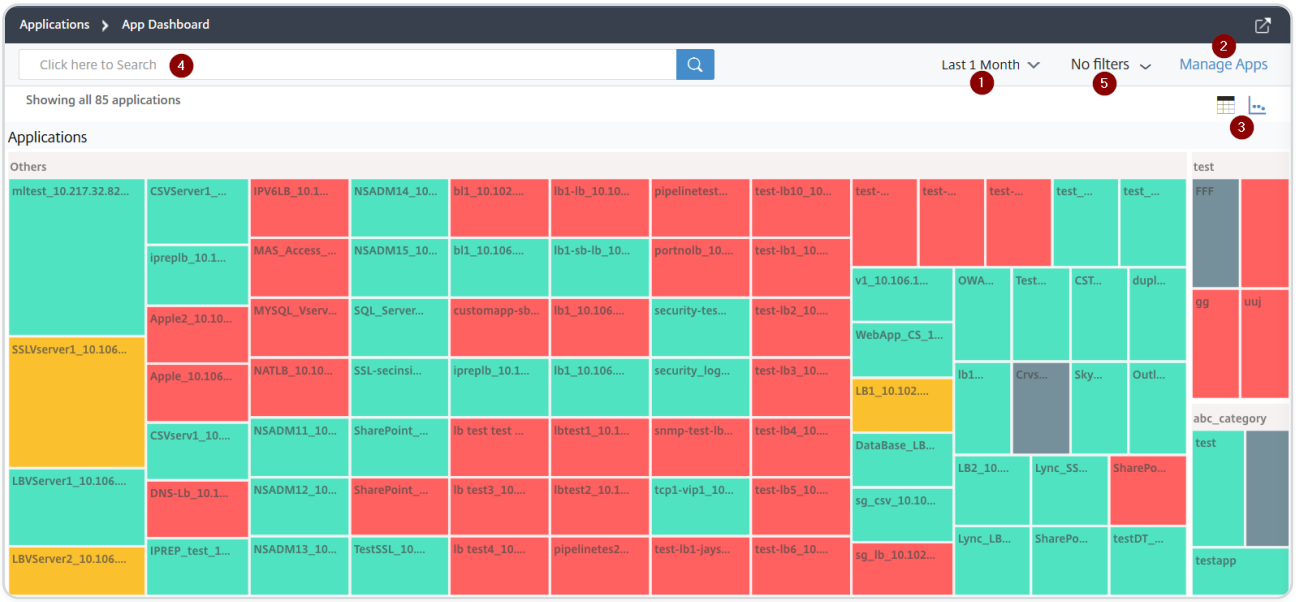
After the application is associated to the custom app, the final app score for the custom app is calculated based on the lowest score between the custom app and the referenced app. In this example, if **ComABC** app score is 85 and **PaymentApp** score is 69, the final score for **ComABC** app becomes 69.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Application dashboard overview

The application dashboard displays the discrete applications under **Others** and the custom applications that are grouped under their respective categories.

Navigate to **Applications** > **Dashboard** to view the app dashboard.



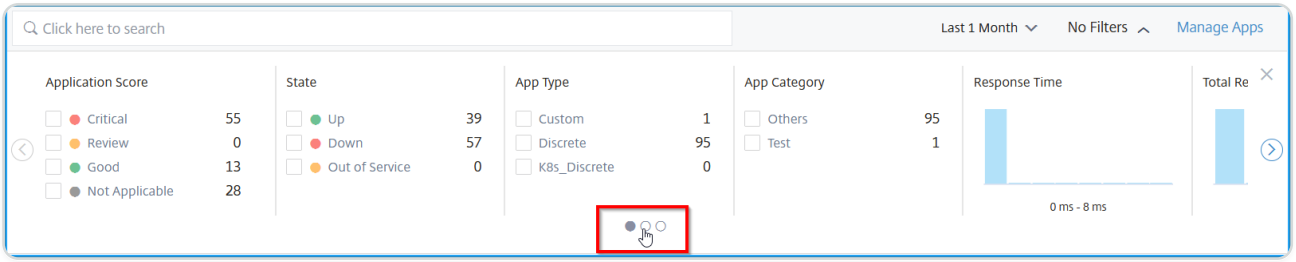
1 – Displays the application details for the selected time duration such as 1 hour, 1 day, 1 week, and 1 month.

2 – Enables you to manage applications and add new applications

3 – Enables you to view applications either in table view or in graph view

4 – Enables you to search an application using the search bar

5 – Enables you to apply filters to view applications. Click to view for details.



The carousel slider enables you an ease of access to all options.

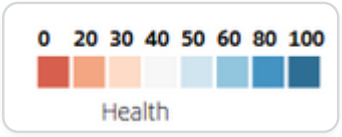
You can:

- Select to view applications based on the scores.
  - **Critical** – Application score is between 0 and < 40

© 1997–2026 Citrix Systems, Inc. All rights reserved.

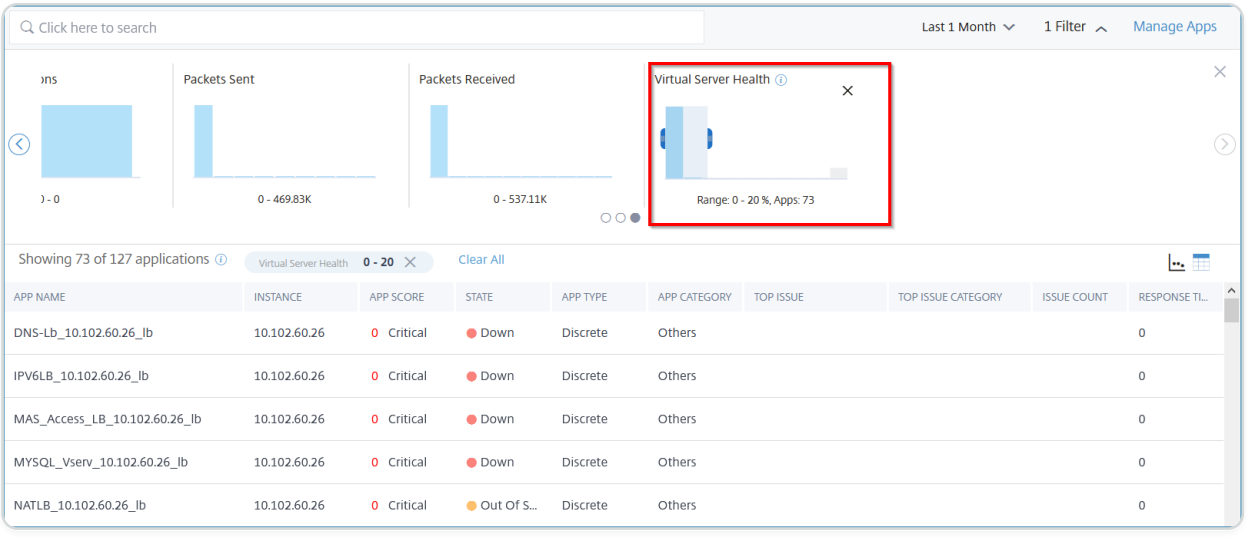
- **Fair** – Application score is between 40 and < 75
- **Good** – Application score is greater than 75
- **Not Applicable** – Either there are no virtual servers configured for the application or the virtual server type is not the load balancing or content switching.

The following table describes the differences between the earlier app score and the present app score.

APPLICATION SCORE (CRITICAL, REVIEW, GOOD, NOT APPLICABLE)	APP SCORE (EARLIER VIEW WITH COLOR LEGENDS)
Score is calculated as **100 minus penalty score of all application current issues**	Score is calculated as **100 – (App server resource + NetScaler system resource)**
Applications are displayed in colors such **Red (critical)**, **Orange (review)**, **Green (good)**, and **Grey (Not Applicable)**	Applications are displayed in color legends. 

- Select to view applications based on the application status such as Up, Down, and Out of Service
- Select to view applications based on the application type such as Discrete or Custom
- Select to view applications based on the categories grouped underneath
- Drag the histogram to apply filters and view applications.

For example, if you want to view applications that have Virtual Server Health between 0 and 20, drag the Virtual Server Health histogram to filter the results.

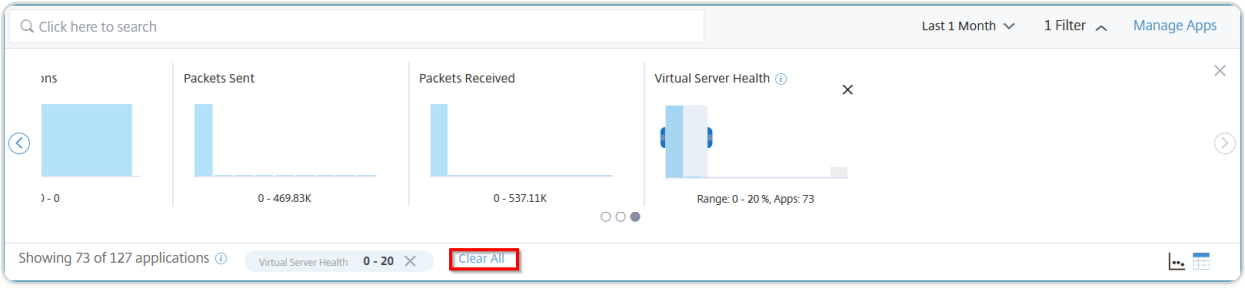


© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

You can also click the histogram to get the relevant applications displayed.

Click **Clear All** to clear the applied filter.



The following are the application summary for which you can apply filters:

- **Application score** – Enables you to view applications based on **Critical**, **Review**, **Good**, and **Not Applicable**.

  NOTE:

  By default, you can view applications that are in Critical, Review, and Good status. To view applications that are in N/A status, you must select the **Not Applicable** option.

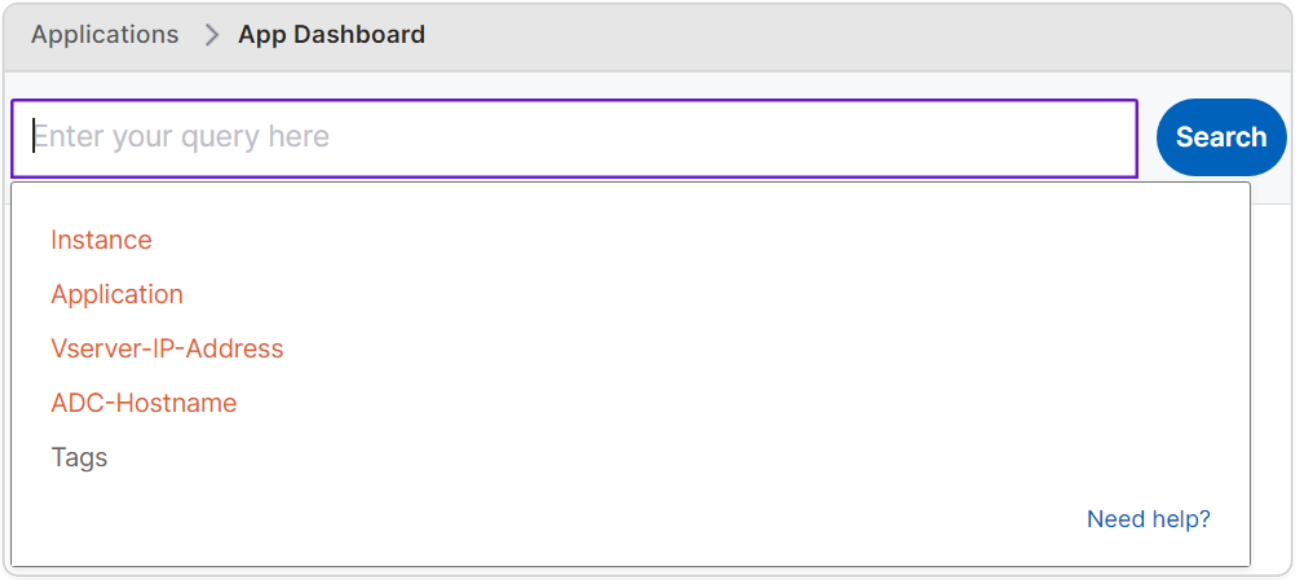
- **State** – Enables you to view application based on the application status such as Up, **Down**, and **Out of Service**.
- **Current Issues** – Enables you to get a list of applications impacted with a specific issue, by choosing the issue type such as **Performance**, **Instance Health**, **Config**, and **System Resources**.
- **App Type** – Enables you to view applications based on the application type such as **Custom**, **Discrete**, and **Kubernetes services**.
- **App Category** – Enables you to view the applications based on the category assigned.
- **Response Time** – A histogram that displays the average response time received by the applications.
- **Total Requests** – A histogram that displays the total number of requests received by the applications.
- **Throughput** – A histogram that displays the total network throughput processed by the applications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Data Volume** – A histogram that displays the total data processed by the applications. Data volume is calculated by the total request bytes and response bytes for the applications.
- **Client Connections** – A histogram that displays the average client connections established by the applications.
- **Server Connections** – A histogram that displays the average server connections established by the applications.
- **Packets Sent** – A histogram that displays the total packets sent by the applications.
- **Packets Received** – A histogram that displays the total packets received by the applications.
- **Virtual Server Health** – A histogram that displays the total applications between the score range 0% to 100%. A virtual server health is (%) of active services associated with the application. For example, if a virtual server is configured with 2 services and if one of them is down, the score is 50%.

Search and filter results using the search bar

You can place the mouse pointer on the search bar and select the category to refine the search.

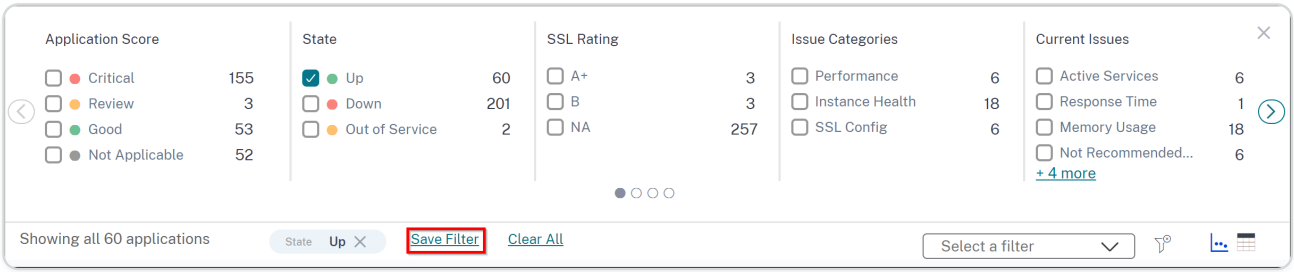


Save filter

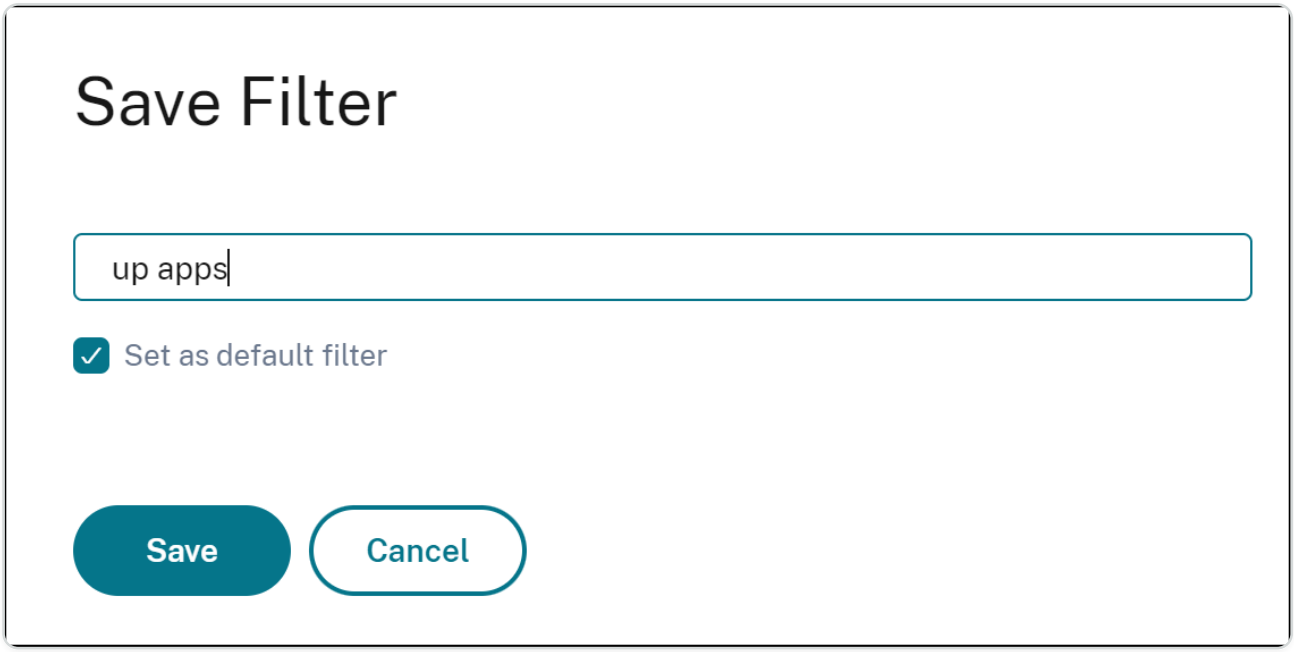
You can apply filters in the app dashboard and save filters. You can then select the filter name from the list and view the customized dashboard whenever required.

Consider that you wanted to create a filter for applications that are in the **Up** status. In **App Dashboard**, after you apply the filter, click **Save Filter**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

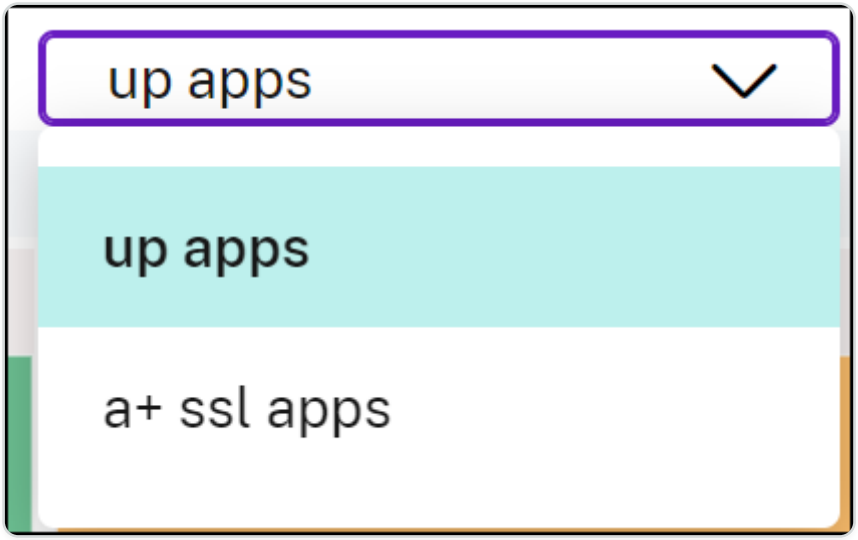


Provide a name of your choice and click **Save**.



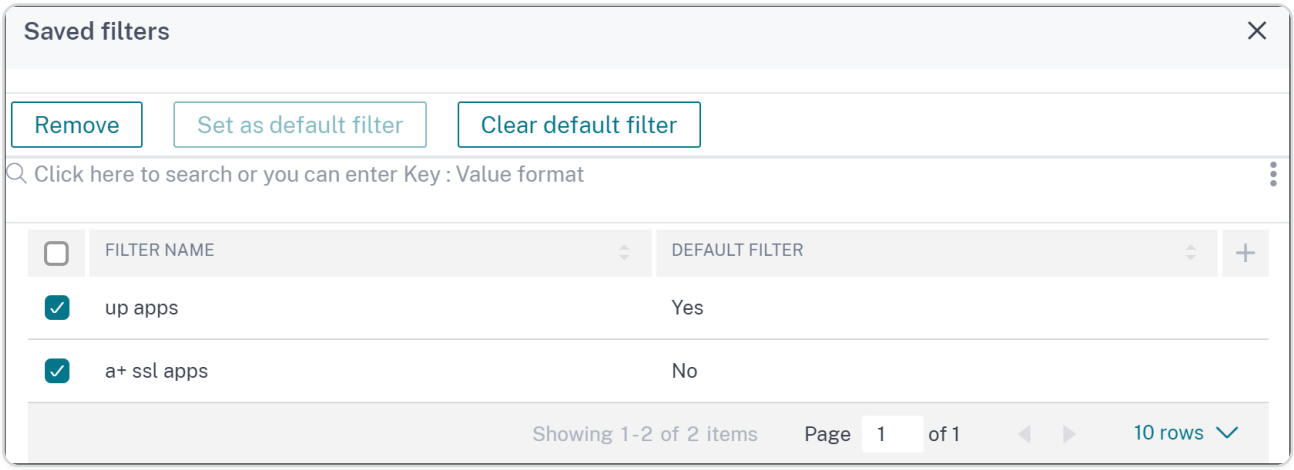
You can also select **Set as default filter** to have this filter as a default view in the app dashboard.

You can save multiple filters and select the filter name from the list to view the customized dashboard whenever required.



To remove the default filter or remove the filter, click the filter icon next to the filter list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



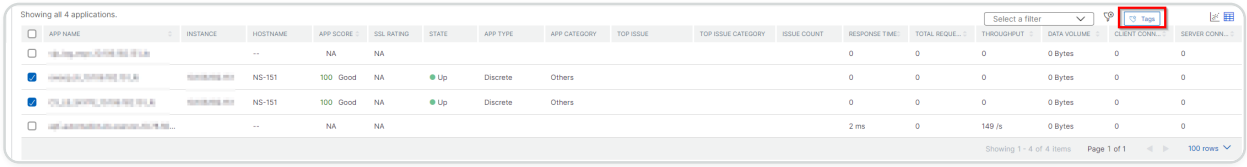
Create and apply tags to applications

If you have a large number of applications, you can create and apply tags to applications. These tags improve the search functionality.

Example:

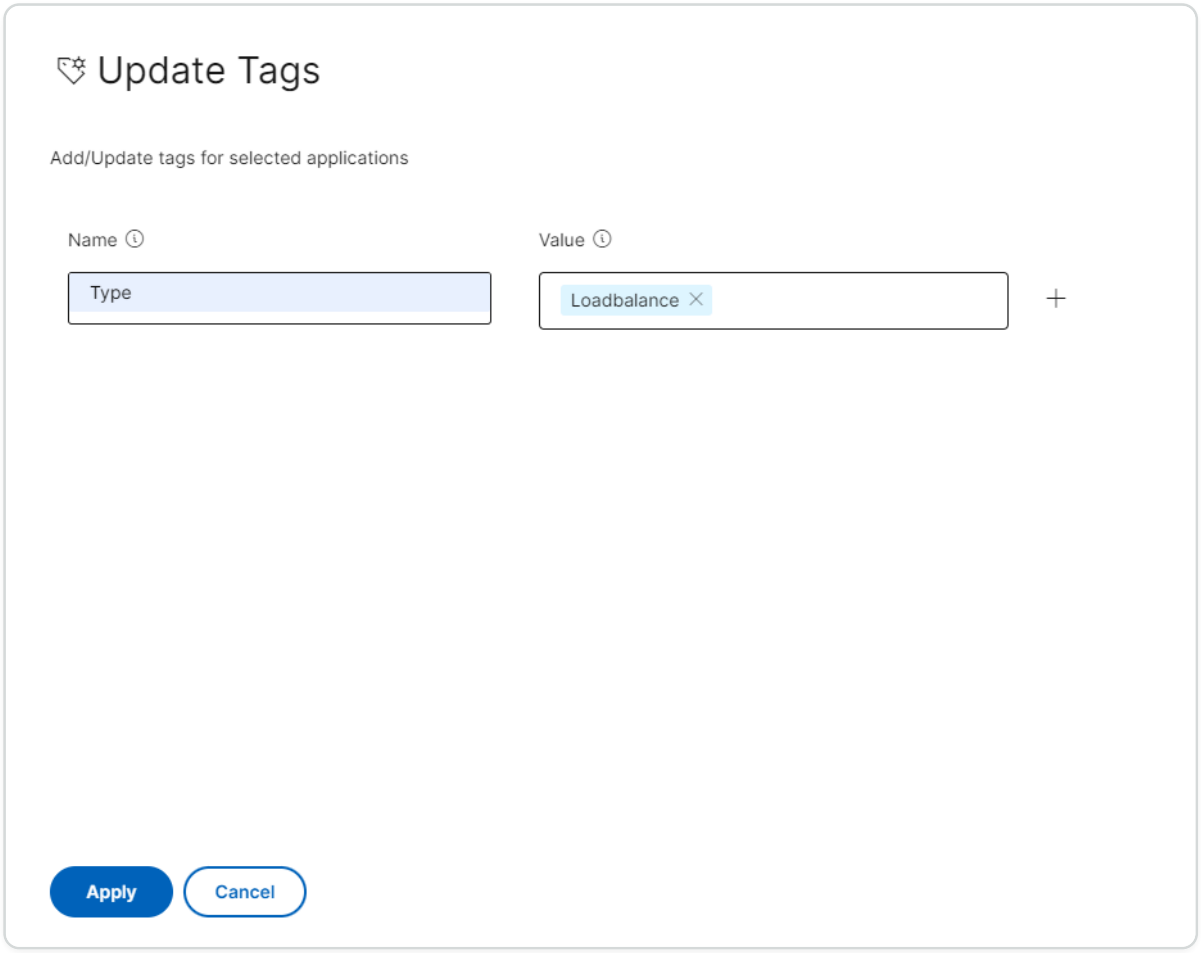
The following procedure lists the steps to create tags for the load balancing applications:

1. In **App Dashboard**, select the load balancing applications that you want to create tags and click **Tags**.



2. In the **Update Tags**:
    - Specify a name of your choice. For example: **Type**.
    - Specify the value that enables you to assign the tags. You can also enter multiple values. For example: **Loadbalance**.
    - Click **Apply**.

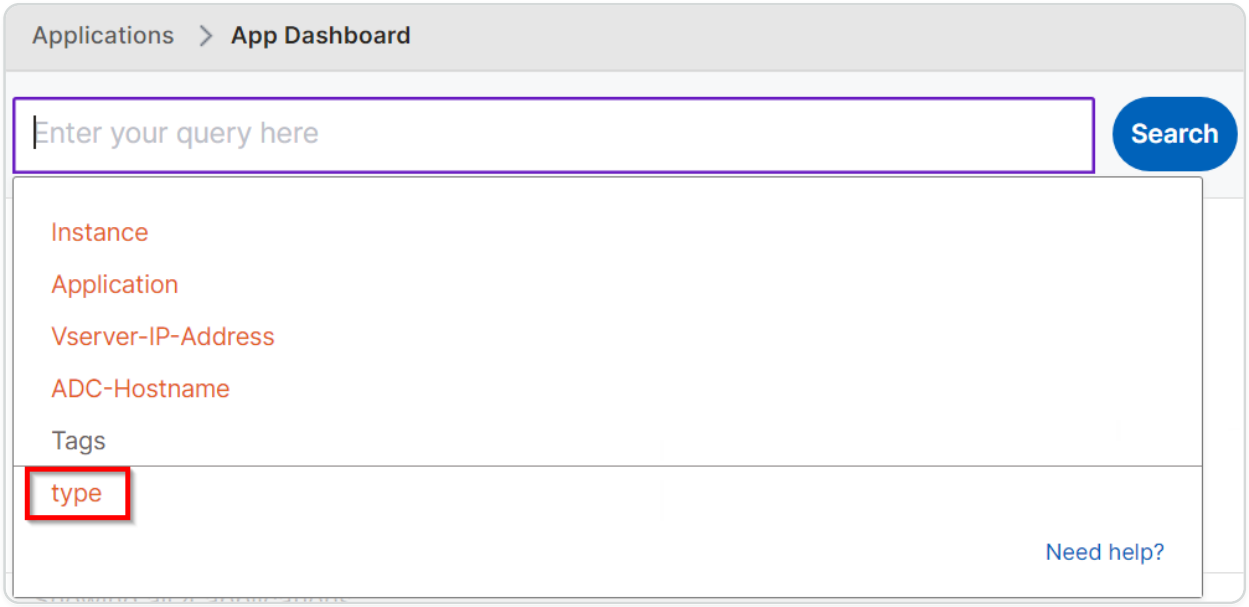
© 1997–2026 Citrix Systems, Inc. All rights reserved.



The tag is created.

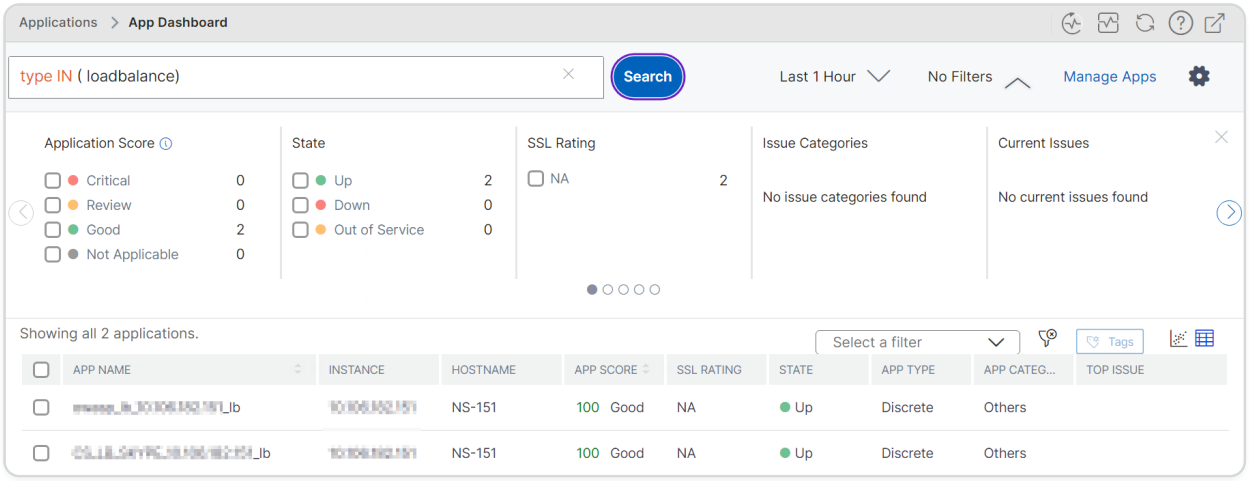
To apply tags and retrieve the load balancing applications:

1. In the app dashboard search bar, click inside the textbox to view the created tag and select the tag name.



2. Select the operator (**IN**) and the value that is created, and then click **Search**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



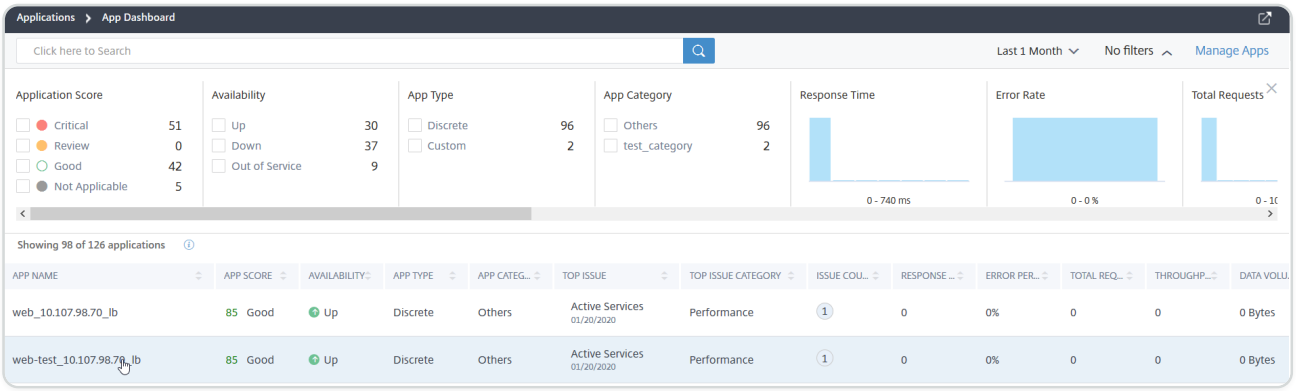
All the load balancing applications that are tagged under **Loadbalance** are listed. Similarly, you can create tags for other applications.

Application details

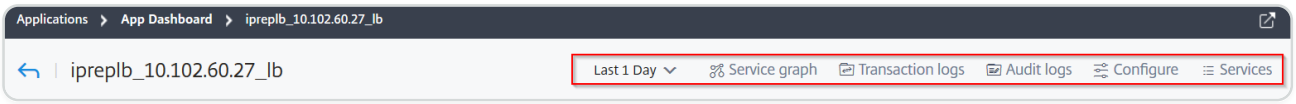
NOTE:

Starting from **14.1 20.x** build, you can view metrics details for applications that are created from the NetScaler admin partitions.

Click an application from the dashboard to drill down for further detailed information.



The selected application page is displayed.



From the application details page:

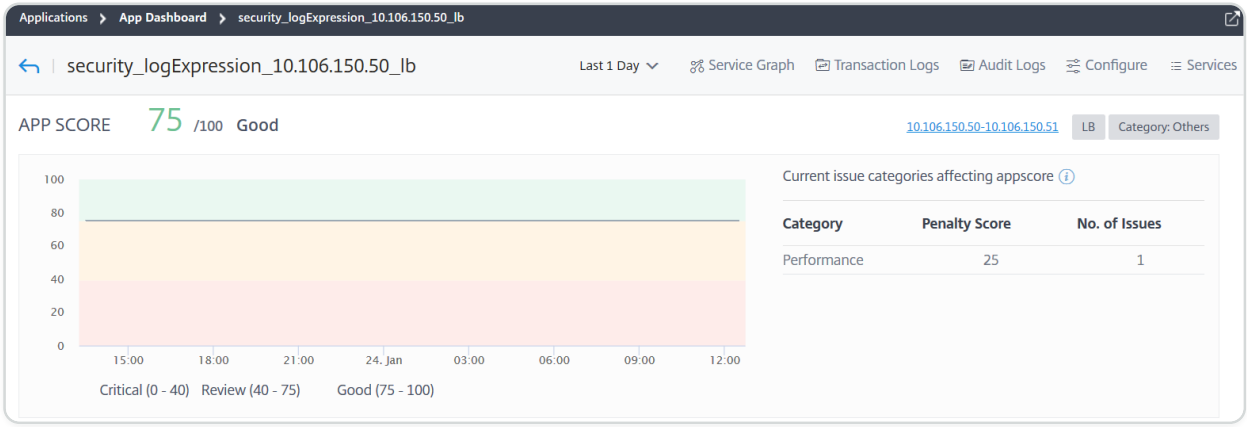
- Select the time duration from the list to view details for the specific time duration
- Click **Service Graph** to view service graph for the selected application. For more information, see Service Graph for Applications

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Click **Transaction Logs** to view the detailed transactions for the selected application
- Click **Audit logs** to view the detailed audit log information
- Click **Configure** to view or edit the service and service group configuration for the selected application
- Click **Service** to view services that bound to the application

After you select the time duration, the following application details are displayed:

- **App Score** – The application score for the selected time duration. The final score is calculated as **100 minus total penalty**.



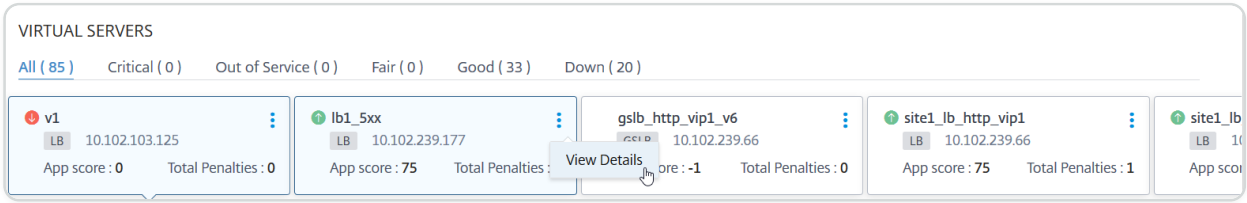
This dashboard also enables you to view the current issues that are affecting the app score. You can view the issues details under Issues.

- **Virtual Servers** –

> **NOTE**
>
> The **Virtual Servers** section is displayed only for the custom applications. For discrete applications, click the **IP address** to view the virtual server details.

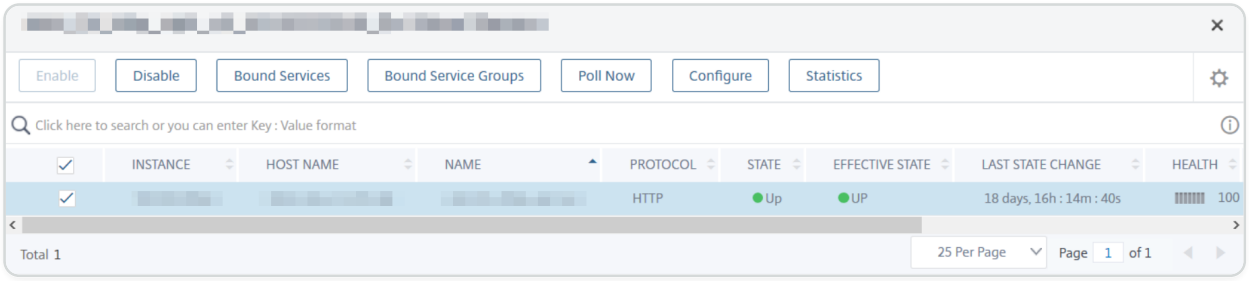


Displays all virtual servers associated with the custom application

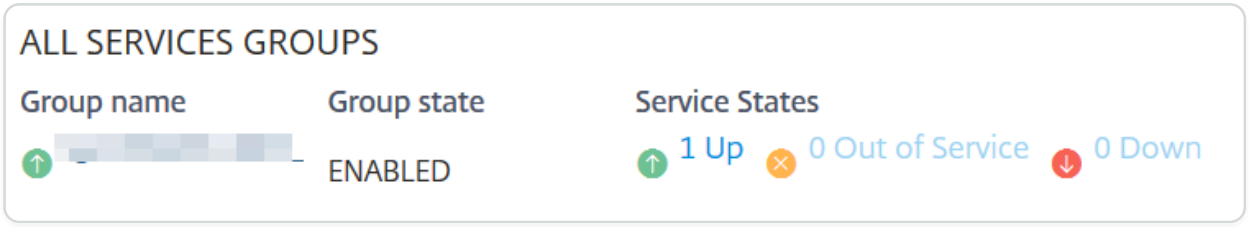


Click **View Details** to view and manage the virtual server settings.

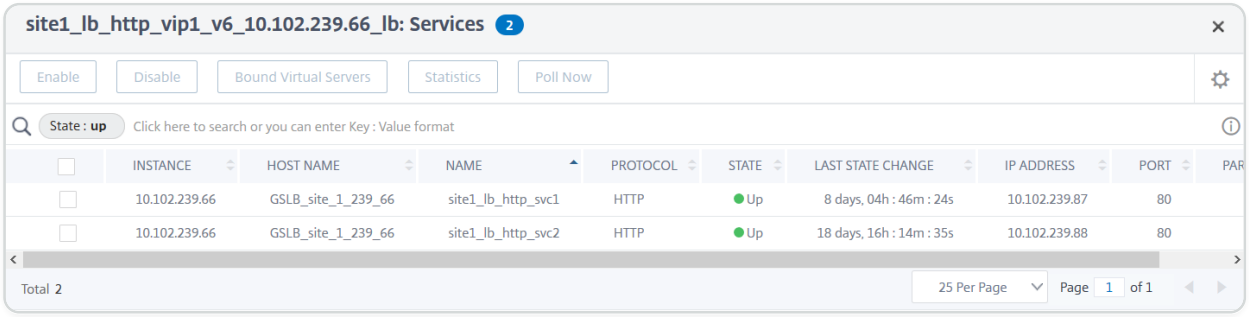
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **All Services** – The services that are bound to the application



Click to view the service details and to manage the service settings



- **Issues** – The issues that are applicable for selected application. You can view the following issues along with its category:

PERFORMANCE	INSTANCE HEALTH	CONFIG	SYSTEM RESOURCES
Response Time	Average CPU Usage	Unstable Server	Improper persistence type
Active Services	Memory Usage	Unusually large HTTP packets	NIC Card Saturation
Low Session Reuse		TCP reassemble queue limit hits	
App CPU Usage			
SurgeQueue Buildup			

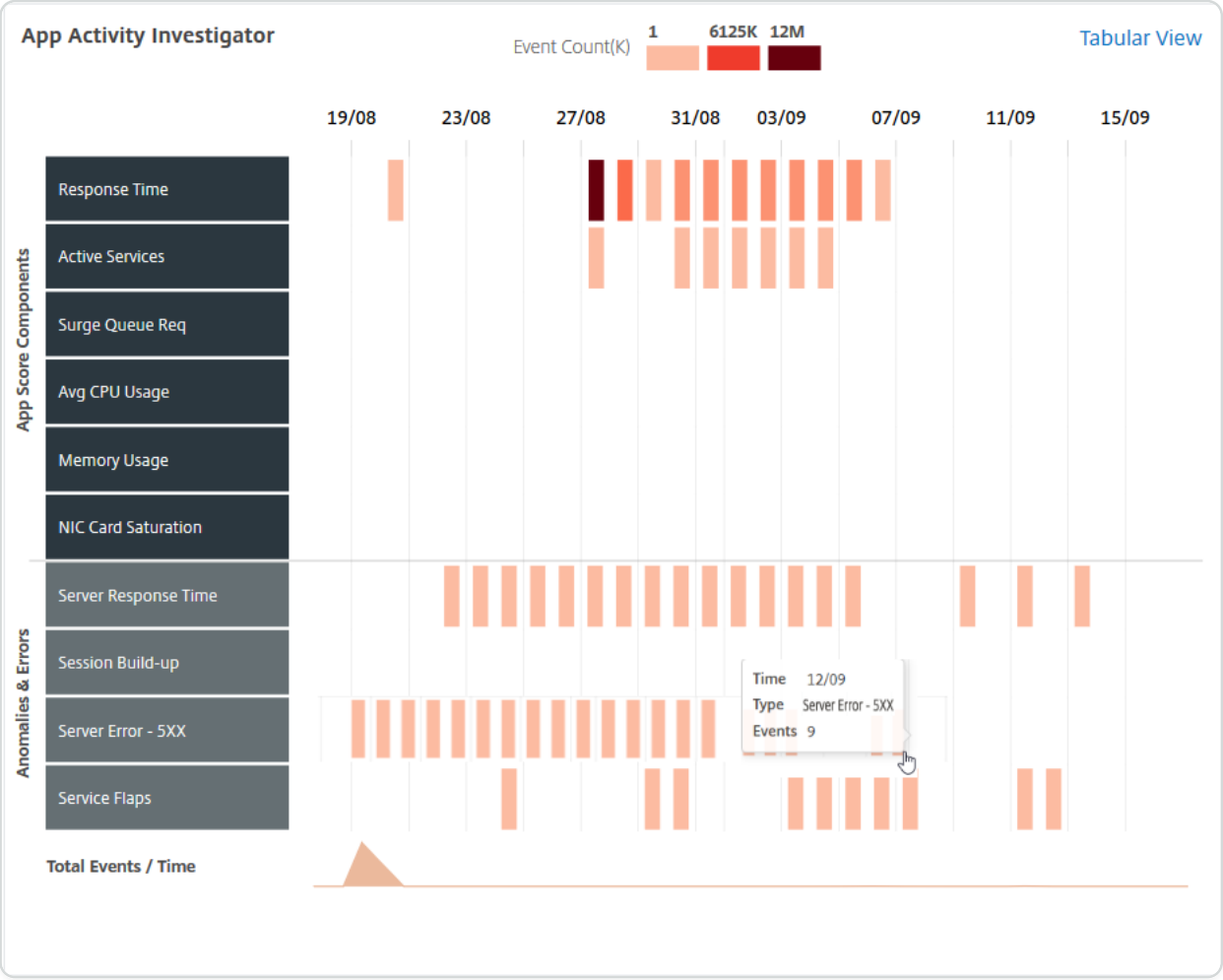
© 1997–2026 Citrix Systems, Inc. All rights reserved.

PERFORMANCE	INSTANCE HEALTH	CONFIG	SYSTEM RESOURCES
SSL Real Time Traffic			
Session buildup			
Server response time			
Service flaps			

Click each issue to check details such as detection message, when the issue has occurred, Recommended actions, and details.

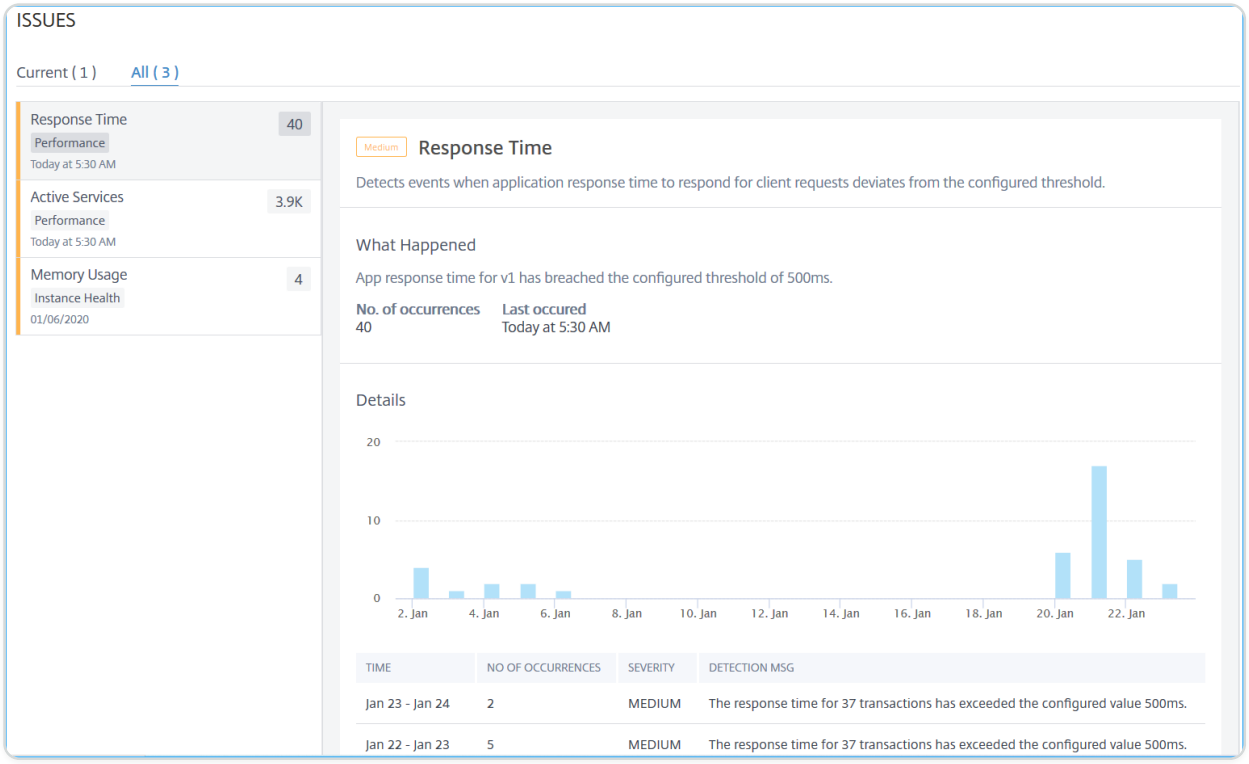
For more information, see Performance indicators for application analytics.

The following image is the earlier view of **App Activity Investigator** page:



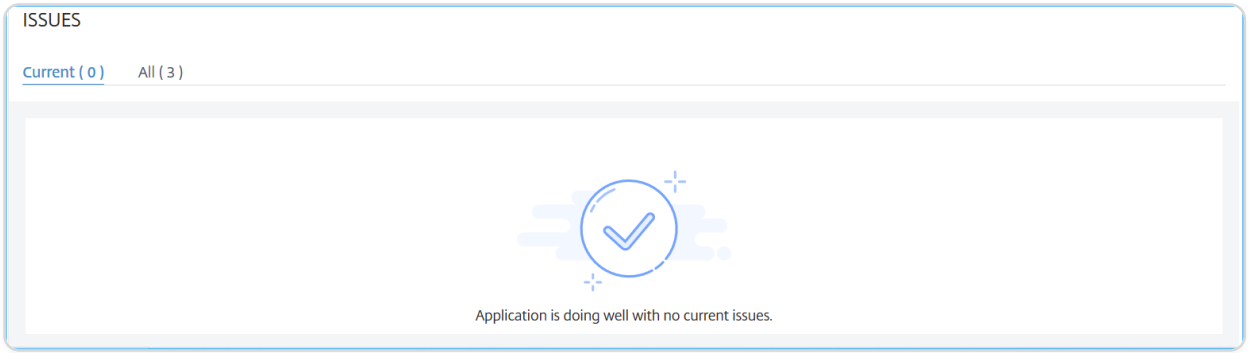
© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can now view all issues in the **Issues** section, along with the category that you were able to view in **App Activity Investigator** page.



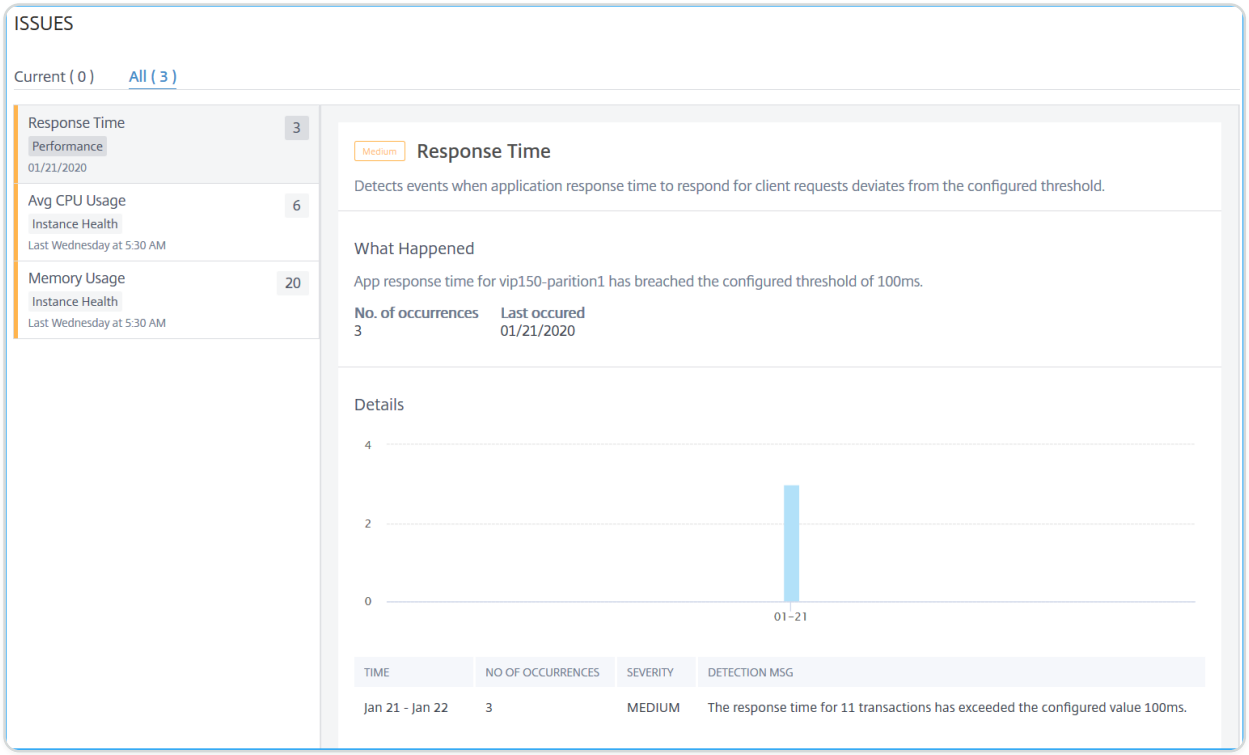
- The issues that display in **Current** tab refer to the application issues for the select time duration.
- The issues that display in **All** tab refer to total application issues.

The following example is the application issues for 1-day duration. The **Current** tab indicates no current issues impacting the app score.



The **All** tab displays the total issues detected for the 1-day duration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

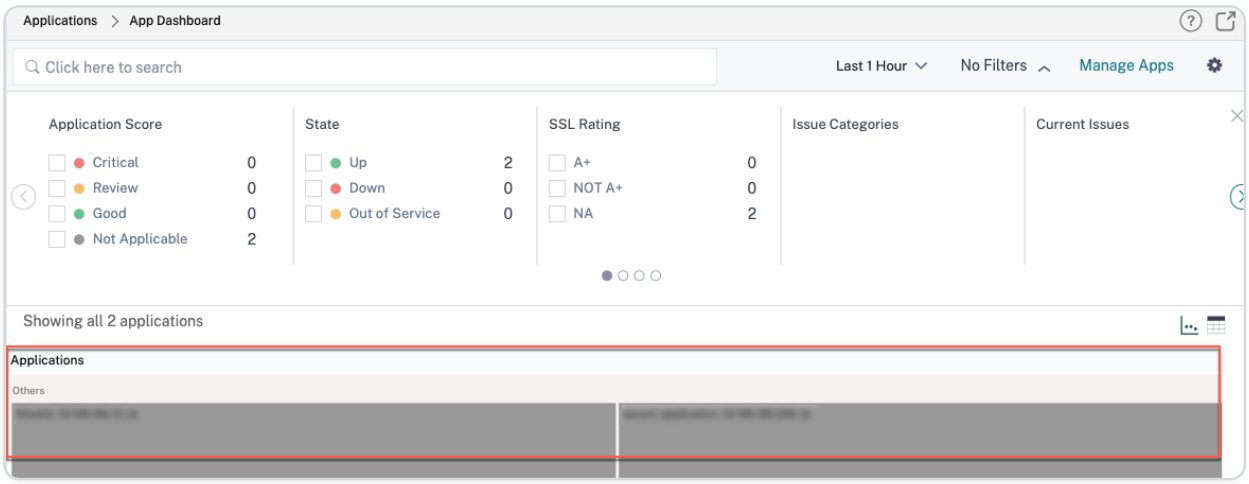


Check monitor status of an application

You can use the application dashboard in the NetScaler Console GUI under **Applications > Dashboard**, to view the health monitor status of an application and the failure message if any. You can bind health monitors can be bound to service or service group of an application, and a service or service group can have multiple monitors bound to it. Monitors help you monitor your services.

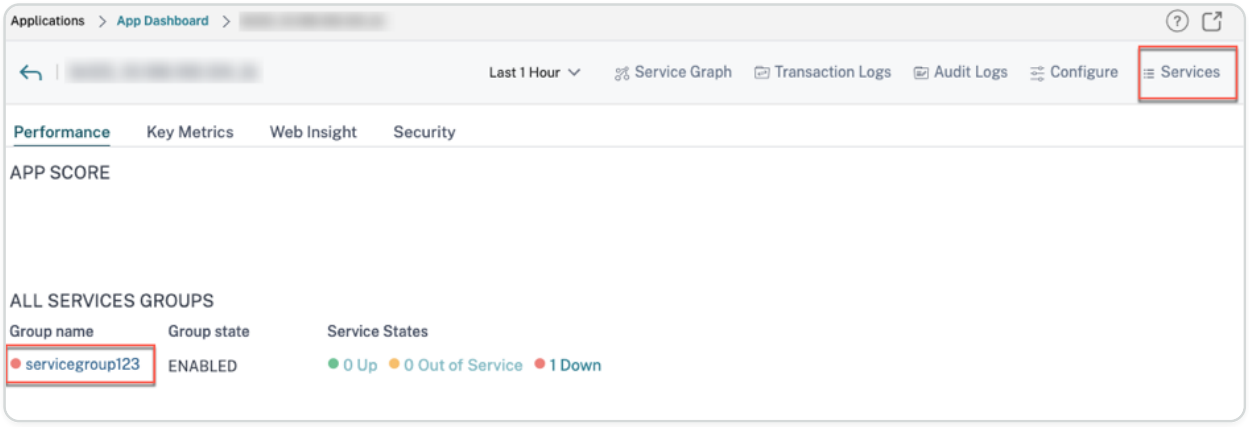
To view the status of the monitors, follow these steps.

1. From the NetScaler Console GUI, navigate to **Applications > Dashboard**. Under **Applications**, select the application whose health you want to check.

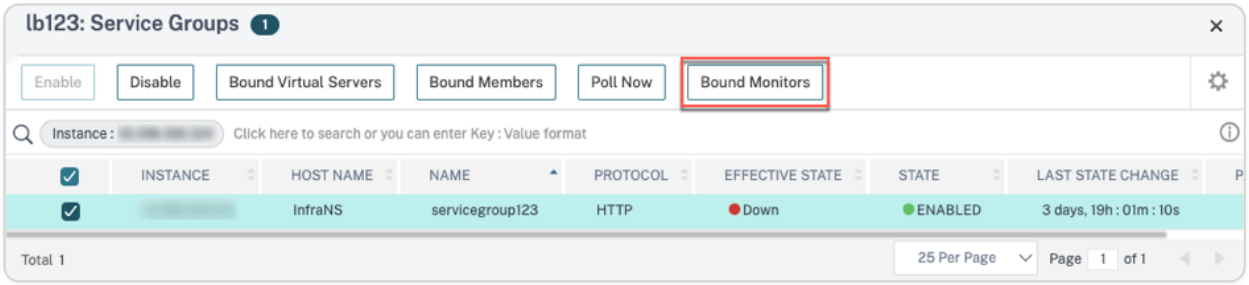


2. Click the application. The app score dashboard appears.

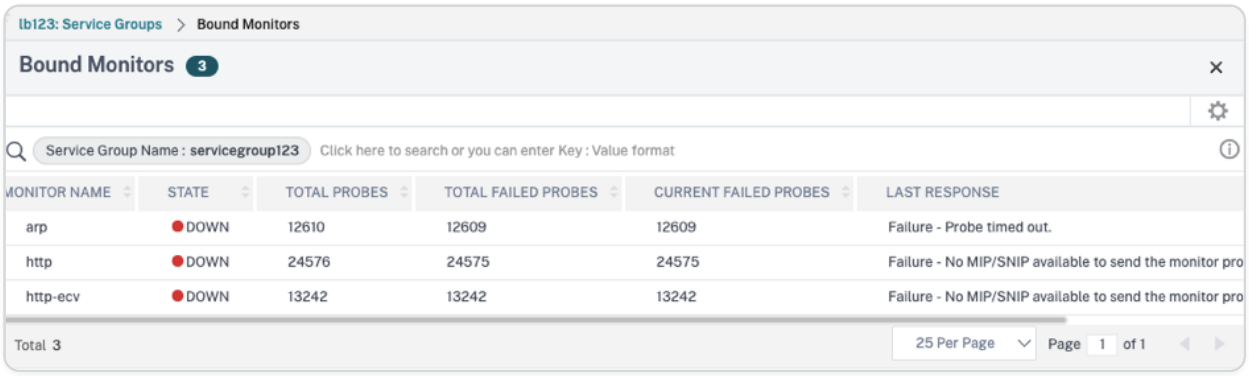
© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Click the **Services** tab on the upper-right corner or the service group under **Group Name**.
4. If you click the **Services** tab, in the next screen, select the service group.
5. If you click the service group, the **Service Group**s window appears. Select the instance and click **Bound Monitors**



The bound monitor screen appears, showing the health monitor status of the application.



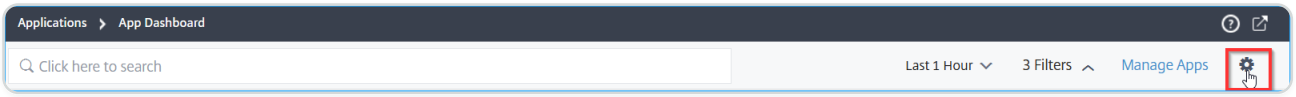
Select App Score components and set thresholds

In **App Dashboard**, as an administrator, you can decide to select the components and configure thresholds for app score calculation. App Score is the scoring system that defines:

- How well an application is performing
- Whether the application is performing well in terms of responsiveness

Navigate to **Applications > Dashboard** and then select the settings icon.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



In the **Configure App Score** page, you can select the components and configure thresholds to determine the final app score.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure App Score

Configure the contributing factors and their thresholds to calculate the App Score values

- [x] ADC Memory Usage
  - Low Memory Threshold (%): 70
  - High Memory Threshold (%): 85
- [x] Surge Queue Build-up
  - Lower Surge Queue Threshold: 0.05
  - Higher Surge Queue Threshold: 0.10
- [x] ADC CPU Usage
  - Low CPU Threshold (%): 80
  - High CPU Threshold (%): 90
- [x] Response Time
  - Response Time (ms): 500
- [x] App CPU Usage
  - Low App CPU Threshold (%): 70
  - High App CPU Threshold (%): 90
- [x] Active Services
  - Active Services Threshold (%): 100
- [x] Improper Persistence Type
- [x] Server Error 5xx
- [x] Unusually Large HTTP Packets
- [x] SSL Real Time Traffic
- [x] SSL Session Build-up
- [x] Low Session Reuse
- [x] NIC Card Saturation
- [x] TCP Reassemble Queue Limit Hits

OK Close

App Score calculation is based on the following components:

APP SCORE COMPONENTS	USER CONFIGURED THRESHOLDS	DESCRIPTION
NetScaler Memory usage	Yes	The low and high threshold value for the total memory usage in the NetScaler instance
Surge queue buildup	Yes	The low and high threshold value for the total surge requests that are in queue and need a response.
NetScaler CPU usage	Yes	The low and high threshold value for the total CPU usage in the NetScaler instance.
Response time	Yes	The time interval between sending a request packet and receiving the first response packet from the service configured on the virtual server.
App CPU Usage	Yes	The low and high threshold value for the total CPU usage by the application.
Active services	Yes	The threshold value of the percentage of services that must be active which are bound to the virtual server.
Improper persistence type	No	Indicates if the persistence usage on a virtual server is low.
Server error (5xx)	No	Indicates if the web server responds with 5xx errors.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

APP SCORE COMPONENTS	USER CONFIGURED THRESHOLDS	DESCRIPTION
Unusually large HTTP packets	No	Indicates the occurrences, if the HTTP messages with HTTP header size exceed the configured values in the NetScaler instance.
SSL real time traffic	No	Analyzes the SSL traffic to identify real time traffic and suggests optimal configuration settings for improving latency.
SSL session buildup	No	Indicates the session build-up over a period of time, which can lead to a large amount of memory being held up by these sessions in the NetScaler instance.
Low session reusage	No	Indicates if the actual number of sessions being reused by the NetScaler instance is less.
NIC card saturation	No	Indicates the total packets discarded by the interfaces.
TCP reassemble queue limit hits	No	Indicates if the Out-of-Order packets on a TCP connection exceed the configured out of order packet queue size.

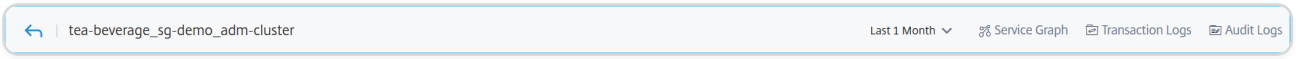
By default, all components are enabled. If you disable any component, NetScaler Console performs the final app score calculation only based on the selected components.

Application details for microservices applications

Click a microservices application from the dashboard to drill down for further detailed information.

The selected application page is displayed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

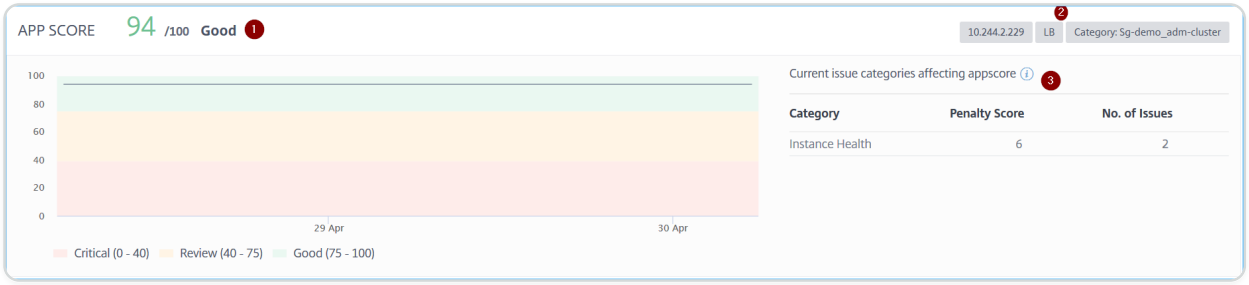


From the application details page:

- Select the time duration from the list to view details for the specific time duration
- Click **Service Graph** to view service graph for the selected application. For more information, see Service Graph for Applications
- Click **Transaction Logs** to view the detailed transactions for the selected application
- Click **Audit logs** to view the detailed audit log information

After you select the time duration, the following application details are displayed:

- **App Score** – The application score for the selected time duration. You can also view the current application issues, which are known as the penalty score applicable based on the issue category. The final score is calculated as **100 minus total penalty**.



1 – Denotes the current app score

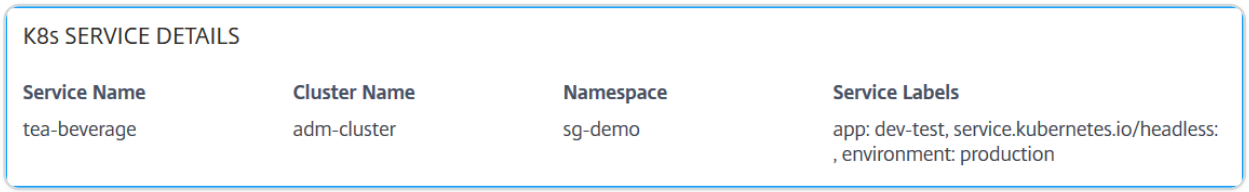
2 – Denotes the CPX IP address, application type such as load balancing or content switching, and service namespace and cluster name where the service is hosted

3 – Denotes the issues affecting the current application score

This dashboard also enables you to view the current issues that are affecting the app score. You can view the issues details under Issues.

- **K8s service details**

  You can view the following details:



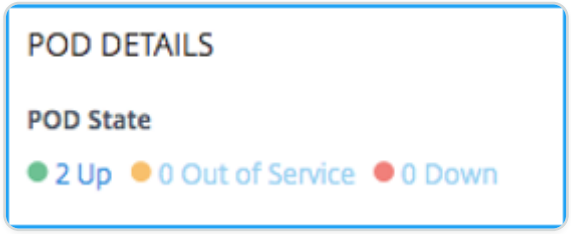
  - **Service Name** – The service name
  - **Cluster Name** – The cluster name where the service is hosted

© 1997–2026 Citrix Systems, Inc. All rights reserved.

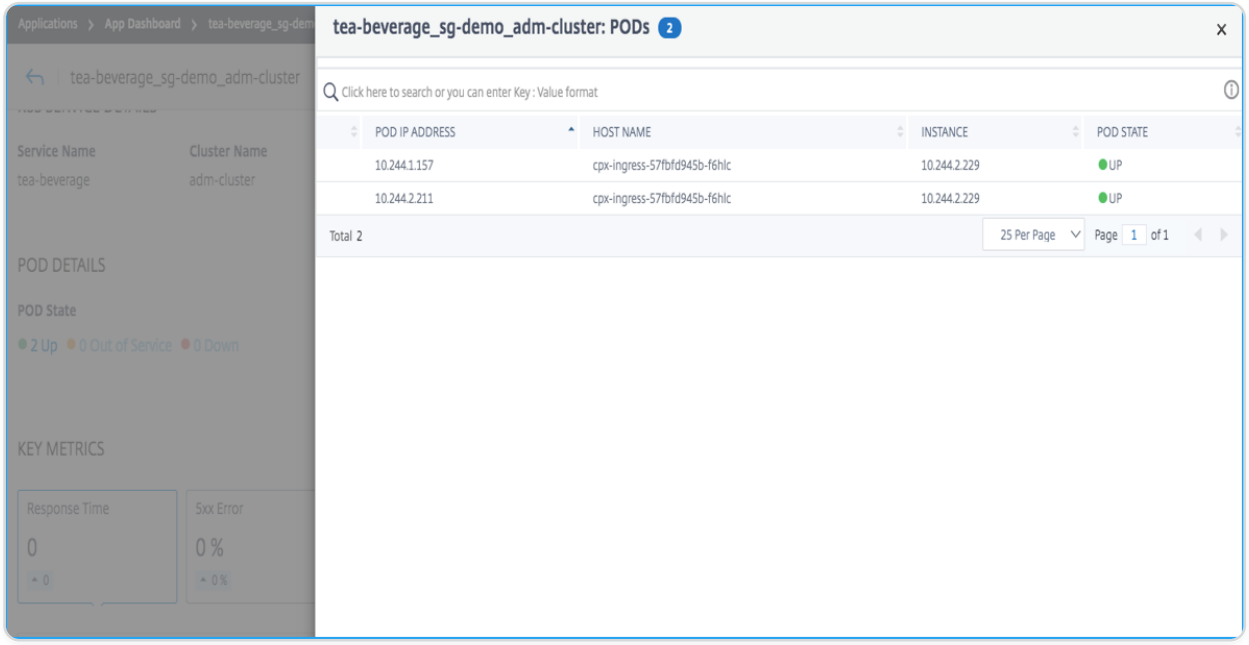
- **Namespace** – The namespace assigned to the service
- **Service Labels** – The service labels assigned to the service

- **Pod Details**

  A pod is a group of containers hosted in the Kubernetes cluster. Inside a pod, you can deploy multiple containerized applications. Each pod is associated with an IP address.



  Click the pod state to view the details



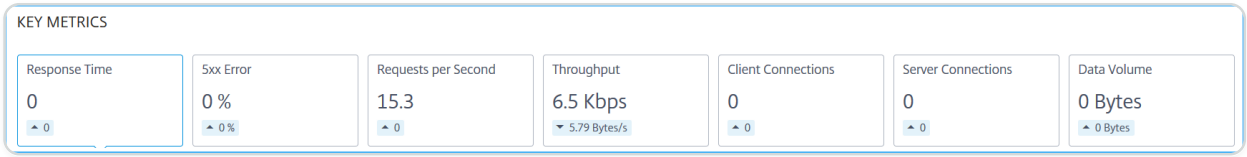
  - **Pod IP Address** – Denotes the Pod IP address
  - **Host name** – Denotes the host name assigned to the pod
  - **Instance** – Denotes the NetScaler CPX IP address
  - **POD state** – Denotes the pod current status

- **Key Metrics** – The key metrics details, such as **Response time**, **5xx errors**, **Requests per second**, **Throughput**, **Client Connections**, **Server Connections**, and **Data Volume** are displayed.

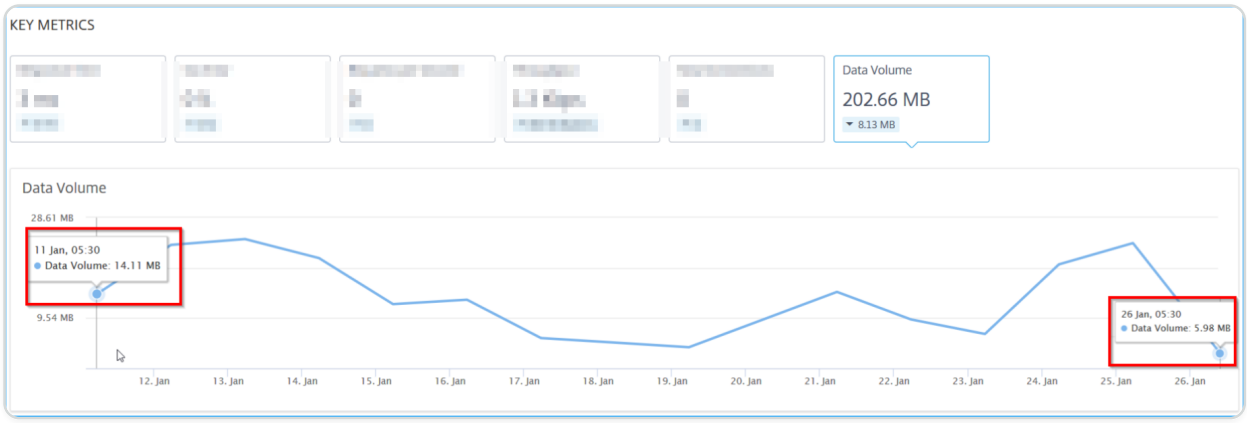
  In each metric, you can view the average value and the difference value for the selected time duration. The difference value is calculated as the **first value minus the last value** of the selected time duration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can view the following instance metrics in a graph format for the selected time duration:



The following image is an example for **Data Volume** and the selected time duration is 1 month. The value 202.66 MB is the total Data Volume for the 1-month duration and the value 8.13 MB is the difference value. In the graph, the first value is 14.11 and the last value is 5.98. The difference value is 14.11 – 5.98 = 8.13 MB.



- **Issues** – The issues that are applicable for the selected application. You can view the following issues along with its category:

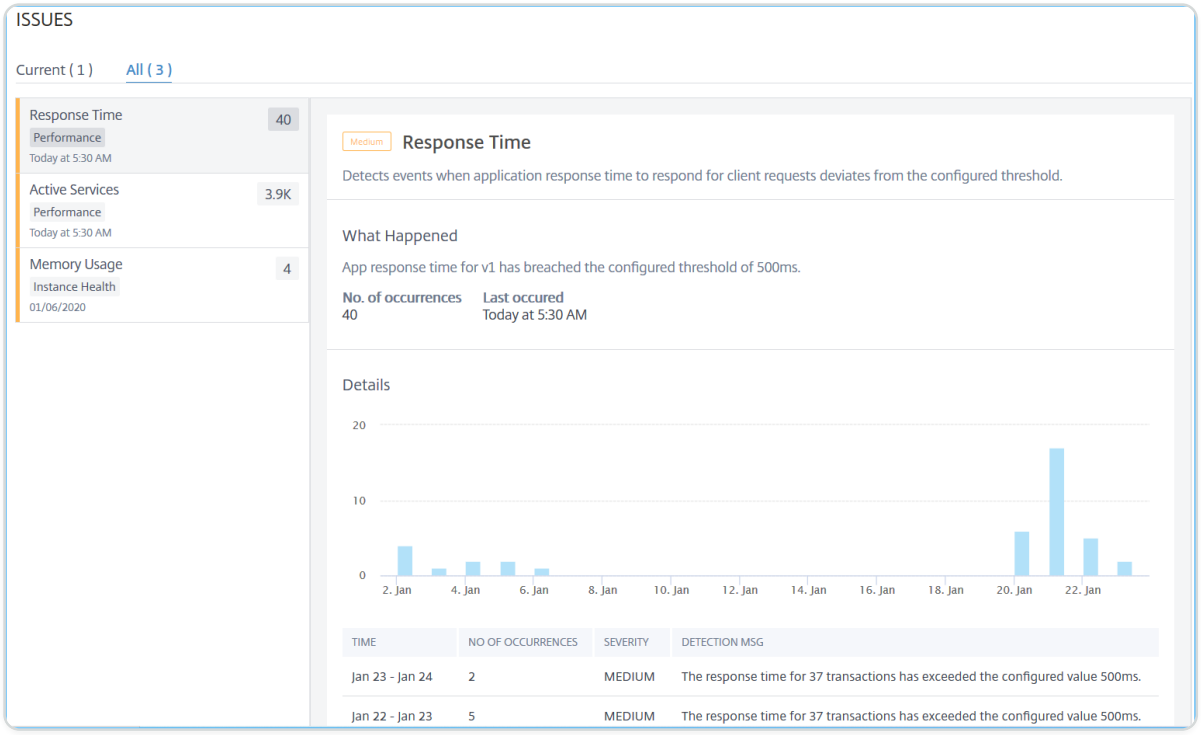
PERFORMANCE	INSTANCE HEALTH	CONFIG	SYSTEM RESOURCES
Response Time	Average CPU Usage	High 5xx response	Improper persistence type
Low Session Reuse	Memory Usage	Unusually large HTTP packets	NIC Card Saturation
SurgeQueue Buildup		TCP reassemble queue limit hits	
SSL Real Time Traffic			

Click each issue to view the following information:

  - Total occurrences
  - Recommended Actions to troubleshoot the issue

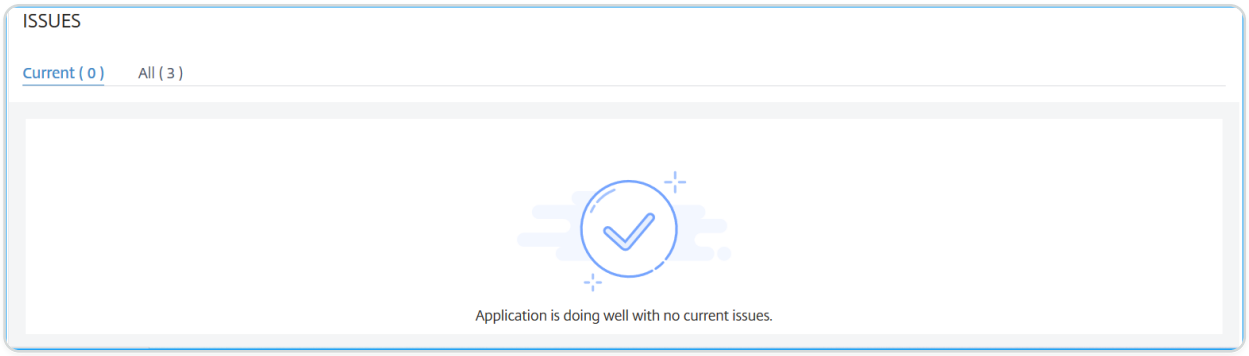
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The issue details such as time, service name, total occurrences, severity, and detection message



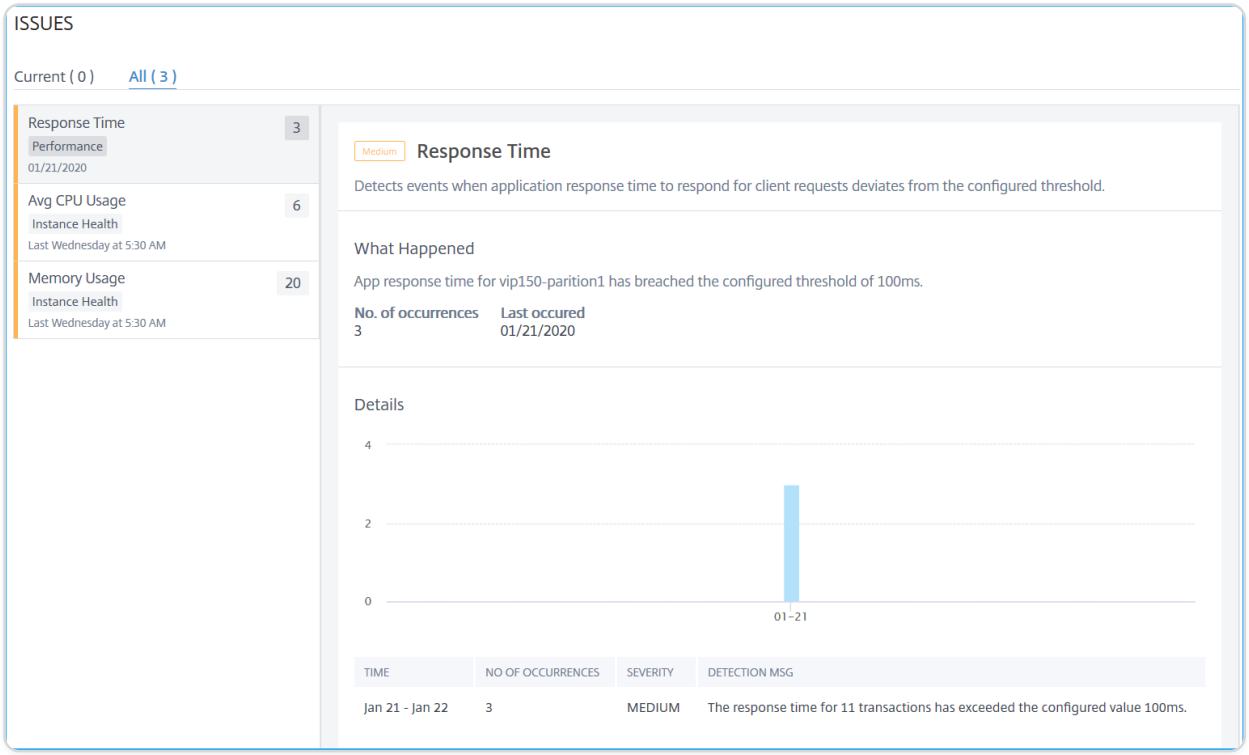
  - The issues that display in **Current** tab refer to the application issues for the select time duration.
  - The issues that display in **All** tab refer to total application issues.

The following example is the application issues for 1-day duration. The **Current** tab indicates no current issues impacting the app score.



The **All** tab displays the total issues detected for the 1-day duration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Intelligent App Analytics

Intelligent App Analytics enables you to identify application performance issues using machine learning and rule algorithms. The Intelligent App Analytics feature of NetScaler Console:

- Provides an easy and scalable solution for monitoring and troubleshooting applications that are delivered through NetScaler instances.
- Monitors all levels of application to reduce the turnaround time for troubleshooting issues and improving the overall application uptime.

In a typical deployment, thousands of servers cater to the data needs of the users. The traffic sent to these servers is load balanced and monitored by virtual servers configured on NetScaler appliances. Each virtual server is bound to multiple services representing the back end servers. In such deployments, the Intelligent App Analytics feature helps you:

- Monitor, manage, and make decisions during outages and other events
- Monitor the virtual servers and services configured for an application
- Display critical information about virtual servers and services, so that you can change the configurations as required to achieve optimum performance by the applications.

Navigate to **Application** > **Dashboard** and select an application to view performance indicators in the **Issues** section.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure Intelligent App Analytics

NOTE:

Starting from **14.1-21.x or later builds**, Metrics Collector is disabled by default in the new NetScaler instances added in NetScaler Console. The metrics collector configuration for the existing managed instances remain unchanged.

The Intelligent App Analytics feature is supported only in **NetScaler 12.1 Build 50.28 or later**. Metrics Collector pushes the NetScaler counter data to NetScaler Console, which is used to detect application issues. To use the Intelligent App Analytics feature, **Metrics Collector** must be configured on each NetScaler instance.

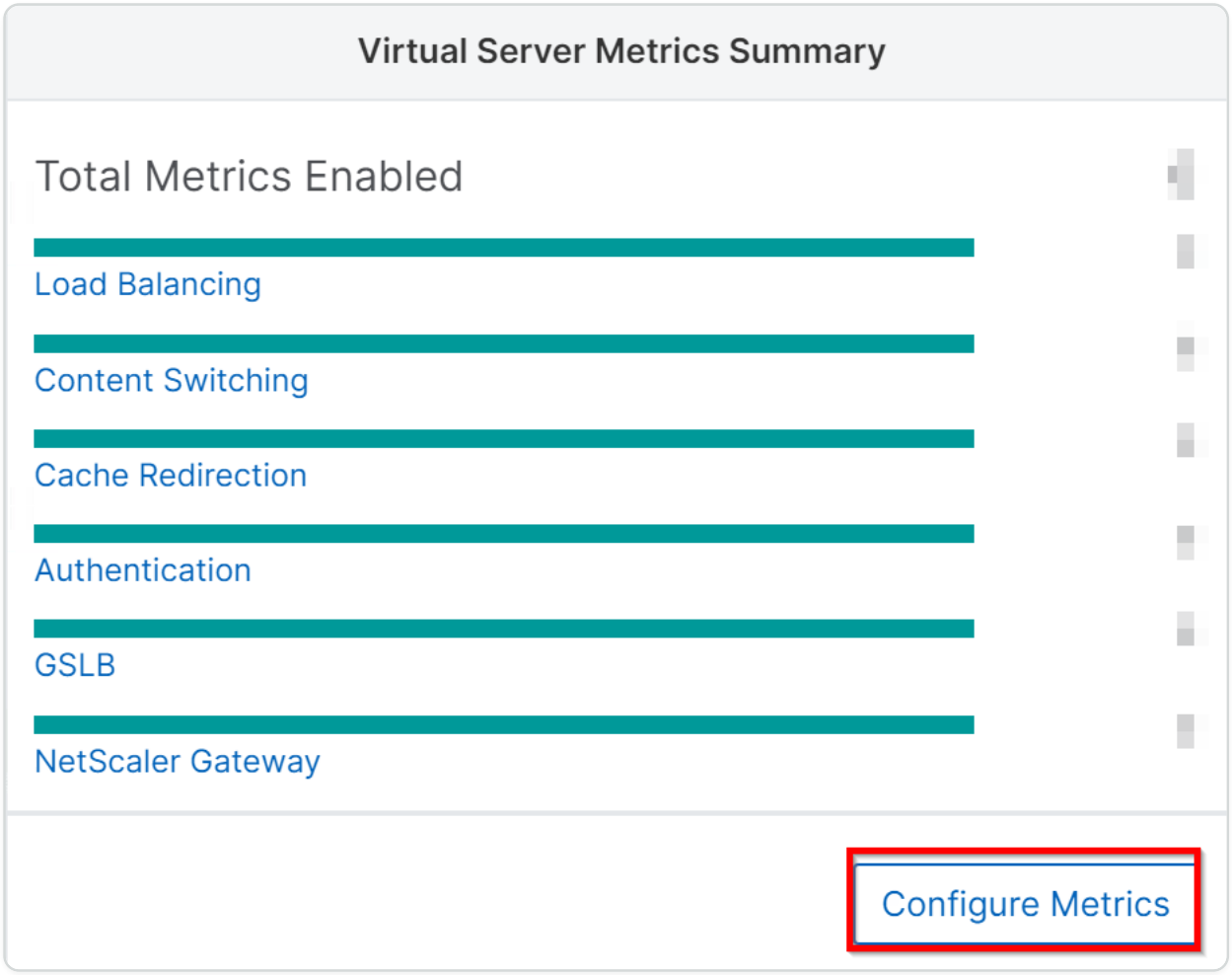
Starting from 14.1-28.x build, Metrics collector and lean usage analytics are enabled at the virtual server level instead of the instance level. With this enhancement, Metrics Collector and lean usage analytics remain enabled only on your active virtual servers with high traffic. For more information, see Peak and lean usage analytics.

You can review your virtual servers and enable Metrics Collector and lean usage on other virtual servers.

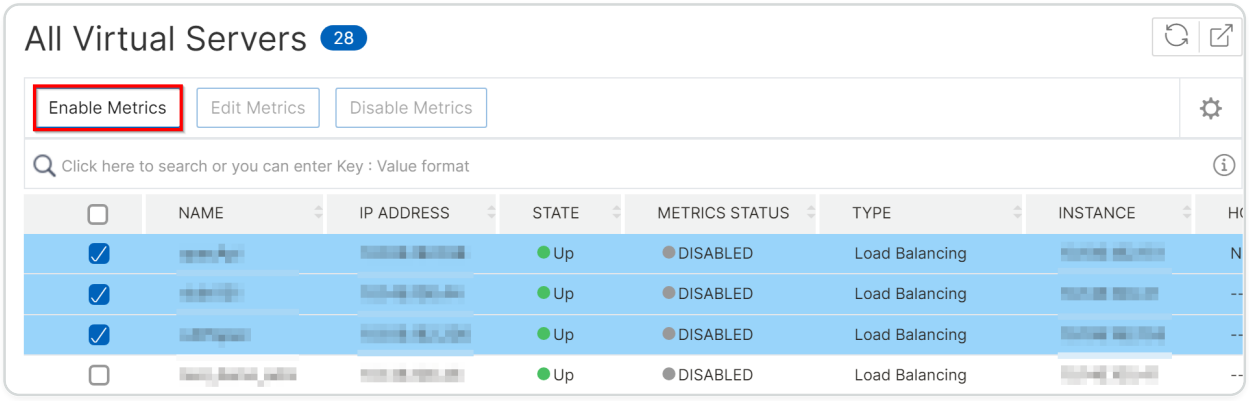
To review and enable Metrics Collector:

1. Navigate to **Settings > Analytics Configuration**.
2. Click **Configure Metrics** under **Virtual Server Metrics Summary**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

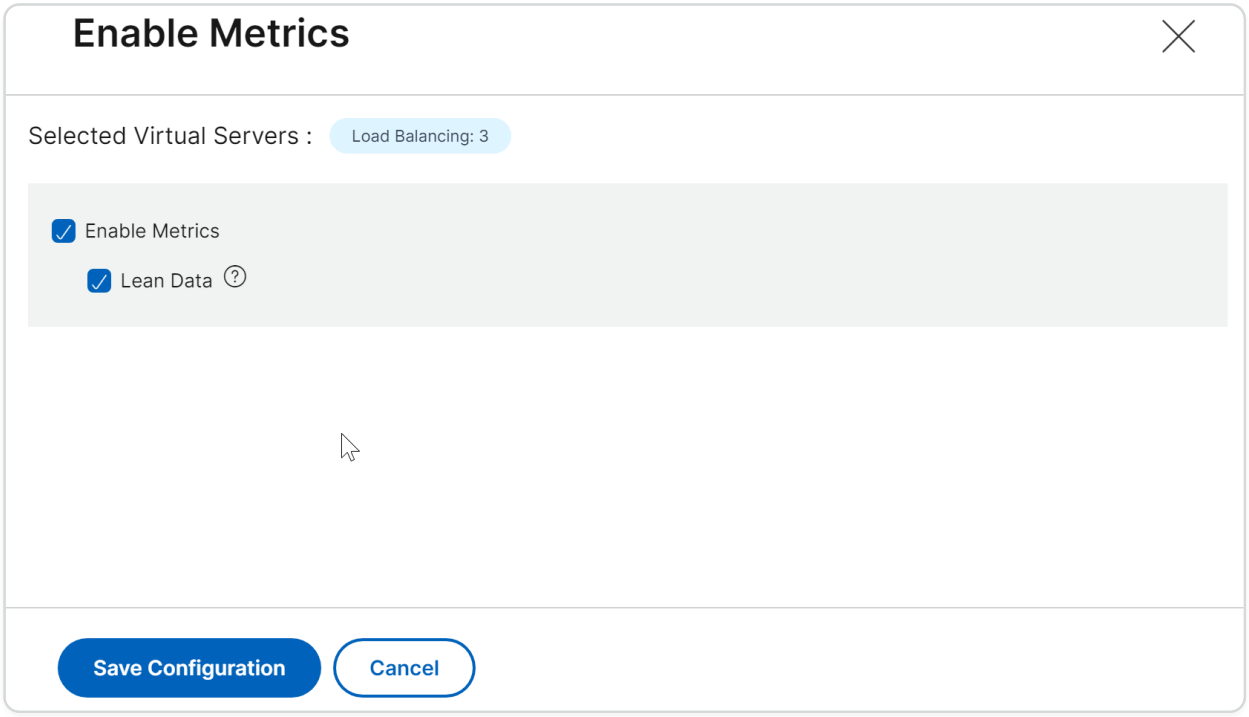


3. In the **All Virtual Servers** page, you can view the status of the metrics collector on each virtual server. Select the virtual servers that you want to enable and click **Enable Metrics**.



4. Select **Enable Metrics** to enable Metrics Collector. You can also select **Lean Data** if you want to enable and view lean period usage analytics. After selecting, click **Save Configuration**. For more information, see Peak and lean usage analytics.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Alternatively, you can also enable metrics collector and lean usage for the virtual servers from the NetScaler® instances page:

1. Navigate to **Infrastructure > Instances**, select the instance type, and select **Metrics Collector** from the **Select Action** list.
2. Select the virtual servers for which you want to enable metrics collector and click **Enable Metrics**.
3. Select **Enable Metrics** to enable Metrics Collector. You can also select **Lean Data** if you want to enable and view lean period usage analytics. After selecting, click **Save Configuration**.

Once the **Metrics Collector** option is enabled on the virtual server, navigate to **Applications** > **Dashboard**. Select an instance to view anomalies under **Issues** section.

We recommended to also enable analytics to visualize issues such as detailed web transactions for server errors (5xx). For more information, see Enable Analytics.

Performance indicators for application analytics

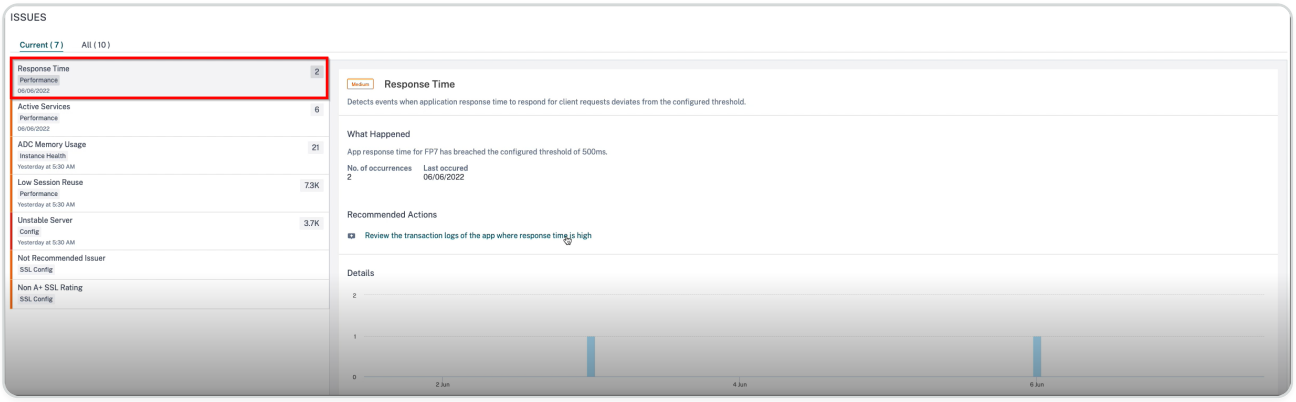
You can view the performance indicators, along with its categories that occur in NetScaler web applications. To view these indicators, you must ensure to enable analytics and metrics collector on the NetScaler instance:

After you enable analytics and metrics collector, you can view the following indicators by navigating to **Applications** > **Dashboard**, selecting an application, and scrolling down to **Issues** section:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Response time

This issue detects when the application response time to respond to client requests deviates from the configured threshold value. Click the **Response Time** tab to view the issue details.



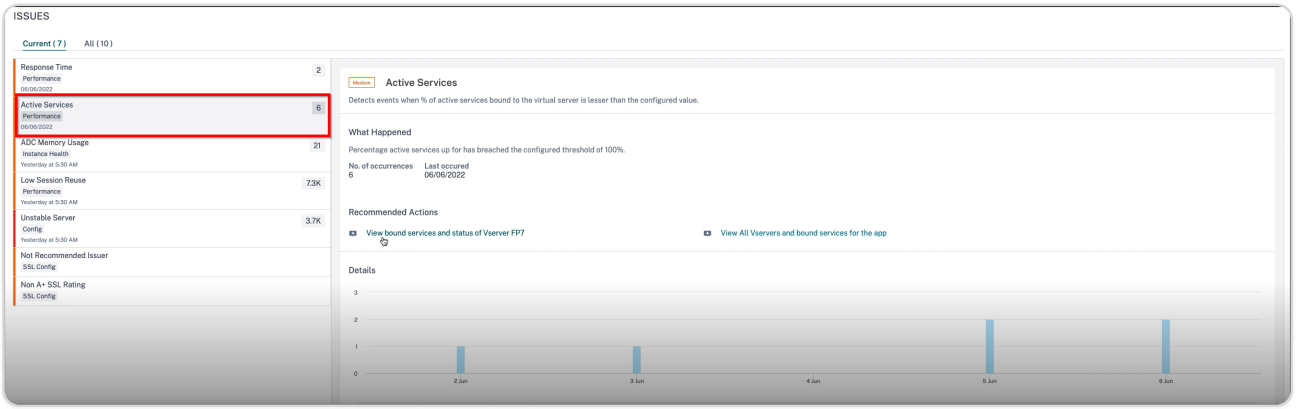
In the **Recommended Actions**, click to view the **Transaction Logs** that show the application with > 500 ms response time.

Under **Details**, you can view:

- The graph indicating the total events for the selected time. Click to apply filter and view details
- When the issue has occurred
- The total occurrences for the selected time
- The issue severity such as low, medium, and high
- The detection message indicating the total transaction response time exceeding the configured threshold value.

Active services

This issue detects when the % of active services bound to the virtual server is lesser than the configured threshold value. Click the **Active Services** tab to view the issue details.



In the **Recommended Actions**, click to view details of the services bound to the virtual server.

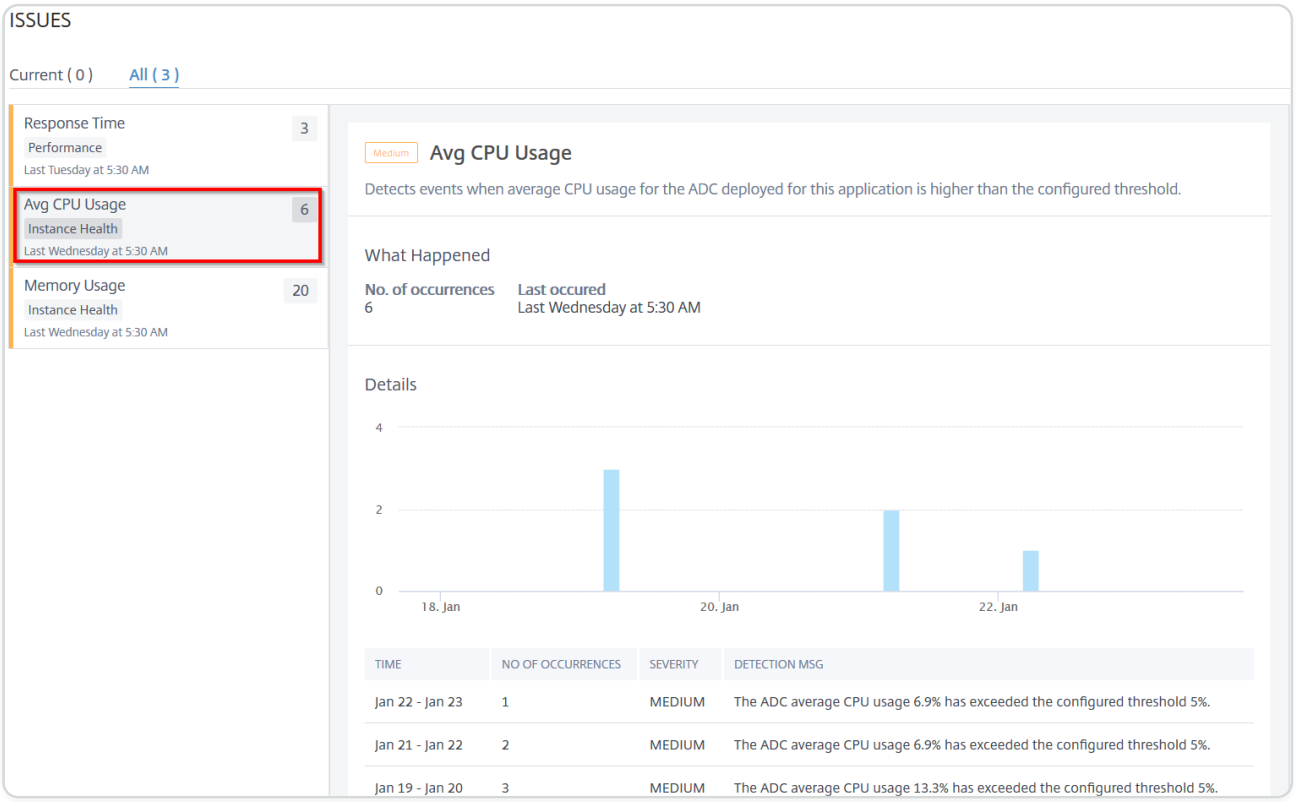
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Under **Details**, you can view:

- The graph indicating the total events for the selected time duration. Click to apply filter and view details
- When the issue has occurred
- The total occurrences for the selected time duration
- The issue severity such as low, medium, and high
- The detection message indicating the % of active service sessions and the configured threshold value.

Average CPU usage

This issue detects when the NetScaler CPU usage for this application exceeds the configured threshold value. Click the **Average CPU Usage** tab to view the issue details.



Under **Details**, you can view:

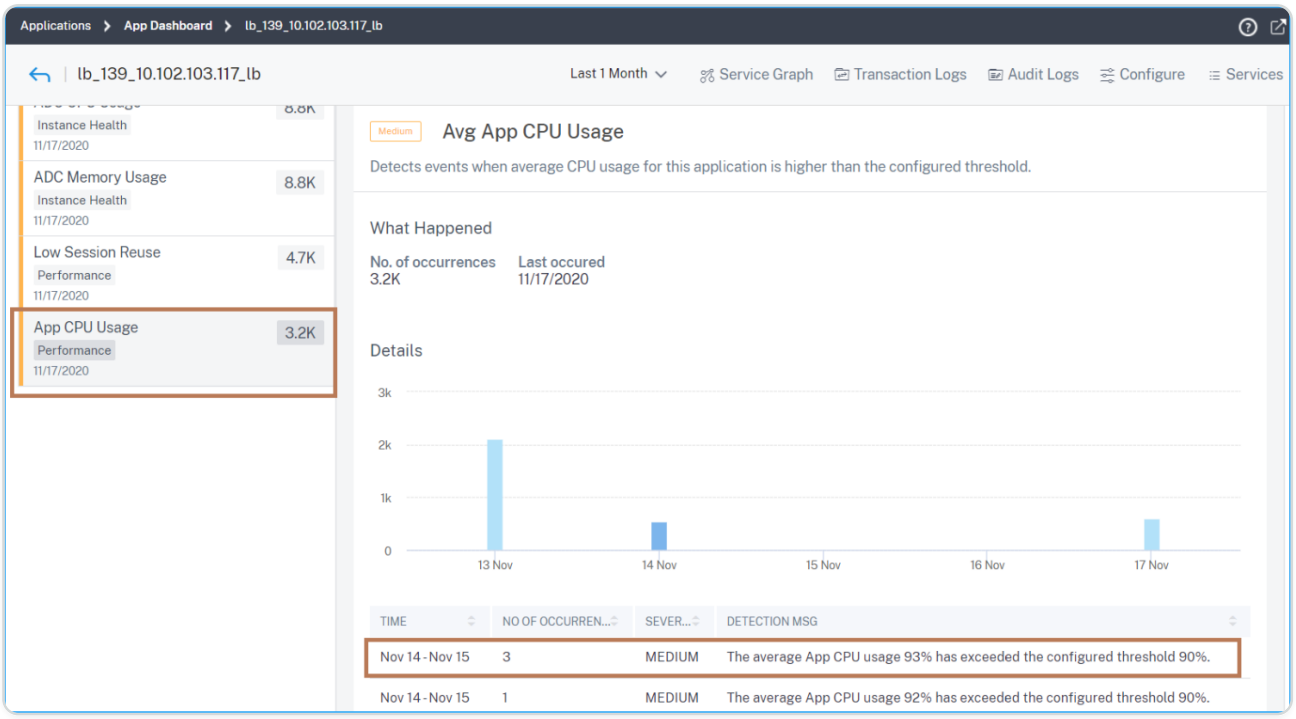
- The graph indicating the total events for the selected time duration. Click to apply filter and view details
- When the issue has occurred
- The total occurrences for the selected time duration
- The issue severity such as low, medium, and high

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The detection message indicating the NetScaler average CPU usage % and the configured threshold value.

Average application CPU usage

This issue detects when the application CPU usage exceeds the configured threshold value. Click the **App CPU Usage** tab to view the issue details.



Under **Details**, you can view:

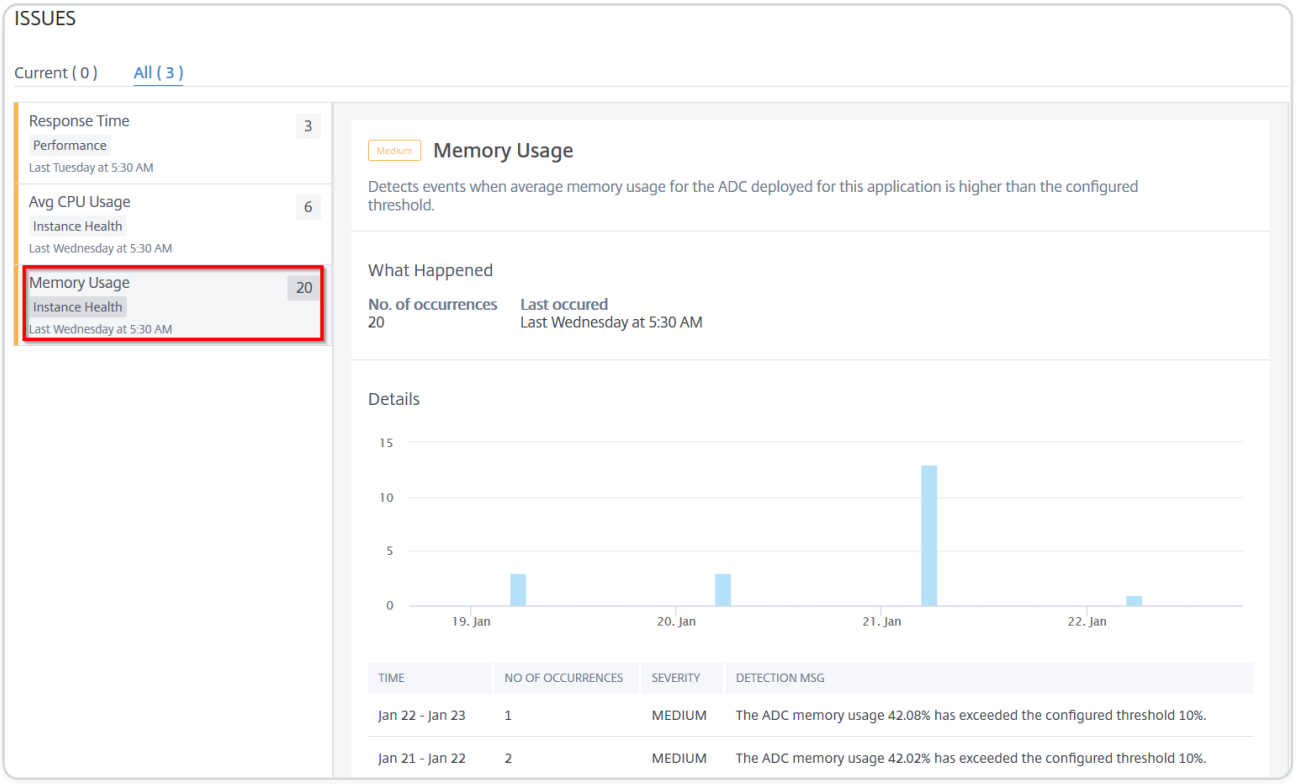
The graph indicating the total events for the selected time duration. Click to apply filter and view details

- When the issue has occurred
- The total occurrences for the selected time duration
- The issue severity such as low, medium, and high
- The detection message indicating the application average CPU usage % and the configured threshold value

Memory usage

This issue detects when the NetScaler memory usage for this application exceeds the configured threshold value. Click the **Memory Usage** tab to view the issue details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Under **Details**, you can view:

- The graph indicating the total events for the selected time duration. Click to apply filter and view details
- When the issue has occurred
- The total occurrences for the selected time duration
- The issue severity such as low, medium, and high
- The detection message indicating the NetScaler average memory usage % and the configured threshold value.

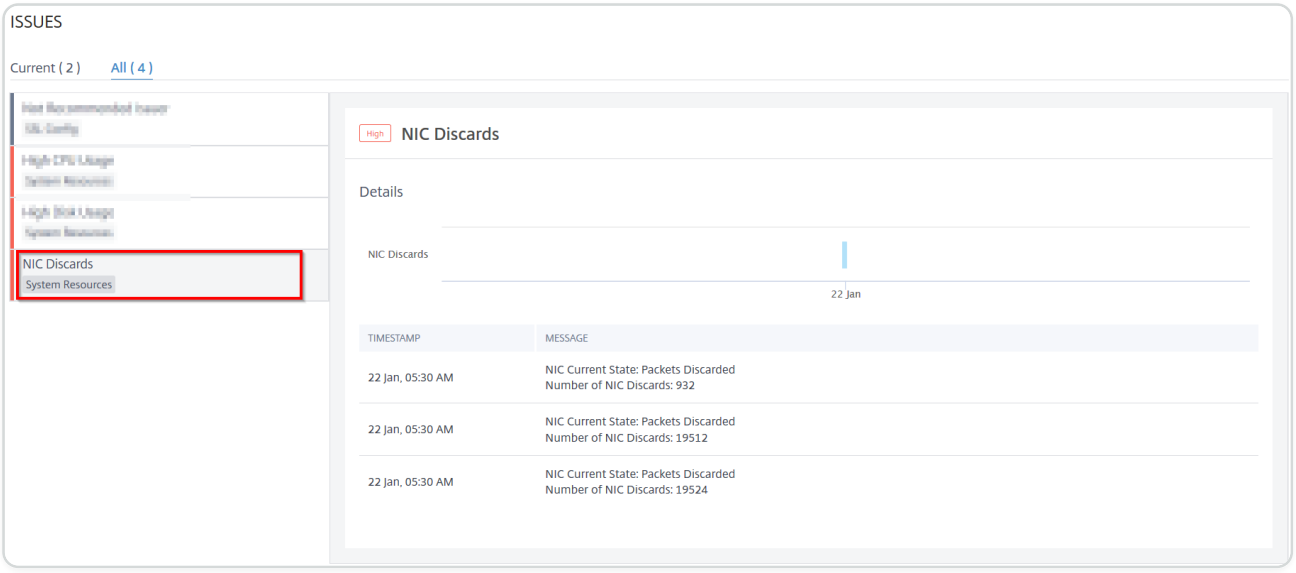
NIC discards

A packet discard can happen when:

- A received packet has some format errors
- A receiving device does not have enough storage for the packets

Using the **NIC Discards** indicator, you can view total packets discarded from the NIC. Click the **NIC Discards** tab to view the details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Under **Details**, you can view:

- The time that occurred the anomaly
- The message indicating the total packets discarded from NIC

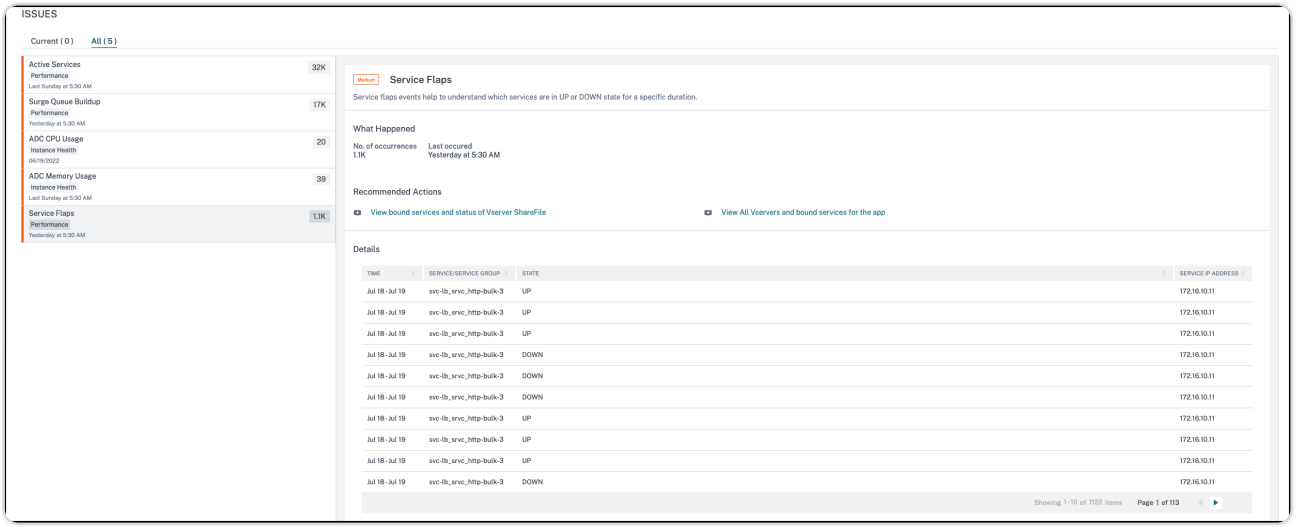
Service flaps

As a network administrator, you must ensure for optimal availability of the application. When there are any network issues or configuration issues, the status and availability of an application server might impact the overall performance.

Using the service flaps events, you can identify the application that has issues. Service flaps events also help you:

- Understand which service is in DOWN status for a specific duration
- Understand how many services are in UP or DOWN state for a specific duration

Click the **Service Flaps** tab to view the service flaps details.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

In the **Recommended Actions**, click to view the details of services that are bound to the virtual server.

You can view details such as number of occurrences and the time of last occurrence.

Under **Details**, you can view:

- The time that occurred the service flap anomaly
- The service/service group name
- The service IP address
- The current service status

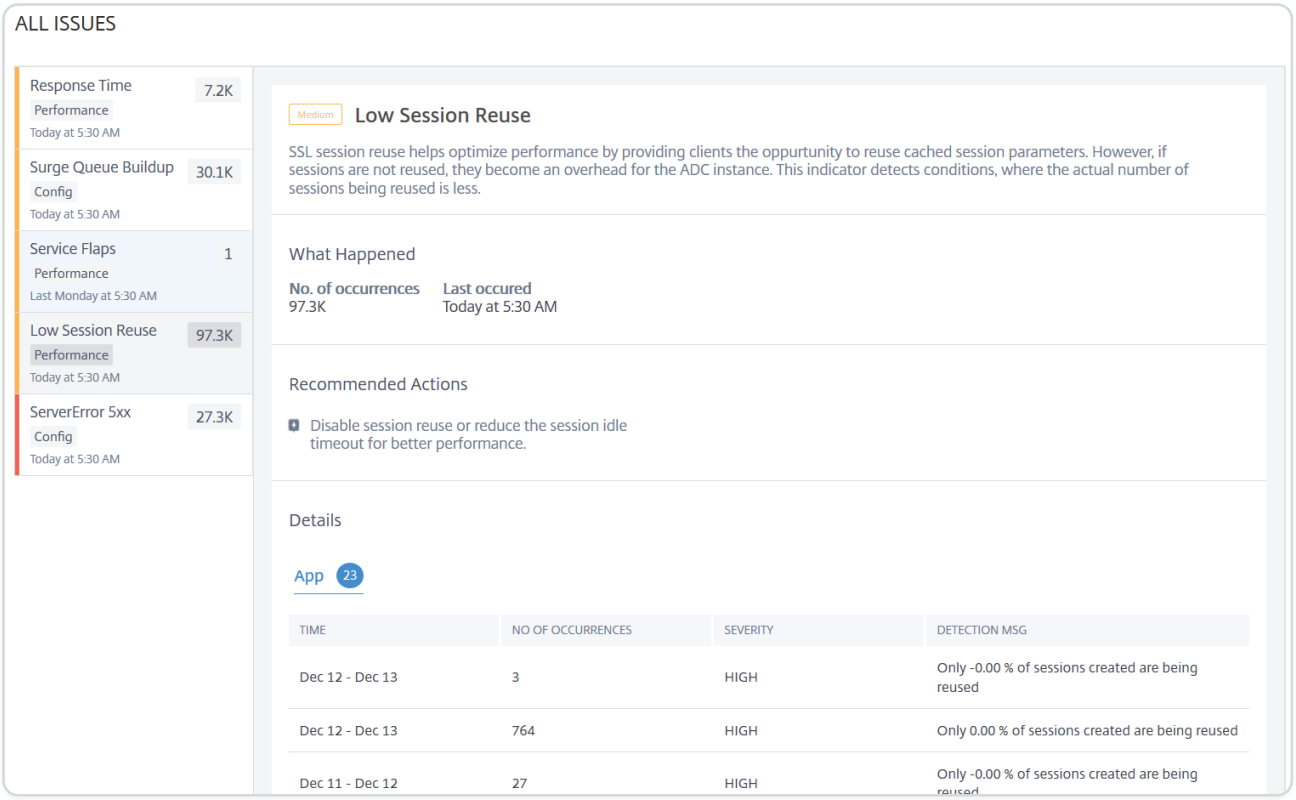
Low session reuse

NetScaler instances process SSL transactions by offloading SSL handshake process from the server. Upon receiving the response from the server, the NetScaler instance completes the secure transaction with the client. Using the cached session parameters, NetScaler instance completes the SSL handshake process for the consecutive requests.

If in case these sessions are not reused, they become an overhead for the NetScaler instances. Using the **Low Session Reuse** indicator, you can identify if the actual number of sessions being reused is less.

Click the **Low Session Reuse** tab to view the issue details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **Recommended Action** to troubleshoot the issue is to either disable the session reuse or reduce the session timeout. For more information, see Session Reuse.

Under **Details**, you can view:

- Total applications that have Low session reusage
- The time that occurred the low session reuse anomaly
- Total occurrences
- The anomaly severity such as high, low, and medium
- The detection message indicating only % of the configured sessions are being reused

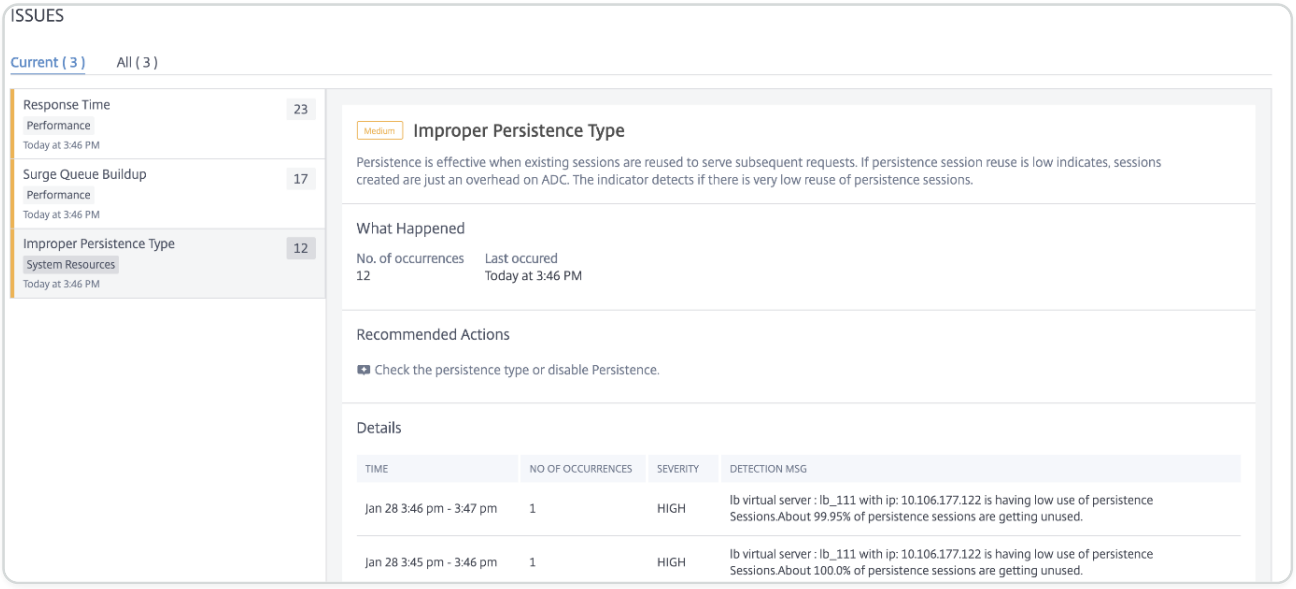
Improper persistence type

You must configure persistence on a virtual server if you want to maintain the states of connections on the servers represented by that virtual server (for example, connections used in e-commerce). The appliance then uses the configured load balancing method for the initial selection of a server, but forwards to that same server all subsequent requests from the same client.

Persistence is effective when existing sessions are reused to serve subsequent requests. If persistence session reuse is low, sessions created on NetScaler are just an overhead.

Using the **Improper Persistence Type** indicator, you can determine if the persistence usage on a virtual server is low. Click the **Improper Persistence Type** tab to view the issue details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **Recommended Action** to troubleshoot the issue is to check the persistence type or disable persistence. For more information, see Persistence Settings.

Under **Details**, you can view:

- The time that occurred the anomaly
- Total occurrences
- The anomaly severity such as high, low, and medium
- The detection message indicating the % of sessions that are unused

Unstable Server

In some scenarios, the web server responds with status codes when it is unable to handle the requests for reasons such as invalid requests, temporary overloading, or server maintenance. These errors are displayed with error codes, which define various scenarios of the errors. For example,

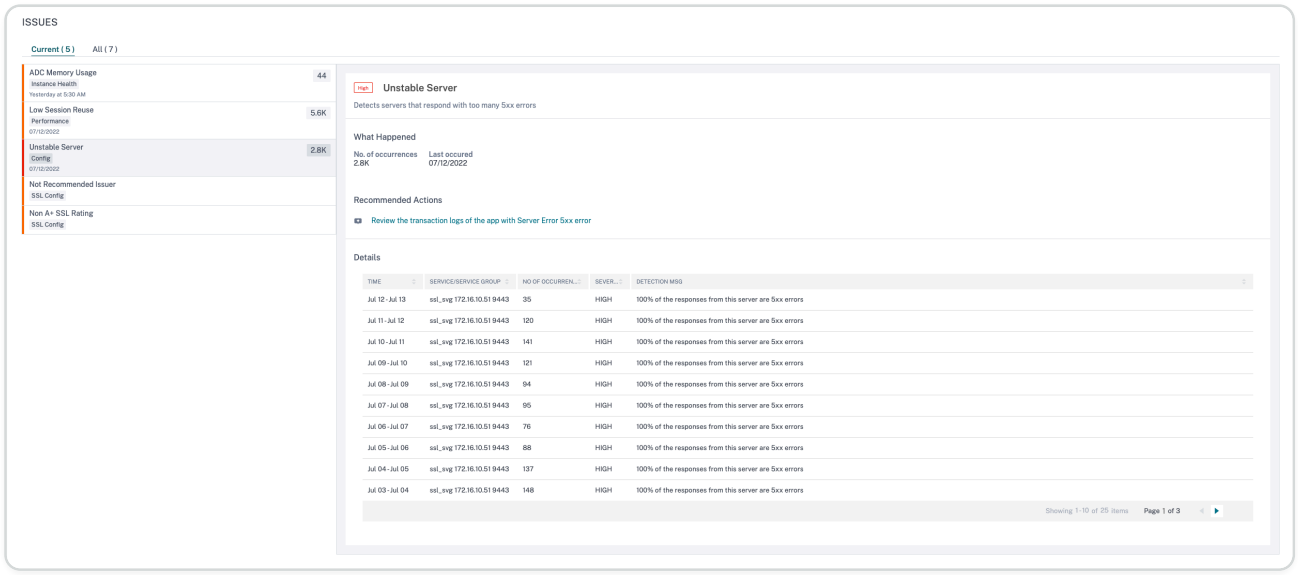
- **502 Bad Gateway** The server is acting as a gateway or proxy and received an invalid response from the upstream server.
- **503 Service Unavailable** The server is unavailable. The servers might be overloaded or down for maintenance.
- **504 Gateway Time-out** The server is acting as a gateway or proxy and did not receive a timely response from the upstream server.

These can be temporary conditions, but sometimes you have to implement a corrective measure on the webservers to make the webpages up and available.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Using the **Unstable Server** indicator, you can view these failures and take decisions about corrective actions to overcome the issues and ensure the client requests are served and the webpages are always available.

Select the **Unstable server** tab to view the issue details.



In the **Recommended Actions**, click to view the **Transaction Logs** that show the application with Response code 5xx error.

You can also try the following troubleshooting methods:

- Configure L7 monitors with appropriate parameters for the server that responds with 5xx errors. A monitor is an entity that tracks the service health. The appliance periodically probes the servers using the monitor bound to each service. If a server does not respond within a specified response timeout, and the specified probes fail, the service is marked DOWN. The appliance then performs load balancing among the remaining services. For more information to configure a monitor, see Custom Monitors
- Troubleshoot the server

Under **Details**, you can view:

- The time that occurred the unstable server anomaly
- The service/service group name
- Total occurrences
- The anomaly severity such as high, low, and medium
- The detection message indicating % of the responses from this service reporting 5xx errors

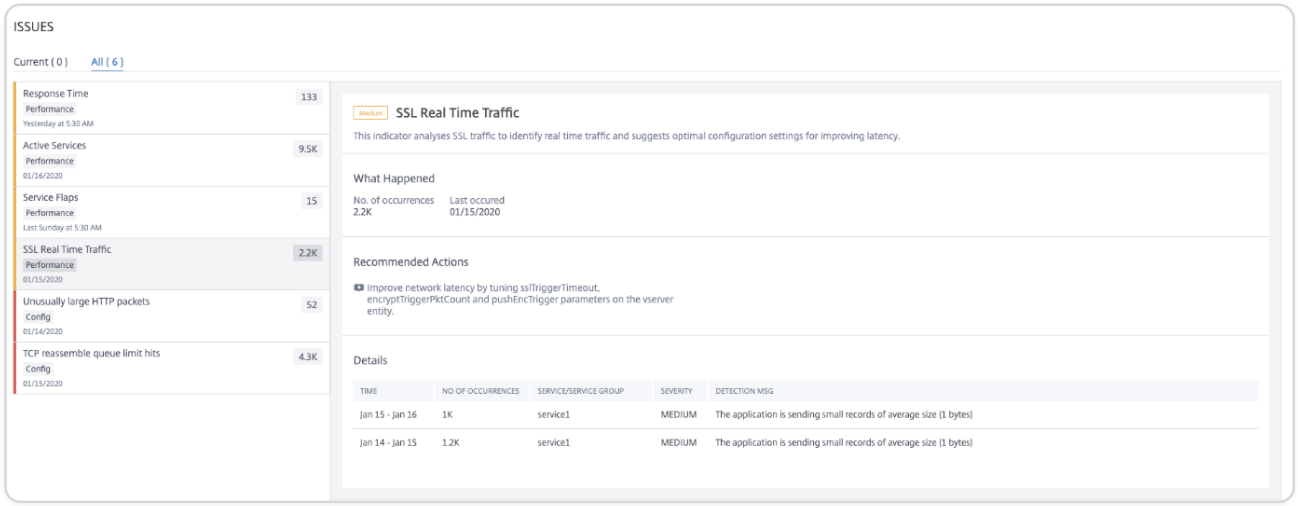
© 1997–2026 Citrix Systems, Inc. All rights reserved.

For detailed information on server error web transaction, see Web transaction analytics for server errors

SSL Real Time Traffic

In NetScaler instance, you can use an SSL profile for processing SSL traffic. The SSL profile comprises certain SSL parameters for virtual servers, services, and service groups. The **SSL Real Time Traffic** indicator analyzes the SSL traffic to identify real time traffic and suggests optimal configuration settings for improving latency.

Click the **SSL Real Time Traffic** tab to view the issue details.



The **Recommended Action** to troubleshoot the issue is to improve the network latency by updating SSL parameters. For more information, see Global SSL Parameters.

Under **Details**, you can view:

- The time that occurred the anomaly
- The service/service group name
- The anomaly severity such as low, medium, and high
- The detection message with the current setting on the application

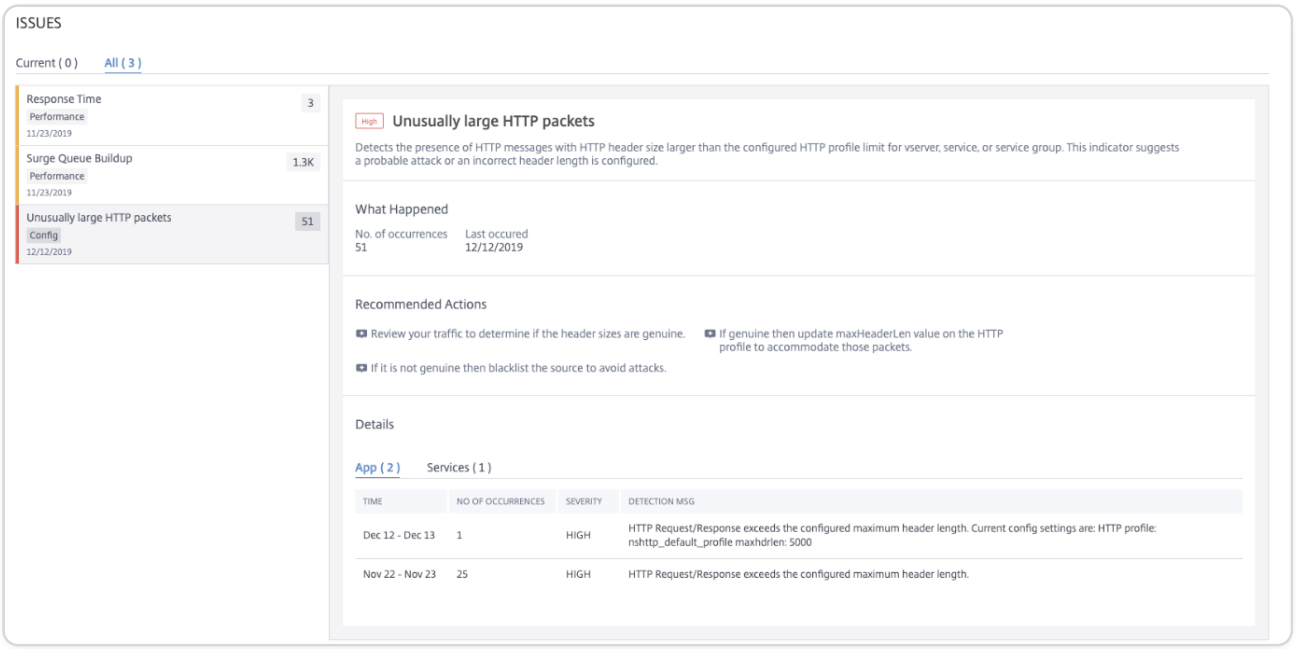
Unusually Large HTTP packets

An HTTP transaction uses request-response messages between the client and the server. In the request and response messages, HTTP headers are the values that are displayed in the HTTP protocol. You can configure the HTTP header length in virtual server, service, or service group to avoid 4xx errors.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When an HTTP request/response exceeds the maximum header length, it can be a possible attack. Using the **Unusually large HTTP packets** indicator, you can view the occurrences where the HTTP messages with HTTP header size exceed the configured values.

Click the **Unusually large HTTP packets** tab to view the issue details.



The **Recommended Actions** to troubleshoot the issue are:

- Review the traffic to determine the header size is genuine. If the header size is genuine, then update the header value on the HTTP profile. For more information, see Buffer Overflow Check.
- If the header size is not genuine, add the source to the block list to avoid attacks.

Under **Details**, you can view:

- The time that occurred the anomaly
- Total occurrences
- The anomaly severity such as high, low, and medium
- The detection message indicating the current HTTP header length configured on the virtual server, server, or service group

TCP reassembly queue limit hits

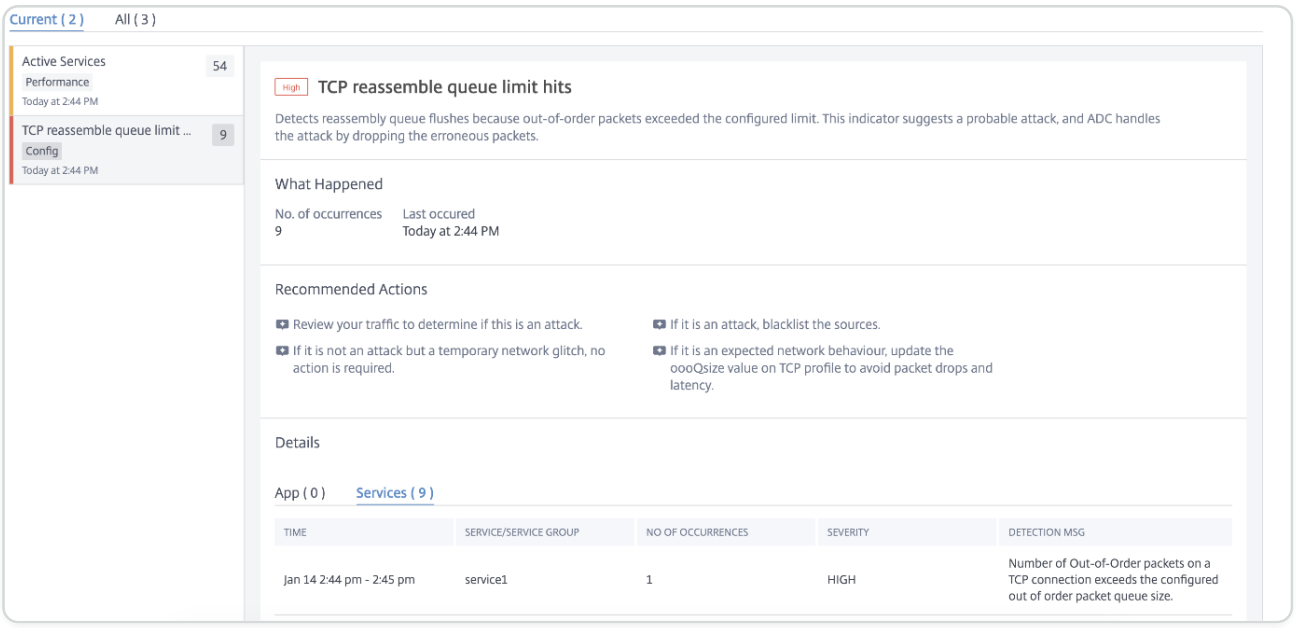
TCP maintains an Out-of-Order queue to keep the OOO packets in the TCP communication. This setting impacts NetScaler memory if the queue size is long as the packets need to be kept in runtime memory.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This needs to be kept at an optimized level based on the kind of network and application characteristics.

Using the **TCP reassemble queue limit hits** indicator, you can view if the Out-of-Order packets on a TCP connection exceed the configured out of order packet queue size.

Click the **TCP reassemble queue limit hits** tab to view the issue details.



The **Recommended Actions** to troubleshoot the issue are:

- Review the traffic and add the source to block list if it is an attack
- If this is an expected network behavior, then update the out-of-order packets size value on TCP profile. For more information, see TCP Optimization
- If it is just a temporary network glitch, then no further action is required

Under **Details**, you can view:

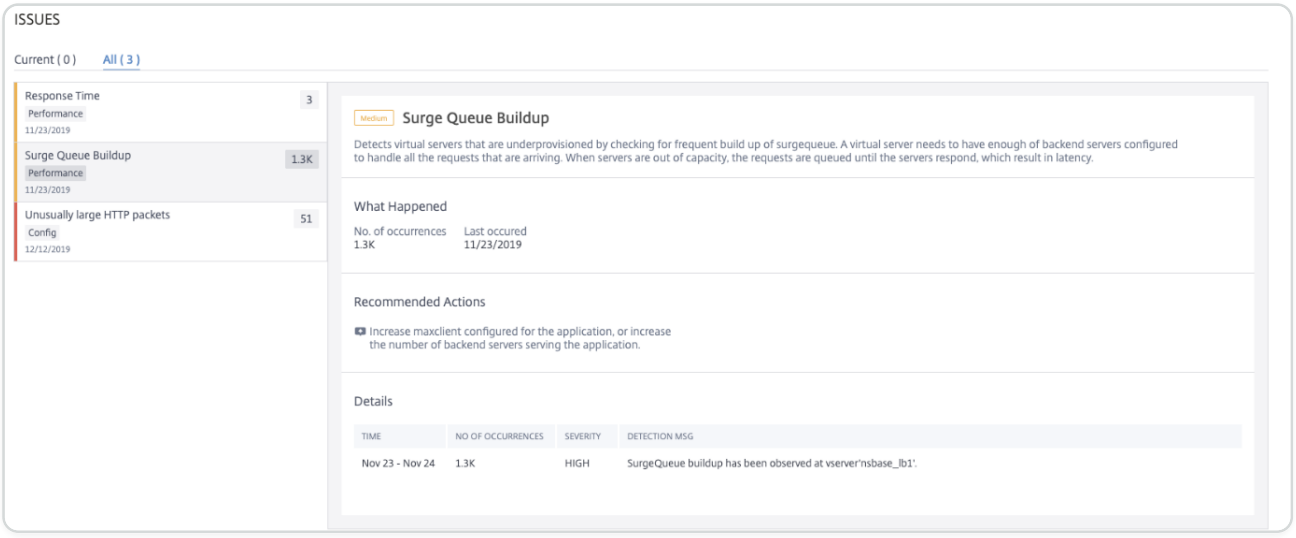
- The time that occurred the anomaly
- Total occurrences
- The anomaly severity such as low, medium, and high
- The detection message indicating the current TCP profile and oooQsize settings

Surge Queue Buildup

When a server receives a surge of requests, the server becomes slow to respond to the clients. Often, the overload also causes clients to receive error pages. A virtual server needs to have enough back end servers configured to handle the incoming requests.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Using the **Surge Queue Buildup** indicator, you can view the virtual servers that have surge queue buildup. Click the **Surge Queue Buildup** tab to view the issue details.



The **Recommended Actions** to troubleshoot the issue are:

- Increase the number of client connections limit. For more information, see Set a limit on the number of client connections
- Increase the back-end servers to serve the application requests

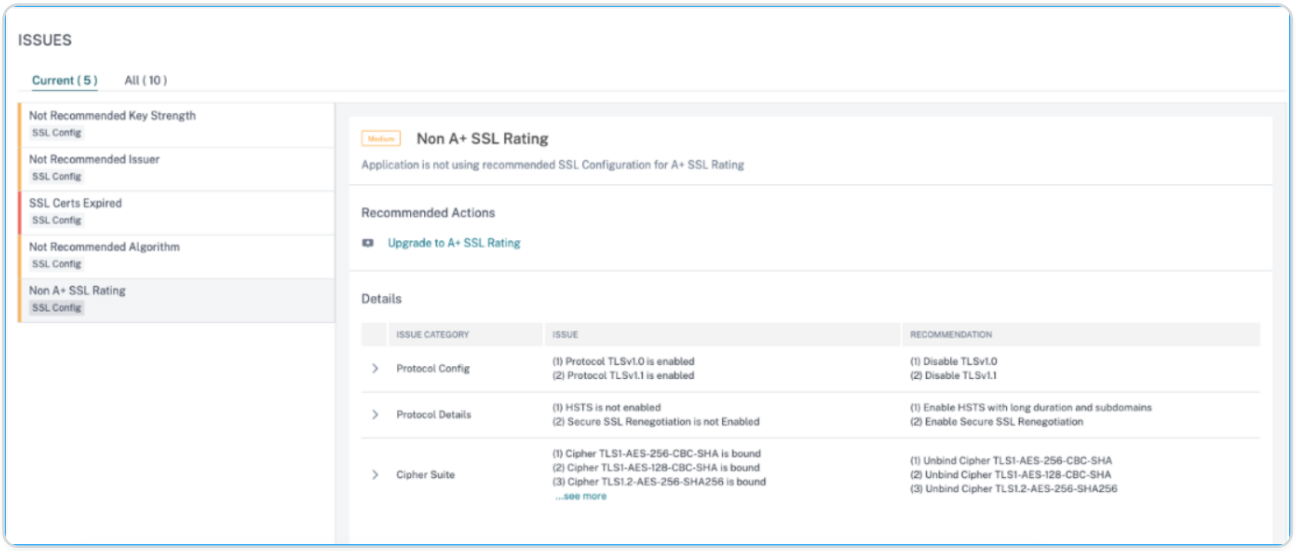
Under **Details**, you can view:

- The time that occurred the surge queue buildup anomaly
- Total occurrences
- The anomaly severity such as high, low, and medium
- The detection message indicating the surge queue buildup on the virtual server

SSL rating

When an application is not having an A+ SSL rating, the app score gets impacted. Using the **Non A+ SSL Rating** indicator, you can analyze the reasons for the application not having an A+ SSL rating. Click the **Non A+ SSL Rating** tab to view the issue details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **Recommended Action** to troubleshoot the issue is to upgrade it to A+ SSL rating. For more information, see Upgrade to A+ SSL Rating.

Under **Details**, you can view the issue details such as issue category, issue, and recommendation.

Troubleshoot App Dashboard

After you add an application in the App Dashboard, the dashboard immediately displays the app basic configuration details. The application analytics details such as app score, key metrics, and issues start to populate within a few minutes (approximately 10 to 15 minutes). For more information, see Applications.

You must ensure that there is no issue with metrics data flow (AppFlow collector or Analytics profile) from the NetScaler instance. You can get more information on AppFlow collector and analytics profile in this document.

This document describes the troubleshooting steps that you need to perform when:

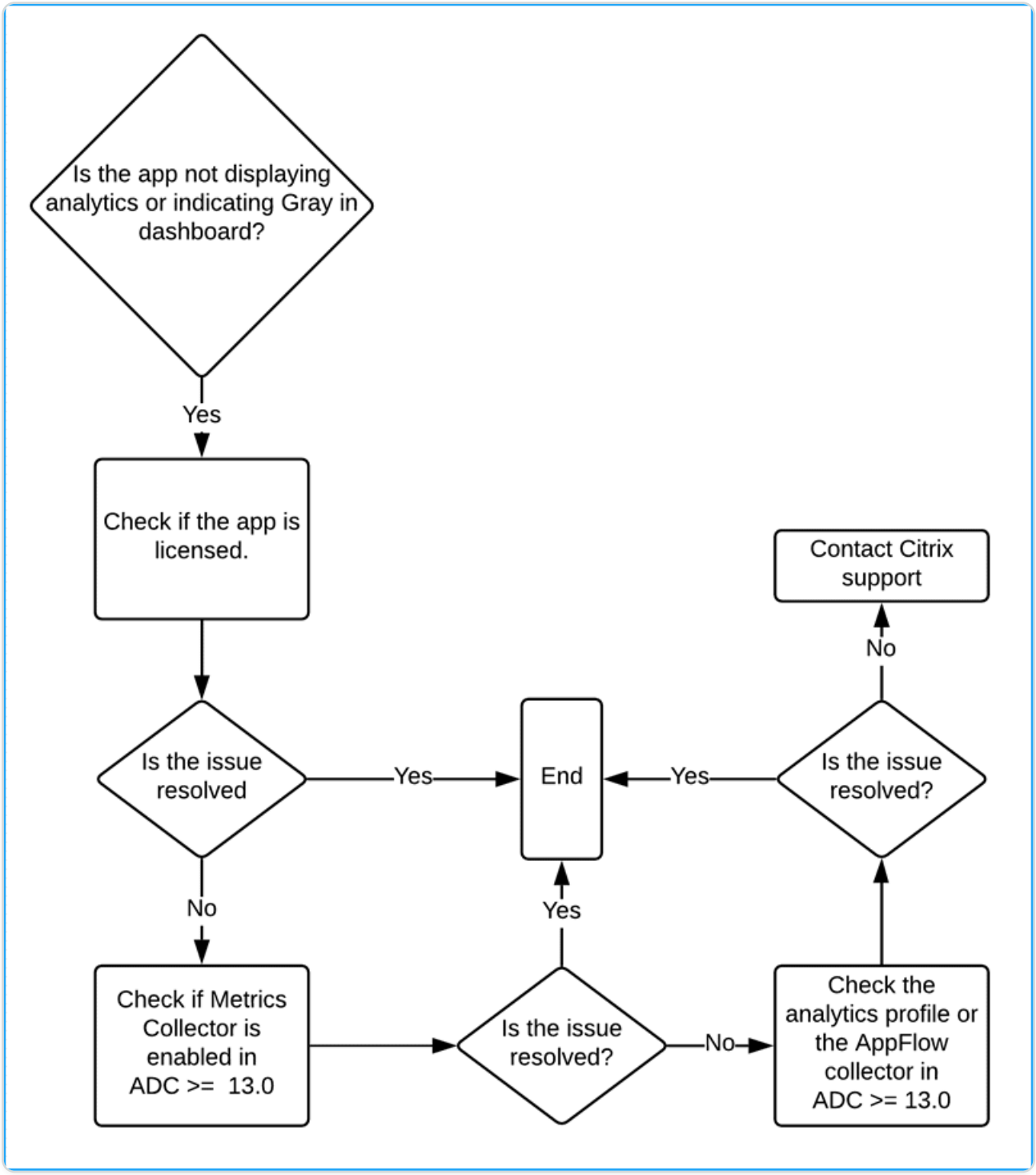
- You click an application, the analytics for the selected application do not display the required data even after the mentioned duration (10–15 minutes).
- The CS or LB application is always indicating Gray color (**Not Applicable** status) in App Dashboard.

NOTE

The troubleshooting procedures mentioned in this document are only applicable to **Content Switching** and **Load Balancing** virtual servers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting scenario



Application is licensed

You must ensure if the application is licensed.

- **NetScaler Console** - Navigate to **Settings > Licensing & Analytics Config** and verify if the application is licensed under **Virtual Server License Summary**. If the application is not licensed, see Manage licensing and enable analytics on virtual servers to license the virtual server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Metrics collector is enabled

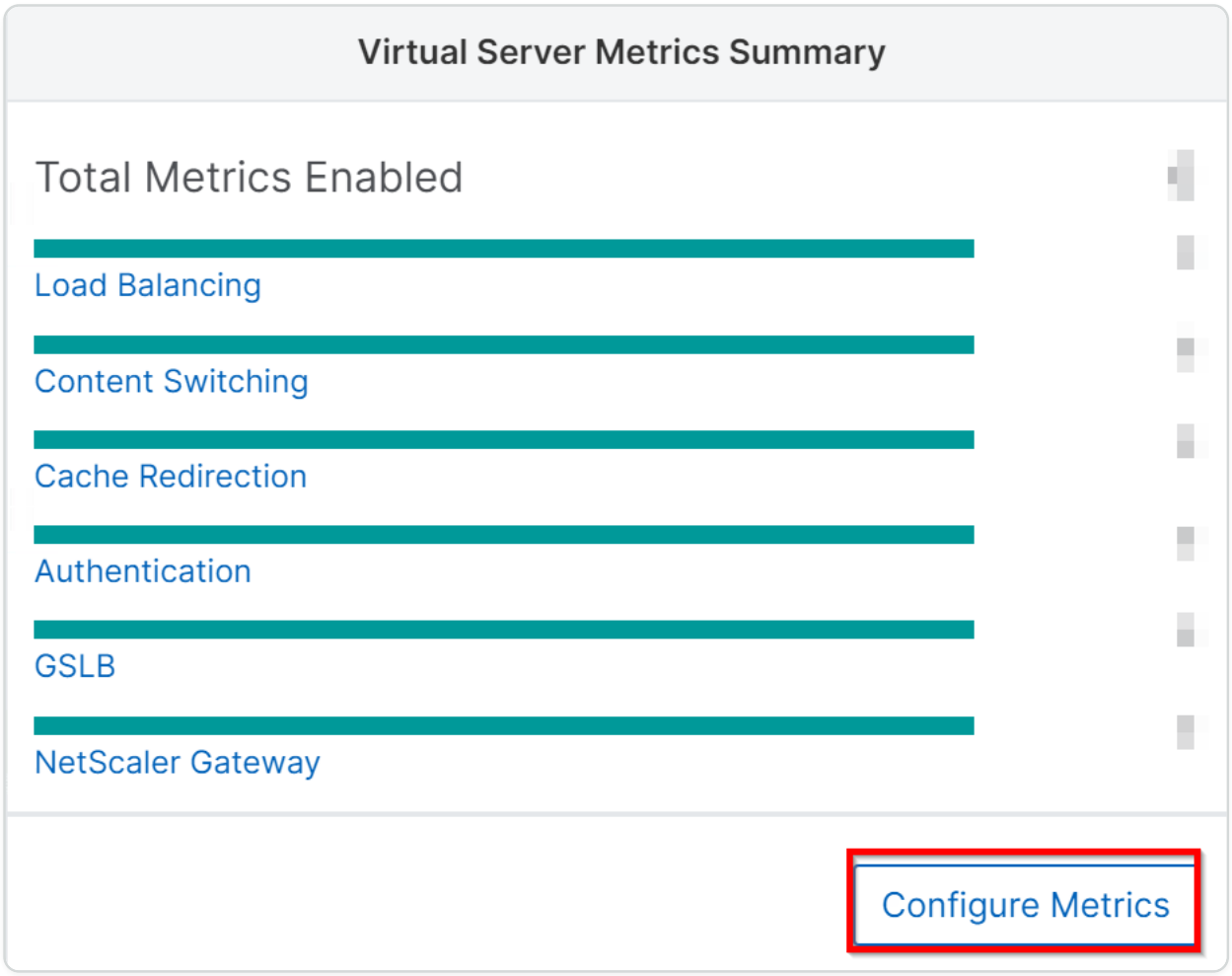
You must ensure if **Metrics Collector** is enabled in the NetScaler instance.

NOTE:

Starting from **14.1-21.x or later builds**, Metrics Collector is disabled by default in the new NetScaler instances added in NetScaler Console. The metrics collector configuration for the existing managed instances remain unchanged.

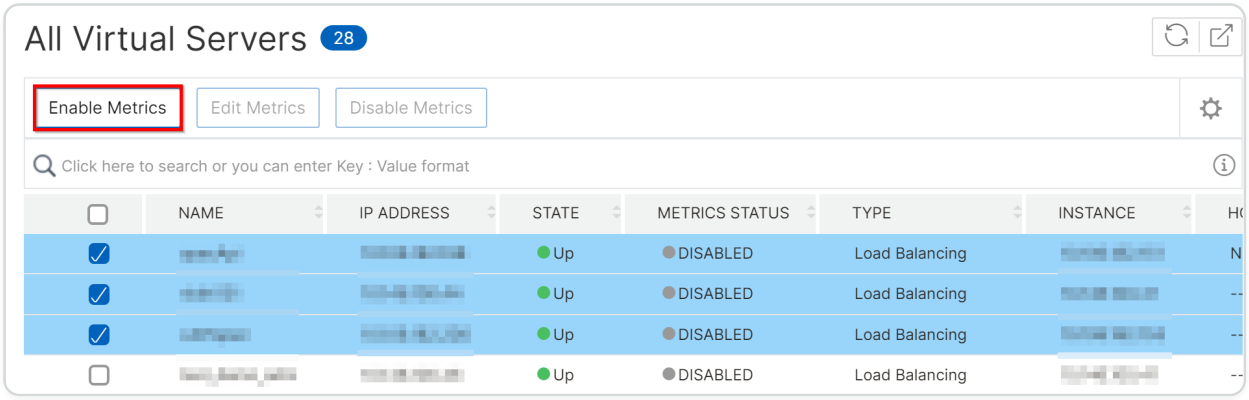
To ensure if metrics collector is enabled:

1. Navigate to **Settings > Analytics Configuration**.
2. Click **Configure Metrics** under **Virtual Server Metrics Summary**.

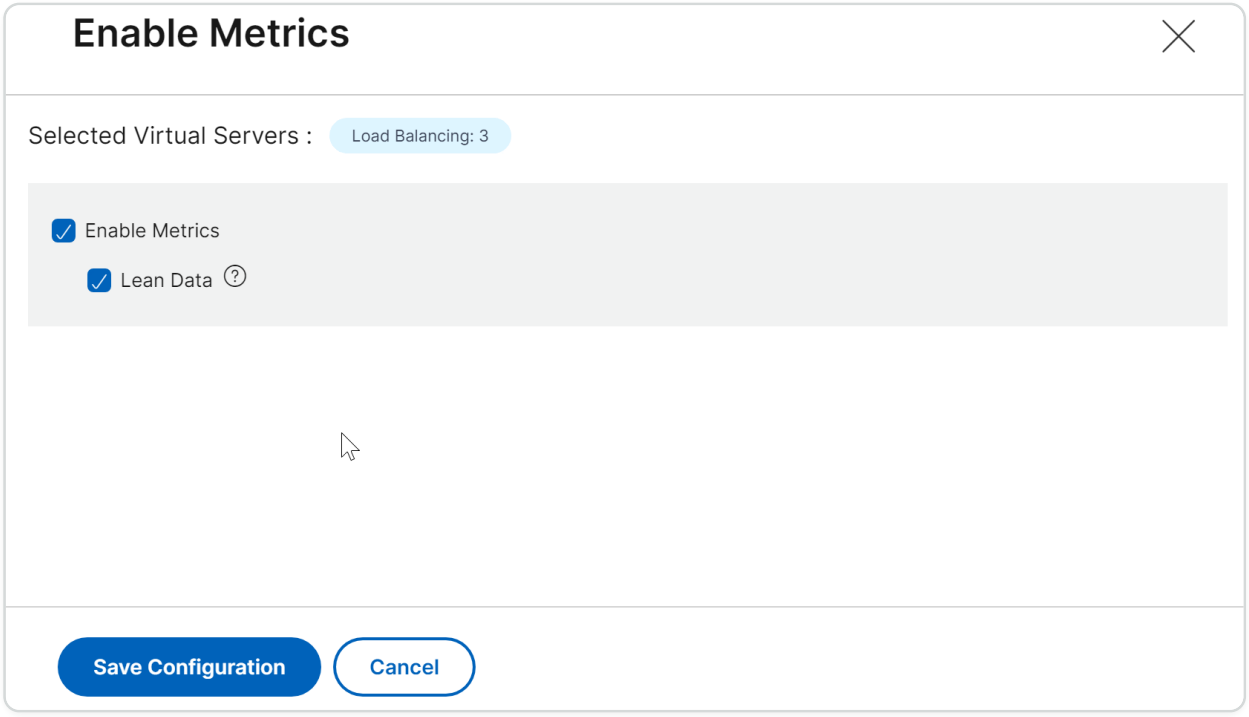


3. In the **All Virtual Servers** page, you can view the status of the metrics collector on each virtual server. Select the virtual servers that you want to enable and click **Enable Metrics**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Select **Enable Metrics** to enable Metrics Collector. You can also select **Lean Data** if you want to enable and view lean period usage analytics. After selecting, click **Save Configuration**.



Alternatively, you can also enable metrics collector and lean usage for the virtual servers from the NetScaler® instances page:

1. Navigate to **Infrastructure > Instances**, select the instance type, and select **Metrics Collector** from the **Select Action** list.
2. Select the virtual servers for which you want to enable metrics collector and click **Enable Metrics**.
3. Select **Enable Metrics** to enable Metrics Collector. You can also select **Lean Data** if you want to enable and view lean period usage analytics. After selecting, click **Save Configuration**.

After you enable metrics collector and if you are still not able to view the data, validate:

- The AppFlow collector in NetScaler instance version 13.0 **earlier than 47.x build**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The analytics profile in NetScaler instance build **47.x or later**.

NetScaler instance earlier than 47.x builds

In NetScaler:

1. Run the following command to ensure if the collector is **UP** and running at Port 5563:

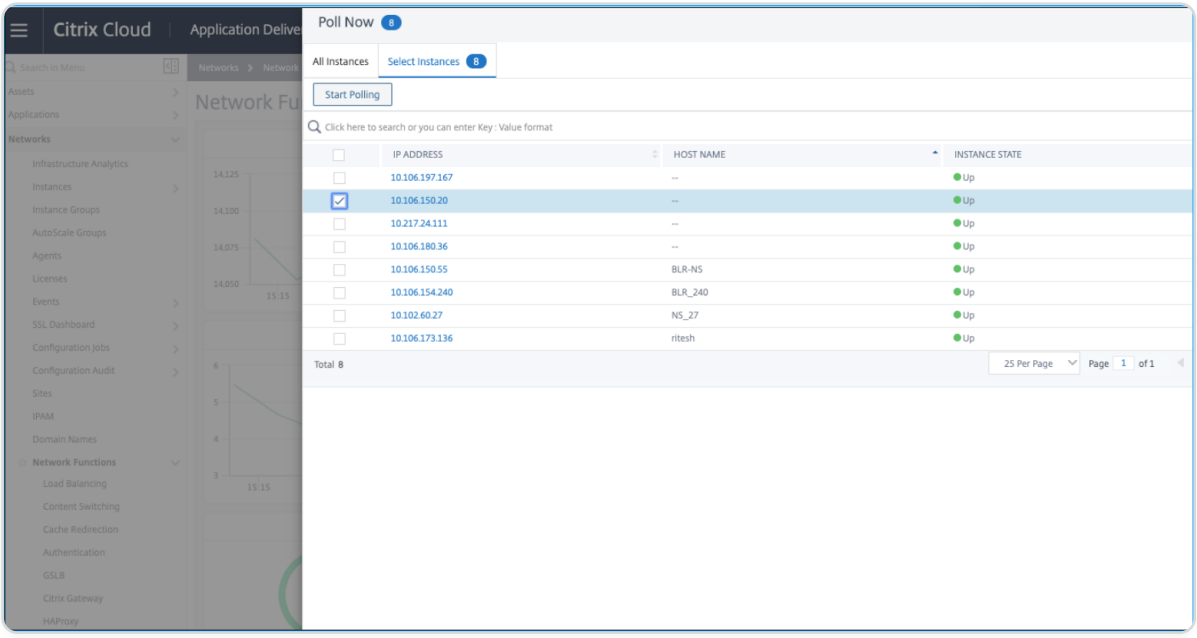
   ```
   sh appflow collector af_collector_rest_<adm_receiver_ip>
   ```

   ```
   > sh appflow collector af_collector_rest_10.102.103.114
   1) Name: af_collector_rest_10.102.103.114
   IPv4 address: 10.102.103.114
   Port: 5563
   Netprofile:
   Transport: rest
   State: UP
   Done
   ```

2. If no collector is available, do an instance manual polling in NetScaler Console.

   a. Navigate to **Infrastructure > Network Function > Poll Now**

   b. Select the instance and click **Start Polling**.

   If polling fails, remove the NetScaler instance from NetScaler Console and then add the NetScaler instance again. When you add the NetScaler instance, the collector gets added on NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If the collector indicates **Down** status:

1. Ensure if SNIP is configured.

```
> sh ip | grep SNIP
2)  10.106.150.34    0              SNIP            Active   Enabled  Enabled  NA       Enabled
```

   If SNIP is not configured, you must configure SNIP. For more information, see Configuring SNIP.

2. Ensure that if NetScaler instance is reachable to NetScaler Console.

   You can validate by doing a ping test. Run `ping -S <SNIP> <adm_receiver_ip>`

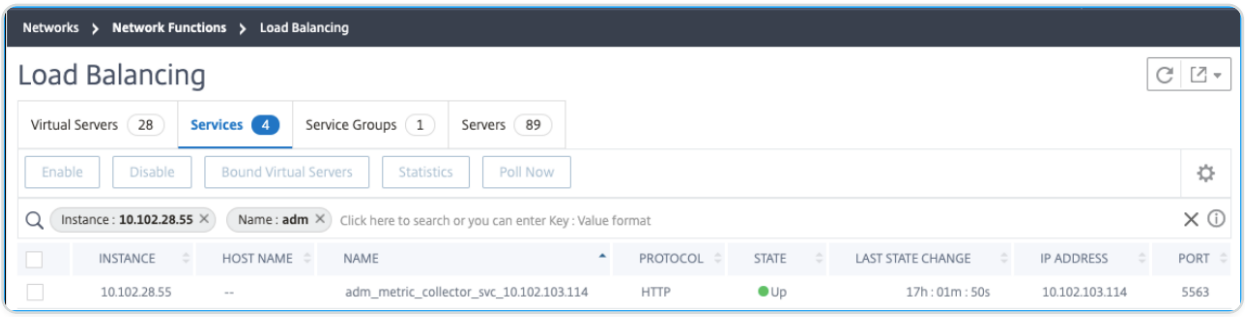
```
> ping -S 10.106.150.34 10.102.103.114
PING 10.102.103.114 (10.102.103.114) from 10.106.150.34: 56 data bytes
64 bytes from 10.102.103.114: icmp_seq=0 ttl=62 time=0.770 ms
64 bytes from 10.102.103.114: icmp_seq=1 ttl=62 time=0.446 ms
64 bytes from 10.102.103.114: icmp_seq=2 ttl=62 time=0.402 ms
```

NetScaler instance later than 47.x builds

In NetScaler Console, ensure that the metrics collector service is available:

1. Navigate to **Infrastructure > Network Function > Load Balancing > Services**.
2. On the search bar, filter by **Instance: (IP address)** and **Name: NetScaler Console**.
3. Ensure if `adm_metric_collector_svc_<adm_receiver ip>` is available. The IP address can be either the NetScaler Console management IP or the agent IP.

   Ensure that this service is in **UP** status and running at Port 5563.



If you still cannot view the data, ensure that the collector service is bound to time series analytics profile in NetScaler.

1. Log on to NetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Run the following command:

   `sh analytics profile ns_analytics_time_series_profile`

```
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector: adm_metric_collector_svc_10.102.103.114
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```

If the collector indicates **Down** status:

1. Ensure if SNIP is configured.

```
> sh ip | grep SNIP
2)  10.106.150.34    0              SNIP            Active   Enabled  Enabled  NA       Enabled
```

   If SNIP is not configured, you must configure SNIP. For more information, see Configuring SNIP.

2. Ensure that if NetScaler instance is reachable to NetScaler Console.

   You can validate by doing a ping test. Run `ping -S <SNIP> <adm_receiver_ip>`

```
> ping -S 10.106.150.34 10.102.103.114
PING 10.102.103.114 (10.102.103.114) from 10.106.150.34: 56 data bytes
64 bytes from 10.102.103.114: icmp_seq=0 ttl=62 time=0.770 ms
64 bytes from 10.102.103.114: icmp_seq=1 ttl=62 time=0.446 ms
64 bytes from 10.102.103.114: icmp_seq=2 ttl=62 time=0.402 ms
```

3. Ensure that the traffic connectivity through telnet is able to connect the service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
root@ns# telnet 10.102.103.114 5563
Trying 10.102.103.114...
Connected to 10.102.103.114.
Escape character is '^]'.
^]
telnet> q
Connection closed.
```

If telnet is able to connect the service, then a firewall exists and is blocking the metric data flow. You must resolve the firewall block issue.

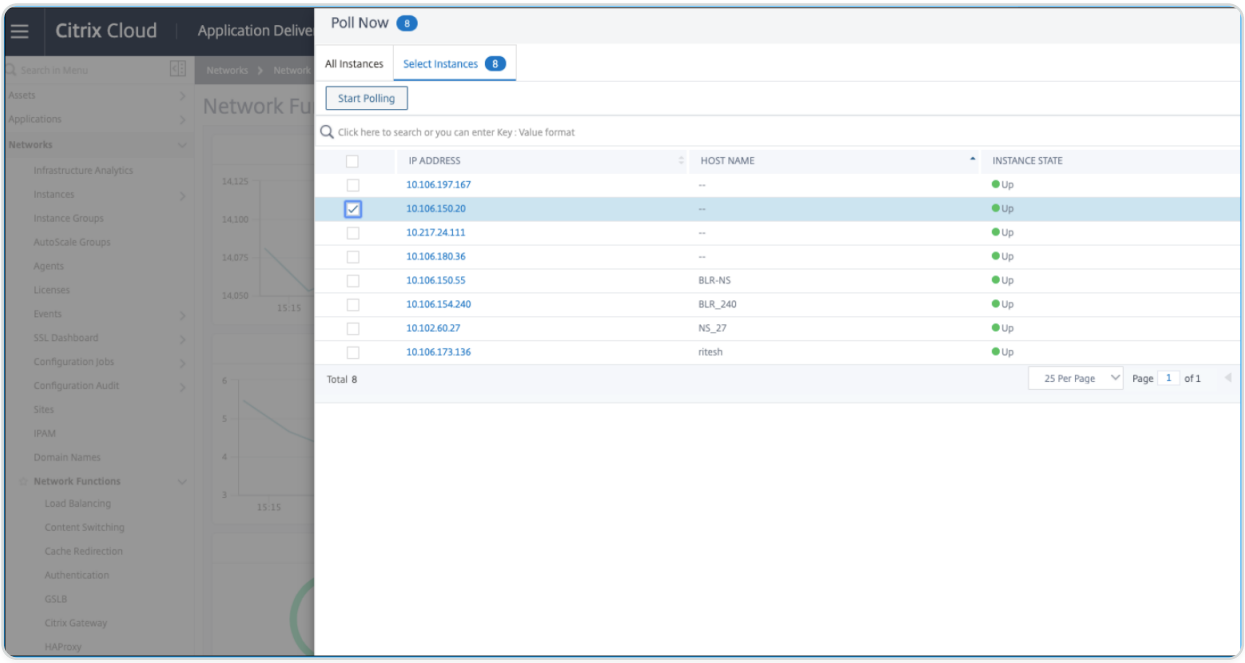
If no collector service is bound to time series analytics profile in NetScaler, the Collector is displayed as blank.

```
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector:
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```

You must do an instance manual polling in NetScaler Console.

1. Navigate to **Infrastructure > Network Function > Poll Now**
2. Select the instance and click **Start Polling**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



If polling fails, add the collector service directly at NetScaler instance using the following commands:

```
add service adm_metric_collector_svc_<adm_receiver_ip> <adm_receiver_ip> HTTP 5563
```

```
unset analyticsprofile ns_analytics_time_series_profile -collectors
```

```
set analytics profile ns_analytics_time_series_profile -collectors adm_metric_collector_svc_<adm_receiver_ip> -metrics enabled -events enabled
```

The analytics time series profile is updated.

```
> add service adm_metric_collector_svc_10.102.103.114 10.102.103.114 HTTP 5563
 Done
> unset analyticsprofile ns_analytics_time_series_profile  -collectors
 Done
> set analytics profile ns_analytics_time_series_profile -collectors adm_metric_collector_svc_10.102.103.114 -metrics enab
 Done
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector: adm_metric_collector_svc_10.102.103.114
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```

If the issue still persists even after performing all the mentioned troubleshooting steps, contact **NetScaler support**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Application usage and anomalies

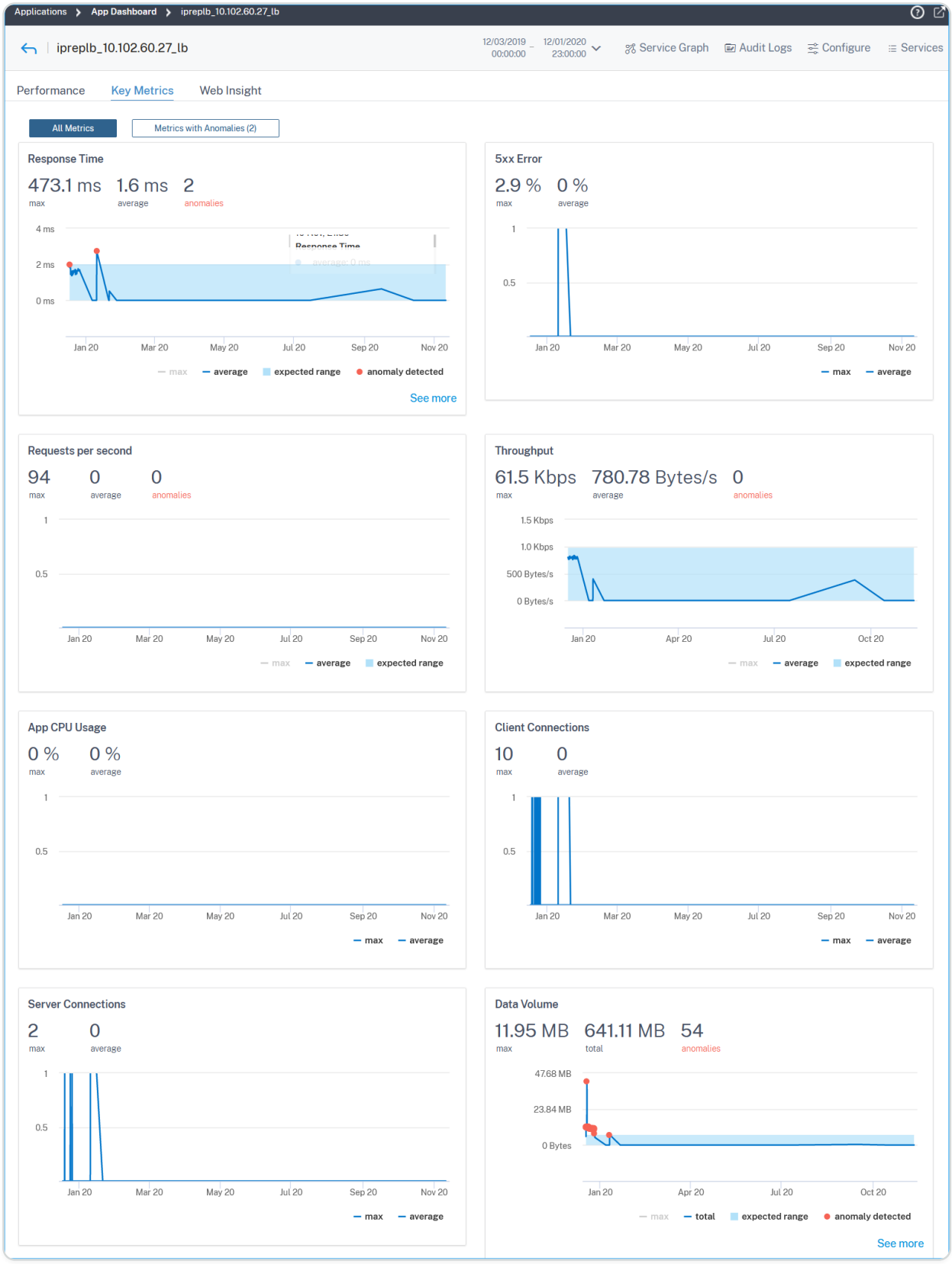
As an administrator, you must ensure how the application is getting utilized. The application key metrics can help you identify the application usage. Since the traffic range to the application is unpredictable, some unusual application performance deviations might occur for a specific duration. In such scenarios, as an administrator, you might want to view and analyze such sudden anomalies, and ensure if any immediate troubleshoot is required.

NetScaler Console detects such anomalies and provides necessary details. Navigate to **Applications > Dashboard**, click an application, and select the **Key Metrics** tab. NetScaler Console monitors the traffic pattern and analyzes if the key metrics are in the expected range. If there is any deviation than the expected range, NetScaler Console reports those deviations as anomalies.

You can view anomalies for the following key metrics:

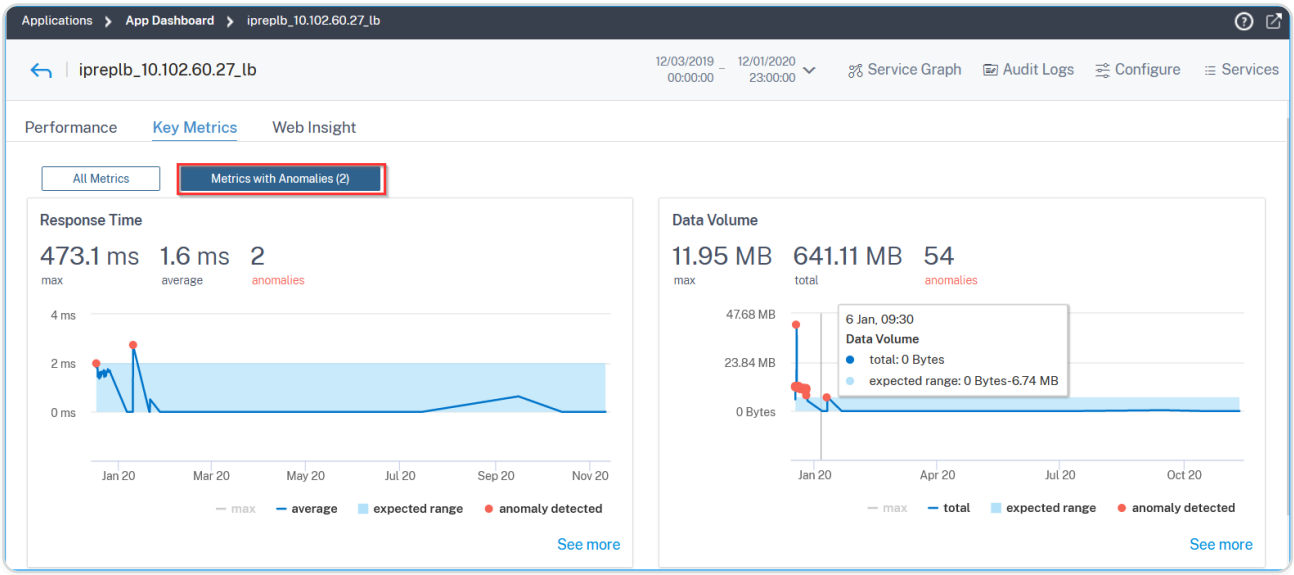
- Response Time
- Throughput
- Data Volume
- Requests per second

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Click the **Metrics with Anomalies** tab to view details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



In each metric, you can also click the **See more** option to view details. The following example is for the application data volume:



You can view:

- The graph indicating the maximum value, total value, expected range, and anomalies
- The **Recommended Actions** to troubleshoot the issue
- The time and anomaly details under **Details**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Peak and lean usage analytics

A web application can either receive high traffic or low traffic, and the traffic range for each day or hour is certainly unpredictable. Similarly, a web application also requires downtime for a specific duration during a scheduled maintenance or an upgrade. As an administrator, you must analyze the traffic and find a right time to:

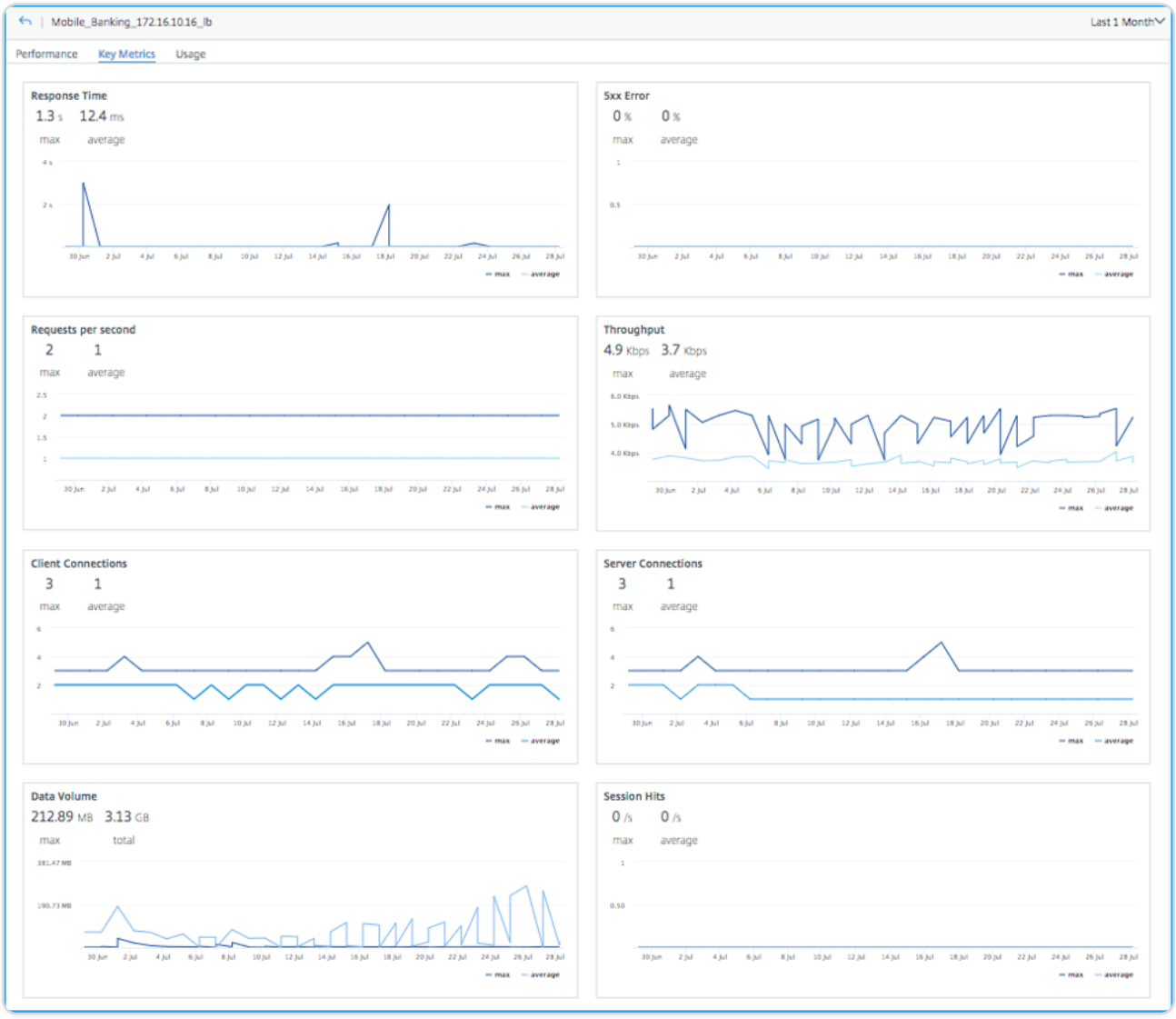
- Scale up the web application
- Plan a web application downtime

The peak usage and lean period analytics feature in NetScaler Console enables you to analyze the key metrics for a selected time duration. From these metrics, you can analyze the traffic and take decision on when you want to scale up the web application or plan a scheduled downtime.

Assess app scale limits

Click an application from the **App Dashboard** and select the **Key Metrics** tab to visualize the consolidated view of all metrics. Select the time duration from the list to analyze the metrics.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For each metric, you can view:

- **Max** – Indicates the maximum value for the selected duration
- **Average** – Indicates the average value for the selected duration

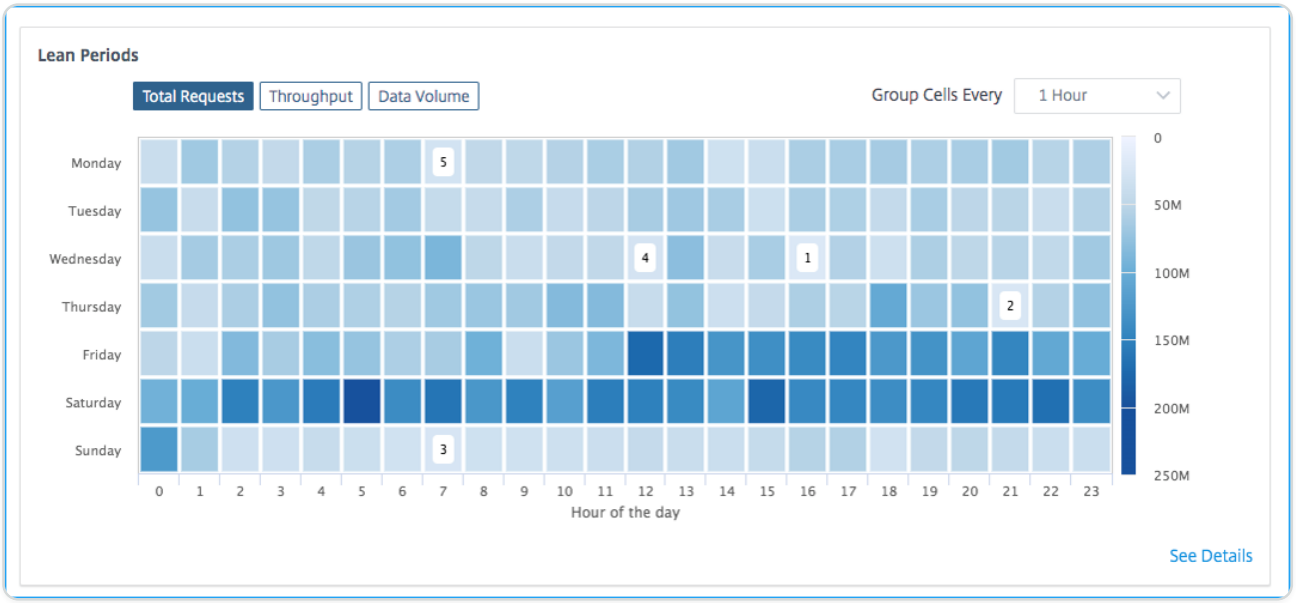
According to the example in the image, the max value for Response Time indicates 1.3 s. From the graph chart, you can analyze how many times the high response time has occurred for the selected time duration. Similarly, you can also view details for other metrics, analyze if the application has received a peak usage, and take decision to scale up the production environment.

Identify top 5 app maintenance window

Click an application from the **App Dashboard** and select the **Key Metrics** tab to view the lean period for the application. A typical downtime for an application can be 1-hour, 2-hour, or 4-hour, depending upon the requirement. You can select the time from the list (1-hour, 2-hour, or 4-hour) that you want to plan for the downtime. After you select the time from the list, you can analyze the traffic for metrics such as Total Requests, Throughput, and Data Volume. You can select the right

© 1997–2026 Citrix Systems, Inc. All rights reserved.

time to schedule for a downtime, when the application usage is less. The following example is to analyze the downtime for the 1-hour duration.



The heatmap view indicates the application usage for the selected time duration. The darker the color (blue), indicates the application usage is higher.

The heatmap view also suggests the top 5 least period (1, 2, 3, 4, and 5) to plan for the application downtime.

1 – Indicates the first suggestion for Wednesday from 4 pm to 5 pm

2 – Indicates the second suggestion for Thursday from 9 pm to 10 pm

3 – Indicates the third suggestion for Sunday from 7 am to 8 pm

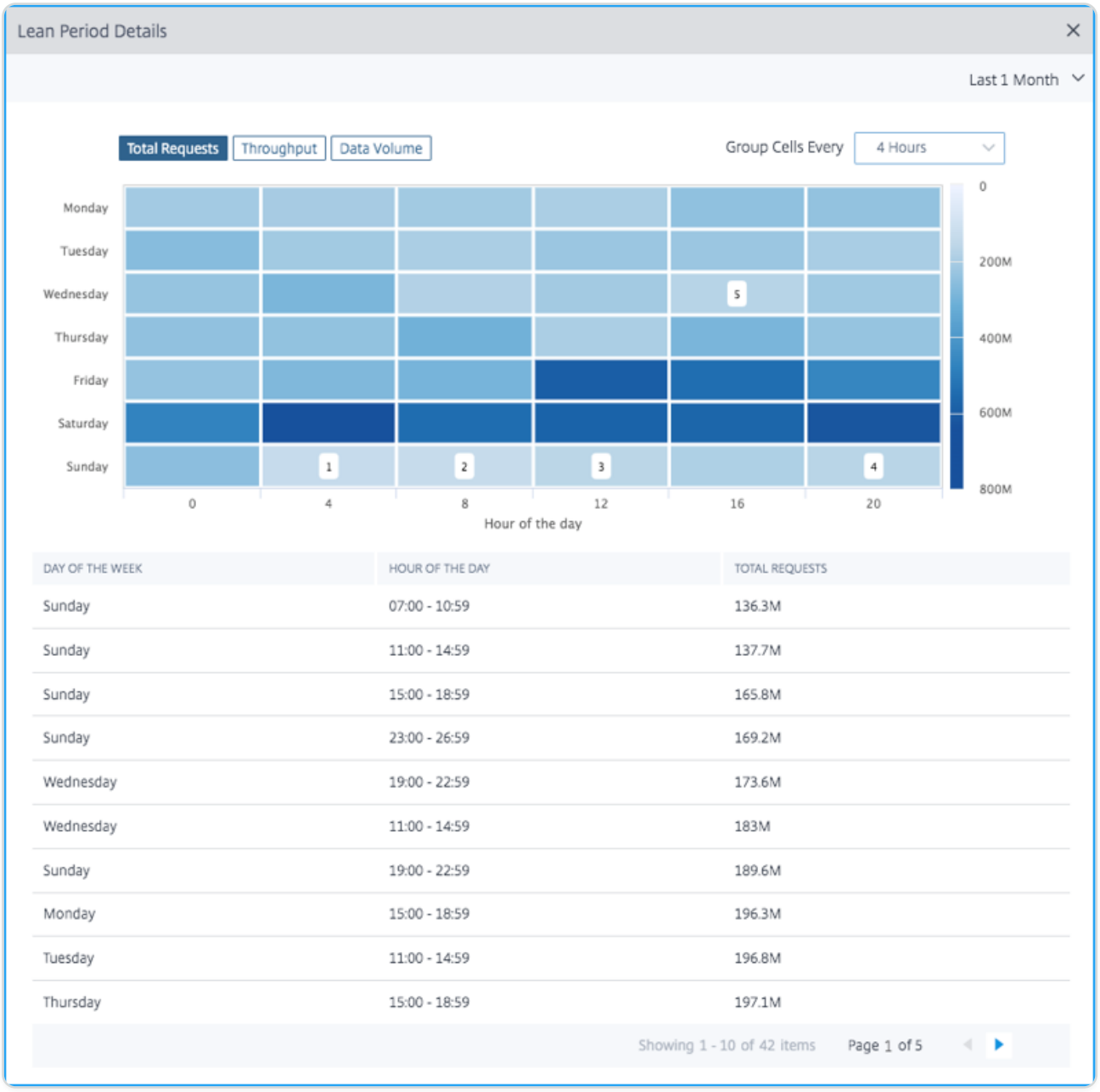
4 – Indicates the fourth suggestion for Wednesday from 12 pm to 1 pm

5 – Indicates the fifth suggestion for Monday from 7 am to 8 pm

You can also select any other day and time to schedule a downtime, after analyzing the traffic for all other days.

Click **See Details** to view further detailed information. Click the **Total Requests**, **Throughput**, or **Data Volume** tab to view details for the top 5 least period and also for the other days.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



DAY OF THE WEEK	HOUR OF THE DAY	TOTAL REQUESTS
Sunday	07:00 - 10:59	136.3M
Sunday	11:00 - 14:59	137.7M
Sunday	15:00 - 18:59	165.8M
Sunday	23:00 - 26:59	169.2M
Wednesday	19:00 - 22:59	173.6M
Wednesday	11:00 - 14:59	183M
Sunday	19:00 - 22:59	189.6M
Monday	15:00 - 18:59	196.3M
Tuesday	11:00 - 14:59	196.8M
Thursday	15:00 - 18:59	197.1M

Showing 1 - 10 of 42 items Page 1 of 5

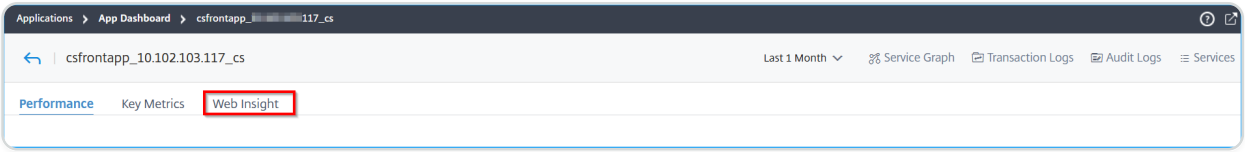
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Application usage analytics

Application owners must have the ability to evaluate and visualize the complete application from the perspectives of performance and usage.

The improvised **App Dashboard** enables you to view all the application performances and usage metrics together. When you click an application, apart from the existing application performance metrics, the **Web Insight** tab displays the metrics details that help you:

- Understand your application usage.
- Correlate any performance deviations with the usage metrics.



NOTES:

- Starting from **14.1-51.x** release, Web Insight analytics are visible for virtual servers that are configured with an IPv6 address.
- Starting from **14.1-1.16** or later release, when you drill down a metric, the analytics view in the time series graph displays nil values (for example, 0 ms and 0 request) for the selected duration. Earlier, if there was no traffic or transaction received for the selected duration, the analytics view displayed the graphs by skipping those nil values.
- For each metric, you can view options that indicate maximum value and total value. For example:

```
>-  ![Example1](/content/dam/netscaler/us/en/netscaler-console-service/
media/wi-sample.png) - The maximum client network latency for the
selected duration. Consider that you have the network latency for
client 1 = 30 ms, client 2 = 15 ms, and client 3 = 3 ms. In this
scenario, the **Client Network Latency** displays 30 ms.

>
```

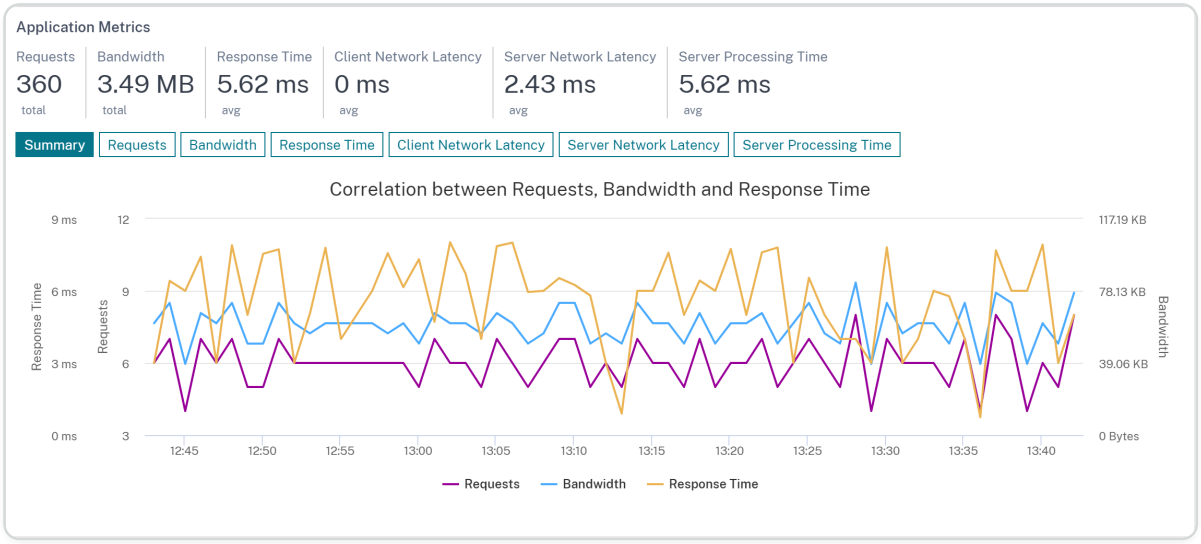
© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
>-  ![Example2](/content/dam/netscaler/us/en/netscaler-console-service/
media/wi-sample1.png) - The total bandwidth consumed across all
available clients/servers for the selected duration. Consider that you
have the bandwidth consumption for client 1 = 30 MB, Client 2 = 45 MB,
Client 3 = 40 MB. In this scenario, the Bandwidth displays (30 MB + 45
MB + 40 MB) = 115 MB.
```

The following are the metrics you can view from the **Web Insight** tab for the selected duration:

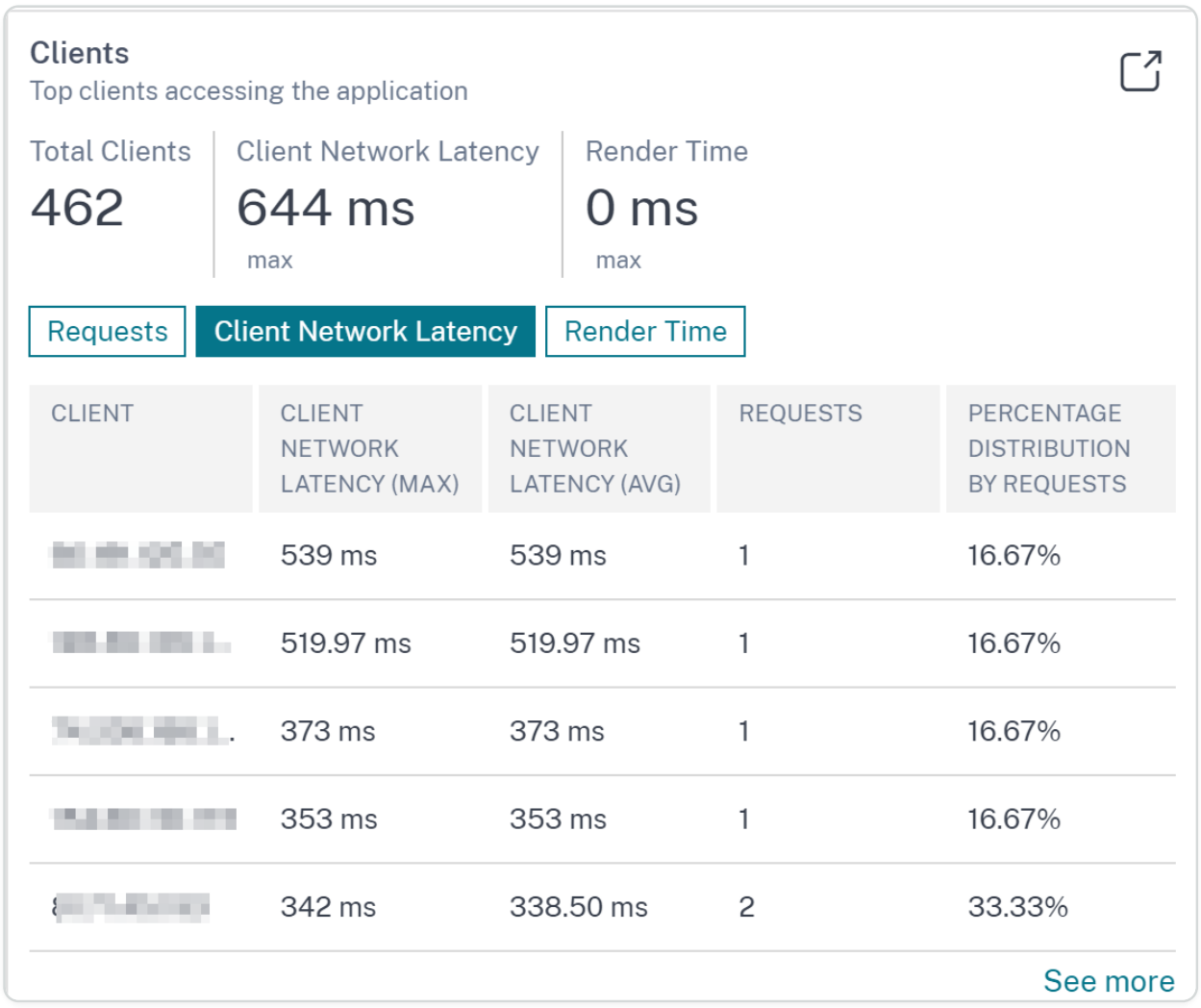
- **Application Summary** - Displays an overview of the application metrics.
  - **Requests** – Displays the total requests received by the application. The **Requests** tab shows the graph view for the total requests and the top 5 client requests. You can use the toggle option to customize the view.
  - **Bandwidth** – Displays the total bandwidth processed by the application. The **Bandwidth** tab shows the graph view for the total bandwidth and the top 5 servers bandwidth. You can use the toggle option to customize the view.
  - **Response Time** – Displays the average response time from the application. The **Request Time** tab shows the graph view of the response time breakdown and client latency, server latency, and server processing time for the selected duration. You can use the toggle option to customize the view.
  - **Client Network Latency** – Displays the average latency from the client. The **Client Network Latency** tab shows the graph view of the latency breakdown for the selected duration.
  - **Server Network Latency** – Displays the average latency from the server. The **Server Network Latency** tab shows the graph view of the latency breakdown for the selected duration.
  - **Server Processing Time** – Displays the average processing time from the server. The **Server Processing Time** tab shows the graph view of the processing time breakdown for the selected duration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **Summary** tab enables you to visualize the correlation between the requests, bandwidth, and response time in graph view.

- **Clients** – Displays the insights for clients accessing the application:



  - **Total Clients** – Displays the total clients accessing the application. Click the **Requests** tab to view:

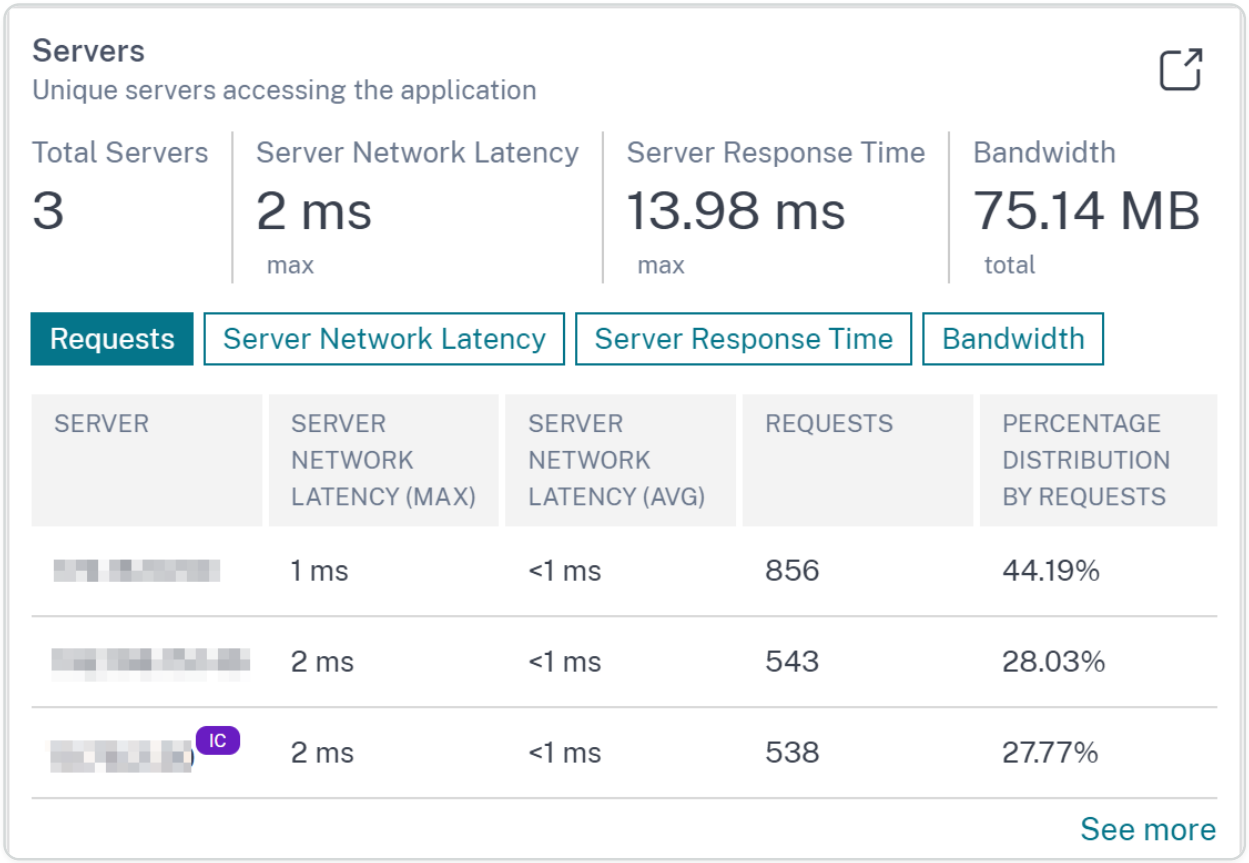
© 1997–2026 Citrix Systems, Inc. All rights reserved.

        - **Client** – The client IP address.
        - **Client Network Latency (avg)** – The average network latency from the client.
        - **Client Network Latency (max)** – The maximum network latency from the client.
        - **Requests** – The total requests from the client.
        - **Percentage distribution by requests** – The percentage distribution based on the requests. For example, if the total client is 4 and each client has 100 requests, the percentage distribution for each client is 25%.
    - **Client Network Latency** – Displays the network latency from client to NetScaler. Click the **Client Network Latency** tab to view:
        - **Client** – The client IP address.
        - **Client Network Latency (avg)** – The average network latency from the client.
        - **Client Network Latency (max)** – The maximum network latency from the client.
        - **Requests** – The total requests from the client.
        - **Percentage distribution by requests** – The percentage distribution based on the requests.
    - **Render Time** – Displays the time taken to render the server response. Click the **Render Time** tab to view:
        - **Client** – The client IP address.
        - **Render Time (avg)** – The average render time from the client.
        - **Requests** – The total requests from the client.
        - **Percentage distribution by requests** – The percentage distribution based on the requests.
- **Servers** – Displays the insights for servers accessing the application.

NOTE

For integrated cache requests, you can view the NetScaler virtual server IP address with an IC notification. For more information, see Integrated cache requests.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

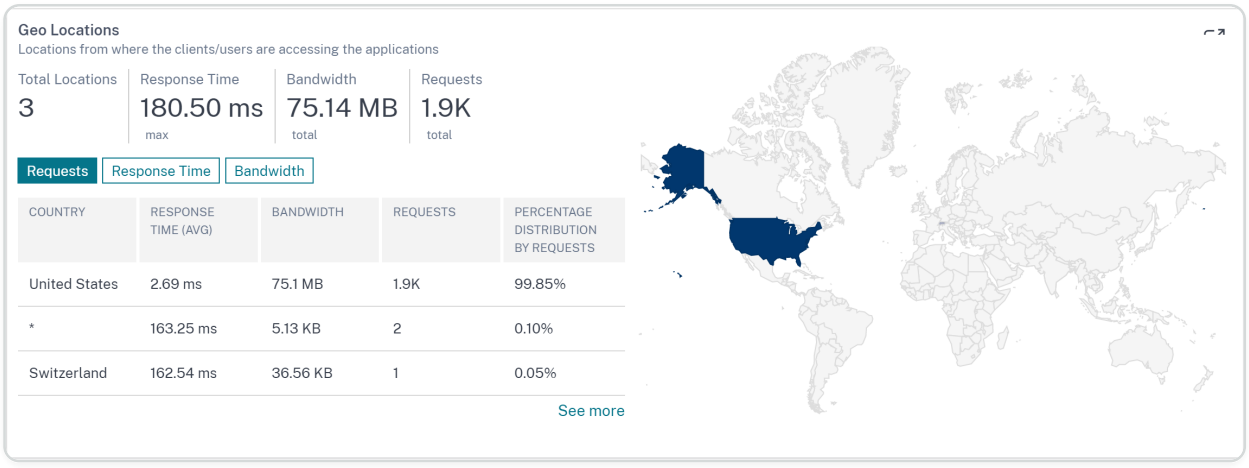


- **Total Servers** – Displays the total servers accessing the application. Click the **Requests** tab to view:
  - **Server** – The server IP address.
  - **Server Network Latency (avg)** – The average network latency from the server.
  - **Server Network Latency (max)** – The maximum network latency from the server.
  - **Requests** – The total requests from the server.
  - **Percentage distribution by requests** – The percentage distribution based on the requests. For example, if the total servers are 10, and if each server has 1000 requests, the percentage distribution for each server is 10%.
- **Server Network Latency (Max)** – Displays the maximum network latency from the server to NetScaler. Click the **Server Network Latency** tab to view:
  - **Server** – The server IP address.
  - **Server Network Latency (avg)** – The average network latency from the server.
  - **Server Network Latency (max)** – The maximum network latency from the server.
  - **Requests** – The total requests from the server.
  - **Percentage distribution by requests** – The percentage distribution based on the total requests.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Server Response Time (Max)** – Displays the maximum time taken for the server to respond to requests. Click the **Server Response Time** tab to view:
  - **Server** – The server IP address.
  - **Server Response Time (avg)** – The average response time from the server.
  - **Server Response Time (max)** – The maximum response time from the server.
  - **Requests** – The total requests from the server.
  - **Percentage distribution by requests** – The percentage distribution based on the total requests.
- **Bandwidth** – Displays the total bandwidth consumed by the servers. Click the **Bandwidth** tab to view:
  - **Server** – The server IP address.
  - **Bandwidth** – The total bandwidth consumed from the server.
  - **Requests** – The total requests from the server.
  - **Percentage distribution by requests** – The percentage distribution based on the total requests.

- **Geo Locations** – Displays the insights for clients accessing the application from a particular location:



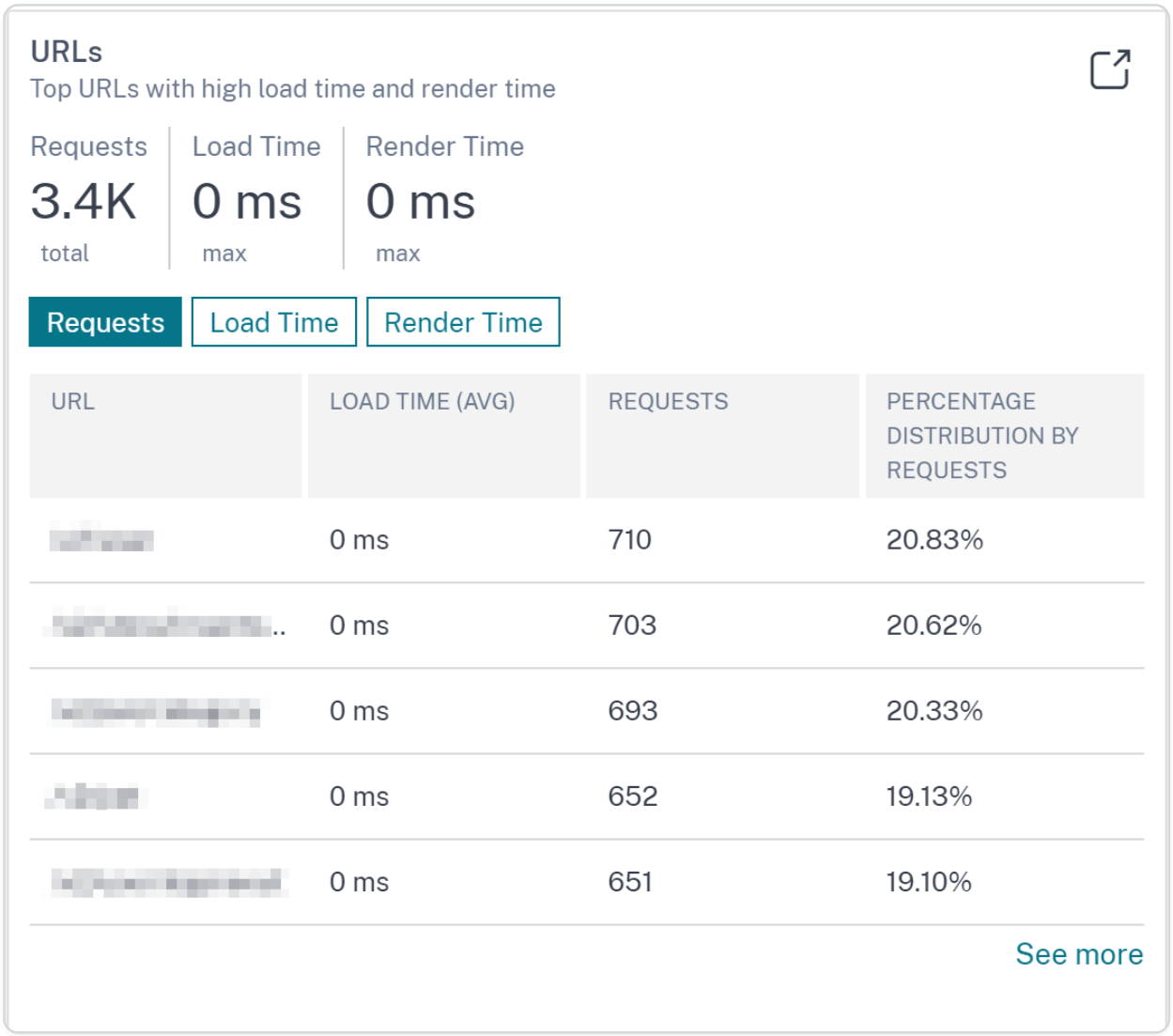
  - **Total locations** – Displays the total client locations accessing the application.
  - **Response Time** – Displays the response time from the client location.
  - **Bandwidth** – Displays the total bandwidth consumed by clients across all locations.
  - **Requests** – Displays the total requests from all client locations.

    Click each tab to view:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Country** – The location name.
- **Response Time** – The average response time from the client location.
- **Bandwidth** – The bandwidth consumed from the client location.
- **Requests** – The total requests from the client location.
- **Percentage distribution by requests** – The percentage distribution based on the total requests. For example, if the total locations are 10, total requests are 1 million, and Country A alone receives 0.9 million, then the percentage distribution for Country A is 90%. The other countries receive the remaining percentage distribution based on the requests received in each country.

- **URLs** – Displays the insights for URLs with high load and render time:



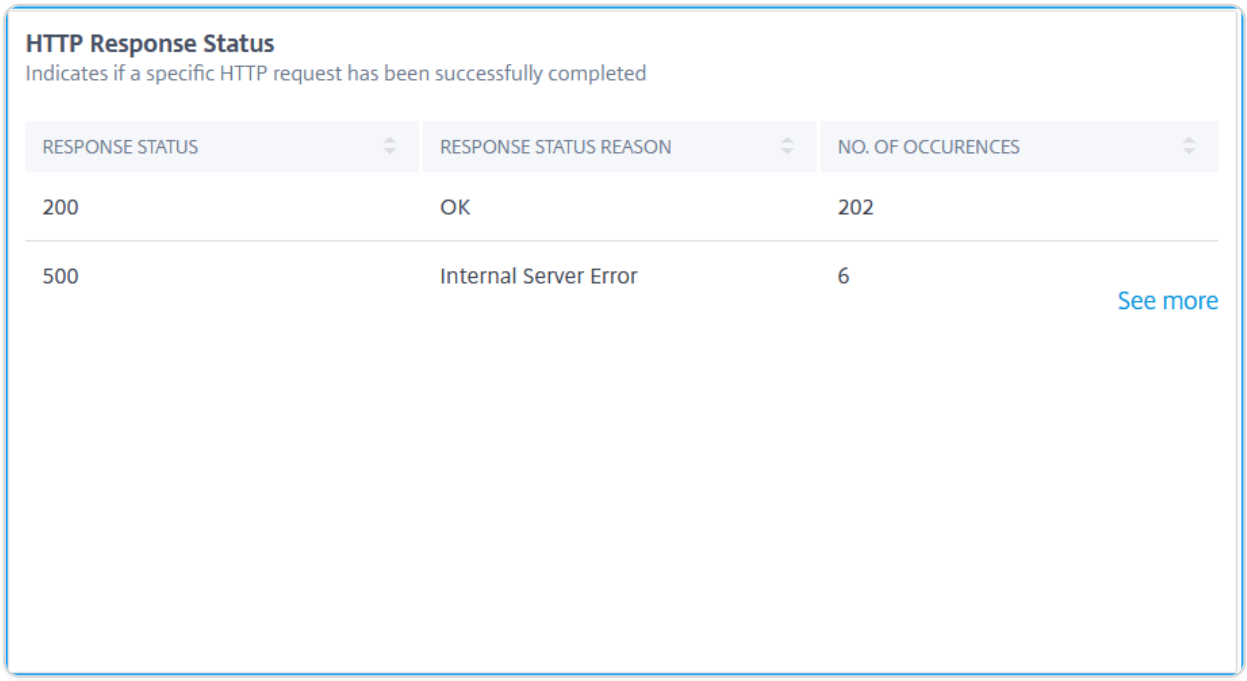
- **Total URLs** – Displays the total URLs. Click the **Requests** tab to view:
  - **URL** – The URL name.
  - **Load Time (avg)** – The average time taken for the URL to load.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Requests** – The total requests from the URL.
- **Percentage distribution by requests** – The percentage distribution based on the total requests and in each URL.

- **Load Time** – Displays the time taken for the URL to load. Click the **Load Time** tab to view:
  - **URL** – The URL name.
  - **Load Time (avg)** – The average time taken for the URL to load.
  - **Requests** – The total requests from the URL.
  - **Percentage distribution by requests** – The percentage distribution based on the total requests.
- **Render Time** – Displays the time taken for the URL to render and display. Click the **Render Time** tab to view:
  - **URL** – The URL name.
  - **Render Time (avg)** – The average time taken for the URL to render.
  - **Requests** – The total requests from the URL.
  - **Percentage distribution by requests** – The percentage distribution based on the total requests.

- **HTTP Response Status** – Displays the insights for a specific completed HTTP request.

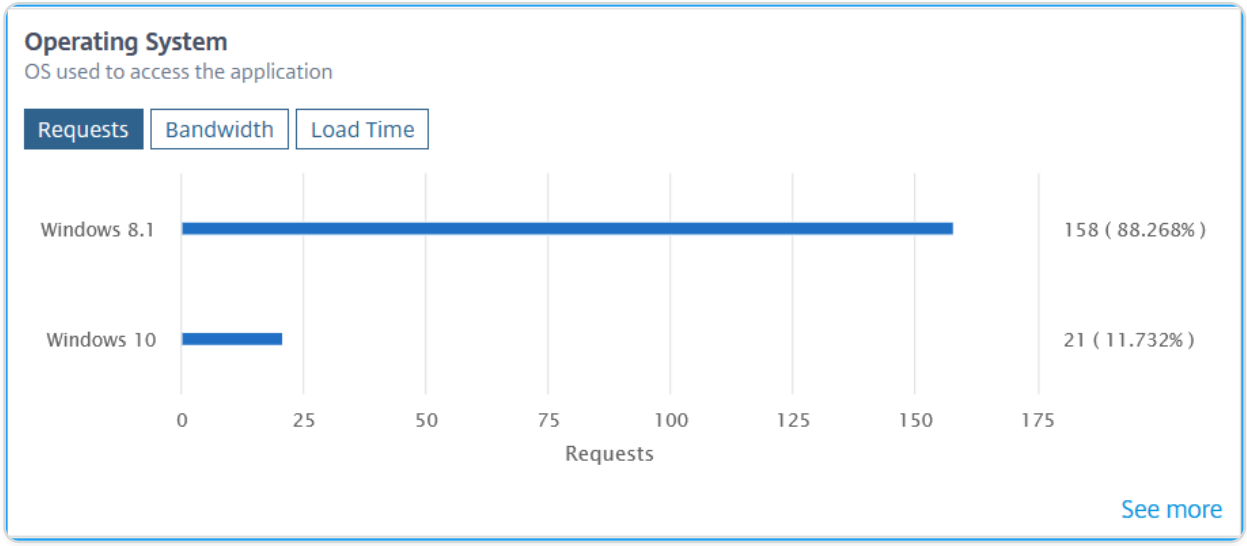


- **Response Status** – Displays the response code such as 2xx, 4xx, 5xx, and so on.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

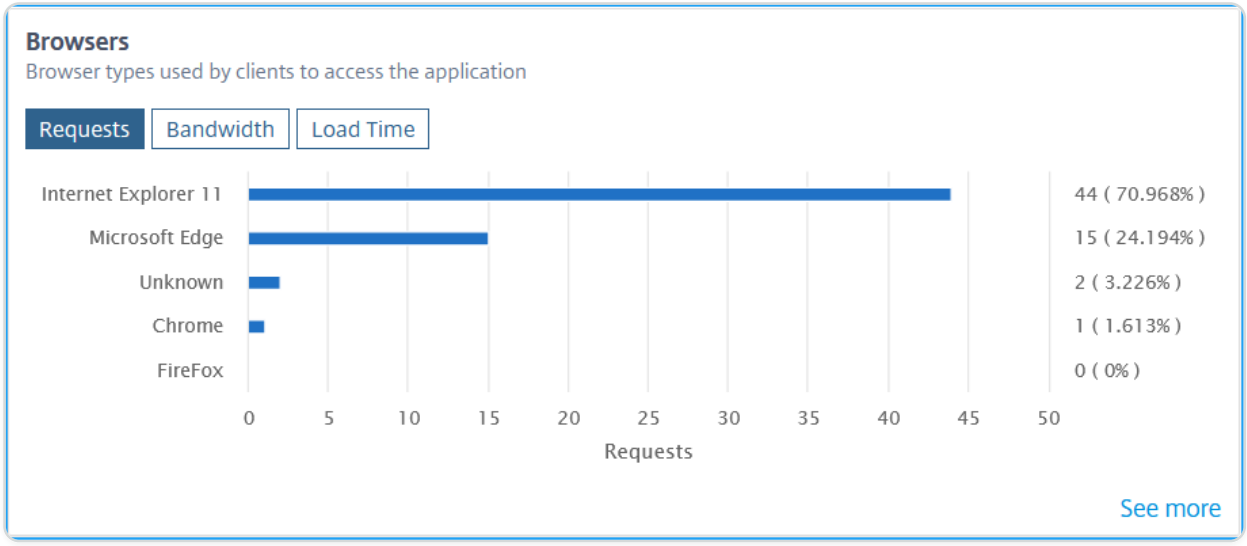
- **Response Status Reason** – Displays the response reason such as internal server error, Not found, and so on.
- **No of Occurrences** – Displays the total number of occurrences.

- **Operating system** – Displays the insights for the OS accessing the application.



- **Requests** – Displays the total requests from each operating system.
- **Bandwidth** – Displays the total bandwidth consumed by each operating system.
- **Load Time** – Displays the total time taken from each operating system to load from the server.

- **Browsers** – Displays the insights for the browser types used by the clients to access the application.

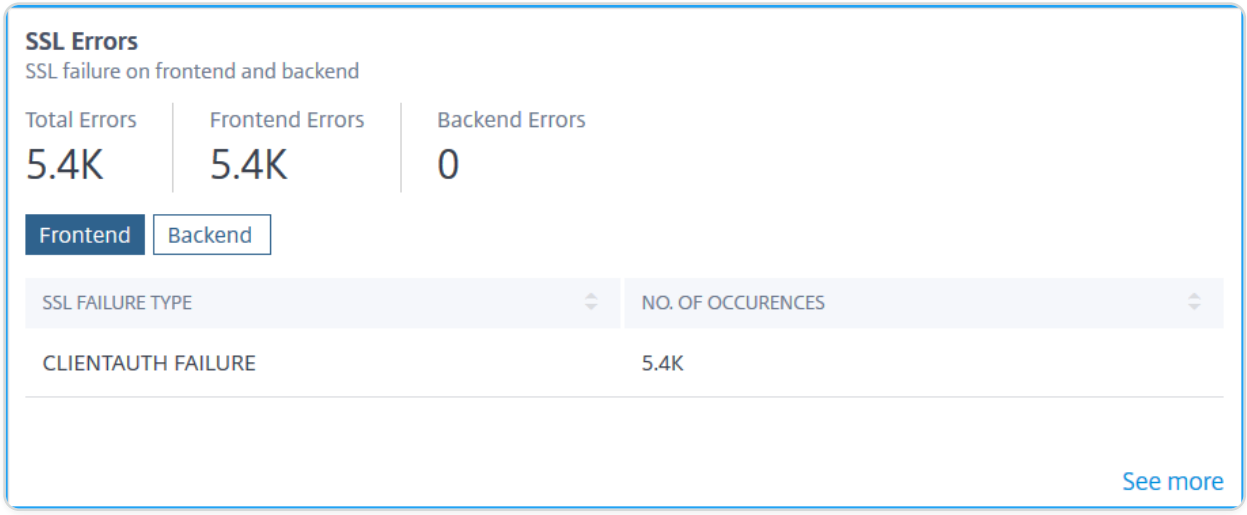


- **Requests** – Displays the total requests from each browser.
- **Bandwidth** – Displays the total bandwidth consumed by each browser.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

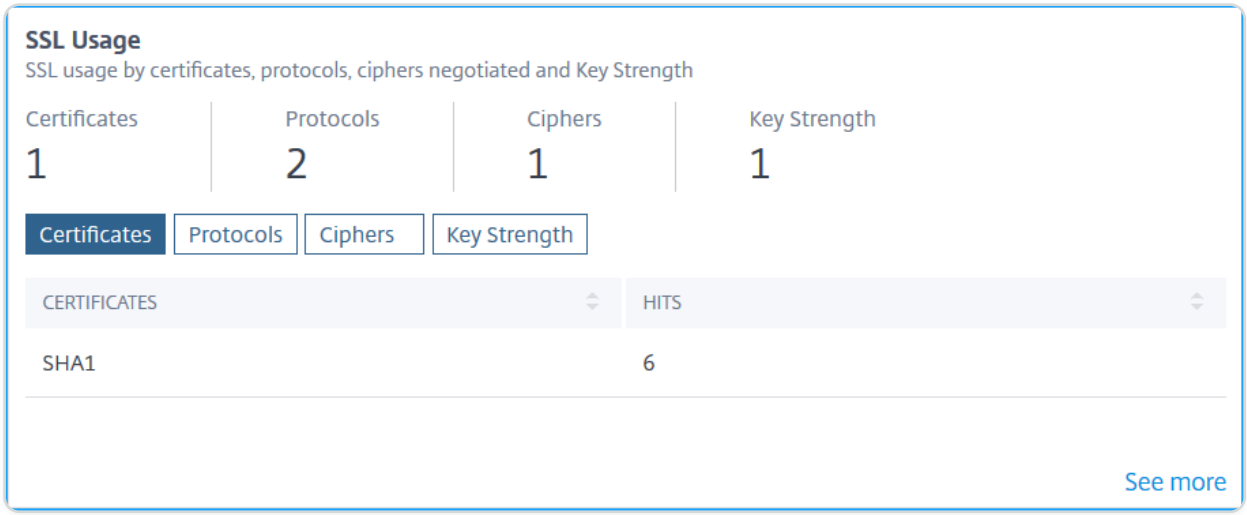
- **Load Time** – Displays the total time taken for a browser to load from the server.

- **SSL Errors** – Displays the insights for the SSL errors from front-end server and back-end server.



  - **Total Errors** – Displays the total SSL error occurrences.
  - **Frontend** – Displays the total SSL errors from the front-end server. Click the **Frontend** tab to view the SSL error type and total occurrences.
  - **Backend** – Displays the total SSL errors from the back-end server. Click the **Backend** tab to view the SSL error type and total occurrences.

- **SSL Usage** – Displays the insights for the SSL usage such as SSL certificates, protocols, Ciphers, and Key Strength.



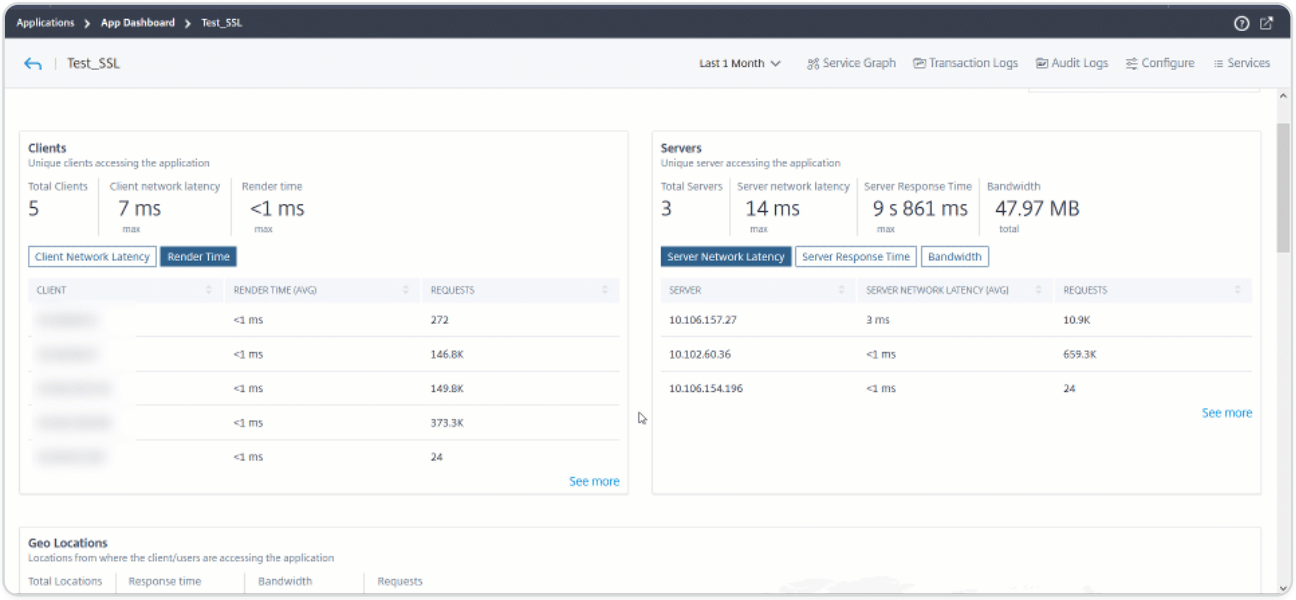
  - **Certificates** – Displays the total SSL certificates. Click the **Certificates** tab to view the certificate name and total hits.
  - **Protocols** – Displays the total SSL protocols. Click the **Protocols** tab to view details with SSL/TSL protocol and total hits.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Ciphers** – Displays the total Ciphers. Click the **Ciphers** tab to view details for each cipher suite name and total hits.
- **Key Strength** – Displays the total key strength used in SSL certificates. Click the **Key Strength** tab to view details for each key strength and total hits.

View metrics details in graphical format

For each metric, you can view more details in a graphical format by clicking **See more** option. Click **>** to view details in a graphical format.



The following are the details you can view for each metric after you click the **See more** option:

INSIGHT NAME	METRICS	DESCRIPTION
Clients	Clients	Denotes the client list
	Client Network Latency (MAX)	Denotes the maximum network latency from the client to NetScaler instance
	Client Network Latency (AVG)	Denotes the average network latency from the client to NetScaler instance
	Render Time (AVG)	Denotes the average time taken for the client to render the server response

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHT NAME	METRICS	DESCRIPTION
	Requests	Denotes the total requests from the client
Servers	Server	Denotes the server list and NetScaler virtual server (in case of integrated cache requests)
	Server Network Latency (AVG)	Denotes the average network latency from the server to NetScaler instance
	Server Network Latency (MAX)	Denotes the maximum network latency from the server to NetScaler instance
	Server Response Time (AVG)	Denotes the average time taken for the server to process the requests
	Server Response Time (MAX)	Denotes the maximum time taken for the server to process the requests
	Requests	Denotes the total hits received by the server
	Integrated Cache Hits	Denotes the total responses that the NetScaler appliance serves from the cache
	Integrated Cache Misses	Denotes the total responses that the NetScaler appliance serves from the origin server
Geo Locations	Country	Denotes the client locations
	Response Time (AVG)	Denotes the average response time from the client location

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHT NAME	METRICS	DESCRIPTION
	Bandwidth	Denotes the total bandwidth consumed from the location
	Requests	Denotes the total requests from the location
URL	Render Time (AVG)	Denotes the average time taken to load the page from the server
	Load Time (AVG)	Denotes the average time taken for the URL to render and display
	Requests	Denotes the total hits from the URL
HTTP Response Status	Response Status	Denotes the response status name such as OK, Not found, Internal Server Error, and so on
	Response Status Reason	Denotes the response status code received from the server such as 200, 400, 500, and so on
	No. of Occurrences	Denotes the total hits from the response code
Operating System	Operating System	Denotes the operating system name such as Windows, MAC
	Render Time	Denotes the total time taken for the operating system to render from the server
	Bandwidth	Denotes the total bandwidth consumed by the operating system

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHT NAME	METRICS	DESCRIPTION
	Requests	Denotes the total requests from the operating system
Browsers	Browsers	Denotes the browser name such as Mozilla Firefox, Chrome, and so on
	Render Time	Denotes the total time taken for a browser to render from the server
	Bandwidth	Denotes the total bandwidth consumed by the browser
	Requests	Denotes the total requests from the browser
SSL Errors	SSL Failure Type	Denotes the error name such as CLIENTAUTH FAILURE
	No. of Occurrences	Denotes the total occurrences for the SSL error
SSL Usage	Denotes the protocol name and versions such as TLS, SSL	
	No. of occurrences	Denotes the total hits from the protocol

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Automate SSL certificate management

To maintain digital security, you must automate management of SSL certificates in your environment. You need ways to proactively manage and monitor all the certificates, notify you of certificates due for expiry, and automatically renew the certificates before they expire. Expired SSL certificates lead to security risks. You can configure Venafi Trust Protection Platform servers with NetScaler Console to automate management of SSL certificates installed on NetScaler instances.

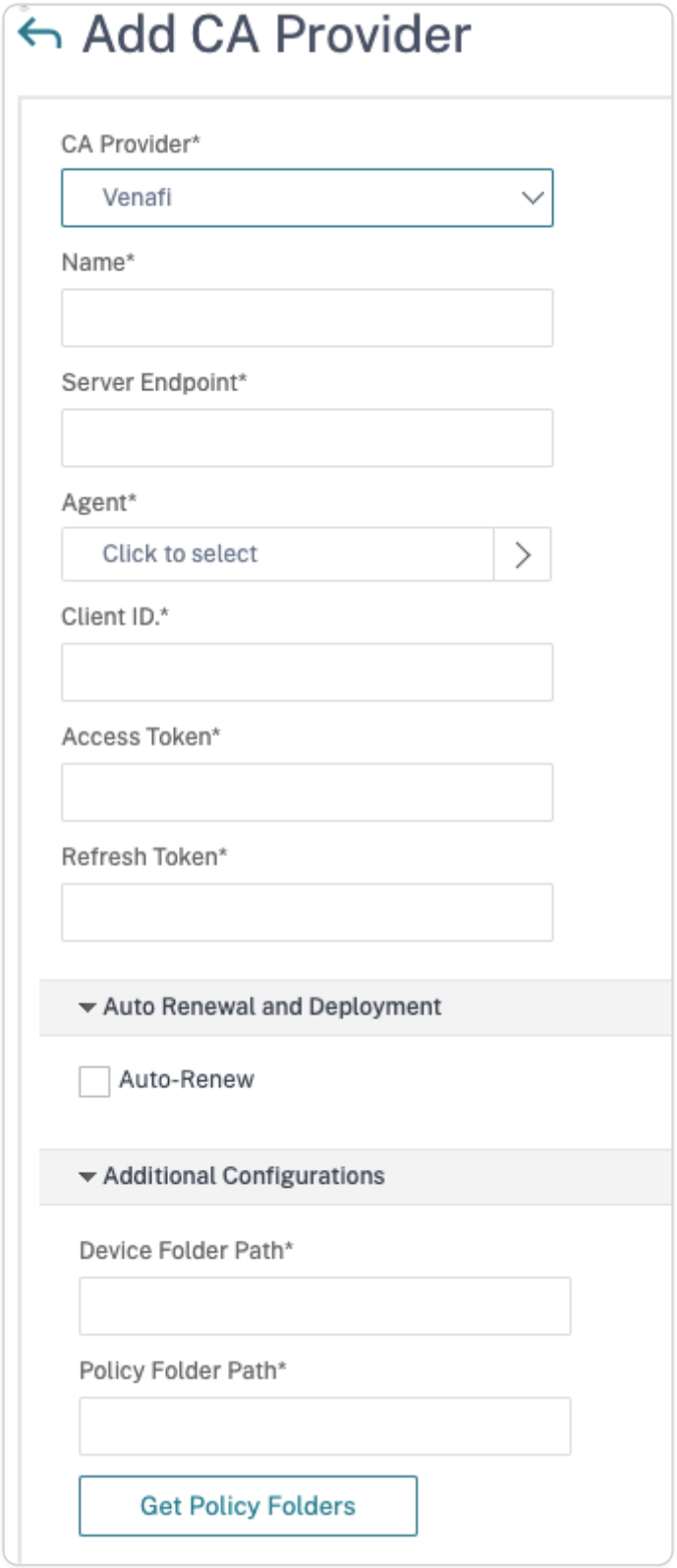
By using Venafi with NetScaler Console, you can manage the SSL certificates through their entire lifecycle. You can do the following tasks in the NetScaler Console **Application** dashboard:

- Check SSL issues and application scores.
- Troubleshoot SSL issues and apply suggested remediation.
- Check certificates bound to an application.
- Create, install, and renew certificates quickly.
- Automate renewal of certificates.
- Secure applications by binding generated certificates to NetScaler virtual servers.
- Check all the SSL task-related logs on a particular application.

Configure a Venafi server on NetScaler Console

Configuring a Venafi server is a two-step process. First, you add the Venafi server on NetScaler Console. Next, you configure the policies on the Venafi server. To add the Venafi server on NetScaler Console, from the NetScaler Console GUI, navigate **Infrastructure > SSL Dashboard > Third party CA**. Click **Add**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Enter the details in the fields provided. Check the **Auto-Renew** option if you want the certificates to be renewed automatically. For details about each field, hover over the field and click the `i` icon.

NOTE

The policy folder must have subfolders configured in it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

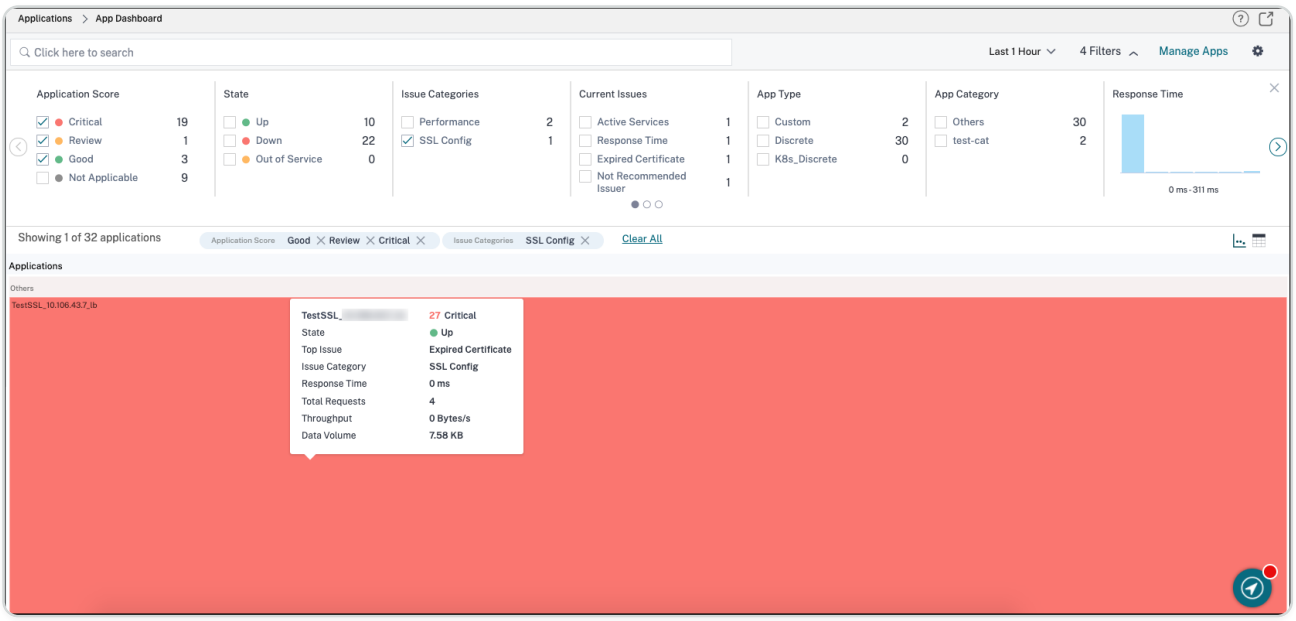
Example:

```
"policy_folder": "\\VED\\Policy\\TLS
TLS Certificates
NetScaler Console"
```

After you've configured the Venafi server, you can use the NetScaler Console dashboard to manage your SSL certificates.

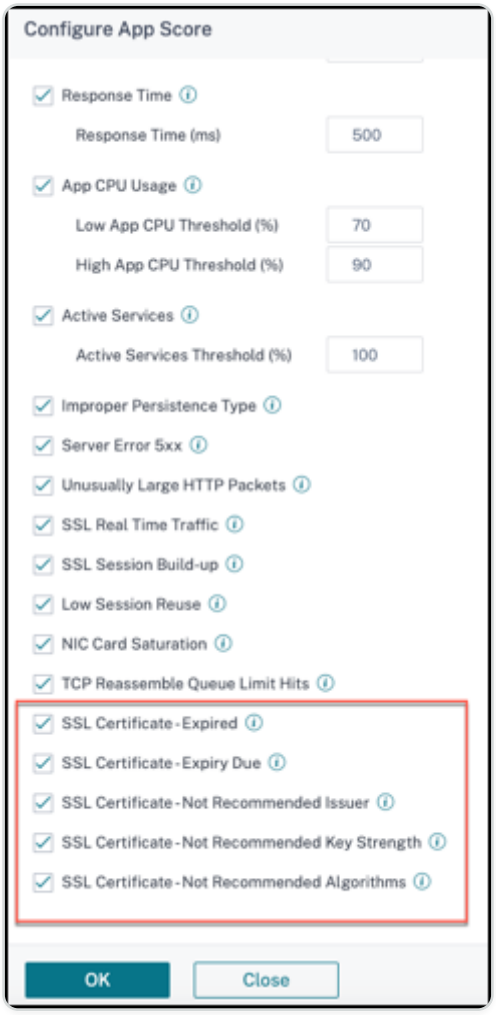
Manage SSL certificate lifecycle

The application dashboard is a one-stop place to manage your SSL certificates end to end. From the NetScaler Console GUI, navigate to **Applications > App Dashboard**. Under **Issue Categories** select **SSL Config**. Under **Current Issues**, you can see the SSL-related issues of your applications. To see the SSL report, under **Applications**, hover over the app. To see details of the report, click the app. In this example, we have an application with a score of 27.

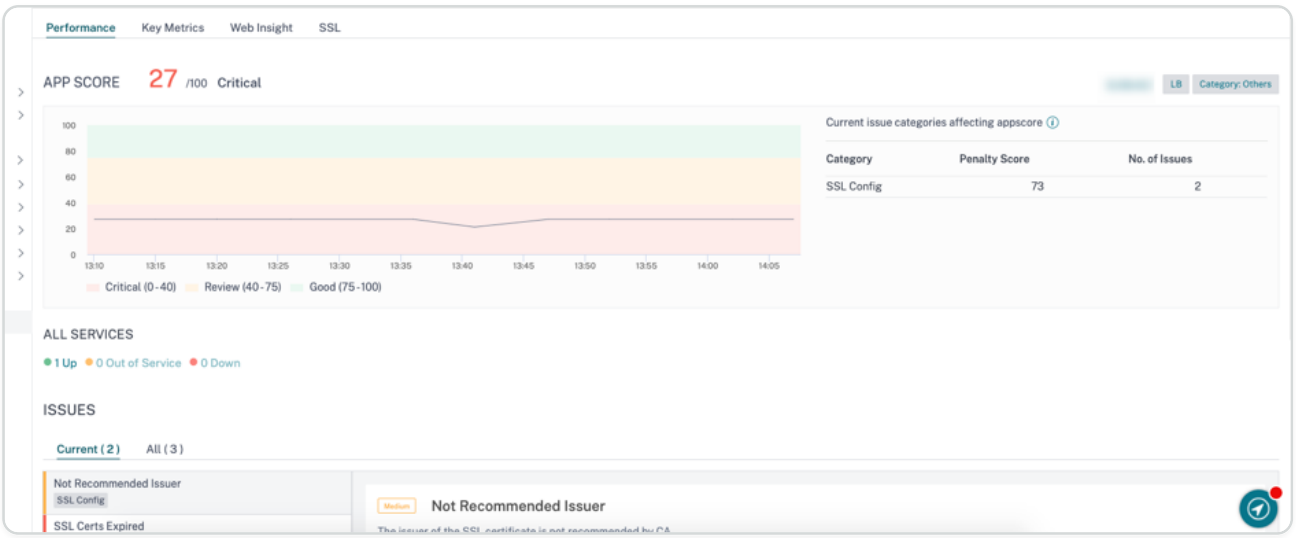


Further, you can filter your issues using **Application Scores** such as critical or review. The SSL application scores are based on SSL parameters, which are enabled by default under **Manage Apps** settings in the upper right corner of the dashboard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



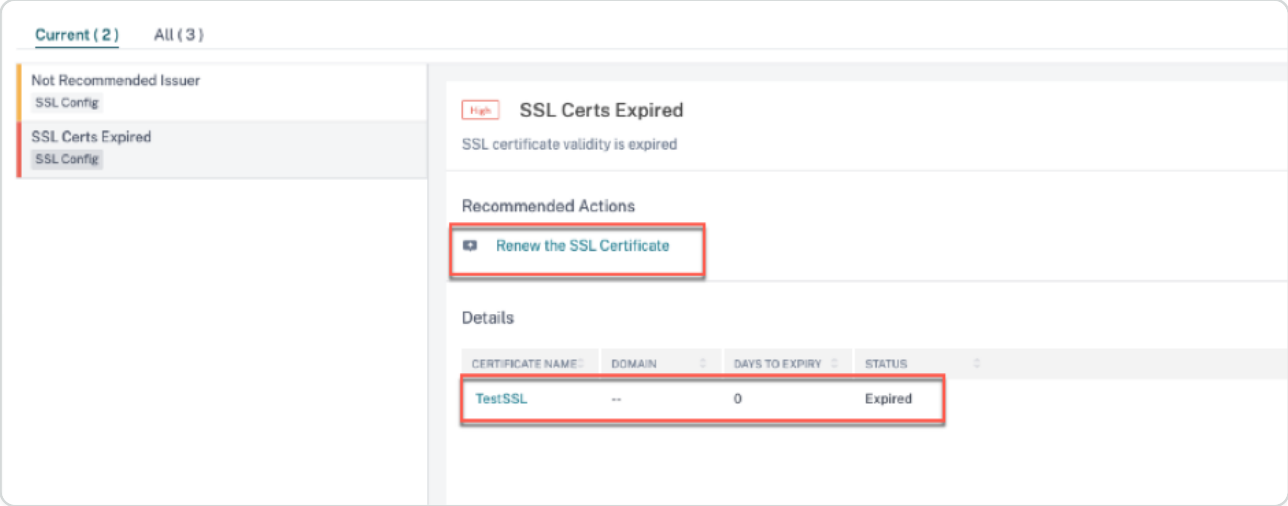
To disable any of the SSL parameters, clear the box and click **OK**. To see the details of the SSL report, under **Applications**, click the app for which you want to see the report.



You can check performance score and scroll down the page to see details such as the virtual servers that the app has and the certificates bound to the virtual servers and the issues with the certificates. To see details of the certificate, click the link under **Certificate Name**. For an expired certificate, can you can renew it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

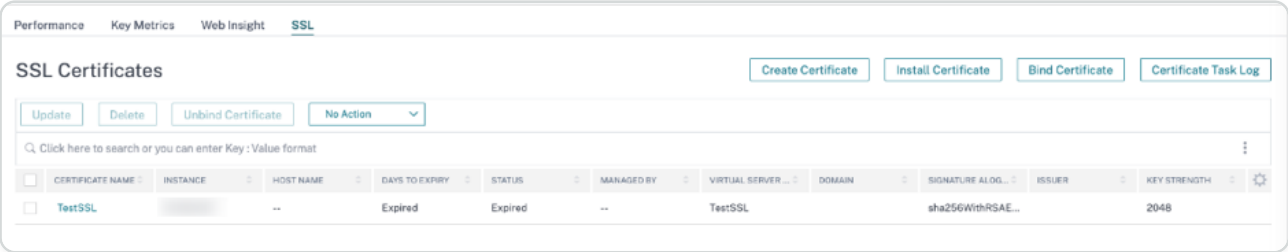
Renewing the certificate involves creating the certificate, installing it, and binding it to the virtual server.



NOTE

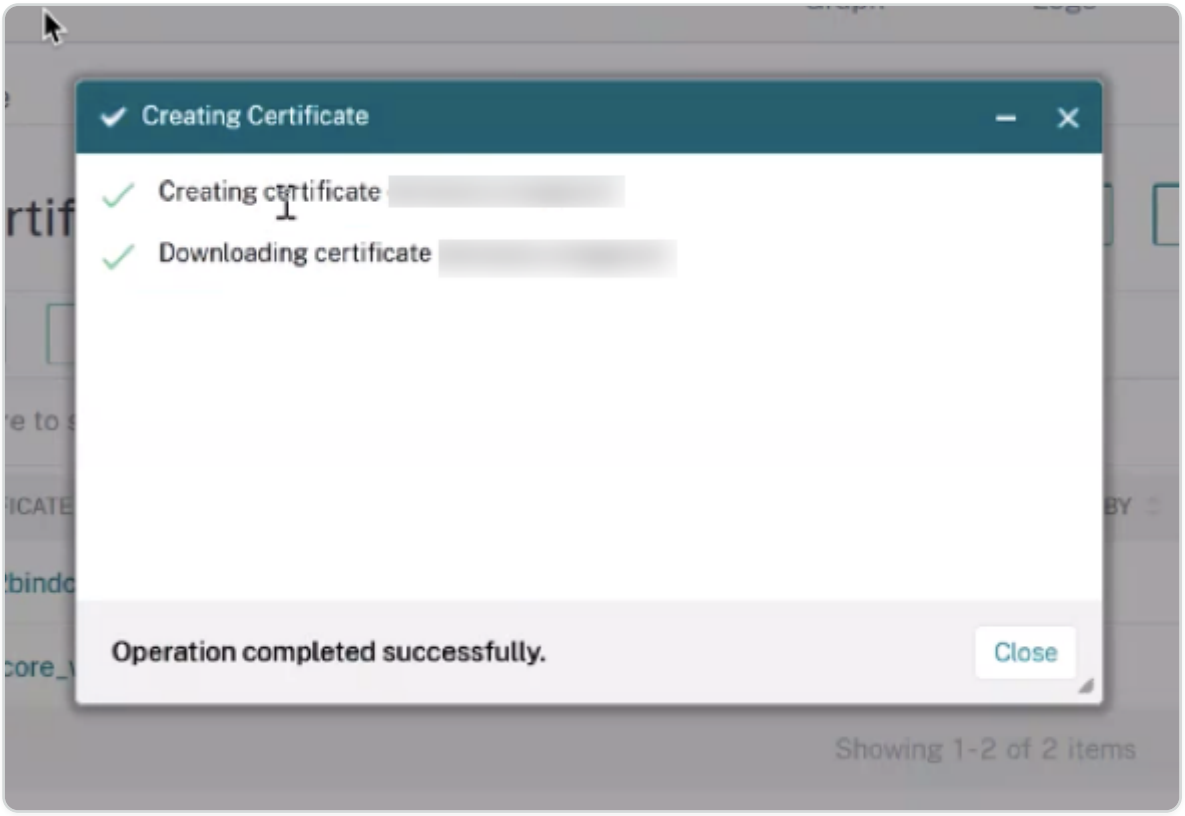
When you add a Venafi server on NetScaler Console, if you enable the auto-renewal option, certificates are automatically renewed before expiry.

Clicking **Renew the SSL Certificate** takes to the **SSL** tab, which lists all the certificates bound to the virtual servers of the application. Using this tab you can create and install certificates and bind them to the virtual servers. Also, you can check all the SSL task-related logs on a particular application on the SSL task-related logs on a particular application.



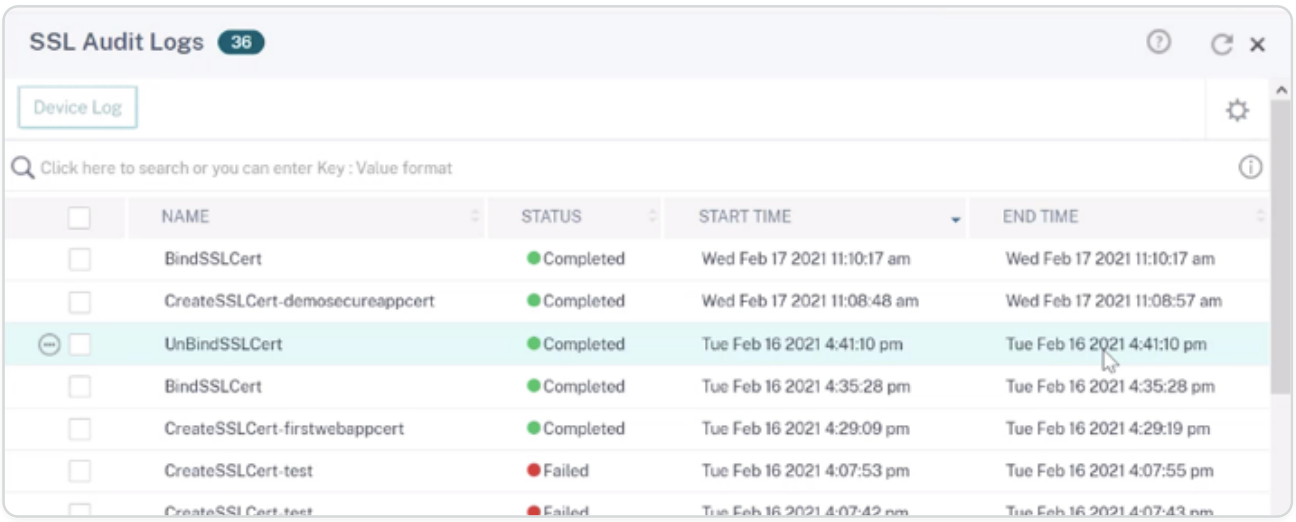
To create a certificate, click **Create Certificate** and enter the details. Provide a password as downloaded certificates are encrypted and click **Create**. NetScaler Console contacts the Venafi server to create the certificate. Click **Close** when the certificate is downloaded.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Next, on the **SSL** tab click **Install Certificate**. Select the downloaded certificate and click **Install**. For more information about how to install an SSL certification on NetScaler, using NetScaler Console, see the section on installing an SSL certificate from NetScaler Console in the topic Install SSL certificates on a NetScaler instance.

Next, click **Bind Certificate**. You can also unbind a certificate if necessary. After the next SSL polling, the Application dashboard is refreshed with the new data. If you want to check all SSL task logs on a particular application click **Certificate Task Log**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

A+ SSL rating analytics

NOTE:

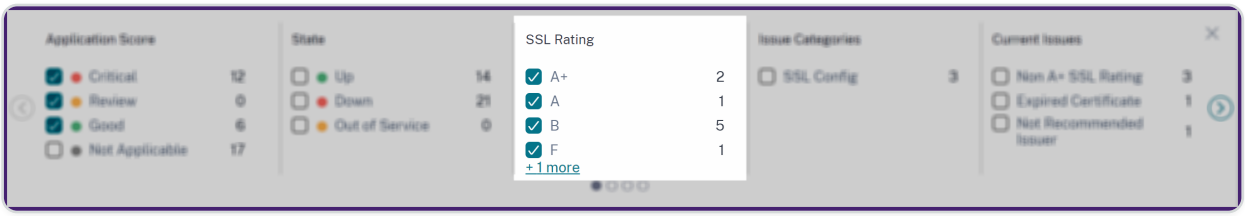
For bulk upgrade of non-complaint SSL certificates, you can use the **SSL A+ rating upgrade** in **Tasks**.

An application must use secure ciphers and protocols for SSL transactions. Otherwise, it can impact the privacy, data integrity, and security of the users accessing the application. NetScaler Console reviews the application's virtual server SSL settings with the NetScaler secure front-end profile. The settings required for an A+ rating is preloaded into the secure front-end profile.

As an application owner, you can assess whether your application has an **A+** rating. You can also view the protocol and cipher suite scores of an application. If your application has no **A+** rating, you can upgrade to **A+** rating.

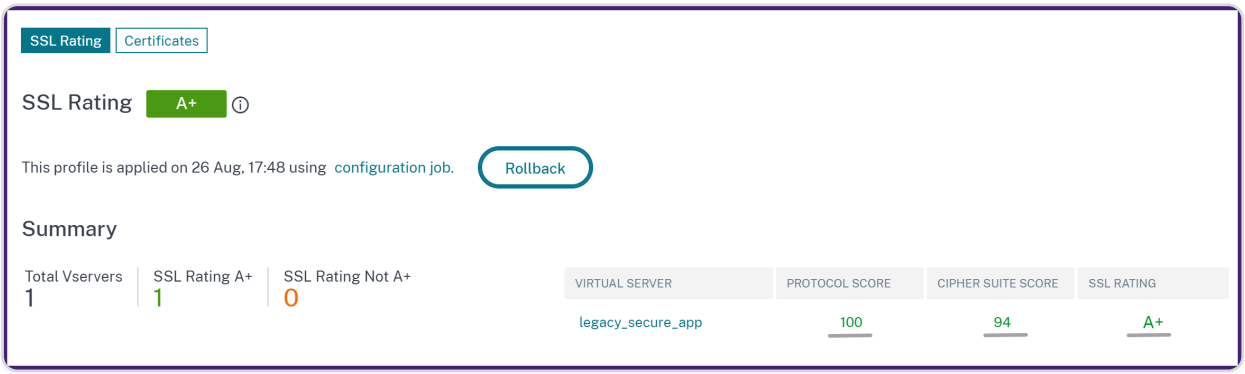
To view the application's SSL rating:

1. Go to **Applications > Dashboard**.
2. Filter applications based on their SSL ratings.



If an application has no rating, it is categorized under **NA**.

3. Select the required application grid from the GUI.
4. Select the **SSL** tab. This tab displays the SSL rating of the application.



The **SSL** tab provides one of the following options to change or upgrade your application's rating:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

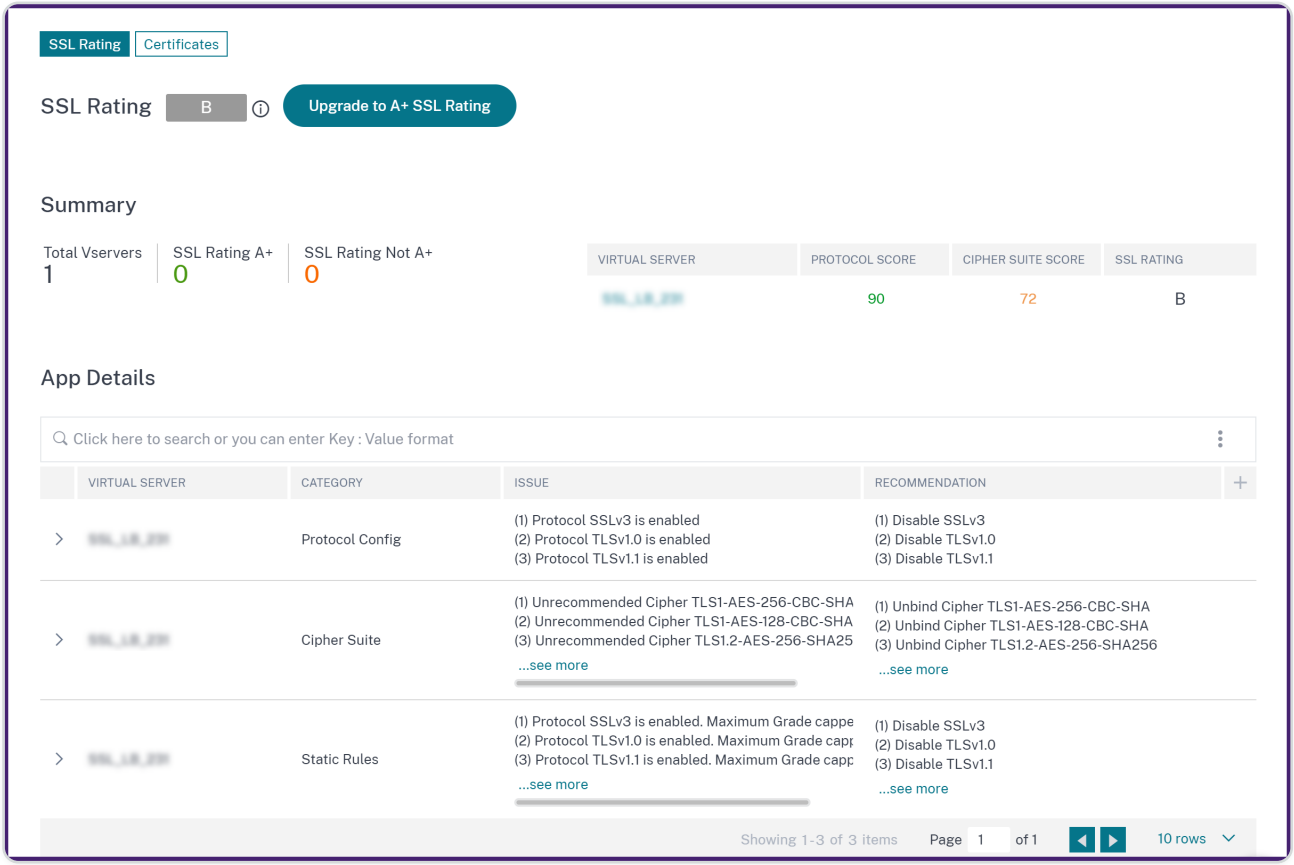
- Upgrade to A+ SSL rating
- Roll back SSL rating

Upgrade to A+ SSL rating

When you upgrade an application to A+ SSL rating, the following changes occur depending on the state of a default SSL profile on a NetScaler instance:

- If the default SSL profile is disabled, NetScaler Console modifies to the recommended SSL settings on the SSL virtual server.
- If the default SSL profile is enabled, NetScaler Console creates a new SSL profile with the recommended A+ settings based on a secure profile.

The application without **A+** rating displays the details affected virtual servers in the **SSL** tab.

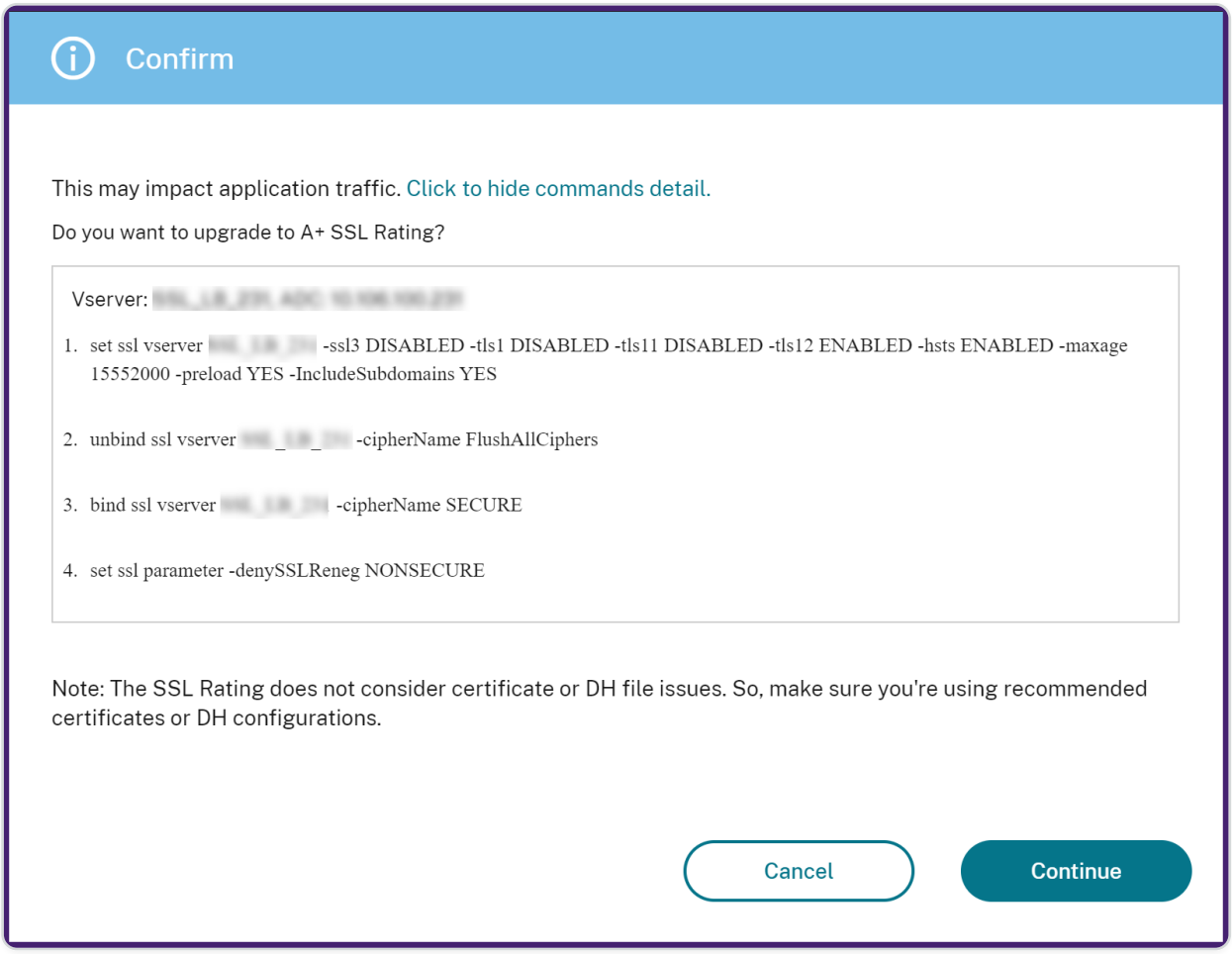


In **App Details**, you can review the virtual server details whose configuration is not compliant with the secure front-end profile. Also, it displays the remediation measures in the **Recommendation** column. These measures are given to make your application compliant with the secure front-end profile.

In this example, the virtual server has a few security issues. **Protocol TLSv1.0 enabled** is one of such issues. The **App Details** section recommends an appropriate action to solve this issue. To solve all such issues with the respective recommendations, do the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Click **Upgrade to A+ rating**.



   The confirmation message displays the commands that run on a virtual server. These commands might affect your application traffic.

2. Review the commands and click **Confirm**.

Roll back SSL rating

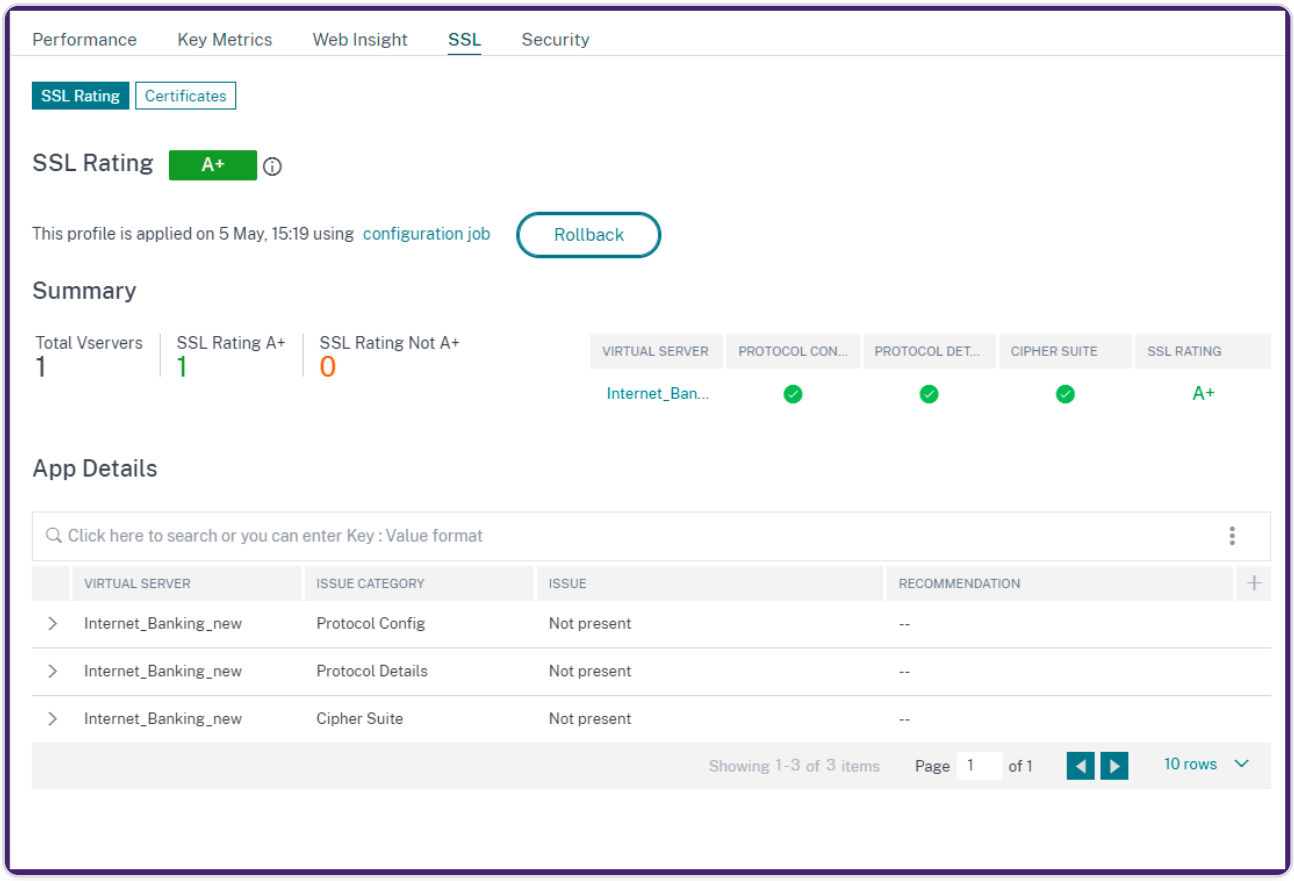
NOTE:

If you upgrade an application to A+ SSL rating, you can revert to its original rating only within 7 days after the upgrade.

After you upgrade the application to A+ rating, you can analyze the incoming traffic in SSL insight. This page displays the ciphers and protocols on which SSL transactions are negotiated.

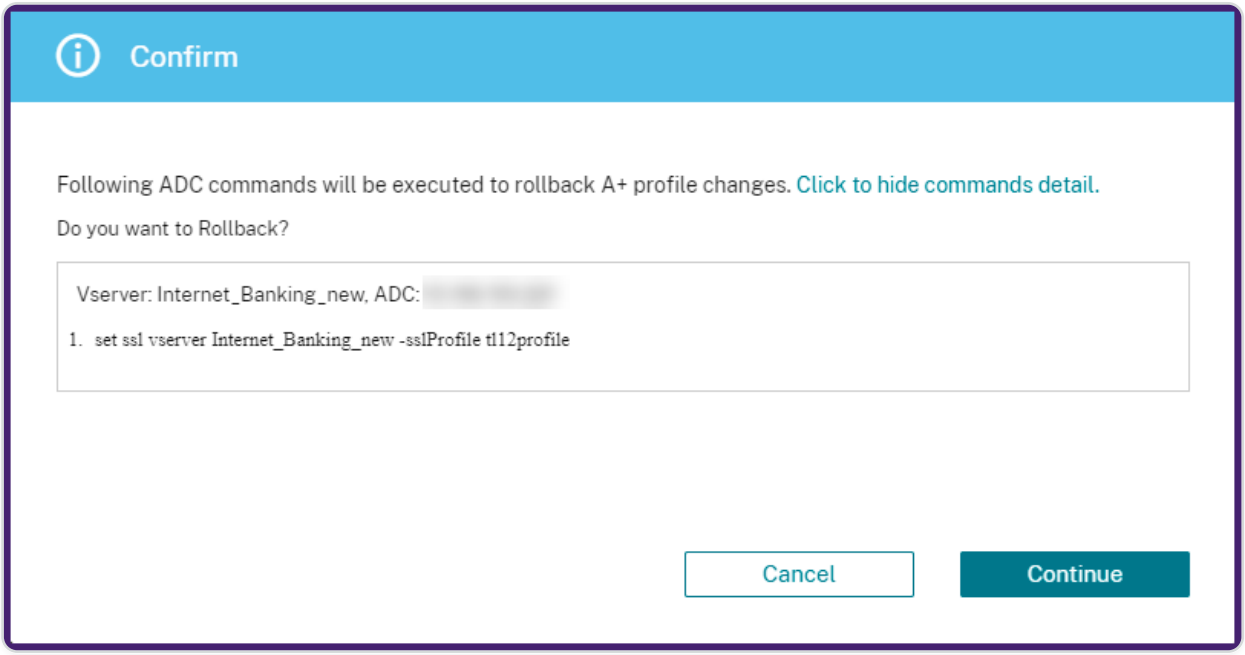
However, if you observe some legitimate traffic are dropped, you can roll back the secure front-end profile configured on your application. This action changes the SSL rating to the earlier rating.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



To roll back an SSL rating, do the following:

1. Click **Rollback**.



The confirmation message displays the commands that run on a virtual server.

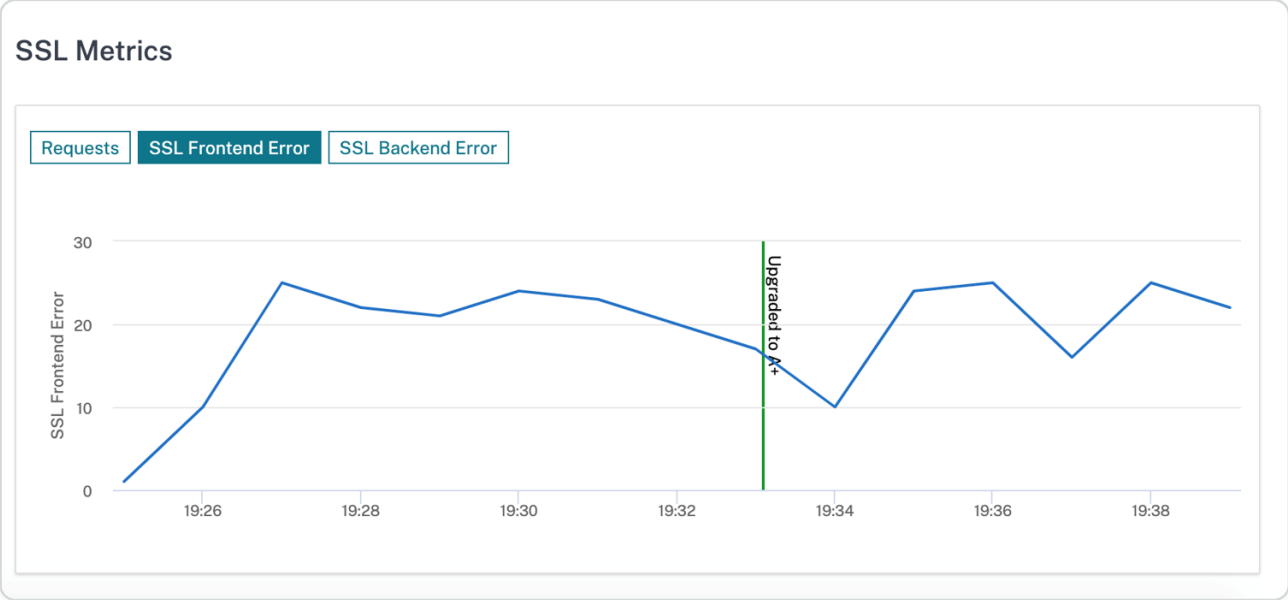
2. Review the commands and click **Confirm**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Determine the impact of SSL-rating on the application traffic

The application traffic might be affected when you upgrade the SSL-rating. In **SSL Metrics**, you can observe whether connections are dropped after the upgrade. With this information, you can decide to continue or roll back the SSL rating.

In the following example graph, some connections are dropped after upgrading the SSL-rating to **A+**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Web Insight dashboard

NOTE:

Starting from **14.1-51.x** release, Web Insight analytics are visible for virtual servers that are configured with an IPv6 address.

The improved Web Insight feature is augmented and provides visibility into detailed metrics for web applications, clients, and NetScaler instances. This improved Web Insight enables you to evaluate and visualize the complete application from the perspectives of performance and usage together. As an administrator, you can view Web Insight for:

- An application. Navigate to **Applications > Dashboard**, click an application, and select **Web Insight** tab to view the detailed metrics. For more information, see Application Usage Analytics.
- All applications. Navigate to **Applications > Web Insight** and click each tab (Applications, Clients, Instances) to view the following metrics:

APPLICATIONS	CLIENTS	URLS	INSTANCES
Application with Response Time Anomalies	Clients	URLs	Instance Metrics
Applications	Geo Locations		Applications
Servers	HTTP Request Methods		Domains
Domains	HTTP Response Status		URLs
Geo Locations	URLs		HTTP Request Methods
URLs	Operating System		HTTP Response Status

© 1997–2026 Citrix Systems, Inc. All rights reserved.

APPLICATIONS	CLIENTS	URLS	INSTANCES
HTTP Request Methods	Browsers		Clients
HTTP Response Status	SSL Errors		Servers
SSL Errors	SSL Usage		Operating System
SSL Usage			Browsers

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Applications | Clients | URLs | Instances

Last 1 Hour

Applications With Response Time Anomalies

Top apps with high number of anomalies

APPLICATION	TOTAL ANOMALIES AND CONTRIBUTORS	RESPONSE TIME RANGE	MAXIMUM ANOMALOUS RESPONSE TIME	MAXIMUM ANOMALY CONTRIBUTOR
Sandy_s Cookie Design	2	1 ms - 9.50 ms	24.02 ms	Server processing time
Concur	1	1 ms - 5.25 ms	20.51 ms	Server processing time
Sandy_s Bundt Cake Bakery	1	1 ms - 4.14 ms	180.97 ms	Client network latency
Sharepoint	1	1 ms - 9.60 ms	24.56 ms	Server processing time

See more

Applications

Top apps with high bandwidth, response time and requests made

Requests | Bandwidth | Response Time

APPLICATION	BANDWIDTH	RESPONSE TIME (AVG)	REQUESTS
Center	21.6 MB	0 ms	7.9K
Concur	21.97 MB	2.84 ms	4.5K
cetflix-192.168.191.78_80_http_192.168.191....	3.13 MB	12.49 ms	4.2K
apigw_Petstore_Application-cs_192.168.10...	3.02 MB	1.67 ms	3.4K
Sharefile	7.27 MB	4.76 ms	2.3K

See more

Servers

Unique servers accessing the application

Requests | Server Network Latency | Server Response Time | Bandwidth

SERVER	SERVER NETWORK LATENCY (MAX)	SERVER NETWORK LATENCY (AVG)	REQUESTS
172.16.10.49	3 ms	1.23 ms	6.1K
172.16.10.57	3 ms	0 ms	4.2K
172.16.10.45	4 ms	1.48 ms	3.9K
192.168.15.146	3 ms	1.39 ms	3.4K
192.168.15.145	2 ms	<1 ms	2.9K

See more

Domains

Top domains

Requests | Bandwidth | Response Time

DOMAIN	BANDWIDTH	REQUESTS
192.168.10.131	21.97 MB	4.5K
192.168.10.134	3.02 MB	3.4K
192.168.10.121	7.27 MB	2.3K
192.168.10.122	38.69 MB	1.9K
192.168.10.114	4.1 MB	1.2K

See more

Geo Locations

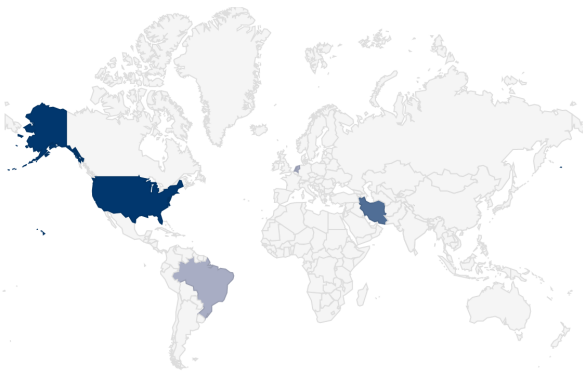
Locations from where the clients/users are accessing the applications

Total Locations	Response Time	Bandwidth	Requests
5	312.64 ms (max)	232.12 MB (total)	30.8K (total)

Requests | Response Time | Bandwidth

COUNTRY	RESPONSE TIME (AVG)	BANDWIDTH	REQUESTS
United States	3.06 ms	186.99 MB	14.3K
*	6.86 ms	8.23 MB	8.9K
Iran	0 ms	32.88 MB	7.5K
Netherlands	0 ms	3.99 MB	118
Brazil	180.97 ms	37.18 KB	1

See more



HTTP Request Methods

Indicates HTTP request methods used to access the applications

REQUEST METHODS	BANDWIDTH	NO. OF OCCURENCES
GET	111.11 MB	21.3K
Unknown	21.6 MB	9.5K

See more

HTTP Response Status

Indicates if a specific HTTP request has been completed along with its status

RESPONSE STATUS	RESPONSE STATUS REASON	NO. OF OCCURENCES
200	OK	11.1K
404	Not Found	8.8K
302	Found	921
500	Internal Server Error	506

In each metric, you can view the top 5 results. You can click to drill down further to analyze the issue and take troubleshooting actions faster.

NOTE

- Starting from **14.1-1.16** or later release, when you drill down a metric, the analytics view in the time series graph displays nil values (for example, 0 ms and 0 request) for the selected duration. Earlier, if there was no traffic or transaction received for the selected duration, the analytics view displayed the graphs by skipping those nil values.
- In some scenarios, NetScaler might not be able to calculate the RTT values for some transactions. For such transactions, NetScaler Console displays the RTT values as:
  - **NA** – Displays when the NetScaler instance cannot calculate the RTT.
  - **< 1ms** – Displays when the NetScaler instance calculates the RTT in decimals between 0 ms and 1 ms. For example, 0.22 ms.

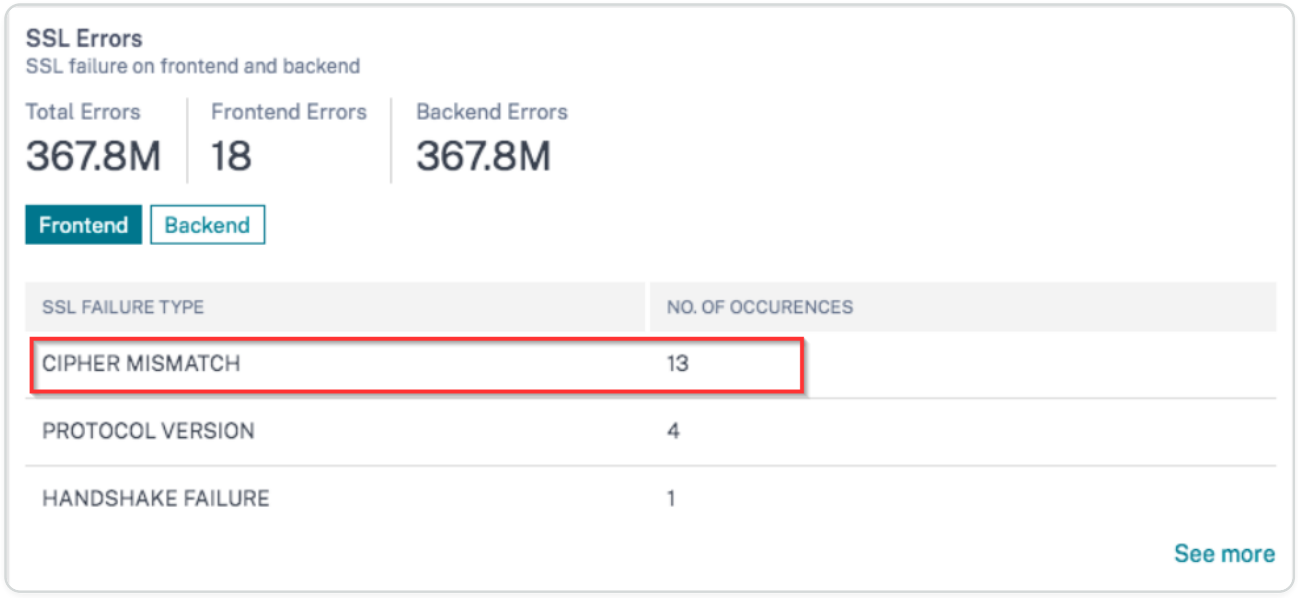
View details for cipher related issues

Under **SSL Errors**, you can view details for the following SSL parameters:

- Cipher mismatch
- Unsupported Ciphers

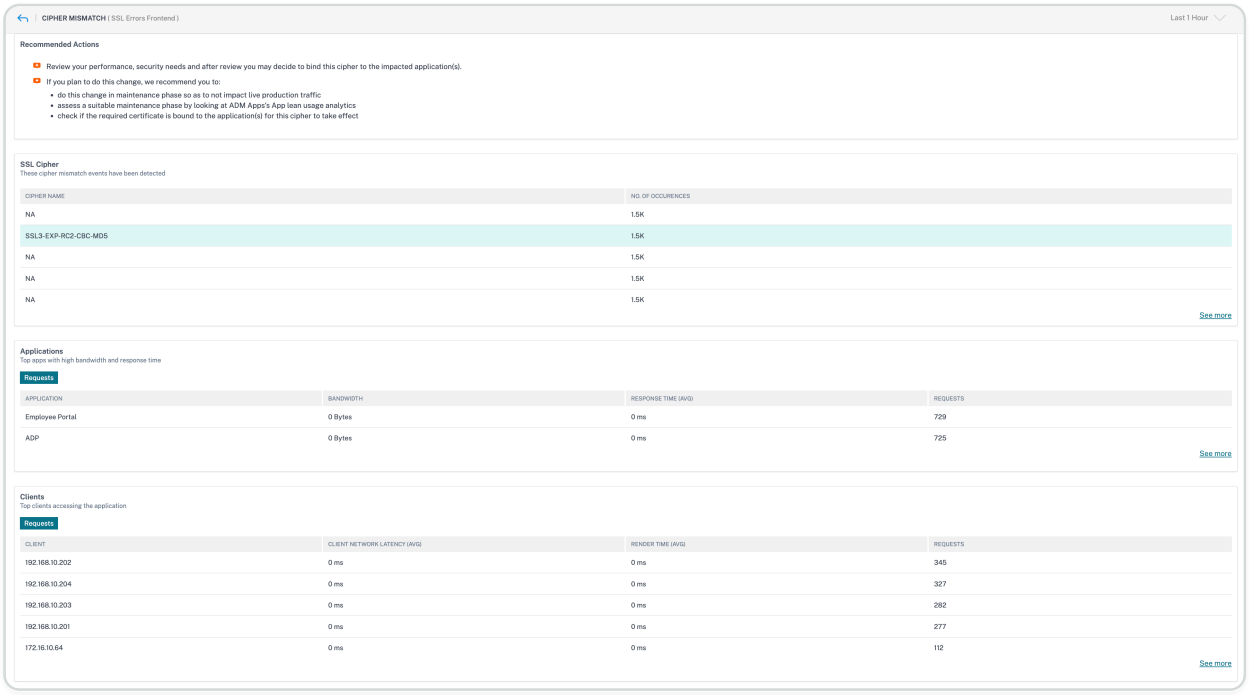
Under **SSL errors**, click an SSL parameter (Cipher Mismatch or Unsupported Ciphers) to view details such as the SSL cipher name, the recommended actions, and the details of the affected applications and clients.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



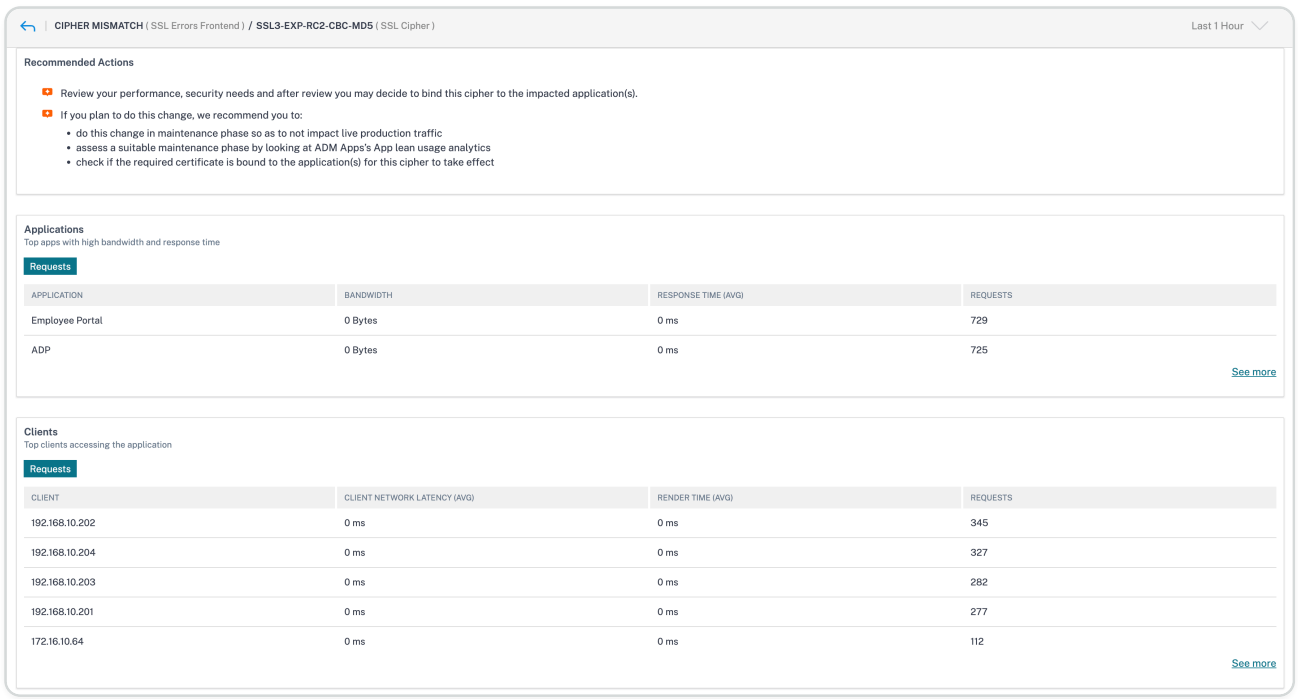
The details page appears for the selected SSL parameter. You can:

- Review the suggestions provided in the **Recommended Actions**.
- View the cipher names and number of occurrences under **SSL Cipher**.
- View the total applications and clients affected.



Click the **SSL Cipher name** to see the applications and clients that are affected with the selected SSL Cipher.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

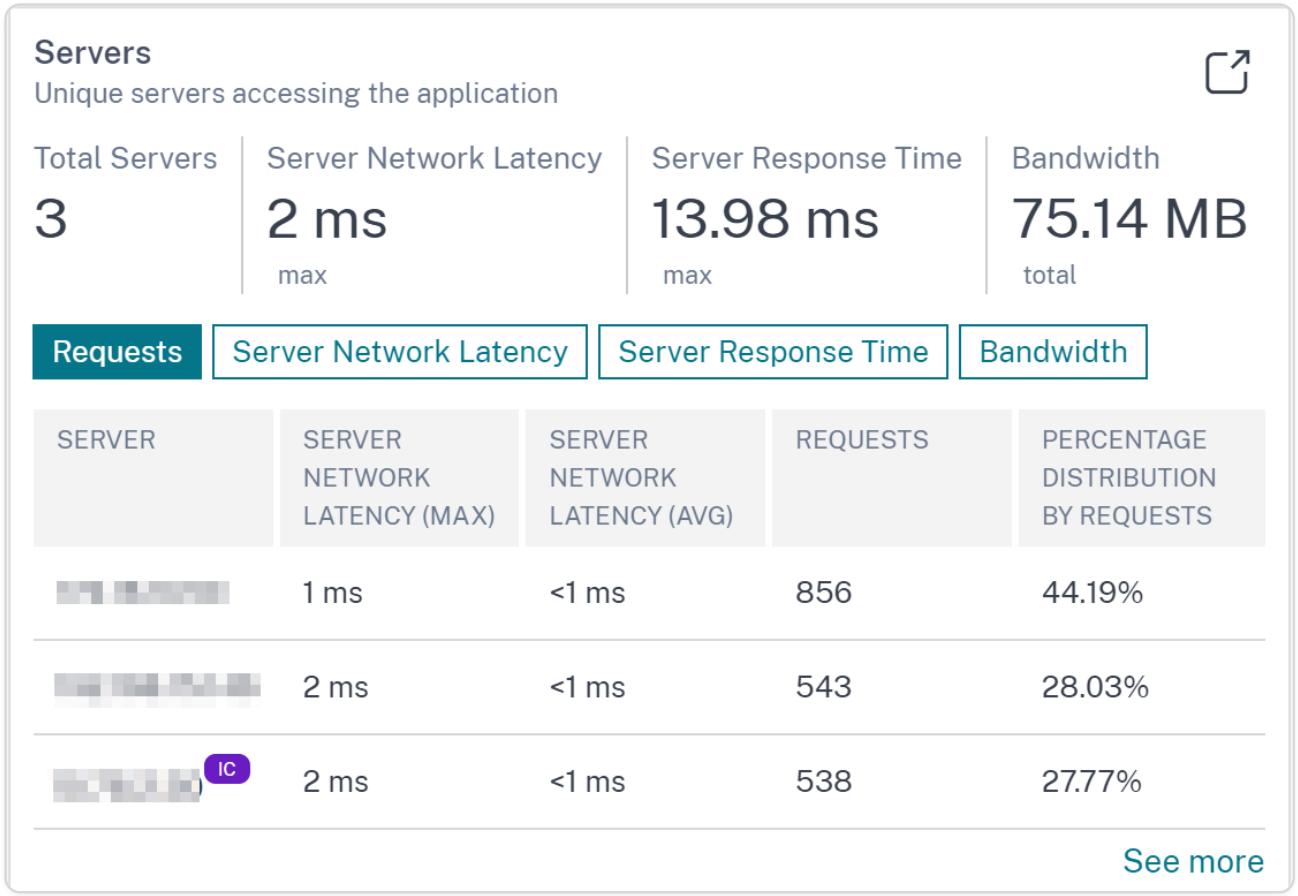


Integrated cache requests

The integrated cache provides in-memory storage on the NetScaler appliance and serves Web content to users without requiring a round trip to an origin server.

The integration cache requests are currently visible under **Servers** with an IC notification next to the NetScaler virtual server IP address. All other requests are visible with the origin server IP address.

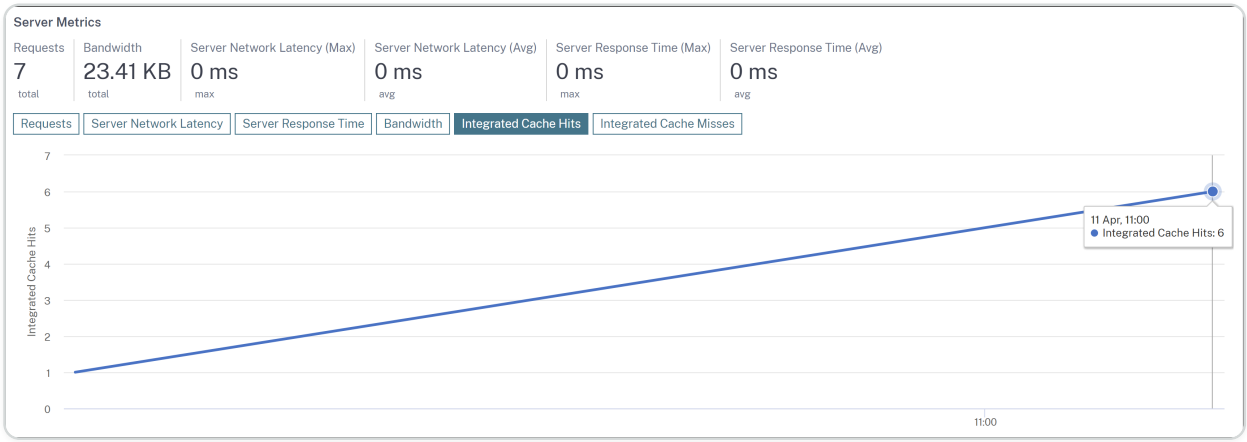
© 1997–2026 Citrix Systems, Inc. All rights reserved.



When you drill down a server to view more details, the **Server Metrics** display integrated cache hits and misses tabs.

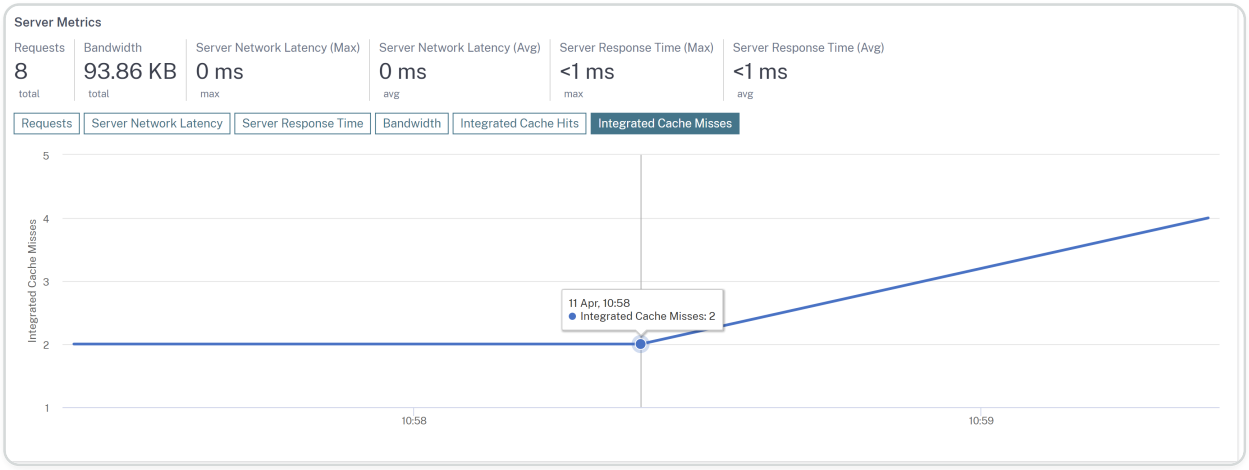
The graph view in:

- The **Integrated Cache Hits** tab enables you to view the total responses that the NetScaler appliance serves from the cache.



- The **Integrated Cache Misses** tab enables you to view the total responses that the NetScaler appliance serves from the origin server.

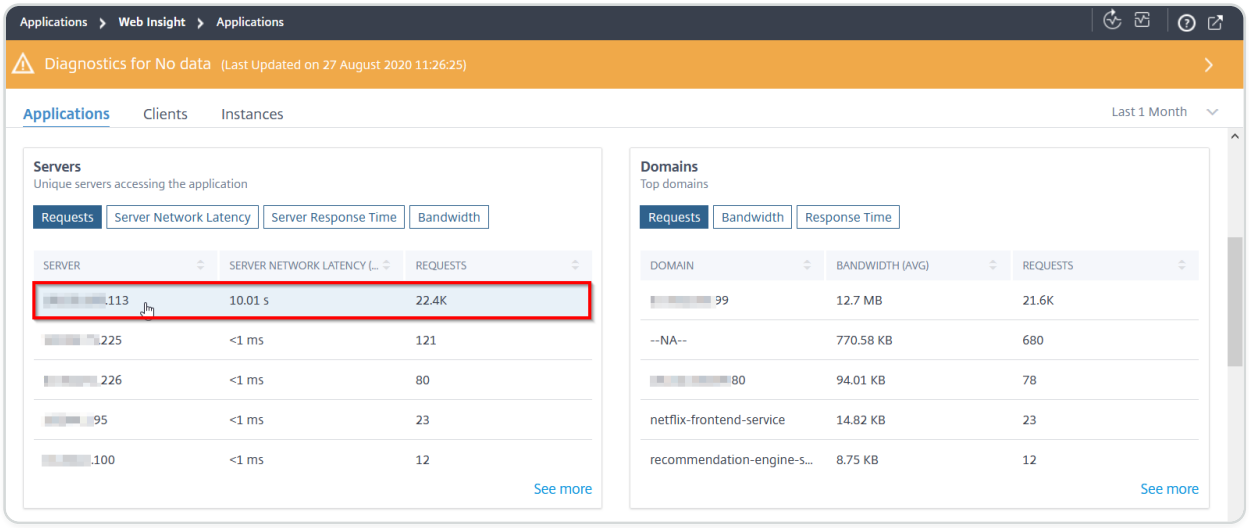
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Other use case

Consider that you want to analyze the server network latency for 1-month time duration and take a decision whether to scale up or scale down the production environment. To analyze this:

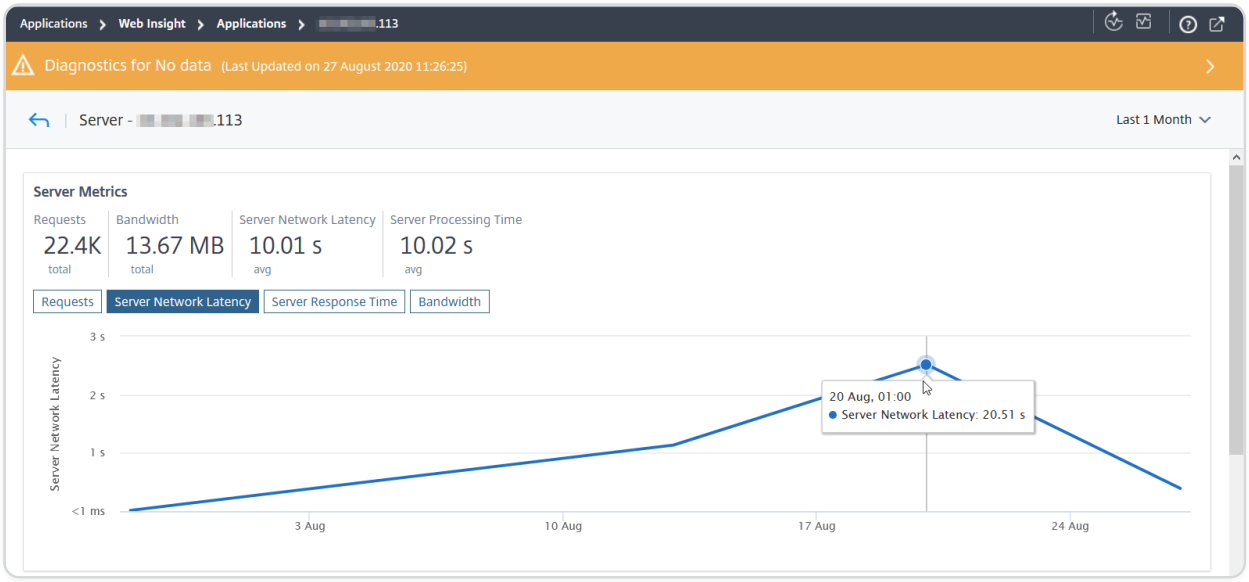
1. Select Last 1 Month from the list and from the **Applications** tab, scroll down to **Servers**, and click a server.



   The metrics details for the selected server are displayed.

2. Select the **Server Network Latency** tab to analyze the latency.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The average latency indicates 10.01 s and from the graph, you can analyze that the server network latency for the last 1 month seems to be high. As an administrator, you can take a decision to scale up the production environment.

Analyze the root cause for application slowness

Application slowness is a major concern for any organization because it results in business impact or productivity. As an administrator, you must ensure that all applications perform optimally to avoid any business impact. When your users experience a slowness in accessing the application, you must ensure if the issue is with:

- Client network latency
- Server network latency
- Server processing time

NetScaler Console performs anomaly checks every hour and reports anomalies for past 1 hour traffic, based on certain prerequisites. For example, to avoid false positive results, if the response time is < 1 ms, the anomaly checks for those results are skipped.

The **Applications > Web Insight** page enables you to view the applications with response time anomalies for the selected duration. The **Applications with Response Time Anomalies** metric displays the top five applications based on the total anomalies. Click **See more** to view all applications.

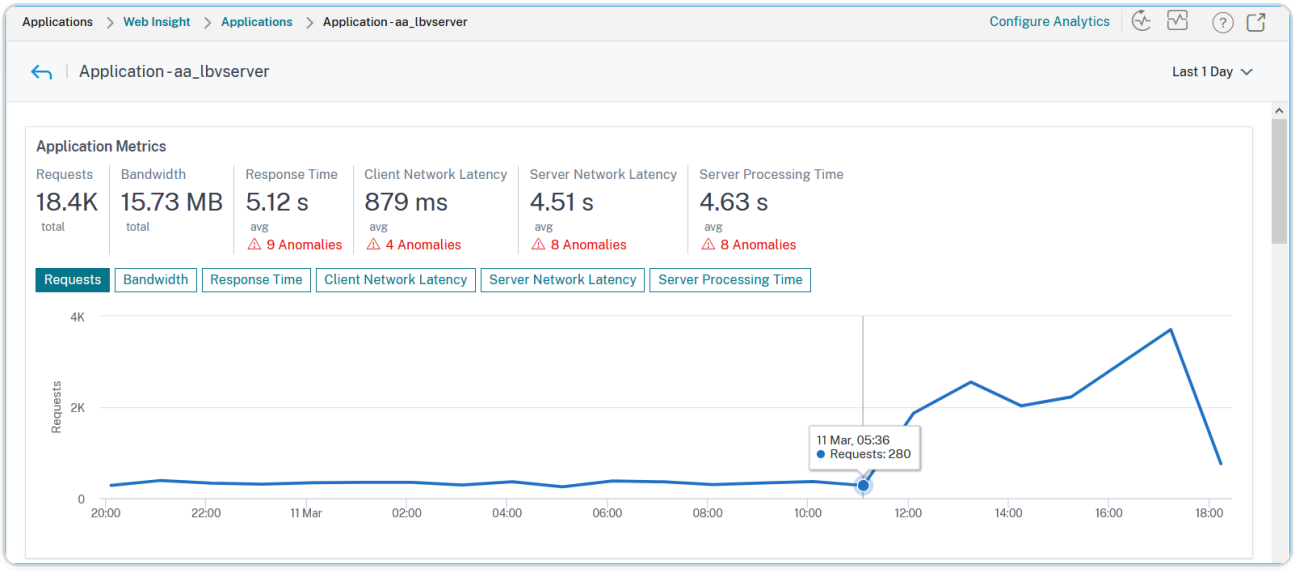
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Application** – Denotes the application name.
- **Total Anomalies and Contributors** – Denotes the total anomalies from the application. When you hover the mouse pointer, you can view the total anomalies that are from the client network latency, server network latency, and server processing time respectively.
- **Response Time Range** – Denotes the expected response time range from the application.
- **Maximum Anomalous Response Time** – Denotes the highest response time from the application.
- **Maximum Anomaly Contributor** – Denotes if the maximum number of anomalies for the application are from client network latency, server network latency, or server processing time.

Application drill-down

Click an application to view the **Application Metrics** details for the selected duration.



The **Application Metrics** enable you to view:

- **Summary** – An overview to visualize the application performance such as Response Time, Requests, and Bandwidth

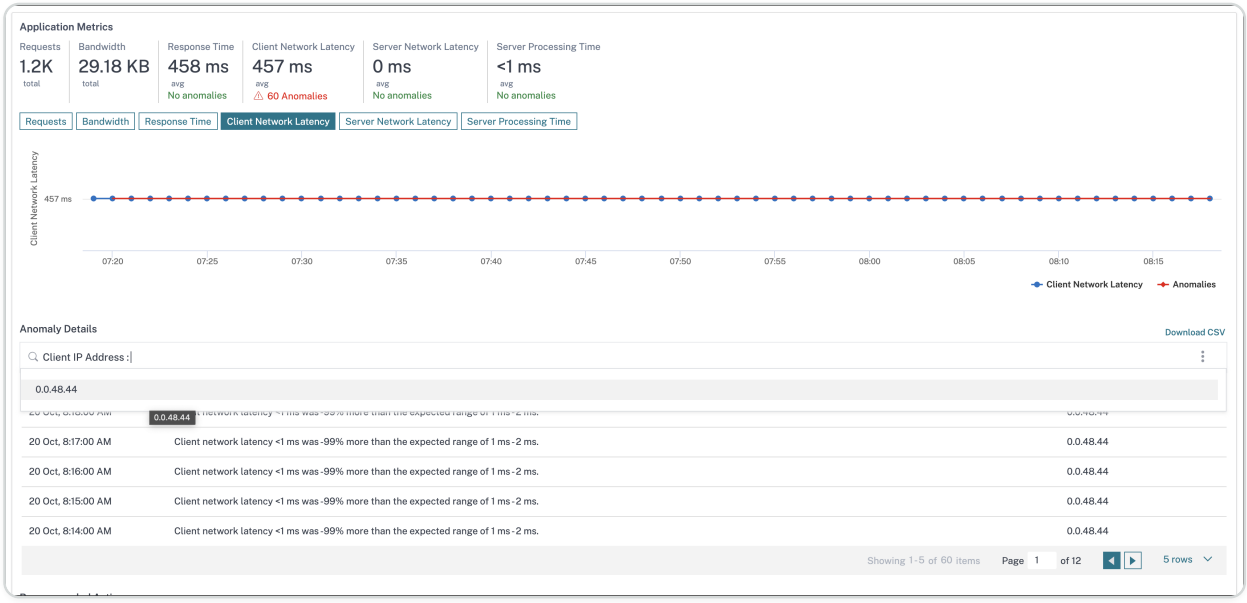
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Requests** – The total requests received by the application. You can also view requests from the top 5 clients based on the total requests
- **Bandwidth** – The total bandwidth processed by the application. You can also view the bandwidth consumption from the top 5 servers based on the total bandwidth consumption
- **Response Time** – An overview to visualize Client Network Latency, Server Network Latency, and Server Processing Time on the same graph
- **Client Network Latency** – The average client network latency (from client to NetScaler)
- **Server Network Latency** – The average server network latency (from NetScaler to server)
- **Server Processing Time** – The average server processing time (from server to NetScaler)

If the application has anomalies, you can view if the anomalies are from client network latency, server network latency, or server processing time. Click each tab to view details.

In the **Client Network Latency** and **Server Network Latency** tabs, you can view:

- **A search bar** - Click the search bar to view the IP address of all clients (in Client Network Latency) and servers (in Server Network Latency). You can select the IP address to filter results.
- **An export option** - Click **Download CSV** to export the details in CSV format.

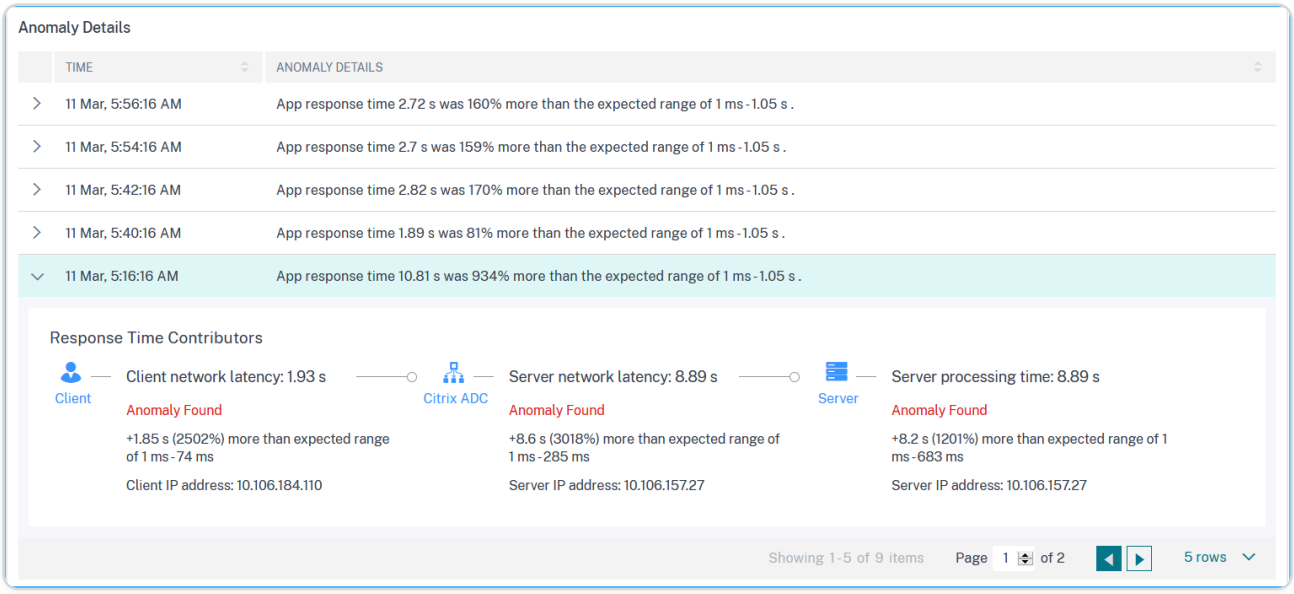


Response Time

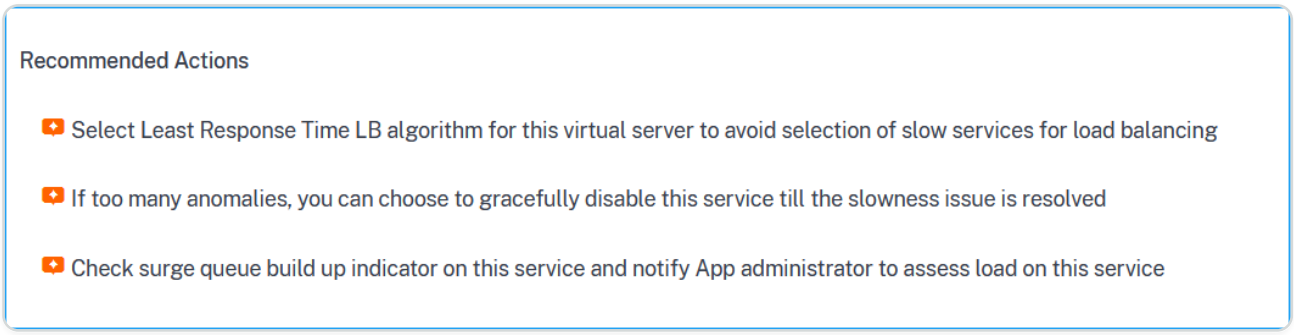
Under **Anomaly Details**, click to view details for the response time contributors (from client to server). The following example has an anomaly for client network latency, server network latency,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

and server processing time. You can also view the expected ranges and the breach that has happened beyond the expected range.



The **Recommended Actions** suggest you the possible resolutions for the anomalies.

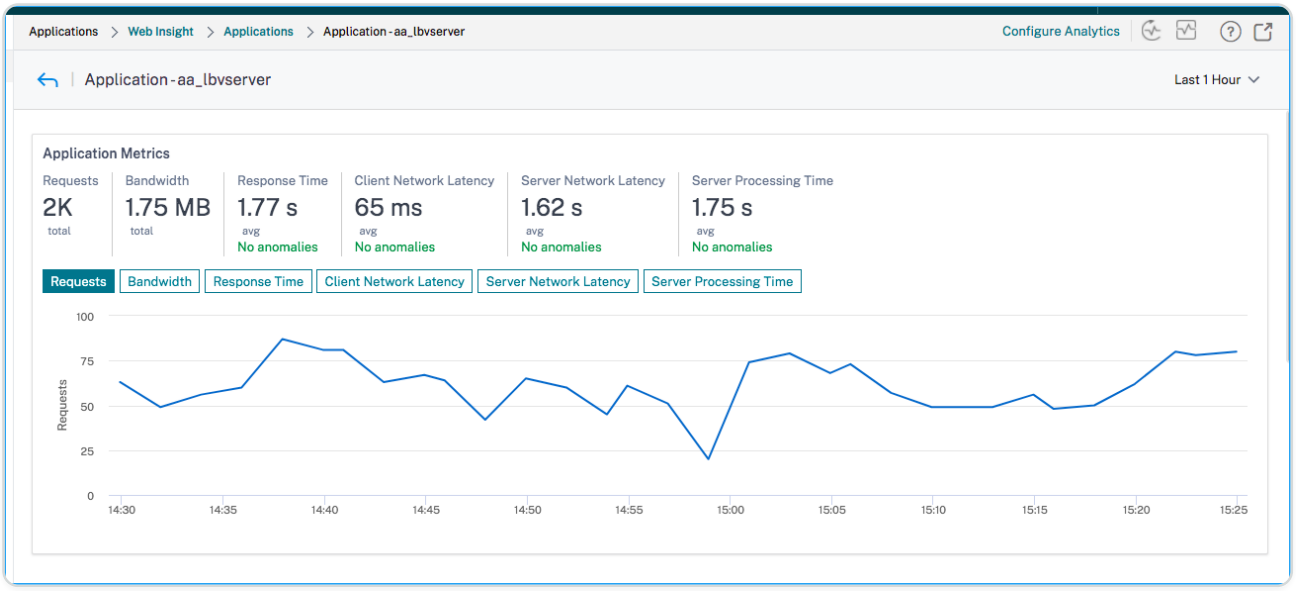


Similarly, you can click the **Client Network Latency**, **Server Network Latency**, and **Server Processing Time** tabs to view:

- Anomaly that has breached the expected range.
- Recommended Actions that suggest you the possible resolutions.

If the application is performing well, you can view application metrics as no anomalies.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service Graph

The service graph feature in NetScaler Console enables you to monitor all Kubernetes services in a graphical representation. This feature also enables you to view a detailed analysis and actionable metrics of the services. Navigate to **Applications > Service Graph** to view service graph for:

- Applications configured across all NetScaler instances
- Kubernetes applications
- 3-tier Web applications

Service graph for applications across all NetScaler instances

The global service graph feature enables you to get a holistic visualization of the `clients to infrastructure to application` view. From this single-pane service graph view, as an administrator, you can:

- Understand from which region the users are accessing the specific applications (3-tier Web apps and microservices app)
- Visualize the infrastructure (NetScaler instance) view that the client request is processed
- Understand if the issues are occurring from the client, infrastructure, or application
- Further drill down to troubleshoot the issue

Navigate to **Applications > Service Graph** and click the **Global** tab to view:

- End-to-end details of all applications connected from client to back-end servers
- All NetScaler instances that are connected to its respective data centers

  NOTE

  You can view data centers only if you have GSLB apps.

- The client metrics information
- The NetScaler metrics information

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- All NetScaler instances that have discrete applications, custom applications, and discrete microservice applications
- The top 4 low-scored applications that belong to custom apps, discrete apps, and microservices apps
- The metrics information for the top 4 low-scored virtual servers
- The applications (discrete apps, custom apps, and microservices apps) status such as **Critical**, **Review**, **Good**, and **Not Applicable**.

For more information, see Holistic view of applications in service graph.

Service graph for Kubernetes applications

Navigate to **Applications > Service Graph** and click the **Microservices** tab to:

- Ensure end-to-end application overall performance
- Identify bottlenecks created by inter-dependency of different components of your applications
- Gather insights into the dependencies of different components of your applications
- Monitor services within the Kubernetes cluster
- Monitor which service has issues
- Check the factors contributing to performance issues
- View detailed visibility of service HTTP transactions
- Analyze the HTTP, TCP, and SSL metrics
- View client metrics and client transaction summary details

By visualizing these metrics in NetScaler Console, you can analyze the root cause of issues and take necessary troubleshooting actions faster. Service graph displays your applications into various component services. These services running inside the Kubernetes cluster can communicate with various components within and outside the application. To get started, see Setting up service graph.

Service graph for 3-tier Web applications

Navigate to **Applications > Service Graph** and click the **Web Apps** tab to view:

- Details on how the application is configured (with content switching virtual server and load balancing virtual server)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For GSLB applications, you can view data center, NetScaler instance, CS, and LB virtual servers.

- End-to-end transactions from client to service
- The location from where the client is accessing the application
- The data center name where the client requests are processed and the associated data center NetScaler metrics (only for GSLB applications)
- Metrics details for client, service, and virtual servers
- If the errors are from the client or from the service
- The service status such as **Critical**, **Review**, and **Good**. NetScaler Console displays the service status based on service response time and error count.
  - **Critical (red)** - Indicates when average service response time > 200 ms AND error count > 0
  - **Review (orange)** - Indicates when average service response time > 200 ms OR error count > 0
  - **Good (green)** - Indicates no error and average service response time < 200 ms
- The client status such as **Critical**, **Review**, and **Good**. NetScaler Console displays the client status based on client network latency and error count.
  - **Critical (red)**- Indicates when average client network latency > 200 ms AND error count > 0
  - **Review (orange)** - Indicates when average client network latency > 200 ms OR error count > 0
  - **Good (green)** - Indicates no error and average client network latency < 200 ms
- The virtual server status such as **Critical**, **Review**, and **Good**. NetScaler Console displays the virtual server status based on the app score.
  - **Critical (red)** - Indicates when app score < 40
  - **Review (orange)** - Indicates when app score is between 40 and 75
  - **Good (green)** - Indicates when app score is > 75

Points to note:

- Only Load Balancing, Content Switching, GSLB virtual servers are displayed in service graph.
- If no virtual server is bound to a custom application, the details are not visible in service graph for the application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You can view metrics for clients and services in service graph only if active transactions occur between virtual servers and web application.
- If no active transactions available between virtual servers and web application, you can only view details in service graph based on the configuration data such as load balancing, content switching, GSLB virtual servers, and services.
- If any changes made in the application configuration, it may take 10 minutes to reflect in service graph.

For more information, see Service graph for applications.

Service graph for Kubernetes apps

The service graph feature in NetScaler Console enables you to monitor your Kubernetes applications in a graphical representation. You can onboard and set up the service graph, view service and ingress details, configure thresholds, trace requests, and troubleshoot issues across your microservices.

The following topics help you set up and use the service graph for Kubernetes apps:

- Simplified onboarding of service graph
- Setting up service graph
- View details in service graph
- Configure thresholds in service graph
- View service details
- View ingress details for troubleshooting
- Distributed tracing
- View diagnostics

Service Graph - Simplified onboarding

The onboarding process of service graph is simplified and you can onboard service graph by:

- Automatically deploying an agent as a Kubernetes job.
- Manually configuring service graph.

Automatically deploying an agent as a Kubernetes job

You can automate the onboarding process of service graph and this process automatically:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Downloads the YAML required for the agent.
- Configures the agent.
- Registers the Kubernetes cluster in NetScaler Console.
- Performs the required settings to populate service graph in NetScaler Console.

Prerequisites

Ensure that you have:

- A Citrix Cloud account.
- Installed Kubernetes version 1.19 or later.
- Installed HELM version 3.x.
- Opened the required ports.
- Established the connectivity by configuring the static routes. For registering NetScaler MPX or VPX in NetScaler Console using the agent, you must ensure to establish the connection between the cluster nodes and NetScaler MPX or VPX.

NOTE:

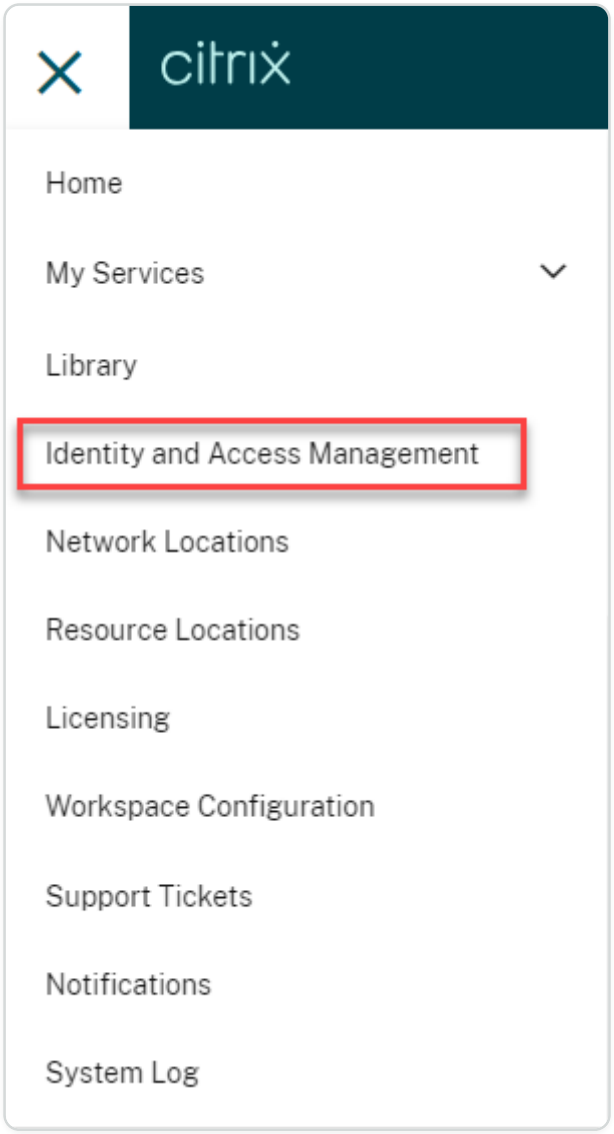
In case you do not want to configure the static routes, you can configure the node controller. For more information, see `https://github.com/citrix/citrix-k8s-node-controller` and `https://github.com/citrix/citrix-helm-charts/tree/master/citrix-node-controller`.

Get the client and secret CSV file from Citrix Cloud™

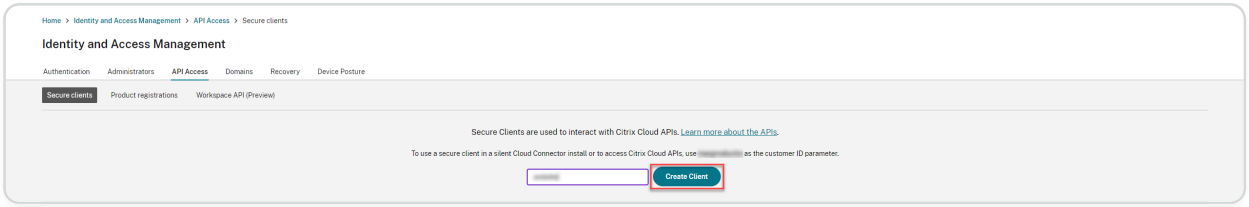
After you configure the agent, get the client and secret CSV file from the Citrix Cloud page:

1. Log on to citrix.cloud.com
2. Click the **Home** icon and select **Identity and Access Management**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

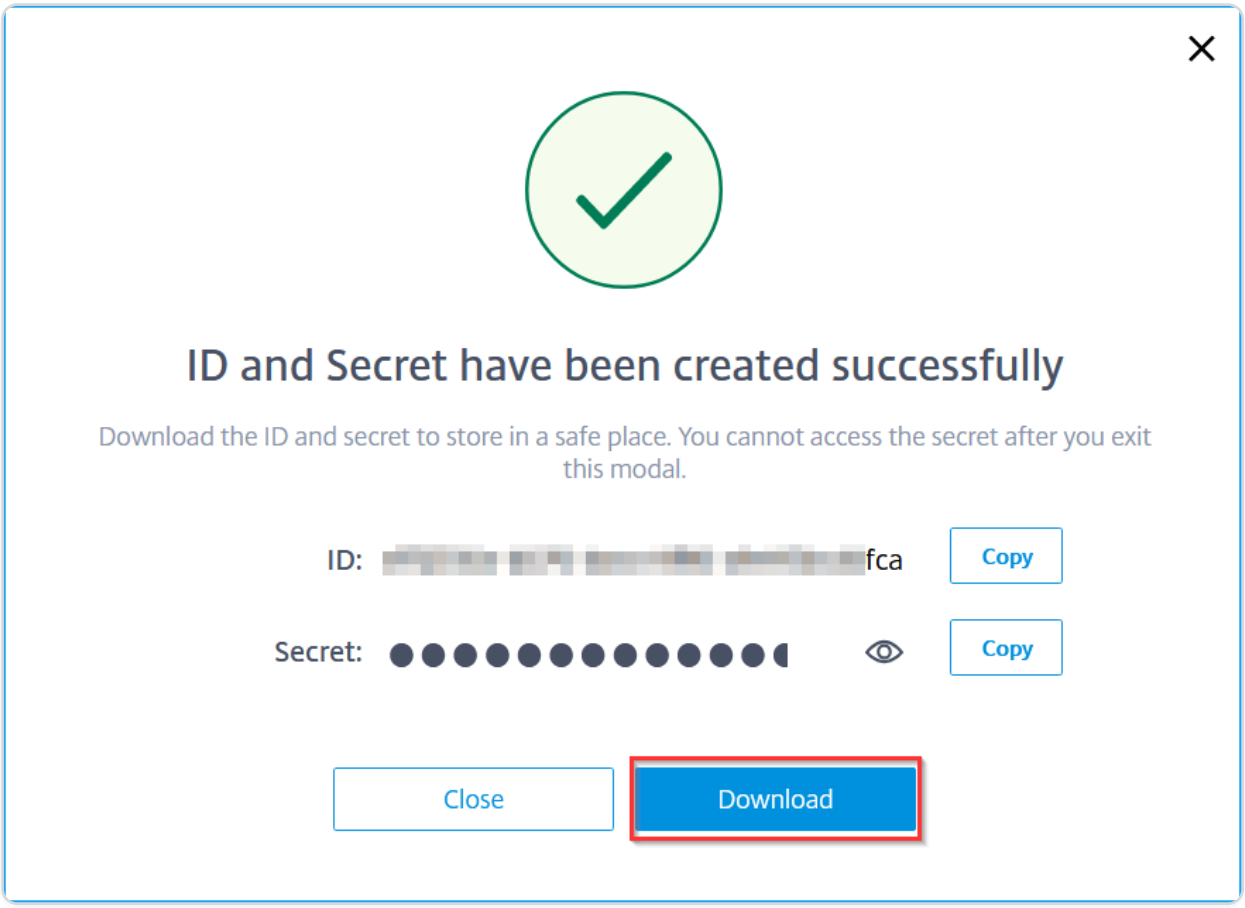


3. From the **API Access** tab, enter a secure client name and click **Create Client**.



4. ID and Secret is generated. Click **Download** and save the CSV file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. On the Kubernetes main node, run the following command to create an authorization token using the ID and secret: `wget https://raw.githubusercontent.com/citrix/citrix-helm-charts/master/generate_token.py`

   `python3 generate_token.py --accessID=<accessID> --accessSecret=<accessSecret>`

   Note

   The authorization token is valid only for 1-hour.

You can configure:

- NetScaler agent by creating an automatic secret

Or

- NetScaler agent by creating a manual secret

CONFIGURE THE NETSCALER CONSOLE BY CREATING AN AUTOMATIC SECRET

Deploy an agent using the helm chart

Run the following commands in the Kubernetes main node to deploy the agent:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
helm repo add citrix https://citrix.github.io/citrix-helm-charts
```

```
helm install citrix-adm citrix/adm-agent-onboarding --namespace <namespace> --set token=<Token>
```

The agent is deployed, and the cluster is registered to the NetScaler Console. When you create the agent using the automatic secret, it also enables you to deploy the `adm-agent-helper`, along with the agent that can create the Kubernetes Secret containing the agent credentials.

This process happens automatically when the namespace is labeled as `citrix-cpx=enabled`. Run the following command on the Kubernetes main node:

```
kubectl label namespace <namespace> citrix-cpx=enabled
```

Note

> If you want not to deploy `adm-agent-helper`, you can create the login secret manually for the agent.

Register NetScaler VPX/MPX with NetScaler Console

Note

> You can register the NetScaler VPX/MPX in NetScaler Console only for additional benefit.

To register the NetScaler VPX/MPX with NetScaler Console, you must establish the connectivity between NetScaler VPX or MPX and cluster nodes, by configuring the static routes. You can ignore this process if you have configured Citrix-node-controller.

You must create a Kubernetes secret containing the NetScaler VPX/MPX login credentials in the namespace. After this process, the agent onboarding is started.

```
kubectl create secret generic nslogin --from-literal=username=<username> --from-literal=password=<adc-password> -n <namespace>
```

You must set the management IP address of NetScaler VPX/MPX as an environment variable: `adc.IP`.

```
helm repo add citrix https://citrix.github.io/citrix-helm-charts
```

```
helm install citrix-adm citrix/adm-agent-onboarding --namespace <namespace> --set adc.IP=<ADC ManagementIP>,adc.loginSecret=nslogin --set token=<Token>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Note

Ensure that the management HTTP port adc.mgmtHTTPPort and HTTPS port adc.mgmtHTTPSPort as 80 and 443 are open.

CONFIGURE THE AGENT BY CREATING A MANUAL SECRET

NetScaler CPX requires the agent login credentials for registering itself to NetScaler Console. You can manually set the namespace to deploy the NetScaler CPX.

```
kubectl create secret generic admlogin --from-literal=username=nsroot --from-literal=password=<adm-agent-password> -n <namespace>
```

After you create the secret, you can use the following command to configure the agent.

```
helm install citrix-adm citrix/adm-agent-onboarding --namespace <namespace> --set admAgent.loginSecret=admlogin --set token=<Token>
```

Register NetScaler VPX/MPX with NetScaler Console

To register the NetScaler VPX/MPX with NetScaler Console, you must establish the connectivity between NetScaler VPX or MPX and cluster nodes, by configuring the static routes. You can ignore this process if you have configured `Citrix-node-controller`.

After configuring the static routes, you must create a Kubernetes secret containing the NetScaler VPX/MPX login credentials in the namespace. After this process, the agent onboarding is started.

```
kubectl create secret generic nslogin --from-literal=username=<username> --from-literal=password=<adc-password> -n <namespace>
```

You must set the management IP address of NetScaler VPX/MPX as an environment variable: `adc.IP`.

```
helm repo add citrix https://citrix.github.io/citrix-helm-charts
```

```
helm install citrix-adm citrix/adm-agent-onboarding --namespace <namespace> --set adc.IP=<ADC ManagementIP>,adc.loginSecret=nslogin --set token=<Token>
```

Note

Ensure that the management HTTP port adc.mgmtHTTPPort and HTTPS port adc.mgmtHTTPSPort as 80 and 443 are open.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After you configure the mentioned steps, service graph starts to populate within 15 minutes duration. In NetScaler Console, navigate to **Applications > Service Graph** and then click **Microservices** to view service graph.

Examples:

- To generate service graph with Service Mesh Lite, see Service graph example.
- To generate service graph of Citrix integration with Istio Service Mesh, see Service graph with NetScaler Observability and NetScaler Console.

Manually configuring service graph

You can populate service graph manually by:

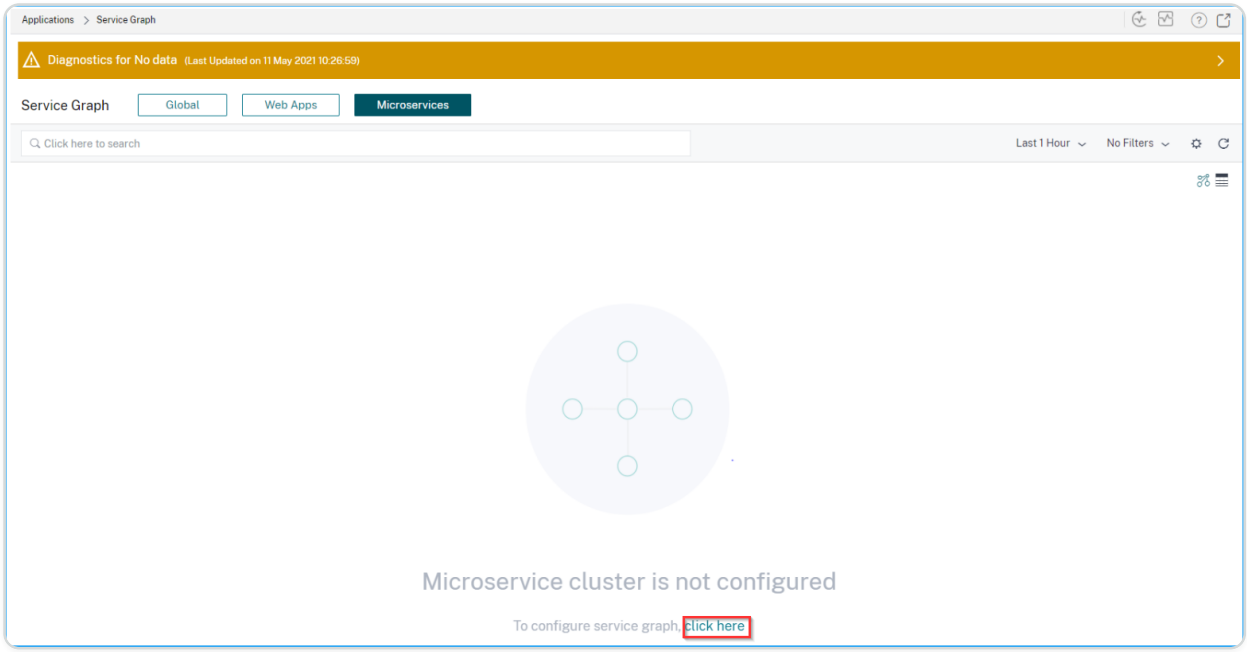
- Configuring the agent as a microservice in the Kubernetes cluster.
- Completing the other workflows such as registering cluster, adding instances, and enabling licensing and detailed TCP and Web transactions.

> **NOTE**
>
> If you want to use an existing agent or configure an on-premises NetScaler agent using a hypervisor, follow the procedures at Setting up service graph to populate the service graph.

1. Navigate to **Applications > Service Graph** and select the **Microservices** tab.

   You can view the microservices cluster is not configured. Click the option to configure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Select **Custom Deployment**.
3. Select the deployment type.
4. Select **Microservices** as the application type.
5. Click **Next** to set up the agent.
6. In the **Download Agent Microservice** page, specify the following parameters:
   a. **Application ID** – A string id to define the service for the agent in the Kubernetes cluster and distinguish this agent from other agents in the same cluster.
   b. **Password** – Specify a password for CPX to use this password to onboard CPX to NetScaler Console through the agent.
   c. **Confirm Password** – Specify the same password for confirmation.

      Note

      You must not use the default password (`nsroot`).

   d. Click **Submit**.
7. Click **Download YAML** File or **Download Helm Chart**.
8. In the Kubernetes main mode, save the downloaded YAML file and run the following command to register the agent:

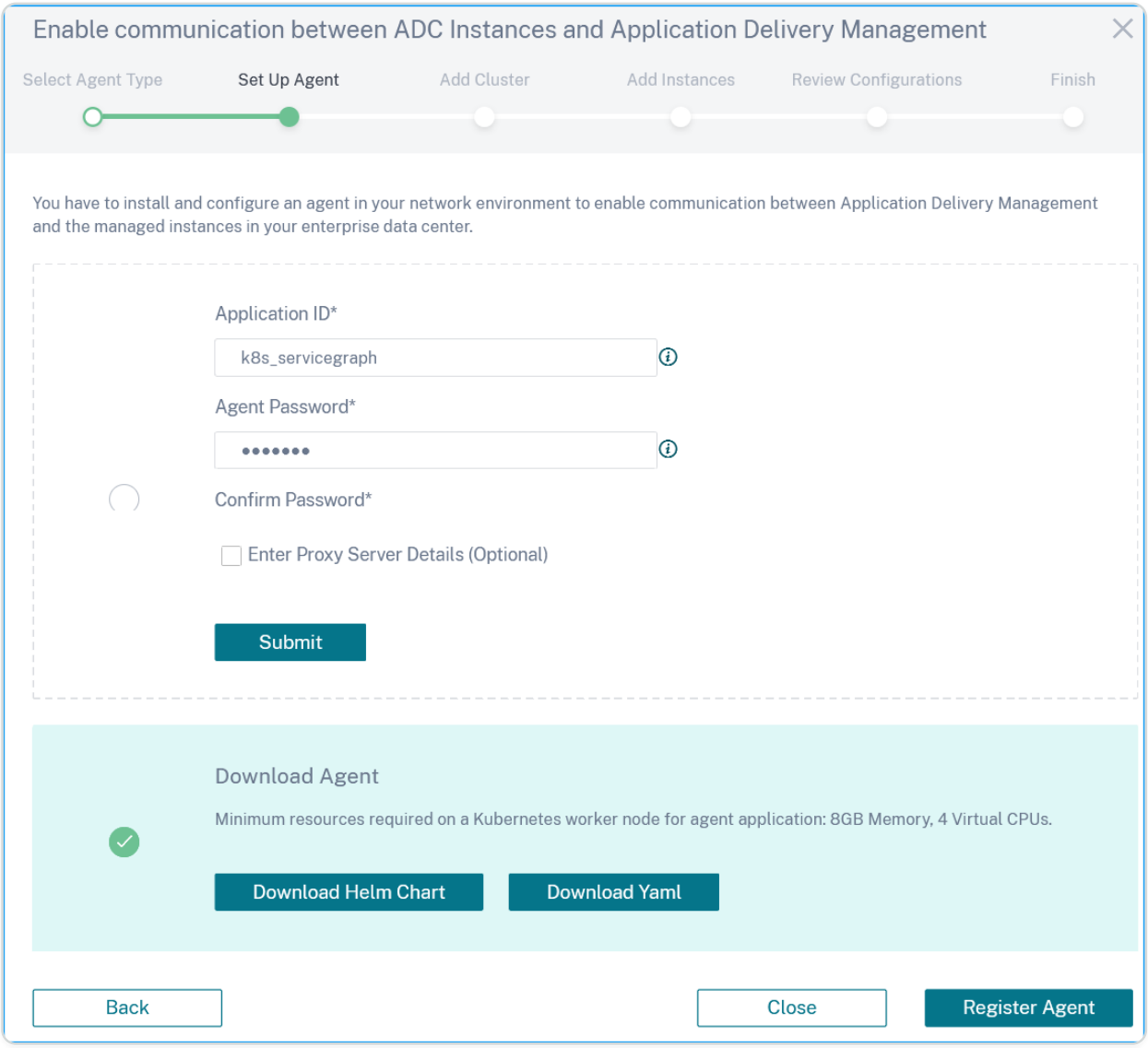
   ```
   kubectl create -f <yaml file>
   ```

   For example, `kubectl create -f testing.yaml`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The agent is successfully created.

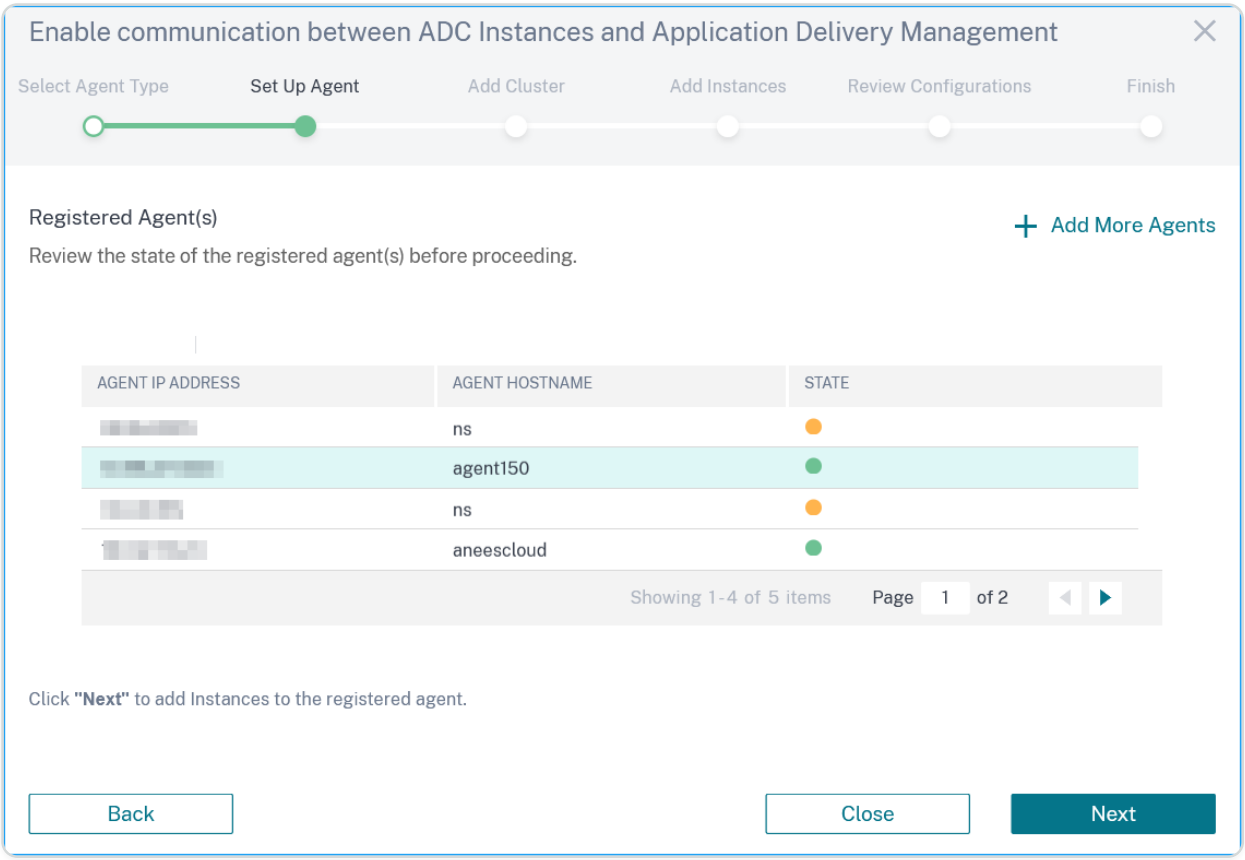
9. Click **Register Agent**.



The page loads for a few seconds and displays the registered agent.

10. Ensure if the agent is present in the list and click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

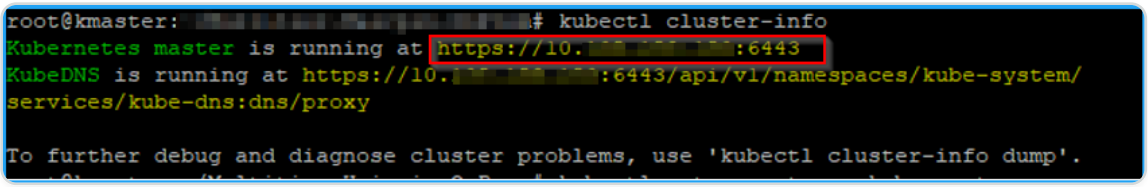


11. You must register the cluster. Click **Add More Clusters** and specify the following parameters:

    a. **Name** - Specify a name of your choice.

    b. **API Server URL** - You can get the API Server URL details from the Kubernetes main node.

        i. On the Kubernetes main node, run the command `kubectl cluster-info`.



        ii. Enter the URL that displays for **"Kubernetes main is running at."**

    c. **Authentication Token** - Specify the authentication token. The authentication token is required to validate access for communication between Kubernetes cluster and NetScaler Console. To generate an authentication token:

        On the Kubernetes main node:

        i. Use the following YAML to create a service account:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
apiVersion: v1

kind: ServiceAccount

metadata:

  name: <name>

  namespace: <namespace>
```

ii. Run `kubectl create -f <yaml file>`.

The service account is created.

iii. Run `kubectl create clusterrolebinding <name> --clusterrole=cluster-admin --serviceaccount=<namespace>:<name>` to bind the cluster role to service account.

The service account now has the cluster-wide access.

A token is automatically generated while creating the service account.

iv. Run `kubectl describe sa <name>` to view the token.

v. To get the secret string, run `kubectl describe secret <token-name>`.

```
root@kmaster:~# kubectl describe secret citrixadm-sa-token-79knw
Name:         citrixadm-sa-token-79knw
Namespace:    default
Labels:       <none>
Annotations:  kubernetes.io/service-account.name: citrixadm-sa
              kubernetes.io/service-account.uid: 136270eb-1fe1-11ea-b603-72328a2
af136

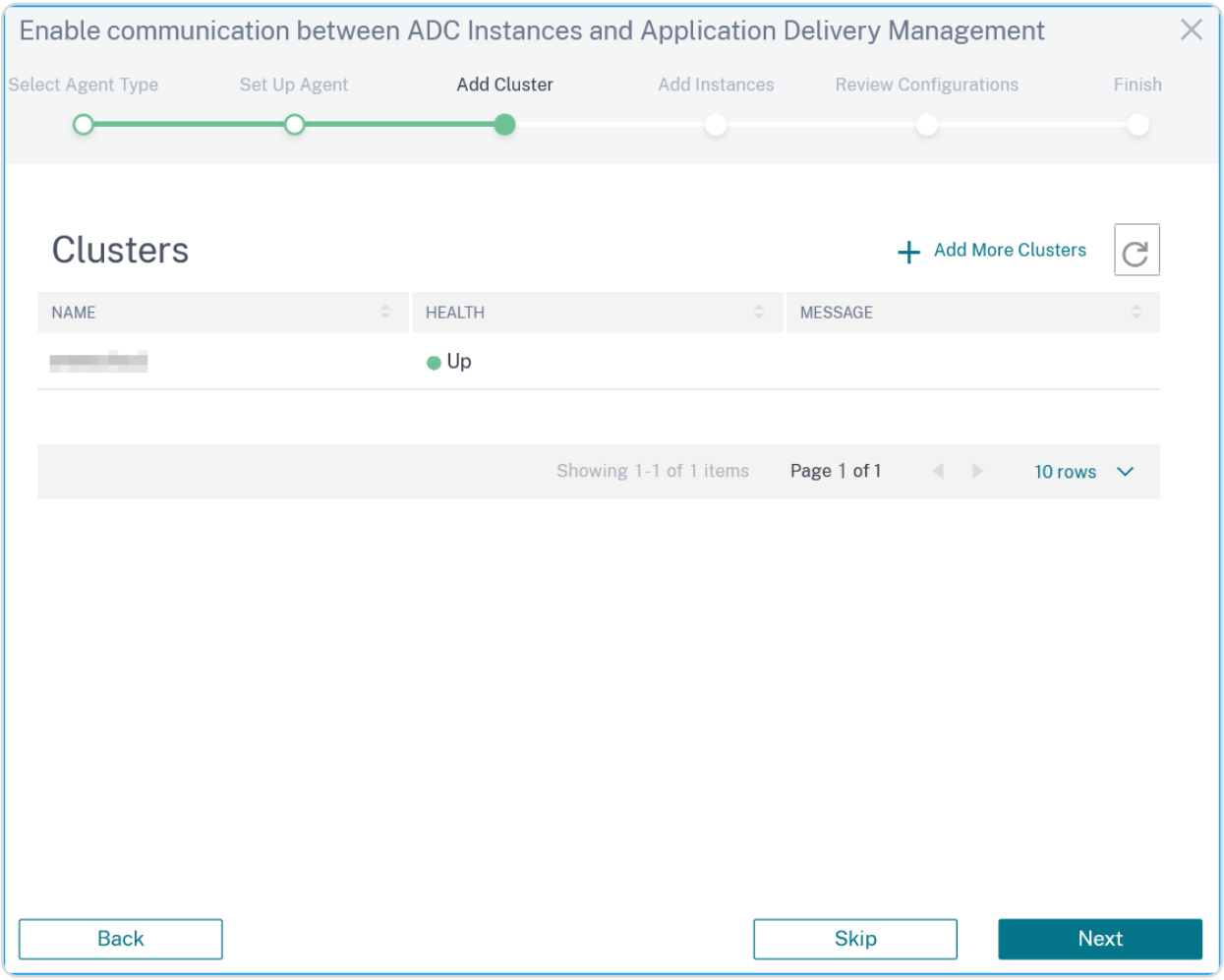
Type:  kubernetes.io/service-account-token

Data
====
ca.crt:     1025 bytes
namespace:  7 bytes
token:      eyJhbGciOiJSUzI1NiIsImtpZCI6IiJ9.eyJpc3MiOiJrdWJlcm5ldGVzL3NlcnZpY2V
hY2NvdW50Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9uYW1lc3BhY2UiOiJkZWZhdWx0Iiw
ia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9zZWNyZXQubmFtZSI6ImNpdHJpeGFkbS1zYS10b2t
lbi03OWtudyIsImt1YmVybmV0ZXMuaW8vc2VydmljZWFjY291bnQvc2VydmljZS1hY2NvdW50Lm5hbWU
iOiJjaXRyaXhhZG0tc2EiLCJrdWJlcm5ldGVzLmlvL3NlcnZpY2VhY2NvdW50L3NlcnZpY2UtYWNjb3V
udC51aWQiOiIxMzYyNzBlYi0xZmUxLTExZWEtYjYwMy03MjMyOGEyYWYxMzYiLCJzdWIiOiJzeXN0ZW0
6c2VydmljZWFjY291bnQ6ZGVmYXVsdDpjaXRyaXhhZG0tc2EifQ.JsU4JPcyFoXA6Vn5Dxa137ca_hI0
wzY1Ajv0ctHN7NeU4YC_I6H5xgNAKnqj2rJPlQEmSZQygPOrxduLDYsNBCT9fH4sv1aBdOzzpkCIDW6y
6BmX4IaC6HTFPGO54zSDzjPmuKkPzyIRa4twUSvxfhwXE6JRy99iJjgPBraL65ct99bcVXF5nMDdexro
Iw23M8lcknV5fPuD33WhieS17WbXlq_ZYEA4WaulGXi9veHczN1S9oFPUlnM3d13R7A63bZjCKvWYlnN
7W5etxd2dfLgEJysixj8lKRxUifL2f04lfWM8ucwKVb8TumsMqG7eturRF5SxSYNodmBKNNkIA
```

12. Select the agent from the list.

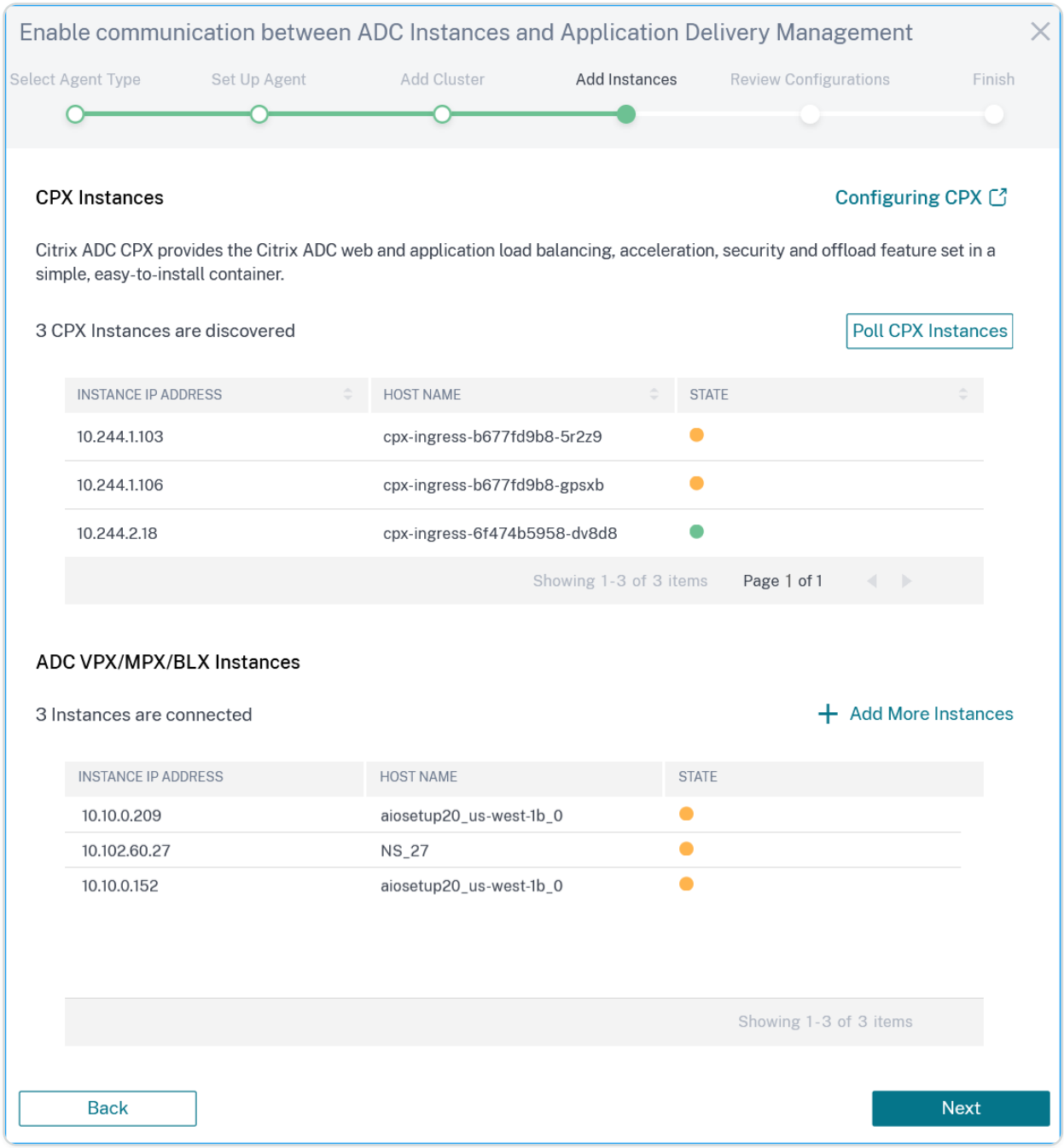
© 1997–2026 Citrix Systems, Inc. All rights reserved.

13. Click **Create**.
14. In the **Clusters** page, the cluster information is displayed. Click **Next**.



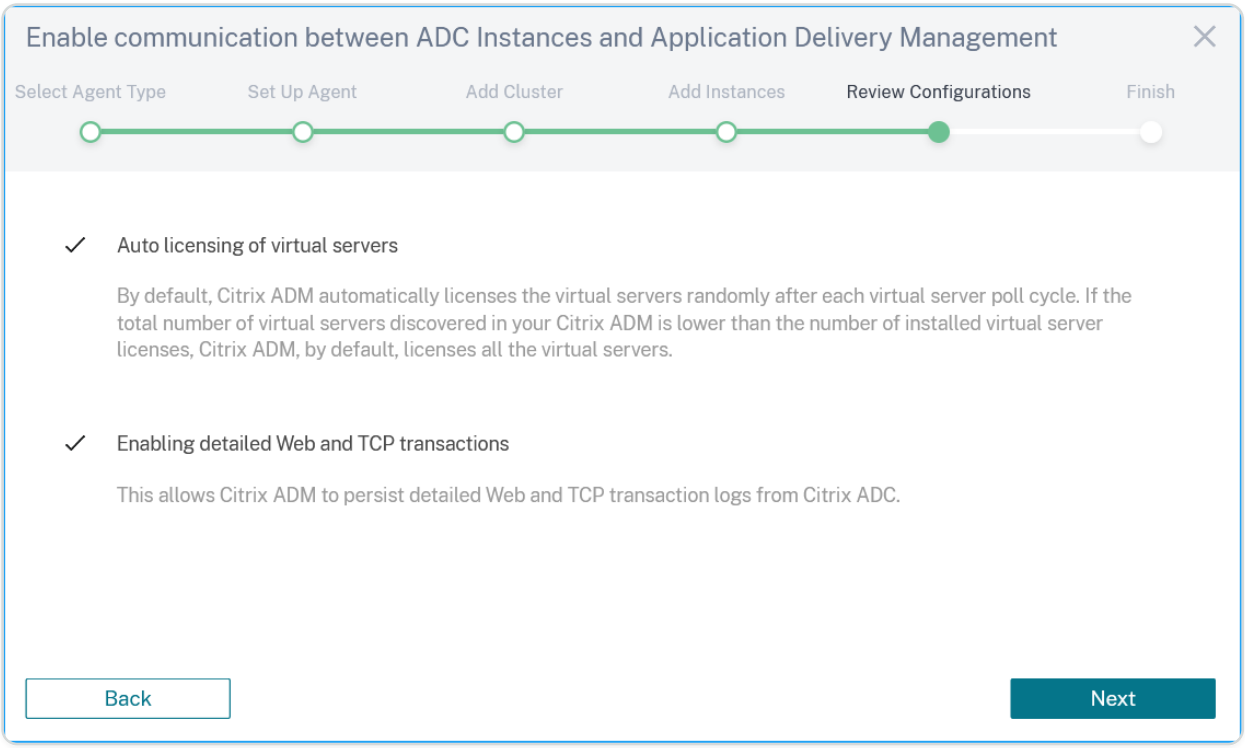
15. Configure the CPX and VPX instances, and click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

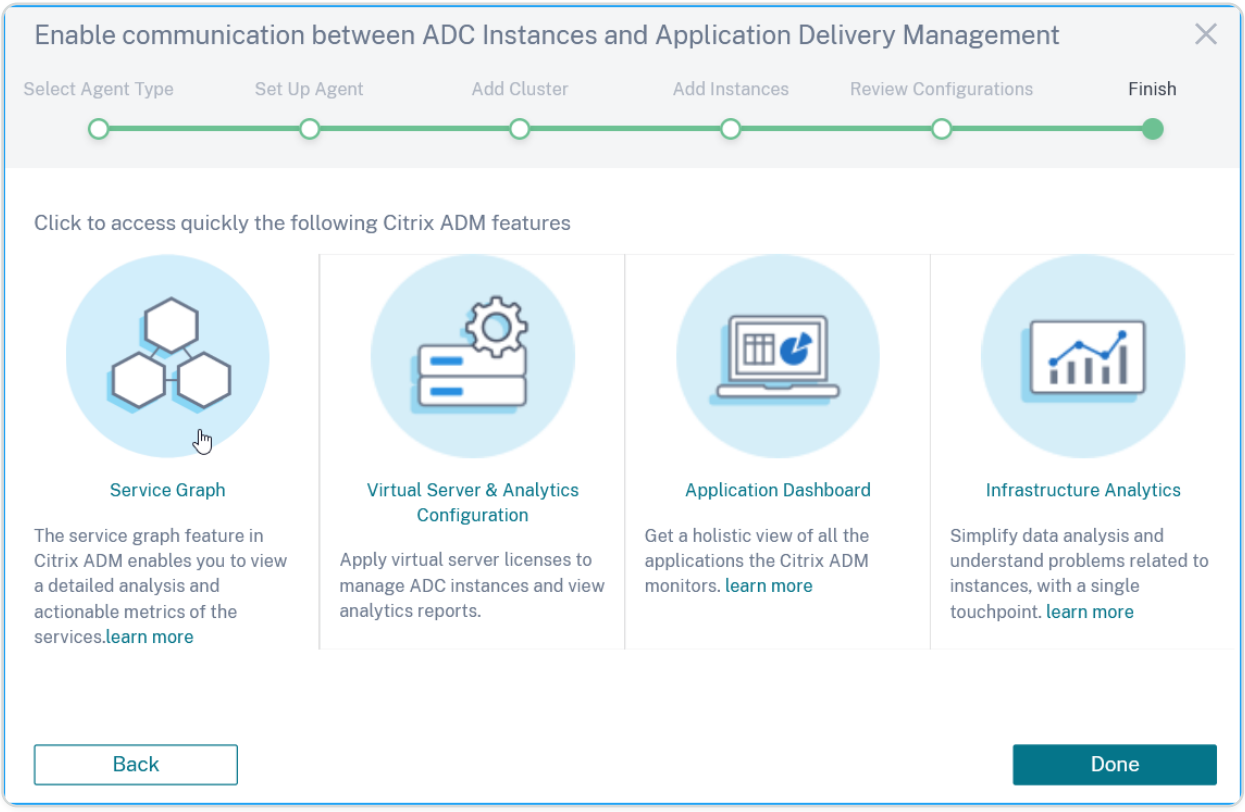


16. Click **Next** to enable detailed web and TCP transactions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



17. The configurations are complete. Select **Service Graph** and click **Done**.



The Service Graph gets populated in approximately 15 minutes. Navigate to **Applications > Service Graph** and select the **Microservices** tab to view service graph.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Setting up service graph

Software requirements

KUBERNETES DISTRIBUTION	KUBERNETES VERSION	CONTAINER NETWORK INTERFACES (CNI)	CPX VERSION	CIC VERSION	AGENT VERSION	
Open source	v1.16.3	Flannel, Calico, or Canal	13.0–47.103 or later	1.6.1 or later	13.0–49.x or later	

You can configure the Kubernetes cluster with various deployment topologies and the following table provides the topologies that are supported in service graph:

TOPOLOGY	SUPPORTED IN SERVICE GRAPH
Single-Tier or Unified ingress	Yes
Dual-Tier	Yes
Cloud	Yes, but cloud load balancer is not shown in the graph
Service mesh lite	Yes
Service mesh	Yes
Services of type LoadBalancer	No
Services of type NodePort	No

To complete setting up service graph in NetScaler Console, click the topology type that you have configured for your Kubernetes cluster and complete the mentioned procedures:

- Single-tier or Unified ingress topology
- Dual-tier or Service Mesh Lite topology
- Service mesh topology

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

The procedure to set up service graph for dual-tier and service mesh lite topologies remains the same.

Single tier or Unified ingress topology

Ensure that you complete the following steps to set up the single tier or unified ingress topology. For more information, see Detailed procedures to setup single tier or unified ingress topology.

- Configured Kubernetes cluster with single tier or unified ingress topology.
- Added VPX, MPX, SDX, BLX instance in NetScaler Console and enabled **Web Insight**.
- Added Kubernetes cluster in NetScaler Console.

Dual tier or Service Mesh Lite topology

Ensure that you complete the following steps to set up the dual tier or service mesh lite topology. For more information, see Detailed procedures to setup dual tier or service mesh lite topology.

- Configured Kubernetes cluster with any one of the supported topologies.
- Installed an agent and configured to enable communication between NetScaler Console and Kubernetes cluster or managed instances in your data center or cloud.

  You can also deploy an agent as a microservice. For more information, see the **Install a NetScaler agent section** in Getting Started.
- Configured Static routes on the agent to enable communication between NetScaler Console and NetScaler CPX.

  NOTE

  You can ignore this procedure if you have deployed an agent as a microservice in the same cluster.
- Downloaded the sample deployment files from GitHub repository.
- Added required parameters in CPX YAML file to ensure successful CPX registration with NetScaler Console.
- Added a VPX, MPX, SDX, or BLX instance in NetScaler Console.
- Added the Kubernetes cluster in NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Deployed a sample microservice application.
- Deployed NetScaler CPX and registered CPX to NetScaler Console (applicable only for two-tier architecture).
- Enabled Web transaction and TCP transaction settings to **All** for the agent to get HTTP and TCP transactions.
- Sent traffic to microservices.

Service mesh topology

Ensure that you complete the following steps to set up the service mesh topology. For more information, see Detailed procedures to setup service mesh topology.

- Configured Kubernetes cluster version `1.14.0` with any one of the following service mesh topologies:
  - NetScaler CPX as a sidecar proxy for Istio
  - NetScaler as an Ingress Gateway for Istio
- Enabled `admissionregistration.k8s.io/v1beta1` API. You can verify the API by using:

  ```
  kubectl api-versions | grep admissionregistration.k8s.io/v1beta1
  ```

  The following output indicates that the API is enabled:

  ```
  admissionregistration.k8s.io/v1beta1
  ```
- Installed Istio `istio v.1.3.0`.
- Installed Helm version 3.x.
- Installed an agent and configured to enable communication between NetScaler Console and Kubernetes cluster or managed instances in your data center or cloud.

  You can also deploy an agent as a microservice. For more information, see the **Install a NetScaler agent section** in Getting Started.
- Configured Static routes on the agent to enable communication between NetScaler Console and NetScaler CPX.

  NOTE

  You can ignore this procedure if you have deployed NetScaler agent as a microservice in the same cluster.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Configured the required parameters to populate the service mesh topology data.
- Deployed a sample application.
- Added the Kubernetes cluster in NetScaler Console.
- Enabled Web transaction and TCP transaction settings to **All** for the agent to get HTTP and TCP transactions.
- Sent traffic to microservices.

After you complete the required setup procedures, you can view service graph populated at **Applications** > **Service Graph** and in the **Microservices** tab. For more information, see Service Graph details.

View details in service graph

After you add the Kubernetes cluster in NetScaler Console, it takes approximately 10 minutes to get the data populated in service graph. Navigate to **Applications** > **Service Graph** and click the **Microservices** tab to view the service graph details.

TWO-TIER/SERVICE MESH LITE TOPOLOGY	SINGLE-TIER/UNIFIED INGRESS TOPOLOGY
	

- **Tier 1 ingress** – NetScaler Ingress Controller inside the Kubernetes cluster configures a NetScaler instance (VPX/MPX/SDX/BLX) outside the Kubernetes cluster.
- **Tier 2 ingress** – NetScaler Ingress Controller running as a sidecar along with NetScaler CPX instance inside the Kubernetes cluster.
- **Ingress** – Displays for all other deployment topologies.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service graph dashboard



1 - End-to-end network map of your application that shows how your component services are communicating

2 – Graph that indicates hits and errors for a specific time duration

3 – Search bar to search for services

4 – Time list to select the time duration

5 - Apply filters to display services

6 – Setting icon

7 – Zoom in and zoom out view

8 – Graph view or tabular view

Based on the selected time duration, you can view the service graph.

SERVICE ICON	DESCRIPTION
	The edge width indicates the number of hits. The greater or more the edge width, indicates the number of hits is higher.
	Service with a warning icon indicates that the service has errors.

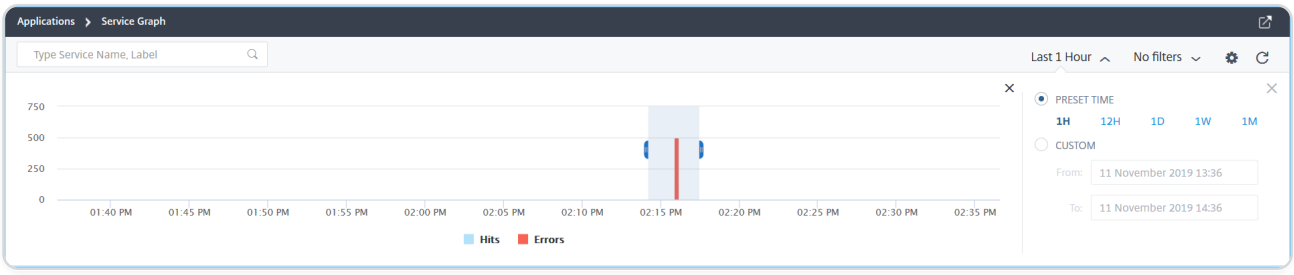
© 1997–2026 Citrix Systems, Inc. All rights reserved.

SERVICE ICON	DESCRIPTION
	Service with a stopwatch icon indicates that the service has latency or response time issues.
	Service with both stopwatch and warning icons indicate that the service has both errors and latency/response time issues.

NOTE

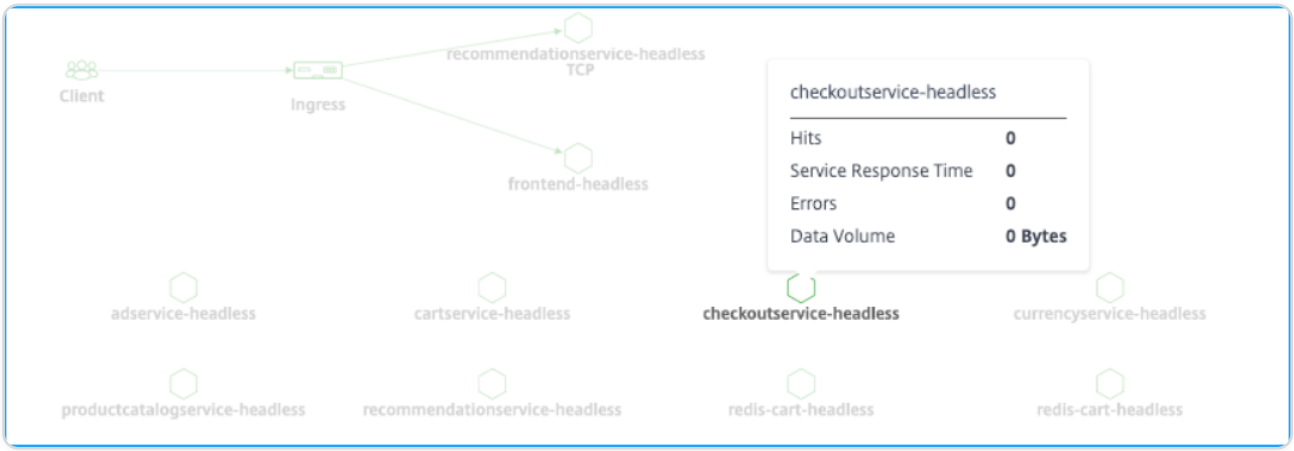
If a service has no warning or stopwatch icon, it indicates that the service has anomalies or threshold breach for Hits.

Select the time period from the graph that indicates hits to drill down further for additional information.



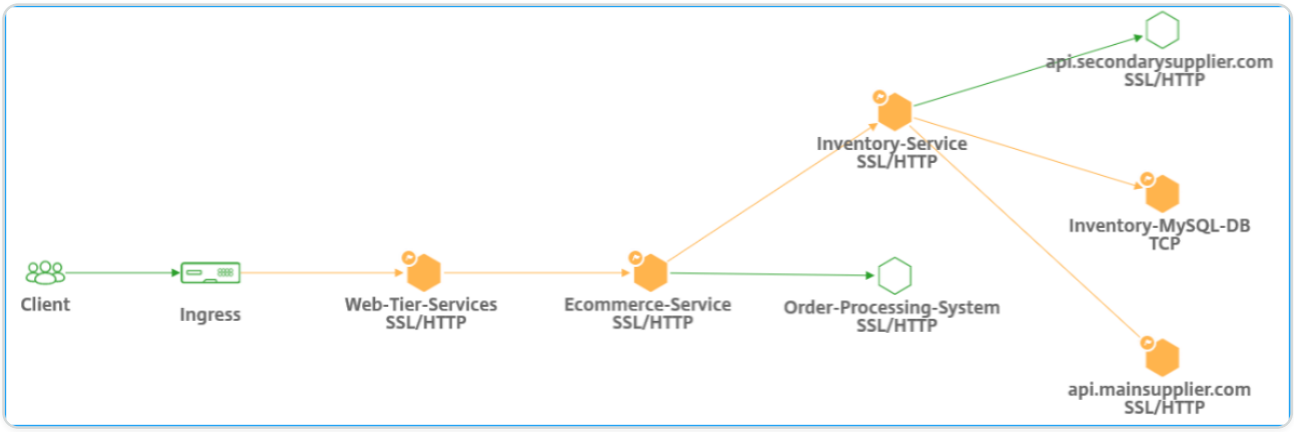
NOTE

If no active transactions received by NetScaler Console, you can view only the services that are load balanced by the NetScaler instance. When you hover the mouse pointer on a service, all metrics are displayed as 0.



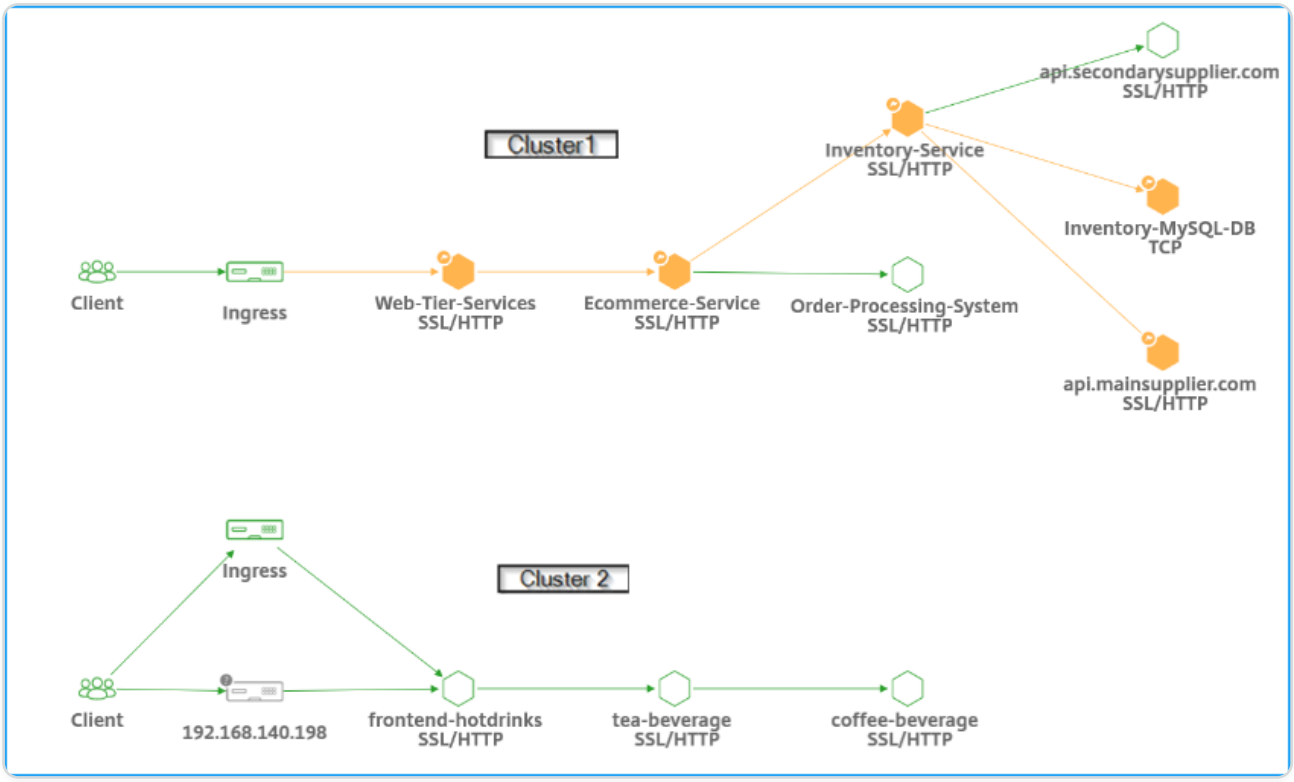
© 1997–2026 Citrix Systems, Inc. All rights reserved.

The service graph is now displayed with the protocol used by the services. Consider that you have the following services running in your Kubernetes cluster as shown in the image:



NOTE

If you have added multiple clusters in **Infrastructure > Orchestration > Kubernetes > Clusters**, you can view services associated with each cluster.



You can view the following status for your services:

- **Critical (red)** - Service has anomalies or threshold breach in multiple metrics. For the default thresholds, Critical status indicates average service response time > 200 ms AND error count > 0

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Review (orange)** - Service has anomalies or threshold breach in any one of the metrics. For the default thresholds, Review status indicates average service response time > 200 ms OR error count > 0
- **Good (green)** - Service with no anomalies or no threshold breach. For the default thresholds, Good status indicates no error and average service response time < 200 ms

  For more information on anomalies, see Monitor services using the golden signal metrics.

  For more information on thresholds, see Configure thresholds in service graph.

The following are protocols that enable you to identify the protocol used by a service:

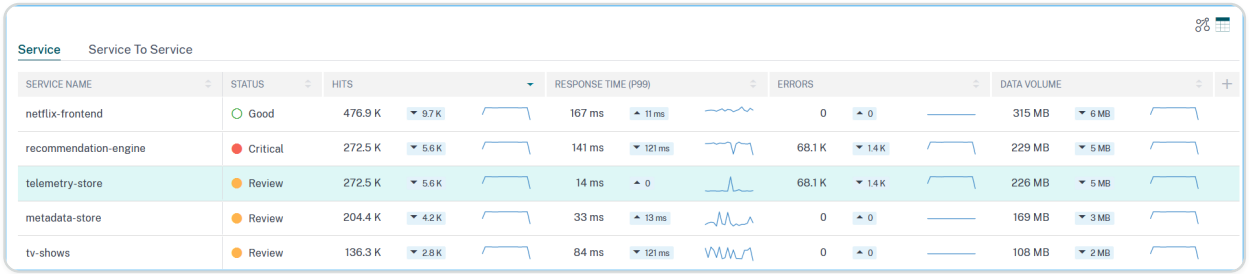
- **TCP** – Indicates the service is using the TCP protocol.
- **SSL, HTTP** – Indicates the service is using the SSL over HTTP protocol.
- **SSL, TCP** – Indicates the service is using the SSL over TCP protocol.

> **NOTE**
>
> The service without a protocol indicates the service is using the HTTP protocol.

View key metrics trends using the tabular view

Using the tabular view, you can see:

- Key metrics for the service
- Key metrics between a source service to a destination service

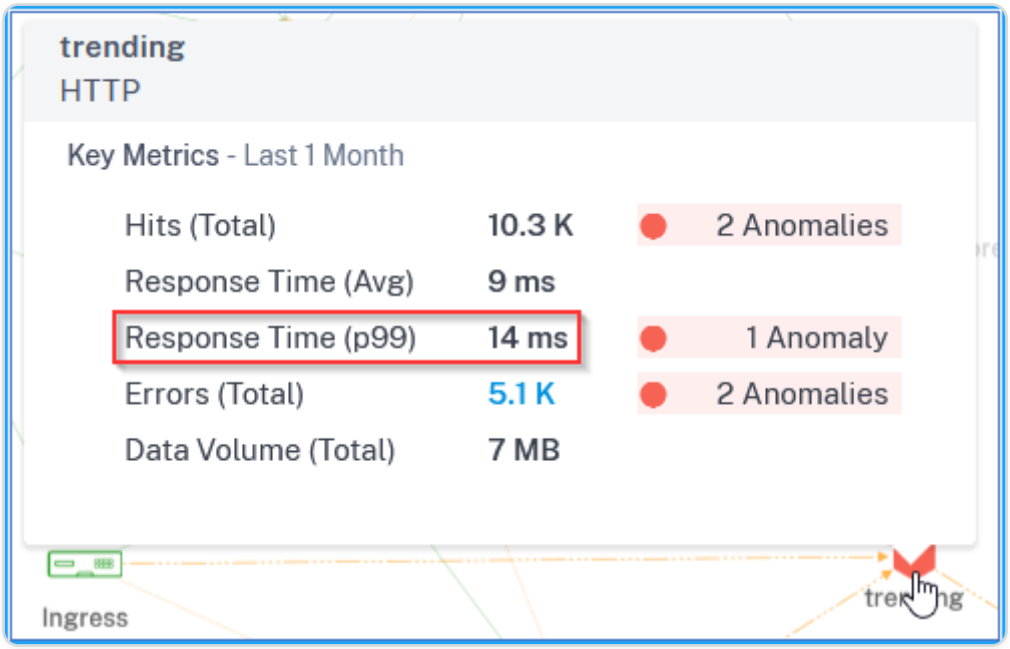


As an administrator, using these key metrics, you can analyze the trends of golden signals for the selected time duration. For more information, see View service details.

View Pxx value for the service response time

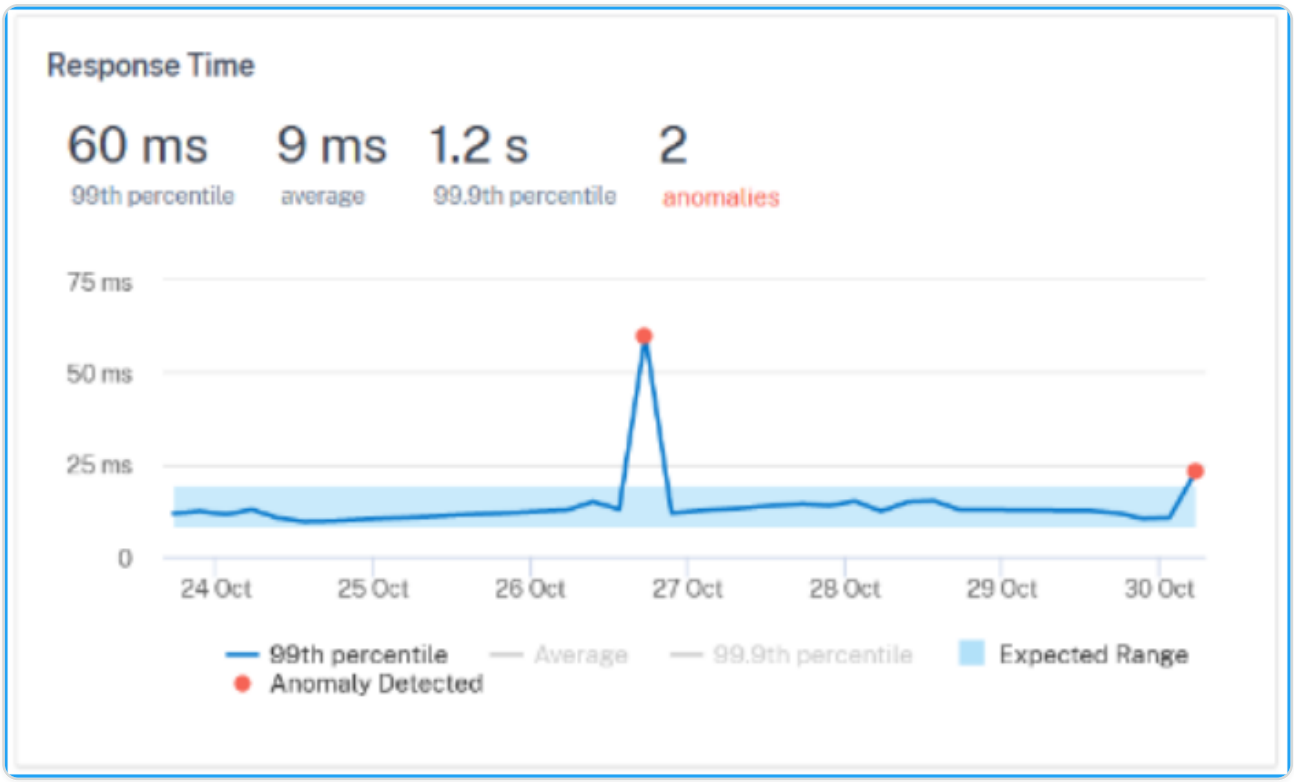
Hover the mouse point on a service to view the Pxx value for the response time.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Response Time (P99) – Denotes that the 99% of the requests for the selected duration is less than P99 value.

When you drill down to view the service details, you can also view the 99th percentile and 99.9th percentile of the response time for the selected duration.

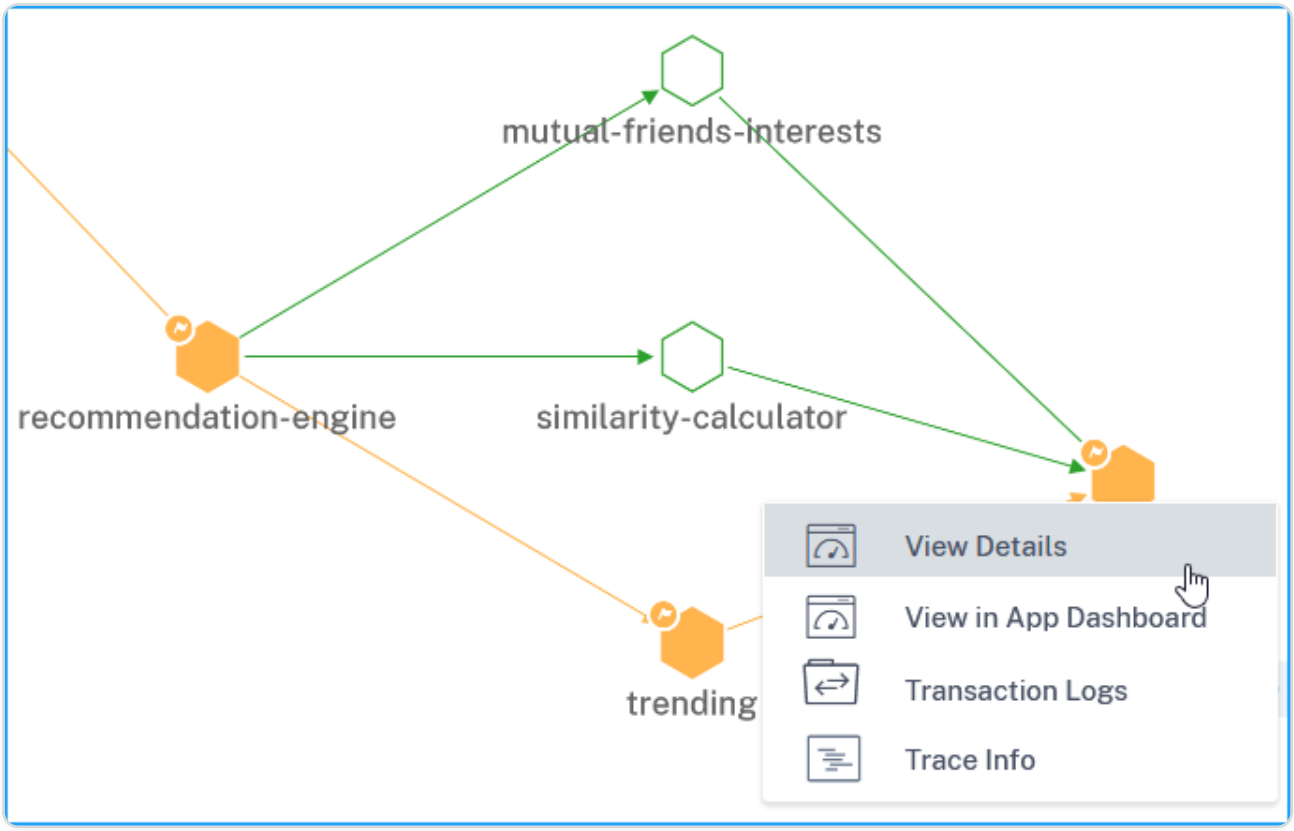


As an administrator, using the pxx value, you can understand the service response time better. For more information, see View service details.

View service details

Click a service to view the following options:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



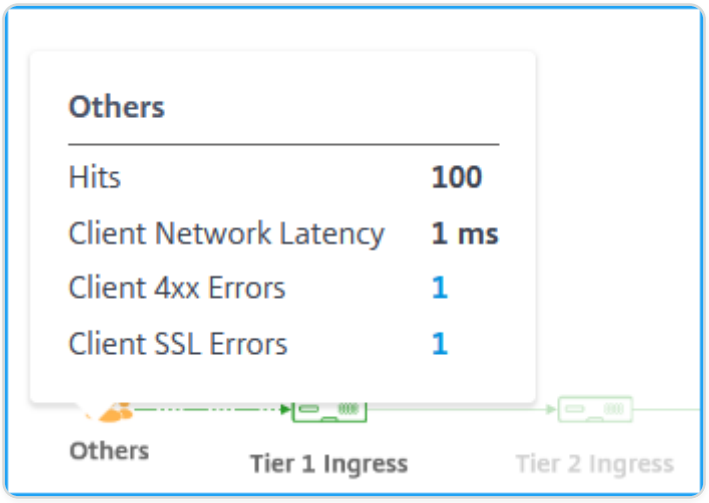
- **View Details** - Enables you to view the service details such as namespace, labels, cluster where the service is hosted, and so on. For more information, see View service details.
- **View in App Dashboard** - Enables you to view the selected application details such as app score, Kubernetes service details, pod details, and so on. For more information, see Kubernetes application details
- **Transaction Logs** - Enables you to view the HTTP and SSL over HTTP transaction details. For more information, see View analytics for Web transactions.
- **Trace Info** - Enables you to view the service distributed tracing. For more information, see Distributed tracing.

View client metrics

You can view from which location the client is accessing the service. As an administrator, you can visualize the client metrics and analyze the issues that occur from the client.

Hover the mouse pointer on a client region to view the metrics.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Hits** - Indicates the total hits received by the client.
- **Client Network Latency** - Indicates the average client network latency.
- **Client 4xx Errors** - Indicates the total client 4xx errors.
- **Client SSL Errors** - Indicates the total client SSL errors.

IP blocks in NetScaler Console - NetScaler Console can recognize the client location if the client uses a public IP address. NetScaler Console has its built-in location CSV file that matches the location based on the client IP address range.

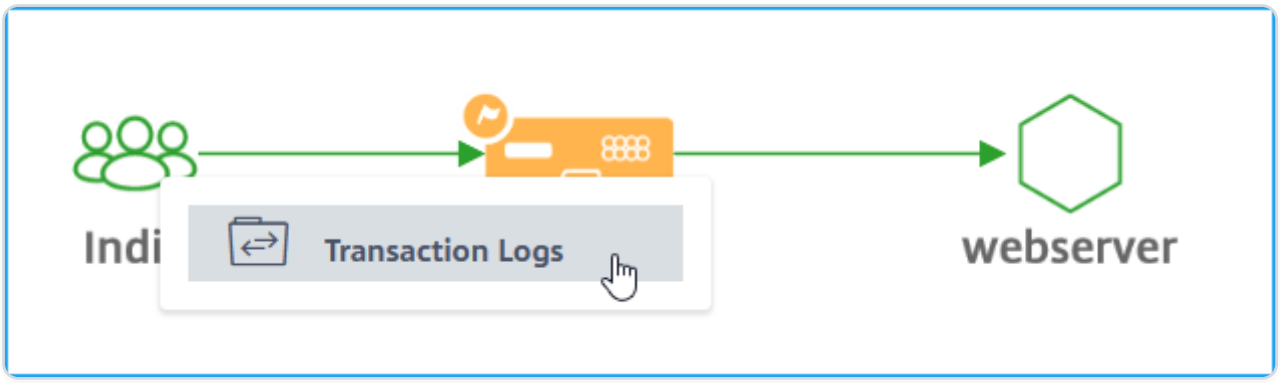
NetScaler Console can recognize the client location with private IP address only when the IP address is added to the NetScaler Console server. For example, if the client IP address falls within a private IP address range associated with City A, NetScaler Console recognizes that the traffic is originating from City A for this client.

View client transaction summary

The detailed client transaction summary enables you to view:

- Response time > 500 ms
- 5xx errors

Click a client location and select **Transaction Logs**.

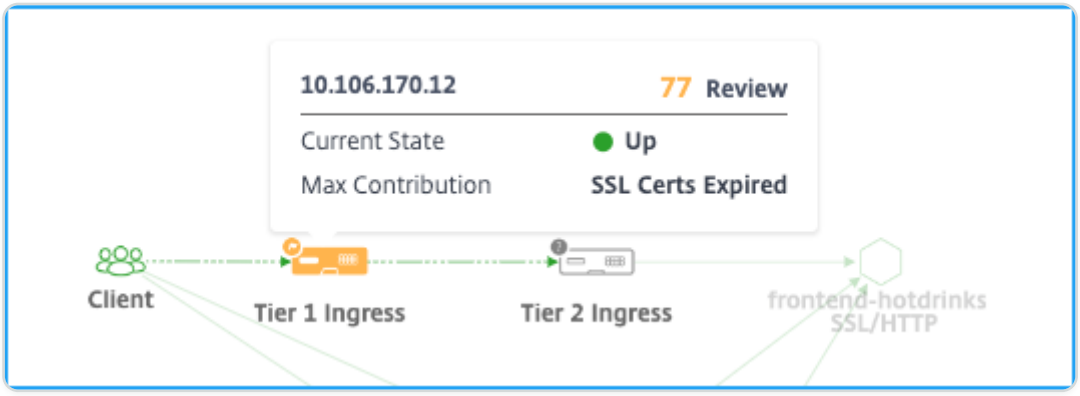


© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information, see Web transaction analytics.

View ingress metrics

You can view the type of ingress used in the Kubernetes cluster.



- NetScaler IP address and its score
- **Current State** – Indicates if the NetScaler instance is Up, Down, or Out of Status
- **Max Contribution** – Indicates the issue that is affecting the instance score

For the single-tier topology, you can view only a single **Ingress**.

Click the **Ingress** to drill down further for details. For more information, see View ingress details for troubleshooting issues.

View TCP and SSL metrics

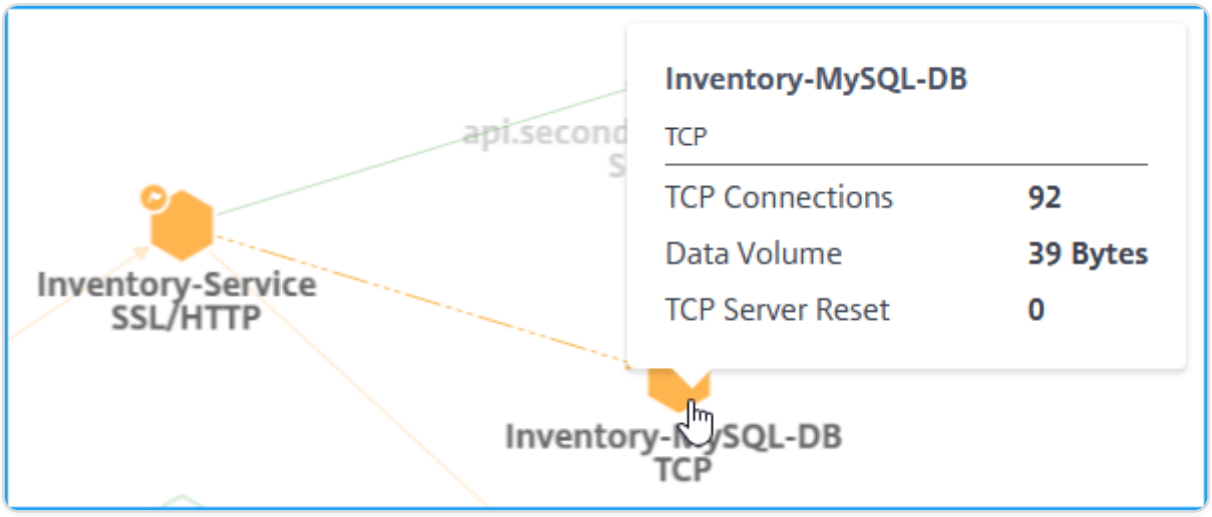
Using the TCP and SSL metrics, you can:

- View TCP connection details between services
- Determine if TCP-related issues are from the source or destination service
- View if the SSL error is from the source or destination service
- View the SSL protocol version used by SSL services

TCP metrics

Hover the mouse pointer over a TCP service or its associated incoming service to view the TCP metrics.

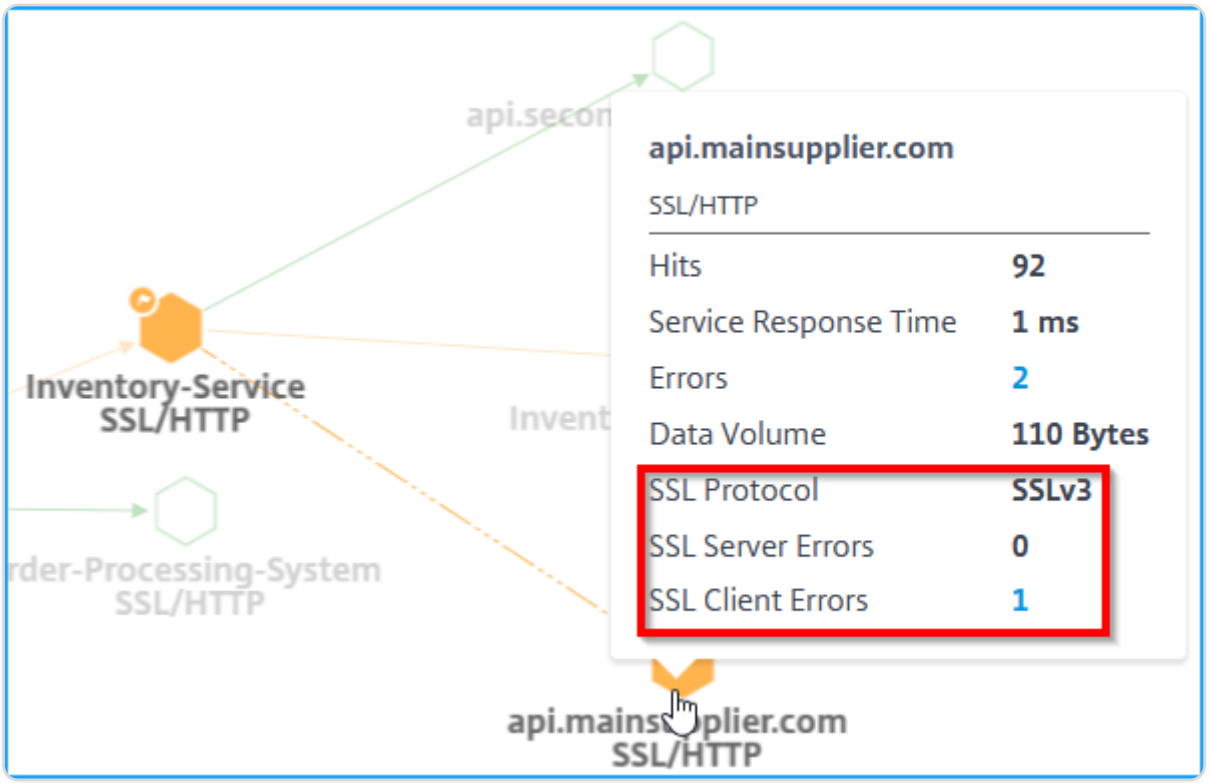
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **TCP connections** – Total connections established between the services
- **Data Volume** – Total data processed by the service
- **TCP Server Reset** – Total TCP resets initiated from the server

SSL metrics

Hover the mouse pointer on a service that uses SSL protocol to view the SSL metrics.



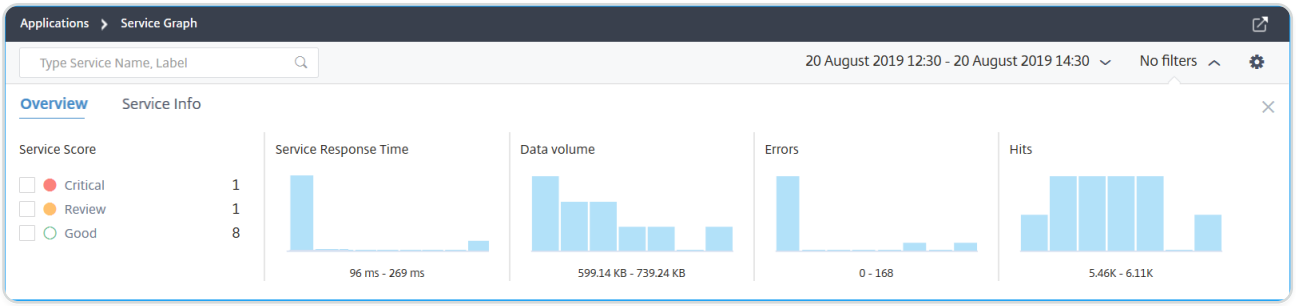
- **SSL Server Errors** – Indicates the total SSL errors from the server. (For example, SSL certificate unknown)
- **SSL Protocol** – Indicates the SSL protocol version used by the service

© 1997–2026 Citrix Systems, Inc. All rights reserved.

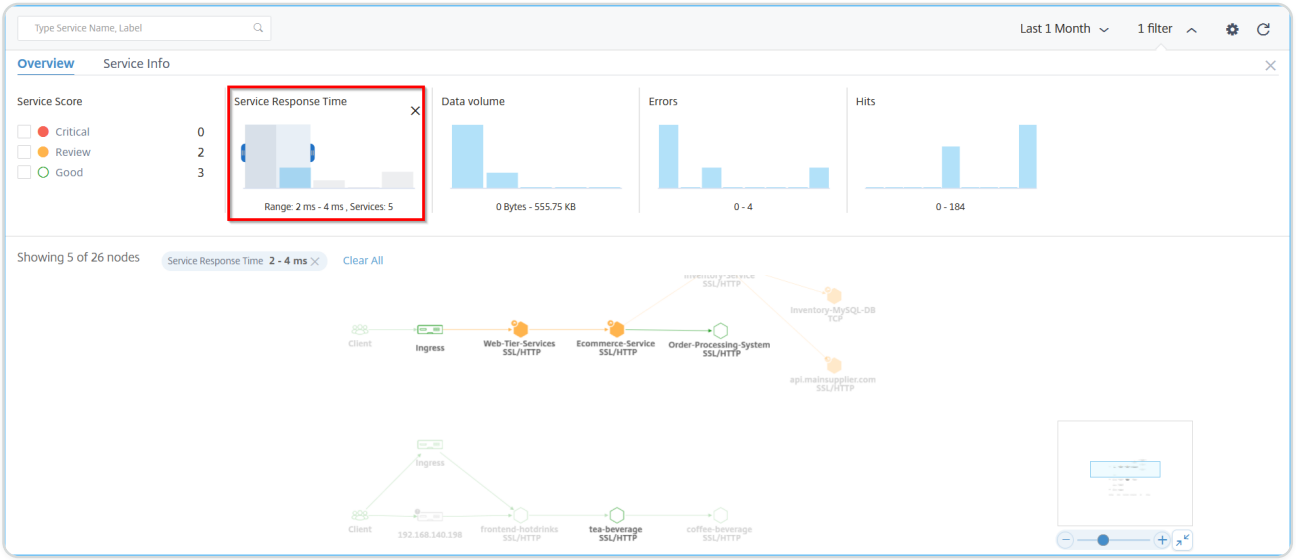
- **SSL Client Errors** - Indicate the total SSL errors from the client. (For example, SSL client authentication error)

Apply filters

You can apply filters to view specific service information. Click **No Filters** list to get the filter options.

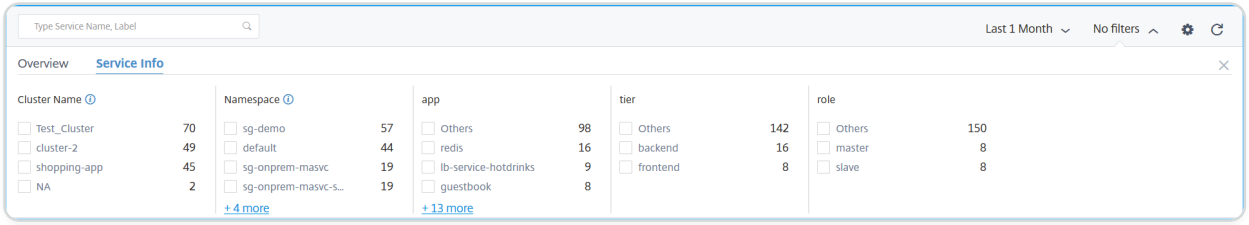


For example, if you want to view services that have latency less than 150 ms, then click the bar graph under **Service Response Time** to display the results.



Click **Service Info** to select and apply filters for:

- **Cluster** – Displays all services applicable for the selected cluster or clusters.
- **Namespace** – Displays all services applicable for the selected namespace.

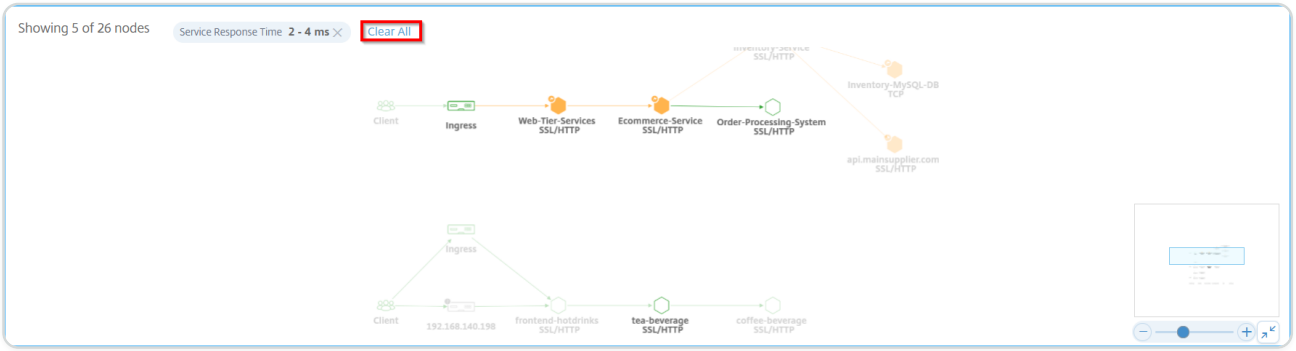


© 1997–2026 Citrix Systems, Inc. All rights reserved.

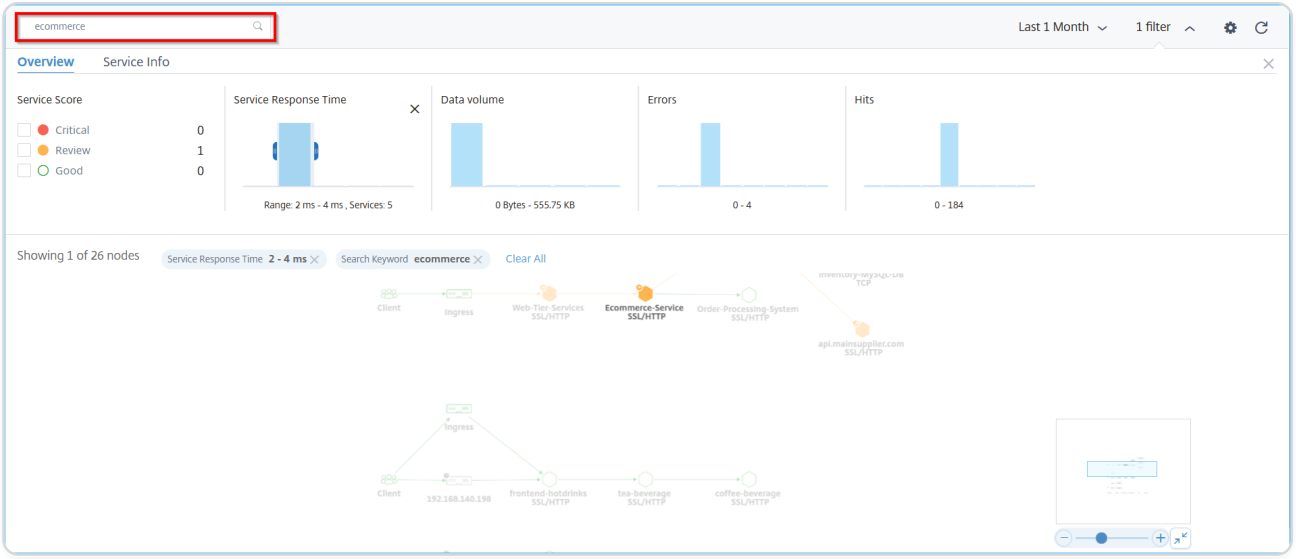
Note

Depending upon the labels configured for the service in Kubernetes service definition YAML, you may also view more filter options.

Click **Clear All** to clear all filters.

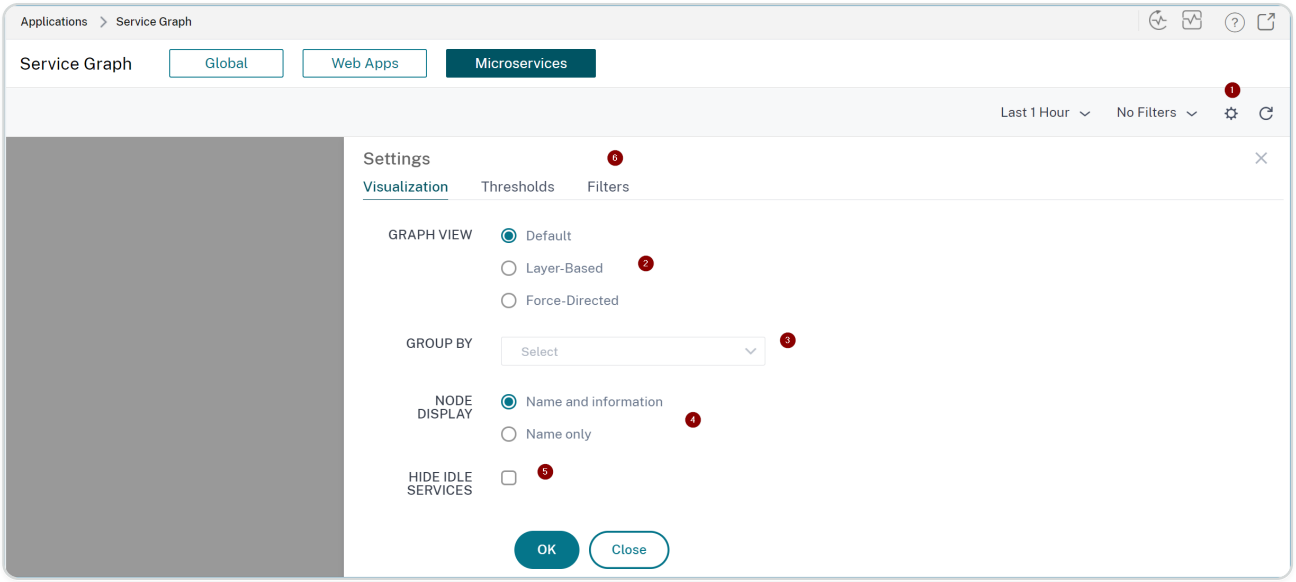


Alternatively, you can also use the search text box and type a service name to display the results on the service graph.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

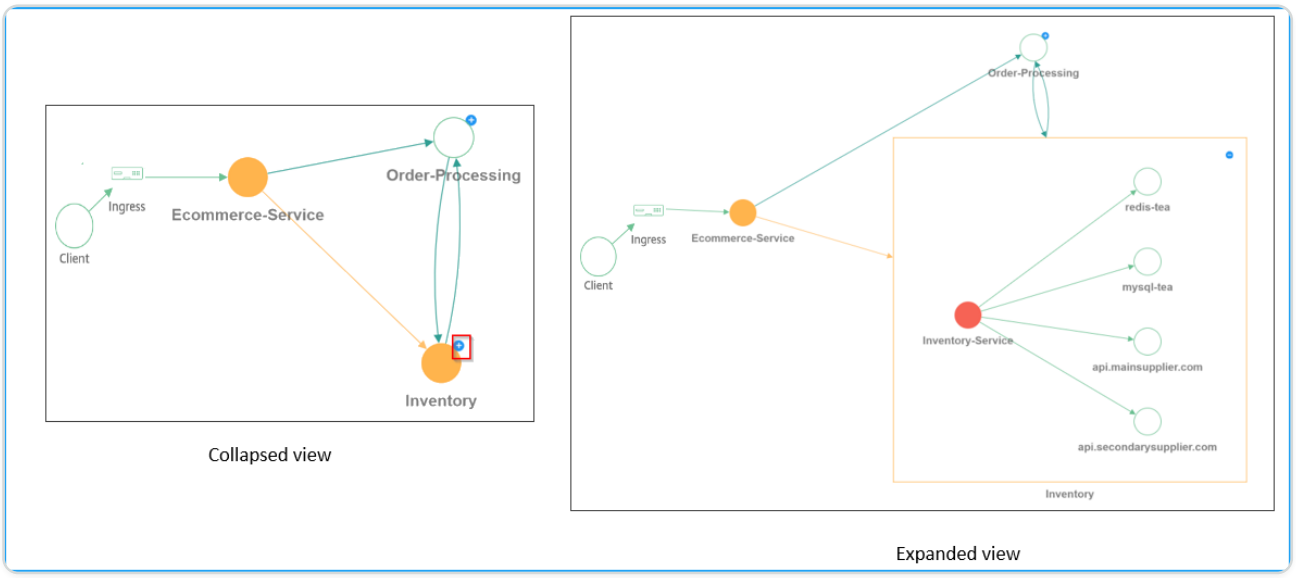
Settings option



1 – Settings icon

2 – Options to display the service graph as Default, Layer-Based, or Force-Directed views

3 – Select the options from the list to view the services based on categories. After you select a category from the list, click **+** on the graph to view all services

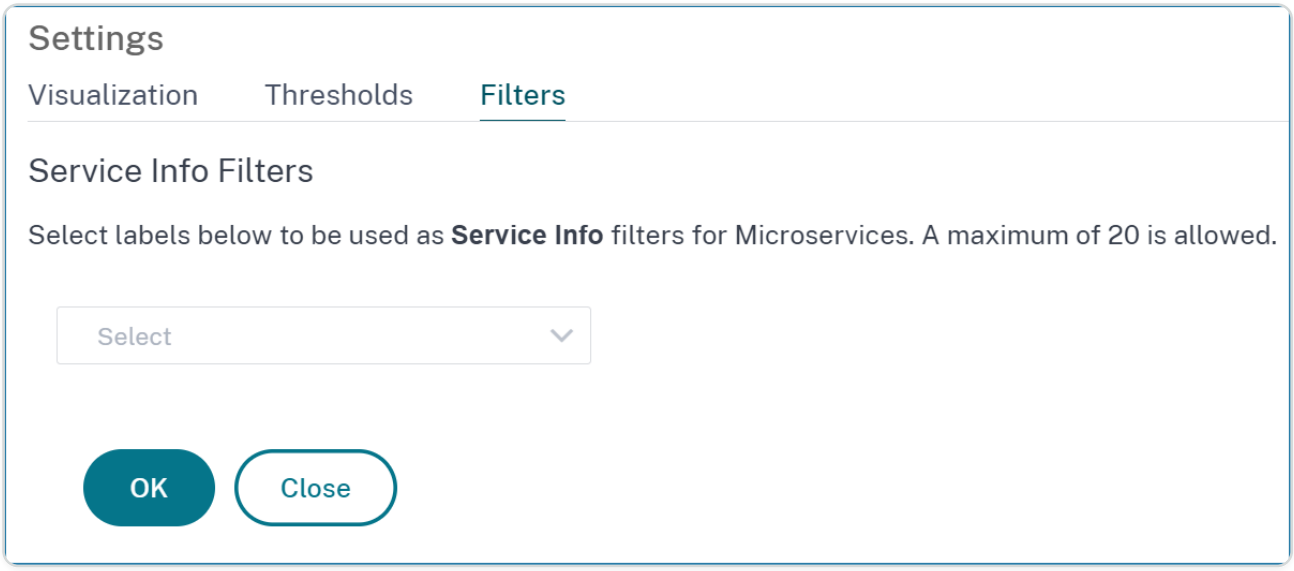


4 – Enables you select the option on how you want to display the services.

5 - Select the **Hide Idle Services** option to display only the active services.

6 - Enables you to change the **Service Info** labels. The **Filters** tab enables you to select the labels (based on the selected duration and the active transactions from the services).

© 1997–2026 Citrix Systems, Inc. All rights reserved.



After selecting the labels, the **Service Info** tab in the **Filters** section enables you to apply filters on the selected labels to filter results.

Analyze the errors

Hover the mouse pointer on a service that indicates errors.

ERROR	DESCRIPTION
	The **TCP Server Reset** indicates the total TCP resets initiated from the server.
	The **TCP Client Reset** indicates the total TCP resets initiated by the client.
	The SSL Client Errors indicate the total SSL errors from the client. (For example, SSL client authentication error).
	The SSL Server Errors Indicate the total SSL errors from the server. (For example, SSL certificate unknown)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

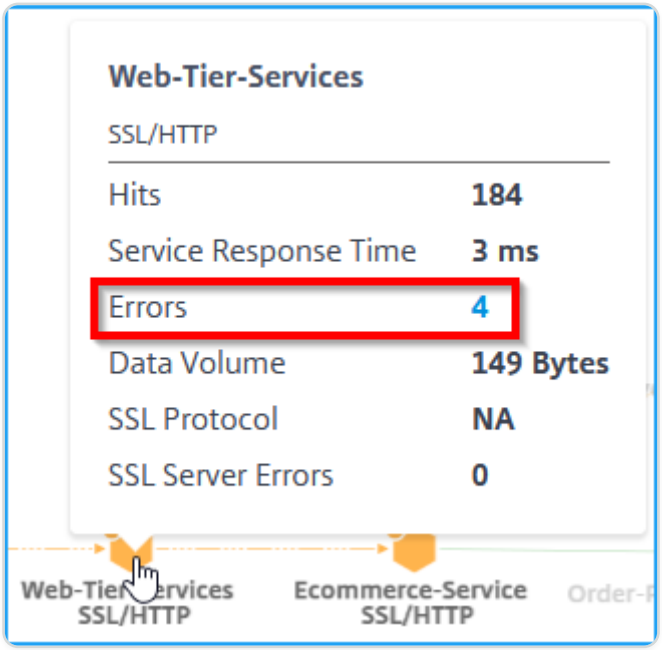
NOTE

- Client error count (irrespective of the protocol type) is displayed in any service if the client error count is **1 or higher**.
- Clients error count displayed for any service indicates that the errors are from the client end.

View HTTP transaction details

NOTE

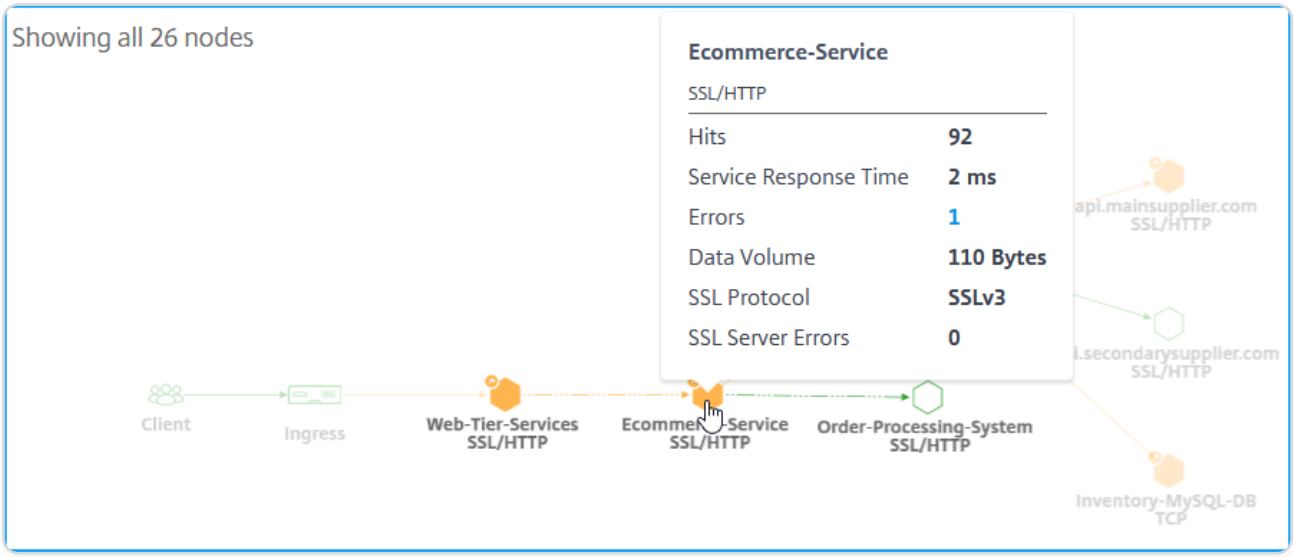
You can view the errors by hovering the mouse pointer on an erroneous service and click the issue count.



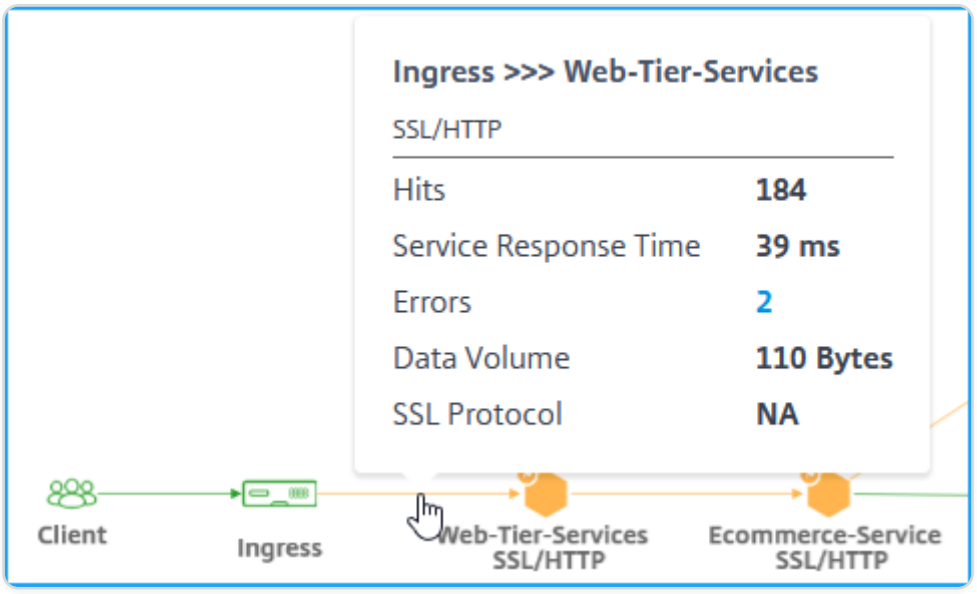
According to the example shown in the image, you can view an end-to-end network map of your application that shows how your component services are communicating.

When you hover the mouse pointer on the **Ecommerce-Service**, you can view metrics details for **Ecommerce-Service**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NetScaler Console also enables you to view transaction details between Ingress and services. Hover the mouse pointer to view details such as total errors, average service response time, and so on between the Ingress and service.



Hits – Indicates the total number of hits received by the service.

Service Response Time – Indicates the average response time taken from the service to respond for Time To First Byte (TTFB).

Errors – Indicates the total errors such as 4xx, 5xx, and so on.

Data volume – Indicates the total volume of data processed by the service.

SSL Protocol – Indicates the SSL protocol version.

Click the arrow between **Ingress** and **service** to view the detailed transactions.

For more information, see View analytics for Web transactions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure thresholds in service graph

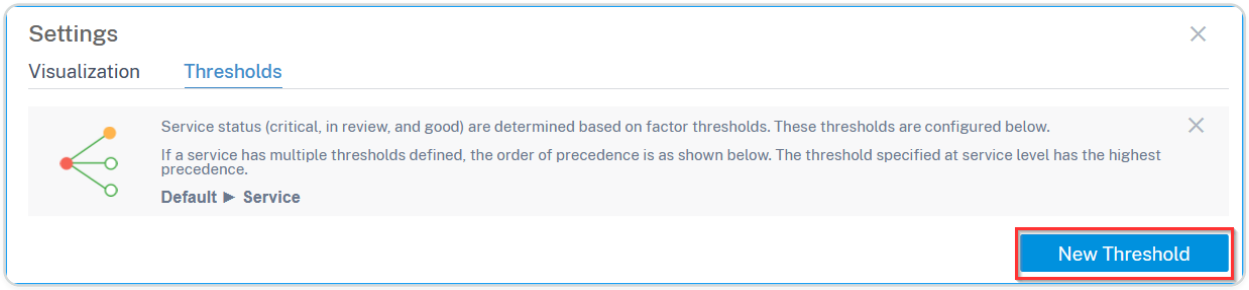
As an administrator, you can configure thresholds for Kubernetes services. NetScaler Console displays the service status (Critical, Review, and Good) based on the service response time and error count. By default, you can view the **Default Threshold** (service response time = 200 ms and error count = 0) applied to all services.

NOTE

You cannot delete the Default Threshold.

To configure a new threshold:

1. In **Applications > Service Graph**, click the **Microservices** tab:
2. Click the settings icon and select the **Thresholds** tab.
3. Click **New Threshold** to configure a new threshold.



The **New Threshold** page is displayed.

4. Configure the following parameters:

   a. **Name** – Specify a name for the threshold.

   b. Under **Microservices**, select the services that you want to apply the threshold.

   c. Under **Thresholds**, select **Single** or **Double** for:

      - High Response Time (Average, P99, P99.9)
      - High Errors
      - High Hits

   d. Specify the threshold values.

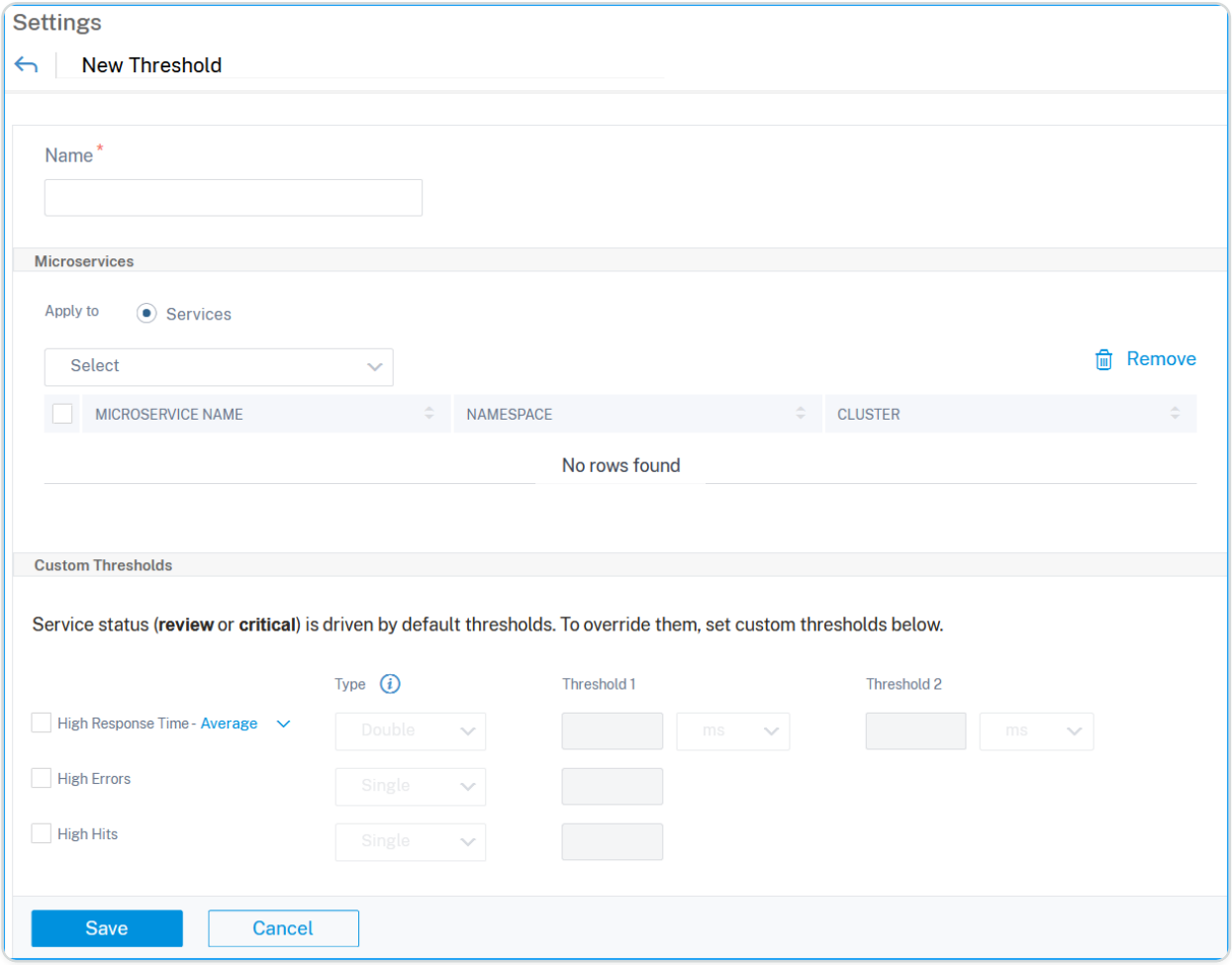
      NOTE

      If you select double threshold, ensure:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Threshold 1 value is lesser than Threshold 2 value. For example, if you configure Threshold 1 as 250 ms, Threshold 2 must be 251 ms or higher.
- Threshold 1 value must not be same as Threshold 2 value.

5. Click **Save**.



The threshold is successfully created. You can view the threshold details in the **Thresholds** page.

NOTE

NetScaler Console calculates the service final score and status based on the selected metrics. For example, if you select only **High Hits** for the threshold configuration, NetScaler Console uses the default threshold (response time = 200 ms and error count = 0) and high hits to calculate the service score and status.

Single threshold

When you configure single threshold for all metrics or selected metrics, NetScaler Console:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Compares the current values in each metric with the configured threshold values in each metric
- Calculates the total penalty based on the exceeded thresholds in each metric

  Note

  > If any metric has not breached the threshold value, the penalty is calculated accordingly

- Displays the service score and service status based on the penalty calculation

Double threshold

When you configure double threshold for all metrics or selected metrics, NetScaler Console:

- Compares the current values in each metric with the configured threshold values in each metric
- Checks if the current values are:
  - Lesser than threshold 1
  - Between threshold 1 and threshold 2
  - Greater than threshold 2
- Calculates the total penalty based on the exceeded thresholds in each metric

  Note

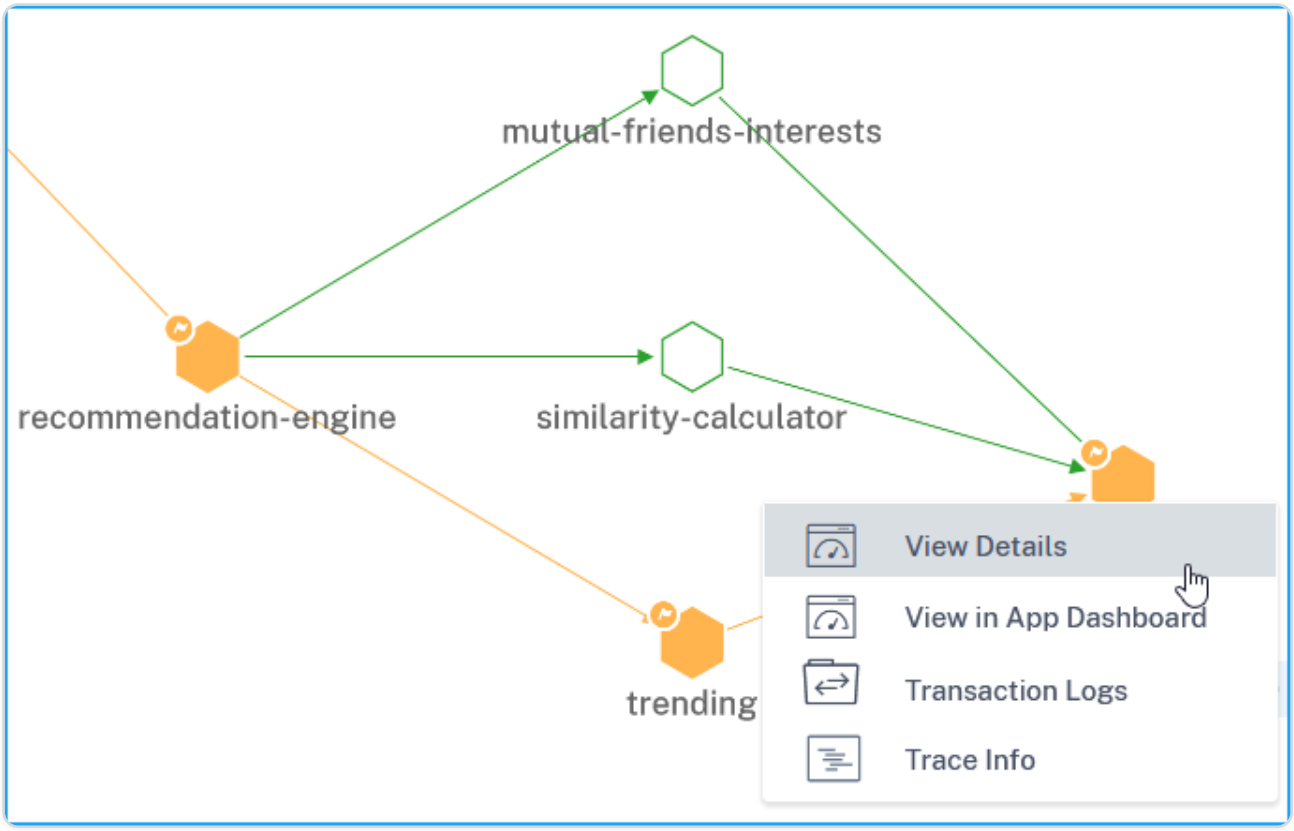
  > If any metric has not breached the threshold value, the penalty is calculated accordingly

- Displays the service score and service status based on the penalty calculation

View service details

Click a service and select **View Details**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

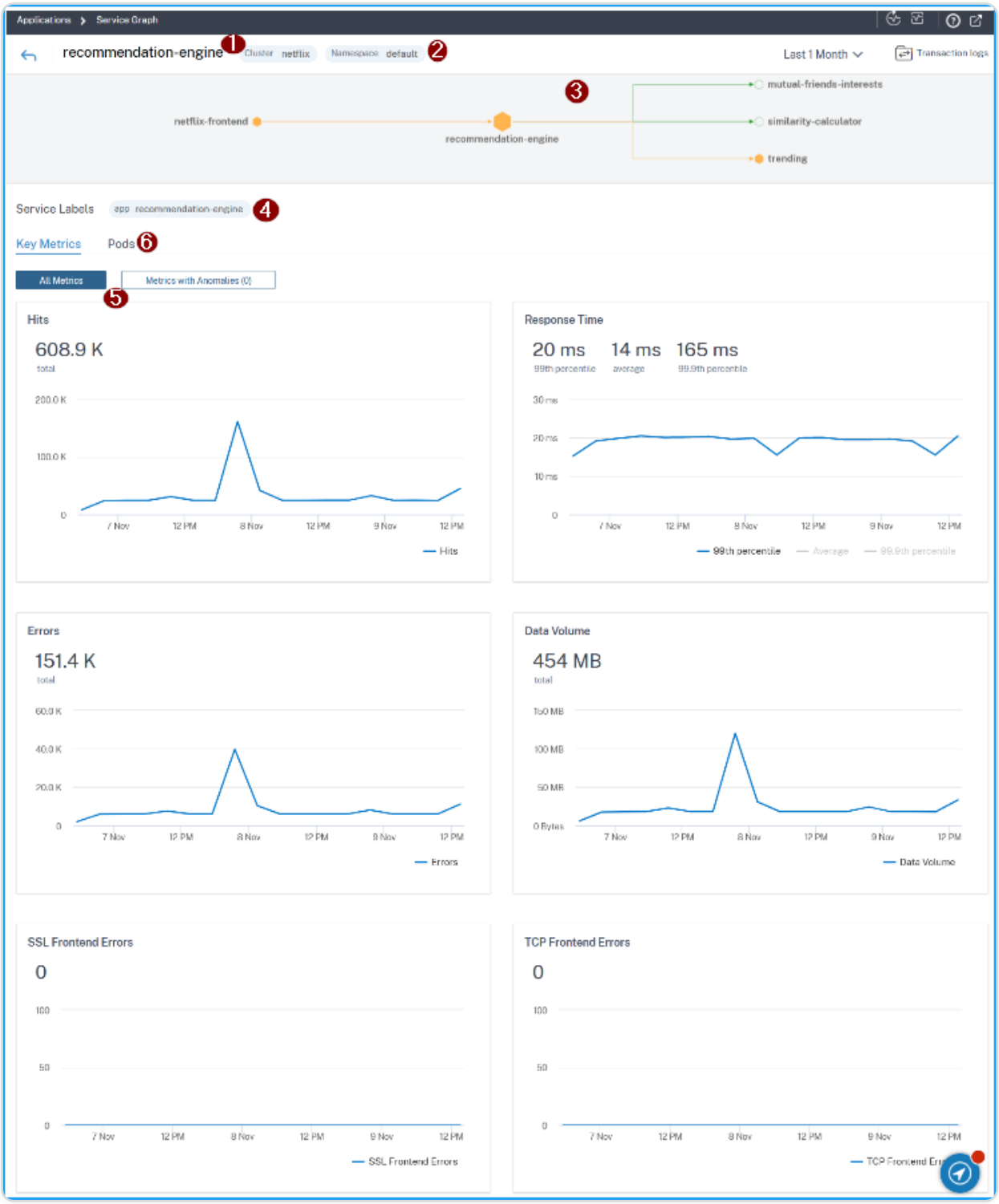


The service details page enables you to view:

- The cluster name where the service is hosted (1)
- The namespace and service labels of the service (2) (4)
- All associated incoming and outgoing services connected with the selected service (3)
- Service key metrics in a graph format such as Hits, Response time, Errors, Data volume, SSL frontend errors, and TCP frontend errors. The **Metrics with Anomalies** tab enables you to view the anomalies for a specific duration (5).

  For more information, see Monitor services using the golden signal metrics.
- The backend pods associated with the service (6).

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Using these key metrics trends, you can analyze how the service is performing for a specific time duration.

For example, consider that a service indicates Service Response Time > 700 ms for all requests. As an administrator, you can:

- Analyze the Service Response Time metric trend for a specific duration
- Troubleshoot the issue

© 1997–2026 Citrix Systems, Inc. All rights reserved.

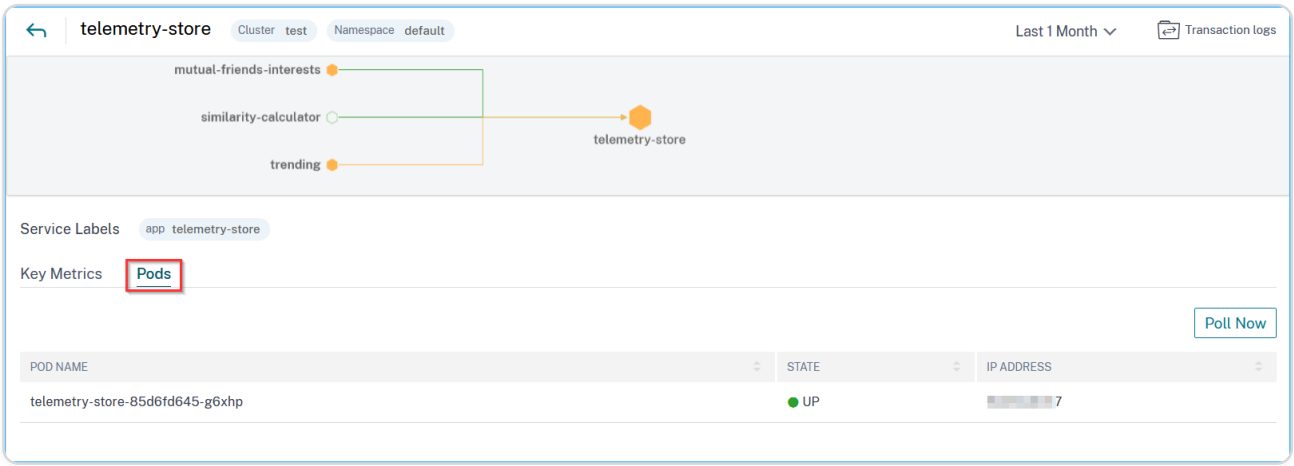
- Check the Service Response Time metric again to analyze if the response time has improved

Metrics details

METRICS	DESCRIPTION
Hits	The total number of requests received by the service
Errors	The total HTTP errors from the service
Service Response Time	The average response time taken from the service to respond for Time To First Byte (TTFB).
Data Volume	The total data volume processed by the service
SSL front-end errors	The total SSL front-end errors from the service. For example: SSL CLIENTAUTH FAILURE
SSL back-end errors	The total SSL back-end errors from the service. For example: SSL Client Errors
TCP back-end errors	The total TCP back-end errors from the service. For example: TCP Server Reset
TCP front-end errors	The total TCP front-end errors from the service. For example: TCP Client Reset

View backend pod details

Click the **Pods** tab to view the backend pods associated with the service.

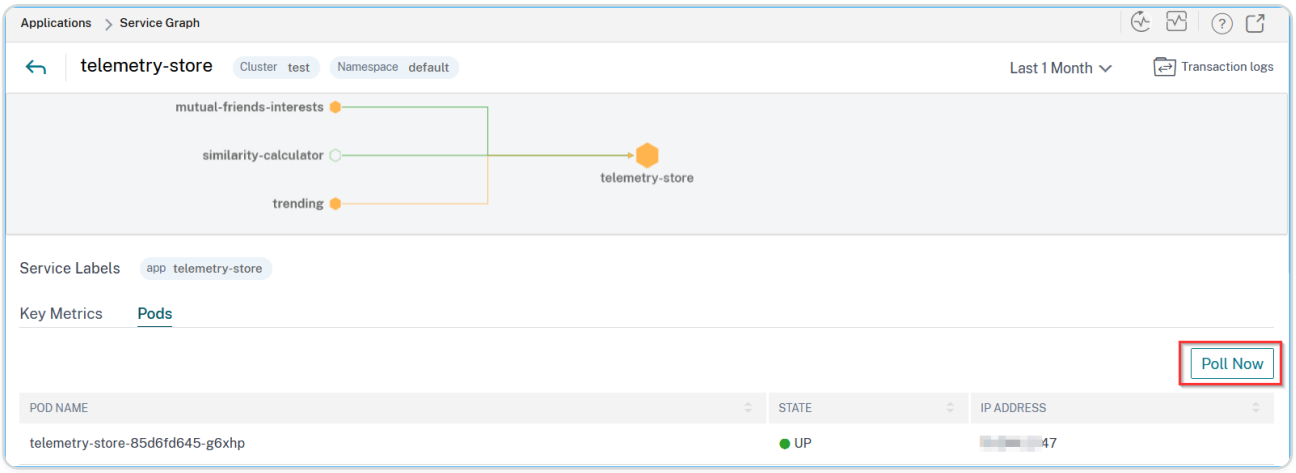


© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Pod name** – Denotes the pod name
- **Status** – Denotes if the pod is running (UP) or not (DOWN).
- **IP address** – Denotes the pod IP address

Use the Poll Now option to get the pod status

The **Poll Now** option fetches the latest pod status from the cluster.



Monitor services using the golden signal metrics

The golden signal metrics in services running in Kubernetes cluster refer to a set of metrics that enable you to detect potential anomalies for a specific duration. When you have 100 s of microservices in the Kubernetes cluster, identifying a service that has frequent issues might be difficult. The following three key metrics are the golden signal metrics that NetScaler Console graph can help you identify potential anomalies for a Kubernetes service:

- Hits
- Response Time (Avg) and Response Time (P99)
- Errors

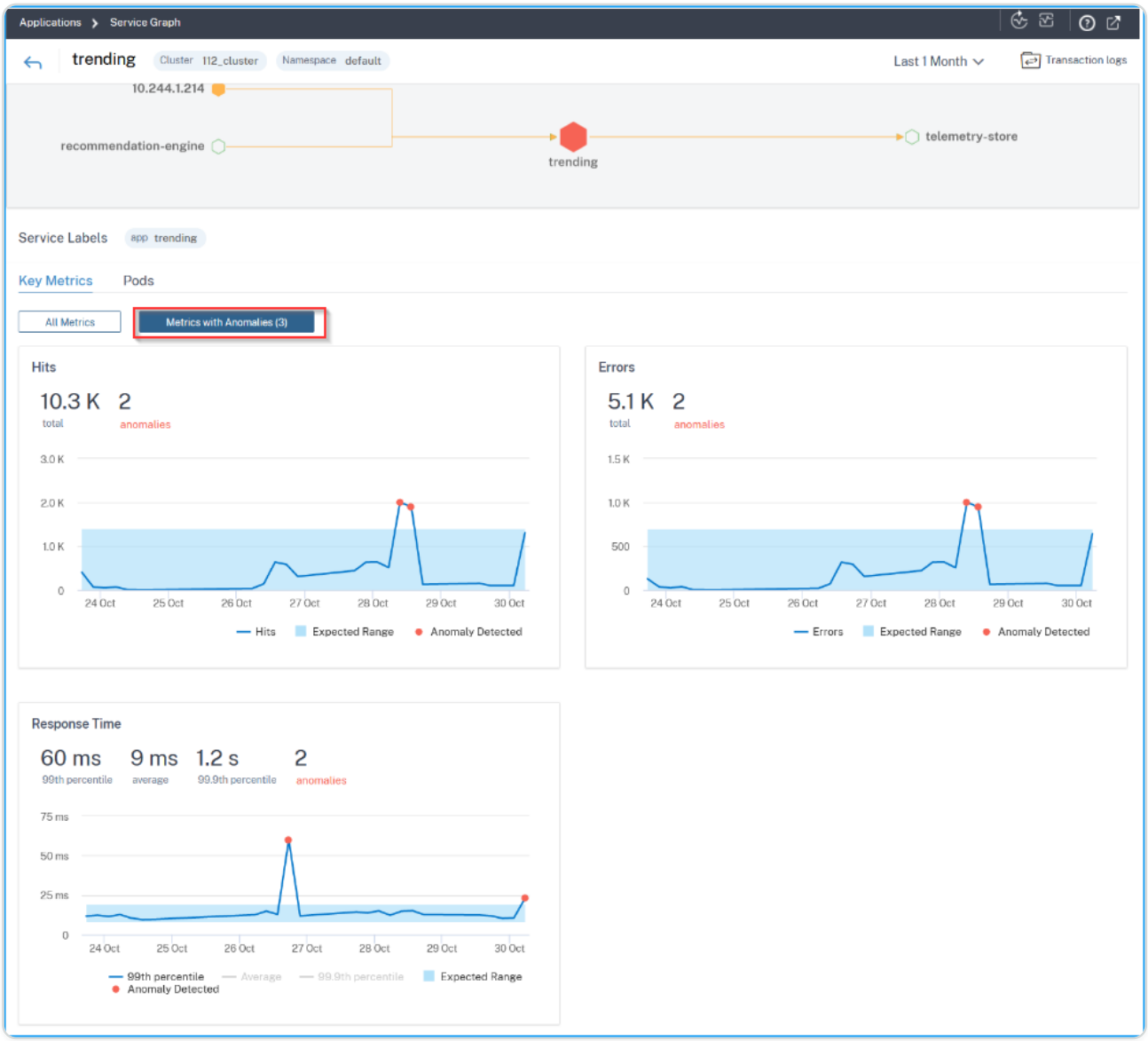
As an administrator, using these metrics, you can:

- Identify the service status
  - **Critical** – Service has anomalies or threshold breach in multiple metrics
  - **Review** – Service has anomalies or threshold breach in any one of the metrics
  - **Good** – Service with no anomalies or no threshold breach
- Analyze how many anomalies are identified in each metric
- Troubleshoot the issue and avoid any major impact

© 1997–2026 Citrix Systems, Inc. All rights reserved.

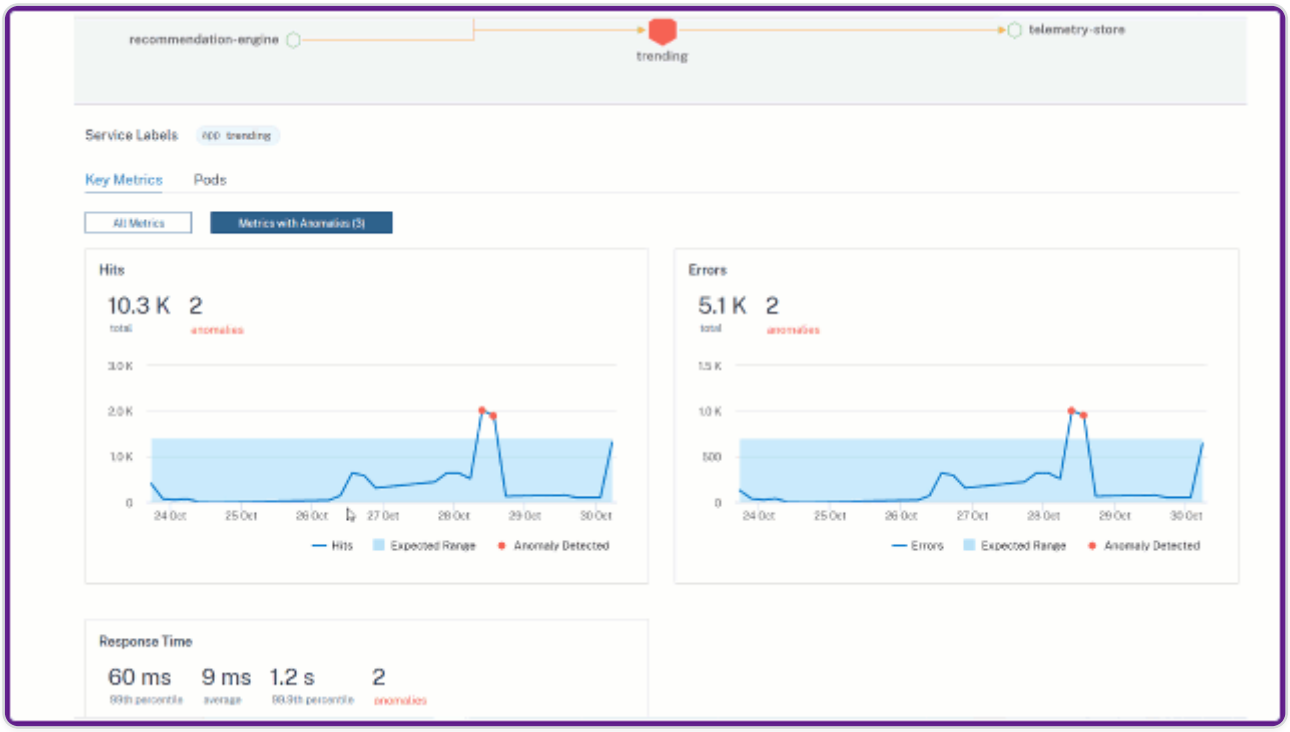
Identify anomalies

When you click a service and select **View Details**, the service details page displays the overview of all metrics. Click **Metrics with Anomalies** tab to view the anomaly details.



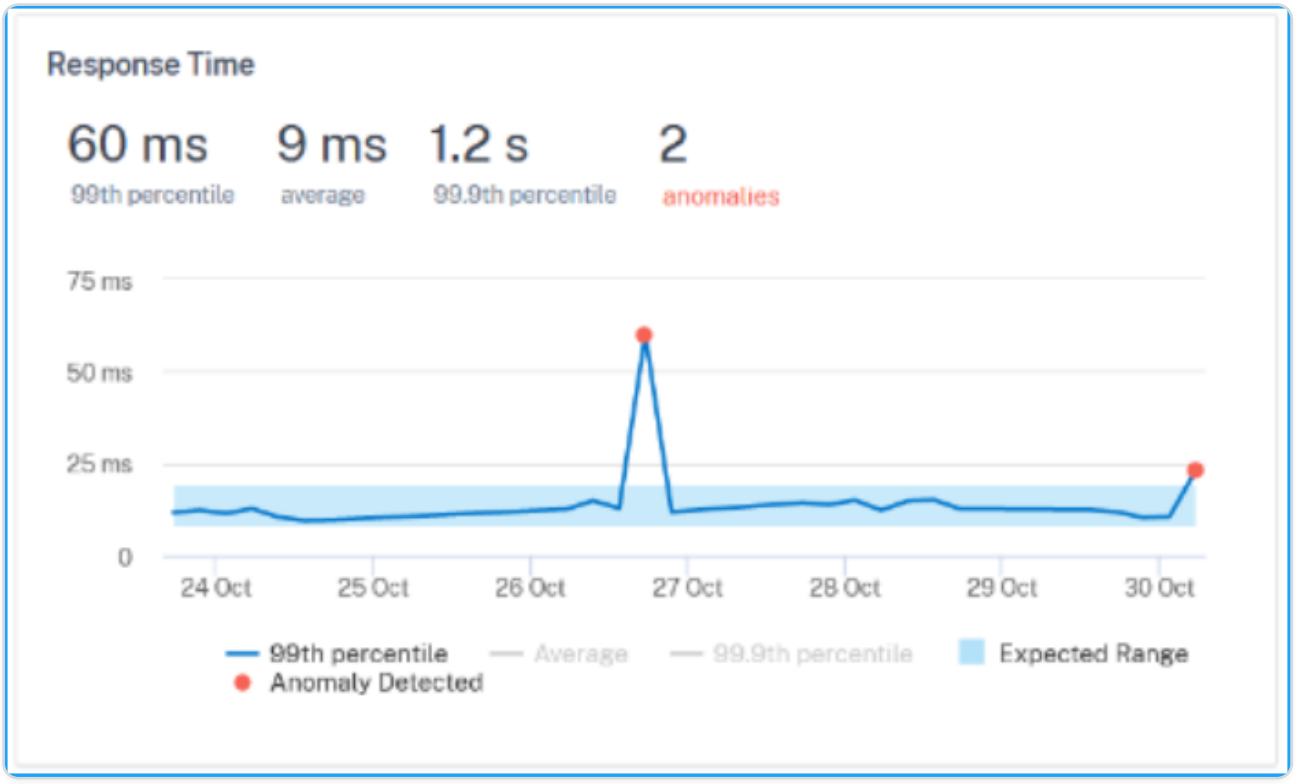
For each metric, the graph enables you to view the anomalies detected whenever the expected range exceeds. You can click the options to filter the views in the graph.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Consider that you want to analyze the anomalies for the service Response Time (P99).

Under **Response Time**, you can view the following details for the selected time duration:



- **99th percentile** – Indicates that the 99% of the requests for the selected duration is less than 60 ms
- **Average** – Indicates the average response time from the service
- **99.9th percentile** – Indicates the highest response time from the service

© 1997–2026 Citrix Systems, Inc. All rights reserved.

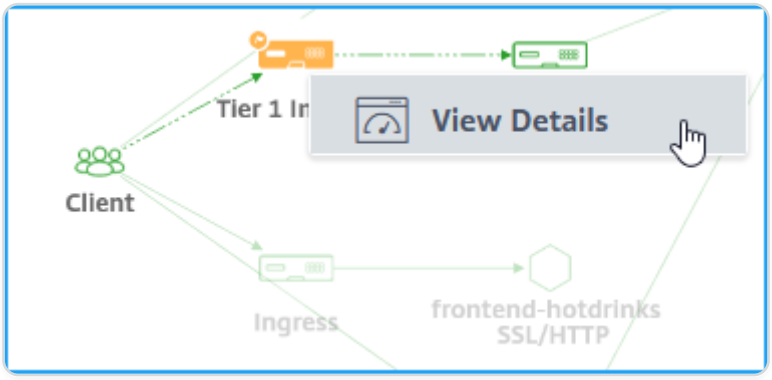
- **Anomalies** – Indicates the total anomalies detected

The graph also enables you to view the expected range for the selected time duration. According to the example, you can view:

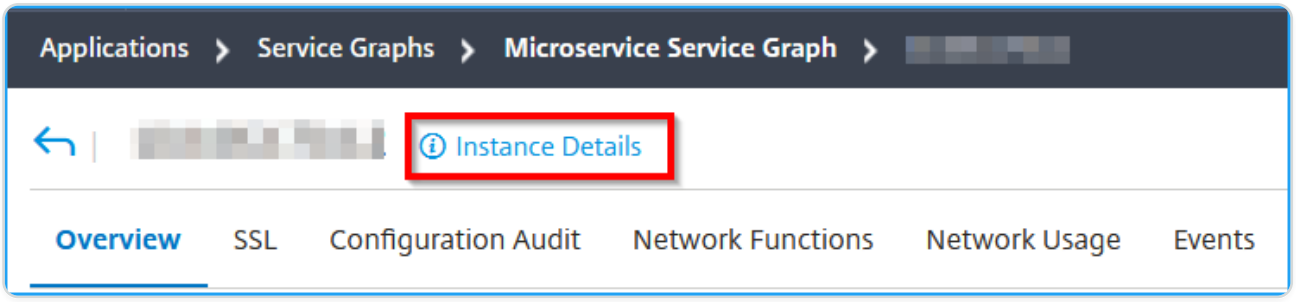
- The response time expected range is between 1 ms and 9 ms.
- Two anomalies detected for the service (one for 60 ms and another for 25 ms), because the service response time has exceeded more than the expected range (between 1 ms and 9 ms).

View ingress details for troubleshooting issues

In service graph, click the ingress and select **View Details** to visualize the details of NetScaler instance that is configured for the Kubernetes cluster.



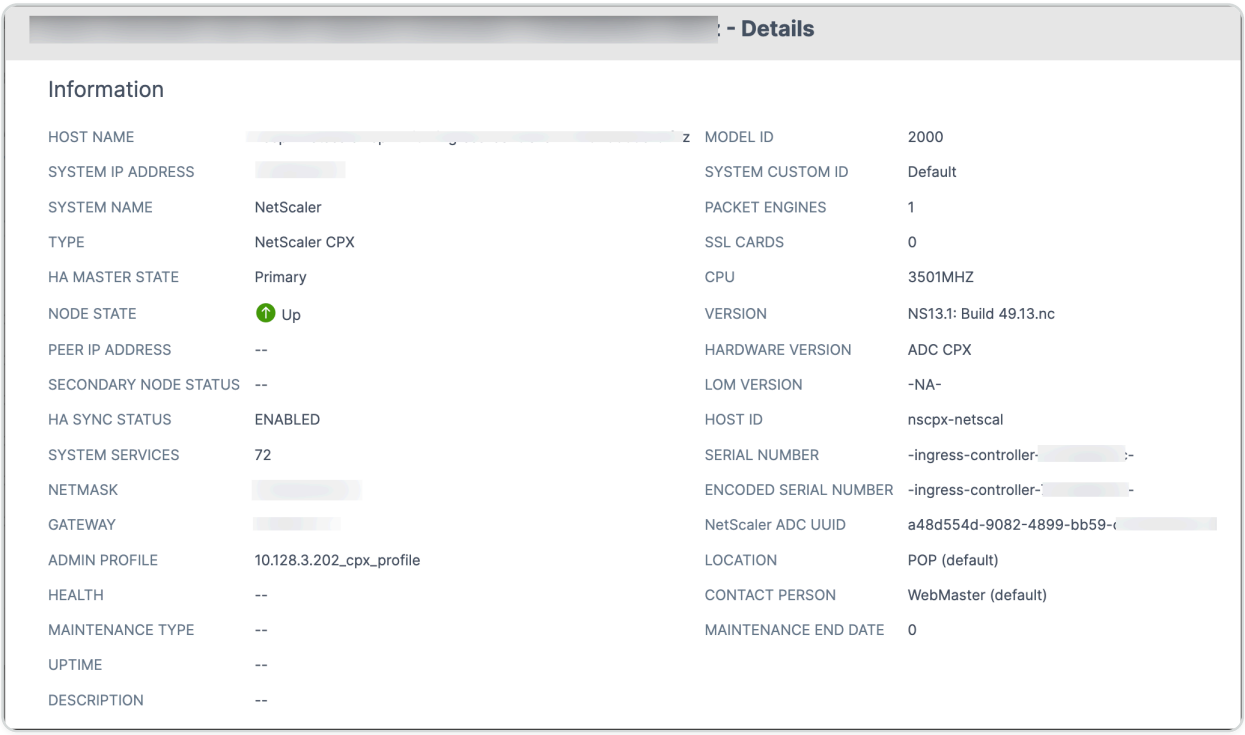
Click **Instance Details** to view the details.



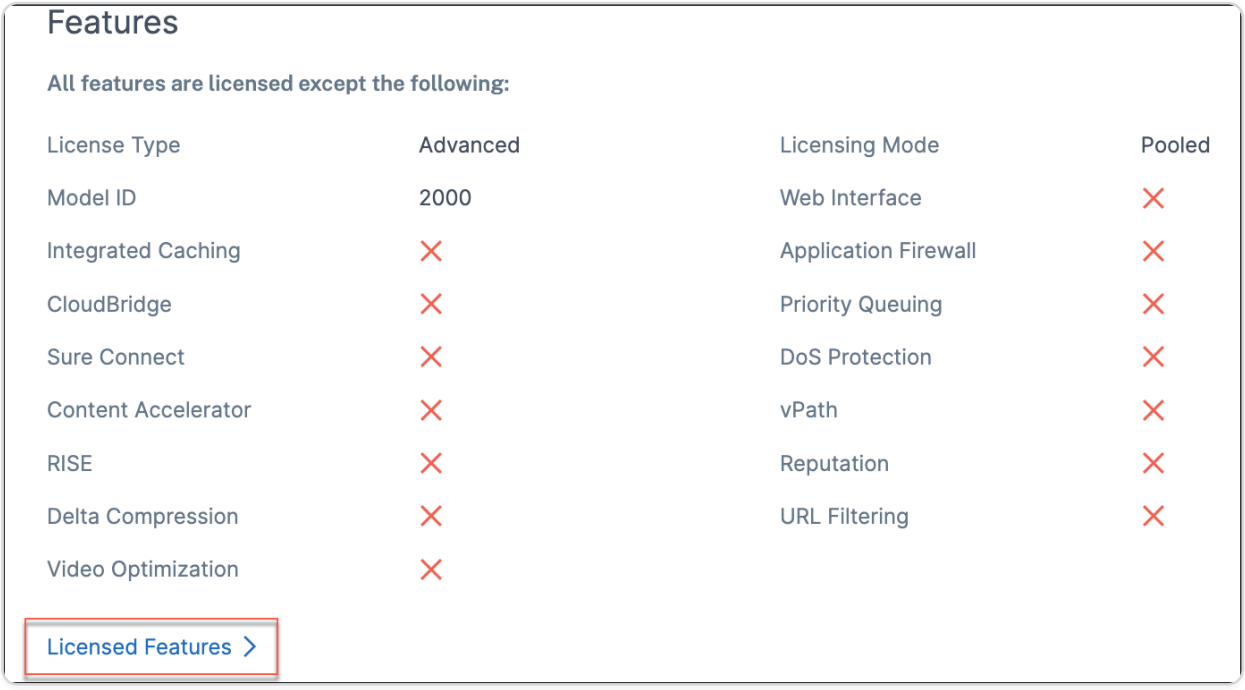
The following details are displayed:

- **Information** - Instance details such as instance type, deployment type, version, model, and so on.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Features** – By default, the features that are not licensed are displayed. Click **Licensed Features** to view the features that are licensed.



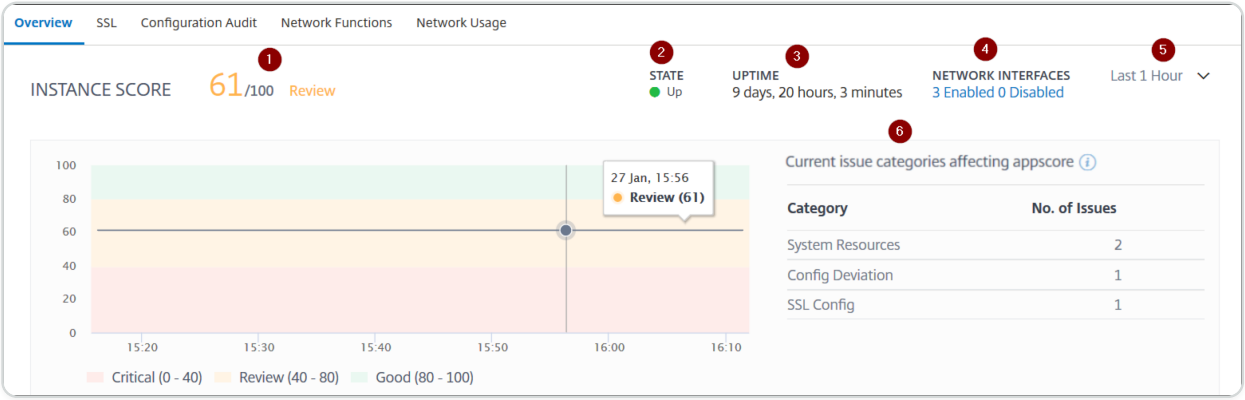
- **Modes** – By default, all modes that are disabled on the instance are displayed. Click **View Enabled Modes** to view the enabled modes on the instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The instance dashboard presents an instance overview where you can see the following details:

- **Instance score**



1 – Indicates the current NetScaler instance score for the selected time duration. The final score is calculated as **100 minus total penalties**. The graph displays the score ranges for the selected time duration.

2 – Indicates the current status of the NetScaler instance, such as **Up**, **Down**, and **Out of Service**.

3 – Indicates the duration that the NetScaler instance is up and running.

4 – Indicates the total network interfaces enabled and disabled for the instance. Click to view the details such as network interface name and the status (enabled or disabled).

5 – Select the time duration from the list to view the instance details.

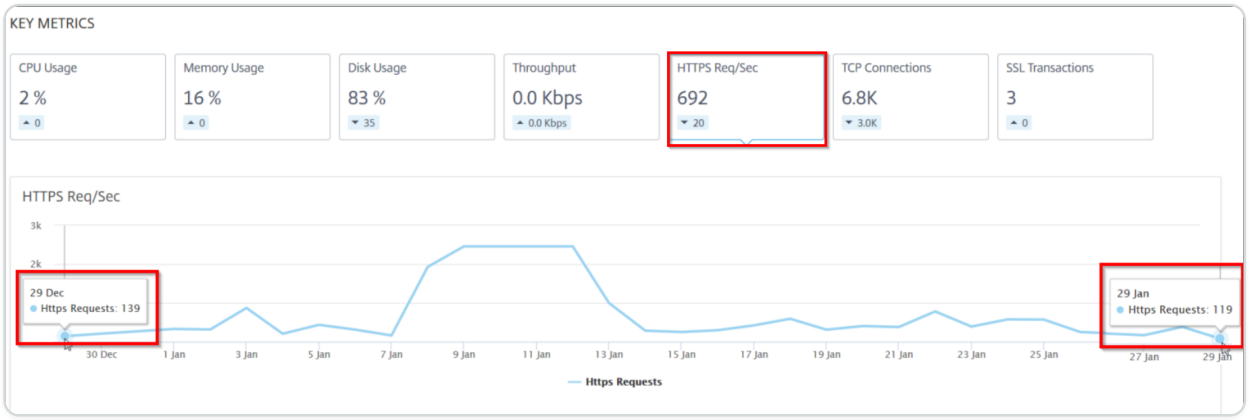
6 – Displays the total issues and issue category of the NetScaler instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Key Metrics**

  Click each tab to view the details. In each metric, you can view the average value and the difference value for the selected time.

  The following image is an example for HTTPS Req/Sec and the selected time duration is for last 1 month. The value **692** is the average HTTPS Req/Sec for the last 1-month duration and the value **20** is the difference value. In the graph, the first value is **139** and the last value is **119**. The difference value is **139 – 119 = 20**.



  You can view the following instance metrics in a graph format for the selected time duration:

  - **CPU Usage** – The average CPU % from the instance for the selected duration (displays for both packet CPU and for management CPU).
  - **Memory Usage** – The average memory usage % from the instance for the selected duration.
  - **Disk Usage** – The average disk space % from the instance for the selected duration.
  - **Throughput** – The average network throughput processed by the instance for the selected duration.
  - **HTTPS request/sec** – The average HTTPs requests received by the instance for the selected duration.
  - **TCP connections** – The average TCP connections established by the client and server for the selected duration.
  - **SSL transactions** – The average SSL transactions processed by the instance for the selected duration.

- **Issues**

  You can view the following issues that occur in NetScaler instance:

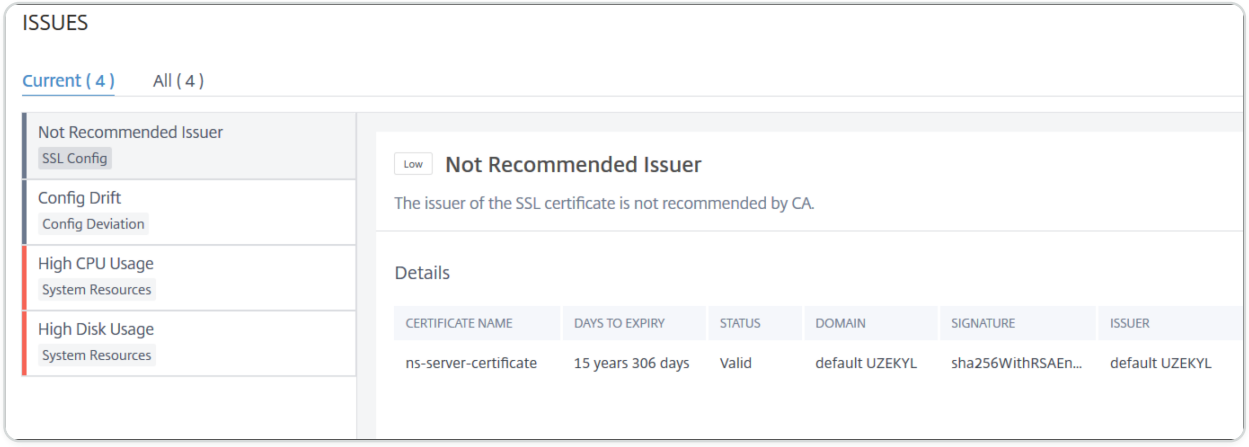
© 1997–2026 Citrix Systems, Inc. All rights reserved.

ISSUE CATEGORY	DESCRIPTION	ISSUES
System Resources	Displays all issues related to the NetScaler system resource such as CPU, Memory, disk usage, and so on.	- High CPU Usage
		- High Memory Usage
		- High Disk Usage
		- SSL Card Failures
		- Power Failure
		- Disk Error
		- Flash Error
		- NIC Discards
SSL Config	Displays all issues related to the SSL configuration on the NetScaler instance.	- SSL Certs Expired
		- Not Recommended Issuer
		- Not Recommended Algo
		- Not Recommended Key Strength
Config Deviation	Displays all issues related to the configuration jobs applied in NetScaler instance.	- Config Drift
		- Running vs Template
Capacity issues	Displays NetScaler capacity issues. The NetScaler Console polls these events every five minutes from the	- Throughput Limit Reached

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ISSUE CATEGORY	DESCRIPTION	ISSUES
	NetScaler instance and displays the packet drops or rate-limit counter increments if exists. The issues are categorized on the following capacity parameters.	
		- PE CPU Limit Reached
		- PPS Limit Reached
		- SSL Throughput Rate Limit
		- SSL TPS Rate Limit
Networking	Displays the operational issues that occur in the instances.	For more information, see Enhanced Infrastructure Analytics with new indicators.

Click each tab to analyze and troubleshoot the issue. For example, consider that an instance has the following errors for the selected time duration:



- The **Current** tab displays the current NetScaler operational issues that are affecting the instance score.
- The **All** tab displays all infra issues detected for the selected duration.

Distributed tracing

In service graph, you can use the distributed tracing view to:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Analyze the overall service performance.
- Visualize the communication flow between the selected service and its inter-dependent services.
- Identify which service indicates errors and troubleshoot the erroneous service.
- View transaction details between the selected service and its each inter-dependent service.

Prerequisites

To view the trace information for the service, you must:

- Ensure that an application maintains the following trace headers, while sending any east-west traffic:

  - `x-request-id`
  - `x-b3-traceid`
  - `x-b3-spanid`
  - `x-b3-parentspanid`
  - `x-b3-sampled`
  - `x-b3-flags`
  - `x-ot-span-context`

- For **CIC builds earlier than 1.7.23**, update the CPX YAML file with `NS_DISTRIBUTED_TRACING` and value as `yes`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
# Add cic as a sidecar
- name: cic
  image: "quay.io/citrix/citrix-k8s-ingress-controller:1.5.6"
  env:
  - name: "EULA"
    value: "yes"
  - name: "NS_IP"
    value: "127.0.0.1"
  - name: "NS_PROTOCOL"
    value: "HTTP"
  - name: "NS_PORT"
    value: "80"
  - name: "NS_DEPLOYMENT_MODE"
    value: "SIDECAR"
  - name: "NS_ENABLE_MONITORING"
    value: "YES"
  - name: "NS_DISTRIBUTED_TRACING"
    value: "yes"
  - name: "NS_LOGPROXY"
    value: "coe-tracing.default.svc.cluster.local"
  - name: POD_NAME
    valueFrom:
      fieldRef:
        apiVersion: v1
        fieldPath: metadata.name
  - name: POD_NAMESPACE
    valueFrom:
      fieldRef:
        apiVersion: v1
        fieldPath: metadata.namespace
  args:
    - --ingress-classes
      watches-ingress
  imagePullPolicy: Always
```

- For **CIC builds later than 1.7.23**, you must use a ConfigMap.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ConfigMaps allow you to separate your configurations from your pods and make your workloads portable. Using ConfigMaps, you can easily change and manage your workload configurations and reduce the need to hardcode configuration data to pod specifications.

With ConfigMap support, you can update the configuration automatically while keeping the NetScaler Ingress Controller pod running. You do not need to restart the pod after the update. For more information, see ConfigMap support for the ingress controller.

Using the ConfigMap, you can enable or disable distributed tracing, events, audit logs, and so on. To use the ConfigMap:

a. Create a YAML file using the required parameters.

   The following example YAML file has the distributed tracing enabled and other variables such as audit logs, events, and transactions disabled:

```
apiVersion: v1

kind: ConfigMap

metadata:

  name: cic-configmap

  namespace: default

data:

  LOGLEVEL: 'debug'

  NS_PROTOCOL: 'http'

  NS_PORT: '80'

  NS_HTTP2_SERVER_SIDE: 'ON'

  NS_ANALYTICS_CONFIG: |

    distributed_tracing:

      enable: 'true'

      samplingrate: 100
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    endpoint:
      server: <AgentIP> / <AppserverIP>
    timeseries:
      port: 5563
      metrics:
        enable: 'true'
        mode: 'avro'
      auditlogs:
        enable: 'false'
      events:
        enable: 'false'
    transactions:
      enable: 'false'
      port: 5557
```

Note

You can provide the values for `Samplingrate` between 0 and 100. NetScaler Console displays the mentioned number of trace transactions.

b. Deploy the ConfigMap by using:

`kubectl create -f <configmap-yaml>.yaml`

c. Edit the CPX YAML file and use either `envFrom` or `args` to specify the following arguments:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
envFrom:

 - configMapRef:

     name: cic-configmap
```

OR

```
 args:
    - --configmap
      default/cic-configmap
```

The ConfigMap YAML configuration is deployed in CIC.

d. If you want to change the value for any variable, edit the values in the ConfigMap. In this example, all other variables are changed from `false` to `true`.

```
apiVersion: v1

kind: ConfigMap

metadata:

  name: cic-configmap

  namespace: default

data:

  LOGLEVEL: 'debug'

  NS_PROTOCOL: 'http'

  NS_PORT: '80'

  NS_HTTP2_SERVER_SIDE: 'ON'

  NS_ANALYTICS_CONFIG: |

    distributed_tracing:

      enable: 'true'
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    samplingrate: 100
  endpoint:
    server: <AgentIP> / <AppserverIP>
  timeseries:
    port: 5563
    metrics:
      enable: 'true'
      mode: 'avro'
    auditlogs:
      enable: 'true'
    events:
      enable: 'true'
  transactions:
    enable: 'true'
    port: 5557
```

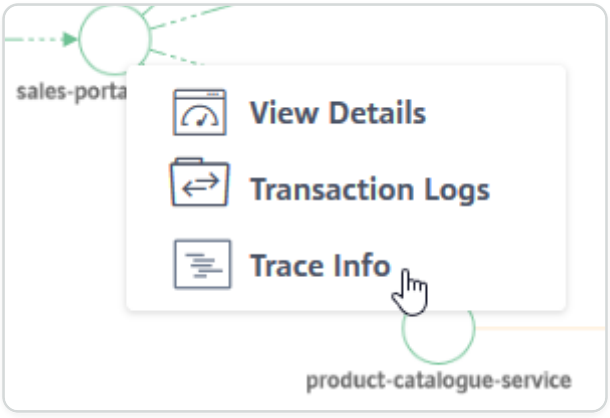
e. Reapply the ConfigMap using the following command:

`kubectl apply -f <yaml-file>.yaml`

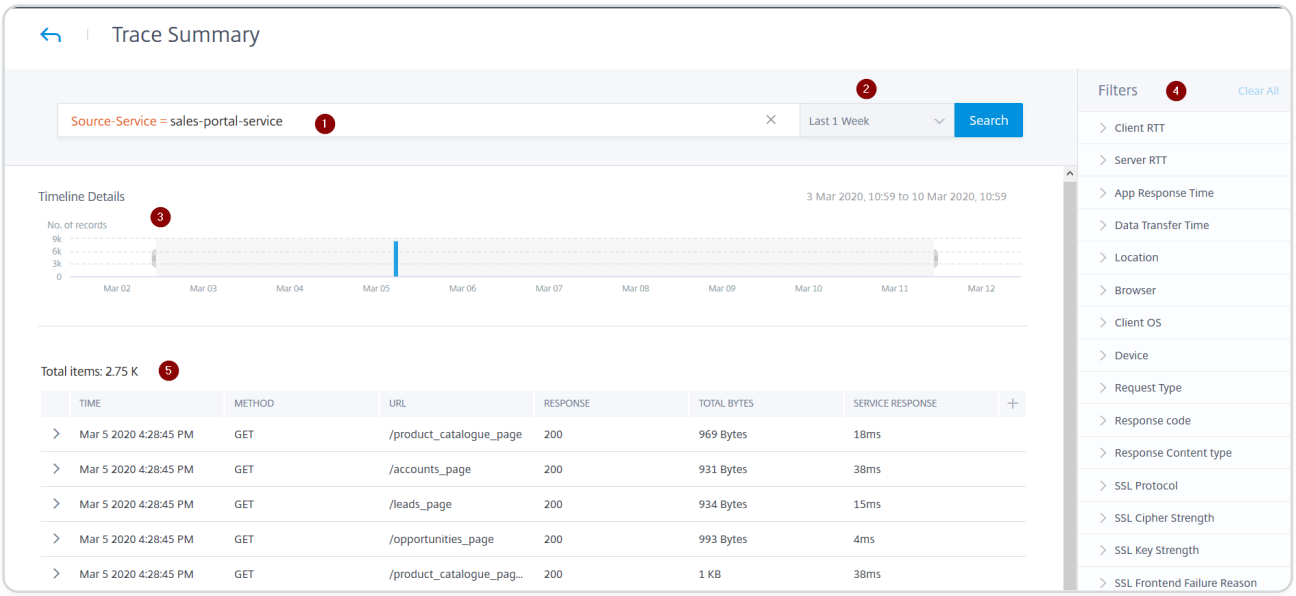
View service trace details

In service graph, click a service, and select **Trace Info**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The Trace Summary page is displayed for the selected service.



The **Trace Summary** displays:

- An advanced search that enables you to search through for transactions with suggestions and operators (1). For more information, see Advanced Search.
- The time duration list that enables you to select the time duration such as 1-hour, 12-hour, 1-day, 1-week, 1-month, and custom time (2).
- The Timeline Details graph that enables you to drag and select to display results for a specific time duration (3).
- The Filters panel that enables you to select options from each metric (4).
- The transaction details for the selected service (5).

View the transaction details

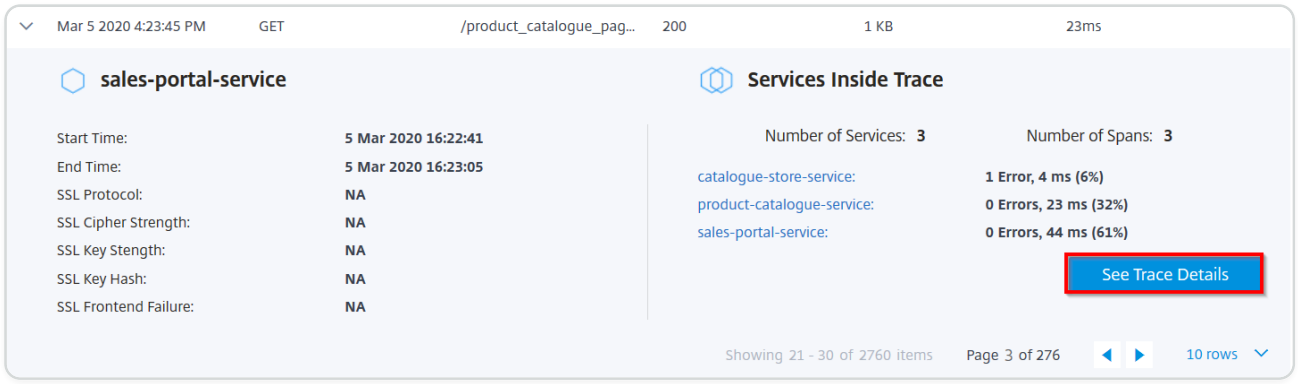
Click a transaction to drill down for detailed information. You can view transaction details for the selected service such as:

- Start time

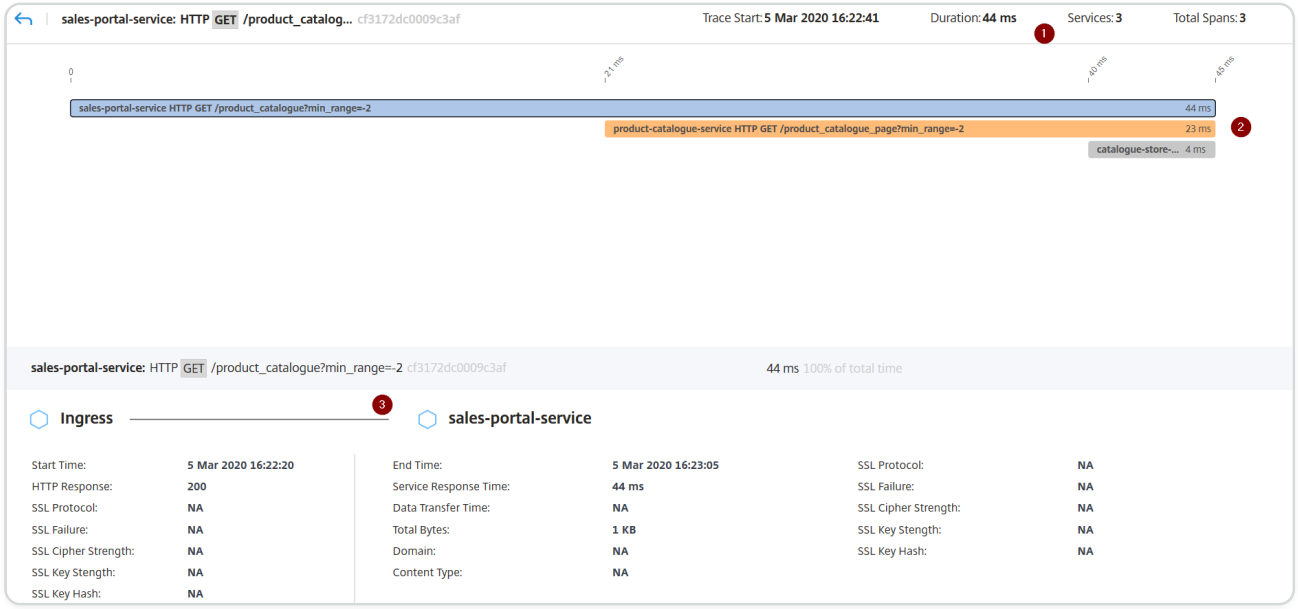
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- End time
- SSL metrics
- Communication with inter-dependent services (along with errors and response time with each service).

The following example indicates an error from `catalogue-store-service`. Click **See Trace Details** for further details.



The Trace Details page is displayed.



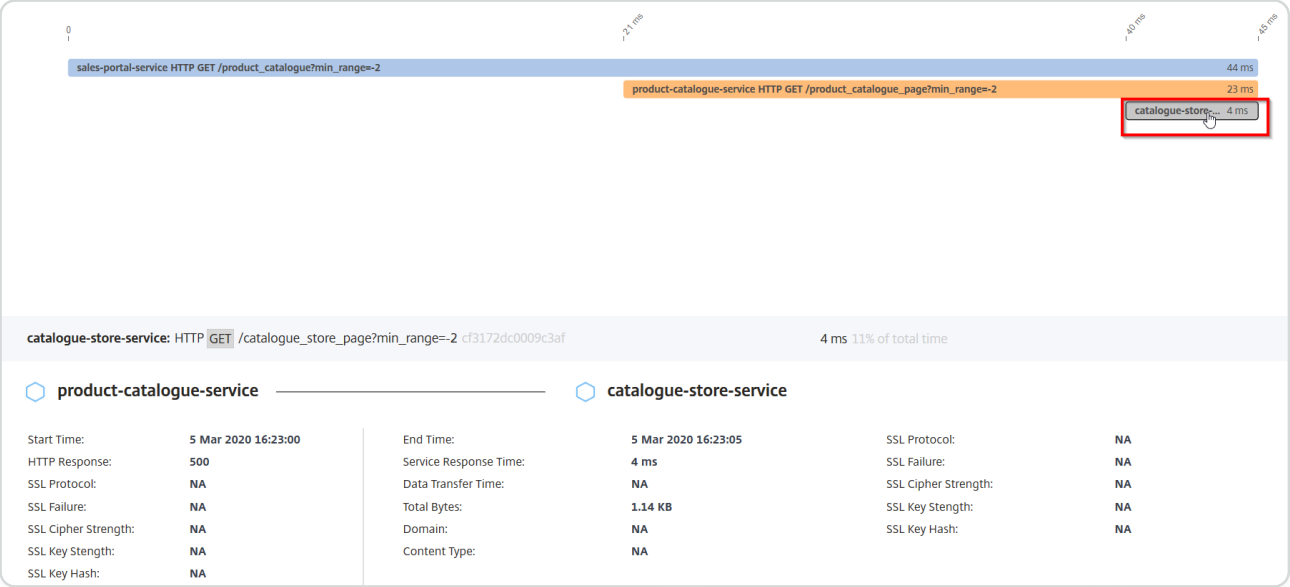
1 – Displays the start time, response time, total services, and total spans for the transaction.

2 – Displays the details for the selected service that has communicated with its inter-dependency services. You can click each transaction to view details.

3 – Displays the transaction details for each service.

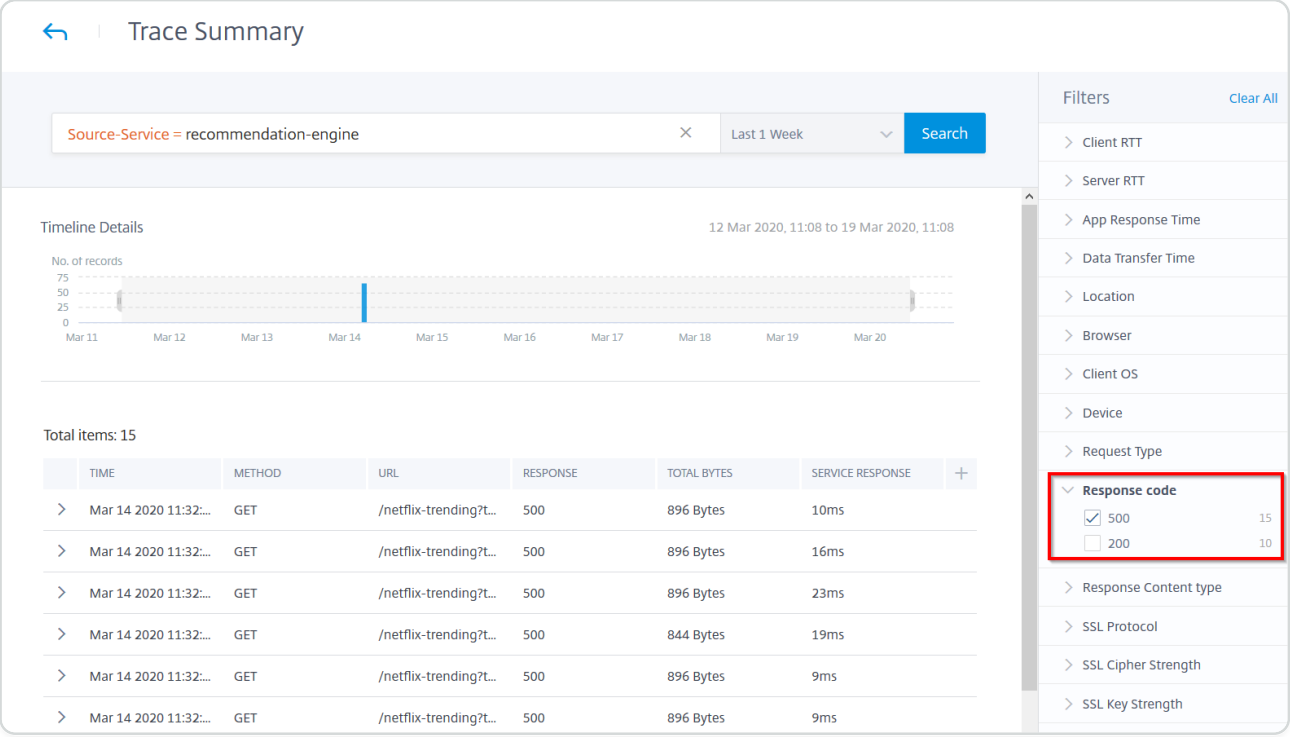
According to the example image, `catalogue-store-service` indicated an error. Click the transaction available for `catalogue-store-service`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The transaction details between `product-catalogue-service` and `catalogue-store-service` indicate HTTP response as 500. With these details, as an administrator, you can analyze the erroneous service and troubleshoot `product-catalogue-service` as a resolution.

You can also filter results by selecting options from each metric under the **Filters** panel. For example, if you want to view all 5xx transactions, click **Response code** and select **500**.



- **Client RTT**: The time duration for a packet to travel from the client.
- **Server RTT**: The time duration for a packet to travel from the server.
- **App Response Time**: The application average response time

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Data Transfer Time**: The data transfer size and the rate at which the transmit can happen from/to a service.
- **Location**: The client location
- **Browser**: The browser types used by the clients. For example: Chrome, Firefox.
- **Client OS**: The client OS based on the User Agent details from the browser.
- **Device**: The devices based on the User Agent details from the browser. For example: Tablet, Mobile.
- **Request Type**: The transaction request type. For example: GET.
- **Response code**: The response code received from the server. For example: 501, 404, 200.
- **Response content type**: The transaction content type. If the client request is for text/html, then the response from the server must be text/html.
- **SSL Protocol**: The SSL protocol version used by the clients. For example: SSLv3.
- **SSL Cipher Strength**: The cipher strength based on the SSL certificate key size such as high, medium, and low.
- **SSL Key Strength**: The SSL cipher strength is calculated from the SSL certificate key size. The key length defines the SSL algorithm security. For example: 2048
- **SSL Frontend Failure reason**: The front end SSL handshake error message. For example: SSL CLIENTAUTH FAILURE

View diagnostic details for partial or no data in service graph

After you complete the required service graph configuration and add the Kubernetes cluster in NetScaler Console, the service graph starts to populate data. In some scenarios, you might observe that service graph displays either partial data or no data. Some of the possible reasons for the partial data or no data in service graph are:

- Static route is not configured
- Kubernetes cluster status is down
- CPX registration is failed
- CPX virtual servers are not licensed
- The required analytics configuration is not set that prevents service graph to load all data

As an administrator, you might find it difficult to analyze the reasons when you see service graph displaying partial data or no data. The diagnostics information in service graph page enables you to see the possible reasons and required actions to troubleshoot the partial data or no data issue.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

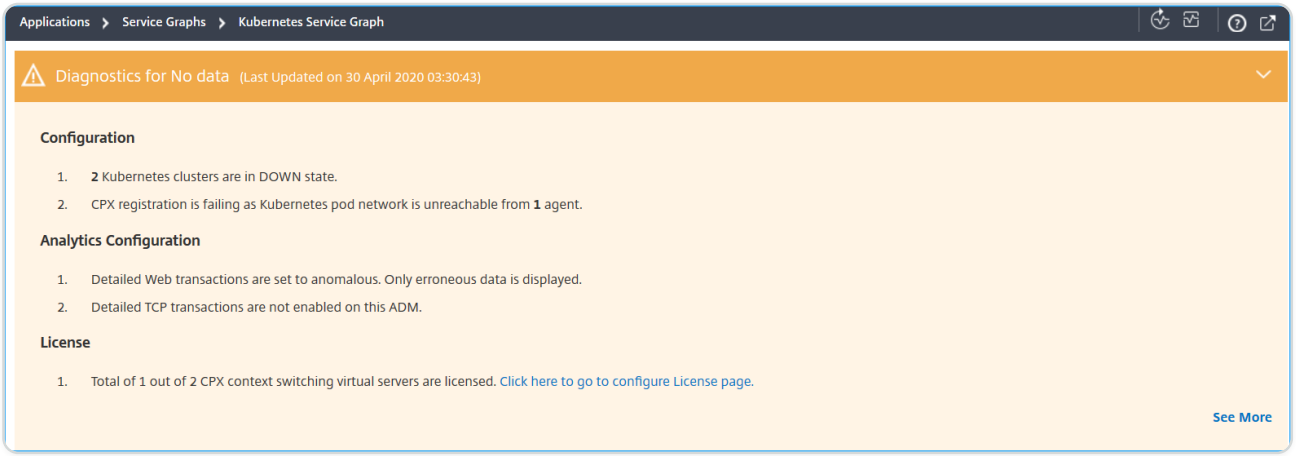
In NetScaler Console, navigate to **Applications** > **Service Graph** and click the **Microservices** tab.

Diagnostics for no data

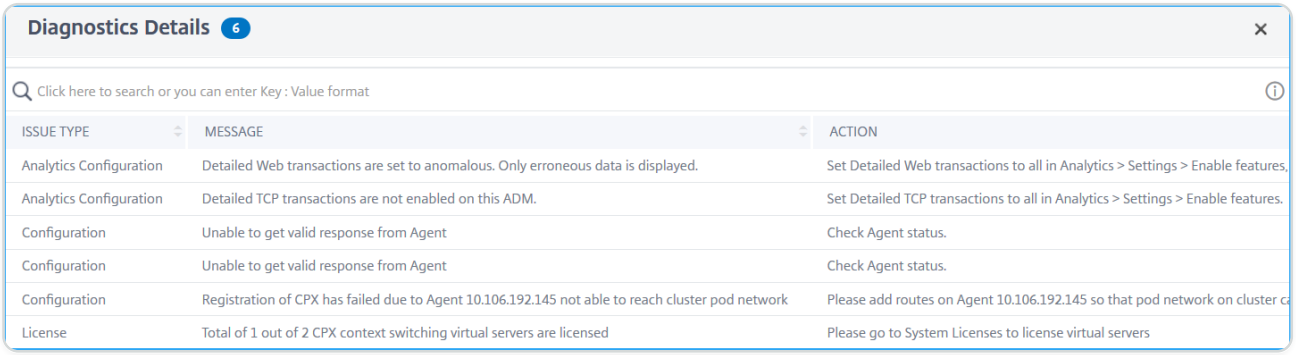
If service graph does not display any data, the following diagnostics message is displayed.



Click **>** to view details. You can view the possible reasons for service graph not displaying any data. The following image is an example for no data in service graph.



Click **See More** to view details for the issues.



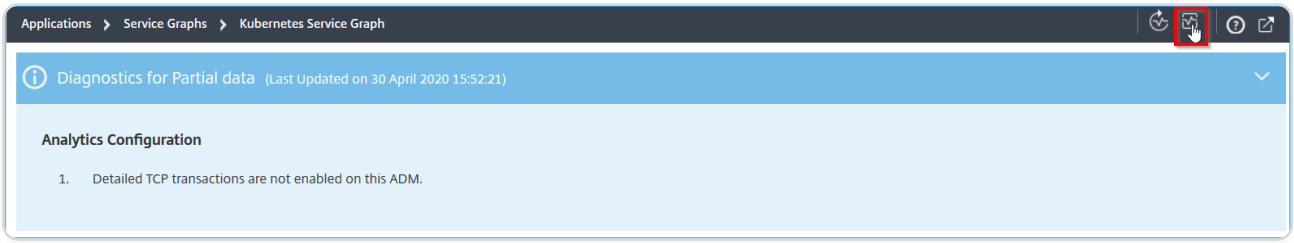
- **Issue Type** – Indicates if the issues occurring from configuration, analytics configuration, or licensing.
- **Message** – Indicates what has caused the issue.
- **Action** – Indicates what action must be performed to troubleshoot the issue.

Diagnostics for partial data

If service graph is displayed only with partial data, click the **Show Diagnostics** button to view the diagnostics information.

The following example indicates the TCP transactions are disabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

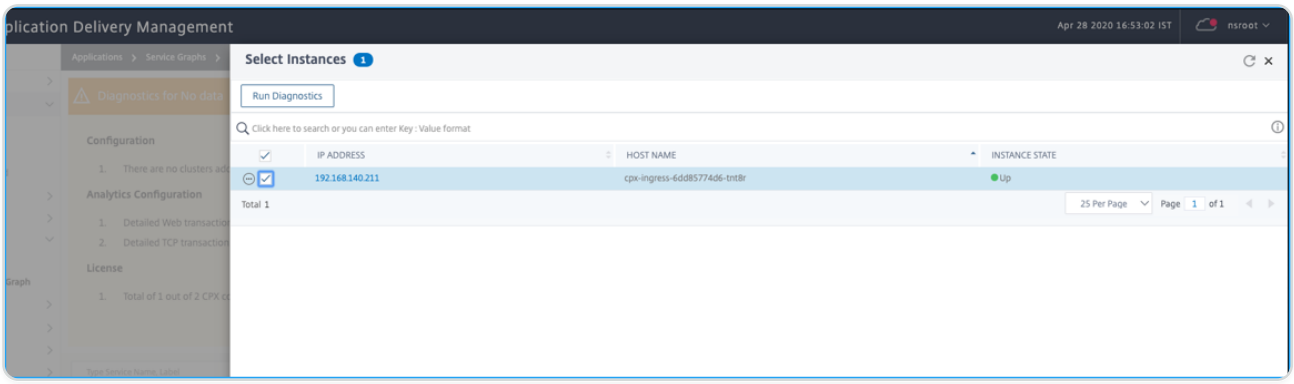


For this example, you must enable the **TCP Transaction Settings** to **All** by navigating to **Settings > Analytics Settings**.

Troubleshooting

As an administrator, using these diagnostics messages, you can validate these issues and try to troubleshoot these issues. After you troubleshoot, NetScaler Console runs a periodic diagnostic check automatically at a regular interval. After the diagnostics check is complete, the partial data or no data in service graph issue will be resolved.

You can also click **Run Diagnostics**, select the **CPX instances**, and click **Run Diagnostics**.



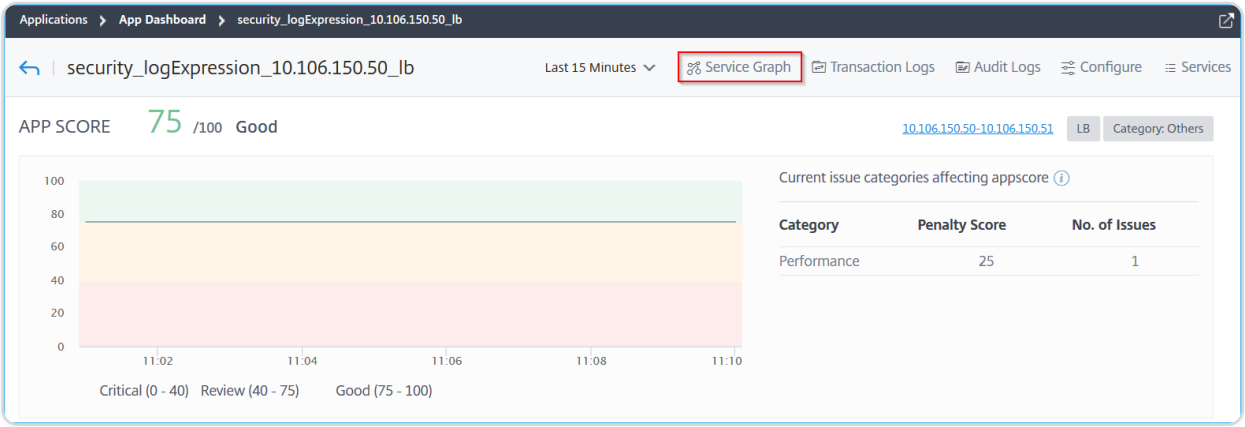
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service graph for 3-tier web applications

To view service graph for an application:

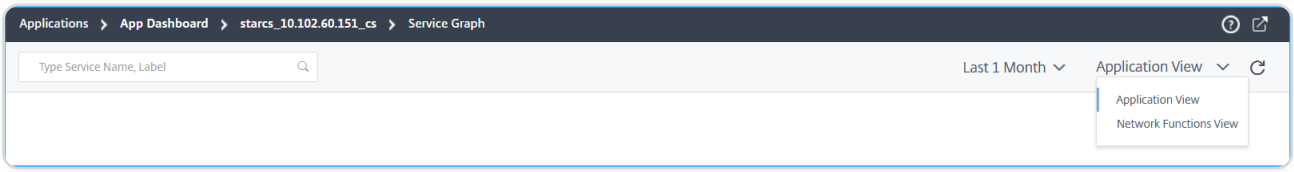
1. Navigate to **Applications** > **Dashboard**.
2. Select an application.

   The application details page is displayed.
3. Select the time duration and click **Service Graph**.



The service graph page is displayed for the selected application.

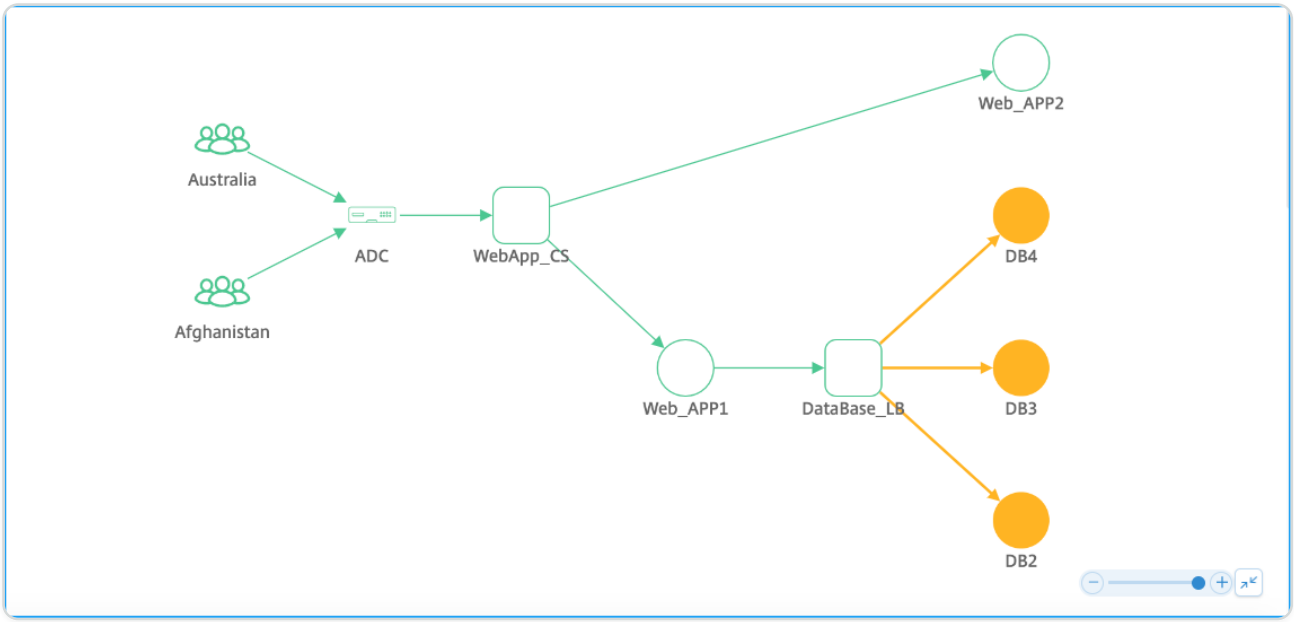
You can view service graph in **Application View** or in **Network Functions View**.



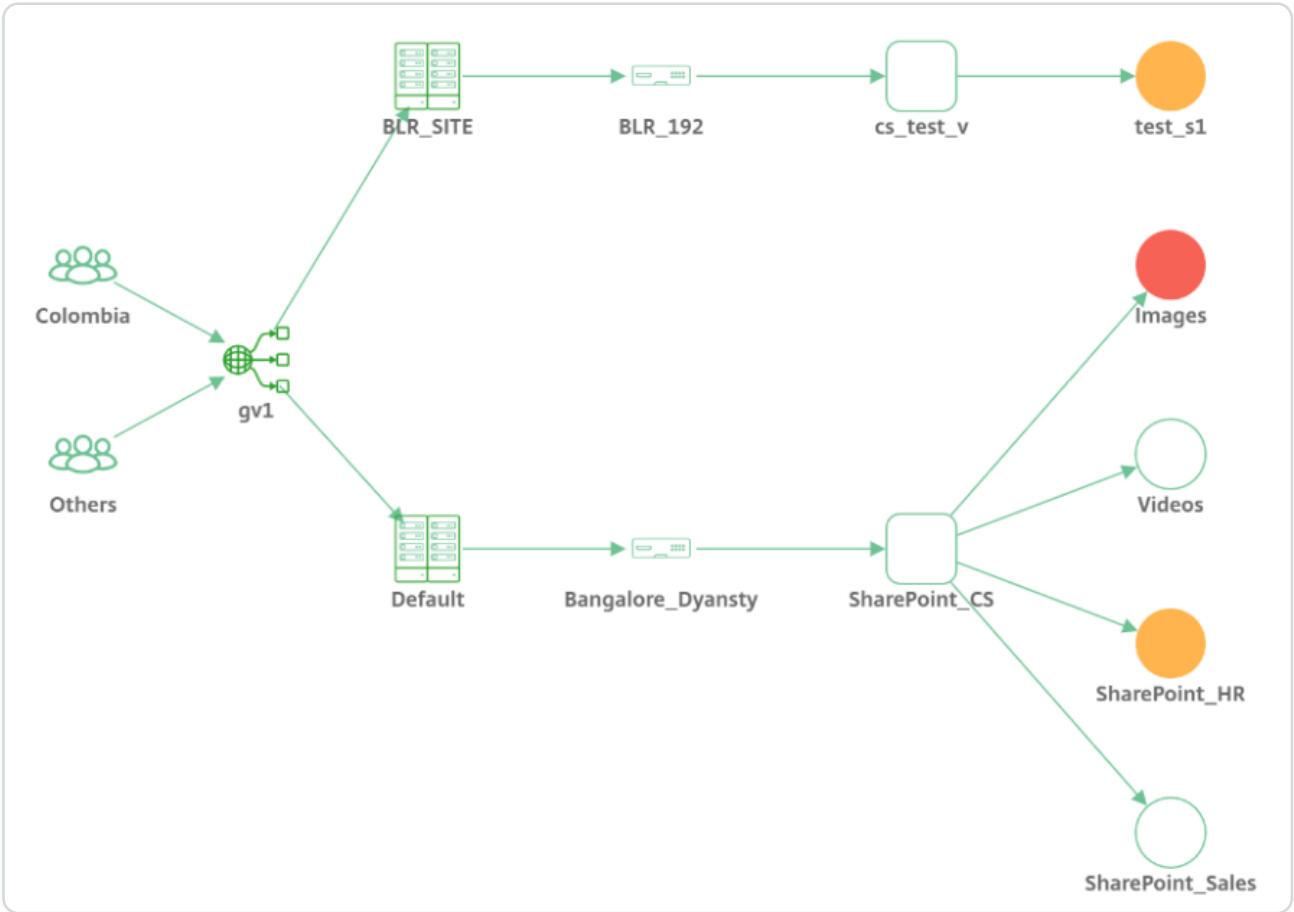
Application view

Displays the overview of the application configuration. In this view, you can visualize the communication between client, NetScaler, and web applications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For a GSLB application, you can visualize the communication between client, data center, NetScaler, and services.

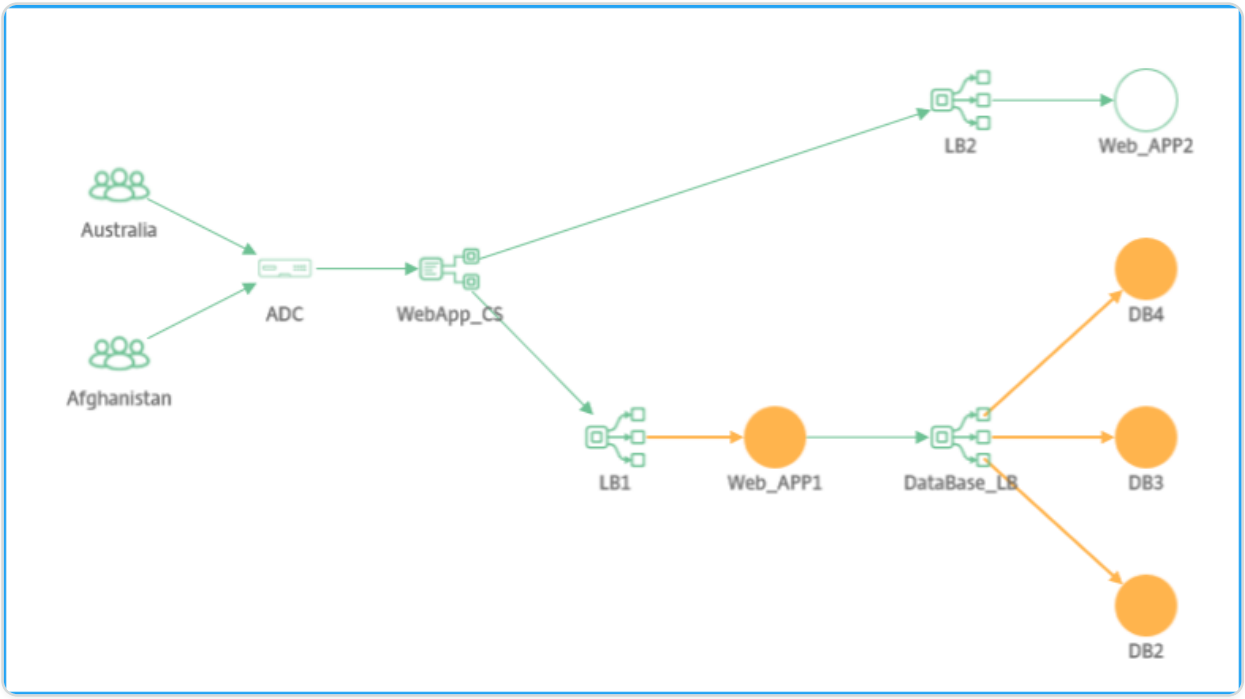


Network functions view

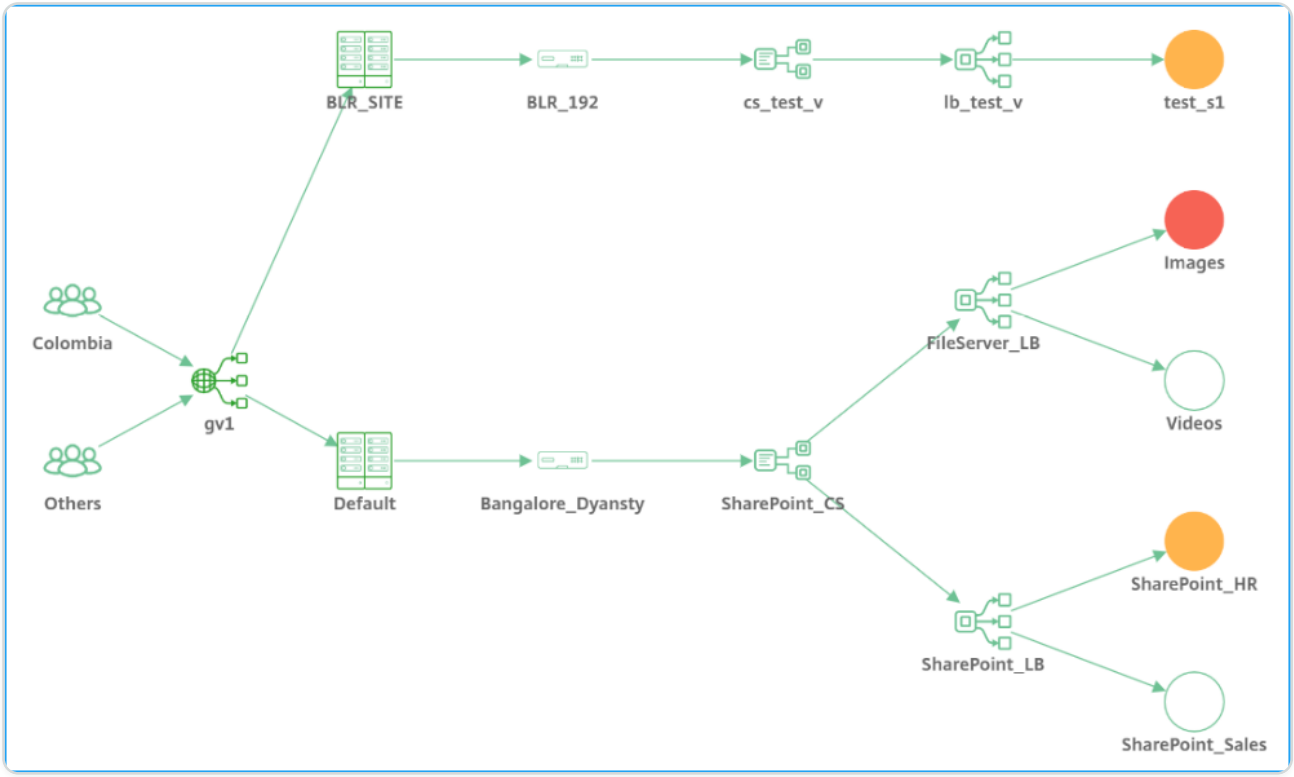
Displays the virtual servers associated with the application. In this view, you can visualize if the NetScaler is communicating with:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Content Switching virtual server to access the application
- Load Balancing virtual server to access the application
- Both Content Switching and Load Balancing virtual servers to access the application



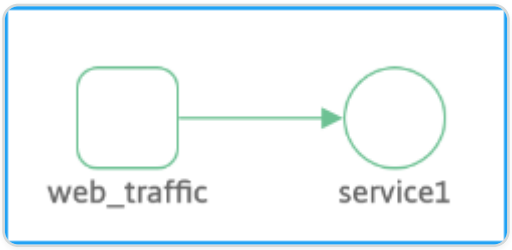
For GSLB application, the details are displayed along with the data center and NetScaler.



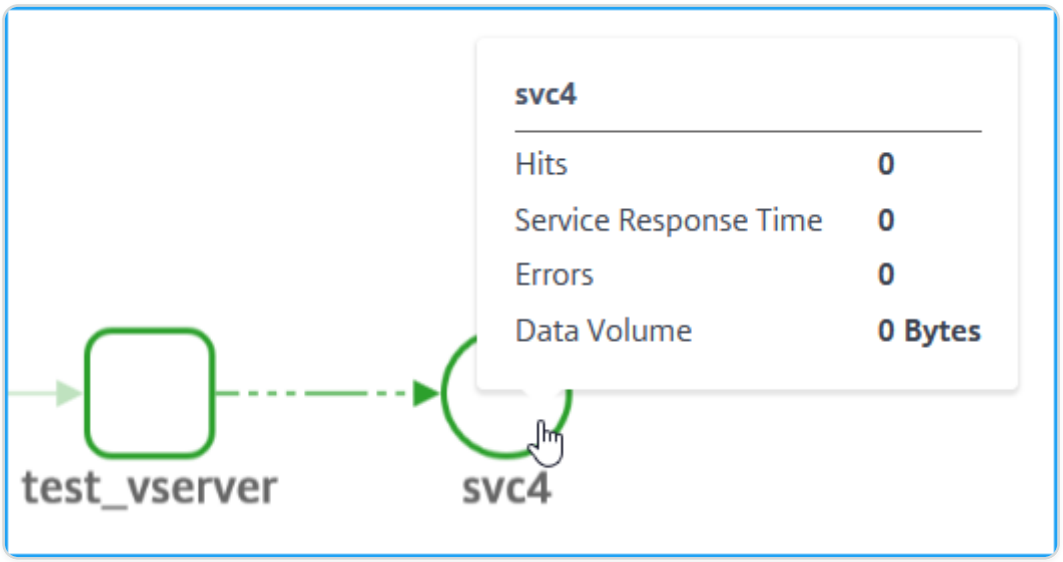
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service graph view for no active transactions

If no active transactions occur between NetScaler and web application, service graph displays only the basic configuration of the application (without client and NetScaler).



When you hover the mouse pointer on a service or virtual server, the details are displayed as 0 for all metrics because of no transactions.



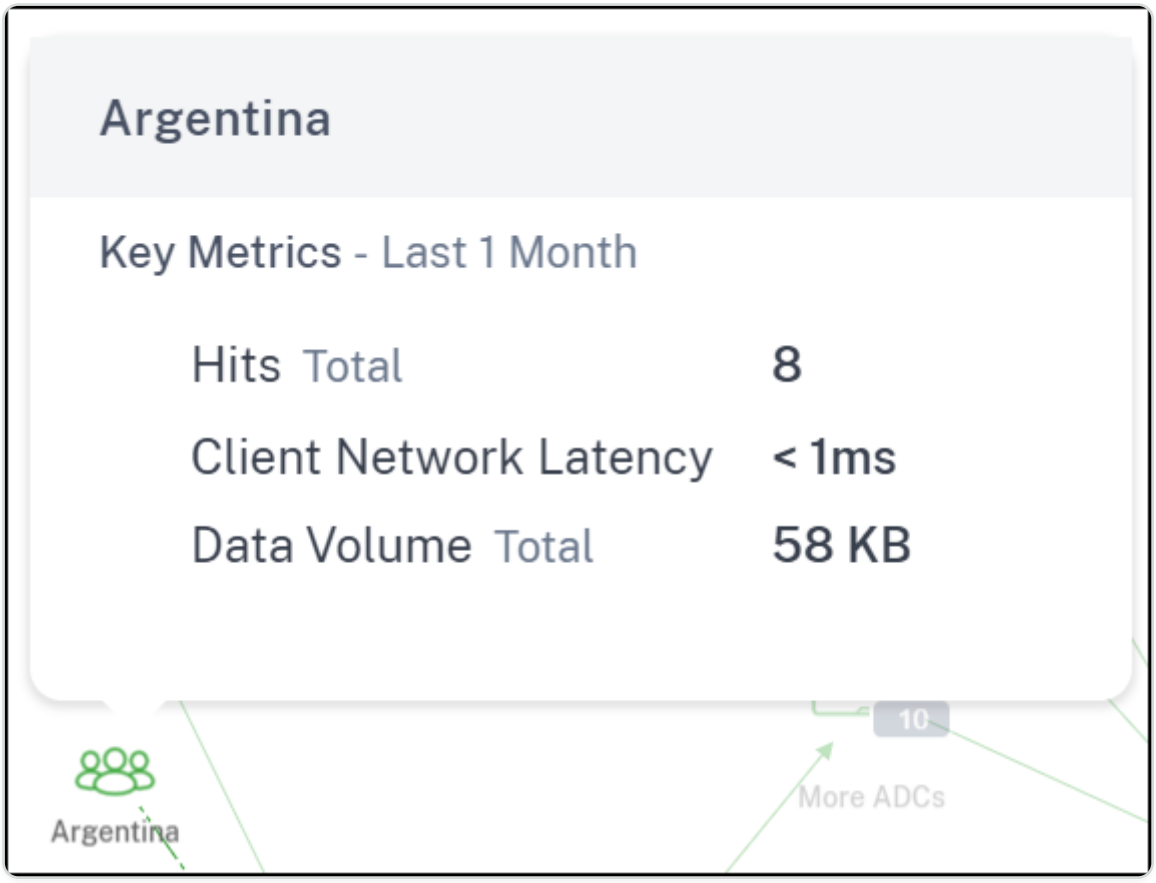
Analyze metrics

Hover the mouse pointer on each service to view metrics details either in **Application View** or **Network Function View**.

Client metrics

Hover the mouse pointer on the client to view client metrics.

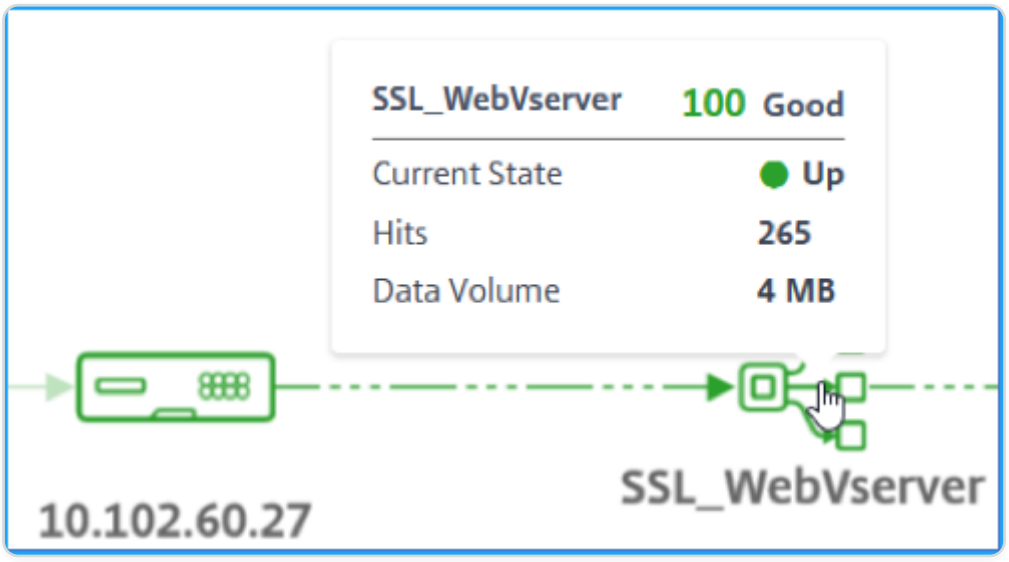
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Hits** - Total requests received by the client.
- **Client Network Latency** – Indicates the network latency from the client.
- **Data Volume** - Indicates the total data processed by the client.

Network function metrics

Hover the mouse pointer on a load balancing or content switching service to view the metrics details.



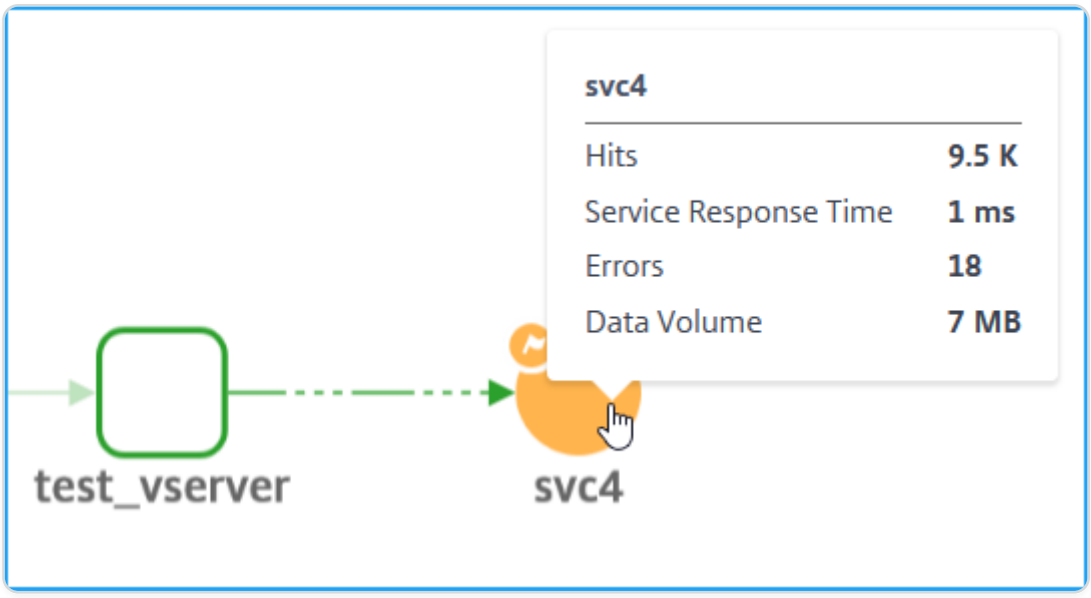
- **Current state** – Indicates the current status of the virtual server

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Hits** – Indicates the total number of hits received by the virtual server
- **Data volume** – Indicates the total data volume processed by the virtual server

Service metrics

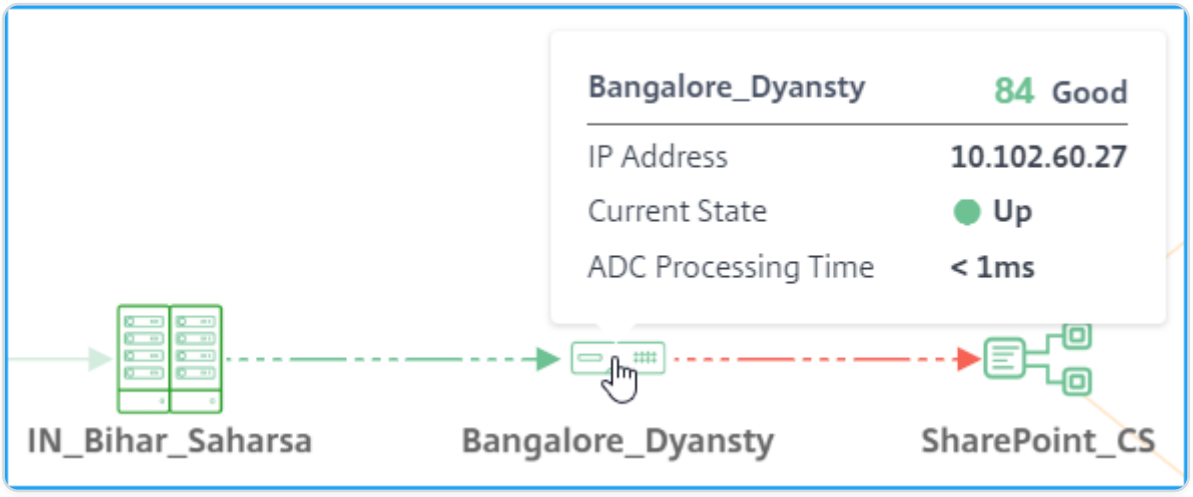
Hover the mouse pointer on a service (web application) to view the metrics



- **Hits** – Indicates the total number of hits received by the service
- **Service response time** – Indicates the average response time from the service
- **Errors** – Indicates the total errors occurred from the service
- **Data Volume** – Indicates the total data processed by the service

NetScaler metrics (only for GSLB applications)

Hover the mouse pointer on the NetScaler to view the metrics.



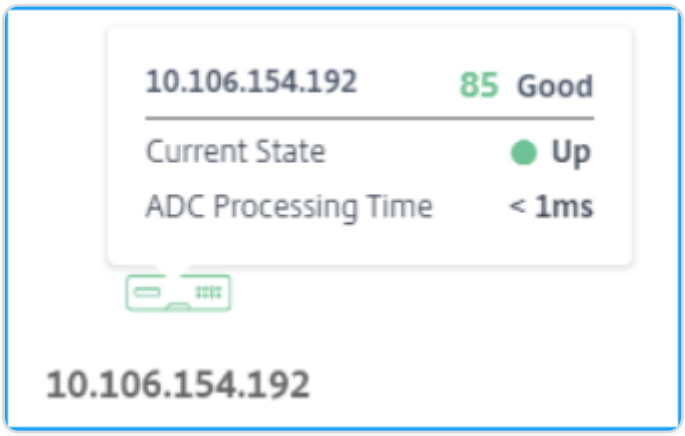
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Displays the host name and the current NetScaler score. The score is calculated based on the different NetScaler potential issues. For more information, see Instance score.
- **IP Address** – Denotes the NetScaler IP address
- **Current state** – Denotes the NetScaler status such as Up, Down, or Out of service
- **NetScaler Processing Time** – Denotes the average processing time by the NetScaler instance

NOTE

If a host name is not assigned to NetScaler:

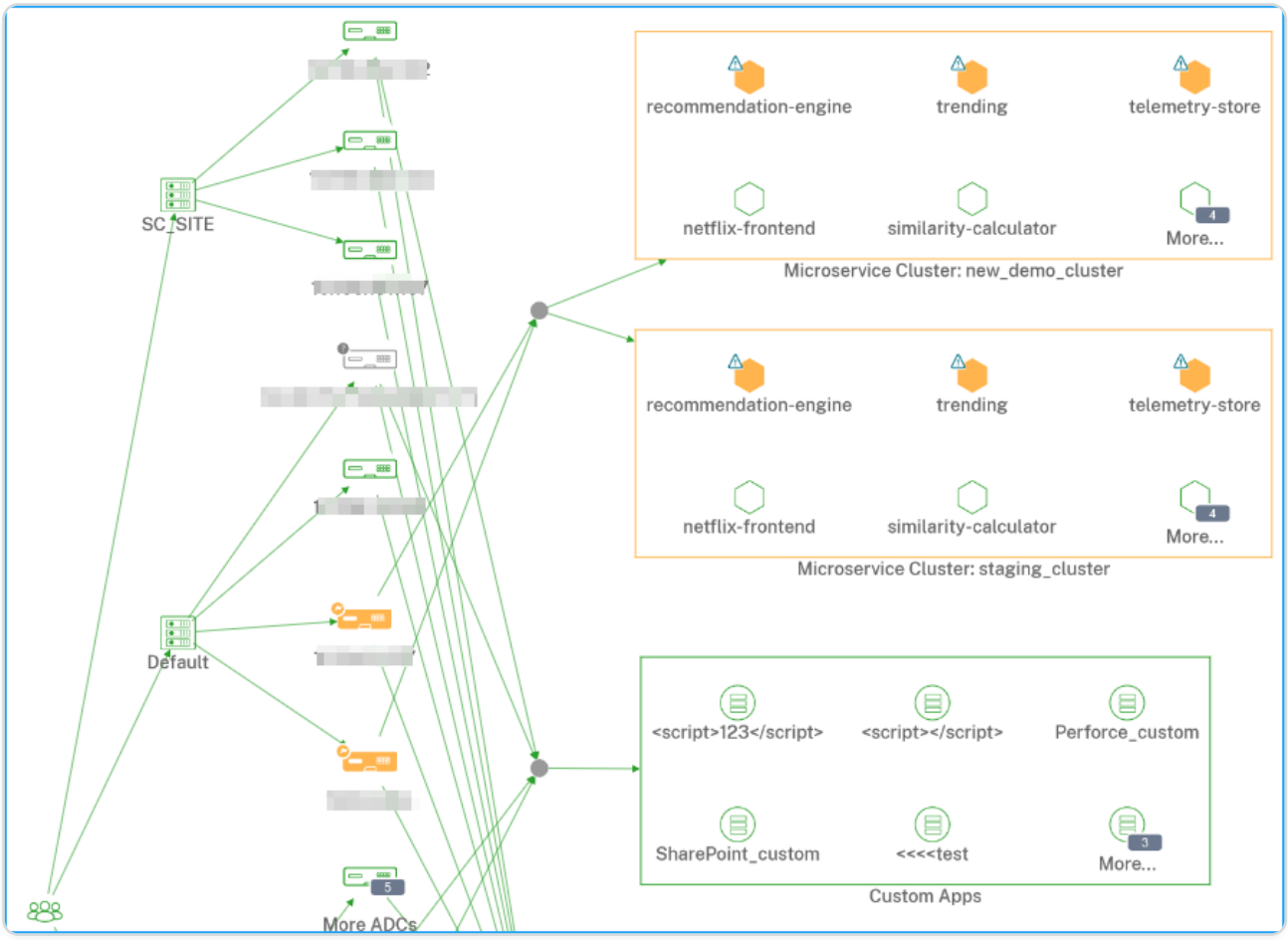
- NetScaler IP address is displayed instead of host name.
- In the metrics, the NetScaler IP address information is not displayed.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Holistic view of all applications in service graph

Navigate to **Applications** > **Service Graph** and then click **Global**.



The service graph displays the following for the selected time duration:

- The region from where the users access the specific application
- Data centers where the NetScaler instances are hosted
- The total discrete applications from all NetScaler instances

NOTE

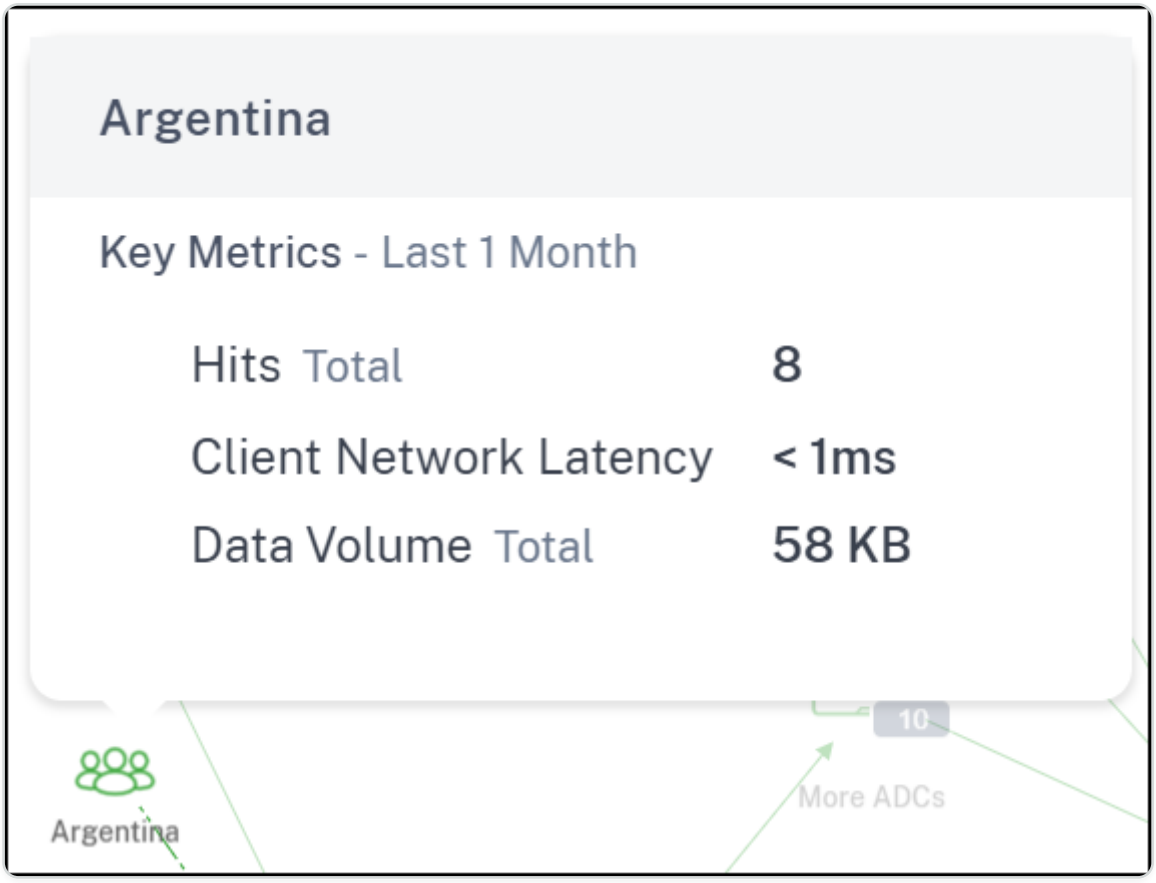
If a NetScaler instance does not have discrete applications, the arrow edge towards the Discrete virtual server from the NetScaler instance is not visible

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The total custom applications from all NetScaler instances
- The total microservice applications from the NetScaler CPX instance

View client metrics

Hover the mouse pointer on a client region to view the metrics.



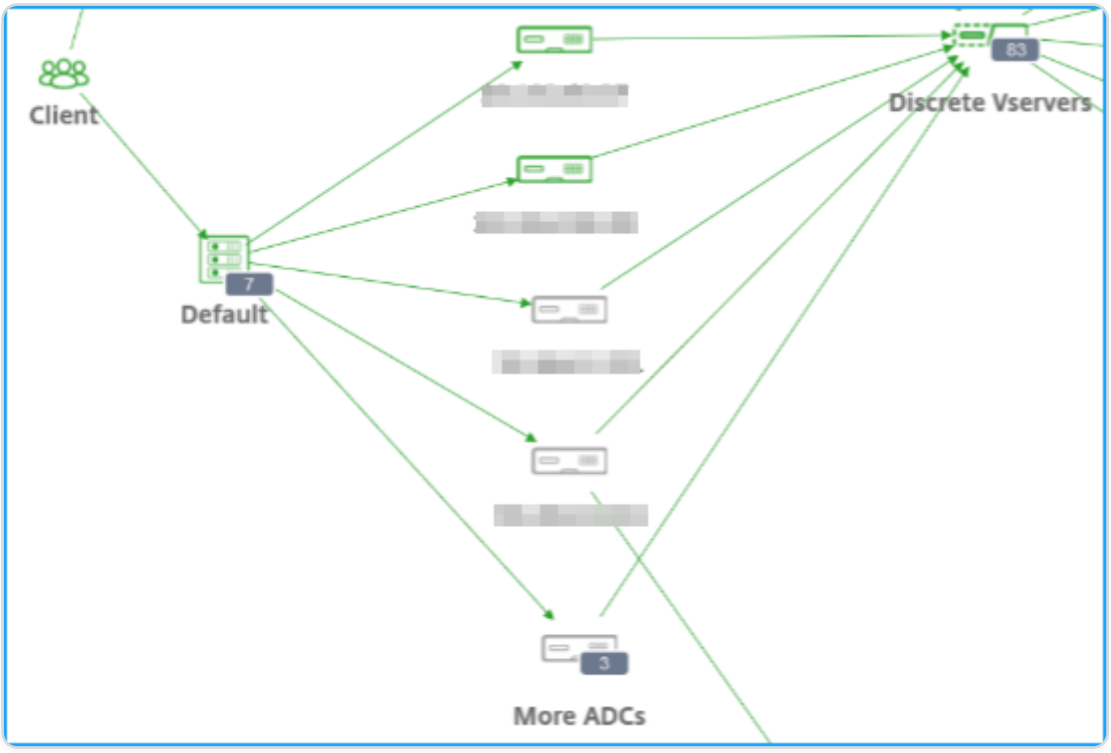
- **Hits** - Total requests received by the client.
- **Client Network Latency** – Indicates the network latency from the client.
- **Data Volume** - Indicates the total data processed by the client.

View NetScaler details

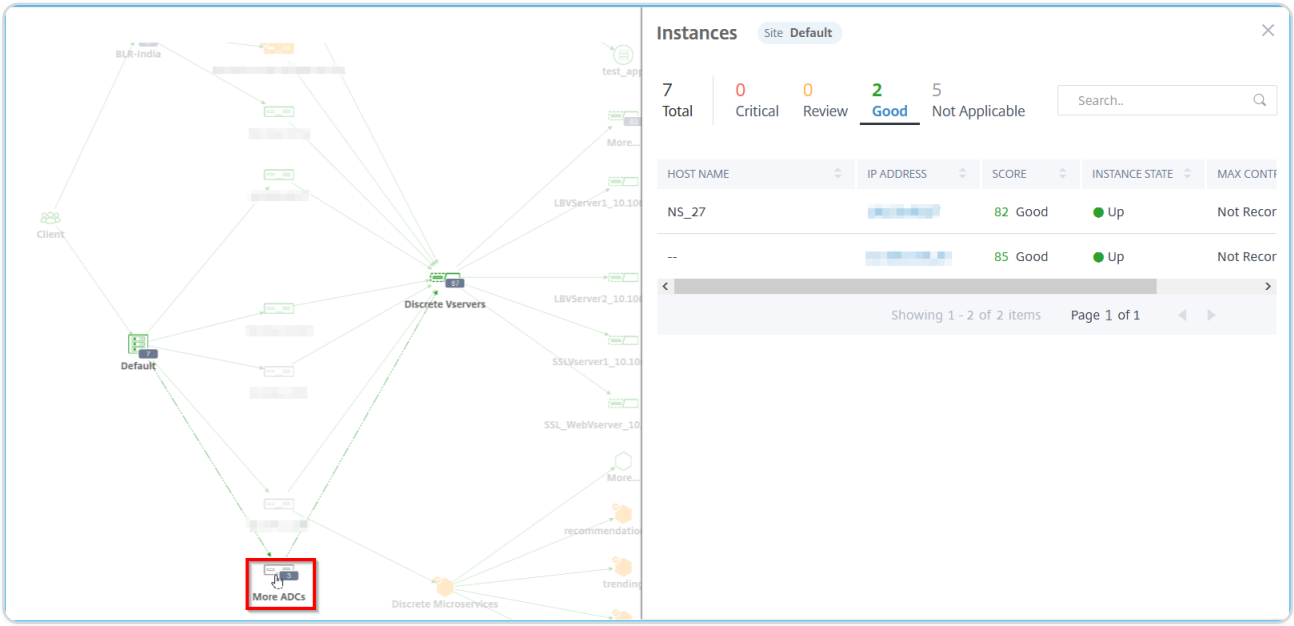
The service graph enables you to view:

- The data center grouped with its total NetScaler instances
- Only the top 4 low-scored NetScaler instances from each data center

© 1997–2026 Citrix Systems, Inc. All rights reserved.

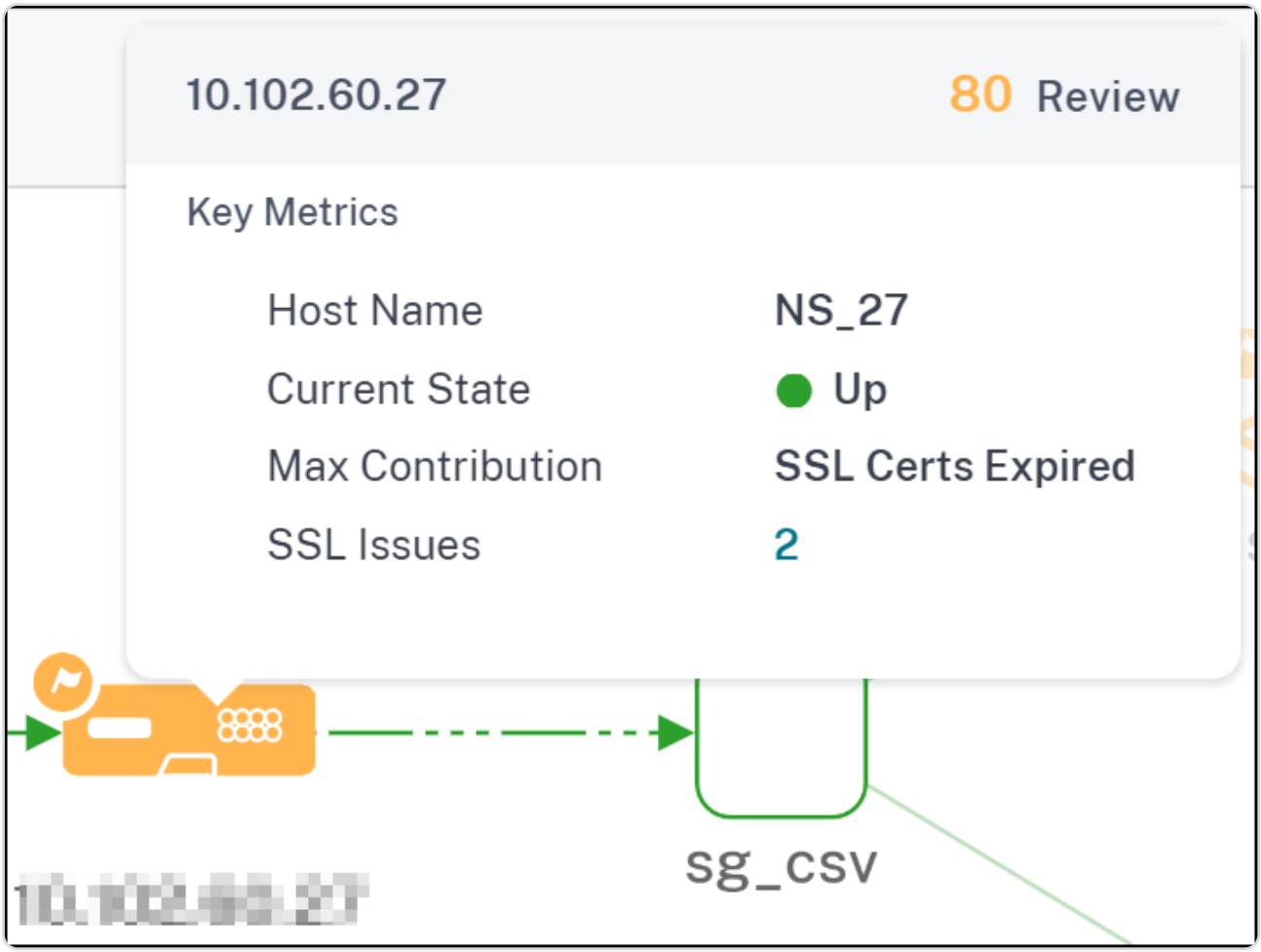


Click **More NetScaler instances** to view all NetScaler instances by selecting the respective status (Critical, Review, Good, and Not Applicable) tabs.



Hover the mouse pointer on a NetScaler instance to view the metrics.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can view:

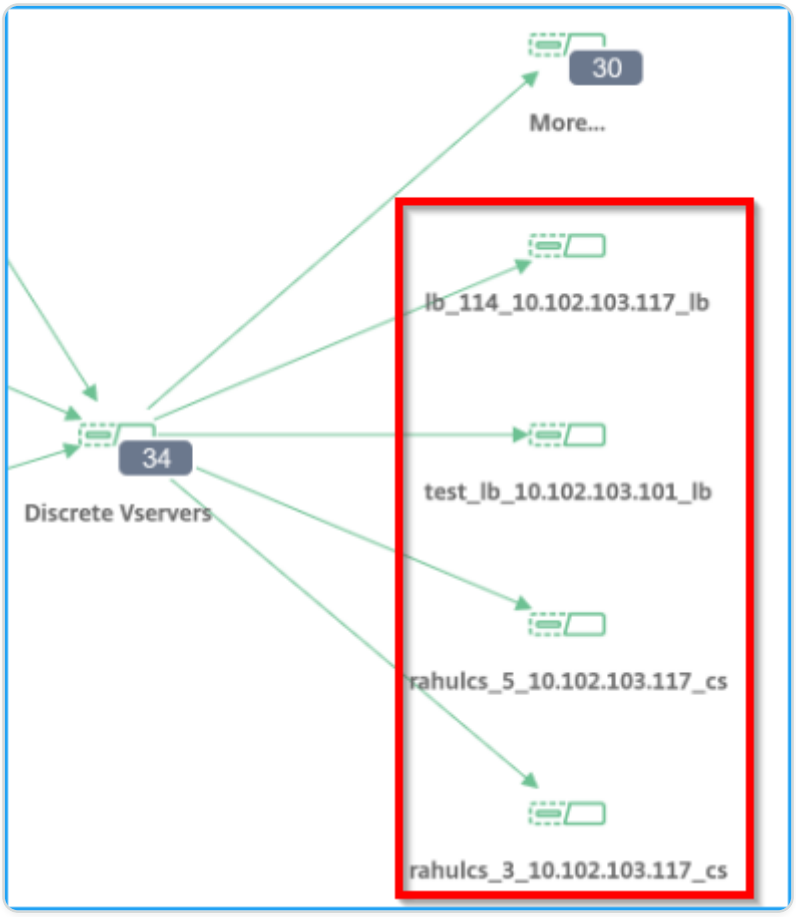
- NetScaler instance IP address and score
- **Host Name** – Indicates the host name that is assigned to the NetScaler instance
- **Current State** – Indicates the current status of the NetScaler instance such as Up, down, out-of-service.
- **Max Contribution** – Indicates the top issue that affects the current NetScaler score.
- **SSL Issues** – Indicates the total SSL issues from the NetScaler instance. Click the error count to drill down and view the SSL error details.

Click the **NetScaler instance** to view the instance details such as instance score, key metrics, and issues associated with the NetScaler instance. For more information, see View instance details in Infrastructure Analytics.

View discrete applications

The service graph displays the top 4 low scored discrete applications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Consider that you have the following discrete applications:

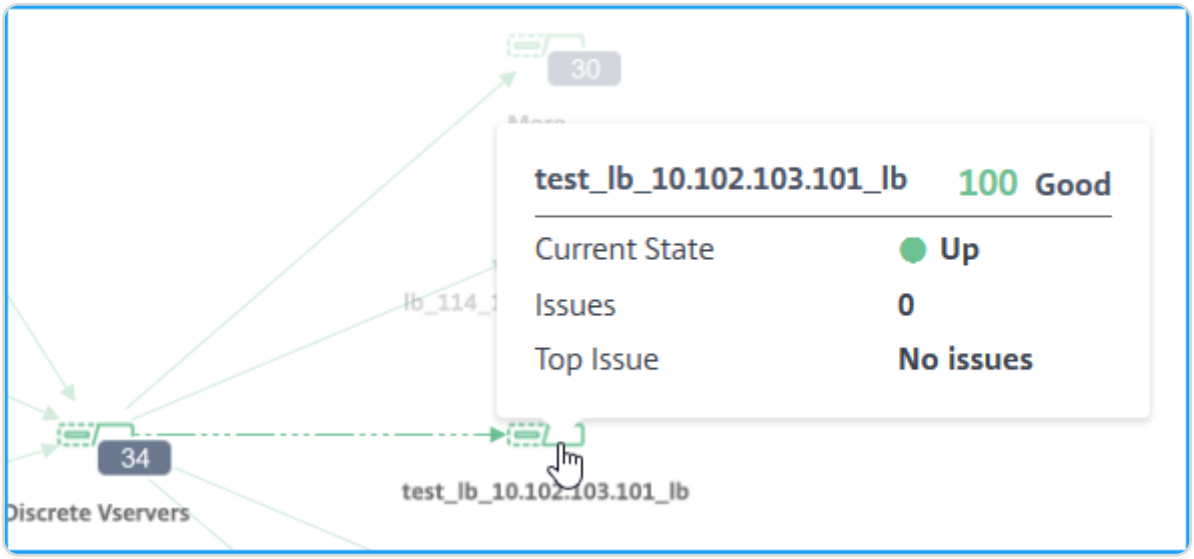
APP NAME	NETSCALER	APP SCORE	APP STATUS
App1	10.102.29.50	35 (Critical)	Up
App2	10.102.29.90	100 (Good)	Down
App 3	10.102.32.40	49 (Review)	Up
App4	10.102.113.208	92 (Good)	Down
App5	10.102.25.25	86 (Good)	Up
App6	10.102.29.41	77 (Good)	Up
App7	10.102.29.102	41 (Review)	Up

In this scenario, you can view App1, App3, App6, and App 7 as the top 4 low-scored applications in service graph.

Similarly, you can also view the top 4 low-scored applications for **Custom** and **Microservices** applications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

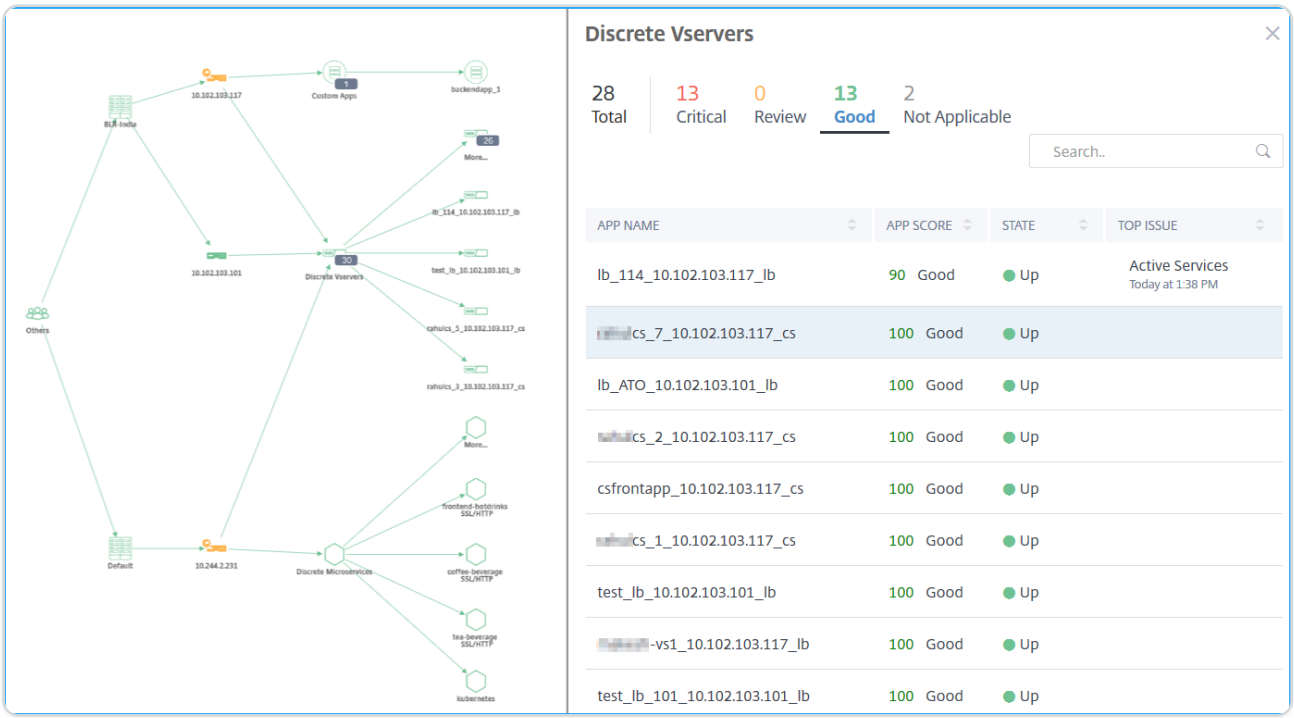
Hover the mouse pointer on a service to view the metrics information.



You can view:

- The application name and score
- **Current State** – Indicates the application current status such as Up or Down
- **Issues** – Indicates the total issues applicable for the application
- **Top Issue** – Indicates the top issue that impacts the overall application score

Click **More** to view all discrete applications. The Discrete virtual server page is displayed as shown in the following image:

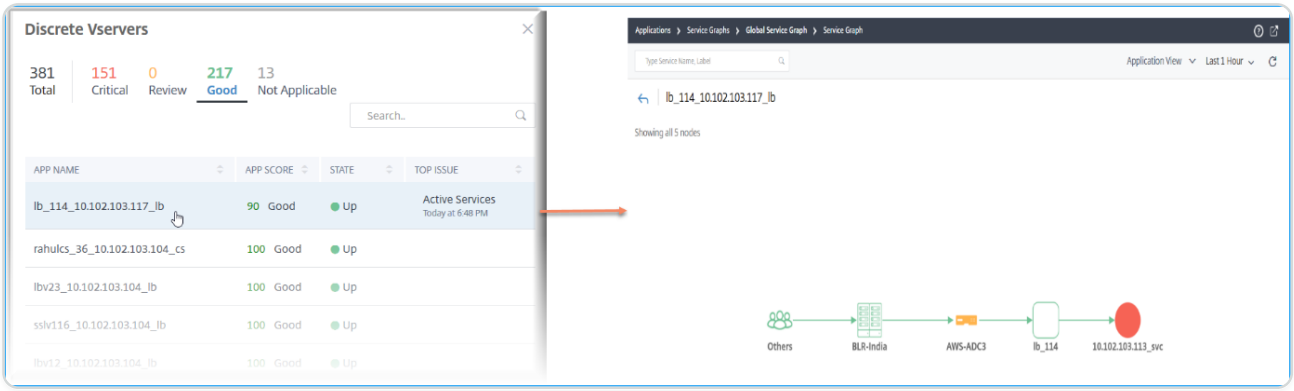


The virtual servers are displayed according to the status.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Total** – Total discrete applications
- **Critical** – App score is between 0 and < 40
- **Review** – App score is between 40 and < 75
- **Good** – App score is > 75
- **Not Applicable** – App is not bound to any virtual server

You can click each tab to view the virtual servers. When you click an application, the service graph for the selected application is displayed.



For more information, see Service Graph for applications.

View microservice applications

The service graph also displays all microservice applications that belong to the Kubernetes clusters. Hover the mouse pointer on a service to view the metrics details.

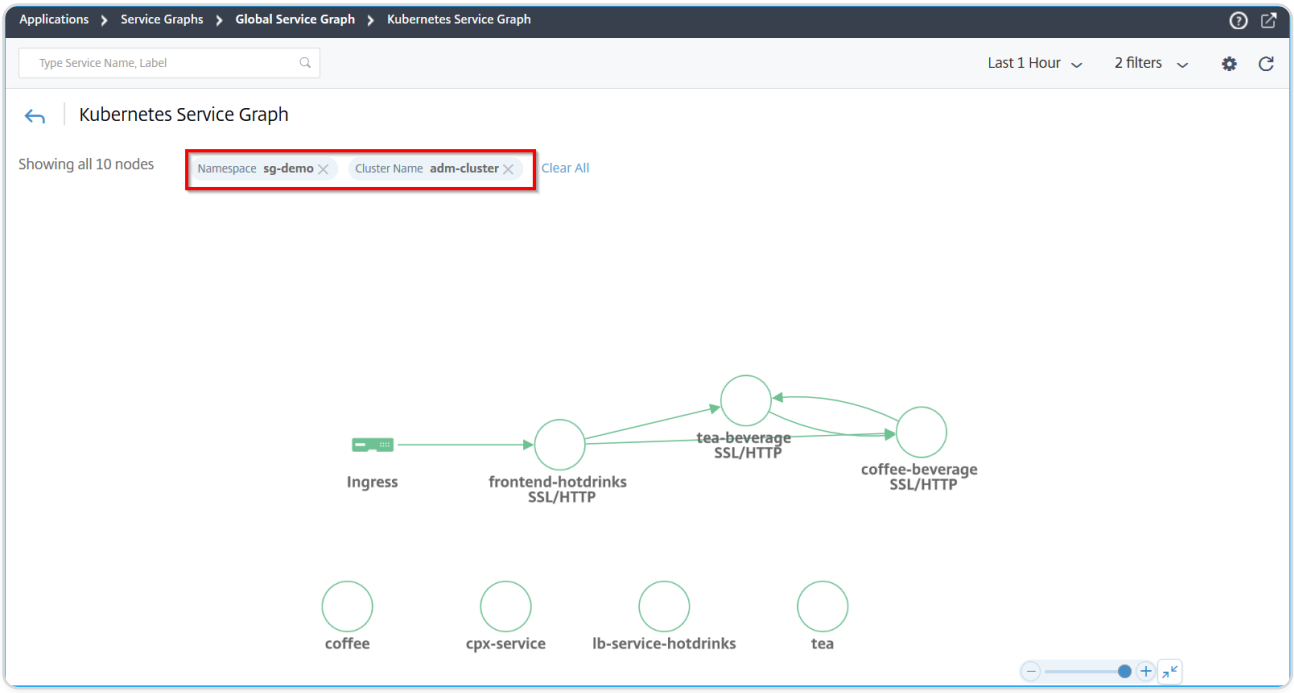
You can view:

- The service name
- The protocol used by the service such as SSL, HTTP, TCP, SSL over HTTP
- **Hits** – The total number of hits received by the service
- **Service Response Time** – The average response time taken from the service.

  (Response time = Client RTT + request last byte – request first byte)
- **Errors** – The total errors such as 4xx, 5xx, and so on
- **Data Volume** – The total volume of data processed by the service
- **Namespace** – The namespace of the service
- **Cluster Name** – The cluster name where the service is hosted
- **SSL Server Errors** – The total SSL errors from the service

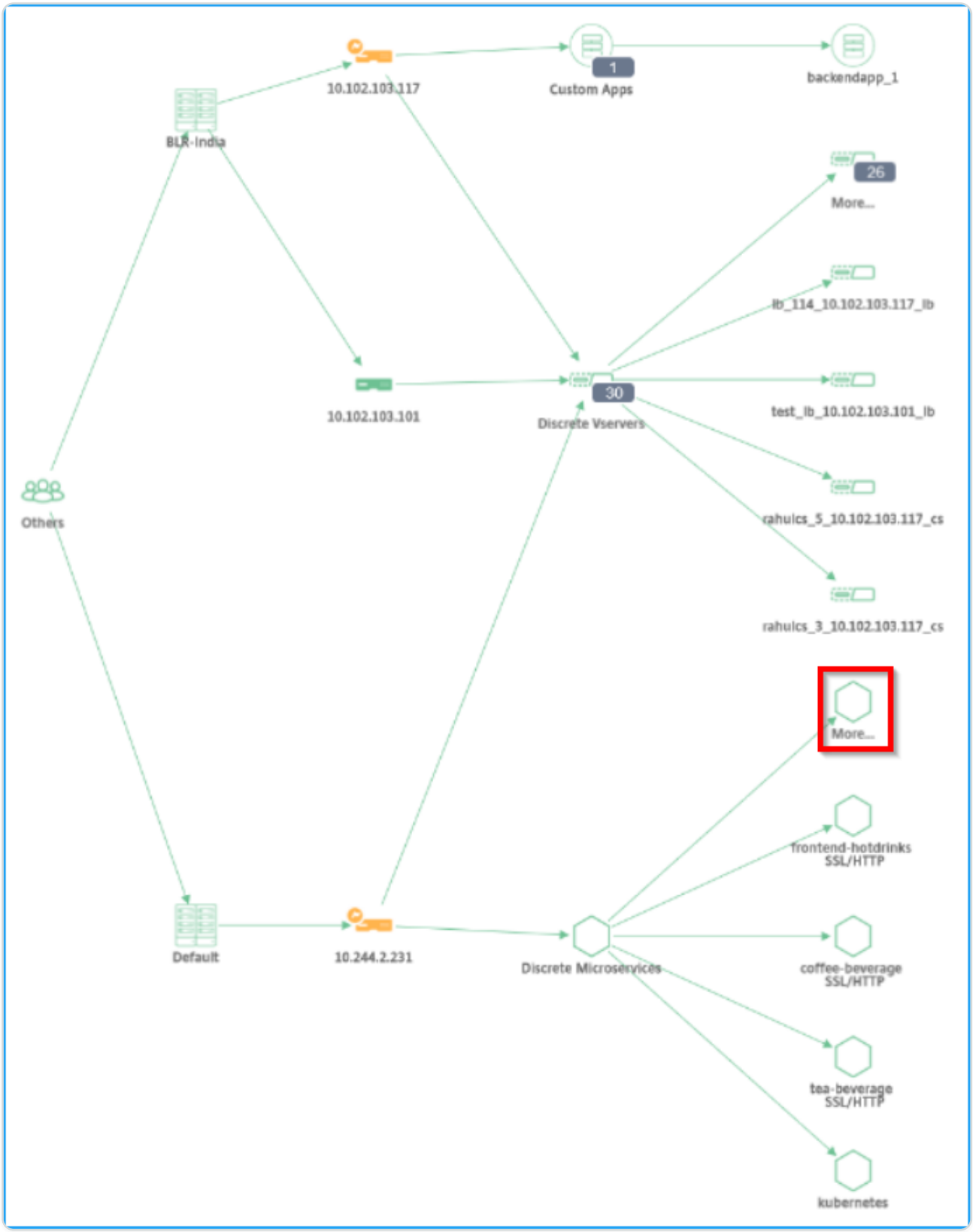
© 1997–2026 Citrix Systems, Inc. All rights reserved.

When you click a service, the Kubernetes service graph for the selected service is displayed, along with the service namespace and cluster name filters applied.



Click **More** to view the Kubernetes service graph that has all services. For more information on Kubernetes service graph, see Service graph for cloud native applications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



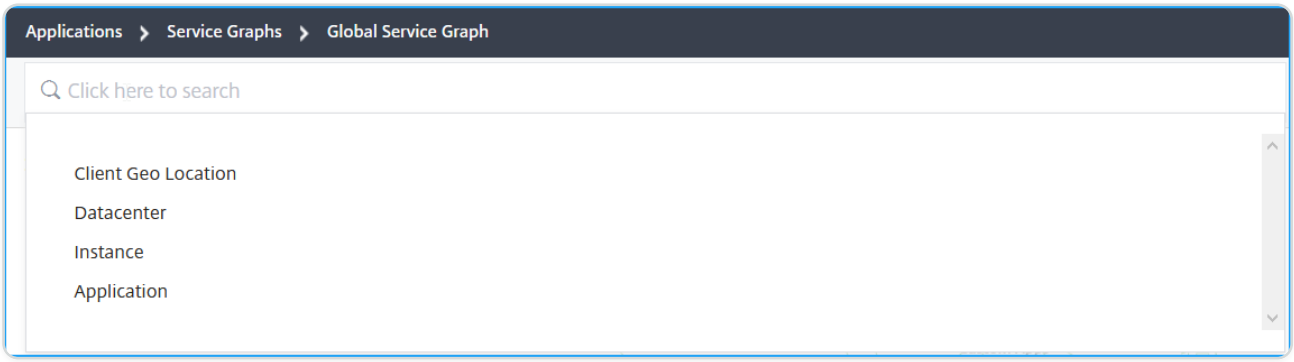
Search bar to filter results

You can use the search bar to filter results. As an administrator, this search bar enables you to narrow-down quickly to a particular instance/client/application/data center, when you have:

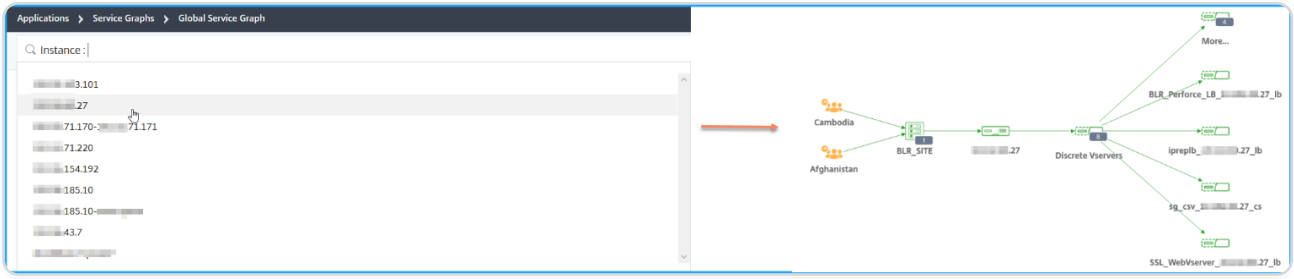
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- A large enterprise with many data centers
- Configured many NetScaler instances for each data center
- Configured many applications deployed or accessed through each NetScaler instance
- Clients accessing the application from different locations

Place the mouse pointer on the search bar and select the category that you want to create the filter.



For example, if you want to view a particular NetScaler instance, select **Instance** from the search bar and select the instance IP address. The global service graph displays the selected instance and its associated applications, data centers, and client locations.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBooks

StyleBooks simplify the task of managing complex NetScaler configurations for your applications. A StyleBook is a template that you can use to create and manage NetScaler configurations.

With a StyleBook, you can:

- Configure a specific feature of NetScaler.
- Create configurations for an enterprise application deployment such as Microsoft Exchange or Lync.

StyleBooks fit in well with the principles of Infrastructure-as-code that is practiced by DevOps teams, where configurations are declarative and version-controlled. The configurations are also repeated and are deployed as a whole. StyleBooks offer the following advantages:

- **Declarative**: StyleBooks are written in a declarative rather than imperative syntax. StyleBooks allow you to focus on describing the outcome or the "desired state" of the configuration rather than the step-by-step instructions on how to achieve it on a particular NetScaler instance. NetScaler Console computes the diff between existing state on a NetScaler and the desired state you specified, and makes the necessary edits to the infrastructure. Because StyleBooks use a declarative syntax, written in YAML, components of a StyleBook can be specified in any order, and NetScaler Console determines the correct order based on their computed dependencies.
- **Atomic**: When you use StyleBooks to deploy configurations, the full configuration is deployed or none of it is deployed and this ensures that the infrastructure is always left in a consistent state.
- **Versioned**: A StyleBook has a name, namespace, and a version number that uniquely distinguishes it from any other StyleBook in the system. Any modification to a StyleBook requires an update to its version number (or to its name or namespace) to maintain this unique character. The version update also allows you to maintain multiple versions of the same StyleBook.
- **Composable**: After a StyleBook is defined, the StyleBook can be used as a unit to build other StyleBooks. You can avoid repeating common patterns of configuration. It also allows you to establish standard building blocks in your organization. Because StyleBooks are versioned,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

changes to existing StyleBooks results in new StyleBooks, therefore ensuring that dependent StyleBooks are never unintentionally broken.

- **App-Centric**: StyleBooks can be used to define the NetScaler configuration of a full application. The configuration of the application can be abstracted by using parameters. Therefore, users who create configurations from a StyleBook can interact with a simple interface consisting of filling a few parameters to create what can be a complex NetScaler configuration. Configurations that are created from StyleBooks are not tied to the infrastructure. A single configuration can thus be deployed on one or multiple NetScaler instances, and can also be moved among instances.
- **Auto-Generated UI**: NetScaler Console auto-generates UI forms used to fill in the parameters of the StyleBook when configuration is done using the NetScaler Console GUI. StyleBook authors do not need to learn a new GUI language or separately create UI pages and forms.
- **API-driven**: All configuration operations are supported by using the NetScaler Console GUI or through REST APIs. The APIs can be used in synchronous or asynchronous mode. In addition to the configuration tasks, the StyleBooks APIs also allow you to discover the schema (parameters description) of any StyleBook at runtime.

You can use one StyleBook to create multiple configurations. Each configuration is saved as a config pack. For example, consider that you have a StyleBook that defines a typical HTTP load balancing application configuration. You can create a configuration with values for the load balancing entities and run it on a NetScaler instance. This configuration is saved as a config pack. You can use the same StyleBook to create another configuration with different values and run it on the same or a different instance. A new config pack is created for this configuration. A config pack is saved both on NetScaler Console and on the NetScaler instance on which the configuration is run.

You can either use default StyleBooks, shipped with NetScaler Console, to create configurations for your deployment, or design your own StyleBooks and import them to NetScaler Console. You can use the StyleBooks to create configurations either by using the NetScaler Console GUI or by using APIs.

This document includes the following sections:

- How to view StyleBooks
- Default StyleBooks
- Stylebooks developed for business applications
- Custom StyleBooks

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- APIs in StyleBooks
- StyleBooks grammar

StyleBook categories

In NetScaler Console, there are two StyleBook categories: default and custom, which can be either public or private. NetScaler Console allows you to view all the StyleBooks that are present in the system and how they are connected with each other.

This document explains the different types of StyleBooks and the following actions that you can do on the StyleBooks from NetScaler Console:

- Download a custom StyleBook and make modifications, or create a StyleBook based on an existing one.
- Hide NetScaler Console default StyleBooks.
- Delete a custom StyleBook from NetScaler Console.
- Add tags to the StyleBooks.

Default and custom StyleBooks

- **Default StyleBooks** are the StyleBooks shipped with NetScaler Console and they allow you to create configurations that you can deploy on your NetScaler instances. You can't delete default StyleBooks, but you can hide them from the NetScaler Console GUI.
- **Custom StyleBooks** are your own StyleBooks that you imported in to NetScaler Console.

Both default and custom StyleBooks can be either public or private.

Public and private StyleBooks

StyleBooks from which you can create config packs can be categorized as **public** StyleBooks. That is, they are all available for your direct usage to create configurations from the NetScaler Console GUI and APIs.

But, some StyleBooks are used as building blocks for other StyleBooks. Such StyleBooks are marked as **private**. The private StyleBooks cannot be directly used to create config packs from the NetScaler Console GUI. But, you can still display and view these StyleBooks on NetScaler Console. To mark any of your custom StyleBooks as **private**, set the private attribute in the StyleBook to **true**. You can still use private StyleBooks to create config packs using the NetScaler Console APIs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example of a StyleBook marked as private

```
name: basic-lb-config

namespace: com.example.stylebooks

version: "0.1"

display-name: Load Balancing Configuration

description: |

    This StyleBook defines a simple load balancing configuration and is a
building block to build other load balancing configurations.

schema-version: "1.0"

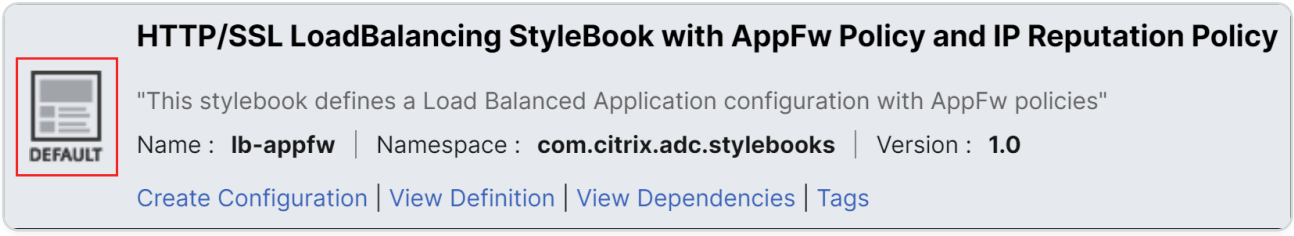
private: true
```

View StyleBooks

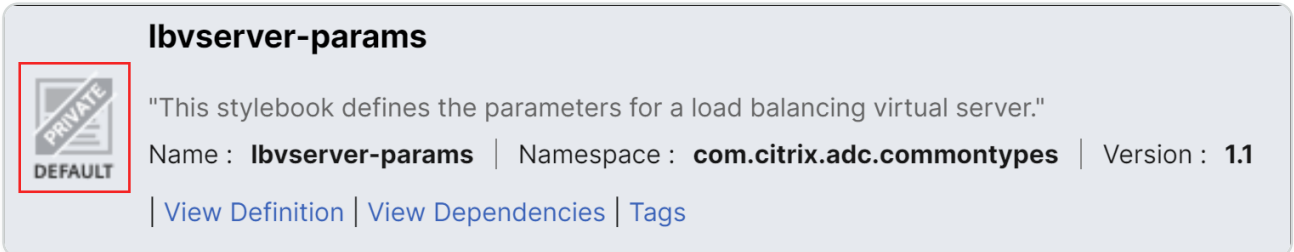
The number of StyleBooks - both default and private are increasing in NetScaler Console. You might want to search for the particular StyleBook that you want to access. You might also want to view both types of StyleBooks separately.

In NetScaler Console, when you navigate to **Applications > Configuration > StyleBooks**, you can view a list of StyleBooks that are present in the system.

A default public StyleBook has the following icon on its panel:



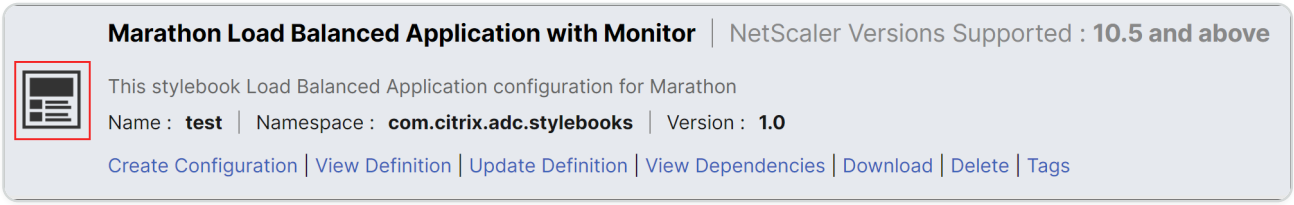
While a default private StyleBook has an icon that declares it as a private StyleBook:



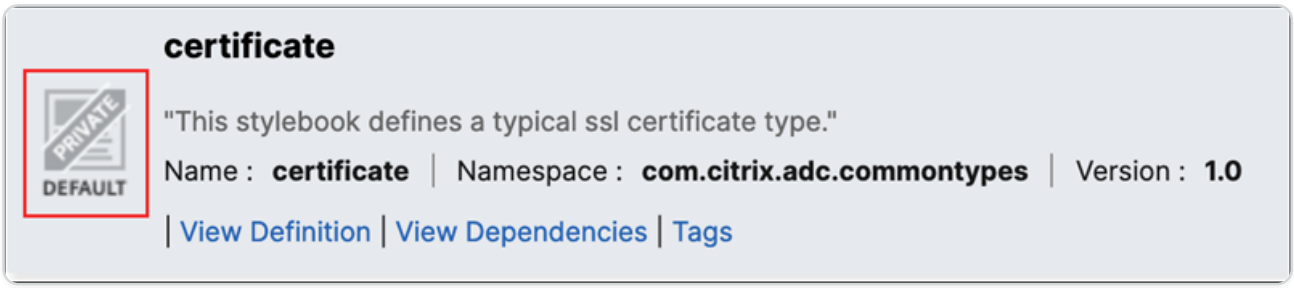
© 1997–2026 Citrix Systems, Inc. All rights reserved.

While you can view the definition and dependencies of a private StyleBook, you cannot create a config pack from a private StyleBook using the GUI. The main purpose of a private StyleBook is to use it as a building block for another StyleBook. Using the building-blocks-StyleBooks encourages the reuse of common configuration patterns.

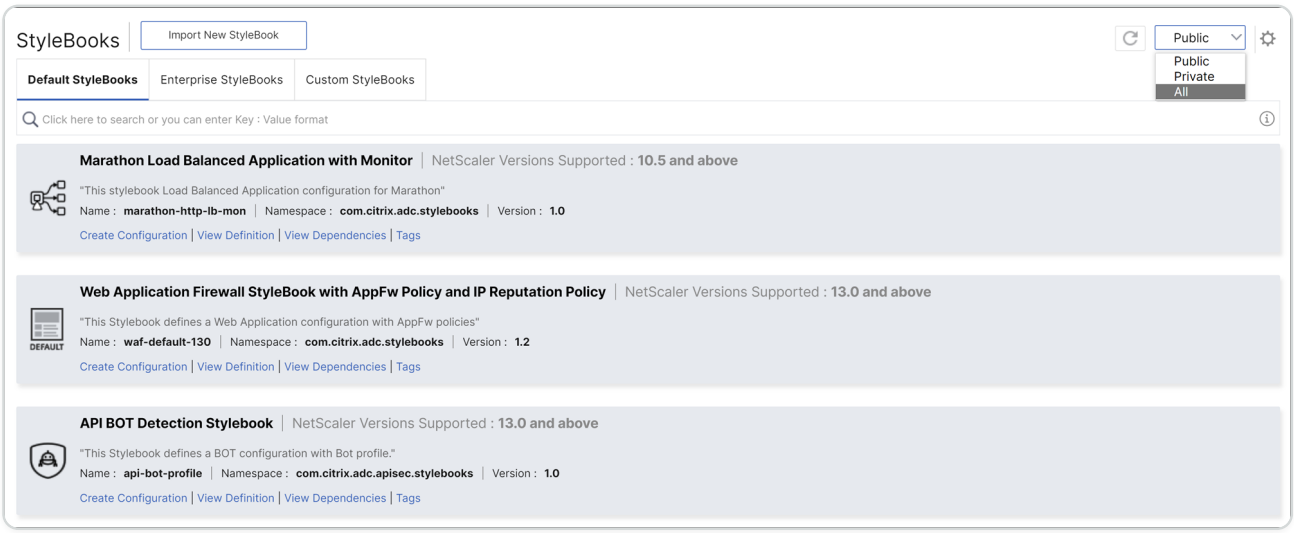
A custom public StyleBook has a different icon as shown in the following image:



While a custom private StyleBook appears with this icon:

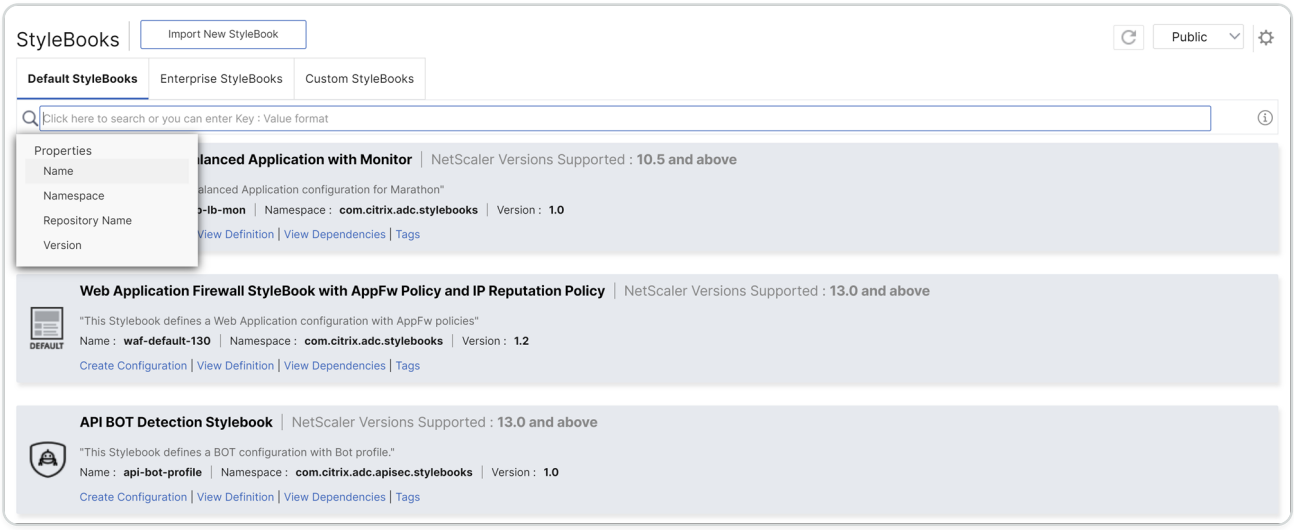


At the top right-side of the page, you can see an option to select the type of StyleBooks to view. There are three options - all, public, or private StyleBooks. Click one of the options.



You can also search for a particular StyleBook by clicking the search icon. You can search by name, namespace, and version attributes or a combination of these options. The search operation is not case-sensitive.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

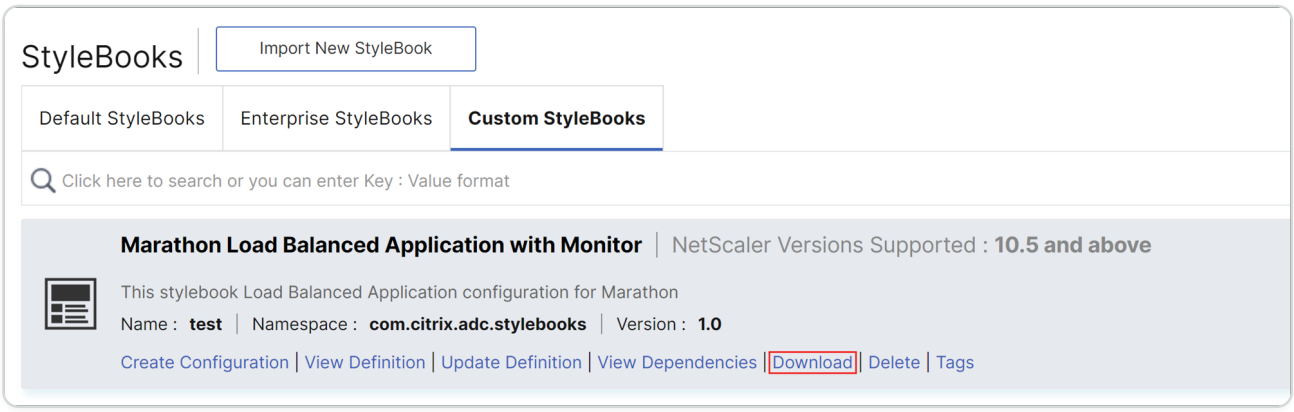


Download custom StyleBooks

To download the custom StyleBooks from NetScaler Console, navigate to **Applications > Configuration > Confg Packs**. In the list of StyleBooks that are displayed on the right-side panel, check the option to download the custom-defined StyleBooks. Click **Download**. If the StyleBook has dependent custom StyleBooks, you can include the dependent StyleBooks in the downloaded bundle.

NOTE

You can download custom StyleBooks that are marked as either public or private.



NOTE

You cannot download the NetScaler Console default StyleBooks. You can view their definitions and dependencies. To do so, click **View Definition** and **View Dependencies** links on the StyleBook panel.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Update custom StyleBook

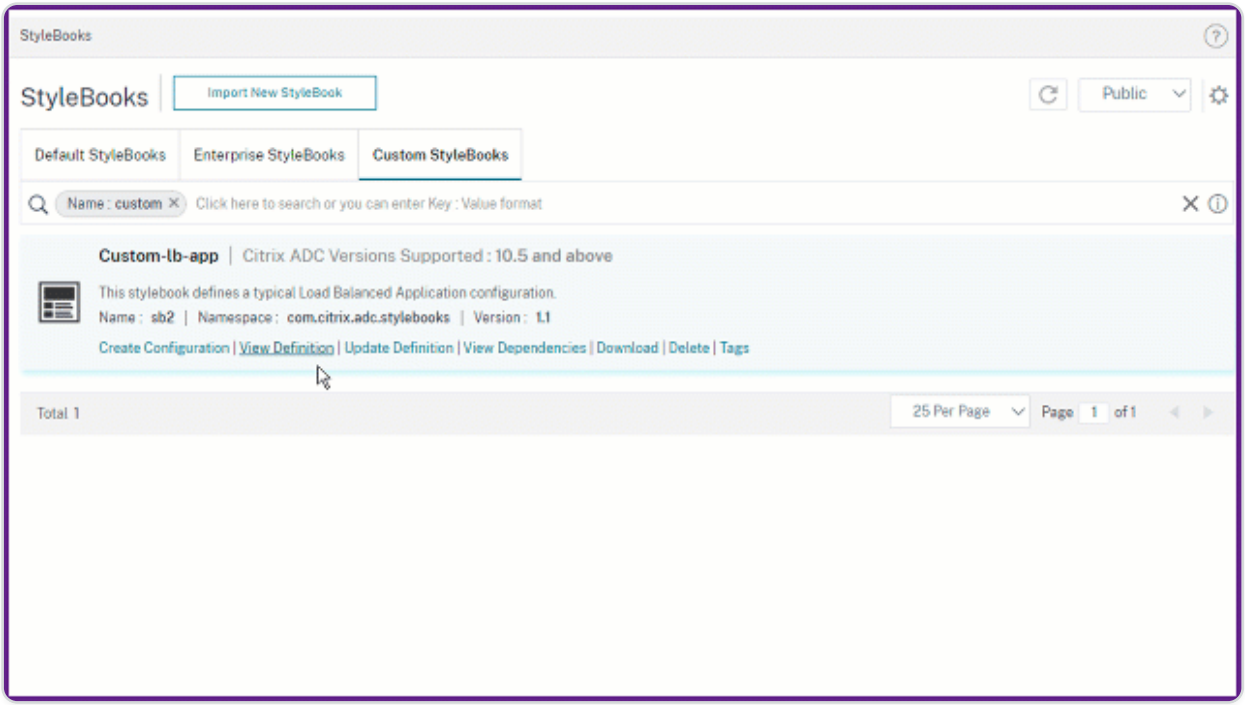
You can update the custom StyleBook definitions from the NetScaler Console GUI itself. So, you can change the StyleBook without changing its version. You can also update the definitions imported from a StyleBook bundle.

IMPORTANT

Before you update the StyleBook definition from the NetScaler Console GUI, ensure the StyleBook definition has no dependent StyleBooks.

You can update a StyleBook definition that has config packs. Ensure that the StyleBook definition is backward compatible. So, all parameters are kept in the updated StyleBook and the newly added parameters appear as optional.

1. Navigate to **Applications > Configuration > StyleBooks**.
2. Select the **Custom StyleBooks** tab.
3. Select **Update Definition** on the StyleBook that you want to update.
4. Update the definition as required and click **Update**.

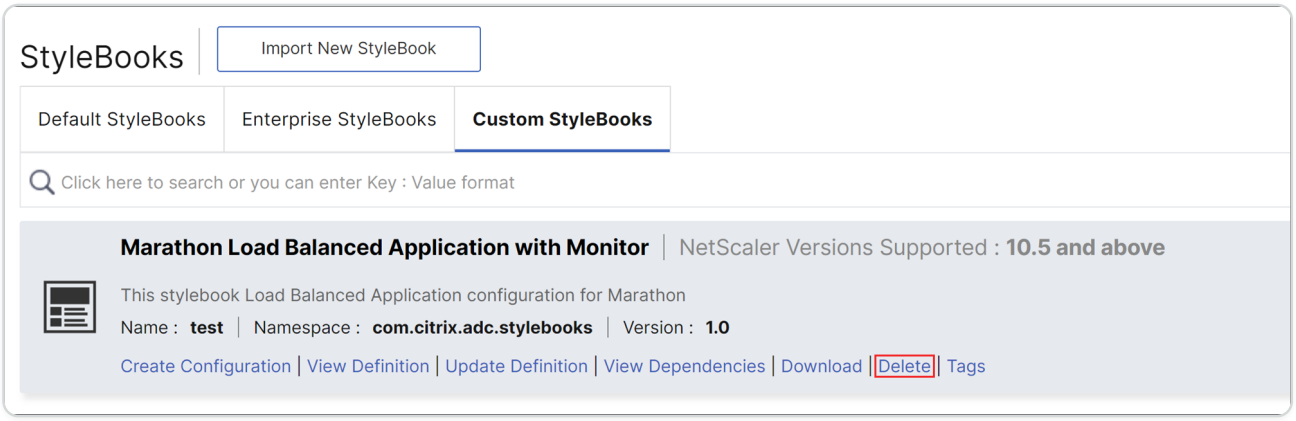


5. Refresh the page to see the latest changes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Delete custom StyleBooks

You can also delete a custom StyleBook by clicking the **Delete** button. A pop-up window prompts you to confirm if you want to remove the StyleBook from NetScaler Console. If the StyleBook uses other custom StyleBooks, you can choose to remove such StyleBooks by selecting the checkbox.



NOTE:

Do not delete a custom StyleBook if it has dependent StyleBooks in NetScaler Console. This action can break the existing StyleBooks.

View StyleBook dependencies

An important and powerful feature of StyleBooks is that they can be used as building blocks for other StyleBooks.

You can:

- **Import a StyleBook into another StyleBook** - An imported StyleBook is declared as a type and is used by the components or parameters of the second StyleBook. View the existing default StyleBooks in NetScaler Console to learn how a StyleBook can be built on top of another StyleBook.
- **View a graphical display of how StyleBooks are connected with each other** - This representation is useful for complex StyleBooks that are built using other StyleBooks as building blocks. The dependency graph allows you to see the relationships and dependencies among the StyleBooks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

You cannot delete a StyleBook that is used by other StyleBooks because this action can break the existing StyleBooks. Use the dependency graph display to identify which StyleBooks are preventing the removal of a StyleBook.

To view StyleBook dependencies

In NetScaler Console, navigate to **Applications > Configuration > StyleBooks**. The StyleBooks page displays all the StyleBooks available for your use in NetScaler Console. Scroll down and find your StyleBook. Click **View Dependencies** to view the dependent StyleBooks.

Forward dependencies

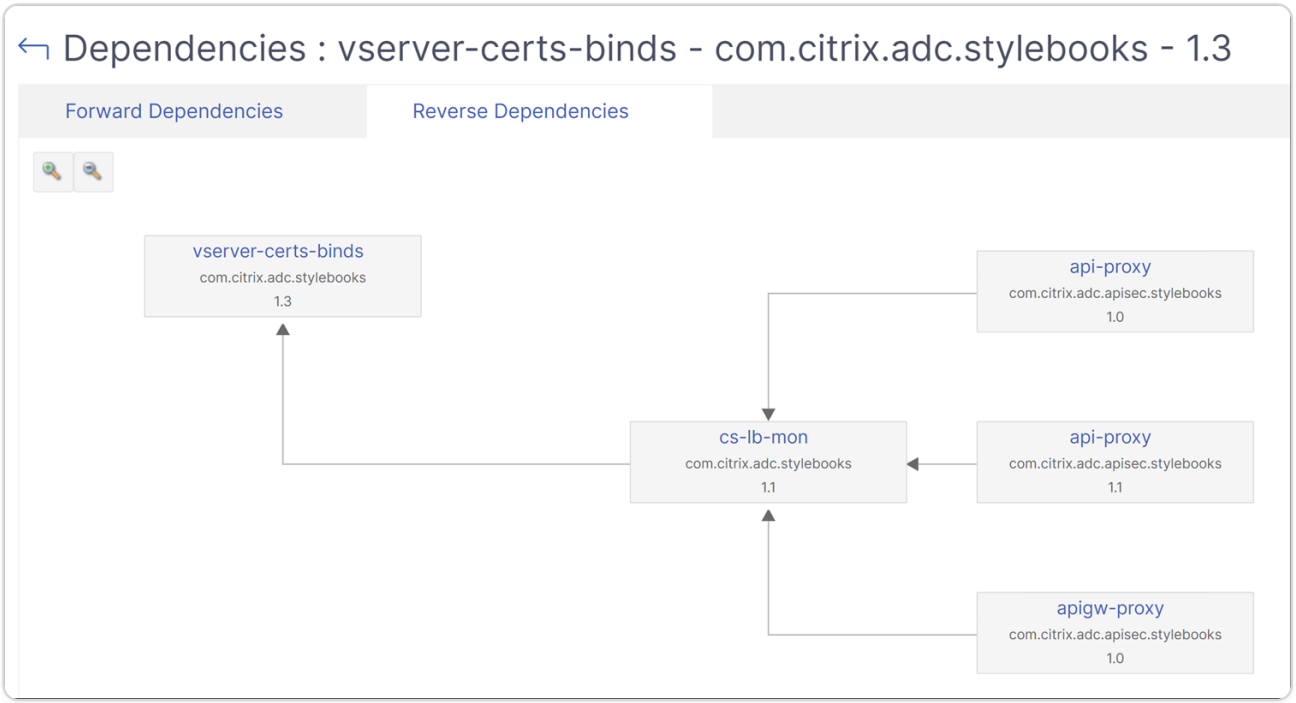
The **Forward Dependencies** tab allows you to view the different default StyleBooks that your StyleBook is using. Follow the arrows to find the StyleBook that a StyleBook is using. When you point your mouse to one of the arrows, the arrow and the StyleBooks that are connected to one another are highlighted. You can also click a StyleBook to view the definition of that StyleBook.



Reverse dependencies

The **Reverse Dependencies** tab allows you to graphically view the StyleBooks that are using your StyleBook. If you follow the arrows, you can see that all the StyleBooks in the display point towards your StyleBook. Some StyleBooks might be directly using the StyleBook and some StyleBooks might be using the StyleBook through another StyleBook.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Audit NetScaler configuration against config packs

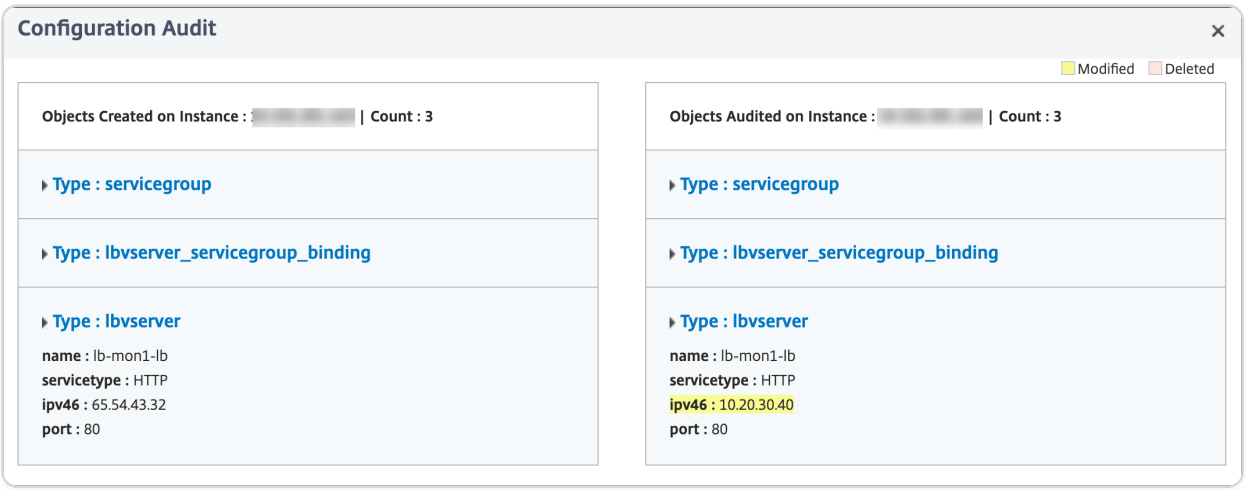
You can compare the changes made by a StyleBook config pack to the current NetScaler configuration. With this comparison, you can do the following:

- Detect the configuration drift between StyleBook config pack and NetScaler configuration.
- Identify any modified and deleted objects on the NetScaler that do not display the changes made by the config pack.

To compare the config pack changes to the NetScaler instance configuration, do the following:

1. Navigate to **Applications > Configuration > Config Packs**.
2. Click **Configuration Audit**.

   The Configuration Audit page displays the objects created and audited.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

While updating a StyleBook config pack that is deployed on a NetScaler instance, it can have differences from its deployed state. And, it fails the config pack update. The StyleBook engine automatically reconciles these differences and updates the config pack.

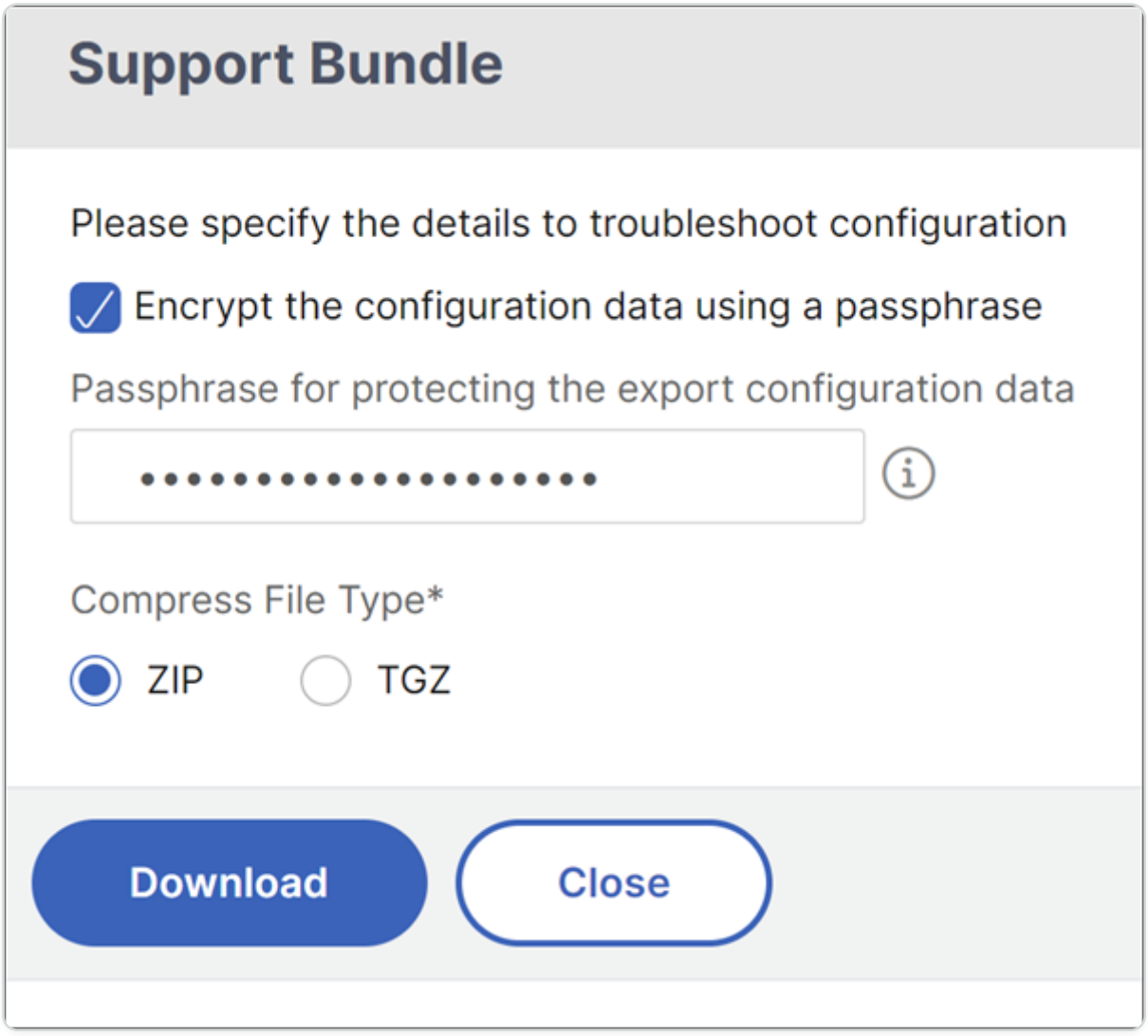
Download the support bundle of a config pack

The support bundle of a config pack helps the Citrix technical support team to view, analyze, and troubleshoot config pack issues. To download the support bundle, do the following steps:

1. Go to **Applications > Configuration > Config Packs**.
2. Select the config pack to which you want to download the support bundle.
3. In **Select Action**, click **Support Bundle**.

   You can compress the bundle in Zip or TGZ file format.
4. Optional, specify the passphrase to encrypt the bundle file.
5. Click **Download**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

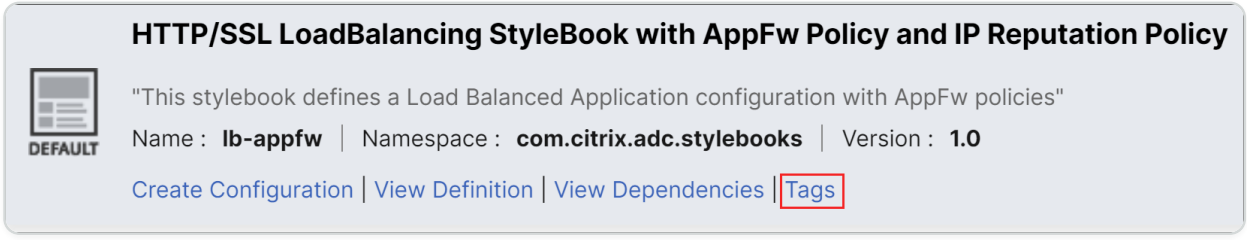


Create a tag for the StyleBook

You can add tags to any StyleBook in NetScaler Console. Tags are key-value pairs that allow you to group StyleBooks using different criteria. You can use these tags while searching or filtering for StyleBooks in NetScaler Console.

To add a tag to the StyleBook:

1. Navigate to **Applications > Configuration > StyleBooks**.
2. Select **Tags** on the StyleBook for which you want to add tags.

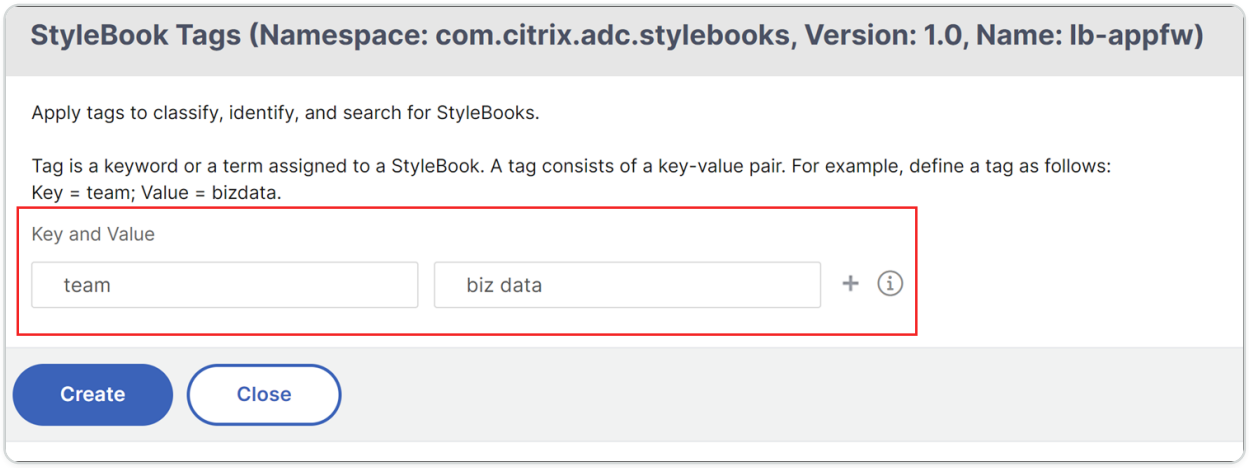


You can add tags to all types of StyleBooks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Specify the required **Key** and **Value** information that helps you filter the StyleBook.

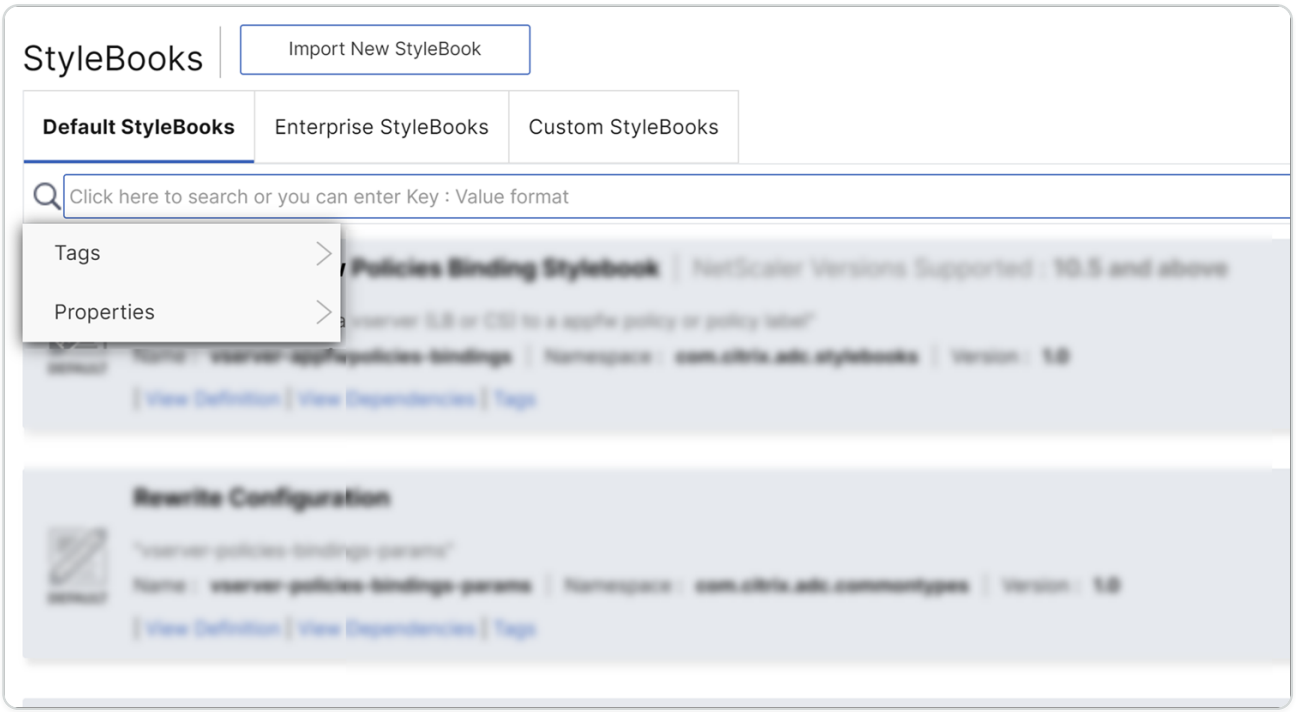
   For example, Key=team and Value=bizdata



   To add more tags, click **+**.

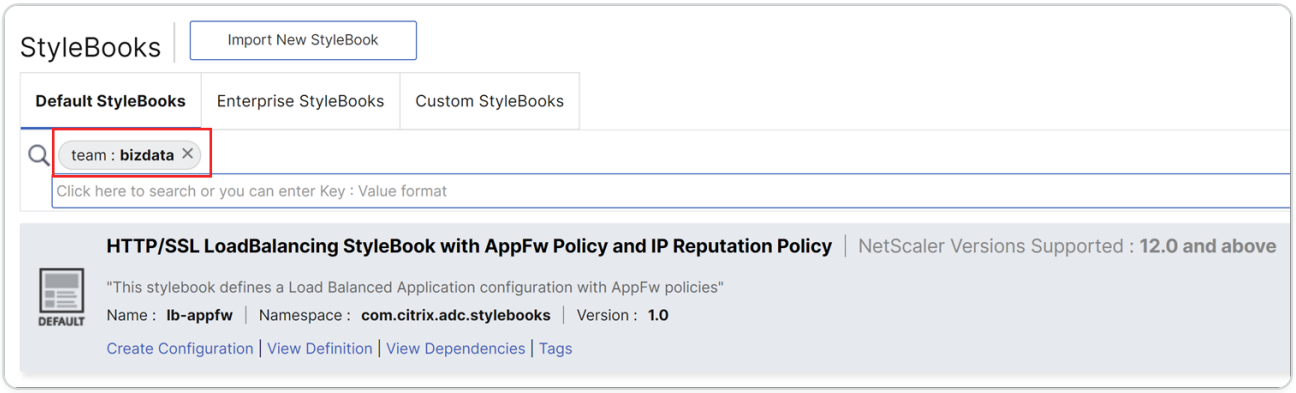
4. Click **Create**.

To filter StyleBooks using tags, click **Tags** in the search bar and select a key and a value from the list. The StyleBooks match the specified tag are displayed.



The following is an example search for the StyleBooks that have a tag where `key=team` and `value=bizdata`:

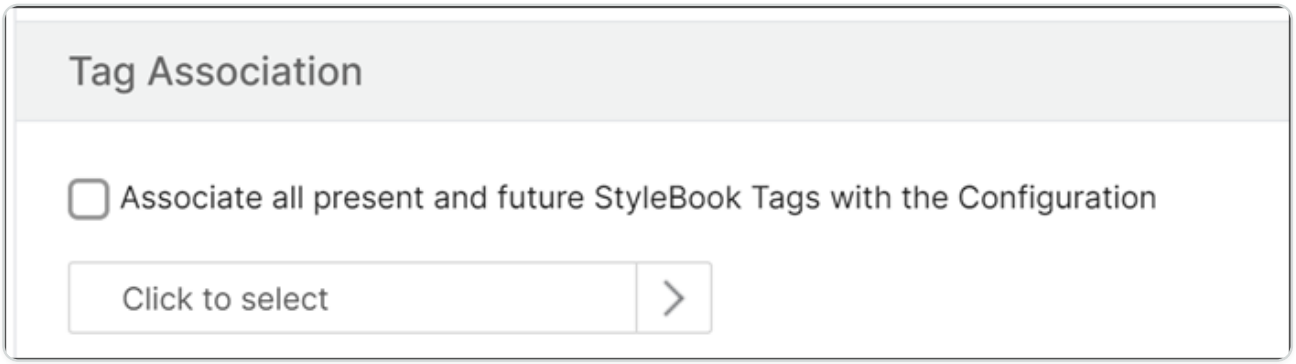
© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can associate the StyleBook tags to its config pack. So, you can search the config packs using the StyleBook tags itself.

When you create a config pack, use one the following options in the **Tag Association** section:

- **Associate all present and future StyleBook tags with the configuration** – This option associates all the StyleBook tags to a config pack. It also makes sure to associate the new tags that you might add to the StyleBooks in future.
- **Select tags** – This option displays the tags of the selected StyleBook. You can select the required StyleBook tags and associate with a config pack.

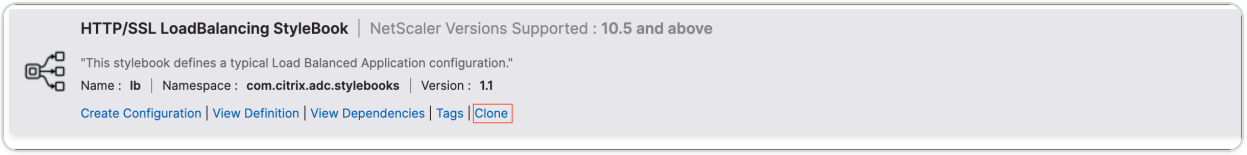


Clone a StyleBook

As admins, you can create a duplicate of a StyleBook, together with their dependent StyleBooks. You can then use this bundle for customization such as updating the `parameters` and `components` sections.

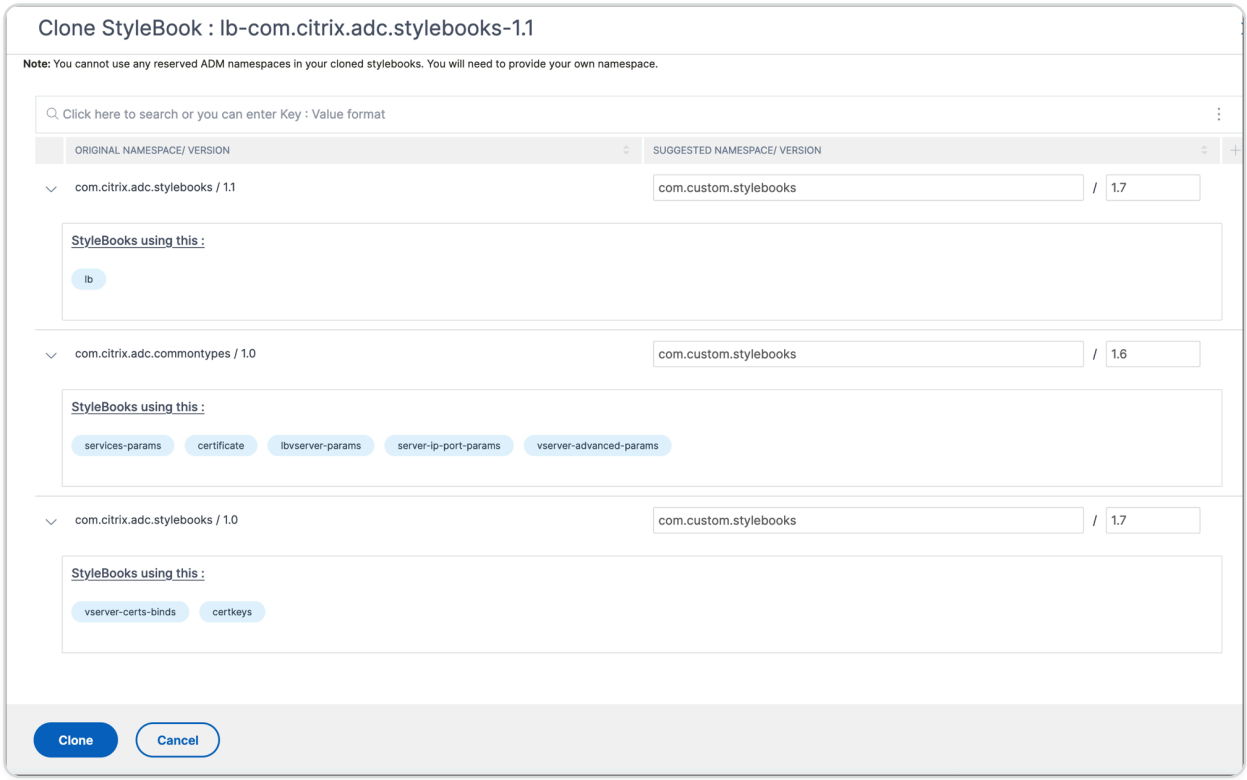
To clone a StyleBook:

1. Navigate to **Applications > Configuration > StyleBooks**.
2. Select **Clone** on the default or custom StyleBook which you want to duplicate.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. In the **Clone StyleBook** page, enter a namespace and version for the StyleBook and the dependent StyleBooks. You can also choose the suggested namespaces and versions.



NOTE:

The cloned StyleBook and its dependent StyleBooks must have different namespaces and versions to differentiate them from the existing StyleBooks. You cannot use any reserved NetScaler Console namespaces for the cloned StyleBooks.

4. Click **Clone**. The cloned StyleBook package is imported to NetScaler Console and appears in the **StyleBooks** page.

Import and synchronize StyleBooks from an external repository

Consider a scenario where you are using CI/CD processes for your development. Or, a scenario where you are managing all the application source code and deployment artifacts in GitHub/ GitLab.

In the GitHub/GitLab repository, you might be maintaining several StyleBooks for deploying the NetScaler configurations and managing these StyleBooks. You must upload these StyleBooks to NetScaler Console. With this feature, you can directly import your StyleBooks present in GitHub/

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GitLab into NetScaler Console. You don't need to manually copy them from GitHub/GitLab and then upload them into NetScaler Console. Or, manually synchronize the files in both NetScaler Console and GitHub/GitLab. Also, you can import and synchronize config packs from GitHub/GitLab.

To import StyleBooks and config packs, define a repository in NetScaler Console that represents a GitHub/GitLab repository. Provide the GitHub/GitLab repository URL and your username and API or Personal Access(PA) token created in GitHub/GitLab. That means, only authorized users who have a valid account in GitHub/GitLab can import and sync StyleBooks.

You can import and synchronize the following types of repositories:

- **Publicly accessible repositories** - The repositories that are open to the public and can be accessed over the internet.
- **On-premise or private GitLab/GitHub repositories** - The repositories that are hosted privately and are typically accessible only within an enterprise’s intranet. For these repositories, you must select a NetScaler agent during the registration process. The NetScaler agent acts as a proxy to access the repositories within the enterprise’s intranet.

After creating the repository, you can sync NetScaler Console your GitHub/GitLab repository. NetScaler Console connects to GitHub/GitLab and imports StyleBooks and config packs found in that repository. NetScaler Console then validates the StyleBooks and adds them to the list of StyleBooks in NetScaler Console. StyleBooks are not added to NetScaler Console if they fail validation. You can identify and correct the errors on your StyleBooks. Then, commit the updated versions into your GitHub/GitLab repository. Later you can try importing them or syncing them again into NetScaler Console.

If you encounter the following error while creating a repository, it indicates that NetScaler Console is unable to verify the SSL certificate for the repository due to a missing or unrecognized Certificate Authority (CA) certificate:

```
certificate verify failed: unable to get local issuer certificate
```

To resolve this issue, you can manually add the required CA certificate to the NetScaler Console agent that is used for accessing the repository. Adding the required CA certificate ensures that secure connections to the external repository is properly validated.

Log in to NetScaler Console agent that is used for accessing the repository and add your CA certificate to the trusted certificate bundle `/var/mps/ca_certs/cacert.pem`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT

- StyleBooks files can be imported and synchronized from any branch of a GitHub/GitLab repository.
- You can import and synchronize StyleBooks that have dependent StyleBooks associated with them too. These dependent StyleBooks can be in the GitHub/GitLab repository or already present in NetScaler Console.
- The synchronization of StyleBooks from a GitHub/GitLab repository must be initiated manually from the NetScaler Console GUI or API. That is, currently, importing and syncing of StyleBooks does not happen automatically based on your GitHub/GitLab commit activity.
- The configuration pack file that you want to import must be in the JSON format. Also, the configuration file contents must follow the exported configuration format. Under your GitHub/GitLab repository, the files associated with the configuration pack must be in the `configpacks` folder.

You can import StyleBook files to NetScaler Console from any folder in the GitHub/GitLab repository. To import config packs, do the following:

1. Create a folder with name `configpacks` under the root directory. Make sure all files associated with configurations are in this folder.
2. In the `configpacks` folder, create a JSON file that contains the payload for the configuration pack. This payload is used to synchronize config packs. The following is an example payload:

```
{

    "config_key": "unique-key-for-configpack",



    "parameters": {

        "param-name1": "param-value1",

        "param-name": "param-value2",

        "param-namen": "param-valuen"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    },
    "stylebook": {
        "namespace": "some namespace",
        "name": "somename",
        "version": "spme-version"
    }
}
```

- `config_key` - A unique ID or name to identify a configuration pack in NetScaler Console. If you do not specify config_key, NetScaler Console auto-generates the ID on creating the configuration pack.

  If the specified ID is found in the NetScaler Console GUI, the sync action updates the configuration pack in the NetScaler Console GUI. Else, it creates a configuration pack with the specified ID.
- `parameters` - It contains all the necessary parameters to create or update the configuration pack.
- `stylebook` - It is a mandatory property in a JSON file. It contains a namespace, version, and StyleBook name with which you want to associate the configuration pack.

3. In the `configpacks` folder, keep all the files that are associated with the configuration pack such as certificates, signature files, and XML files.

Add a repository

1. In NetScaler Console, go to **Applications > Configuration > Repositories**. Click **Add**.
2. In the **Add Repository** window, enter the following parameters:

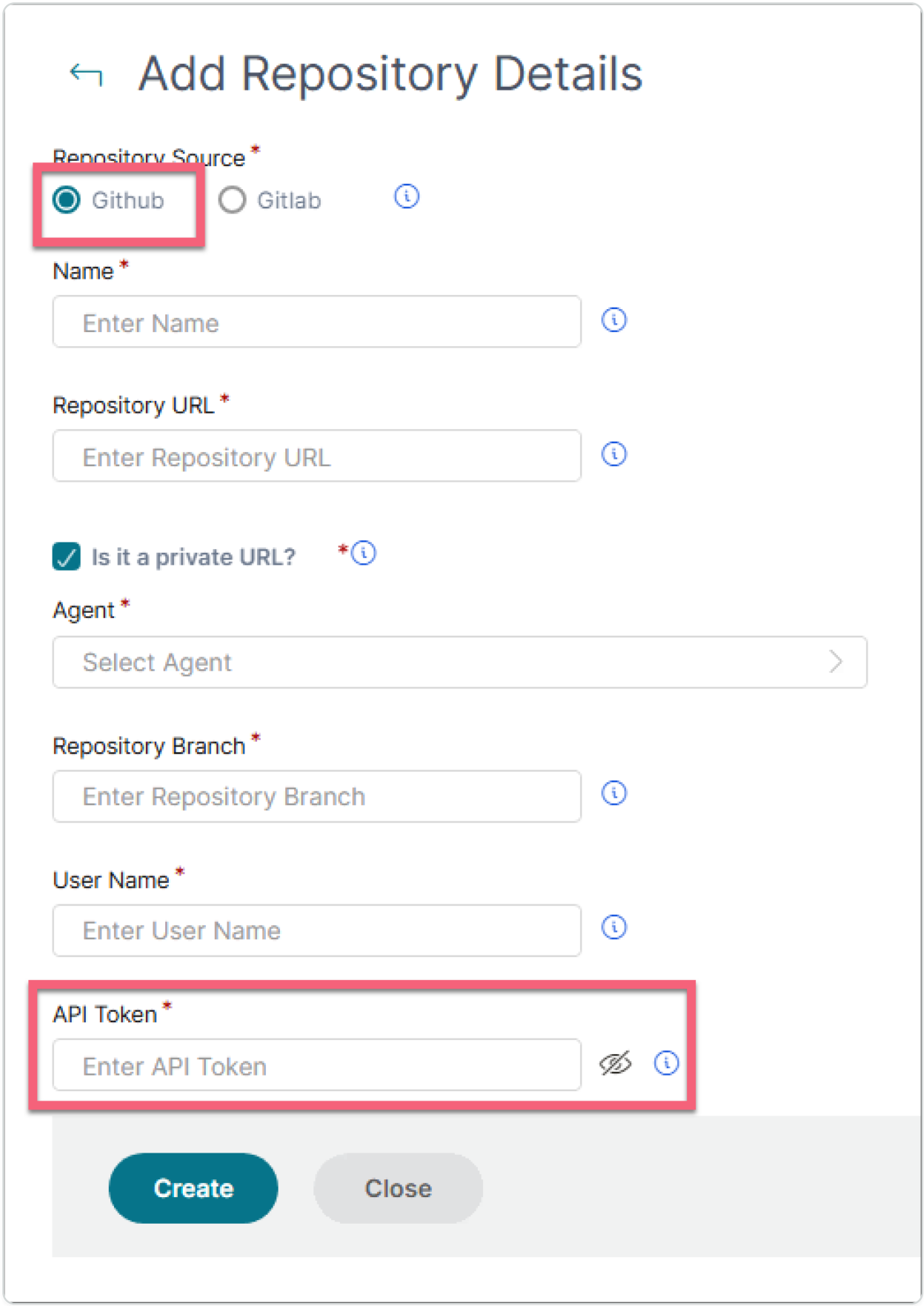
   - **Name** - Type the name of the repository. This name can be the same as the repository name in GitHub/GitLab or a different one.
   - **Repository URL** - Type the GitHub/GitLab repository URL.

     You can specify a GitHub/GitLab enterprise URL. It helps you import or synchronize StyleBooks and config packs from GitHub/GitLab enterprise accounts.

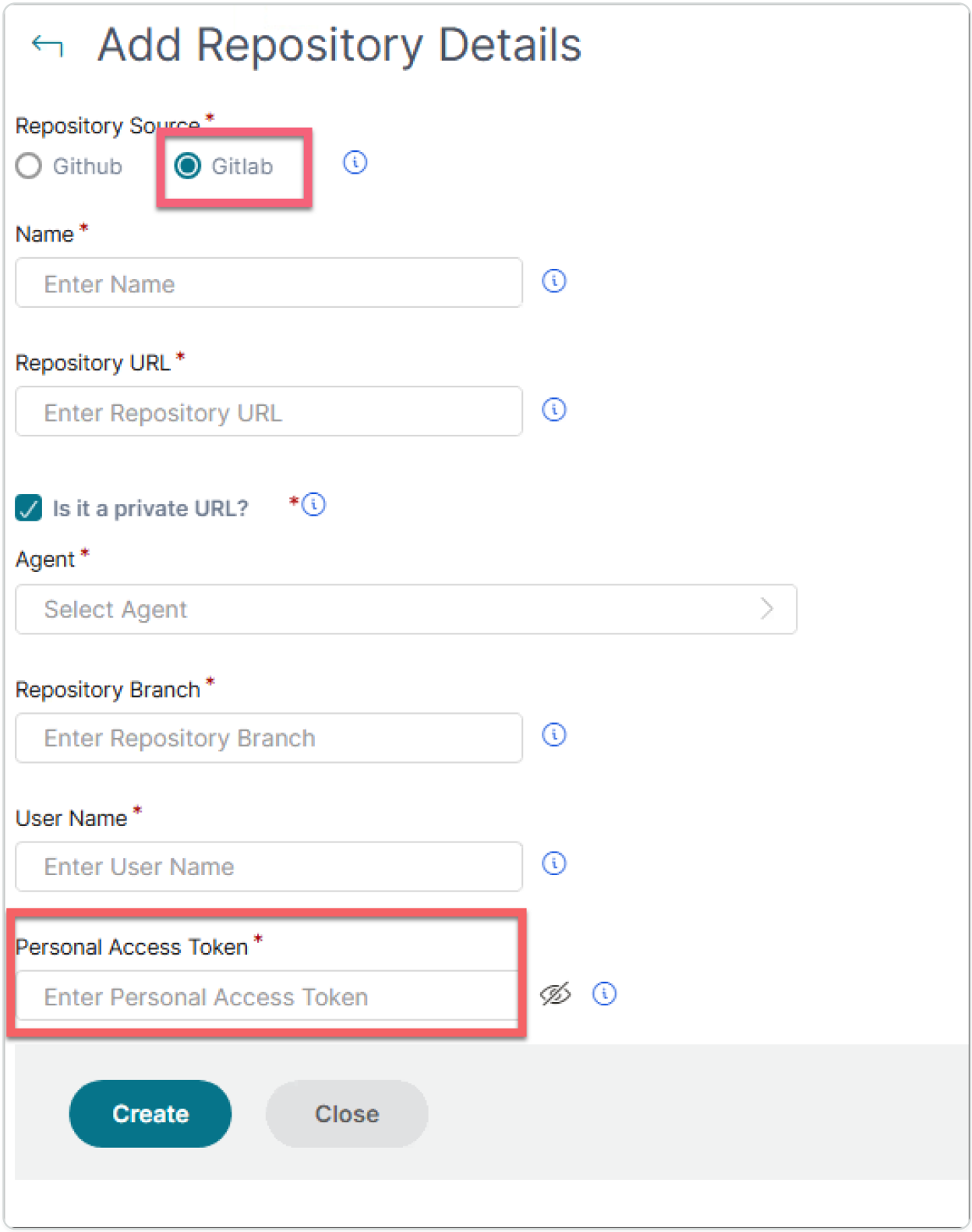
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Is it a private URL?** - If the repository is an on-premise or private GitLab/GitHub repository, select this checkbox and then select an **Agent**.
- **User Name** - Type the username that you use to access the GitHub/GitLab account or enterprise account.
- **API/PA Token** - This token is used to access your GitHub/GitLab repository. For information on how to create API/PA tokens for your GitHub/GitLab repository, see the GitHub/GitLab documentation for creating personal access tokens.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Click **Create**.

   The repository is created in NetScaler Console.

Repository options

The following are the additional options for your repositories:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Edit** - You can edit the repository URL, user name, and API token.
- **Delete** - You can delete the repository along with all the StyleBooks present in NetScaler Console that were imported previously from that GitHub/GitLab repository.

  NOTE

  You cannot delete a repository from NetScaler Console if it has any StyleBooks that have config packs associated with them. First, delete all the config packs of these StyleBooks. You can later remove the repository from NetScaler Console to clean up the StyleBooks from that repository.

- **Reset** - You can remove all StyleBooks in NetScaler Console synced from that repository without actually deleting the repository entry.
- **List files** - You can see a list of all StyleBooks present in NetScaler Console that originates from the GitHub/GitLab repository.

Steps to import StyleBooks and config packs from GitHub/GitLab

After you complete the prerequisites, follow the steps to import StyleBooks and config packs from a GitHub/GitLab repository:

1. Optional, add a repository if you haven't added.
2. Select the repository in the **Repositories** page.
3. Click **Sync**.

Use default StyleBooks

A set of default StyleBooks is provided along with NetScaler Console. When you use a default StyleBook, you have to specify values for the parameters in the StyleBook and select the IP addresses of the NetScaler instances where you want to run the configuration. After you submit the configuration, NetScaler Console validates the parameter values you have specified, creates a graph of the configuration, connects to the NetScaler instances, and runs the configuration on the instances.

NetScaler features

This table lists the StyleBooks that help you to configure virtual servers for load-balancing, content-switching, and GSLB:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

STYLEBOOK NAME	DESCRIPTION	VERSIONS
`lb`	Configure a simple load-balancing virtual server. See, Load Balancing.	1.1, 2.0
`lb-mon`	Configure a load-balancing virtual server with monitors. See, Configure monitors in a load balancing setup.	1.0, 2.0
`cs-lb-mon`	Configure a content-switching virtual server with monitors. For more information, see Content Switching.	1.0, 1.1
`lb-mon-full`	Configure a load-balancing virtual server with monitors on your NetScaler instances. Also, configure the NetScaler features like rewrite, responder, compression, and SSL ciphers.	1.0
`cs-lb-mon-full`	Configure a content-switching virtual server with monitors on your NetScaler instances. Also, configure the NetScaler features like rewrite, responder, and compression.	1.0
`gslb`	Configure one or more NetScaler instances of different sites in the GSLB setup. Before you begin, configure the SNIP IP address on NetScaler instances. This StyleBook uses the SNIP IP address as the site IP address.	1.0
`multicloud-glb`	Configure GLB for NetScaler instances. These instances	1.1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

STYLEBOOK NAME	DESCRIPTION	VERSIONS
	are deployed as GLB nodes in public clouds and on-premises data centers. You can use this StyleBook to configure GLB nodes in hierarchical deployment.	

Web Application Firewall features

This table lists the default StyleBooks for Web Application Firewall (WAF) features:

STYLEBOOK NAME	DESCRIPTION	VERSIONS
`waf-basic`	Configure a basic web application with application firewall policies.	1.2
`waf-adv`	Configure a advanced web application with application firewall policies.	1.2
`waf-default-130` and `waf-default-131`	Configure WAF and IP reputation policies for your NetScaler instances.	1.2
`lb-appfw`	Deploy a load-balancing configuration along with the application firewall and IP reputation policy on NetScaler instances.	1.0
`appfw-import-object`	Create or upload an application firewall object.	1.1
`appfw-general-settings`	Configure global settings for your application firewall. These settings apply to all applications within the NetScaler instance.	1.0

© 1997–2026 Citrix Systems, Inc. All rights reserved.

STYLEBOOK NAME	DESCRIPTION	VERSIONS
`apic-http-lb`	Create an HTTP load-balancer application through Cisco APIC.	1.0
`api-waf-profile`	Create a WAF profile in NetScaler Console. With this profile, you can configure WAF policies to an API resource.	1.0

Application Security features

This table lists the default StyleBooks for application security features:

STYLEBOOK NAME	DESCRIPTION	VERSIONS
`api-proxy`	Create an API proxy in your NetScaler instance. You can create multiple proxies with the same policy type.	1.1
`appsec-for-gateway`	Before you begin, create a custom bot signature. Configure an authentication policy using WAF and bot to protect your Gateway login page. Bind this authentication policy with your authentication virtual server.	1.0
`appsec-for-gateway-with-insights`	Before you begin, create a custom bot signature. Configure an authentication policy using WAF and bot to protect your Gateway login page with security insights. Bind this authentication policy with your authentication virtual server.	1.0

© 1997–2026 Citrix Systems, Inc. All rights reserved.

STYLEBOOK NAME	DESCRIPTION	VERSIONS
`appvserver-contentrule-networkfunction-bind`	Apply your own `contentRule` configuration to application traffic from your NetScaler instance.	1.0
`appsec-owasptop10-protection`	Create a protection configuration using WAF and bot policies. This StyleBook maps the NetScaler configurations to the OWASP top 10 vulnerabilities.	1.0

Bot management features

This table lists the default StyleBooks for bot management features:

STYLEBOOK NAME	DESCRIPTION	VERSIONS
`api-bot-profile`	Create a bot profile in NetScaler Console. With this profile, you can configure bot policies to an API resource.	1.0
`bot-signature`	Create a bot signature for your NetScaler instances.	1.2
`bot-management`	Define a web application configuration with bot policies.	1.2
`bot-general-settings`	Configure global settings of bot management checks on your NetScaler instances. For more information, see Bot Management.	1.2

NetScaler network configurations

This table lists the default StyleBooks for NetScaler network configurations:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

STYLEBOOK NAME	DESCRIPTION	VERSIONS
`adc_globalparam_configuration`	Set global parameters for your NetScaler instances.	1.0
`snmp_configuration`	Deploy SNMP configurations on a NetScaler instance. A Simple Network Management Protocol (SNMP) application helps you log NetScaler events in NetScaler Console. For more information, see SNMP Configuration.	1.0
`adv_network_configuration`	Deploy advanced network configurations like VXLAN, cluster, and more. For more information, see Networking.	1.0
`storefront`	Configure your NetScaler instances for Citrix StoreFront.	1.0
`ntp_configuration`	Configure Network Time Protocol (NTP) resources in your NetScaler instances.	1.0
`network_param_configuration`	Configure network parameters like AppAlg, ARP, Inbound NAT, and so on.	1.0
`network_configuration`	Deploy basic networking components. For more information, see Networking.	1.0
`cs-netfunc`	Configure the advanced network functions of a content-switching virtual server for your NetScaler instances.	1.0

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What's next?

To create a configuration pack from default StyleBooks, follow the steps in Create a configuration pack.

Web application firewall StyleBook

NetScaler Web App Firewall is a web application firewall (WAF) that protects web applications and sites from both known and unknown attacks, including all application-layer and zero-day threats.

NetScaler Console now provides a default StyleBook with which you can more conveniently create an application firewall configuration on NetScaler instances.

Deploying application firewall configurations

The following task assists you in deploying a load balancing configuration along with the application firewall and IP reputation policy on NetScaler instances in your business network.

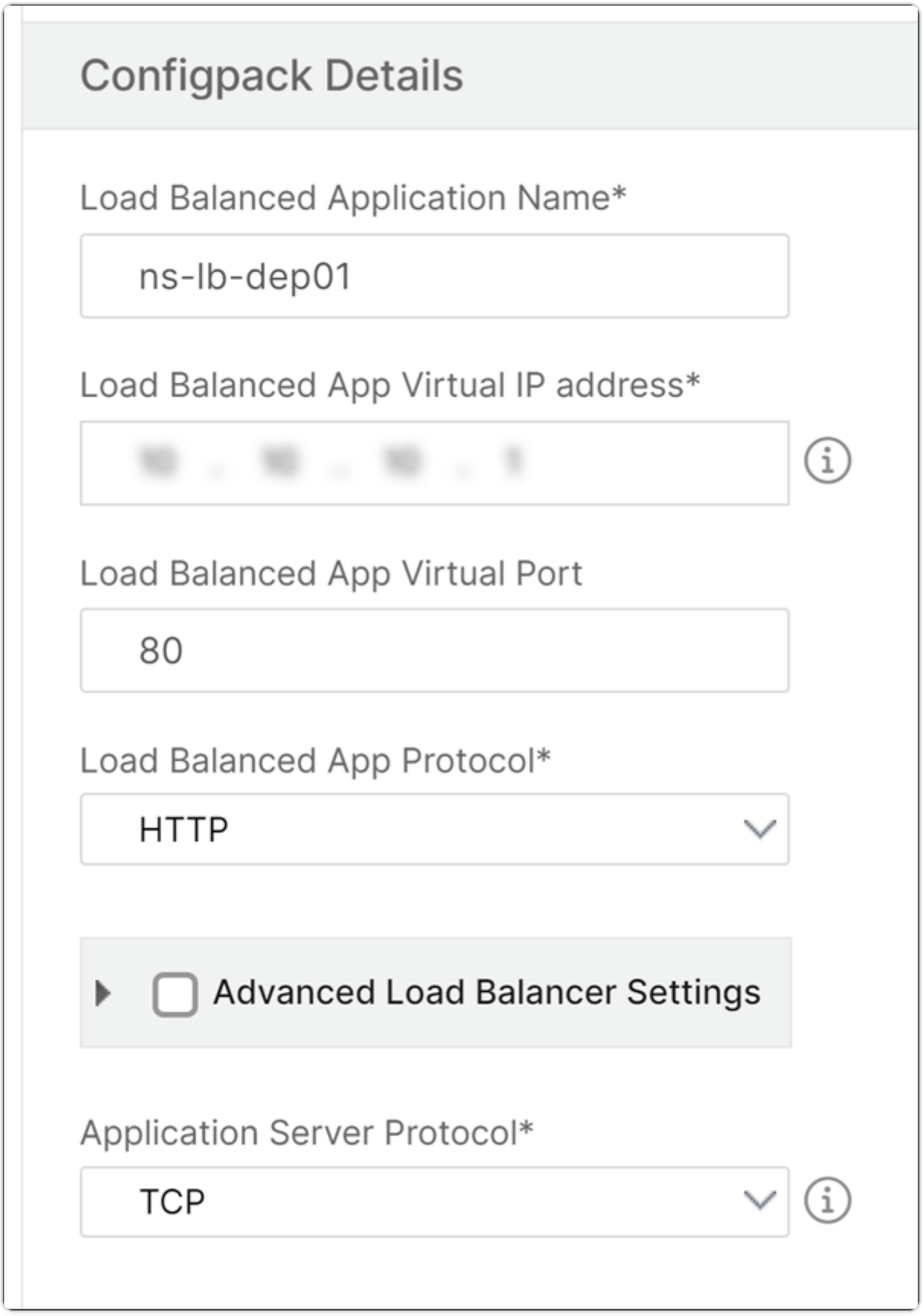
To create an LB configuration with application firewall settings:

1. In NetScaler Console, navigate to **Applications** > **Configurations** > **StyleBooks**. The StyleBooks page displays all the StyleBooks available for your use in NetScaler Console. Scroll down and find HTTP/SSL Load Balancing StyleBook with application firewall policy and IP reputation policy. You can also search for the StyleBook by typing the name as `lb-appfw`. Click **Create Configuration**.

   The StyleBook opens as a user interface page on which you can enter the values for all the parameters defined in this StyleBook.
2. Enter values for the following parameters:

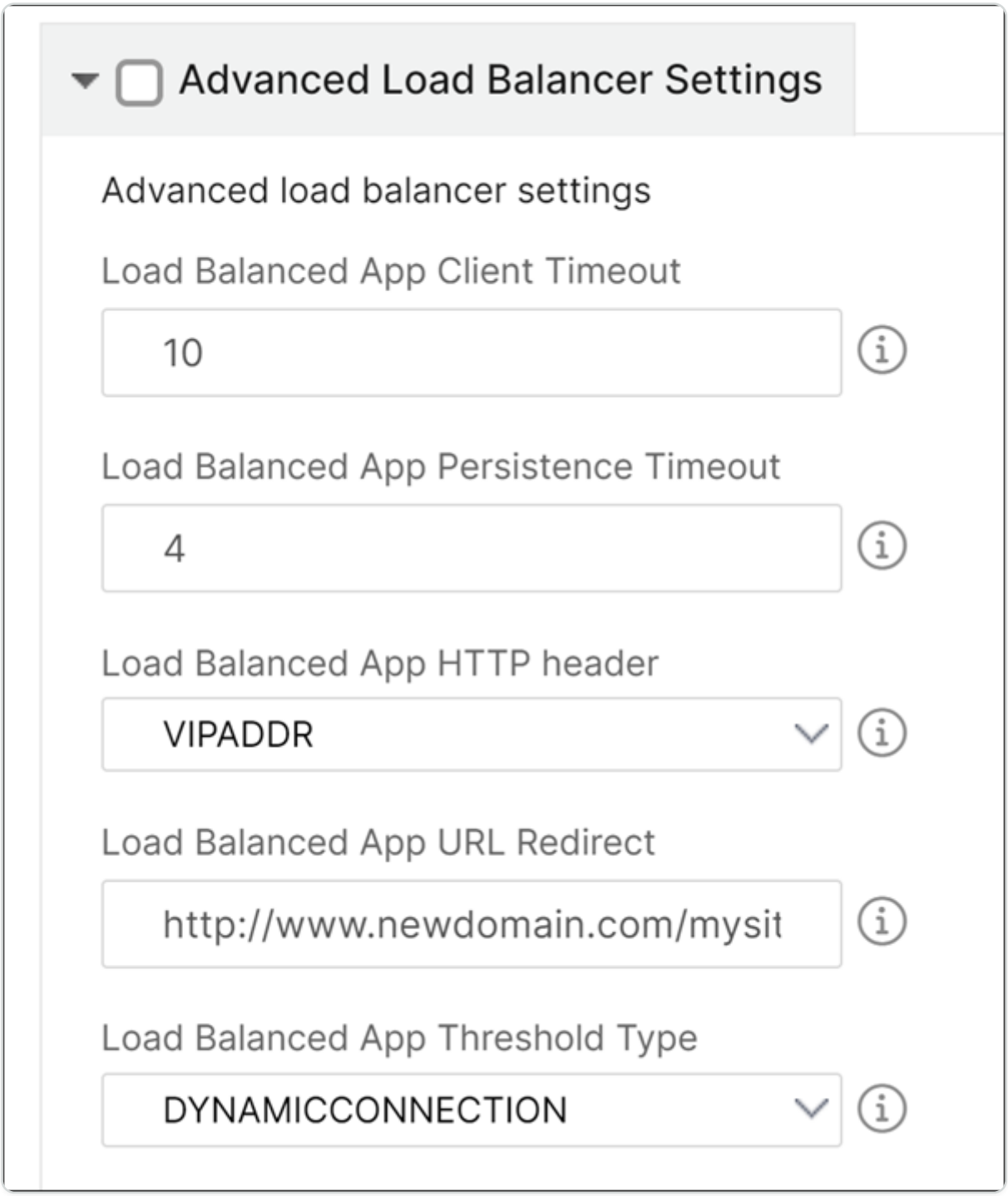
   - **Load Balanced Application Name**. Name of the load balanced configuration with application firewall to deploy in your network.
   - **Load balanced App Virtual IP address**. Virtual IP address at which the NetScaler instance receives client requests.
   - **Load Balanced App Virtual Port**. The TCP Port to be used by the users in accessing the load balanced application.
   - **Load Balanced App Protocol**. Select the front-end protocol from the list.
   - **Application Server Protocol**. Select the protocol of the application server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



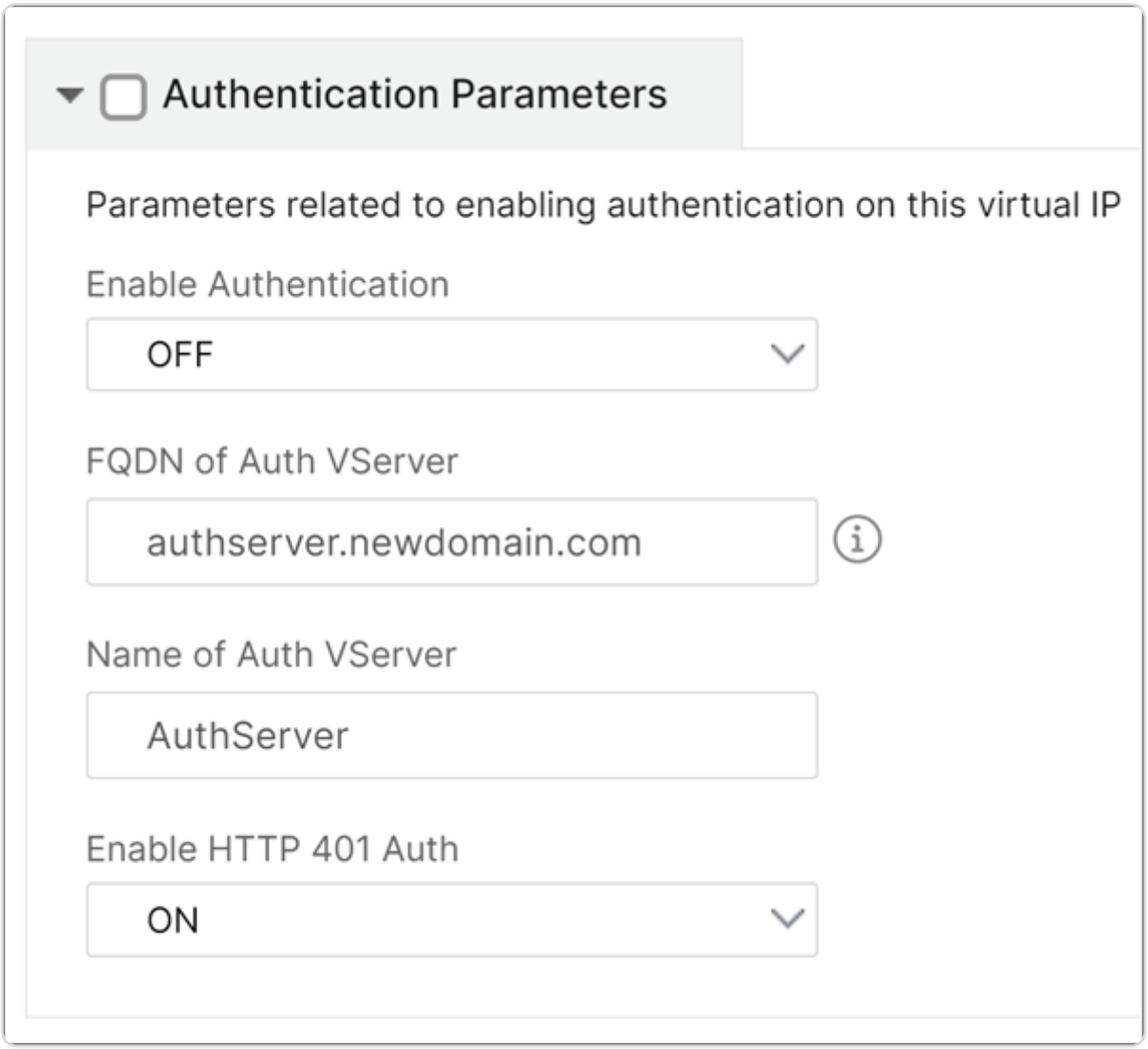
3. As an option, you can enable and configure the **Advanced Load Balancer Settings**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



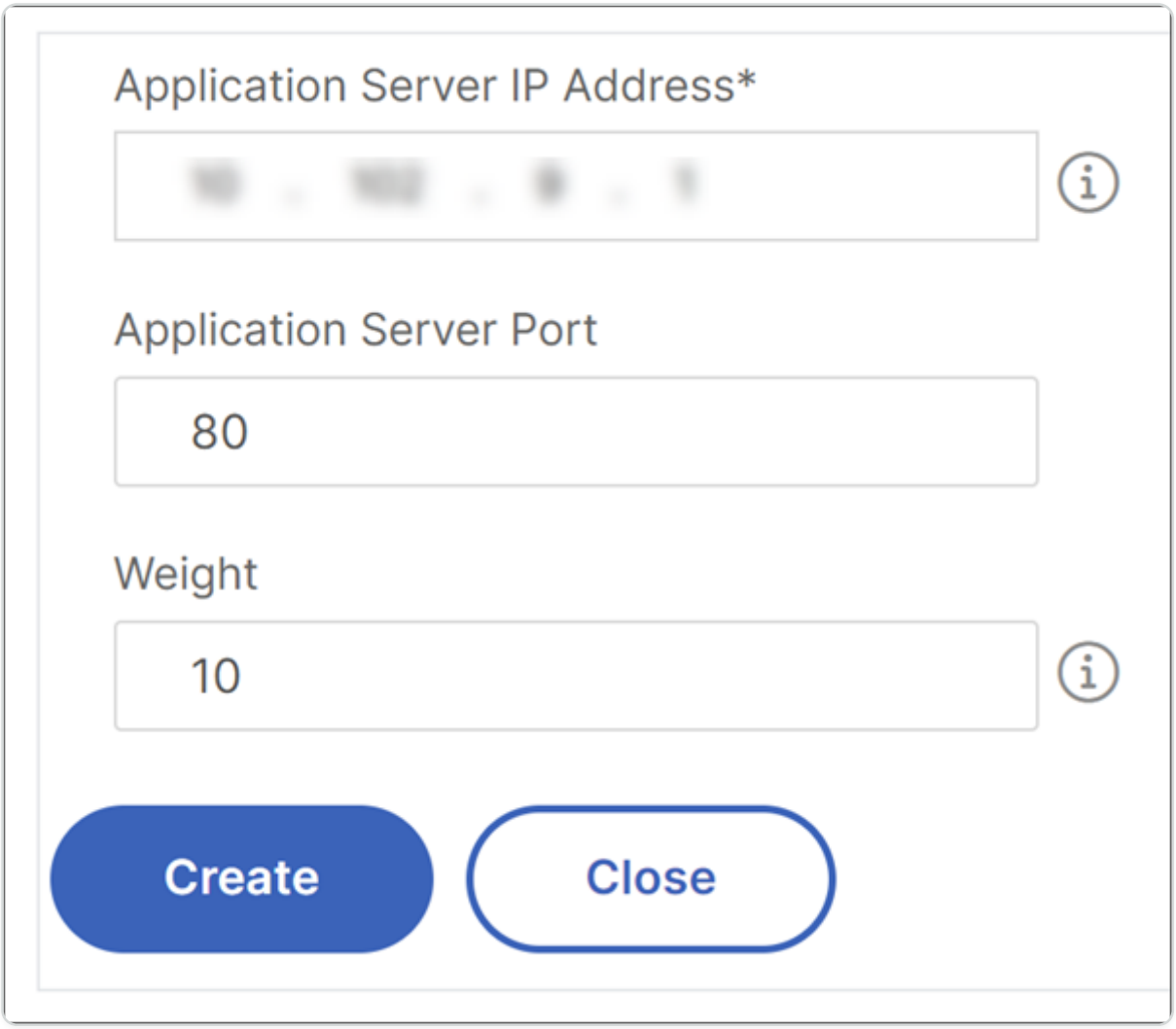
4. Optionally, you can also set up an authentication server for authenticating traffic for the load balancing virtual server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



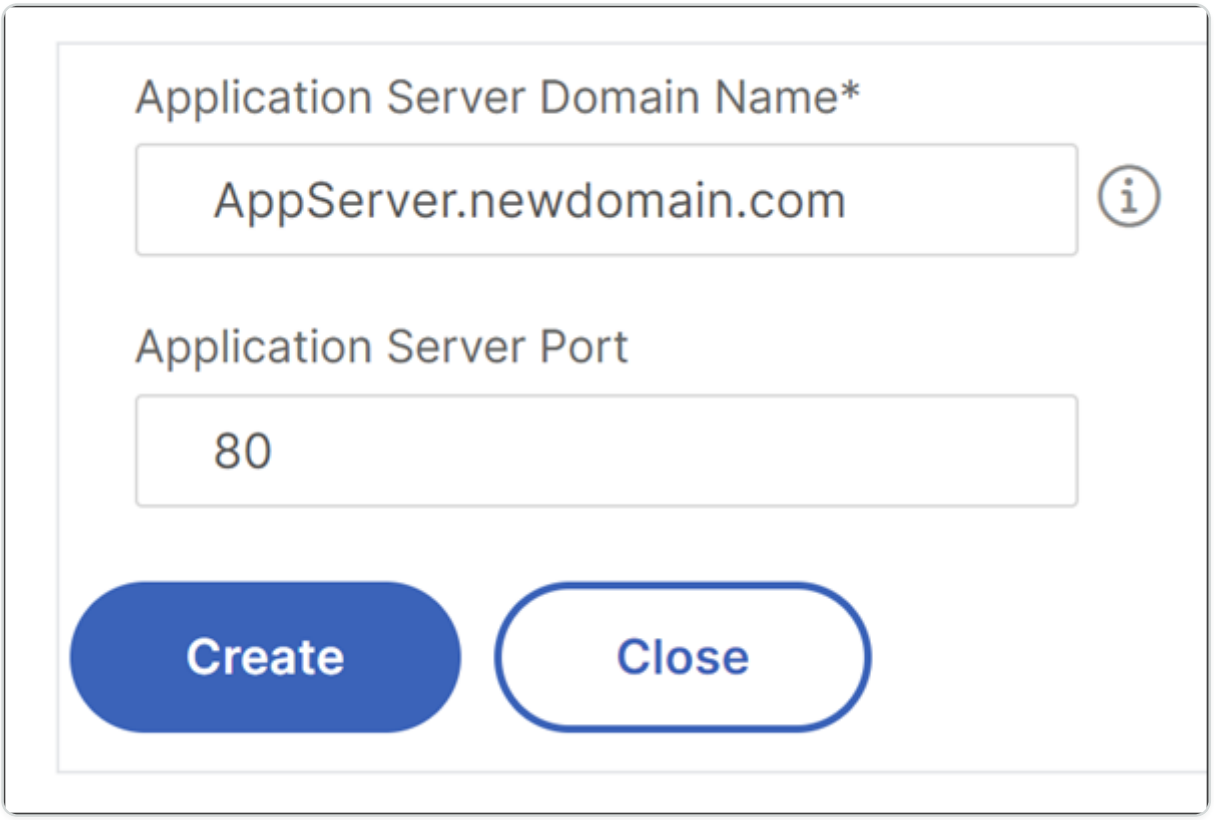
5. Click "+" in the server IPs and Ports section to create application servers and the ports that they can be accessed on.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



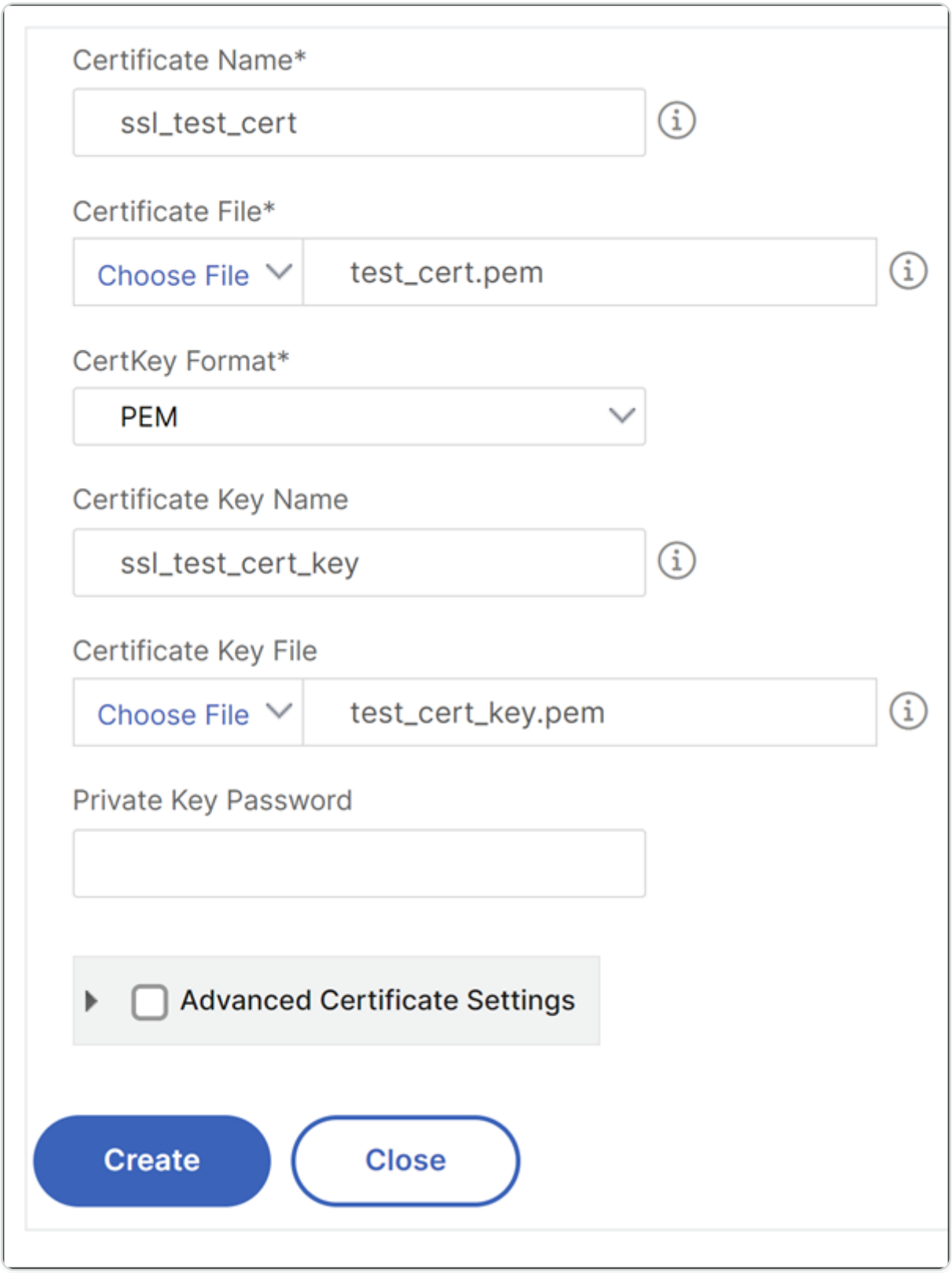
6. You can also create FQDN names for application servers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



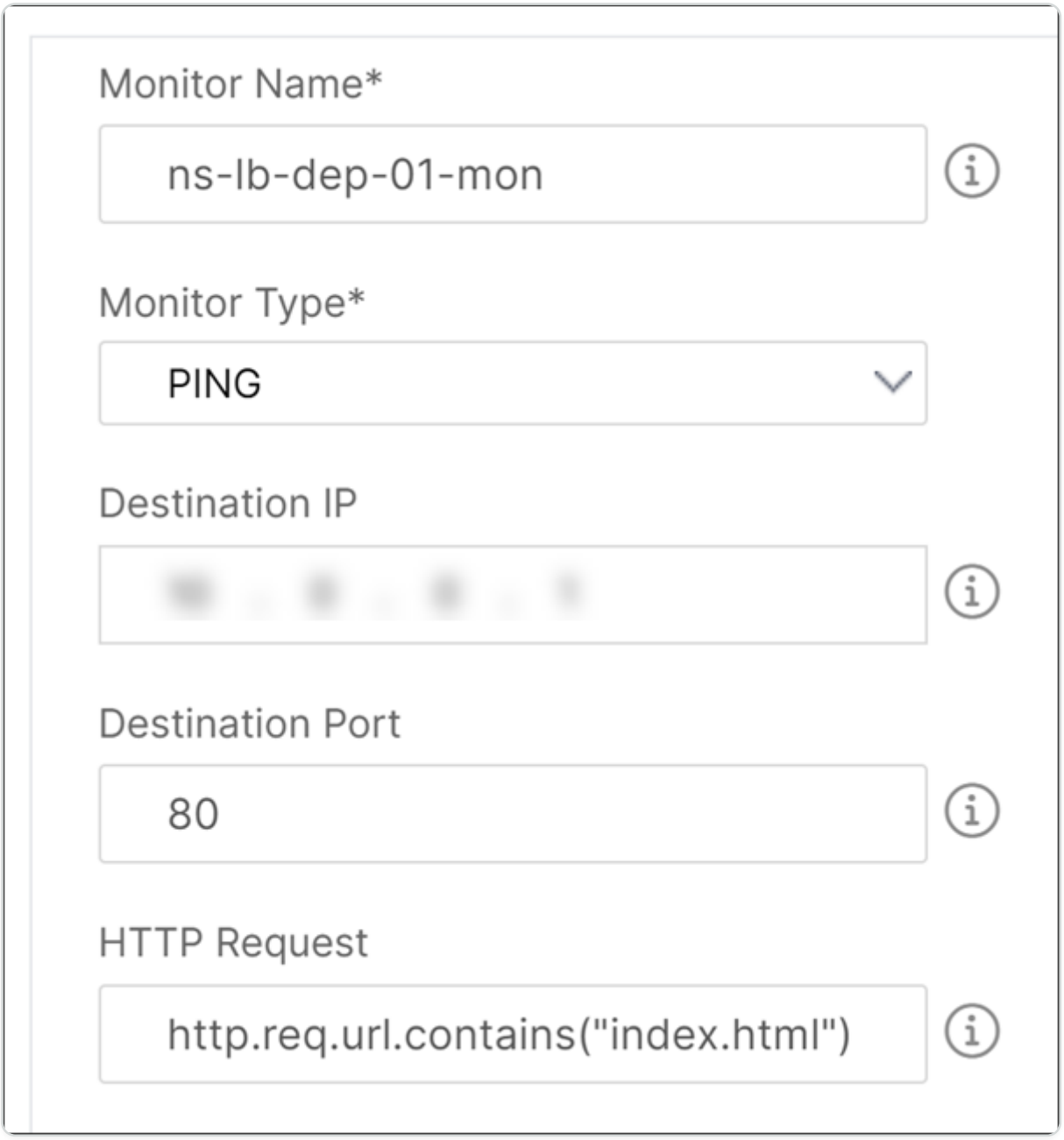
7. You can also specify the details of the SSL certificate.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. You can also create monitors in the target NetScaler instance.

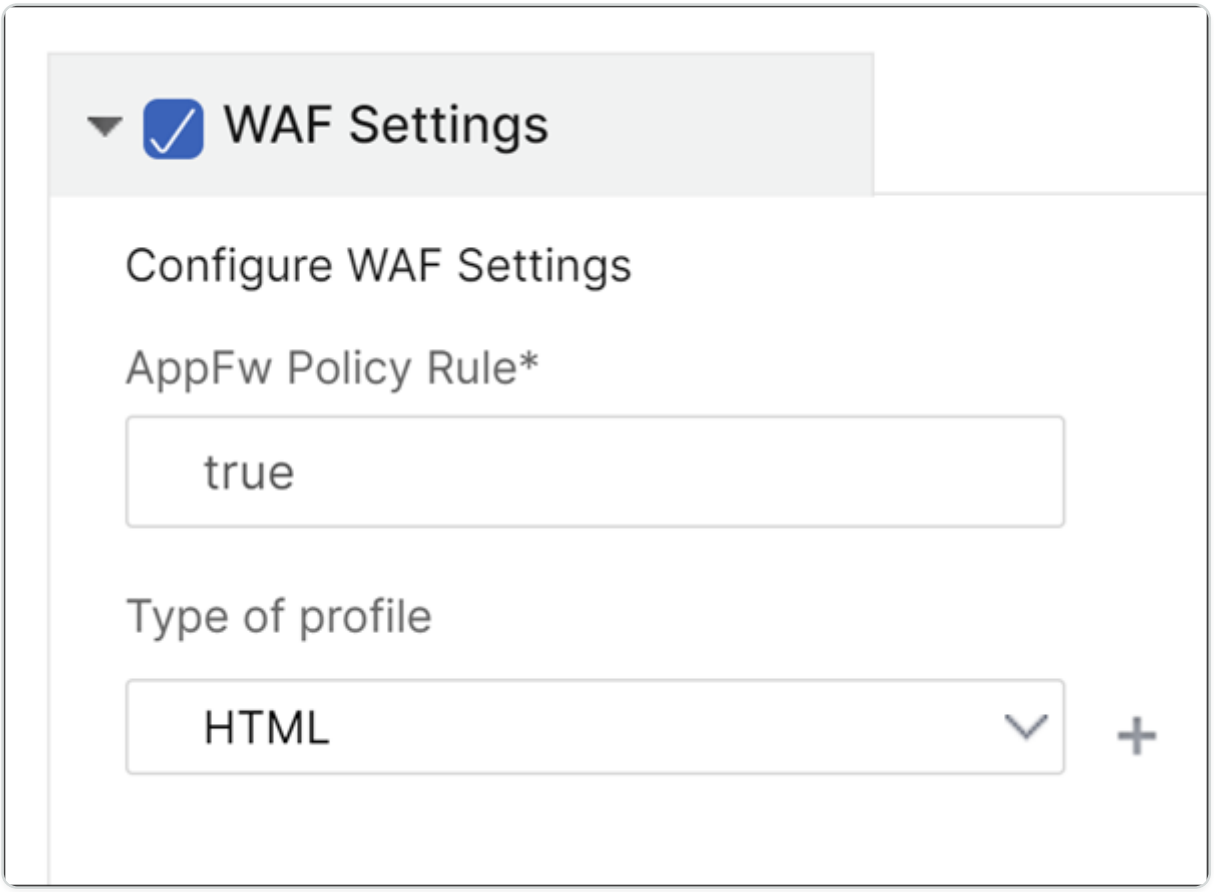
© 1997–2026 Citrix Systems, Inc. All rights reserved.



9. To configure an application firewall on the virtual server, enable WAF Settings.

   Ensure that the application firewall policy rule is true if you want to apply the application firewall settings to all traffic on that VIP. Otherwise, specify the NetScaler policy rule to select a subset of requests to which to apply the application firewall settings. Next, select the type of profile that has to be applied - HTML or XML.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



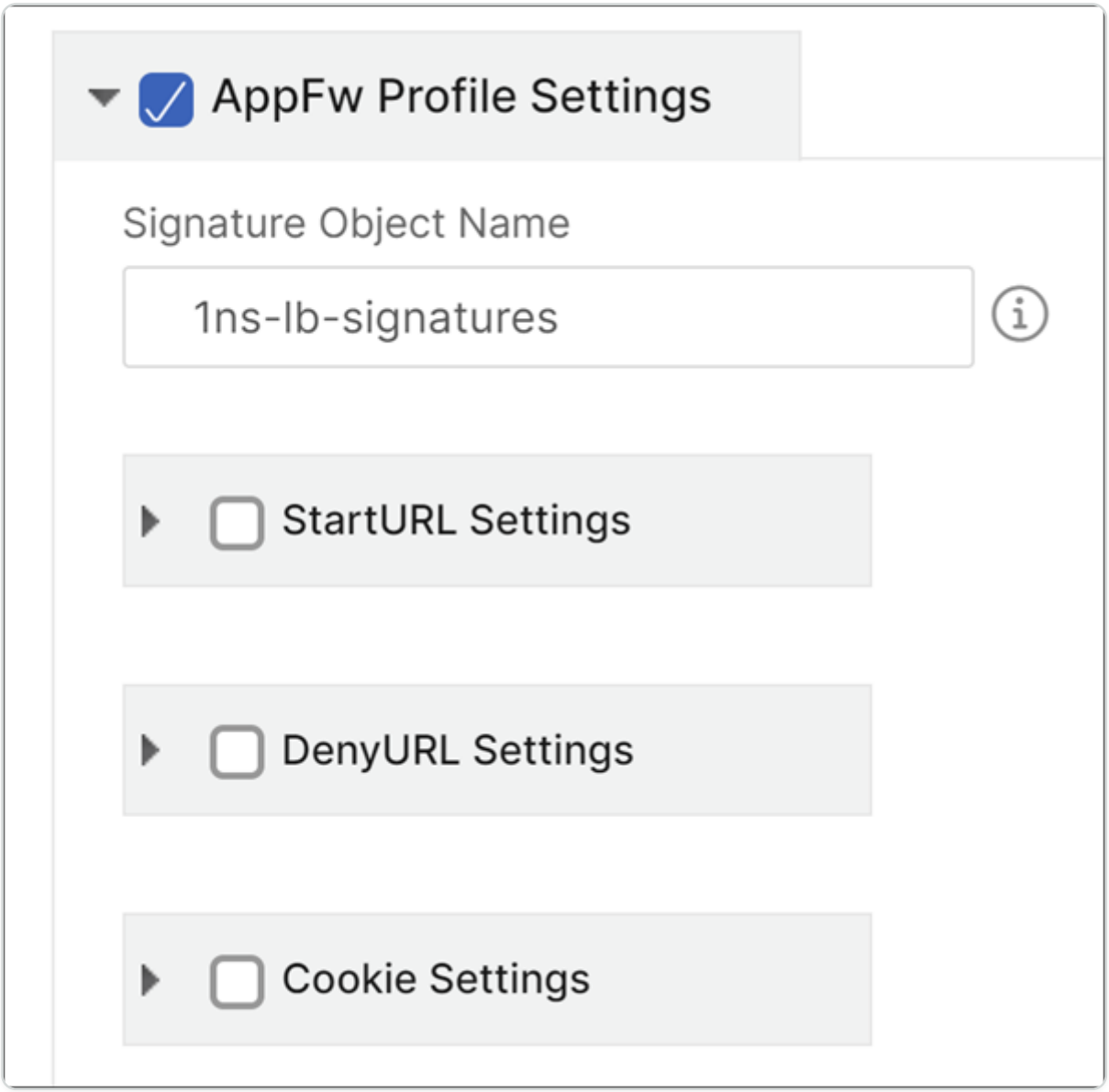
10. Optionally you can configure detailed application firewall profile settings by enabling the application firewall Profile Settings check box.
11. Optionally, if you want to configure application firewall signatures, enter the name of the signature object that is created on the NetScaler instance where the virtual server is to be deployed.

    NOTE

    You cannot create a signature object by using this StyleBook.

12. Next, you can also configure any other application firewall profile settings such as, StartURL settings, DenyURL settings and others.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For more information on application firewall and configuration settings, see Application Firewall.

13. In the **Target Instances** section, select the NetScaler instance on which to deploy the load balancing virtual server with the application firewall.

> **NOTE**
>
> You can also click the refresh icon to add recently discovered NetScaler instances in NetScaler Console to the available list of instances in this window.

14. You can also enable **IP Reputation check** to identify the IP address that is sending unwanted requests. You can use the IP reputation list to preemptively reject requests that are coming from the IP with the bad reputation.
15. Click **Create** to create the configuration on the selected NetScaler instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TIP

We recommend you to select **Dry Run** to check the configuration objects that must be created on the target instance before you run the actual configuration on the instance.

When the configuration is successfully created, the StyleBook creates the required load balancing virtual server, application server, services, service groups, application firewall labels, application firewall policies, and binds them to the load balancing virtual server.

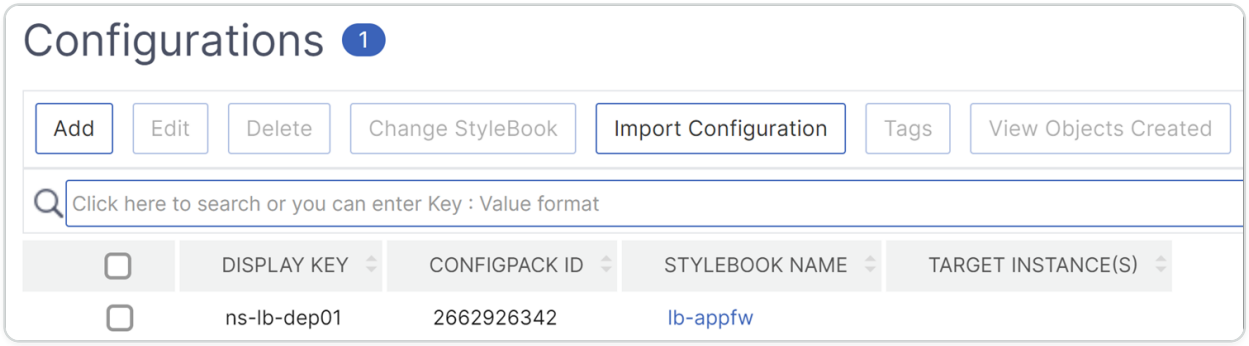
The following figure shows the objects created in each server:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



16. To see the ConfigPack created on NetScaler Console, navigate to **Applications** > **Configurations**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



SNMP configuration StyleBook

A Simple Network Management Protocol (SNMP) application helps you log NetScaler events in NetScaler Console. This application runs on NetScaler Console and queries the SNMP agent on a NetScaler instance. The agent searches the management information base (MIB) for data requested by the network management application and sends the data to the application.

When a configuration change occurs on an instance, an SNMP trap is generated. The traps are then sent to a remote device called a trap destination server or the SNMP trap destination. NetScaler Console is configured as the trap destination. You can query the SNMP agent for system-specific information from a remote device called an SNMP manager. The agent then searches the management information base (MIB) for requested data and sends the data to the SNMP manager.

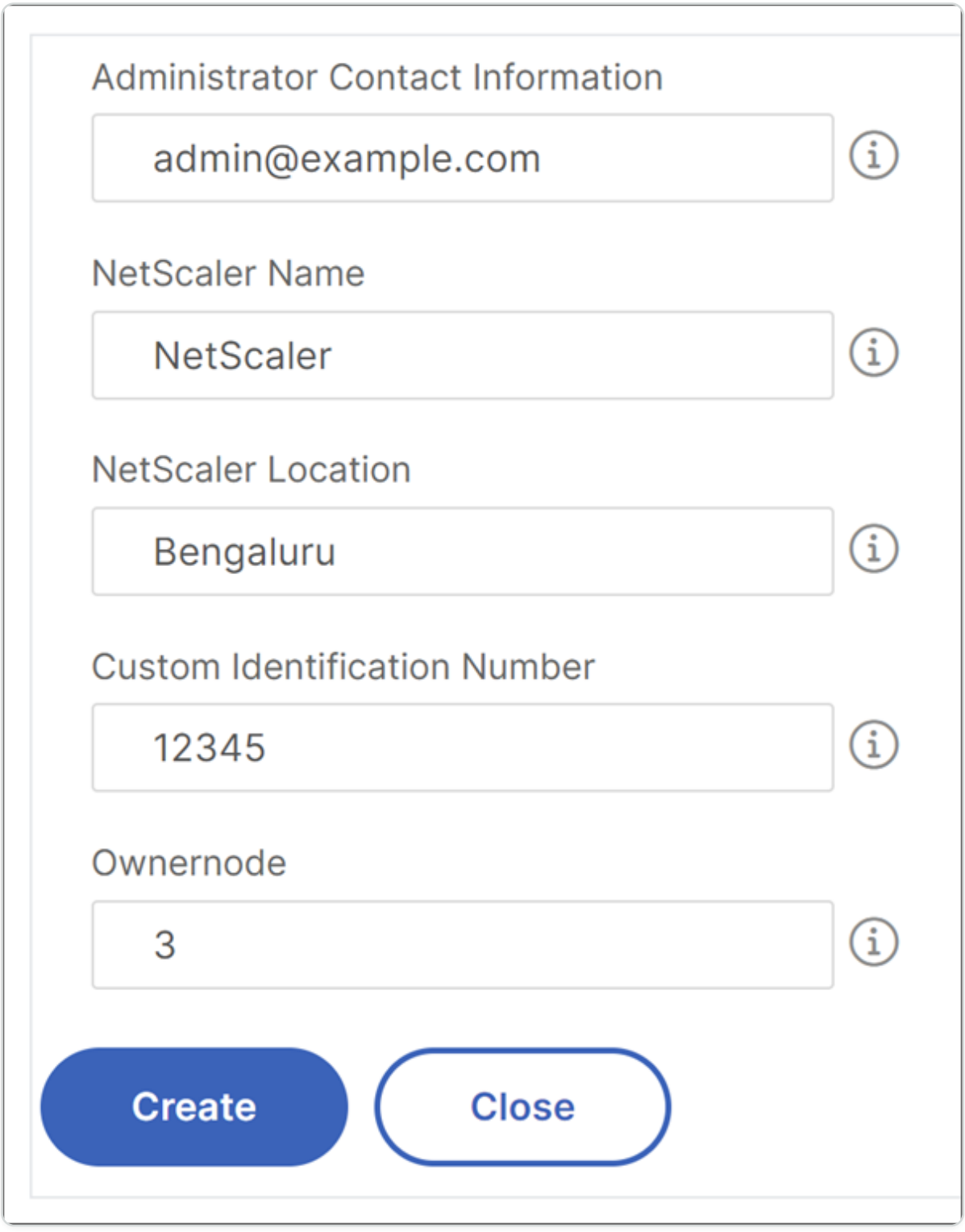
Do the following steps to deploy SNMP configurations on a NetScaler instance using StyleBook:

1. In NetScaler Console, go to **Applications > Configuration > StyleBooks**. Search for the StyleBook by typing the name as `snmp_configuration`. Click **Create Configuration**.

   The StyleBook opens as a user interface page on which you can enter the values for all the parameters defined in this StyleBook.
2. Specify the following parameters:

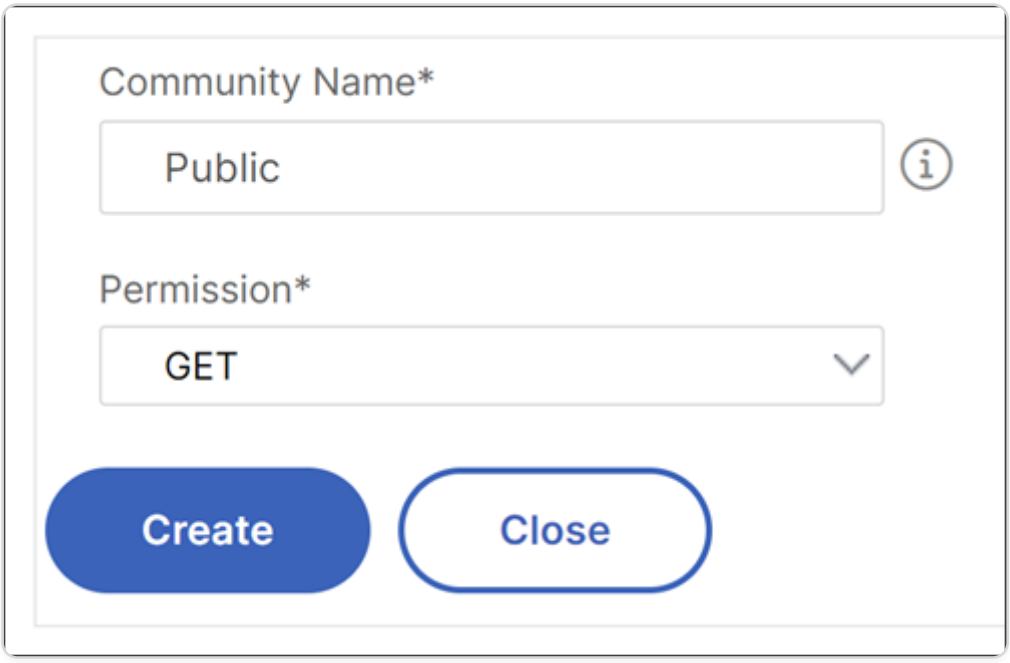
   - **SNMP MIB configuration** - Specify the following instance information:
     - **Administrator's contact**: The email address of an administrator.
     - **NetScaler Name**: Name of a NetScaler instance.
     - **NetScaler Location**: The physical location of an instance.
     - **Custom identitfication number**: Custom identification number for the NetScaler. This number helps to identify an instance.
     - **Ownernode**: The cluster node ID where you set this MIB. This field is mandatory to set SNMP MIB on CLIP.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

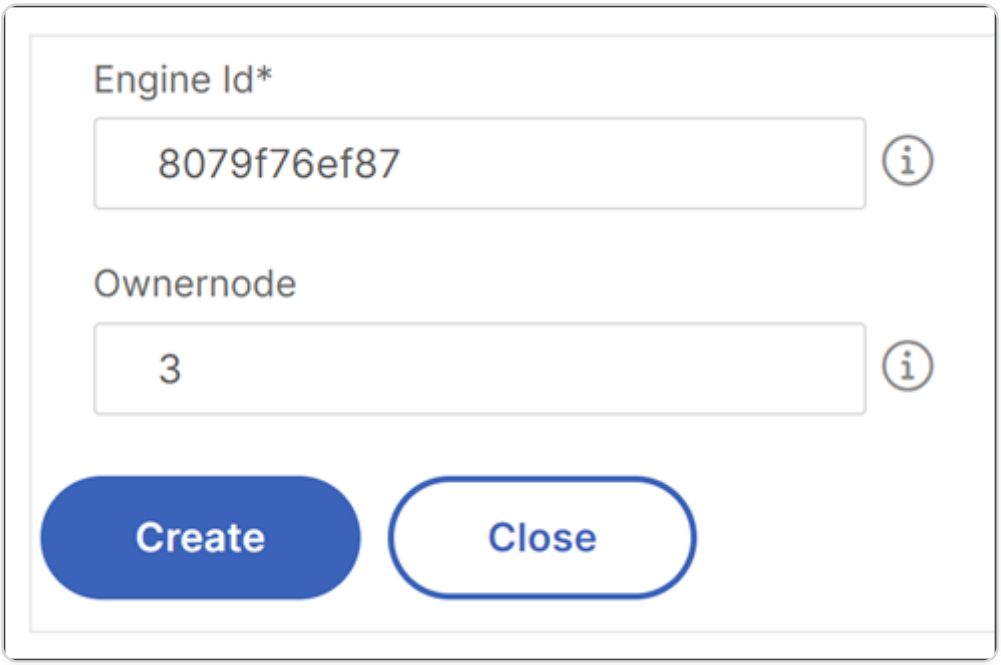


- **SNMP Comunity configuration** - An SNMP community configuration authenticates SNMP queries from SNMP managers. You can associate this string with any SNMP query types such as GET, GET NEXT, ALL, GET BULK.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



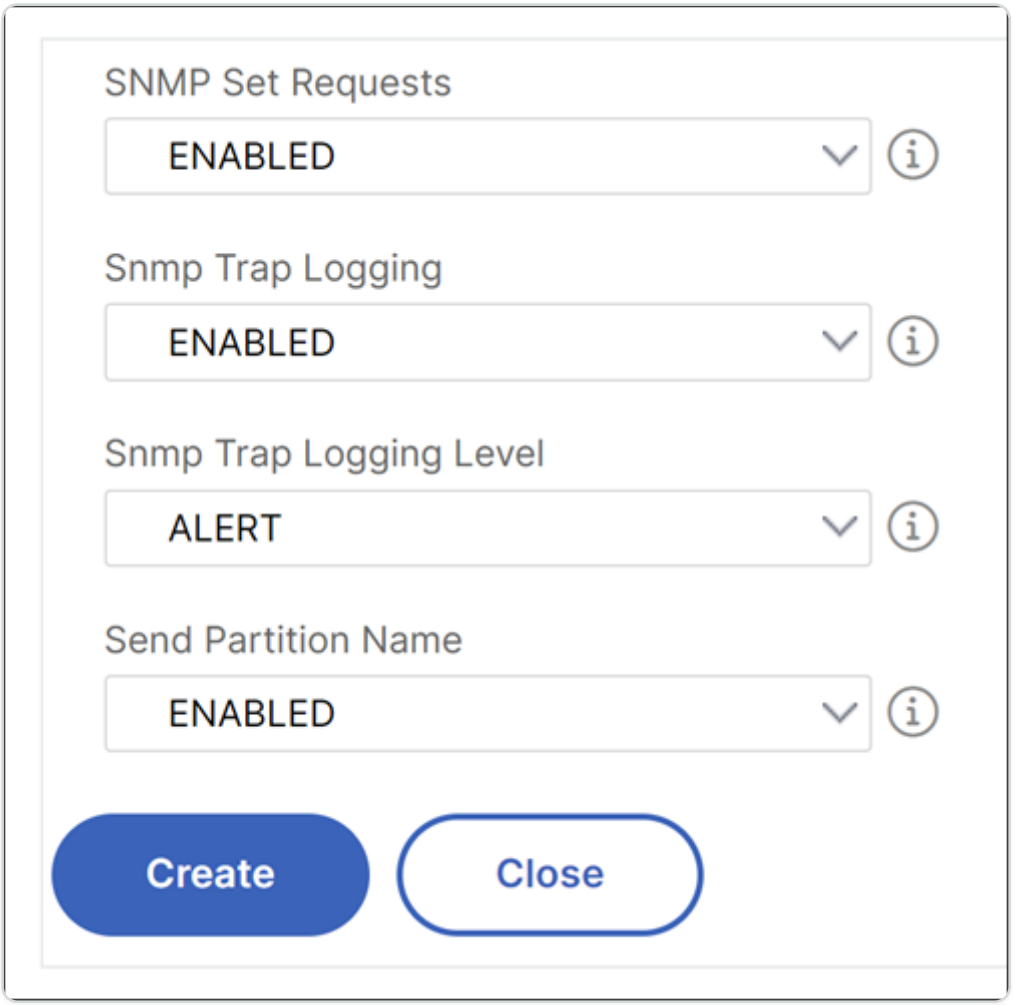
- **SNMP Engine id configuration** - The SNMPv3 engine has a unique identification (ID). This ID is used in the communication between SNMPv3 user and SNMPv3 engine. This ID is a hexadecimal value of minimum 10 characters. In this configuration, specify the `Ownernode` that you mention with the MIB configuration.



- **SNMP Option configuration** - You can enable or disable SNMP options for an SNMP manager.
  - **SNMP Set Requests**: Enable this option that allows SNMP managers to write values to MIB objects.
  - **SNMP Trap Logging**: This option logs SNMP trap events.
  - **SNMP Trap Logging Level**: This option sends an audit log level of SNMP trap logs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

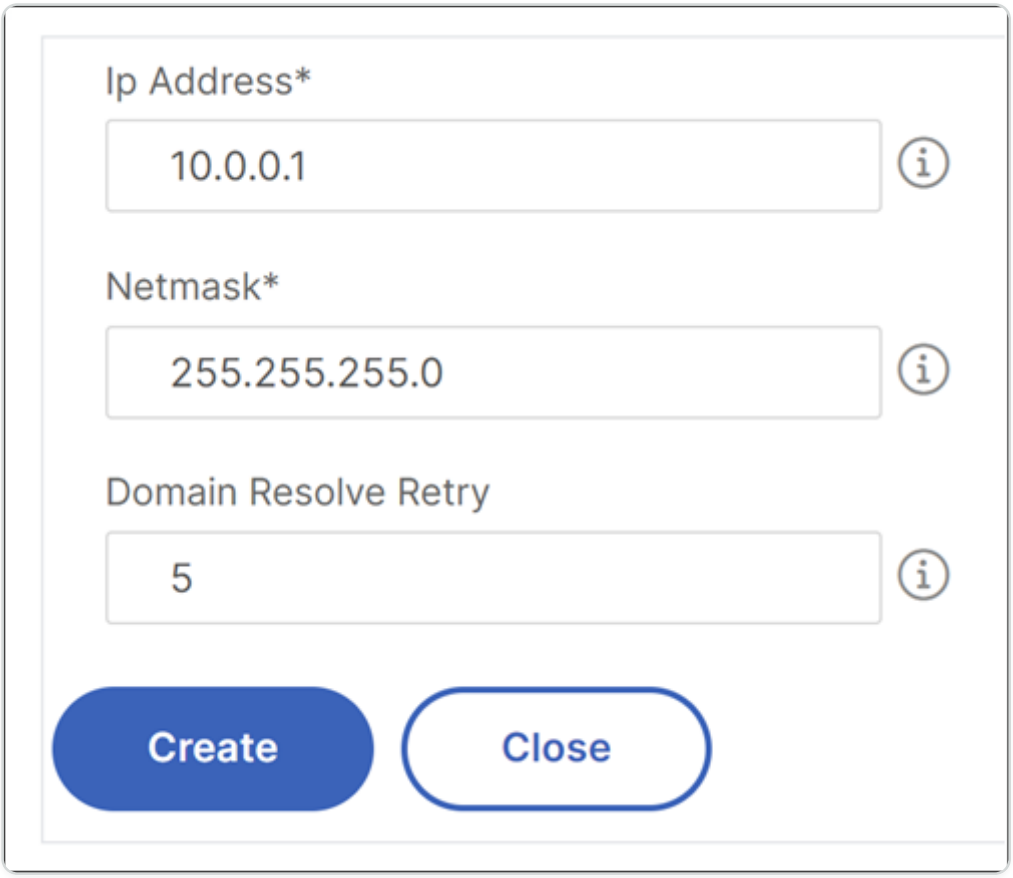
- **Send Partition Name**: This option sends the partition name.



- **SNMP Manager configuration** - An SNMP manager to query a NetScaler instance. The manager complies with SNMP V1, V2, and V3. If you specify one or more SNMP managers, the instance does not accept SNMP queries from any hosts except the specified SNMP managers.

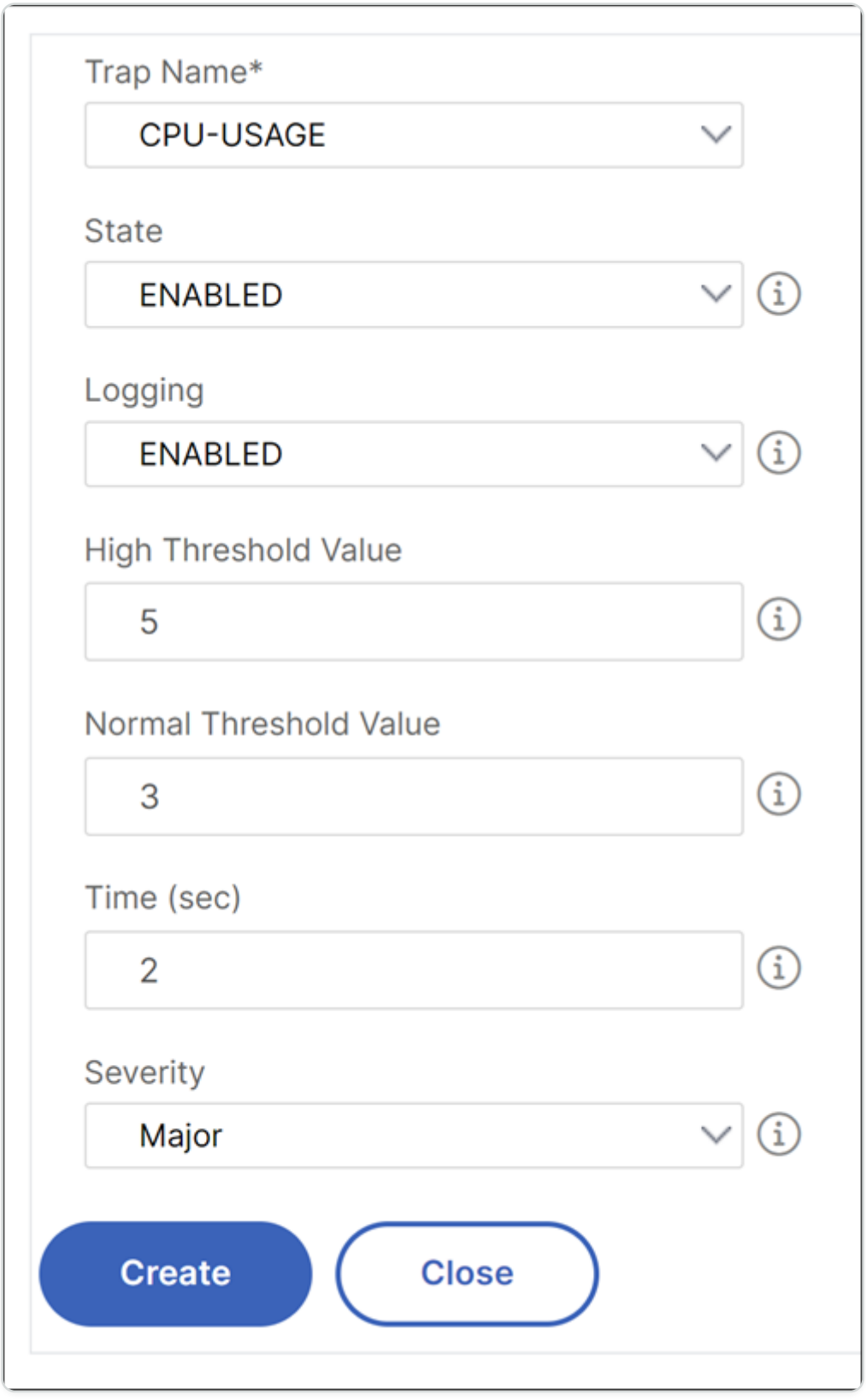
  - **IP Address**: An IP address of the SNMP manager.
  - **Netmask**: Subnet mask associated with an IPv4 network address.
  - **Domain Resolve Retry**: If the last DNS query fails to resolve the SNMP manager host name, the NetScaler instance waits for the specified interval before sending another DNS query.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **SNMP Alarm configuration** - Add SNMP alarms to generate enterprise-specific trap messages. A NetScaler instance sends the trap messages only to trap listeners of type (class) SPECIFIC. The SNMP alarms are either event based or threshold based.
    - **Trap Name**: Name of the SNMP alarm.
    - **State**: A NetScaler instance generates trap messages only for SNMP alarms that are enabled.
    - **Logging**: When you enable logging, the NetScaler instance logs every trap message that is generated for this alarm.
    - **High Threshold Value**: This value is the maximum limit of an attribute associated with this alarm. When the attribute reaches or exceeds this value, a NetScaler instance generates an SNMP trap message.
    - **Normal Threshold Value**: This value is the minimum limit of an attribute associated with this alarm. When the attribute reaches or drops below this value, an NetScaler instance generates an SNMP trap message.
    - **Time (sec)**: An interval at which the NetScaler instance generates SNMP trap messages when the specified conditions are met.
    - **Severity**: The severity level for the trap messages generated by this alarm. This field helps when you want an instance to send trap messages based on severity level.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

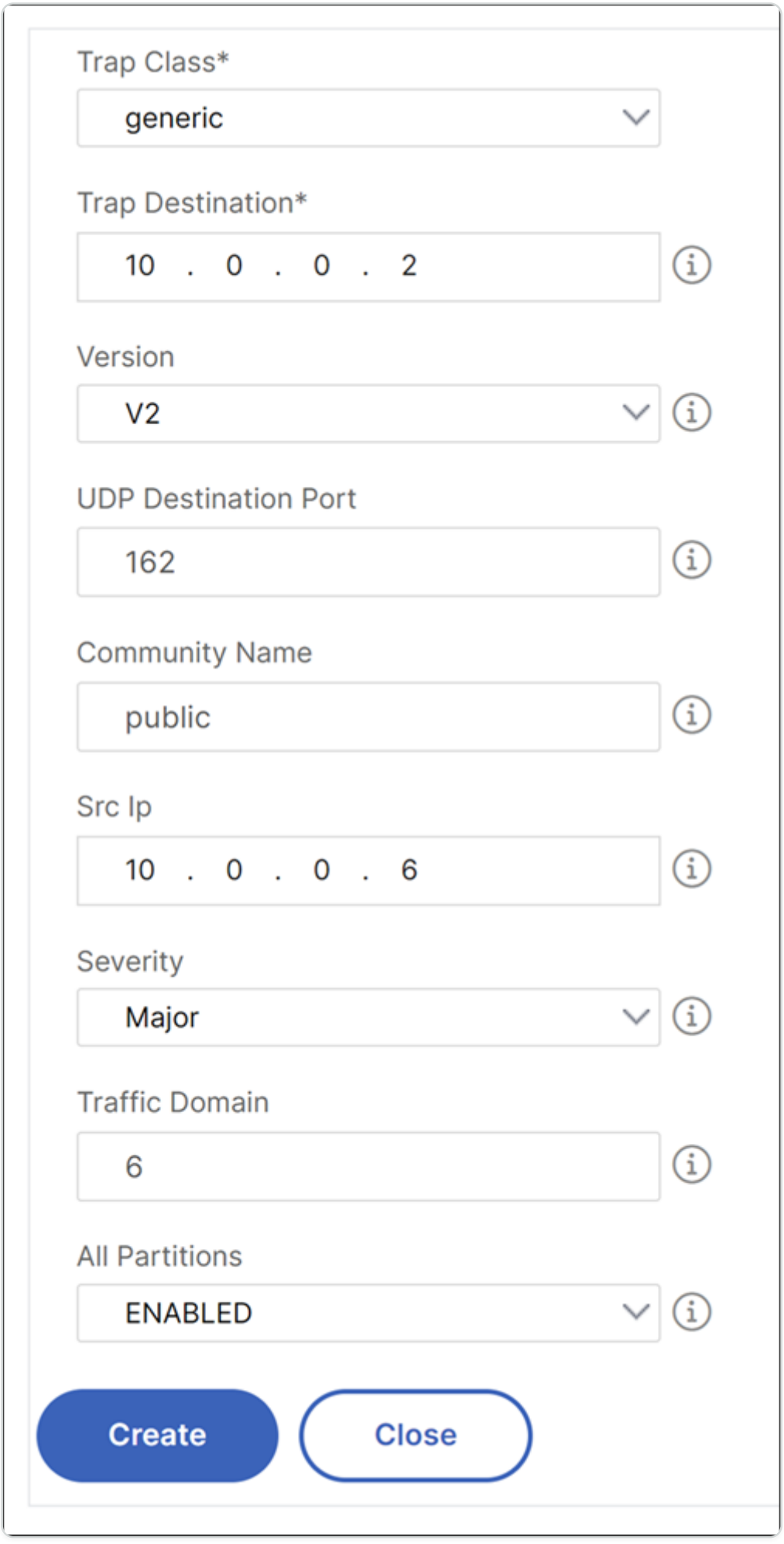


- **SNMP Trap configuration** - This configuration adds SNMP trap listeners. A NetScaler instance generates trap messages to report abnormal conditions. The trap messages are sent to a trap listener to help administrators to monitor the instance and respond promptly to any issues.
    - **Trap Class**: Type of trap messages that an instance sends to a trap listener.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Trap Destination**: The IPv4 or IPv6 address of the trap listener. An instance sends SNMP trap messages to this IP address.
- **Version**: An SNMP version. This version must match the version on the trap listener. Otherwise, the listener drops the trap messages.
- **UDP Destination Port**: UDP port at which the trap listener receives for trap messages. This value must match the value on the trap listener. Otherwise, the listener drops the trap messages.
- **Community Name**: A string is sent with the trap messages. Trap listener uses this string for authentication.
- **Src IP**: Source IP address. The IPv4 or IPv6 address of a NetScaler instance.
- **Severity**: The severity level for the trap messages. A NetScaler instance sends the trap messages for the specified and above severity levels.
- **Traffic Domain**: An integer value that uniquely identifies the traffic domain.
- **All Partitions**: If this option is enabled, an instance sends the trap messages of all partitions to the destination IP address.

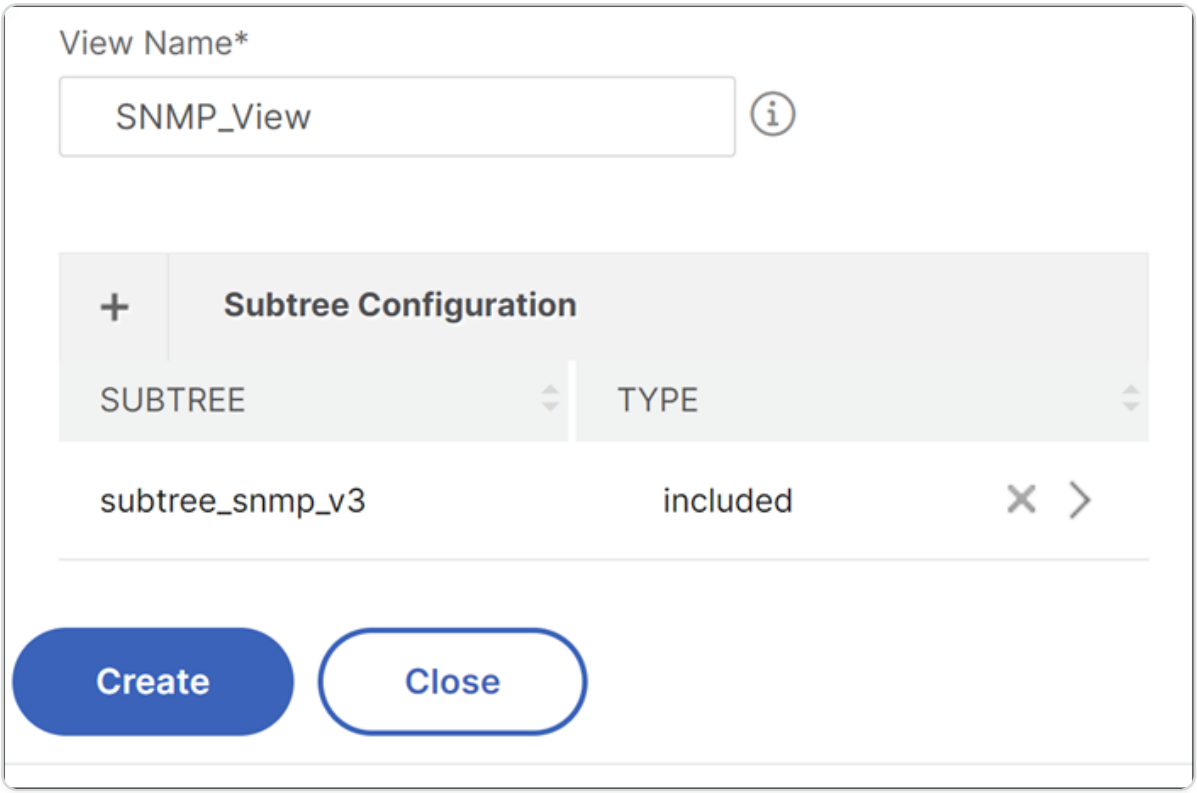
© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

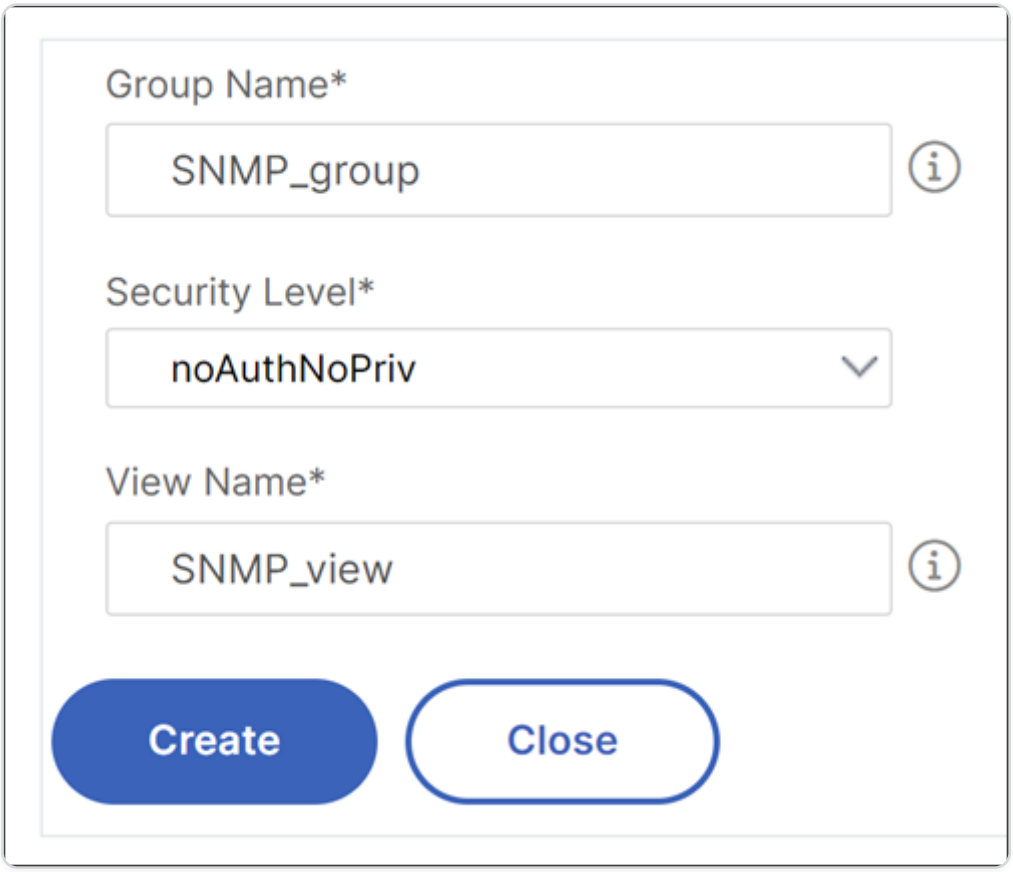
- **SNMP View configuration** - SNMP views are used to implement access control for an SNMPv3 user. The SNMP views restrict the user access to specific portions of MIB.
  - **View Name**: A name for the SNMPv3 view.

    An instance can have multiple SNMPv3 views with the same name, differentiated by subtree parameter settings. You can add a maximum of 1000 SNMPv3 views.
  - **Subtree**: A particular branch (subtree) of the MIB tree that you want to associate with this SNMPv3 view. You must specify the subtree as an SNMP OID.
  - **Type**: This field allows you to include or exclude subtrees from a view.



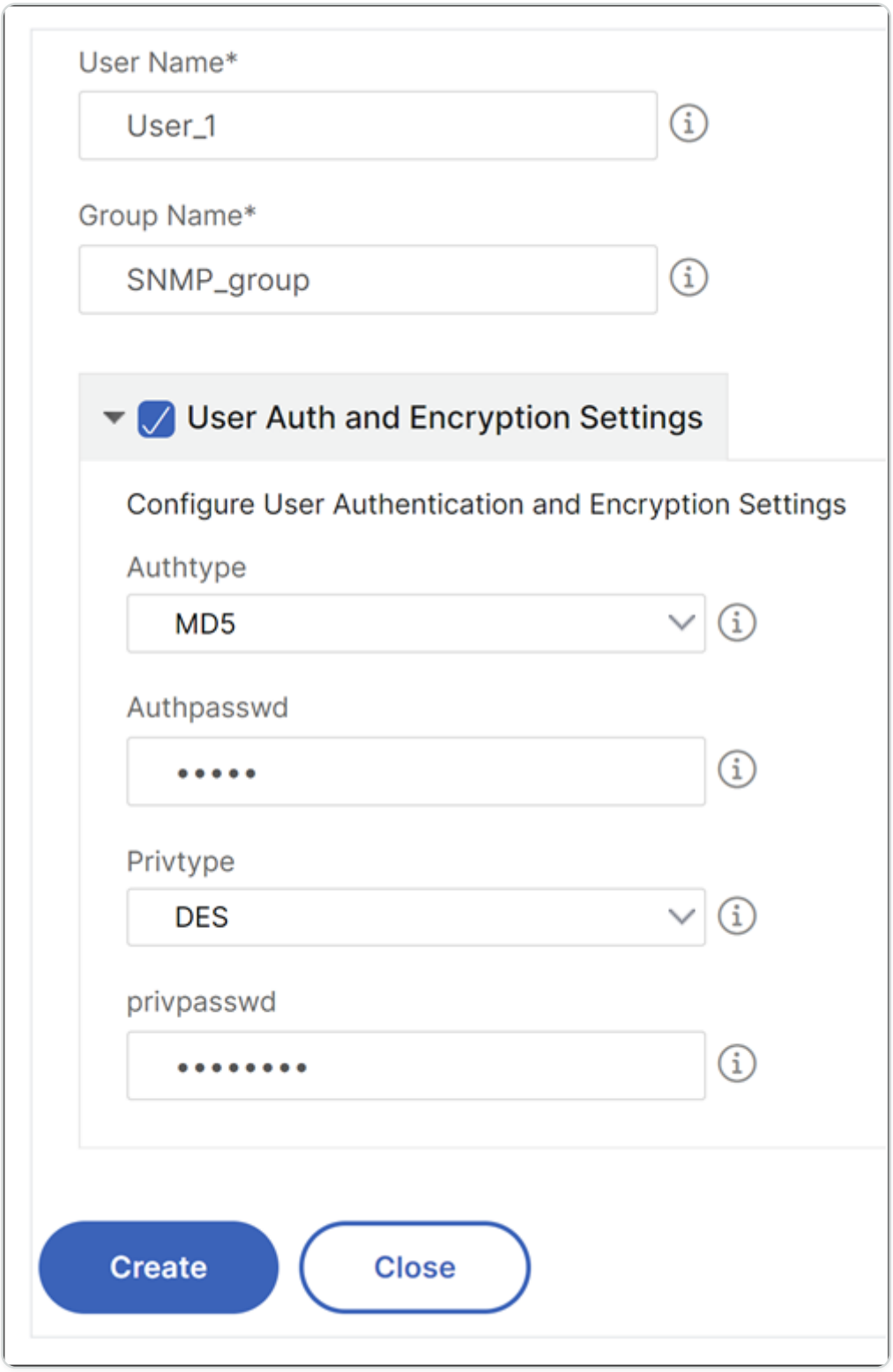
- **SNMP Group configuration** - The SNMPv3 user groups on an instance. These groups are logical aggregations of SNMPv3 users. SNMPv3 groups are used to implement access control and define the security levels for the users. You can add a maximum of 1000 SNMPv3 groups to a NetScaler instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



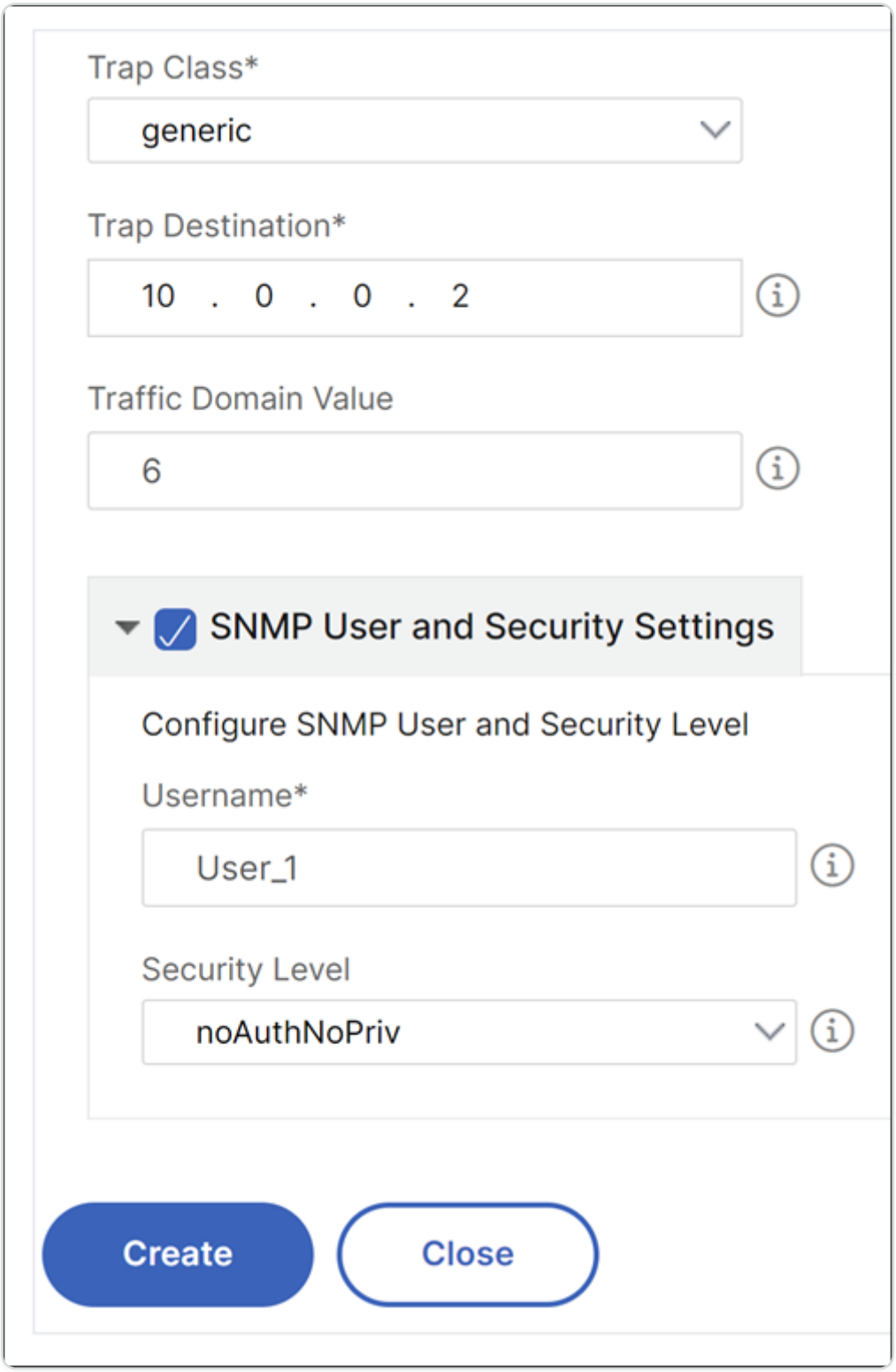
- **SNMP User Configuration** - Add SNMPv3 users who can send SNMP queries to a NetScaler instance. You can add a maximum of 1000 SNMPv3 users.
  - **Name**: Name of the SNMPv3 user.
  - **Group**: Name of the configured SNMPv3 group that you want to bind with the SNMPv3 user. The access rights (bound SNMPv3 views) and security level set for this group are assigned to this user.
  - **Authype**: An algorithm used to authenticate the SNMPv3 user to access the NetScaler instance. You must specify the same authentication algorithm when you configure the SNMPv3 user in the SNMP manager.
  - **Authpassword**: A password for authentication. This password uses the specified authentication algorithm type.
  - **Privtype**: An algorithm that encrypts the communication between a SNMPv3 user and the NetScaler instance.
  - **privpasswd**: An encryption key for the encryption algorithm specified in **Privtype**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **SNMP User Trap binding configuration** - SNMPv3 provides security capabilities such as authentication and encryption by using the credentials of SNMP users. An SNMP manager can receive SNMPv3 trap messages only if its configuration includes the password assigned to the SNMP user.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. In **Target Instances**, select instances or instance groups where you want to run the configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

You can deploy the configuration on more than one NetScaler, by specifying as many target instances as needed.

4. In **Tag Assosiation**, associate all present and future StyleBook tags with the configuration.

   This option associates all the StyleBook tags to a configuration pack. It also makes sure to associate the new tags that you might add to the StyleBooks in future.

5. Click **Dry Run**.

   The Objects page displays the objects that get created, modified, or removed from the NetScaler instances.

6. Click **Create**.

   The configuration pack appears in the **StyleBook > Configurations** page.

NetScaler network configurations StyleBook

When you want to deploy various networking components on a NetScaler instance, you can use NetScaler Console StyleBooks. Use the following StyleBooks to create NetScaler networking components:

- `network_configuration`: For basic networking components.
- `adv_network_configuration`: For advanced configurations such as VXLAN, cluster, and more.

To learn more about NetScaler networking components, see Networking.

Deploy basic networking components

The basic networking components can be interface, channel, VLAN, NSIP, Address Resolution Protocol (ARP), or bridge group configurations. Do the following steps to deploy any of these components:

1. In NetScaler Console, navigate to **Applications > Configuration > StyleBooks**. Search for the StyleBook by typing the name as `network_configuration`.
2. Click **Create Configuration**.
3. Add the following configurations as per your need:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

Click the (+) icon on each section to add configurations.

- **Interface Configurations** - The number of interfaces in your configuration is different for the different models of the NetScaler instance. For more information on interfaces, see Interfaces. Specify the fields that are required to configure an interface.
- **Channel Configurations** - Configuring link aggregation increases the capacity and availability of the communication channel between the NetScaler instance and other connected devices. An aggregated link is also referred to as "channel". Link aggregation combines data coming from multiple ports into a single high-speed link. For more information, see Configuring Link Aggregation.
- **Channel Interface Binding Configurations** - Specify the interface and channel IDs to bind the configurations.
- **VLAN Configurations** - You can configure VLANs and bind them to IP subnets. The NetScaler then performs IP forwarding between these VLANs (if it is configured as the default router for the hosts on these subnets). For more information, see Understanding VLANs. Specify the details to configure a VLAN.
- **NS IP Configurations** - The NSIP address is the IP address at which you access the NetScaler instance for management purposes. The instance can have only one NSIP, which is also called the management IP address. For more information, see Configuring the NSIP address.
- **NS IP6 Configurations** - You can also configure an IPv6 address to a NetScaler instance as NSIP.
- **Configurations for VLAN Interface Binding** - When you bind a network interface to a VLAN, the network interface is removed from the default VLAN. If the network interfaces must be a part of more than one VLAN, you can bind the network interfaces to the VLANs as tagged members.
- **Configurations for VLAN NS IP Binding** - You can bind NetScaler IP address (NSIP) with VLAN. When an IP address is associated with a VLAN, all IP addresses in that subnet are automatically associated with the VLAN.
- **Route Configurations for IPv4** - Add a network IP address (IPv4) for which you want to add a route entry in the NetScaler instance route table.
- **Route Configurations for IPv6** - Add a network IP address (IPv6) for which you want to add a route entry in the NetScaler instance route table.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ARP Configurations** - You can add static ARP entries and remove static ARP entries from the ARP table. For more information, see Static ARP.
- **ND6 Variables Configurations** - Neighbor discovery (ND) is one of the most important protocols of IPv6. It is a message-based protocol that combines the functionality of the Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), and Router Discovery. ND allows nodes to advertise their link layer addresses and obtain the MAC addresses or link layer addresses of the neighboring nodes. For more information, see Neighbor Discovery.

  You can configure the ND6 variables for a NetScaler instance.
- **Neighbor Discovery Configurations for IPv6** - You can configure ND for an IPv6 address.
- **Bridge Group Configurations** - The bridge groups feature works the same way as a VLAN. Multiple VLANS can be bound to a single bridge group, and all VLANs bound to the same bridge group from a single broadcast domain. For more information, see Configuring Bridge Groups.
- **Bridge Group NS IPv46 Binding Configurations** - Bind a NetScaler IP (NSIP) address to a bridge group.
- **Bridge Group VLAN Binding Configurations** - Bind a VLAN to a bridge group.

4. In **Target Instances**, select the NetScaler instances or instance groups.
5. In **Tag Assosiation**, associate all present and future StyleBook tags with the configuration.

   This option associates all the StyleBook tags to a configuration pack. It also makes sure to associate the new tags that you might add to the StyleBooks in future.
6. Click **Dry Run**.

   The Objects page displays the objects that get created, modified, or removed from the NetScaler instances.
7. Click **Create**.

The configuration pack appears in the **StyleBook > Configurations** page.

Deploy advanced networking components

The advanced networking components can be VXLAN, VRID, Bridge Table, Failover Interface Set (FIS), INAT, RNAT configurations, and more. Do the following steps to deploy such advanced networking components:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. In NetScaler Console, navigate to **Applications > Configuration > StyleBooks**. Search for the StyleBook by typing the name as `adv_network_configuration`.
2. Click **Create Configuration**.
3. Add the following configurations as per your need:

> **NOTE**
>
> Click the (+) icon on each section to add configurations.

- **VXLAN Configurations** - VXLANs provide higher scalability and flexibility than VLANs. For more information, see VXLAN.
- **VXLAN VLAN MAP Configurations** - Create a mapping table on the NetScaler instance. This table maps a VXLAN ID to a respective VLAN ID.
- **VRID Configurations** - Add an IPv4 address that identifies a virtual MAC (VMAC). You can also configure other VRID options and binding information.
- **VRID6 Configurations** - Add an IPv6 address that identifies a virtual MAC (VMAC). You can also configure other VRID6 options and binding information.
- **BridgeTable Configurations** - A NetScaler instance bridges the frames on the basis of a bridge table lookup of the destination MAC address and the VLAN ID. Specify the required details to monitor the Bridge Table.
- **FIS Configurations** - A FIS is a logical group of interfaces. In a NetScaler HA configuration, using a FIS is a way to prevent failover by grouping interfaces so that, when one interface fails, other functioning interfaces are still available. A FIS can also be configured for the nodes of a NetScaler cluster. For more information, see Configuring failover interface set.
- **Configurations for ForwardingSession** - A forwarding-session rule creates forwarding-session entries for traffic that originates from or is destined for a particular network and is forwarded by the NetScaler instance. You can create forwarding session rules for IPv4 traffic as well as IPv6 traffic. See, Configuring Forwarding Session Rules.
- **INAT Configurations** - When a client sends a packet to a NetScaler instance that is configured for Inbound Network Address Translation (INAT), the instance translates the packet's public destination IP address to a private destination IP address. And, the instance forwards the packet to the server at that address. See, Inbound Network Address Translation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **NAT64 Configurations** - The stateful NAT64 enables communication between IPv6 clients and IPv4 servers through IPv6 to IPv4 packet translation, and vice versa, while maintaining session information on the NetScaler appliance. See, Stateful NAT64 Translation.
- **RNAT Configurations** - In Reverse Network Address Translation (RNAT), the NetScaler appliance replaces the source IP addresses in the packets generated by the servers with public NAT IP addresses. See, RNAT.
- **RNAT6 Configurations** - Reverse Network Address Translation (RNAT) rules for IPv6 packets are called RNAT6s. See, Configure RNAT6.
- **IPSet Configurations** -An IP set is a set of IP addresses, which are configured on the NetScaler instance as Subnet IP addresses (SNIPs) or Virtual IP addresses (VIPs). Specify the required details to create an IP set.
- **IPTunnel Configurations** - Specify the details to create an IP Tunnel and its bindings. See, IP Tunnels.
- **IP6 Tunnel Configurations** - For IPv6 addresses, specify the details to create IP Tunnel and its bindings.
- **Linkset Configurations** - Linkset is a group of interfaces of cluster nodes that belong to the same broadcast domain. See, Configuring linksets.
- **MAP-T Basic Mapping Rule Configurations** - Mapping Address and Port using Translation (MAP-T). It is a mechanism that performs double translation (IPv4 to IPv6 and vice versa) on customer edge (CE) devices and border routers (in the ISP core network). Specify the details to add a basic mapping rule. See, Mapping Address and Port using Translation.
- **MAP-T Default Mapping Rule Configurations** - Specify the details to add a default mapping rule.
- **MAP-T Map Domain Configurations** - Specify the details to add a map domain.
- **NetProfile Configurations** - Add a net profile and configure override `lsn`.
- **NetBridge Configurations** - Bind a VXLAN-VLAN map to a network bridge.
- **On-link IPv6 global prefixes for Router Advertisment Configurations** - For IPv6 cluster configuration, configure global prefixes and router advertisements. See, IPv6 ready logo support for clusters.

4. In **Target Instances**, select the NetScaler instances or instance groups.
5. In **Tag Assosiation**, associate all present and future StyleBook tags with the configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This option associates all the StyleBook tags to a configuration pack. It also makes sure to associate the new tags that you might add to the StyleBooks in future.

6. Click **Dry Run**.

   The Objects page displays the objects that get created, modified, or removed from the NetScaler instances.

7. Click **Create**.

The configuration pack appears in the **StyleBook > Configurations** page.

Prometheus analytics StyleBook

You can export metrics from NetScaler to Prometheus by creating an analytics profile in NetScaler and specifying the schema file. In StyleBooks, you can use the `Prometheus TimeSeries Analytics Configuration` StyleBook and run the configuration to all managed instances.

Prerequisite

Ensure that the managed NetScaler instances are in **13.1 build 39-27 or later**.

To configure using the `Prometheus TimeSeries Analytics Configuration` StyleBook:

1. Navigate to **Applications** > **Configurations** > **StyleBooks**, search for the StyleBook by typing the name as `Prometheus TimeSeries Analytics Configuration`, and click **Create Configuration**.
2. In **Configpack Details**:
   a. Specify the analytics profile name. For more information, see Configure metrics collector.
   b. **Counter Schema File**:
      - If you want to proceed with the default schema, you can skip this step.
      - If you want to proceed with the custom schema, upload the schema file that you have modified with the parameters. In NetScaler, a reference file `reference_schema.json` with all supported counters is available under the path `/var/metrics_conf/`. You can use an FTP client to copy the file in your local.
3. In **Target Instances**, select the instances or instance group that you want to run the configuration.
4. In **Tag Assosiation**, associate all present and future StyleBook tags with the configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This option associates all the StyleBook tags to a configuration pack. It also makes sure to associate the new tags that you might add to the StyleBooks in future.

NOTE:

Click **Dry Run** to view results that get created, modified, or removed from the NetScaler® instances.

5. Click **Create** to run the configuration.

Migrate NetScaler application configuration using StyleBooks Configuration Builder

The StyleBooks Configuration Builder is used to migrate an existing NetScaler configuration to StyleBooks. This feature also automates the application configuration migration from one NetScaler instance to another instance or an Autoscale group.

The Configuration Builder provides a structured application StyleBook that can be used to any variants of the NetScaler configuration. This feature helps you get started with StyleBooks without in-depth knowledge of StyleBooks grammar and constructs. Otherwise, the knowledge of StyleBooks grammar and constructs is necessary to create a StyleBook.

The Configuration Builder also creates a configuration pack that reflects the same NetScaler configuration on a new NetScaler instance. With this configuration pack, the initial NetScaler configuration from one NetScaler instance can be duplicated to another NetScaler instance. The initial configuration source can be one of the following:

- **A NetScaler instance:** Specify the instance where the application configuration that you want to duplicate is hosted.

  The Configuration Builder converts the NetScaler configuration to StyleBook and configuration pack even if you do not specify the target instance. You can later use this configuration pack to migrate the NetScaler configuration to other NetScaler instances.

  If the target instance is an Autoscale™ group, the configuration pack appears in the **Network > AutoScale Group** page. Under the **Configuration** tab.

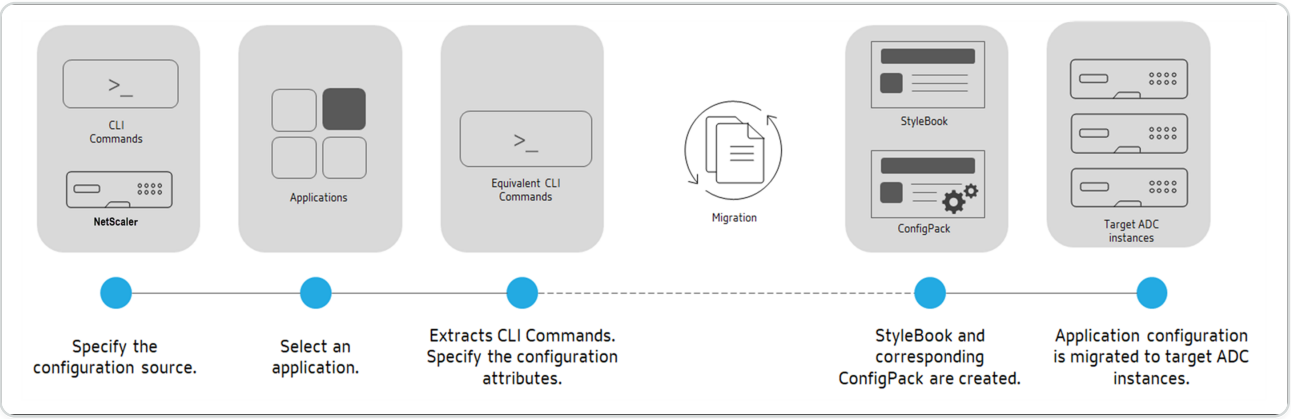
- **A set of CLI Commands:** Paste the configuration from `ns.conf` or `Application config`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The Configuration Builder identifies the list of distinct applications embedded in the source configuration. When you select the application configuration of your interest, the Configuration Builder extracts the set of CLI commands for the selected application. These CLI commands are extracted from the source configuration. Also it identifies the deployment and configuration attributes that might require your input.

- **IP Address/ports** - You can view and edit the IP address and port of the virtual servers, services, service group members from the original configuration.
- **Configuration Files/Secrets** - These attributes can be passwords or certificates specified in the source configuration.

After specifying the necessary information, start migrating or duplicating the application configuration on a target NetScaler instance.



After the application creation and migration, a configuration pack is created in NetScaler Console using `adc_nitro_application` StyleBook. This StyleBook is created based on the NetScaler NITRO resources. This configuration pack represents the application configuration on the target NetScaler instance. To view the created configuration pack, navigate to **Applications > Configuration > Confg Packs**.

Sharing configuration entities between migrated configurations

You can reuse configuration entities when migrating configurations using the Config Migration utility. Subsequent migrations successfully reuse existing configuration entities. Previously, the migration of configurations failed with an error **Resource already exists** when migrating two configurations that shared some configuration entities. This option streamlines the migration workflow by allowing the reuse of configuration entities in scenarios where they are used across multiple configurations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Supported NetScaler Features

The StyleBook Configuration Builder recognizes and supports the following NetScaler features in the source configuration:

- Content Switching
- Load Balancing
- Monitoring
- SSL Offloading
- Rate limiting
- Rewrite
- Responder
- Web application firewall (WAF)
- Bot management
- Compression Control

Create a StyleBook to migrate the NetScaler application configuration

The following procedure is to create a StyleBook that migrates the NetScaler application migration in NetScaler Console:

1. Navigate to **Applications > Configuration > Confg Packs**.
2. Click **Migrate NetScaler Configuration**.
3. Click **Get Started**.
4. In **Specify Configuration**, select the configuration source:
    - **Import from a NetScaler**: This option discovers the active applications on the selected NetScaler instance.
    - **Import using CLI Commands**: This option analyses the CLI commands and extracts the applications from the CLI commands.
5. Specify the **Source NetScaler Instance** from which you want to migrate or duplicate the application configuration.

    To migrate the application configuration to an Autoscale group, ensure the following information is not included in the source configuration:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `IPset`
- Device profile
- Protocol
- Port

6. Specify the **Target NetScaler Instance** to which you want to migrate or duplicate the application configuration.

   To migrate an application configuration to an Autoscale group, select the Autoscale group from the list.

7. In **Define Application**,

   a. In **Application Name**, specify the name of the application.

      If the target instance is an Autoscale group, specify the following Autoscale parameters:

      - **Access Type** - You can use the NetScaler Console autoscaling solution to both external and internal applications. Select the required application access type.
      - **Domain Name** - Specify the domain name of an application. This option is applicable only when you select User-Defined FQDN type.
      - **Zone of the Domain** - Select the zone name of an application from the list. This option is applicable only when you select User-Defined FQDN type.

        This domain and zone name redirects to the virtual servers in Azure. For example, if you host an application in `app.example.com`, the `app` is the domain name and `example.com` is the zone name.

   b. Select the virtual servers that you want to migrate.

   c. Click **Next**.

8. In **Equivalent CLI Commands**, review the commands and click **Next**.

   These commands are specific to the selected application configuration.

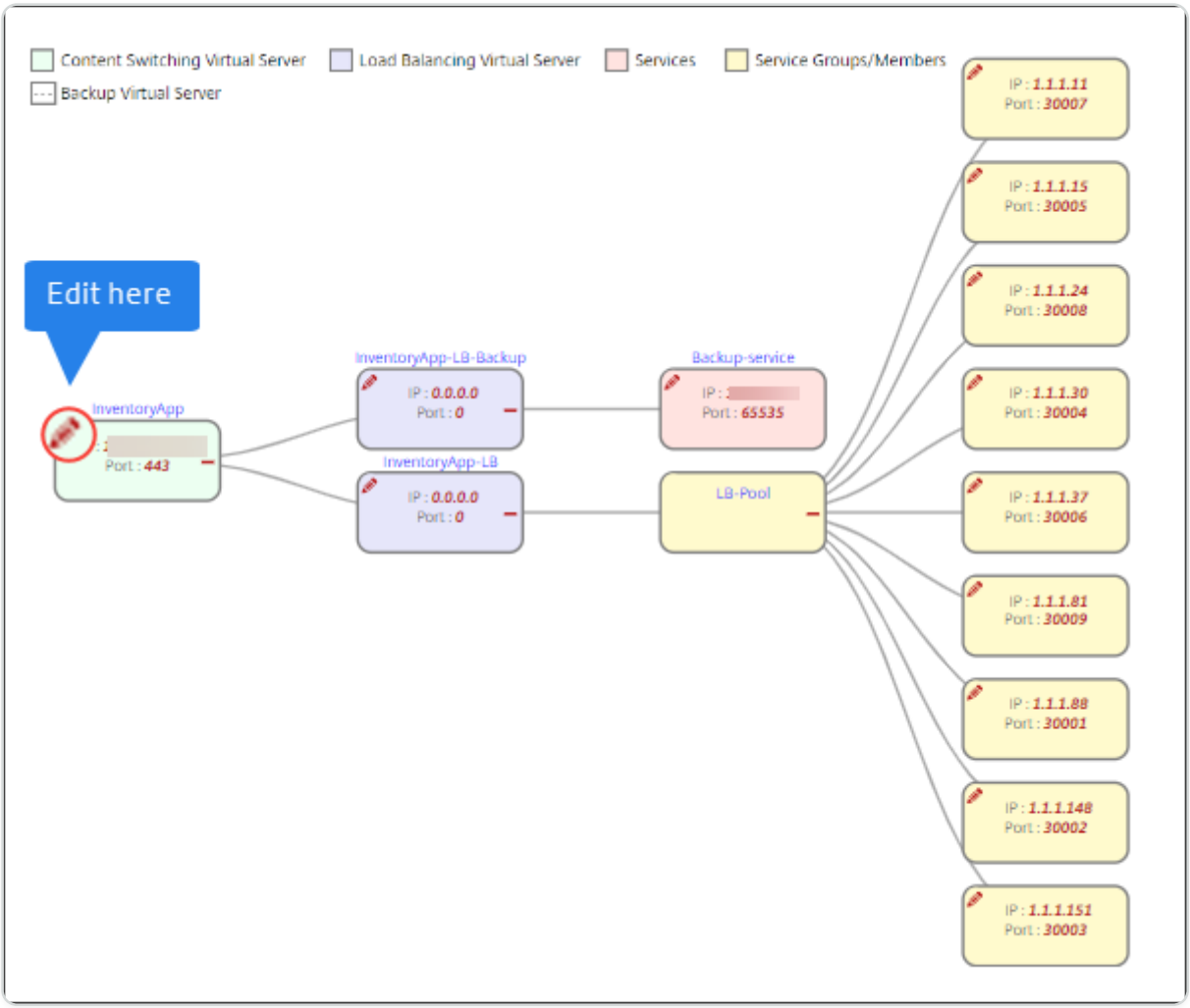
   NOTE:

   You can also add or edit the configuration if needed.

9. In **Deployment Attributes**, you can view and edit the IP address and port of the virtual servers, services, and service group members.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To edit the IP address and port, click the edit icon on the virtual server, service, or service group member in the flow diagram.



NOTE:

If the target instance is an Autoscale group, editing the front end IP address is disabled.

This tab appears only in the following cases:

- The source and target instances are different.
- Import configurations using CLI commands.

10. In **Configuration Attributes**, specify the necessary details and click **Next**.

    This tab lists the secrets such as keys to decrypt passwords and certificates.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Before you start the migration, the missed or unsupported configurations are displayed in any of the following tabs:

- **Unsupported Configurations**
- **Unsupported Global Configurations**

To migrate these configurations successfully, you must apply the missed or unsupported configurations separately on the target instance. And, click **Next**.

11. In **Migrate**, click **Migrate**.

Limitations

- The named expressions and `responderhtmlpages` mentioned in the source instance are not identified. Make sure to configure the named expressions and `responderhtmlpages` on the target instance before migration.
- If the source has a configuration for `servicegroup` and monitor binding as follows:

  `bind serviceGroup <Name> <Port> -monitorName <Monitor_Name>`

  The following error appears:

  ```
  CLI Command conversion failed: 100 - No such command [{ "errorcode":
  1090, "message": "No such argument [XXX]", "severity": "ERROR" }]
  ```

  This error occurs because NetScaler saves the binding between Service Group and Monitor in an invalid format. This issue is fixed from NetScaler 12.1.52.15 build.

Business application StyleBooks

NetScaler Console provides the StyleBooks that helps you deploy a NetScaler configuration for specific business applications. For more information on such StyleBooks, see the following topics:

- SSO Google Apps StyleBook
- SSO Office 365 StyleBook
- Microsoft Skype for Business StyleBook
- Microsoft Exchange StyleBook

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Microsoft SharePoint StyleBook
- Microsoft ADFS proxy StyleBook
- Oracle e-business StyleBook

SSO Google Apps StyleBook

Google Apps is a collection of cloud computing, productivity and collaboration tools, software and products that are developed by Google. Single Sign-On (SSO) enables users to access all of their enterprise cloud applications—including administrators signing in to the admin console—by signing in one time for all services using their enterprise credentials.

The NetScaler Console SSO Google Apps StyleBook allows you to enable SSO for Google Apps through NetScaler instances. The StyleBook configures the NetScaler instance as a SAML identity provider for authenticating users to access Google Apps.

Enabling SSO for Google apps in a NetScaler instance using this StyleBook results in the following steps:

1. Configuring the authentication virtual server
2. Configuring a SAML IdP policy and profile
3. Binding the policy and profile to the authentication virtual server
4. Configuring an LDAP authentication server and policy on the instance
5. Binding the LDAP authentication server and policy to your authentication virtual server configured on the instance

Configuration details:

The following table lists the minimum required software versions for this integration to work successfully. The integration process also supports higher versions of the same.

PRODUCT	MINIMUM REQUIRED VERSION
NetScaler	Release 11.0, Advanced/Premium License

The following instructions assume that you have already created the appropriate external and internal DNS entries to route authentication requests to a NetScaler-monitored IP address.

Deploying SSO Google apps StyleBook configurations:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The following task assists you in deploying the Microsoft SSO Google Apps StyleBook in your business network.

To deploy SSO Google apps StyleBook

1. In NetScaler Console, navigate to **Applications** > **Configurations** > **StyleBooks**. The StyleBooks page displays all the StyleBooks available for your use in NetScaler Console. Scroll down and find **SSO Google Apps StyleBook**. Click **Create Configuration**.
2. The StyleBook opens as a user interface page on which you can enter the values for all the parameters defined in this StyleBook.
3. Enter values for the following parameters:

    a. **Application Name**. Name of the SSO Google apps configuration to deploy in your network.

    b. **Authentication Virtual IP address**. Virtual IP address used by the NetScaler AAA virtual server to which the Google apps SAML IdP policy is bound.

    c. **SAML Rule Expression**. By default, the following NetScaler Policy (PI) expression is used: HTTP.REQ.HEADER("Referrer").CONTAINS("google"). Update this field with another expression if your requirement is different. This policy expression matches the traffic to which these SAML SSO settings are applied and makes sure that the Referrer header is coming from a Google domain.

4. The SAML IdP Settings section allows you to configure your NetScaler Instance as a SAML identity provider by creating the SAML IdP profile and policy that is used by the NetScaler AAA virtual server created in step 3.

    a. **SAML Issuer Name**. In this field, enter the public FQDN of your authentication virtual server. Example: `https://<Citrix_ADC_VIP>/saml/login`

    b. **SAML Service Provider (SP) ID**. (optional) NetScaler identity provider accepts SAML authentication requests from an issuer name that matches this ID.

    c. **Assertion Consumer Service URL**. Enter the service provider's URL where NetScaler identity provider needs to send the SAML assertions after successful user authentication. The assertion consumer service URL can be initiated at the identity provider server site or the service provider site.

    d. There are other optional fields that you can enter in this section. For example, you can set the following options:

        i. SAML binding profile (the default is the "POST" profile).

        ii. Signature algorithm to verify/sign SAML requests/responses (default is "RSA-SHA1").

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iii. Method to digest hash for SAML requests/responses (default is "SHA-1").

iv. Encryption algorithm (default is AES256), and other settings.

NOTE

Citrix recommends that you retain the default settings as these settings have been tested to support Google Apps.

e. You can also enable User Attributes check box to enter the user details such as:

i. Name of the user attribute

ii. NetScaler PI expression that is evaluated to extract the attribute's value

iii. User-friendly name of the attribute

iv. Select the format of the user attribute.

These values are included in the issued SAML Assertion. You can include as many as five sets of user attributes in an Assertion issued by NetScaler using this StyleBook.

5. In LDAP Settings section, enter the following details to authenticate Google Apps users. For domain users to be able to log on to the NetScaler instance by using their corporate email addresses, you must configure the following:

a. **LDAP (Active Directory) Base**. Enter the base domain name for the domain in which the user accounts reside within the Active Directory (AD) for which you want to allow authentication. For example, `dc=netscaler,dc=com`

b. **LDAP (Active Directory) Bind DN**. Add a domain account (using an email address for ease of configuration) that has rights to browse the AD tree. For example, `cn=Manager,dc=netscaler,dc=com`

c. **LDAP (Active Directory) Bind DN Password**. Enter the password of the domain account for authentication.

d. A few other fields that you need to enter in this section are as follows:

i. LDAP server IP Address that NetScaler connects to for authenticating users

ii. LDAP server's FQDN name

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

You must specify at least one of the above two - the LDAP server IP address or the FQDN name.

iii. LDAP server port that NetScaler connects to for authenticating users (default is 389).

iv. LDAP host name. This is used to validate the LDAP Certificate if validation is turned on (by default, it is turned off).

v. LDAP login name attribute. The default attribute used to extract login names is `samAccountname`.

vi. Other optional miscellaneous LDAP settings

6. In SAML IdP SSL Certificate section, you can specify the details of the SSL certificate:

   a. **Certificate Name**. Enter the name of the SSL certificate.

   b. **Certificate File. C**hoose the SSL certificate file from the directory on your local system or on NetScaler Console.

   c. **CertKey Format**. Select the format of the certificate and the private-key files from the drop-down list box. The formats supported are `.pem` and `.der` extensions.

   d. **Certificate Key Name**. Enter the name of the certificate private key.

   e. **Certificate Key File**. Select the file containing the private key of the certificate from your local system or from NetScaler Console.

   f. **Private Key Password**. If your private key file is protected by a passphrase, enter it in this field.

   g. You can also enable Advanced Certificate Settings check box to enter details such as certificate expiry notification period, enable or disable the certificate expiry monitor.

7. Optionally, you can select IdP SSL CA Certificate if the SAML IdP Certificate entered above requires a CA public Certificate to be installed on NetScaler. Make sure you select "Is a CA Certificate" in the advanced settings.

8. Optionally, you can select SAML SP SSL Certificate to specify Google SSL certificate (public key) used to validate authentication requests from Google Apps (SAML SP).

9. Click **Target Instances** and select the NetScaler instance(s) on which to deploy this Google Apps SSO configuration. Click **Create** to create the configuration and deploy the configuration on the selected NetScaler instance(s).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

You can also click the refresh icon to add recently discovered NetScaler instances in NetScaler Console to the available list of instances in this window.

Also,

TIP

SSO Office 365 StyleBook

Microsoft Office 365 is a suite of cloud-based productivity and collaboration applications provided by Microsoft on a subscription basis. It includes Microsoft's popular server-based applications such as Exchange, SharePoint, Office, and Skype for Business. Single Sign-On (SSO) enables users to access all their enterprise cloud applications:

- Including administrators signing in to the admin console
- One-time sign on for all Microsoft Office 365 services using their enterprise credentials.

The SSO Office 365 StyleBook allows you to enable SSO for Microsoft Office 365 through NetScaler instances. You can now configure SAML authentication with NetScaler as the SAML Identity Provider (IdP) and Microsoft Office 365 as the SAML service provider.

Enabling SSO for Microsoft Office 365 in a NetScaler instance using this StyleBook involves the following steps:

1. Configuring the authentication virtual server
2. Configuring a SAML IdP policy and profile
3. Binding the policy and profile to the authentication virtual server
4. Configuring an LDAP authentication server and policy on the instance
5. Binding the LDAP authentication server and policy to your authentication virtual server configured on the instance.

The table lists the minimum required software versions for this integration to work successfully. The integration process also supports higher versions of the same.

PRODUCT	MINIMUM REQUIRED VERSION
NetScaler	11.0, Advanced/Premium License

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The following instructions assume that you have already created the appropriate external and internal DNS entries. These entries are essential to route authentication requests to a NetScaler-monitored IP address.

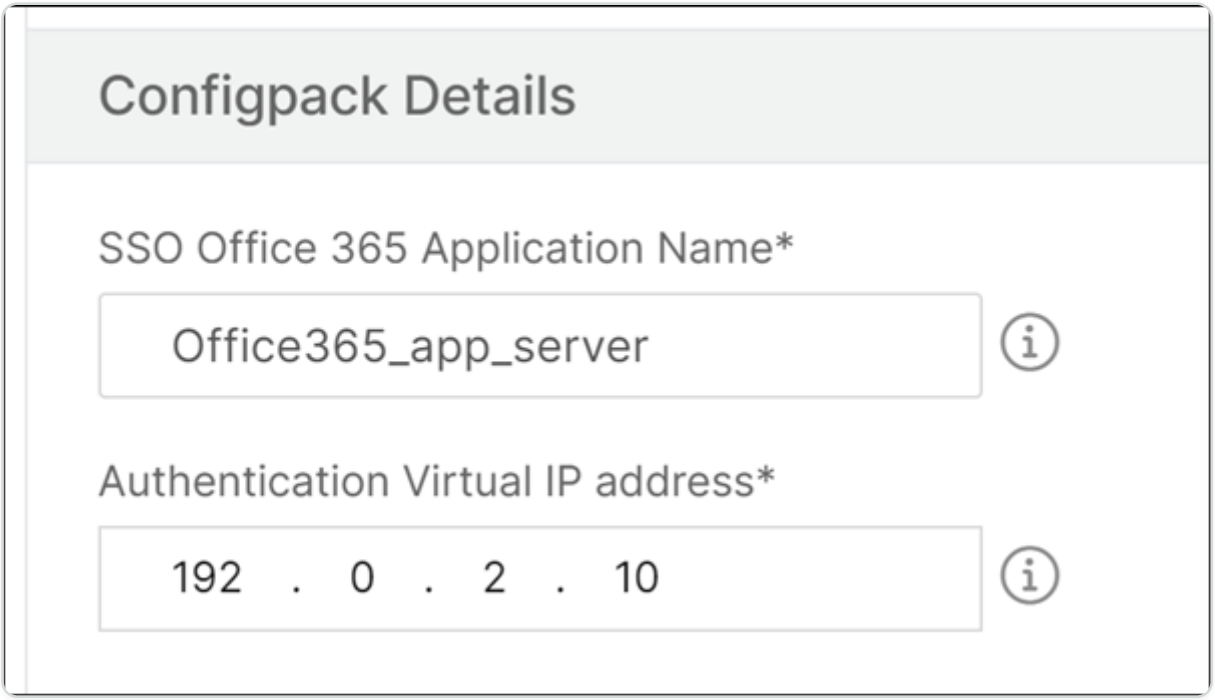
The following instructions assist you in implementing the SSO Office 365 StyleBook in your business network.

To deploy SSO Microsoft Office 365 StyleBook

1. In NetScaler Console, navigate to **Applications > Configuration > StyleBooks**. The **StyleBooks** page displays all the StyleBooks available for your use in NetScaler Console. Scroll down and find **SSO Office 365 StyleBook**. Click **Create Configuration**.
2. The StyleBook opens as a user interface page on which you can enter the values for all the parameters defined in this StyleBook.
3. Enter values for the following parameters:

    a. **Application Name**. Name of the SSO Microsoft Office 365 configuration to deploy in your network.

    b. **Authentication Virtual IP address**. Virtual IP address to be used by the NetScaler AAA virtual server to which the Microsoft Office 365 SAML IdP policy is bound.



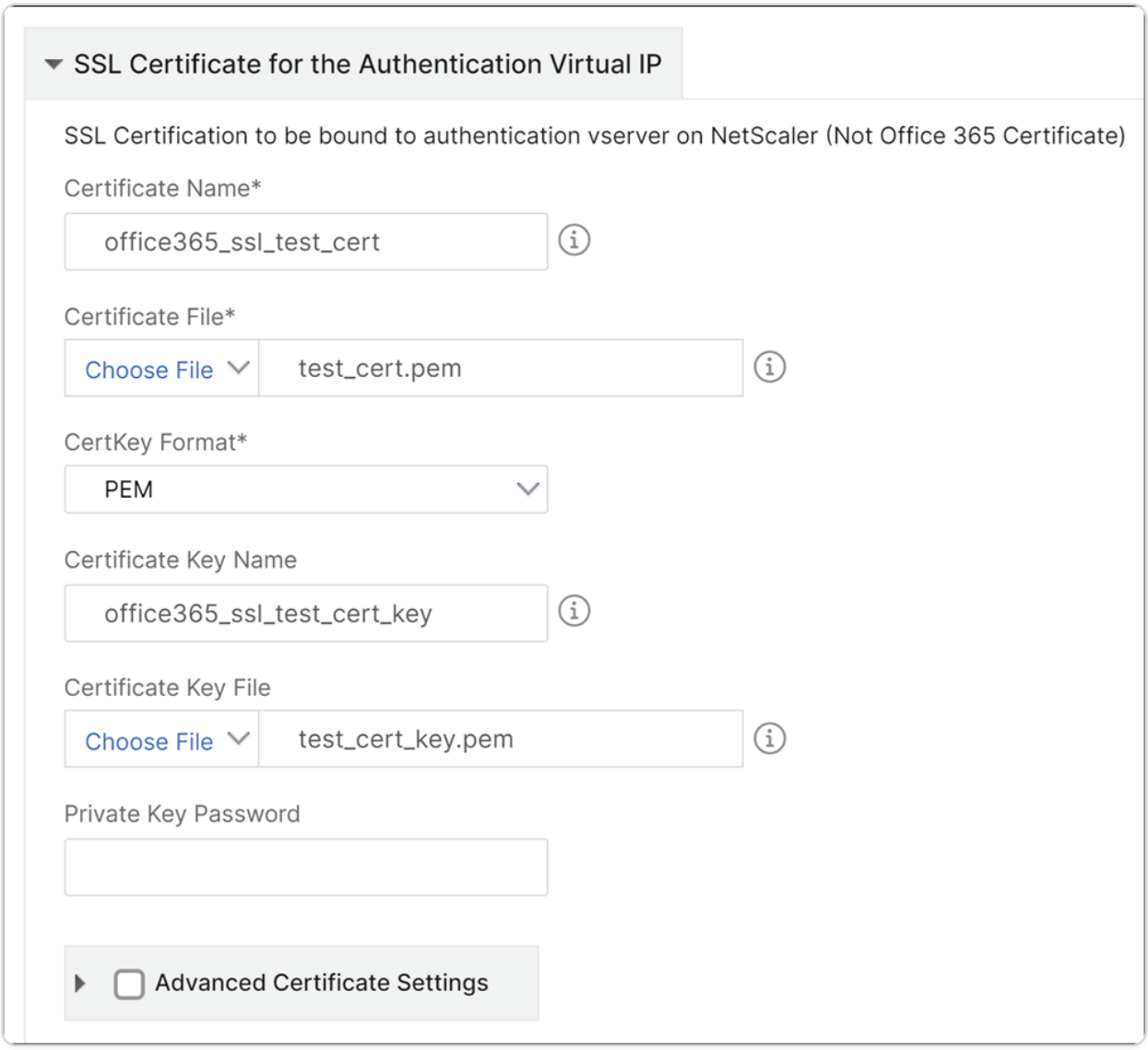
4. In **SSL Certificates Settings** section, enter the names of the SSL certificate and the certificate key.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

This is not the Office 365 service provider certificate. This SSL certificate is bound to the virtual authentication server on the NetScaler instance.

5. Select the respective files from your local storage folder. You can also type in the private key password to load encrypted private keys in PEM format.



6. You can also enable **Advanced Certificate Settings** check box. Here you can enter details such as certificate expiry notification period, enable or disable the certificate expiry monitor.
7. Optionally, you can select **SSL CA Certificate for the authentication virtual** IP check box if the SSL certificate requires a CA public certificate to be installed on NetScaler. Make sure you choose "Is a CA Certificate" in the above **Advanced Certificate Settings** section.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. In **LDAP Settings for SSO Office 365** section, enter the following details to authenticate Office 365 users. To allow domain users to log on to the NetScaler instance by using their corporate email addresses, configure the following:

    a. **LDAP (Active Directory) Base**. Enter the base domain name for the domain in which the user accounts reside within the Active Directory (AD) to allow authentication. For example, `dc=netscaler,dc=com`

    b. **LDAP (Active Directory) Bind DN**. Add a domain account (using an email address for ease of configuration) that has rights to browse the AD tree. For example, `cn=Manager,dc=netscaler,dc=com`

    c. **LDAP (Active Directory) Bind DN Password**. Enter the password of the domain account for authentication.

    d. A few other fields that you need to enter in this section are as follows:

        i. LDAP server IP Address that NetScaler connects to for authenticating users.

        ii. LDAP server's FQDN name.

        > **NOTE**
        >
        > You must specify at least one of the above two - the LDAP server IP address or the FQDN name.

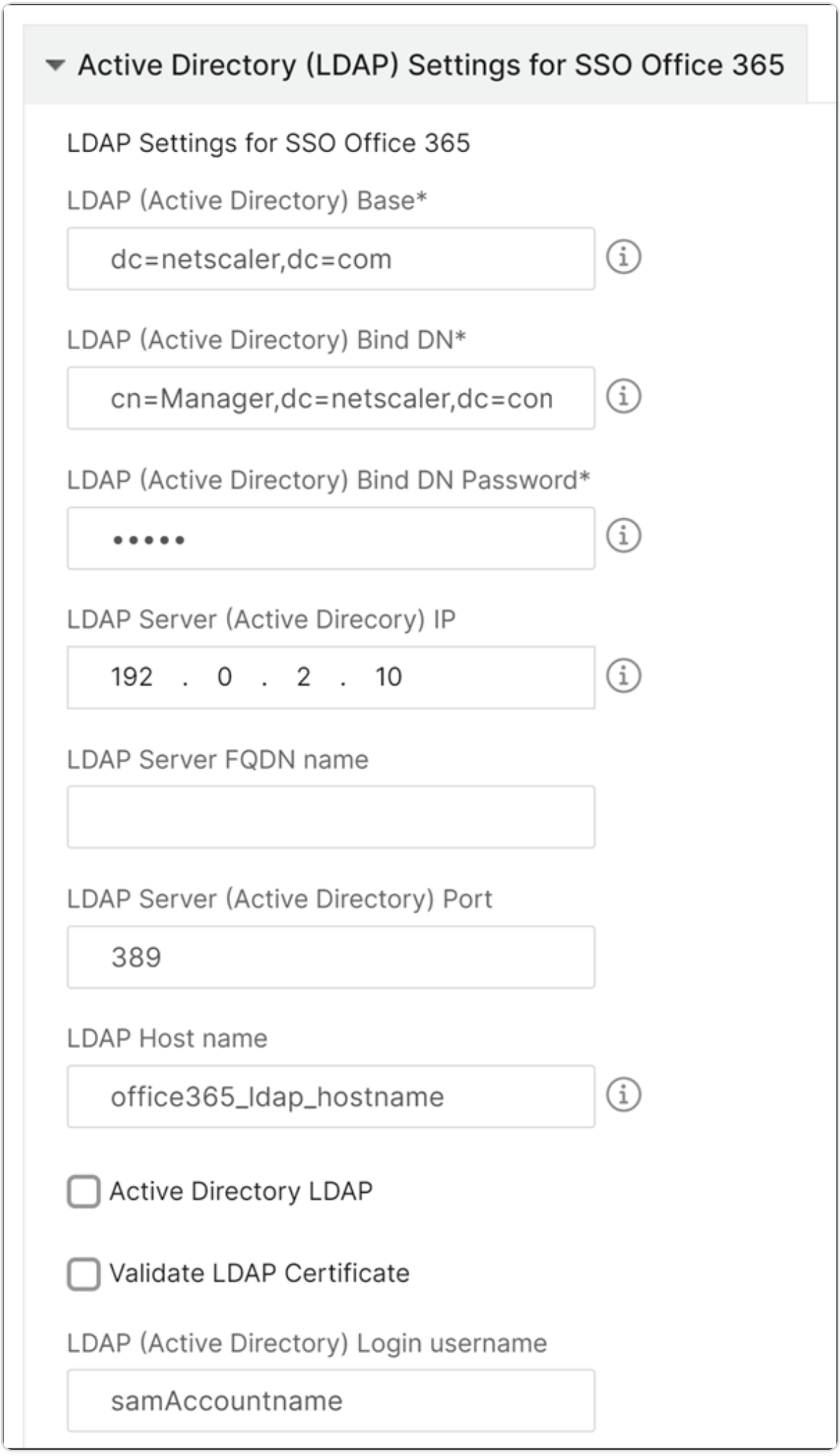
        iii. LDAP server port that NetScaler connects to for authenticating users (default is 389). LDAPS uses 636.

        iv. LDAP host name. The host name is used to validate the LDAP Certificate if validation is turned on (by default, it is turned off).

        v. LDAP login name attribute. The default attribute used to extract login names is "sAMAccountName."

        vi. Other optional miscellaneous LDAP settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.


Active Directory (LDAP) Settings for SSO Office 365
LDAP Settings for SSO Office 365
LDAP (Active Directory) Base*
dc=netscaler,dc=com
LDAP (Active Directory) Bind DN*
cn=Manager,dc=netscaler,dc=con
LDAP (Active Directory) Bind DN Password*
•••••
LDAP Server (Active Direcory) IP
192 . 0 . 2 . 10
LDAP Server FQDN name
LDAP Server (Active Directory) Port
389
LDAP Host name
office365_ldap_hostname
Active Directory LDAP
Validate LDAP Certificate
LDAP (Active Directory) Login username
samAccountname

9. In **SAML IdP Certificate** section, you can specify the details of the SSL certificates used for SAML assertion.

    a. **Certificate Name**. Enter the name of the SSL certificate.

    b. **Certificate File**. Choose the SSL certificate file from the directory on your local system.

    c. **CertKey Format**. Select the format of the certificate and the private-key files from the drop-down list box. The formats supported are .pem and .der extensions.

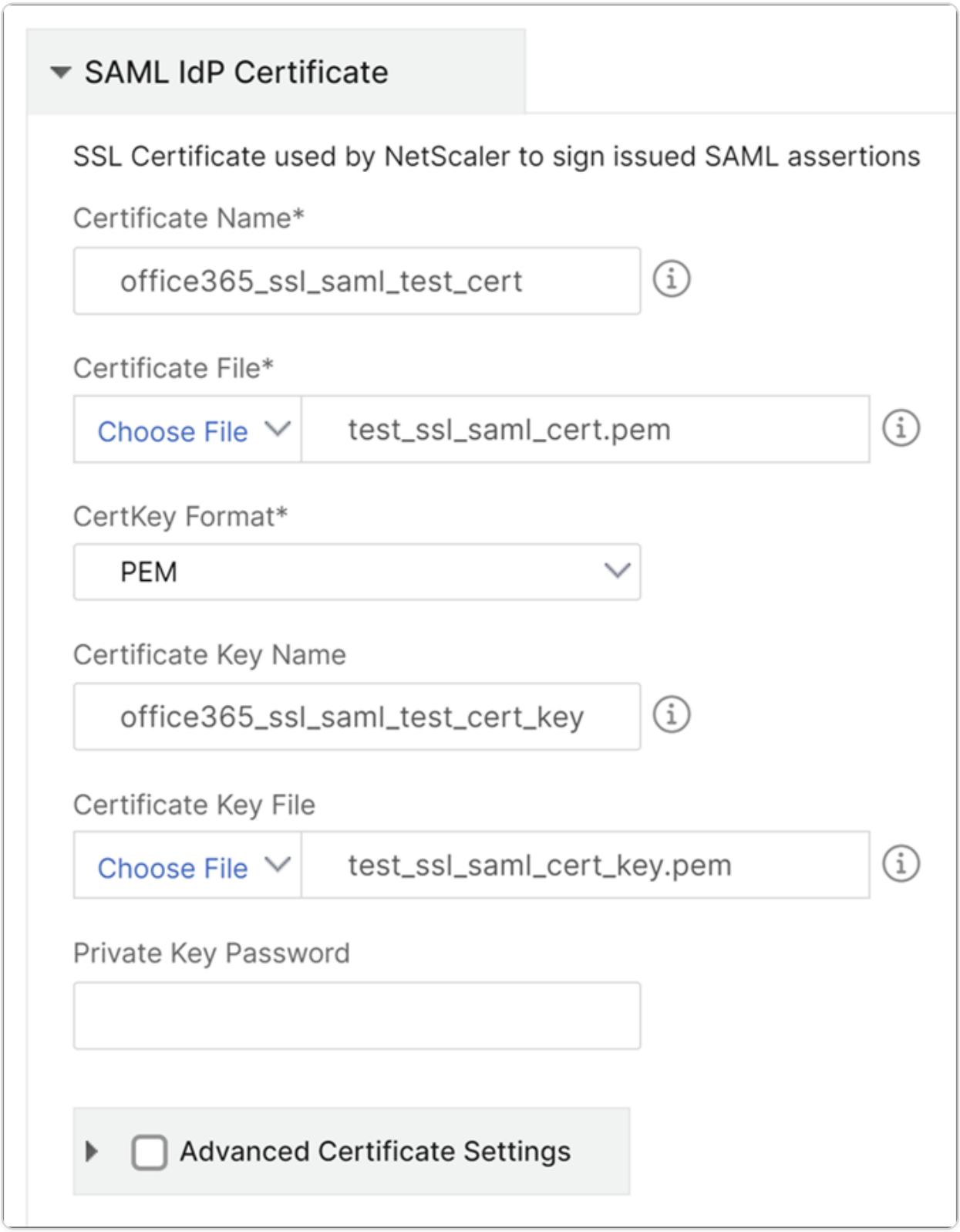
    d. **Certificate Key Name**. Enter the name of the certificate private key.

    e. **Certificate Key File**. Select the file containing the private key of the certificate from your local system.

    f. **Private Key Password**: Type in the passphrase that protects your private key file.

    You can also enable **Advanced Certificate Settings** check box. Here you can enter details such as certificate expiry notification period, enable or disable the certificate expiry monitor.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



10. Optionally, you can select **SAML IdP CA Certificate** if the SAML IdP certificate entered above requires a CA public certificate to be installed on NetScaler. Make sure you select "Is a CA Certificate" in the above **Advanced Certificate Settings** section.
11. In the **SAML SP Certificate** section, enter the following details for the Office 365 SSL public certificate. This certificate is used by the NetScaler instance to verify incoming SAML authentication requests.

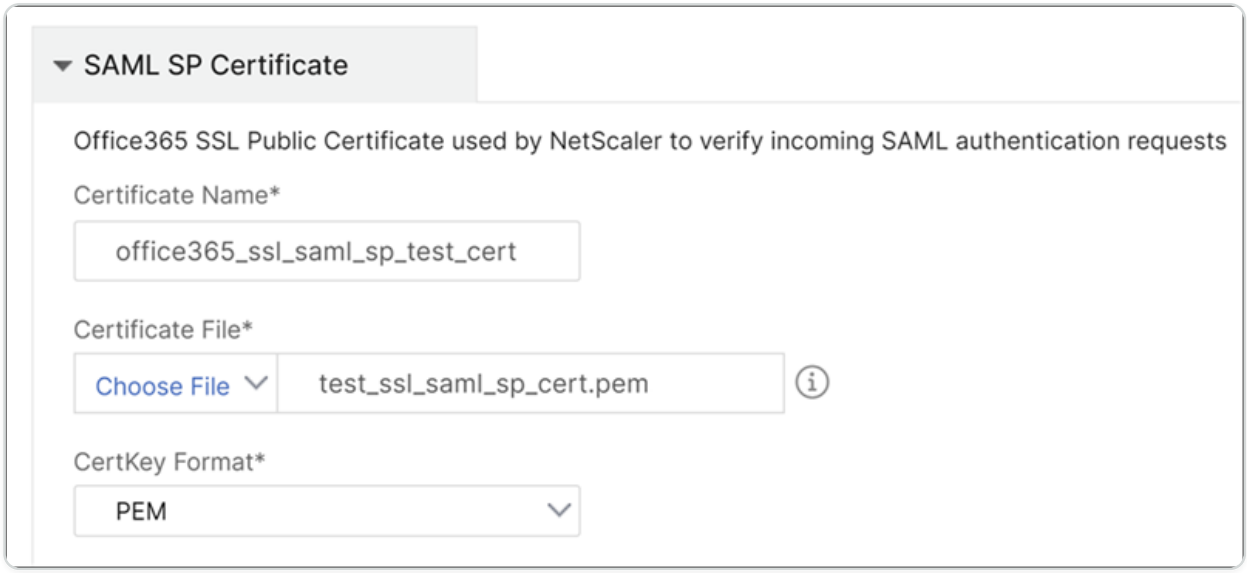
© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. **Certificate Name**. Type the name of the SSL certificate.

b. **Certificate File**. Choose the SSL certificate file from the directory on your local system.

c. **CertKey Format**. Select the format of the certificate and the private-key files from the drop-down list box. The formats supported are .pem and .der extensions.

You can also enable **Advanced Certificate Settings** check box. Here you can enter details such as certificate expiry notification period, enable or disable the certificate expiry monitor.



12. The **SAML Idp Settings** section allows you to configure your NetScaler Instance as a SAML identity provider by creating the SAML IdP profile and policy that is used by the NetScaler AAA virtual server created in step 3.

a. **SAML Issuer Name**. In this field, type the public FQDN of your authentication virtual server. Example: `https://<NetScaler_VIP_Address\>/saml/login`

b. **Name Identifier Expression**. Type in the NetScaler expression that is evaluated to extract the SAML NameIdentifier sent in the SAML assertion. Example: `"HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE"`

c. **Signature algorithm**: Select the algorithm to verify/sign SAML requests/responses (default is "RSA-SHA256").

d. **Digest Method**. Select the method to digest hash for SAML requests/responses (default is "SHA256").

e. **Audience name**. Type in the entity name or URL that represents the service provider (Microsoft Office 365).

f. **SAML Service Provider (SP) ID**. (optional) NetScaler identity provider accepts SAML authentication requests from an issuer name that matches this ID.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

g. **Assertion Consumer Service URL**. Enter the service provider's URL where NetScaler identity provider needs to send the SAML assertions after successful user authentication. The assertion consumer service URL can be initiated at the identity provider server site or the service provider site.

h. There are other optional fields that you can enter in this section. For example, you can set the following options:

   i. **SAML attribute name**. Name of user attribute sent in SAML Assertion.

   ii. **SAML attribute friendly name**. Friendly Name of the user attribute sent in SAML Assertion.

   iii. **PI expression for SAML attribute**. By default, the following NetScaler Policy (PI) expression is used: HTTP.REQ.USER.ATTRIBUTE(1). This field specifies the first user attribute sent from the LDAP server (mail) as the SAML authentication attribute.

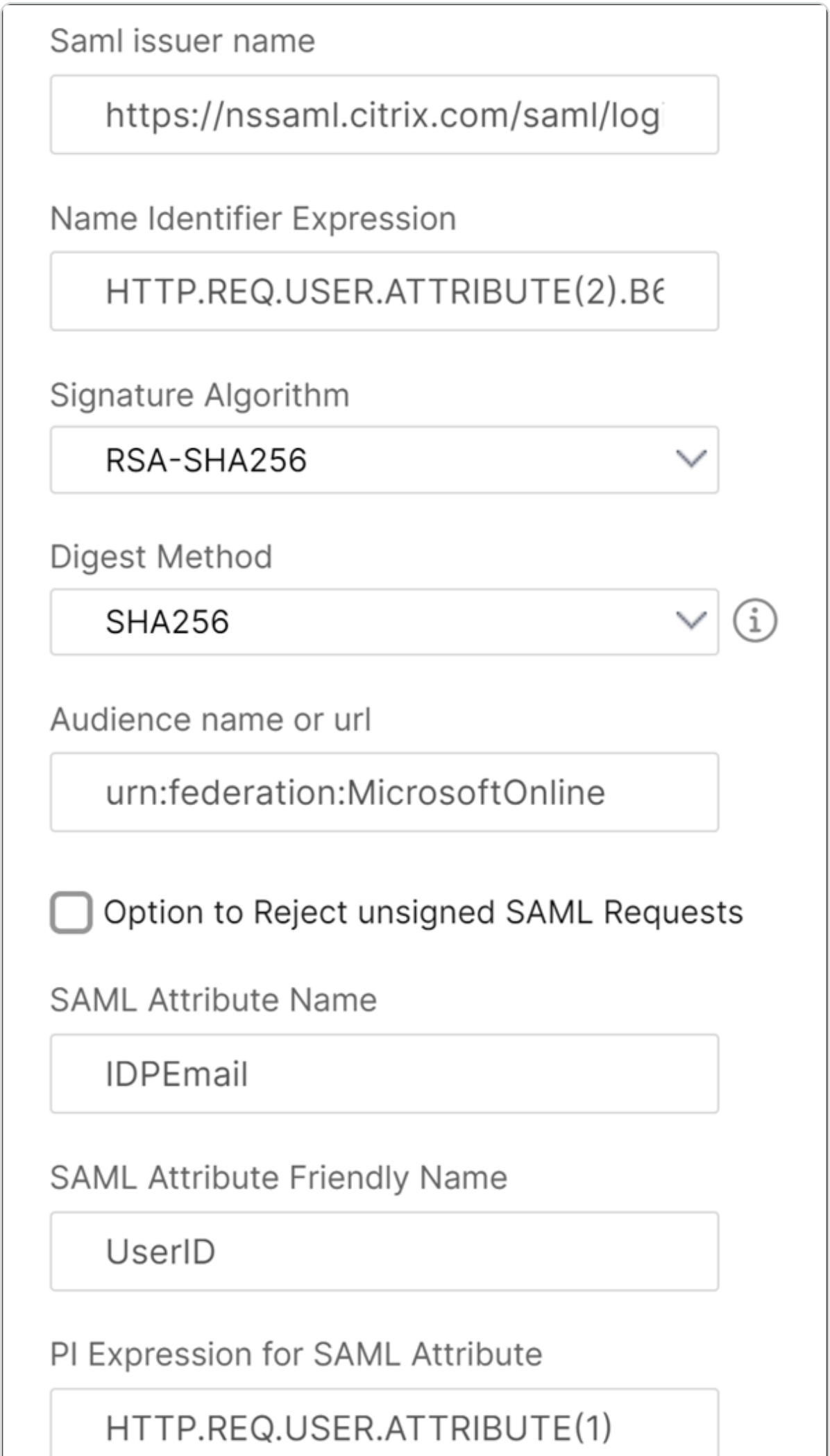
   iv. Select the format of the user attribute.

   These values are included in the issued SAML Assertion.

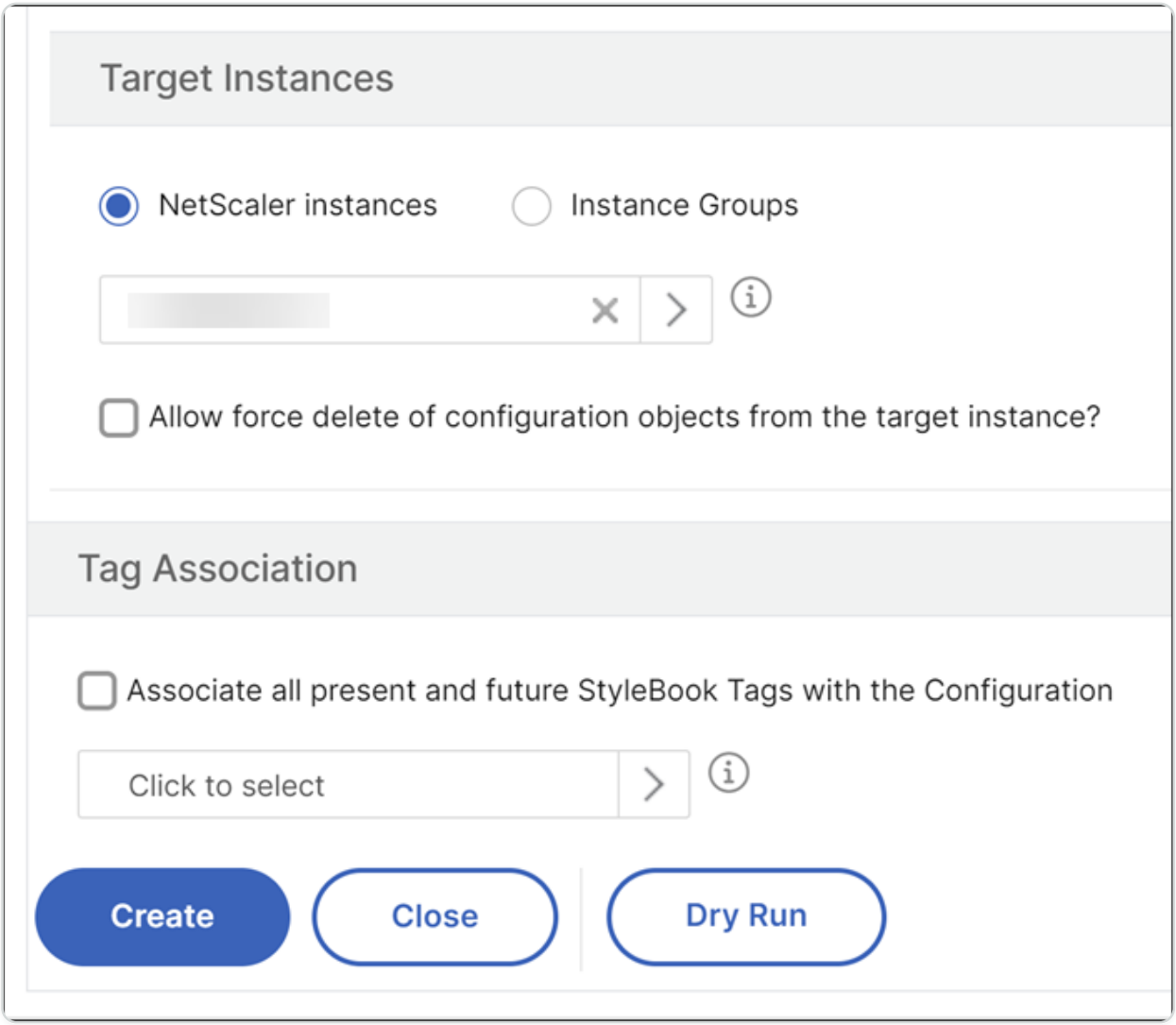
   TIP

   Citrix recommends that you retain the default settings as these settings have been tested to supportt Microsoft Office 365 apps.

© 1997–2026 Citrix Systems, Inc. All rights reserved.


Saml issuer name
https://nssaml.citrix.com/saml/log
Name Identifier Expression
HTTP.REQ.USER.ATTRIBUTE(2).B
Signature Algorithm
RSA-SHA256
Digest Method
SHA256
Audience name or url
urn:federation:MicrosoftOnline
Option to Reject unsigned SAML Requests
SAML Attribute Name
IDPEmail
SAML Attribute Friendly Name
UserID
PI Expression for SAML Attribute
HTTP.REQ.USER.ATTRIBUTE(1)

13. Click **Target Instances** and select the NetScaler instance(s) on which to deploy this Microsoft Office 365 SSO configuration. Click **Create** to create the configuration and deploy the configuration on the selected NetScaler instance(s).



TIP

Citrix recommends that before running the actual configuration, you select **Dry Run** to view the configuration objects that are created on the target NetScaler instances by the StyleBook.

Microsoft Skype for Business StyleBook

The Skype for Business 2015 application relies on several external components to function. The Skype for Business network consists of various systems, such as servers and their operating systems, databases, authentication and authorizing systems, networking systems and infrastructure,and telephone PBX systems. Skype for Business Server 2015 is available in two

© 1997–2026 Citrix Systems, Inc. All rights reserved.

versions, Standard Edition and Advanced Edition. The primary difference is in support for high-availability features that are only included in the Advanced Edition. To implement high availability, multiple Front-End servers must be deployed to a pool and SQL servers must be mirrored.

An Advanced Edition deployment enables the creation of multiple servers with different roles.

The primary components in Skype for Business 2015 application are:

- Front-End servers
- Edge Servers
- Director servers
- Database (SQL) servers

Front-end servers:

In the Skype for Business application, the Front-End server is the core server in your network. It provides the links and services for user authentication, registration, presence, address book, A/V conferencing, application sharing, instant messaging, and web conferencing. If you are deploying Skype for Business 2015 Enterprise edition, the topology typically consists of at least two Front-End servers load balanced in a Front-End pool with a database server that hosts the SQL Server instance holding the Skype for Business database.

Edge servers:

Deploying Edge Servers for Skype for Business is necessary if external users who are not logged into your

organization's internal network need to be able to interact with internal users. These external users can be authenticated and anonymous remote users, federated partners, or other mobile clients.

There are four types of roles in Skype for Business Edge Server:

- Access Edge, which handles SIP Traffic and authenticates external connections, allows remote connection and allows federation Connection
- Web Conferencing, which handles Data Conferencing Packets, and allows external users to access Skype for Business
- A/V Conferencing, which handles A/V Conferencing Packets, and extends audio and video, app sharing and file transfer to external users
- XMPP Proxy, which handles XMPP packets, and allows XMPP based servers or clients to connect to Skype for Business.

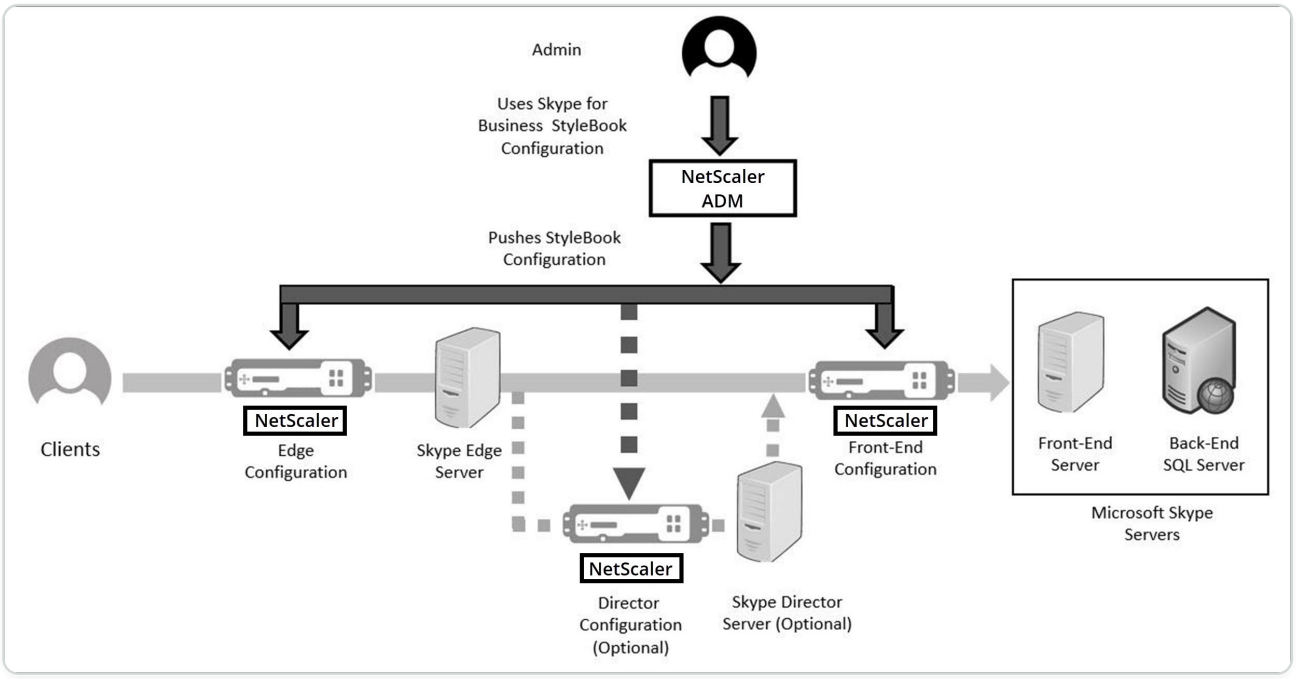
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Director servers:

The main function of the Director server in Skype for Business 2015 is to authenticate endpoints and "direct" the users to the pool that contains their account. In Skype for Business 2015, though the Director is a completely dedicated and specific role on a standalone server, it is an optional server. This facilitates security by making it easier to deploy or remove the configurations.

Directors are most useful where multiple pools exist because they provide a single point of contact for authenticating endpoints. Also, for remote users, a Director serves as an extra hop between the Edge pool and Front-End pool, adding an extra layer of protection against attacks.

The following figure diagrammatically represents the deployment of Skype servers in the network:



Configuring NetScaler instances in an enterprise

The following table lists the IP addresses used in the sample configuration included in the instructions below:

SKYPE FOR BUSINESS SERVERS	VIRTUAL IP ADDRESS	SERVER IP ADDRESSES	NETSCALER INSTANCE
Edge Servers	External VIP - 192.20.20.20	192.20.20.21; 192.20.20.22	10.102.29.141
	Internal VIP - 10.10.10.20	10.10.10.21; 10.10.10.22	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SKYPE FOR BUSINESS SERVERS	VIRTUAL IP ADDRESS	SERVER IP ADDRESSES	NETSCALER INSTANCE
Front-end Servers	10.10.10.10	10.10.10.11; 10.10.10.12	10.102.29.60
Director Server	10.10.10.30	10.10.10.31; 10.10.10.32	10.102.29.93

To configure front-end servers:

1. In NetScaler Console, navigate to **Applications** > **Configuration**, and click **Create New**. The **Choose StyleBook** page displays all the StyleBooks available for your use in NetScaler Console. Scroll down and select **Microsoft Skype for Business 2015 StyleBook**. The StyleBook opens as a user interface page on which you can enter the values for all the parameters defined in this StyleBook.
2. In the **Edge Server** section, enter the following virtual IP (VIP) addresses and IP addresses of all the Edge Servers in the network.
    a. External VIP address and IP addresses for the Edge Servers that will be used for Access Edge, web conferencing Edge, and A/V Edge.
    b. Internal VIP address and IP addresses for the Edge Servers that will be connected to the internal network.
    c. Two external and two internal Edge Servers in your network.
3. In the **Front-End Server** section, enter the IP address of the virtual Front-End server (VIP) that is to be created for the Skype for Business Front-End servers. Also, enter the IP addresses of all the Skype for Business Front-End servers in the network.
4. In the **Director Server** section, enter the virtual IP address (VIP) for the Director servers that is to be created for the Skype for Business application. Also, enter the IP addresses for all the Skype for Business Director servers in the network. Create at least two Director servers for high-availability.
5. The **Advanced Settings** section lists all the default ports configured on the NetScaler instances for the three Skype servers.

The following table provides you a list of all default ports and protocols:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LABEL	PORT	PROTOCOL	DESCRIPTION
HTTP Port	80	HTTP	Used for communication from Front-End Servers to the web farm FQDNs when HTTPS is not used.
HTTPS Port	443	HTTPS	Used for communication from Front-End Servers to the web farm FQDNs.
Auto Discover Internal Port	4443	HTTPS	HTTPS (from Reverse Proxy) and HTTPS Front-End inter-pool communications for Auto Discover sign-in.
RPC Port	135	DCOM and remote procedure call (RPC)	Used for DCOM based operations such as moving users, user replicator synchronization, and address book synchronization.
SIP Port	5061	TCP (TLS)	Used by Front-End servers for all internal SIP communications.
SIP Focus Port	444	HTTPS, TCP	Used for HTTPS communication between the Focus (the component that manages the Skype conference state)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LABEL	PORT	PROTOCOL	DESCRIPTION
			and the individual servers.
SIP Group Port	5071	TCP	Used for incoming SIP requests for the response group application.
SIP AppSharing Port	5065	TCP	Used for incoming SIP listening requests for application sharing.
SIP Attendant Port	5072	TCP	Used for incoming SIP requests for the attendant (that is, for dial-in conferencing).
`SIP Conf Announcement Port`	5073	TCP	Used for incoming SIP requests for the Skype for Business server conferencing announcement service (that is, for dial-in conferencing).
SIP CallPark Port	5075	TCP	Used for incoming SIP requests for the CallPark application.
SIP Call Admission Port	448	TCP	Used for call admission control by the Skype for Business server bandwidth policy service.
SIP Call Admission TURN Port	5080	TCP	Used for call admission control by the bandwidth policy service for Audio/

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LABEL	PORT	PROTOCOL	DESCRIPTION
			Video Edge TURN traffic.
SIP Audio Test Port	5076	TCP	Used for incoming SIP requests for the audio test service.
HTTPS External Port	443	HTTPS	Used for external ports for SIP/ TLS communication for remote user access, accessing internal Web conferences, and STUN/TCP inbound and outbound media communications for accessing internal media and A/V sessions.
HTTPS Internal Port	443	HTTPS	Used for internal ports for SIP/ TLS communication for remote user access, accessing internal Web conferences, and STUN/TCP inbound and outbound media communications for accessing internal media and A/V sessions.
SIP External Remote Access Port	5061	TCP	Used for external ports for SIP/MTLS communication for remote user access or federation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LABEL	PORT	PROTOCOL	DESCRIPTION
SIP Internal Remote Access Port	5061	TCP	Used for internal ports for SIP/MTLS communication for remote user access or federation.
SIP External STUN UDP Port	3478	UDP	Used for external ports for STUN/ UDP inbound and outbound media communications.
SIP Internal STUN UDP Port	3478	UDP	Used for internal ports for STUN/UDP inbound and outbound media communications.
SIP Internal IM Port	5062		Used for internal ports for SIP/MTLS authentication of IM communications flowing outbound through the internal firewall.
HTTP Port	80	TCP	Used for initial communication from Directors to the web farm FQDNs.
HTTPS Port	443	HTTPS	Used for communication from Directors to the web farm FQDNs.
Auto Discover Internal Port	4443	HTTPS	Used for HTTPS (from Reverse Proxy) and HTTPS Director inter-pool communications for

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LABEL	PORT	PROTOCOL	DESCRIPTION
			Auto Discover sign-in.
SIP Internal Port	5061	TCP	Used for internal communications between servers and for client connections.

1. In the **Target Instances** section, select the three different NetScaler instance on which to deploy the three Skype for Business servers.

   NOTE

   You can also click the refresh icon to add recently discovered NetScaler instances in NetScaler Console to the available list of instances in this window.

2. Click **Create** to create the configuration on the selected NetScaler instances.

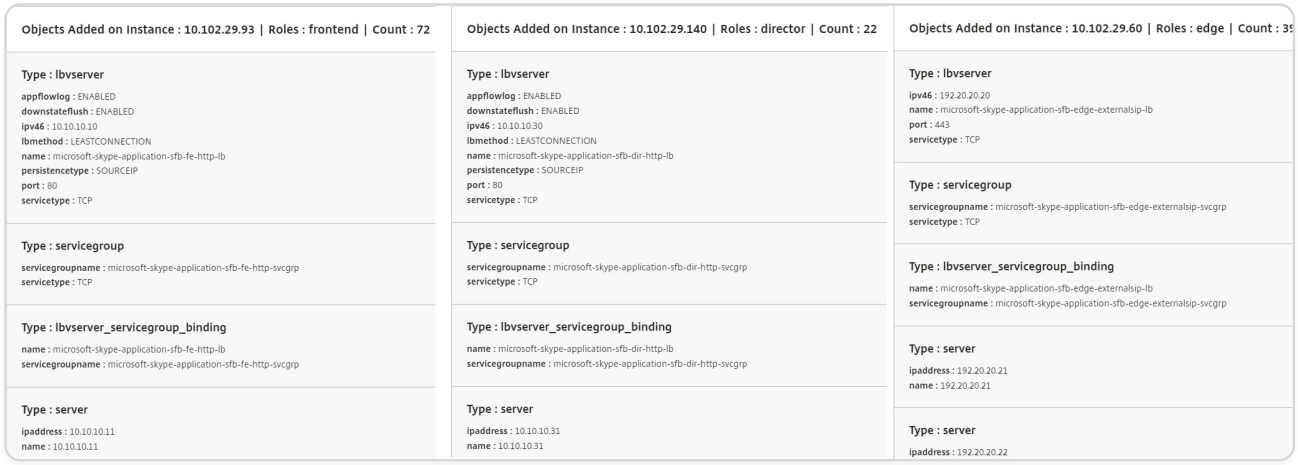
   TIP

   Citrix recommends that you select **Dry Run** to check the configuration objects that must be created on the target instance before you run the actual configuration on the instance.

When the configuration is successfully created, the StyleBook creates 25 load balancing virtual servers. That is, for each port, one load balancing virtual server is defined along with one service group, and the service group is bound to the load balancing virtual server. The configuration also adds the Front-End servers as service group members and binds them to the service group. The number of service group members created is equal to the number of Front-End servers created.

The following figure shows the objects created in each server:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Microsoft Exchange StyleBook

You can use the Microsoft Exchange 2016 StyleBook to deploy a NetScaler configuration that optimizes and secures a Microsoft Exchange 2016 enterprise application in your network. Microsoft Exchange 2016 is a key enterprise application for providing email, personal information management, and messaging services to your employees and other stakeholders.

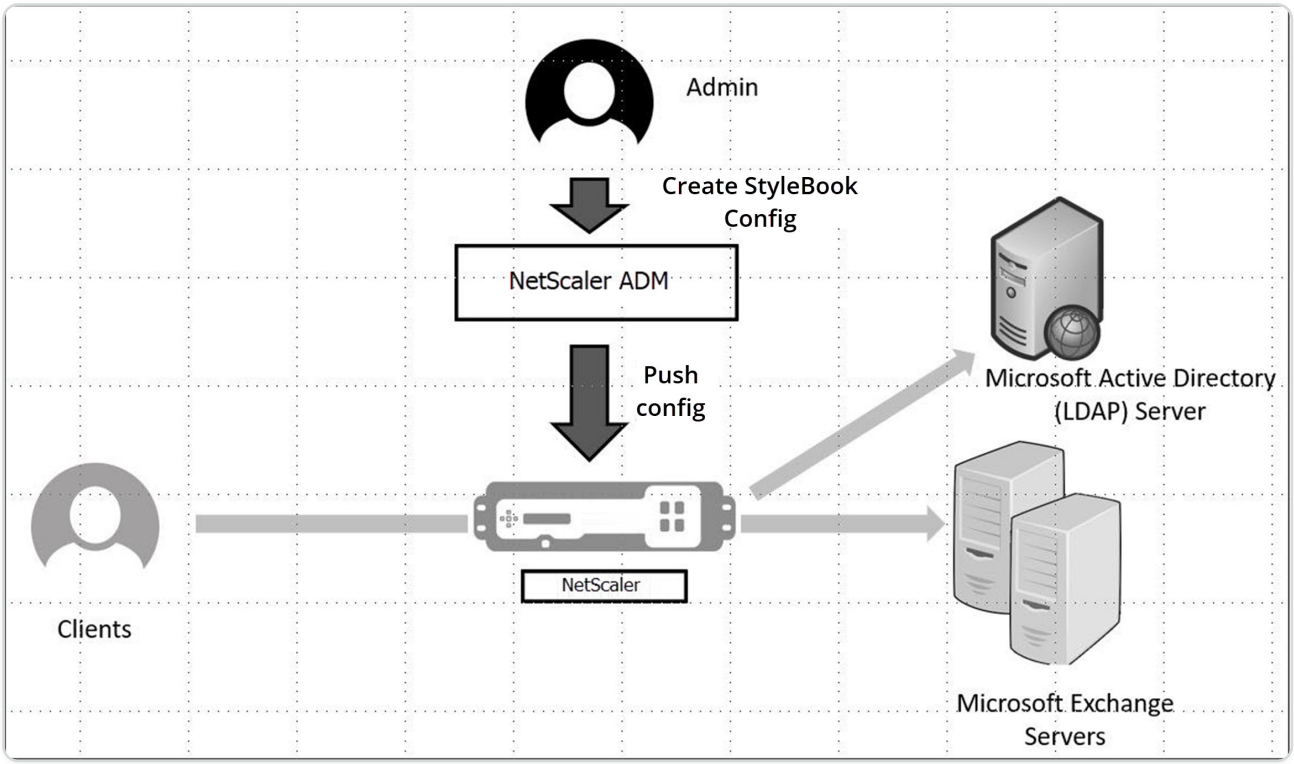
NetScaler features configured by using Microsoft Exchange StyleBook

The Microsoft Exchange 2016 StyleBook enables and configures the following NetScaler features for Microsoft Exchange 2016 servers:

- Load balancing - Basic load balancing that enables load balancing of multiple Exchange servers
- Content switching - Content switching that enables single-IP access and redirection of queries to the correct load balancing virtual servers
- Rewrite - Redirects users to secure pages
- SSL offload - Offloads SSL processing to the NetScaler, therefore reducing the load on the Exchange server

The following figure diagrammatically represents the deployment of Exchange servers in the network:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Prerequisites

- For certificate-based authentication, all addressable hosts that are part of the network setup must have resolvable domain names and not just IP addresses.
- Ensure that the SIP ports are accessible in Microsoft Exchange 2016 server.

Configuring Microsoft Exchange StyleBook

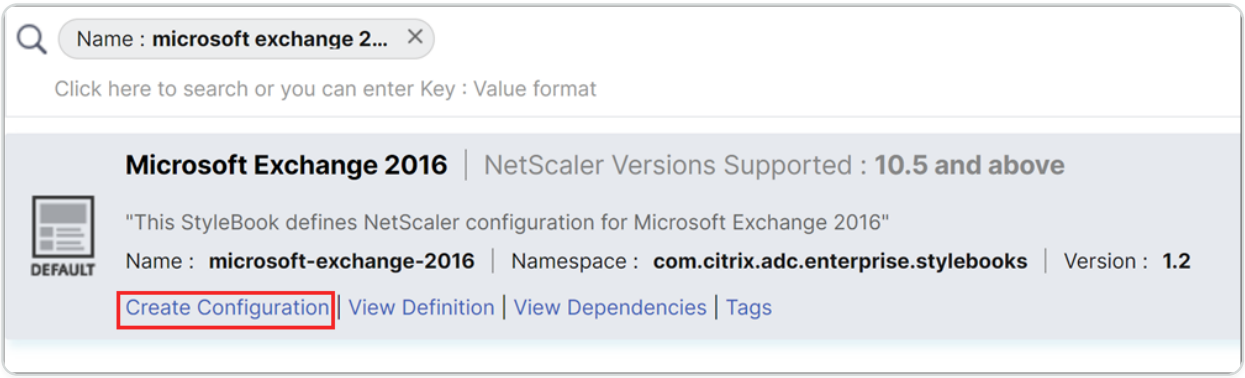
Configure the Microsoft Exchange StyleBook in your business enterprise to deploy the NetScaler configuration.

To configure Microsoft Exchange application

1. In NetScaler Console, navigate to **Applications > Configuration > StyleBooks**.
2. Search for **Microsoft Exchange 2016 StyleBook** and click **Create Configuration**.

   The StyleBook appears as a user interface form on which you can enter the values for all the parameters defined in this StyleBook.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Enter the details for the following parameters:

   - **Exchange Application Name** - Name of the Microsoft Exchange Application in your network
   - **Exchange VIP** - Virtual IP address on NetScaler that receives client requests for the Microsoft Exchange application
   - **Exchange Server IPs** - IP addresses of all the Exchange servers in the network.

     If you want to add more IP addresses, click the plus (**+**) icon. Usually, two Exchange servers are configured in the network.

4. In the **Exchange Certificates** section, upload exchange certificates to NetScaler Console. Enter the names of both the certificate and the key files and upload from the local storage. You can also provide a private key password to encrypt the key file.

   NOTE

   Ensure that the certificate files are of ".pem" or ".der" format. NetScaler Console rejects the files of other formats.

   If you want to specify certificate expiration details or any advanced settings, select **Advanced Certificate Settings**.

5. In the **Exchange Active Directory Authentication config** section, configure the AD Settings by entering the data.

   - **Active Directory Authentication VIP** - The virtual IP address used to create and configure the AD (LDAP) virtual server on a NetScaler appliance.
   - **Active Directory Server IP** - The IP address of your Active Directory domain controller.
   - **Active Directory Base String** - The LDAP Base String in Active Directory. For example, CN=Users,DC=CTXNSSFB,DC=COM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Active Directory LDAP Bind Distinguished Name (DN)** - LDAP Bind Distinguished Name (DN) is used to bind this object to the LDAP server (AD). For example "cn=Administrator,cn=Users,dc=acme,dc=com"
- **Active Directory LDAP Bind Distinguished Name (DN) Password** - LDAP Bind Distinguished Name (DN) is the password for AD Authentication
- **Active Directory User Name Attribute** - AD attribute for the user name. The NetScaler uses the LDAP attribute to query external Active Directory Servers. For example, "sAMAccountName"
- **Active Directory group Attribute Name** - the LDAP group attribute names configured on the LDAP server. For example, "memberOf" for the group attribute in LDAP.
- **Active Directory Sub-Attribute Name** - the LDAP subattribute names configured on the LDAP server. For example, "cn" for the subattribute in LDAP.
- **Active Directory Authentication Domain** - The AD/LDAP domain name used for authentication. For example, ctxnssfb.com.

6. In the **Target Instances** section, select the NetScaler instance on which to deploy this Exchange configuration.

   NOTE

   If you want to view the recently discovered NetScaler instances, click the refresh icon.

7. Click **Create** to create the configuration file and run the configuration on the selected NetScaler instance.

   Citrix recommends that you first select **Dry Run** to check the configuration objects that are created on the target instance before running the actual configuration on the instance.

When the configuration has been created successfully, the StyleBook has created a content switching virtual server, five load balancing virtual servers, and one LDAP policy bound to one LDAP authentication virtual server. Also, the corresponding service groups created and bound to the load balancing virtual servers.

Microsoft SharePoint StyleBook

Microsoft SharePoint 2016 is a key enterprise application that primarily provides a document management and storage system, which is highly configurable and supported by all major browsers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can use the Microsoft SharePoint 2016 StyleBook to deploy a NetScaler configuration that optimizes and secures the Microsoft SharePoint 2016 enterprise application in your network.

Prerequisites

- Microsoft SharePoint 2016
- NetScaler Console, version 12.0 and later
- NetScaler, version 10.5 and later

NetScaler features configured by the Microsoft SharePoint 2016 StyleBook

You can use the Microsoft SharePoint 2016 StyleBook to enable and configure the following NetScaler features for Microsoft SharePoint 2016:

- Load balancing
- Content Switching
- Responder
- Rewrite
- Compression
- Integrated Caching

LOAD BALANCING

NetScaler load balancing evenly distributes requests to back end SharePoint servers. Intelligent monitoring of back end servers prevents requests from being sent to malfunctioning servers.

The SharePoint StyleBook configures 12 load balancing virtual servers, each dedicated to load balancing requests for a certain type of content, such as documents, images, audio, video, and other file types.

NetScaler Console now supports SSL Mode of SharePoint application by configuring SSL based LB virtual servers. Make sure you select SSL as the front-end protocol. Note that the virtual port is set to 443 by default.

CONTENT SWITCHING

The content switching feature is used to distribute client requests across multiple load balancing virtual servers on the basis of specific types of requested SharePoint content (for example, documents, images, and audio or video files). The content switching module directs incoming traffic to an optimal matching load balancing virtual server that can process that type of content. You can therefore apply different optimization policies to different types of traffic. For example, you might want to use different compression or caching policies for video than for text documents.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RESPONDER

The responder functionality of a NetScaler instance can be used to seamlessly redirect users from HTTP to HTTPS. Responder can also be configured to provide customized error pages. The Responder policy determines the requests (traffic) on which an action has to be taken, and binds each policy to a load balancing virtual server. The SharePoint StyleBook includes a configuration that redirects users from HTTP to HTTPS URLs.

REWRITE

The rewrite module is used to modify request/response headers, URLs, or content on the fly. This module works in-line with traffic processing and can therefore change the traffic flow as appropriate for particular use cases. For example, rewriting can provide access to the requested content without exposing unnecessary details about the website's server.

In the SharePoint StyleBook, the rewrite feature is used to removed unnecessary headers from user requests.

COMPRESSION

The NetScaler compression engine identifies and compresses content that is compressible. This process improves data transmission time and reduces network bandwidth requirements for the clients, while saving CPU cycles on SharePoint content servers. A NetScaler instance can compress both static and dynamically generated data. It applies the GZIP or the DEFLATE compression algorithm to remove extraneous and repetitive information from the server responses and represent the original information in a more compact and efficient format. The client browser's ability to decompress the data depends on which algorithm or algorithms it supports: GZIP, DEFLATE, or both of these.

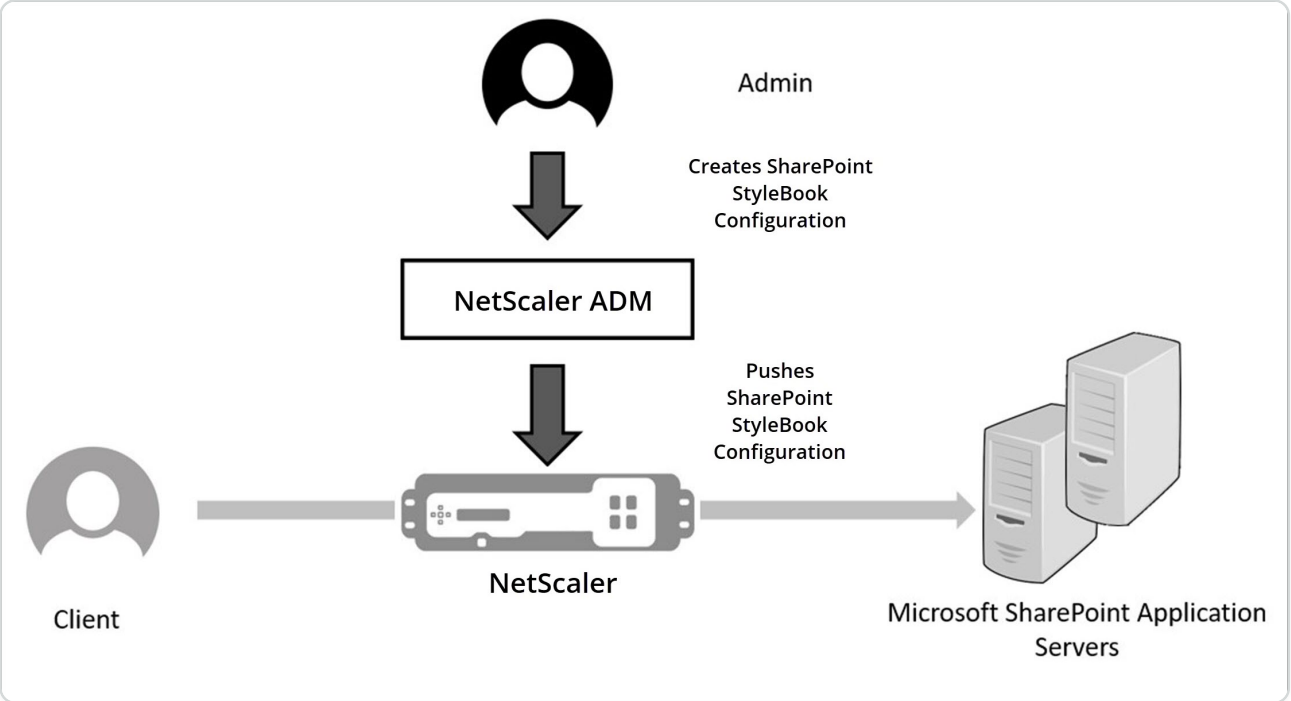
A NetScaler instance is configured to compress the text in HTML, XML, plain text, Cascading Style Sheet (CSS), and Microsoft Office documents, but does not compress images in GIF or JPG format. The major benefits of compressed traffic include reduced bandwidth costs, WAN latency reduction, and better server performance.

INTEGRATED CACHING

The NetScaler in-memory cache can store SharePoint objects in order to quickly deliver frequently requested content to users. Cached content includes downloaded documents and audio, video, and image files.

The following figure diagrammatically represents the deployment of SharePoint servers in a network front-ended by a NetScaler instance on which NetScaler Console is used to deploy a SharePoint StyleBook configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Deploying SharePoint StyleBook configurations

The following task will assist you in deploying the Microsoft SharePoint 2016 StyleBook in your business network.

To deploy Microsoft SharePoint 2016 StyleBook:

1. In NetScaler Console, navigate to **Applications** > **Administration** > **Configuration**, and click **Create New**.

   The **Choose StyleBook** page displays all the StyleBooks available for your use in NetScaler Console.

2. Scroll down and select **Microsoft SharePoint 2016 StyleBook**.

   NOTE

   In NetScaler Console, navigate to **Applications** > **Configurations** > **StyleBooks**. Scroll down to find the **Microsoft SharePoint 2016 StyleBook**. In the **Microsoft SharePoint 2016 StyleBook** panel, click **Create Configuration**.

   The StyleBook opens as a user interface form on which you can enter the values for all the parameters defined in this StyleBook.

   Enter values for the following parameters:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. **SharePoint Application Name**. Name of the SharePoint configuration to deploy in your network.

b. **SharePoint Virtual IP**. Virtual IP address at which the NetScaler instance receives client requests for the Microsoft SharePoint application.

c. **SharePoint Virtual Port**. The TCP Port to be used by the Users in accessing the SharePoint application

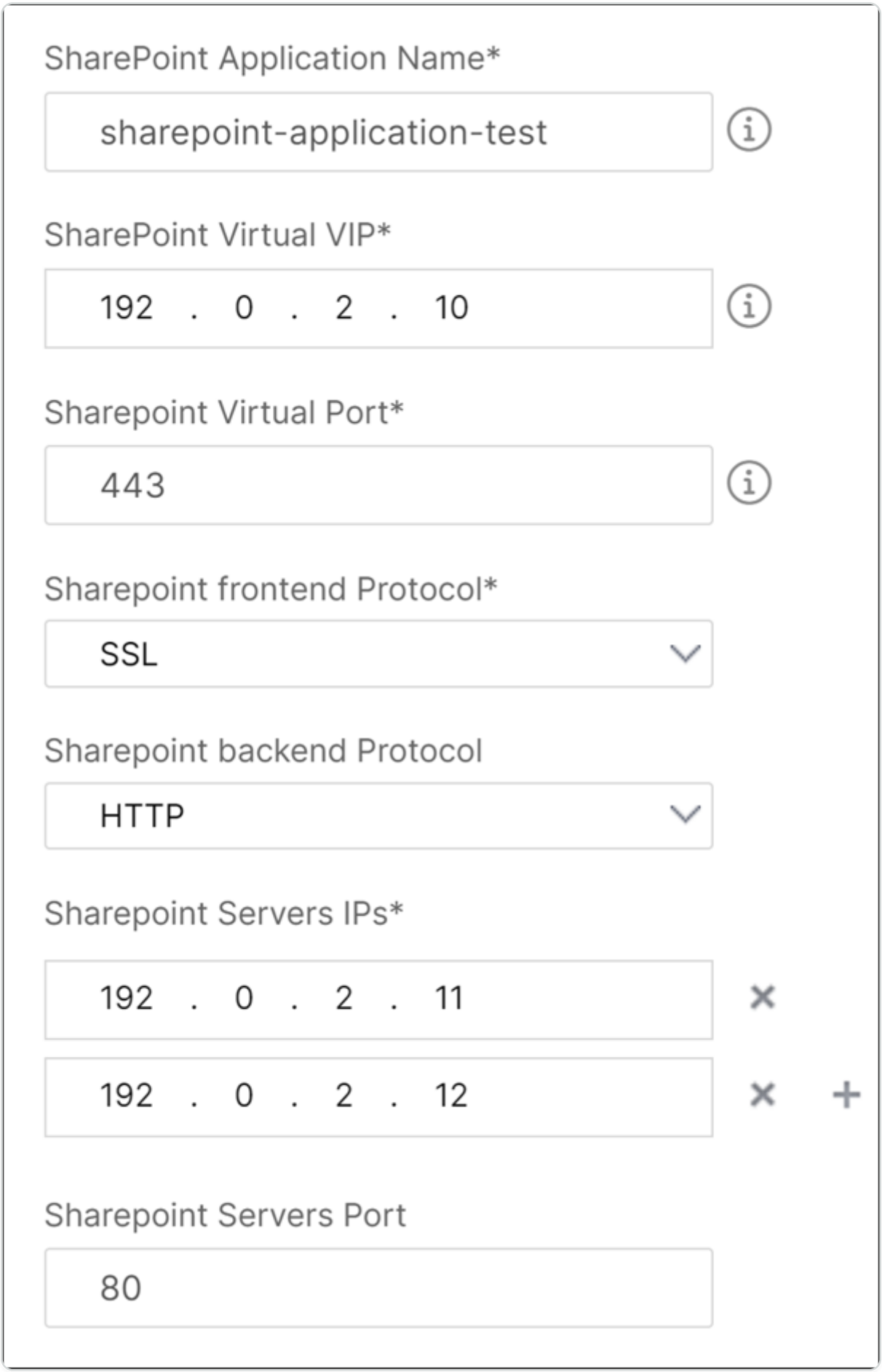
d. **SharePoint frontend Protocol**. Select the SharePoint front end protocol from the drop-down list. The options available are HTTP or SSL.

> **NOTE**
>
> If you select SSL, make sure that the Rewrite Configuration parameter is enabled in the SharePoint Advanced Settings section in this StyleBook.

e. **SharePoint Server IPs**. IP addresses of all the SharePoint servers in the network.

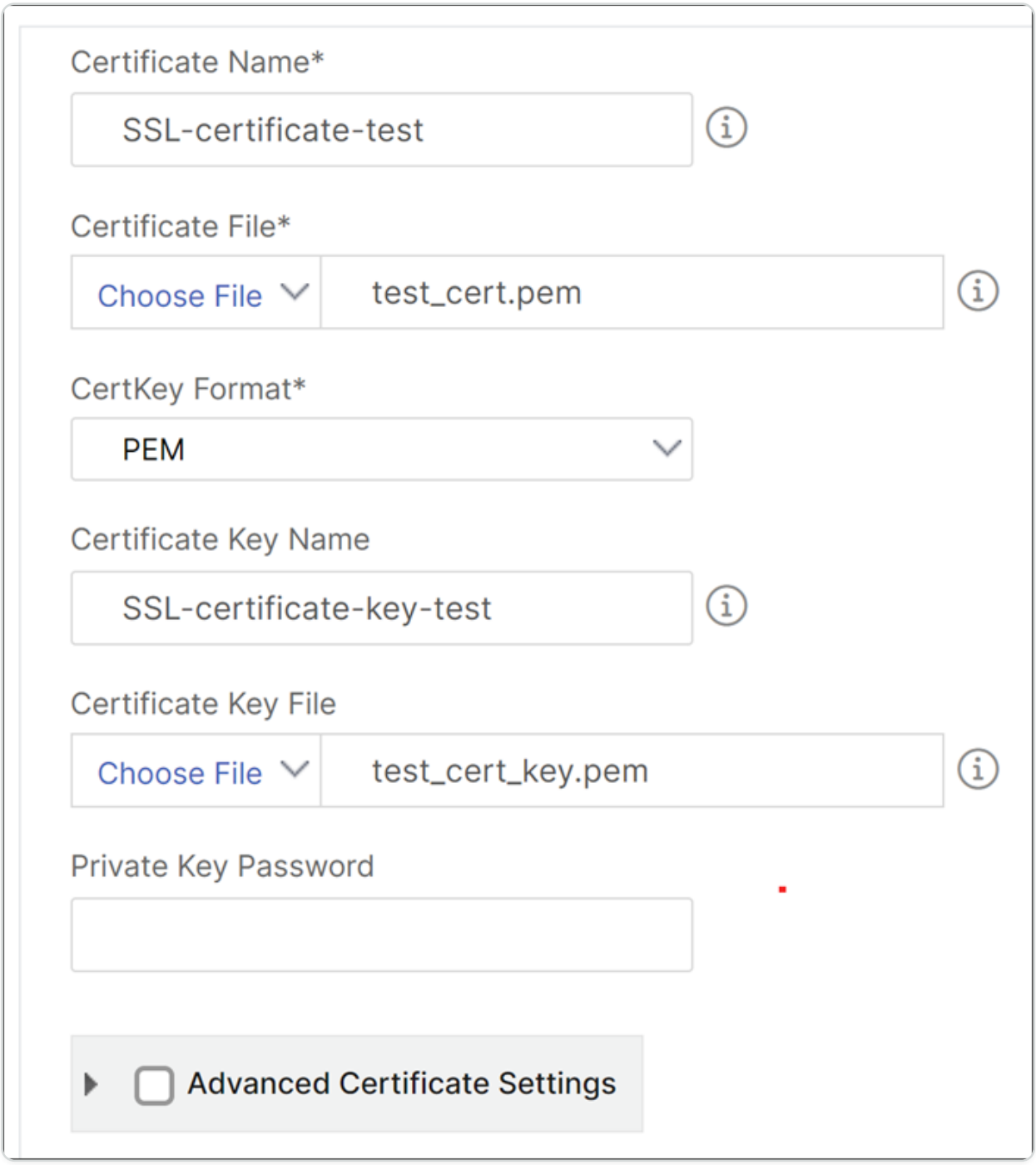
f. **SharePoint Servers Port**. TCP port number used by the SharePoint servers. By default, this is 80. You can edit this value if required, but make sure that this port is accessible on Microsoft SharePoint 2016 servers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



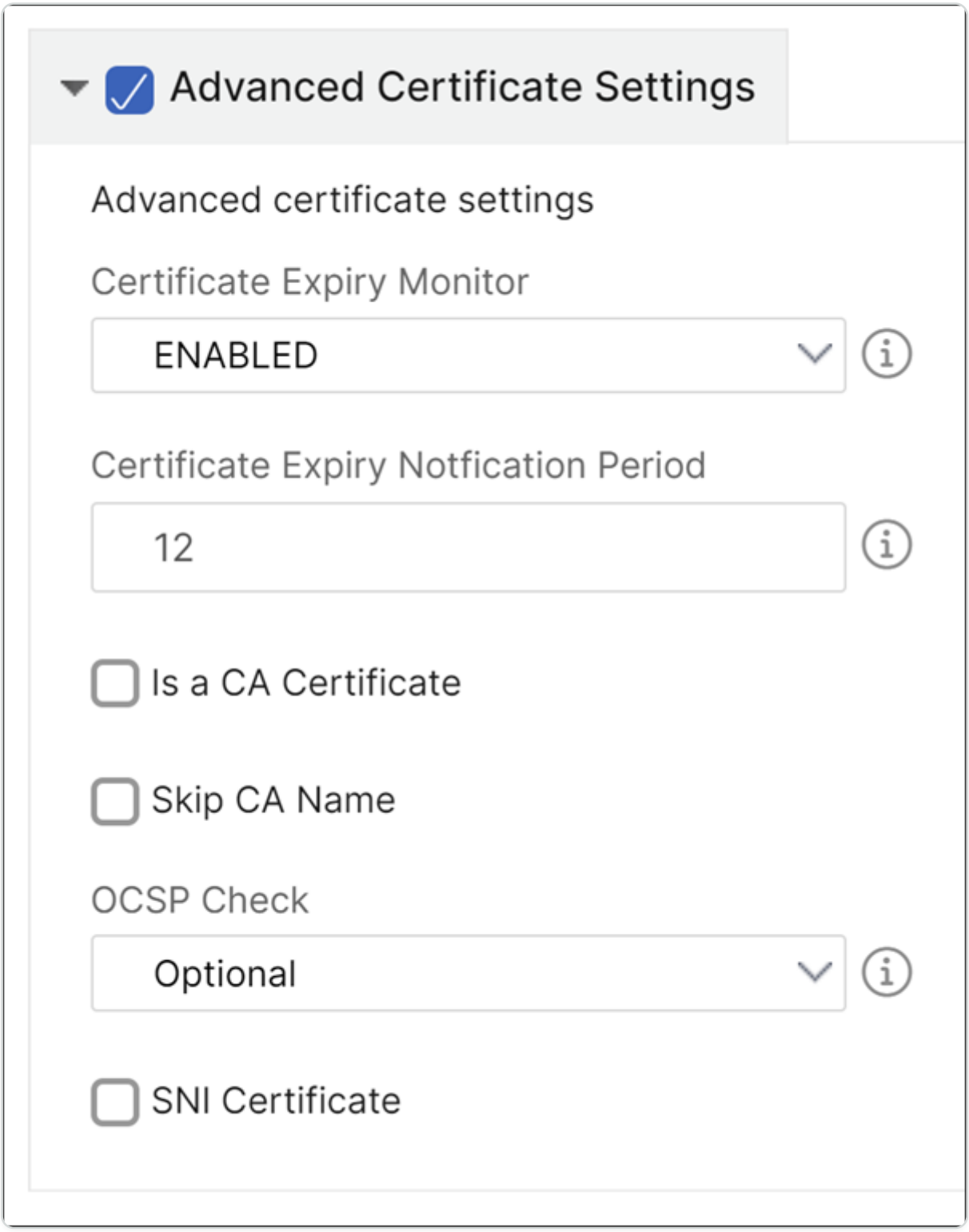
© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. In the **SSL Certificates settings** section, click + to enter the name of the SSL certificate, the certificate key, and select the respective files from your local storage folder.



4. Optionally click **Advanced Certificate Settings** to enable or disable SSL certificate expiry monitoring. If you enable the certificate expiry monitoring, set the number of days so that NetScaler Console issues an alarm after these many days when the certificate is about to expire. You also have an option to make the OCSP checking as an optional feature or a mandatory feature.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



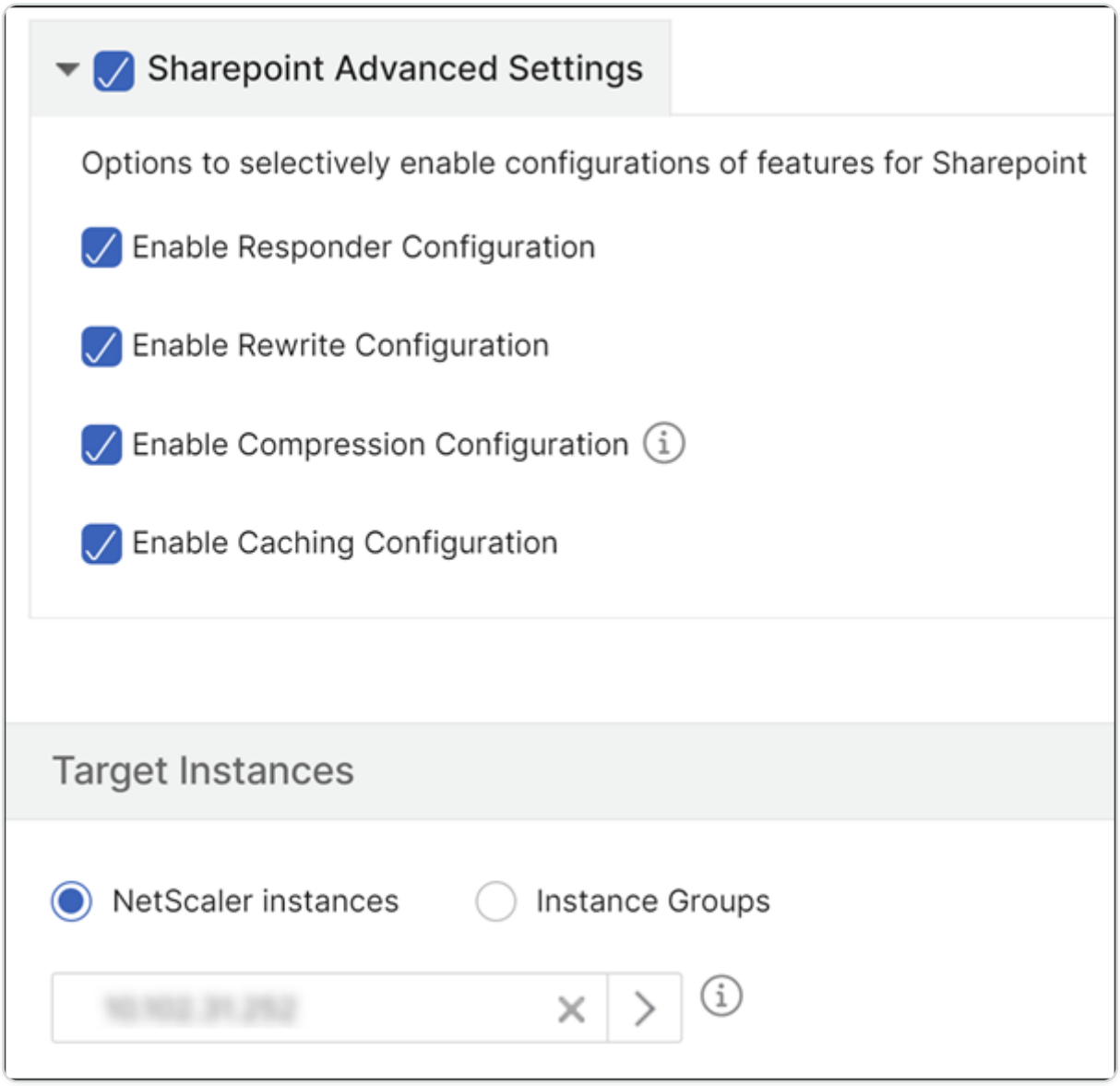
5. The SharePoint **Advanced Settings** section allows you to enable the NetScaler features that will be configured on the NetScaler instances. While the load balancing and content switching features are configured on the instances by default, you can choose the other features, that is, responder configuration, rewrite configuration, compression configuration, and integrated caching configuration, that you want to be configured on the instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Click **Target Instances** and select the NetScaler instance on which to deploy this SharePoint configuration. Click **Create** to create the configuration and deploy the configuration on the selected NetScaler instance.

   NOTE

   You can also click the refresh icon to add recently discovered NetScaler instances in NetScaler Console to the available list of instances in this window.



NOTE

Citrix recommends that before running the actual configuration, you select **Dry Run** to check the configuration objects that will be created on the target instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When the configuration is created and successfully deployed, the SharePoint StyleBook creates one content switching virtual server and 12 load balancing virtual servers. It also creates policies and service groups and binds them to the load balancing virtual servers. Which policies are created depends on the features selected in the StyleBook during creation of the configuration pack.

Viewing the objects defined on the NetScaler instance

After the configuration pack is created on NetScaler Console, you can view all the objects created on the NetScaler instance for the SharePoint StyleBook. Navigate to **Applications** > **Administration** > **Configuration**, and click **View Objects Created**. The following figure shows some of the created objects, with the IP addresses specified in the example shown in "Deploying SharePoint StyleBook Configurations from NetScaler Console."

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type : lbvserver

appflowlog : DISABLED
backuppersistencetimeout : 20
downstateflush : DISABLED
ipv46 : 0.0.0.0
lbmethod : LEASTCONNECTION
name : sharepoint application test frontpage services lb
persistencebackup : SOURCEIP
persistencetype : COOKIEINSERT
port : 0
servicetype : HTTP
timeout : 20

Type : servicegroup

cip : DISABLED
cka : YES
cmp : NO
downstateflush : DISABLED
healthmonitor : NO
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp
servicetype : HTTP
sp : ON
state : ENABLED
tcpb : NO
useproxyport : NO
usip : NO

Type : lbvserver_servicegroup_binding

name : sharepoint-application-test-frontpage-services-lb
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.10.10.11
port : 80
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

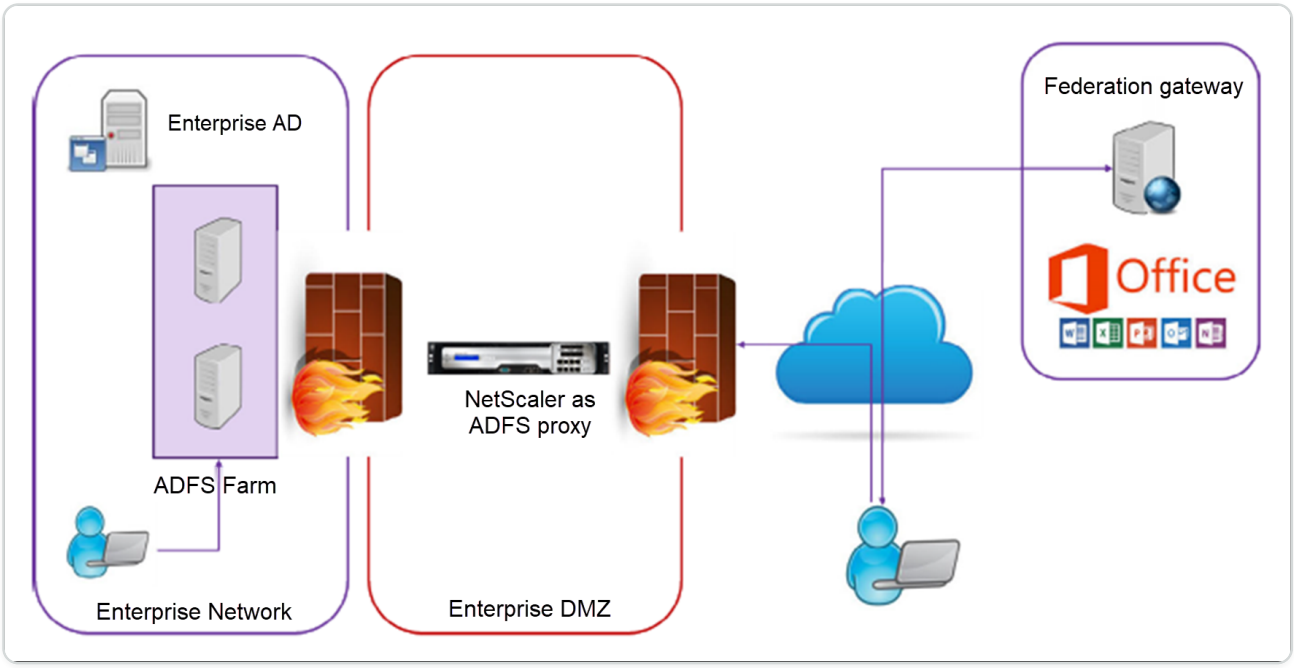
Microsoft ADFS proxy StyleBook

Microsoft ADFS proxy plays a significant role by giving single sign-on access for both internal federation-enabled resources and cloud resources. One such example of cloud resources is Office 365. The purpose of the ADFS proxy server is to receive and forward requests to ADFS servers that are not accessible from the internet. ADFS proxy is a reverse proxy and typically resides in your organization's perimeter network (DMZ). The ADFS proxy plays a critical role in remote user connectivity and application access.

NetScaler has the precise technology to enable secure connectivity, authentication, and handling of federated identity. Using NetScaler as ADFS proxy avoids the need to deploy an extra component in the DMZ.

The Microsoft ADFS Proxy StyleBook in NetScaler Console allows you to configure an ADFS proxy server on a NetScaler instance.

The following image illustrates the deployment of a NetScaler instance as an ADFS proxy server in the enterprise DMZ.



Benefits of using NetScaler as ADFS proxy

1. Caters to both load balancing and ADFS proxy needs
2. Supports both internal and external user access scenarios
3. Supports rich methods for pre-authentication
4. Provides a single sign-on experience for users
5. Supports both active and passive protocols

© 1997–2026 Citrix Systems, Inc. All rights reserved.

   a. Examples of active protocol apps are – Microsoft Outlook, Microsoft Skype for Business
   b. Examples of passive protocol apps are –Microsoft Outlook web app, web browsers

6. Hardened device for DMZ-based deployment
7. Adds value by using additional core NetScaler features

   a. Content Switching
   b. SSL offload
   c. Rewrite
   d. Security (NetScaler AAA)

For active protocol-based scenarios, you can connect to Office 365 and provide your credentials. Microsoft Federation Gateway contacts the ADFS service (through ADFS Proxy) on behalf of the active protocol client. The gateway then submits the credentials using basic authentication (401). NetScaler handles the client authentication before access to ADFS service. Post authentication, the ADFS service provides a SAML token to the Federation Gateway. The Federation Gateway, in turn, submits the token to Office 365 to provide client access.

For passive clients, the ADFS Proxy StyleBook creates Kerberos Constrained Delegation (KCD) user account. The KCD account is necessary for Kerberos SSO authentication to connect to the ADFS servers. The StyleBook also generates an LDAP policy and a session policy. These policies are later bound to the NetScaler AAA virtual server that handles the authentication for passive clients.

The StyleBook can also ensure that the DNS servers on the NetScaler are configured for ADFS.

The configuration section below describes how to set up NetScaler for handling both active and passive protocol-based client authentication.

Configuration details

The table below lists the minimum required software versions for this integration to be deployed successfully.

PRODUCT	MINIMUM REQUIRED VERSION
NetScaler	11.0, Advanced/Premium License

The following instructions assume that you have already created the appropriate external and internal DNS entries.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Deploying Microsoft ADFS proxy StyleBook configurations from NetScaler Console

The following instructions assist you when implementing the Microsoft ADFS proxy StyleBook in your business network.

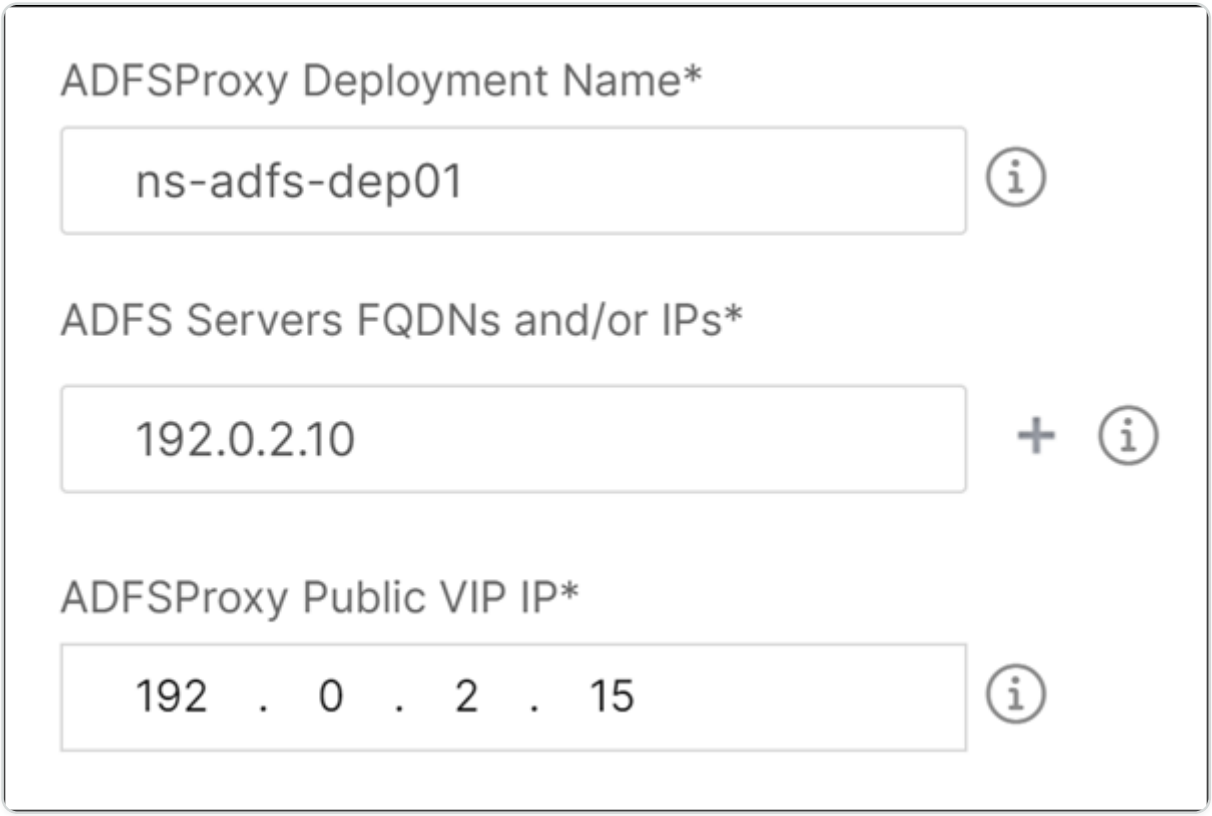
To deploy Microsoft ADFS proxy StyleBook

1. In NetScaler Console, navigate to **Applications > Configuration > StyleBooks**. The **StyleBooks** page displays all the StyleBooks available for your use in NetScaler Console.
2. Scroll down and find the **Microsoft ADFS proxy StyleBook**. Click **Create Configuration**. The StyleBook opens as a user interface page on which you can type the values for all the parameters defined in this StyleBook.
3. Type values for the following parameters:

    a. **ADFS Proxy Deployment Name**. Select a name for the ADFS proxy configuration deployed in your network.

    b. **ADFS Servers FQDNs or IPs**. Type the IP addresses or FQDNs (domain names) of all ADFS servers in the network.

    c. **ADFS Proxy Public VIP IP**. Type the public virtual IP address on the NetScaler that performs as an ADFS proxy server.



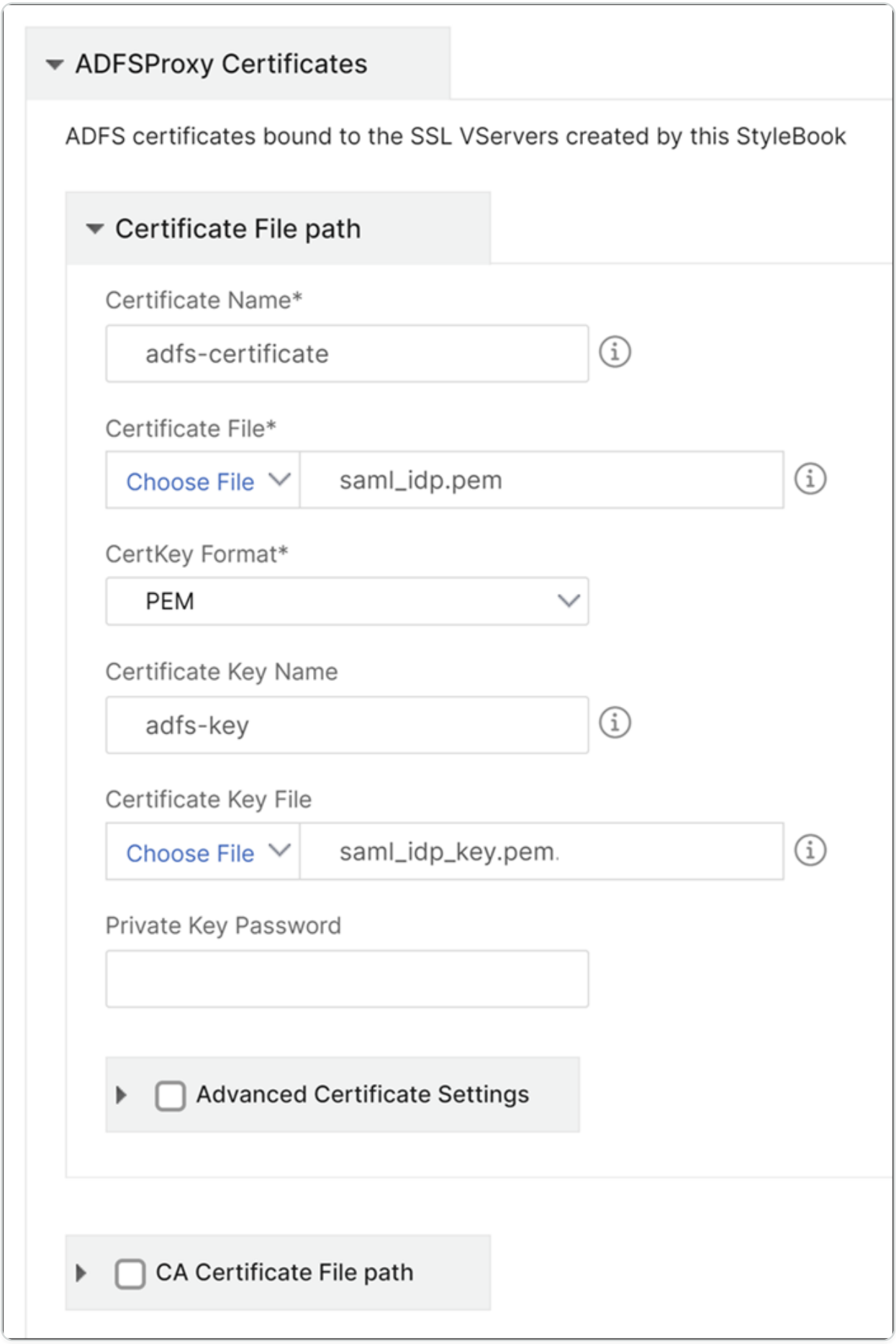
4. In the **ADFS Proxy Certificates** section, type the details of the SSL certificate and the certificate key.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This SSL certificate is bound to all the virtual servers created on the NetScaler instance.

Select the respective files from your local storage folder. You can also type in the private key password to load encrypted private keys in .pem format.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can also enable **Advanced Certificate Settings** check box. Here you can type details such as certificate expiry notification period, enable, or disable the certificate expiry monitor.

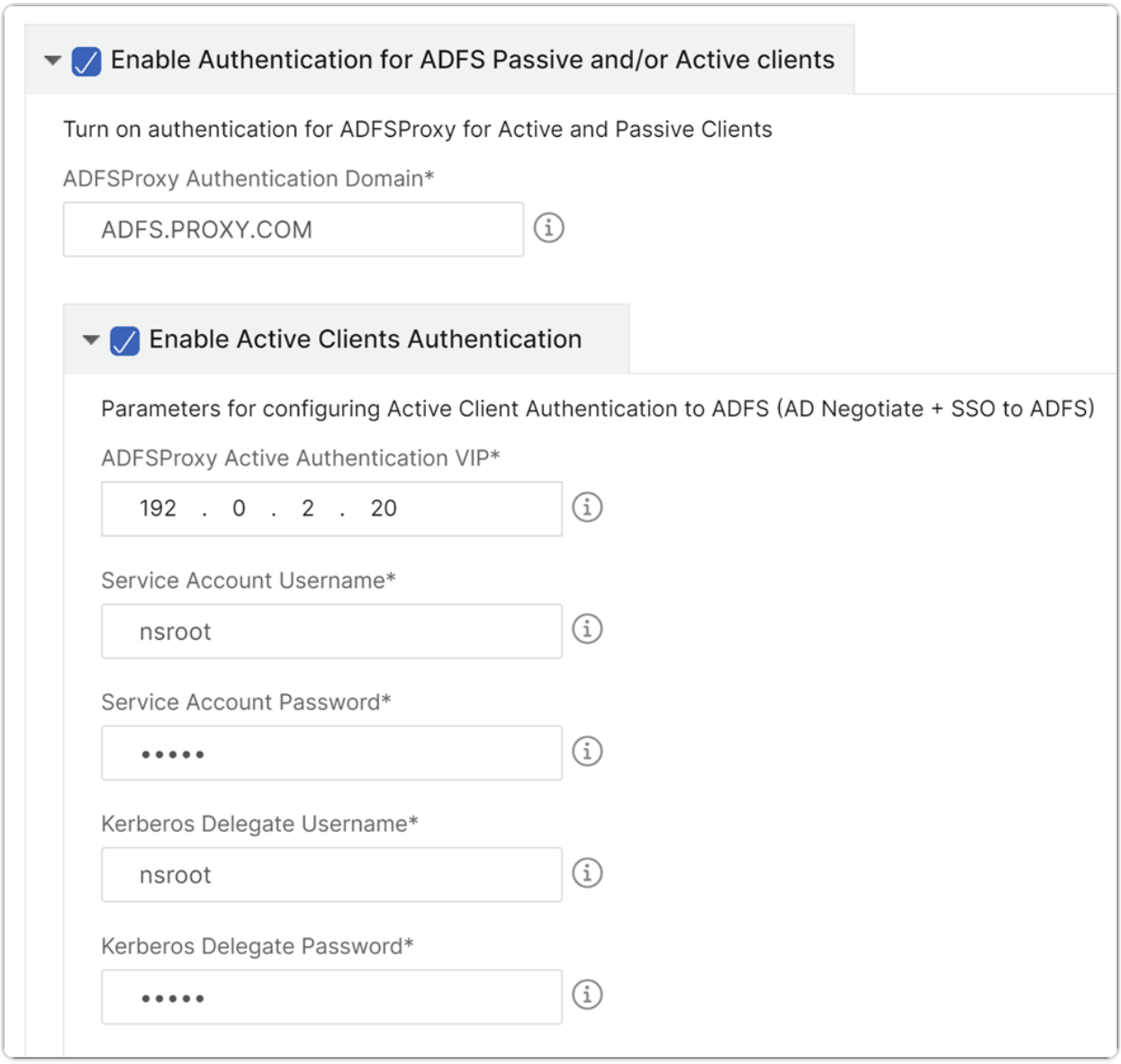
5. Optionally, you can select **SSL CA Certificate** check box if the SSL certificate requires a CA public certificate to be installed on NetScaler. Ensure that you select "Is a CA Certificate" in the **Advanced Certificate Settings** section.
6. Enable authentication for active and passive clients. Type the DNS Domain Name used in Active Directory for user authentication. You can then configure authentication either for active or passive clients, or both.
7. Type the following details to enable authentication for active clients:

NOTE

It is optional to configure support for active clients.

   a. **ADFS Proxy Active Authentication VIP**. Type the virtual IP address of the virtual authentication server on the NetScaler instance where the active clients are redirected for authentication.
   b. **Service Account Username**. Type the service account user name used by NetScaler to authenticate your users to the active directory.
   c. **Service Account Password**. Type the password used by NetScaler to authenticate your users to the active directory.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. Configure authentication for passive clients by enabling the corresponding option and configuring the LDAP settings.

NOTE

It is optional to configure support for passive clients.

Type the following details to enable authentication for passive clients:

a. **LDAP (Active Directory) Base**. Type the base domain name for the domain in which the user accounts reside within the active directory (AD) to allow authentication. For example, `dc=netscaler,dc=com`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. **LDAP (Active Directory) Bind DN**. Add a domain account (using an email address for ease of configuration) that has privileges to browse the AD tree. For example, cn=Manager, `dc=netscaler,dc=com`

c. **LDAP (Active Directory) Bind DN Password**. Type the password of the domain account for authentication.

A few other fields that you must type in the values in this section are as follows:

d. **LDAP Server (Active Directory) IP**. Type the IP address of the active directory server for AD authentication to work correctly.

e. **LDAP Server FQDN name**. Type the FQDN name of the active directory server. FQDN name is optional. Provide the IP address as in step 1 or the FQDN name.

f. **LDAP Server Active Directory port**. By default, the TCP and UDP ports for LDAP protocol are 389, whereas the TCP port for Secure LDAP is 636.

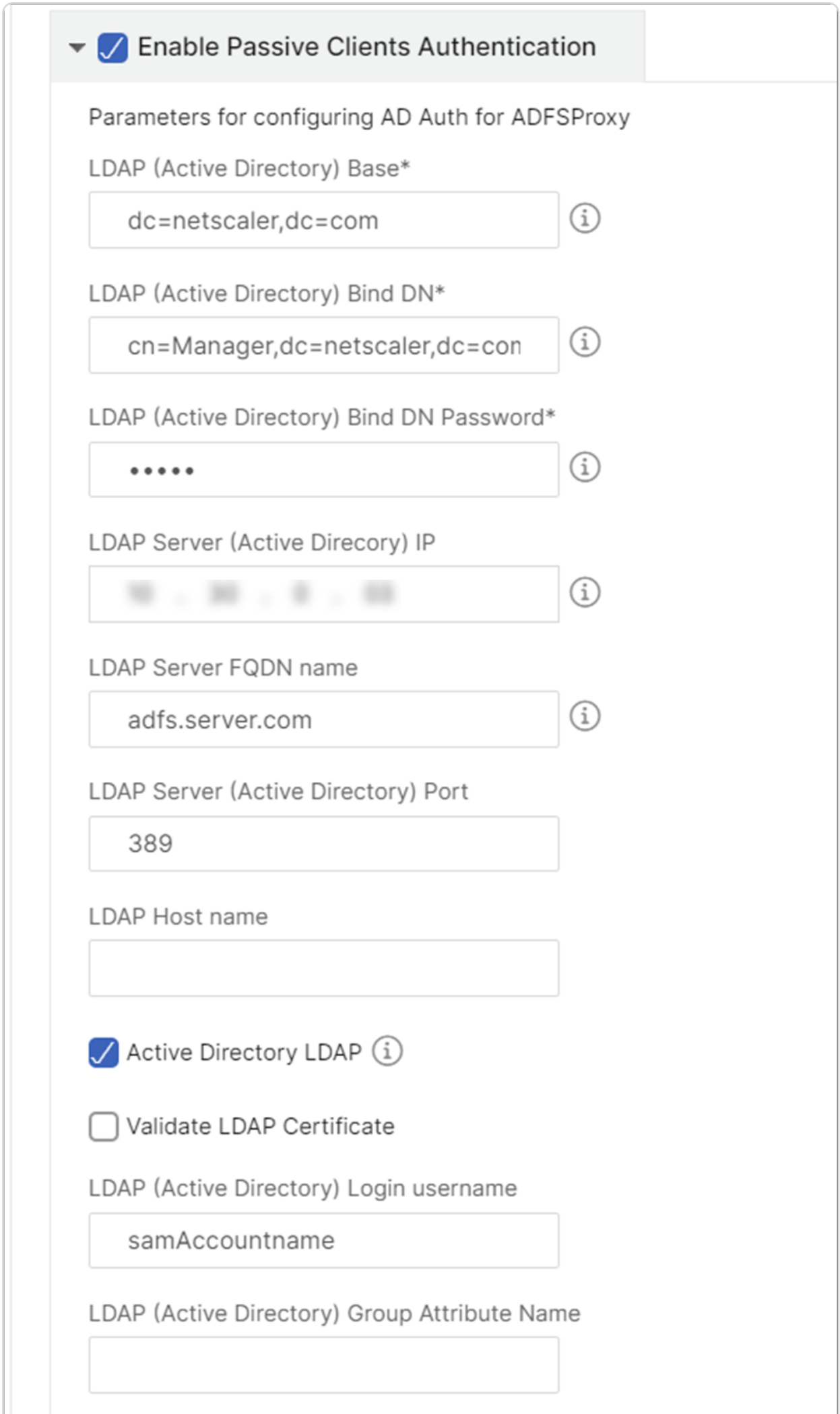
g. **LDAP (Active Directory) login username**. Type the user name as "sAMAccountName."

h. **ADFS Proxy Passive Authentication VIP**. Type the IP address of the ADFS proxy virtual server for passive clients.

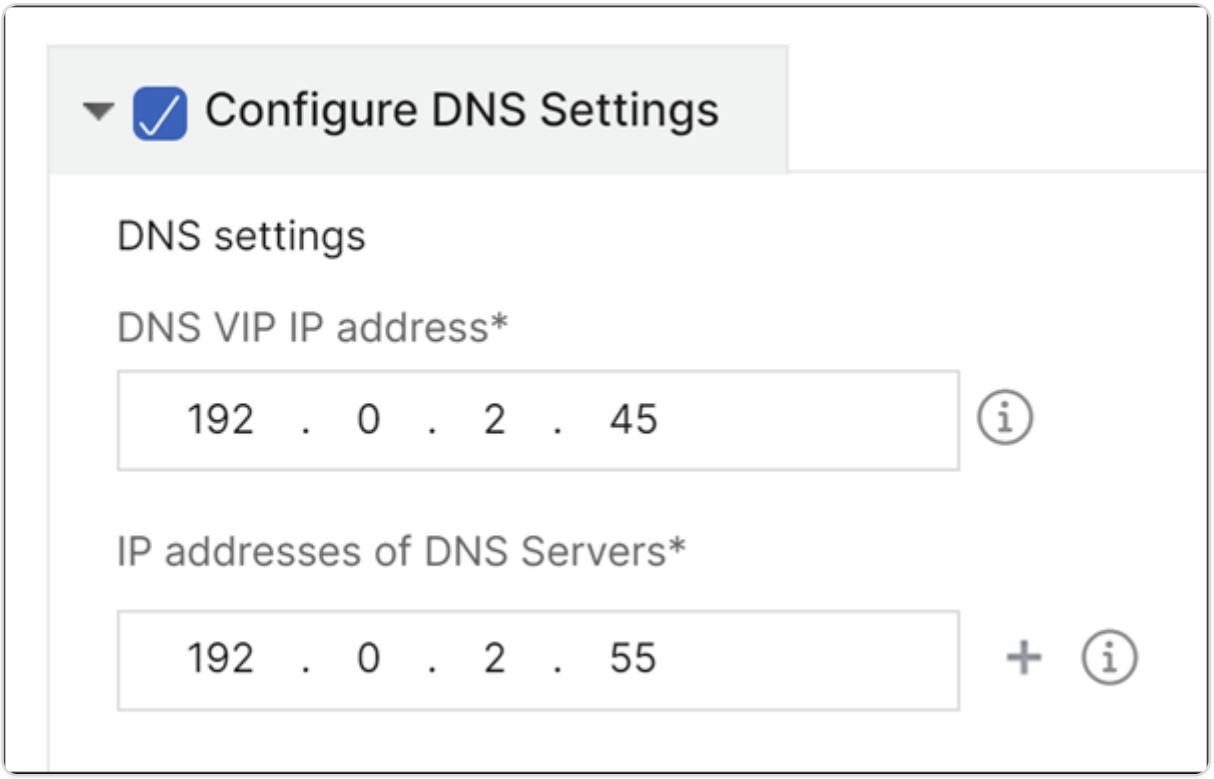
NOTE

The fields marked with "*" are mandatory.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

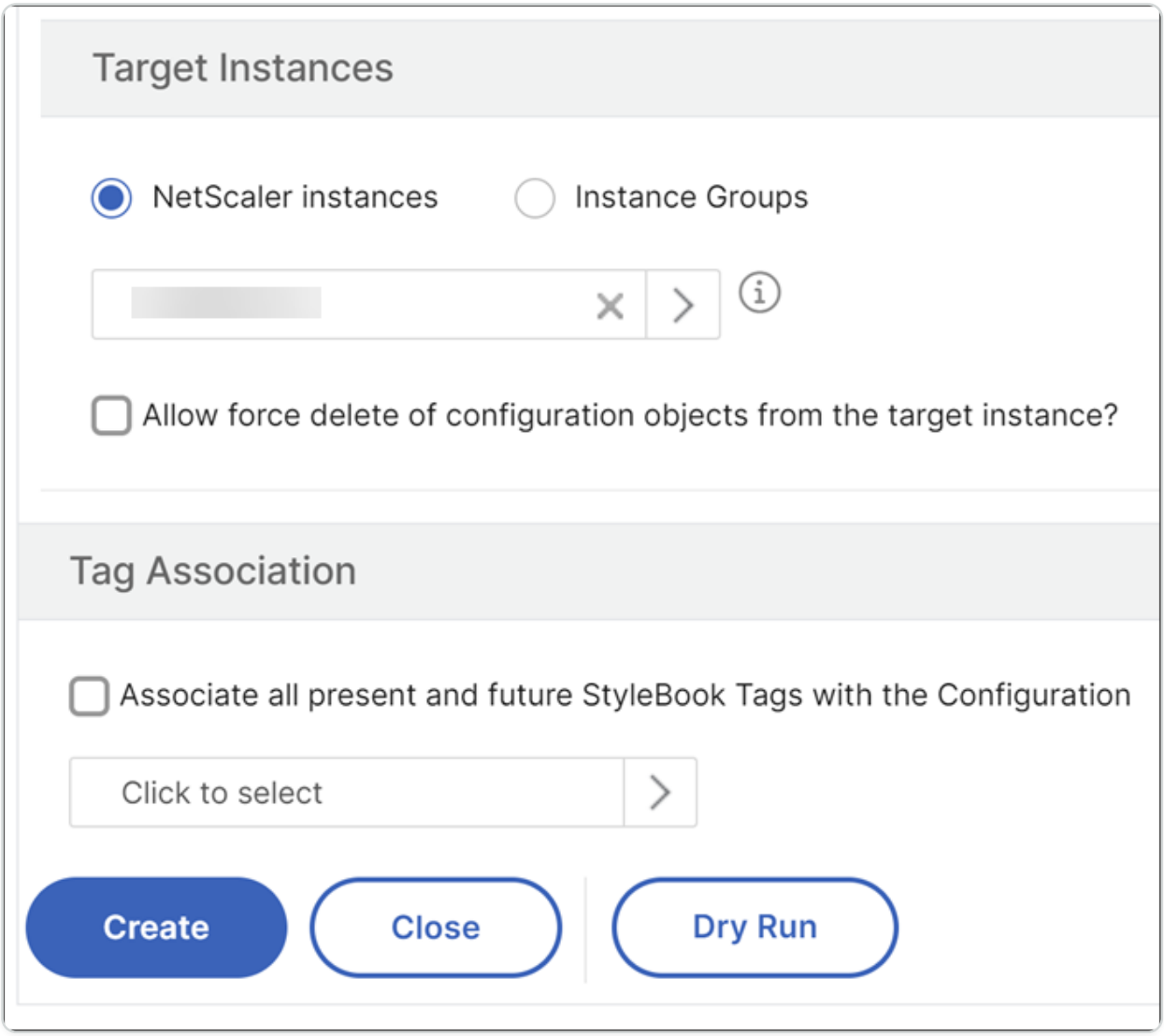

Enable Passive Clients Authentication
Parameters for configuring AD Auth for ADFSProxy
LDAP (Active Directory) Base*
dc=netscaler,dc=com
LDAP (Active Directory) Bind DN*
cn=Manager,dc=netscaler,dc=con
LDAP (Active Directory) Bind DN Password*
•••••
LDAP Server (Active Direcory) IP
LDAP Server FQDN name
adfs.server.com
LDAP Server (Active Directory) Port
389
LDAP Host name
Active Directory LDAP
Validate LDAP Certificate
LDAP (Active Directory) Login username
samAccountname
LDAP (Active Directory) Group Attribute Name

9. Optionally, you can also configure a DNS VIP for your DNS servers.



10. Click **Target Instances** and select the NetScaler instances to deploy this Microsoft ADFS proxy configuration. Click **Create** to create the configuration and deploy the configuration on the selected NetScaler instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE

Citrix recommends that before running the actual configuration, you select **Dry Run.** You can first view the configuration objects that are created on the target NetScaler instances by the StyleBook. You can then click **Create** to deploy the configuration on the selected instances.

Objects created

Several configuration objects are created when the ADFS proxy configuration is deployed on the NetScaler instance. The following image displays the list of objects created.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type : systemfile

filecontent :
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSURtVENDQW9HZ0F3SUJBZ0lCQXpBTkJna3Foa2lHOXcwQkFRc0ZBI
VFHRXdKVlV6RW1NQ1FHQ1NxR1NjYjNEUUVKQVJZWAplVzkxWTJWbUxXTmhRR0ZqYldVdFkyOXljQzVqYjlweEZEQV
1URXlPVEExTVRrd05Wb1hEVEl5TVRFeU9EQTFNVGt3TlZvd2dZZ3gKR0RBV0JnTlZCQU1NRDNsdmRXTmxaaTF6WVcx
FRa0JGaGw1YjNWalpXWXRjMkZ0YkVCaFkyMWxMV052Y25BdVkyOXRNUkl3CkVBWURWUVFLREFsQlEwMUZMVU5
GQUFPQ0FROEFNSUlCQ2dLQ0FRRUF5L1gza0VCd2F0SEpoQmFXR2Z6WmwxQ1FkZ2JtbDFlYgpZT3hadG4xOHNpS
9kNXJCOHNmeG56K2RvbjJyaUhHaktEazVPYkFScmd2NVNHaGhmL3pvQVpDa3MybkVocjh6UElxOWoKQm8wc3NlTl
HV3VlpBakQxVitnNTVHSkdXMW9ubndyTlc0Q3ViTzMyRTFDNjh1WG1TZnlwdUlzTzlvRDF2ZnovSDh0QlM4CjFlV0Vla
0RBSkJnTlZIUk1FQWpBQU1Bc0dBMVVkRHdRRUF3SUY0REFOQmdrcWhraUc5dzBCQVFzRkFBT0NBUUVBbk1RSQpz
KOGc3CjNlUzlkbE15UkUveXh4N3V5SXpqR0ZaV1VBclMxL09PcUxGRHR2NEFZWXZ6UVhGL0pWM2phWjZnUkdMS0
zFRclNHdVYrdgoxRW1tMlNNcWxrbGVVclN5QXBuSlVWNHA0QTVDbTh6UTRVVDhtZjZQRkU2TFhRTHZCYzhWdUJvR
NBVEs1azE1NVZSd2UKaWt3OFYzR082MmdRc0hvV05RPT0KLS0tLS1FTkQgQ0VSVElGSUNBVEUtLS0tLQo=
fileencoding : BASE64
filelocation : /nsconfig/ssl
filename : saml-idp.pem

Type : systemfile

filecontent :
LS0tLS1CRUdJTiBSU0EgUFJJVkFURSBLRVktLS0tLQpNSUlFcEFJQkFBS0NBUUVBeS9YM2tFQndhdEhKaEJhV0dmelpsM
Q2eWJWY1NzajFIT0JEdU9CbVpnRS9LQS9kNXJCOHNmeG4keitkb24ycmlIR2pLRGs1T2JBUnJndjVTR2hoZi96b0FaQ2t
BhTU1tV3dyQmN0OUhKdEJxcEpVUHV3VlpBakQxVitnNTVHCkpHVzFvbm53ck5XNEN1Yk8zMkUxQzY4dVhtU2ZyMH
h0bW1YT2tLb0JWaXdjREFRQUJBb0lCQUVtS1FGOEV2UVBtN0cveAo3T0VsNkJiRTk3RjJ2NEhtRnFJVjFpc1VoL2Q2Y2h2
WTUdnTHBZcDYvRS9DcFFQdkhyNEJSS3hiVXBvQkpaZ0g0eloKRHZjT1dadlJtc0hXYVBkUmoxVDNaaHdsd21aMEQ4U
wrSXBBRHJybkdOdUNHMld4NUorNHM3VG9aMXYzc1NtRThaK2pqdWtYCk5DTFBKcnh3dFJlSXc3ajRTenlDNWFCR1M
1RrZHhTc2ZPblF6THgwYUNQWnFWNCtQVkoycThzbkpvMXhJOWI1dE9mRlBNVApGRHZNYXZwKytHQnpWTyszRWI
wWDA2NWlSTnZVYnVrQklqWDgvYkhTNlllTjFWR2o2RVFYQmtrNmJmSXNDZ1lFQXpNQ2kkMkFhd0FTY3htT0Q1Zm
1PZTNPU2dVMWh4WmNDdjlUMGhNNEdWVVQyVFhqWkZNWWFBWk8yNjFwdWVKbTRkMXZqdDY3CjJrN0tVclhpY
iMzgxNW5tUmpyZTFrK21QN2tuL0xFQk1pVUVXV0tybXpFanRsbzhRTFhXVjZzU3ltVXJCVU11bnVLWgo1Y1B5bFdFTE
VCcUwwQjh5a0djUGVUbkRlS3dLQmdRQ0tBME1BMkNrazdkVkpsa08xb05jTDhrUGNYL0ZzckJURi8xL0QKRTcva1AxT
GR1Blb3NJK3FxQWw1aktiY3AxMFZYNUJ1cS9xbm9vREVkN2d0NGNFcEM0RTUvQW85VThGWVVGR3ZpcC9wdGwxC
EeloKUmllWXlWUnRkbkU5TE5kYU5STXdpTWFCYkhFazF4R1lxSDByQnFEYUE0M1B4Zm9FYjdndEdCaHE2azRUempa
otLS0tLUVORCBSU0EgUFJJVkFURSBLRVktLS0tLQo=
fileencoding : BASE64
filelocation : /nsconfig/ssl
filename : saml-idp.key

Type : sslcertkey

cert : saml-idp.pem
certkey : adfs-certificate
inform : PEM
key : saml-idp.key

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Objects Added on Instance : 192.168.153.160 | Count : 57

Type : nsfeature

Meta Properties
action : **enable**

feature : cs lb ssl rewrite aaa

Type : lbvserver

ipv46 : 192.50.50.12
name : ns-adfs-dep01-adfs-dns
port : 53
servicetype : DNS

Type : service

ip : 10.30.30.5
name : ns-adfs-dep01-dns-svc-1
port : 53
servicetype : DNS

Type : lbvserver_service_binding

name : ns-adfs-dep01-adfs-dns
servicename : ns-adfs-dep01-dns-svc-1

Type : authenticationnegotiateaction

domain : ADFS.CITRIX.COM
domainuser : nsroot
domainuserpasswd : nsroot
name : ns-adfs-dep01-negotiate-action

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type : authenticationpolicy

action : ns-adfs-dep01-negotiate-action
name : ns-adfs-dep01-negotiate-policy
rule : true

Type : aaakcdaccount

delegateduser : nsroot
kcdaccount : ns-adfs-dep01-adfs-auth401-kcd-
kcdpassword : nsroot
realmstr : ADFS.CITRIX.COM

Type : tmsessionaction

kcdaccount : ns-adfs-dep01-adfs-auth401-kcd-
name : ns-adfs-dep01-adfs-auth401-tmsession-action
persistentcookie : ON
persistentcookievalidity : 3
sso : ON

Type : tmsessionpolicy

action : ns-adfs-dep01-adfs-auth401-tmsession-action
name : ns-adfs-dep01-adfs-auth401-tmsession-policy
rule : ns_true

Type : authenticationvserver

authenticationdomain : ADFS.CITRIX.COM
failedlogintimeout : 1
ipv46 : 192.50.50.40
maxloginattempts : 255
name : ns-adfs-dep01-adfs-auth401-auth-vserver
port : 443
servicetype : SSL

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-adfs-auth401-auth-vserver

Type : authenticationvserver_authenticationpolicy_binding

name : ns-adfs-dep01-adfs-auth401-auth-vserver
policy : ns-adfs-dep01-negotiate-policy
priority : 10

Type : authenticationvserver_tmsessionpolicy_binding

name : ns-adfs-dep01-adfs-auth401-auth-vserver
policy : ns-adfs-dep01-adfs-auth401-tmsession-policy
priority : 10

Type : authenticationldapaction

authentication : ENABLED
authtimeout : 30
followreferrals : OFF
ldapbase : dc=netscaler,dc=com
ldapbinddn : cn=Manager,dc=netscaler,dc=com
ldapbinddnpassword : nsroot
ldaploginname : samAccountname
name : ns-adfs-dep01-ldap-action
passwdchange : DISABLED
sectype : PLAINTEXT
serverip : 10.30.30.3
serverport : 389
ssonameattribute : userPrincipalName
svrtype : AD
validateservercert : NO

Type : authenticationpolicy

action : ns-adfs-dep01-ldap-action
name : ns-adfs-dep01-ldap-policy
rule : true

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type : aaakcdaccount

kcdaccount : ns-adfs-dep01-adfs-ldap-kcd-acc
realmstr : ADFS.CITRIX.COM

Type : tmsessionaction

kcdaccount : ns-adfs-dep01-adfs-ldap-kcd-acc
name : ns-adfs-dep01-adfs-ldap-tmsession-action
persistentcookie : OFF
sso : ON

Type : tmsessionpolicy

action : ns-adfs-dep01-adfs-ldap-tmsession-action
name : ns-adfs-dep01-adfs-ldap-tmsession-policy
rule : ns_true

Type : authenticationvserver

authenticationdomain : ADFS.CITRIX.COM
failedlogintimeout : 1
ipv46 : 192.50.50.30
maxloginattempts : 255
name : ns-adfs-dep01-adfs-ldap-auth-vserver
port : 443
servicetype : SSL

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-adfs-ldap-auth-vserver

Type : authenticationvserver_authenticationpolicy_binding

name : ns-adfs-dep01-adfs-ldap-auth-vserver
policy : ns-adfs-dep01-ldap-policy
priority : 10

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type : authenticationvserver_tmsessionpolicy_binding

name : ns-adfs-dep01-adfs-ldap-auth-vserver
policy : ns-adfs-dep01-adfs-ldap-tmsession-policy
priority : 10

Type : csvserver

ipv46 : 192.50.50.50
name : ns-adfs-dep01-cs
port : 443
servicetype : SSL

Type : lbvserver

ipv46 : 192.50.50.50
name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
port : 445
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

Type : server

ipaddress : 192.30.30.30
name : 192.30.30.30

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol
rule : HTTP.REQ.URL.CONTAINS("/adfs/services/trust") || HTTP.REQ.URL.CONTAINS("/federa

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol
priority : 9800

Type : lbvserver

appflowlog : ENABLED
authentication : ON
authenticationhost : ADFS.CITRIX.COM
authn401 : OFF
authnvsname : ns-adfs-dep01-adfs-ldap-auth-vserver
downstateflush : ENABLED
ipv46 : 192.50.50.50
lbmethod : LEASTCONNECTION
name : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb
port : 446
servicetype : SSL

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol
rule : HTTP.REQ.URL.CONTAINS("/adfs/ls/auth/integrated") || HTTP.REQ.URL.CONTAINS("/adfs/ls/wia")

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol
priority : 9900

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type : lbvserver

appflowlog : ENABLED
authentication : OFF
authn401 : ON
authnvsname : ns-adfs-dep01-adfs-auth401-auth-vserver
downstateflush : ENABLED
ipv46 : 192.50.50.50
lbmethod : LEASTCONNECTION
name : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb
port : 444
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-cspol
rule : true

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-cspol
priority : 10000

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-cs

Type : rewritepolicylabel

labelname : ns-adfs-dep01-request-rewritepolicylabel
transform : HTTP_REQ

Type : rewritepolicylabel

labelname : ns-adfs-dep01-response-rewritepolicylabel
transform : HTTP_RES

Type : rewriteaction

name : ns-adfs-dep01-HTTP.REQ.URL-rewrite-action
stringbuilderexpr : "/adfs/services/trust/proxymex"
target : HTTP.REQ.URL
type : REPLACE

Type : rewritepolicy

action : ns-adfs-dep01-HTTP.REQ.URL-rewrite-action
name : ns-adfs-dep01-HTTP.REQ.URL-rewrite-policy
rule : HTTP.REQ.URL.CONTAINS("/adfs/services/trust") && (!HTTP.REQ.URL.CONTAINS("/trust/proxymex"))

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Oracle e-business StyleBook

Oracle E-Business Suite is the most comprehensive suite of integrated, global business applications. This suite enables organizations to make better decisions, reduce costs, and increase performance and consists of the following applications.

- Enterprise resource planning (ERP)
- Customer relationship management (CRM)
- Supply-chain management (SCM)

These computer applications are either developed or acquired by Oracle. The Oracle E-Business Suite 12.2 StyleBook allows you to deploy the configuration on the selected NetScaler instances.

This StyleBook creates a load balancing configuration that comprises a load balancing virtual server, a service group, and a list of services. It also binds the services to the service group and binds the service group to the virtual server. You can choose encrypted communication by selecting SSL and providing the SSL files and key files from your local system.

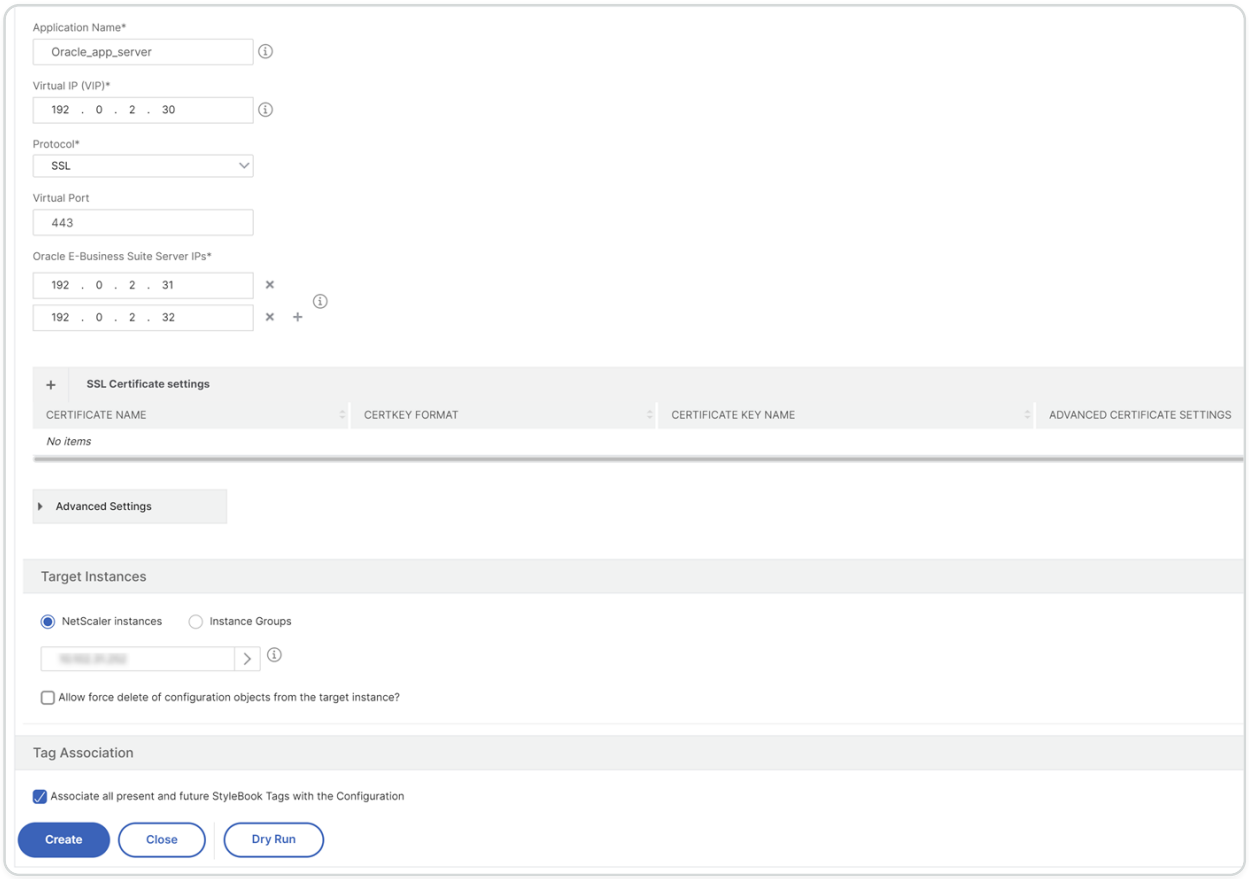
To create a configuration for Oracle E-Business Suite 12.2

1. In NetScaler Console, navigate to **Applications > Configuration > StyleBooks.** The **StyleBooks** page displays all the StyleBooks that are available in your NetScaler Console. Scroll down and select **Oracle E-Business Suite 12.2**. You can also use the search option to search the StyleBook.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Click **Create Configuration** in the StyleBook panel.
3. Type the name of the load balancer application and the virtual IP address in the load balancer settings section.
4. Select the required protocol. You have two options here - HTTP and HTTPS/SSL. You can also type the port number.
5. Type the IP addresses of all the Oracle E-Business Suite application servers in the network that are to be load balanced. Click **+** to add more server IP addresses.
6. In **SSL Certificates Settings** section, select the respective files from your local storage. You can also enable **Advanced Certificate Settings** check box. Here, you can configure more details such as certificate expiry notification period. You can also enable or disable the certificate expiry monitor.

   Select the target NetScaler instance on which the configuration must be created, and click **Create**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

TIP

You can also click the refresh icon to add recently discovered NetScaler instances in NetScaler Console to the available list of instances in this window. The refresh icon is available only on NetScaler Console.

Create and use custom StyleBooks

You can write your own StyleBook for your deployment, import it to NetScaler Console, and create configuration objects. You can also use APIs to create configurations from your StyleBooks.

This document includes the following information:

Before you begin

Before you begin creating StyleBooks, make sure you have knowledge of the following:

- NITRO API. For more information, see NITRO API documentation.
- YAML

StyleBook files use the YAML format. For information about the YAML format, see YAML Syntax.

The following is a list of YAML guidelines you must be aware of while creating StyleBooks:

- YAML is case sensitive.
- YAML requires proper indentation
- Use the `<spacebar>` key to create proper indentation. Do not use the `<tab>` key. Using the `<tab>` key creates compilation error while importing your StyleBook to MA Service.
- Do not use strings within quotation marks. Include the string within quotation marks only if a string has punctuation marks (dashes, colons, and so on.) If you want to interpret a number as a string, either include the number within quotation marks or use the str() built-in function of StyleBooks.
- Literals like YES/Yes/yes/Y/y/NO/no/No/n/N, ON/On/on/OFF/Off/off, and TRUE/true/truthy/ FALSE/False/false/falsely are considered Booleans, and are equivalent to true and false respectively. To interpret them as strings, include them within quotation marks. For example:
  - "YES"
  - "No"

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- "True"
- "False" and so on.

NOTE

Before importing your StyleBook file into NetScaler Console, it is recommended that you validate if your file is compliant with the YAML format. Citrix recommends that you use the built-in YAML validator in StyleBooks to validate and import the YAML content.

For more information, see NITRO APIs documentation.

Anatomy of a StyleBook

Writing StyleBooks requires that you understand the grammar, syntax, and structure of StyleBooks. A typical StyleBook has the following sections:

- **Header**: This section lets you define the identity of a StyleBook and describe what it does. This is a mandatory section.
- **Import StyleBooks**: This section lets you declare which other StyleBook you want to refer to from your current StyleBook. Importing NetScaler NITRO configuration StyleBooks or other StyleBooks is required to write a StyleBook. This is a mandatory section.
- **Parameters**: This section lets you define the parameters you require in your StyleBook to create a configuration. It describes the input that your StyleBook takes. This is an optional section.
- **Components**: This section lets you define the entities (configuration objects) that are created by the StyleBook for a specific configuration. This section is considered as the core of a StyleBook. Components generally use the input provided in the parameters section to adapt the configuration generated by the StyleBook. This is an optional section.

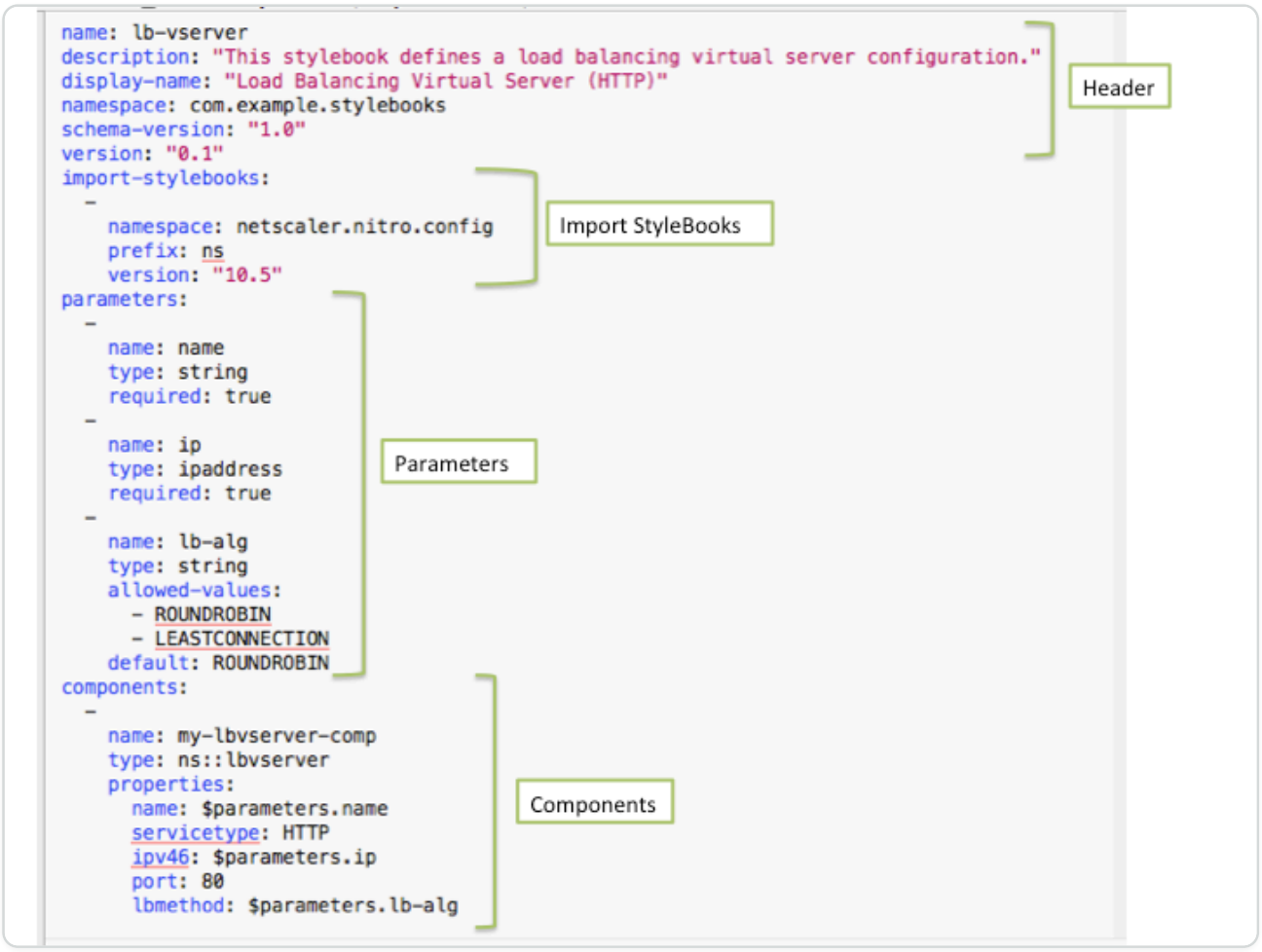
  A StyleBook may have a parameters section, or a components section, or both. A StyleBook with only the parameters section is useful to define a list of parameters that can be used by other StyleBooks. This promotes reusability of parameter groups across a set of StyleBooks. A StyleBook with only a components section may be used when you want to specify the values for attributes in the StyleBook instead of defining parameters to take user input.
- **Outputs**: While the parameters section defines the inputs of the StyleBook, this optional section defines its outputs. In this optional outputs section, you can specify the components that you want to expose to users creating a configuration from this StyleBook and to other

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBooks that import this StyleBook. Users and importing StyleBooks can then reference the properties of the exposed components.

- **Operations**: A StyleBook may contain an optional section to enable Analytics in NetScaler Console on any virtual server that is part of the StyleBook.

The following figure shows a simple outline of a StyleBook.



The following examples help you learn about the grammar and structure of a StyleBook and how to write StyleBooks with increasing levels of complexity.

- StyleBook to create a load balancing virtual server
- StyleBook to create a basic load balancing configuration
- Create a composite StyleBook
- Customize your StyleBook by using GUI attributes

Create and edit a configuration pack

In NetScaler Console, you can create a configuration pack from a StyleBook. The configuration pack is tied to the StyleBook from which it is created. Any updates to the configuration pack are made through the StyleBook to which it is tied.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a configuration pack

To create a configuration pack from a StyleBook, do the following:

1. Navigate to **Applications > Configuration > Config Packs**.
2. Click **Add**.
3. In **Choose StyleBooks**, select the required StyleBooks from which you want to create a configuration pack.

   This page categorizes StyleBooks into default, enterprises, and custom StyleBooks. Select the respective tabs to find the required StyleBooks.
4. Optional, specify a unique **Config Key** to your configuration pack. This key appears as a **Display Key** for this configuration pack.

   - If you specify a **Config Key** that exists, NetScaler Console can't create the configuration pack.
   - If you don't specify a **Config Key**, NetScaler Console automatically assigns the **Configpack ID**. However, this value doesn't appear as a **Display Key**.
   - If you don't specify a **Config Key** and any of the StyleBook parameters has set the `key` attribute, that parameter value appears as the **Display Key**. For more information, see Parameters.
5. Specify the required details such as application name, IP address, port, or protocol type.

   The GUI fields differ from one StyleBook to another StyleBook.
6. In **Target Instances**, select instances or instance groups where you want to run the configuration.

   NOTE:

   You can deploy the configuration on more than one NetScaler, by specifying as many target instances as needed.
7. Click **Dry Run**.

   The **Objects** page displays the objects that get created, modified, or removed from the NetScaler instances.
8. Click **Create**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The configuration pack appears in the **StyleBook > Configurations** page.

If you want to edit the existing config packs, select the configuration pack and click **Edit**.

Reuse configurations created outside of StyleBooks and share configurations between ConfigPacks

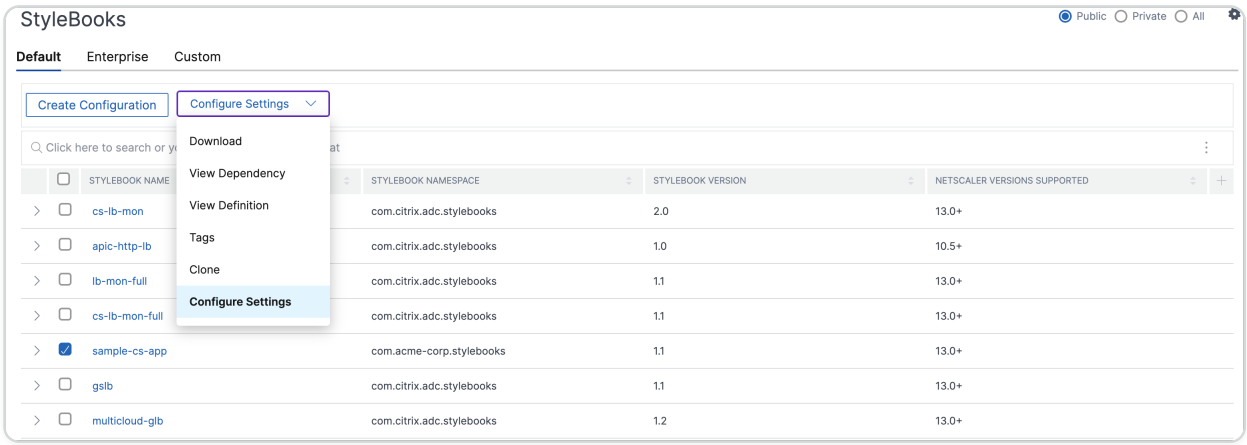
Sometimes, you might have created NetScaler® configurations outside of Stylebooks, whether due to particular operational needs or legacy setups. You can now integrate and manage these previously existing configurations as part of Stylebook config packs enabling more flexible and centralized management.

For example, before this feature, if NetScaler is already configured with an SSL Profile, and if StyleBook's config pack operation attempts to create an SSL Profile with the same name, the config pack operation would have failed with the "Resource Already Exists" error. Now with this feature enabled, the configpack operation succeeds and the existing SSL Profile with the same name can be reused in the new config pack.

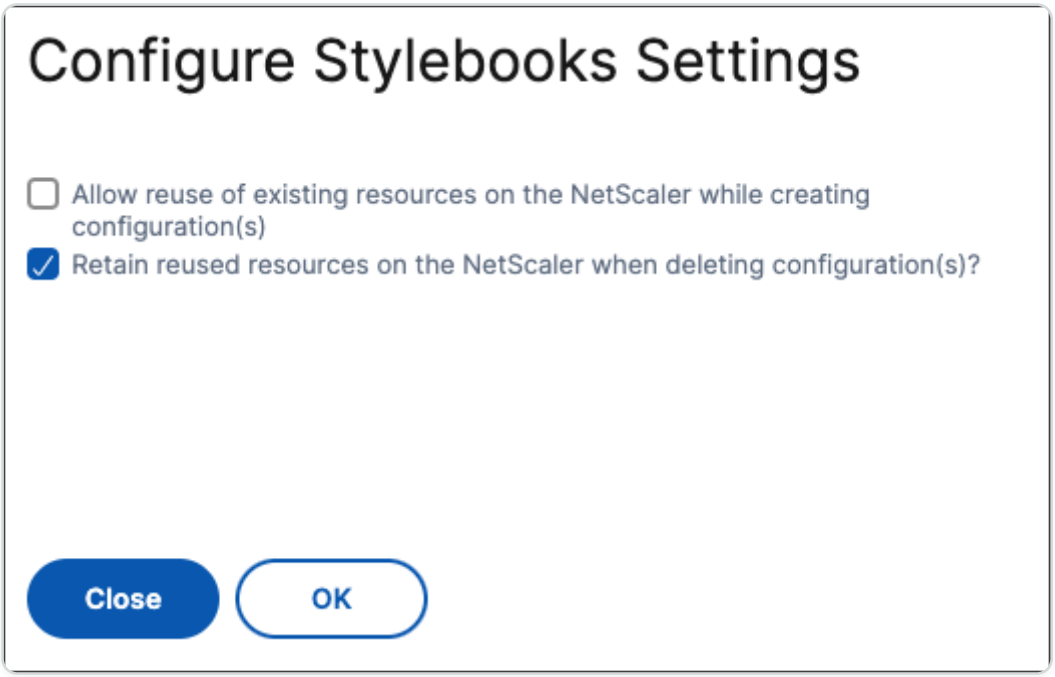
Similarly, you might also face scenarios where resources like network settings, security policies, or part of application configurations are required across multiple applications or configurations. This feature enables you to share the configurations across multiple config packs.

To enable this feature, follow these steps:

1. Navigate to **Applications > Configuration > Stylebooks**.
2. On the **Stylebooks** page, select the Stylebook you will use for creating a new config pack or the one associated with the config pack you are editing.
3. In **Select Action**, click **Configure Settings**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Adjust the settings by choosing one or both of the following options:

   - To enable reuse of existing resources on the NetScaler when creating configurations, select the option **Allow reuse of existing resources on the NetScaler while creating configuration(s)**.
   - To retain reused resources on the NetScaler when deleting configurations, select the option **Retain reused resources on the NetScaler when deleting configuration(s)?**. This option retains the resources originally created outside of Stylebooks on the NetScaler, even if the last config pack referencing them is deleted, ensuring their continued availability.

5. Click **OK**.

Change the StyleBook of a configuration pack

Sometimes, you need to update the StyleBook to add functionality or fix an issue. If you already have created config packs using the old StyleBook, you might want to update them to use the new updated StyleBook. To use a new StyleBook, change the existing StyleBook of the configuration pack.

Consider an example StyleBook **example-lb** that deploys a basic load balancer configuration on a NetScaler instance. And, you create a configuration pack CP1 from this StyleBook.

To configure monitors with the basic load balancer configuration, you need a new StyleBook. To do that, create a **example-lb-mon** StyleBook that includes the ability to configure monitors along with the basic load balancer configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After you create a StyleBook, update the existing configuration pack CP1 to add monitors. To update the configuration pack, do the following:

1. Navigate to **Applications > Configuration > Config Packs**.
2. Select the configuration pack for which you want to change the StyleBook.

   In this example, select CP1 from the list.
3. Click **Change StyleBook**.
4. Select the required StyleBook from the list. Then, click **Save Selection**.
5. Click **Change**.

   In this example, select **example-lb-mon** from the list.

   When you change the StyleBook of a configuration pack, the parameters in the new StyleBook might have a different structure than the existing StyleBook. If the parameter structure is similar to the previous StyleBook, the parameters' values are automatically retained in their respective fields. Otherwise, only parameters that have the same structure between the two StyleBooks are transferred. For example, the same parameter name, type, parameter parent, and more.

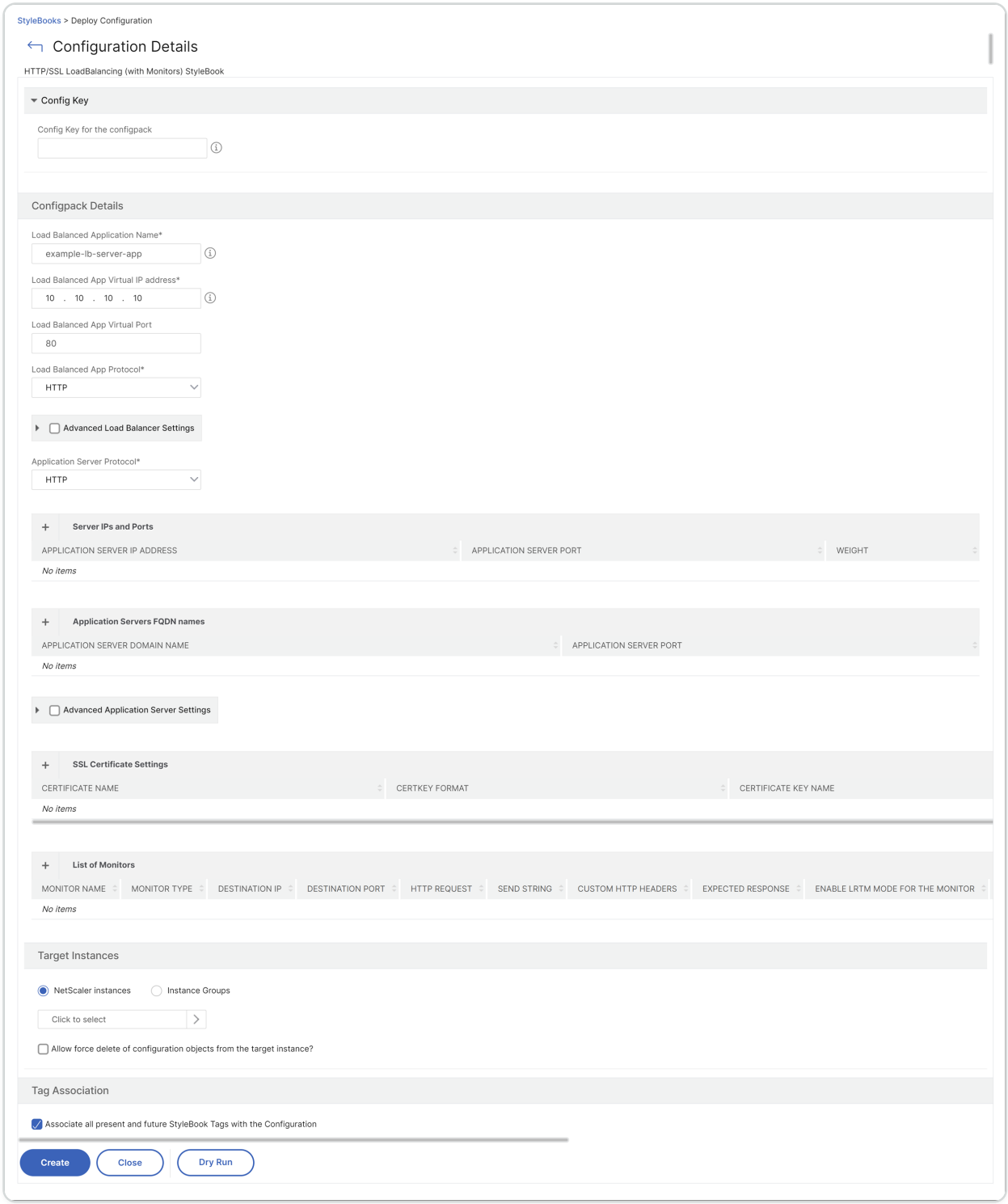
   NOTE:

   The **StyleBook Compatibility** page displays the differences in the parameters. This page helps you decide whether to change the StyleBook or continue with the existing StyleBook. If you want to change the StyleBook, review the changes, then click **Next**.

   If new parameters are added in the new StyleBook, after changing the StyleBook, you have to manually specify the values for such parameters.

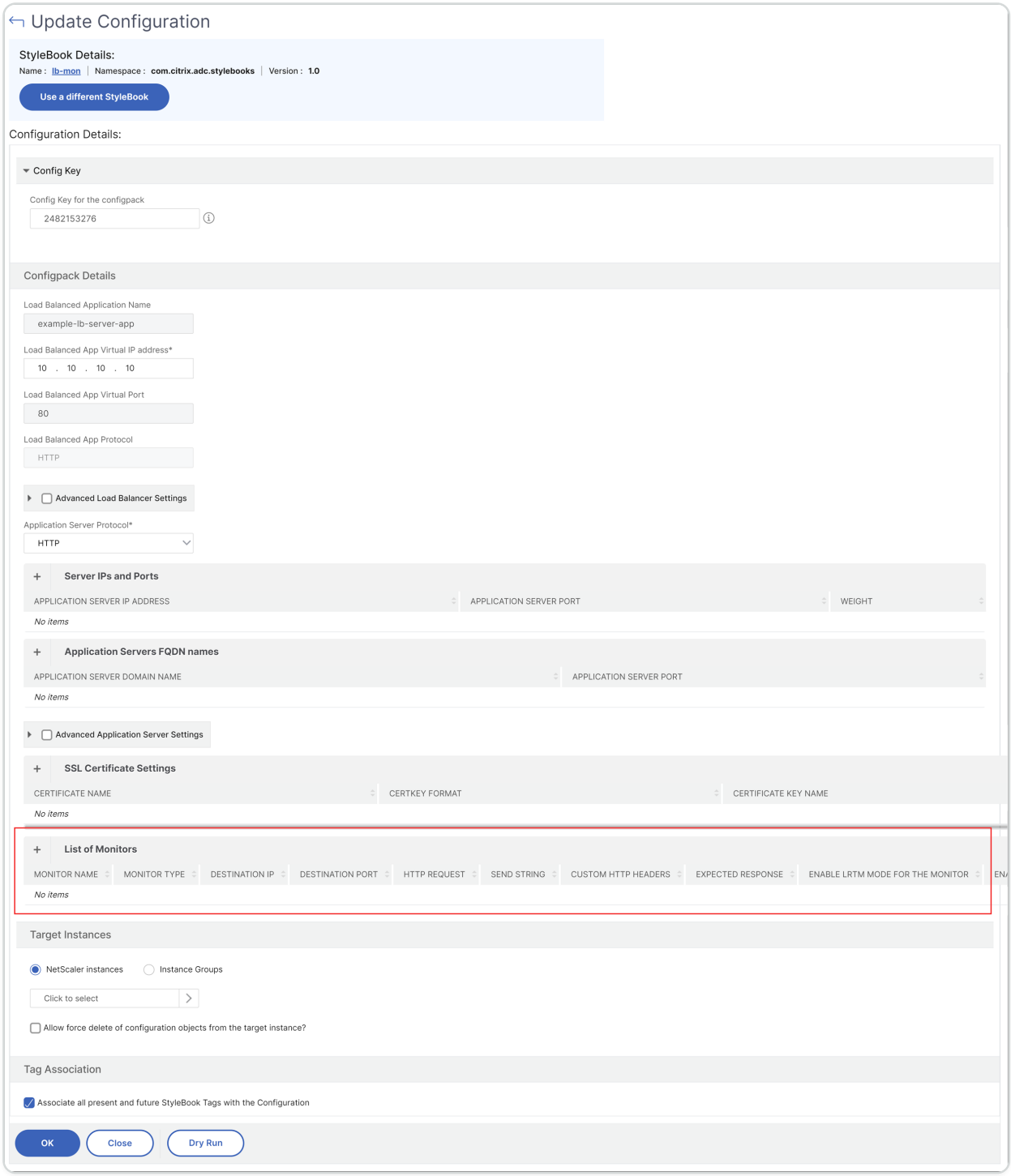
   In this example, the parameters that appear on the configuration page for the **example-lb** StyleBook are as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The parameters that appear on the configuration page for the new **example-lb-mon** StyleBook are as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



In this case, the StyleBooks keeps the older values for the basic load balancer configuration because the new StyleBook hasn't changed existing parameters. And, it adds only the new parameters. For monitor parameters, manually specify the required values.

6. In **Target Instances**, review the selected instances and update the list if necessary.
7. Click **Dry Run**.

   The **Objects** page displays the objects that get created, modified, or removed from the NetScaler instances.
8. Click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In the **StyleBook > Configurations** page, the **StyleBook Name** column displays the new StyleBook name for the selected configuration pack. In this case, it displays **example-lb-mon**.

Change the StyleBook that has multiple config packs

When you want to change an existing StyleBook that has multiple config packs, do the following:

1. Import a new StyleBook to NetScaler Console.

   Typically, the new StyleBook has the same name and namespace with a higher version than the existing StyleBook. However, you can skip this step if the name, namespace, or version are different.
2. Change the StyleBook for the config packs that are associated with the existing StyleBook.

   You can select **Change StyleBook** only when the selected config packs are associated with the same StyleBook.

   For the selected config packs, the NetScaler Console successfully changes the StyleBook when the following conditions are met:

   - All the configuration parameters of the existing StyleBook must present in the selected StyleBook.
   - The new parameters from the selected StyleBook are optional.

   To see the progress of the selected config packs, select **Configurations in Progress/Failed** in the **Configurations** page.
3. Remove the old StyleBook from NetScaler Console once all config packs are tied to the new StyleBook.

Export or import config packs

You can export or import a configuration pack like StyleBooks. With this feature, you can readily share the StyleBook configuration to another NetScaler Console server. When you export a configuration pack, a `tgz` or `zip` bundle downloads to your local computer. This bundle includes a JSON file with all the parameters defined in a configuration pack.

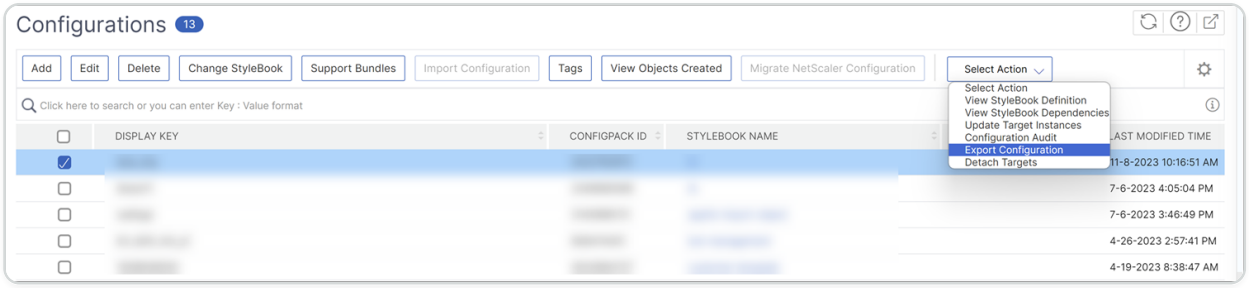
Export configuration

Do the following to export a configuration pack:

1. Navigate to **Applications > Configuration > Config Packs**.
2. Select a configuration pack that you want to export.

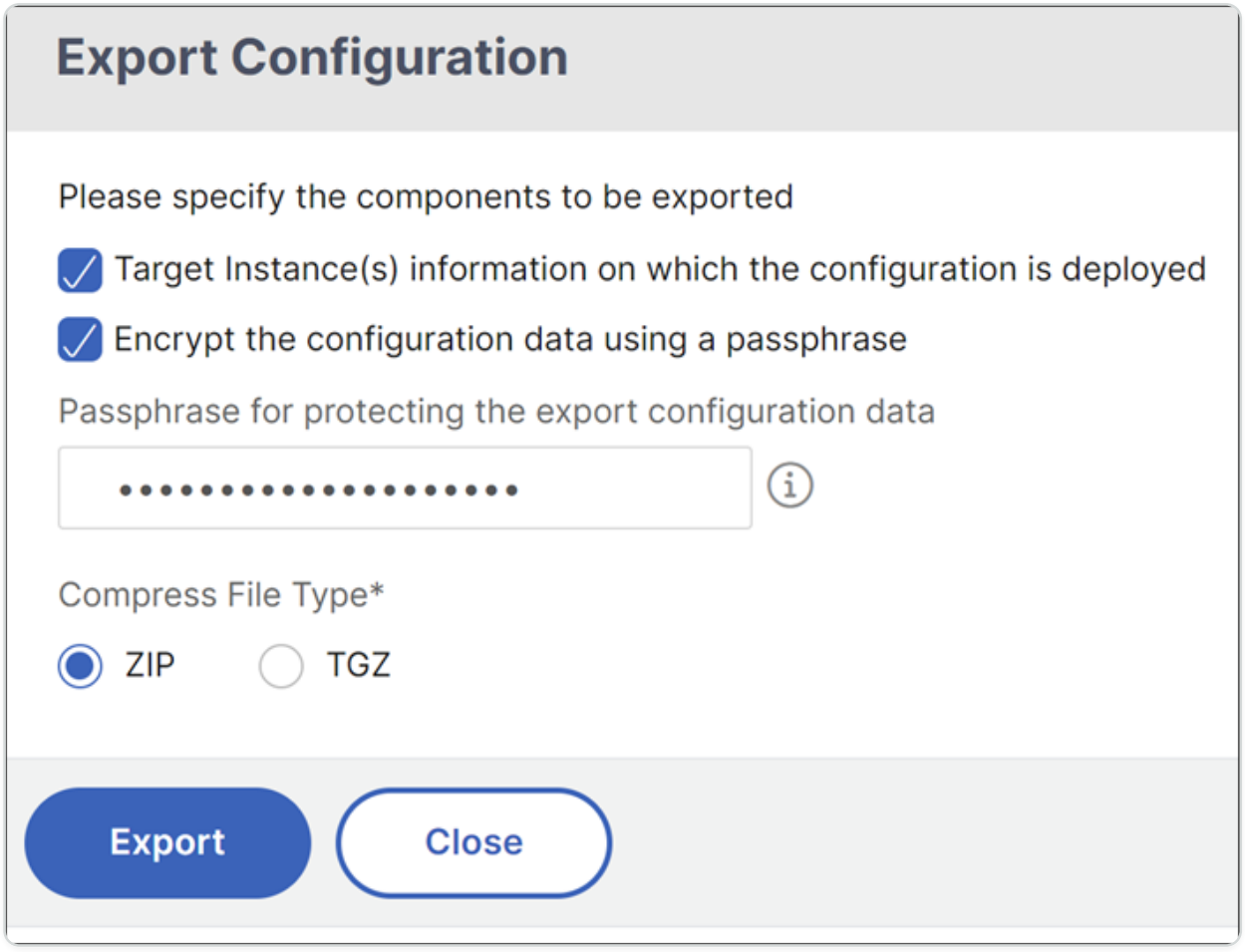
© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. In **Select Action**, select **Export Configuration**.



4. In the **Export Configuration** pane, specify the following:

   - **Target instance(s) information on which the configuration is deployed**: Select this option to include target instances' information with the export bundle.
   - **StyleBook associated with Configuration**: Select this option to include the StyleBook in the export bundle.
   - **Passphrase for protecting the export configuration data**: Specify a passphrase to encrypt the export bundle. This passphrase secures the sensitive data of a configuration pack.
   - **Compress file type**: Select either **ZIP** or **TGZ** file type.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Click **Export**.

   Save the export bundle on your local computer.

Import configuration

You can import a configuration pack from your local computer to a different NetScaler Console server. To import a configuration pack, do the following:

1. Navigate to **Applications > Configuration > Config Packs**.
2. Select **Import Configuration**.
3. Choose the import file bundle from your computer.
4. Use the passphrase that you specified during export.
5. Optional, in Advanced Options, select **Only allow creation of new configuration if all config objects already exist on NetScaler**.

   This option does not alter the objects that are already created on the NetScaler instance.

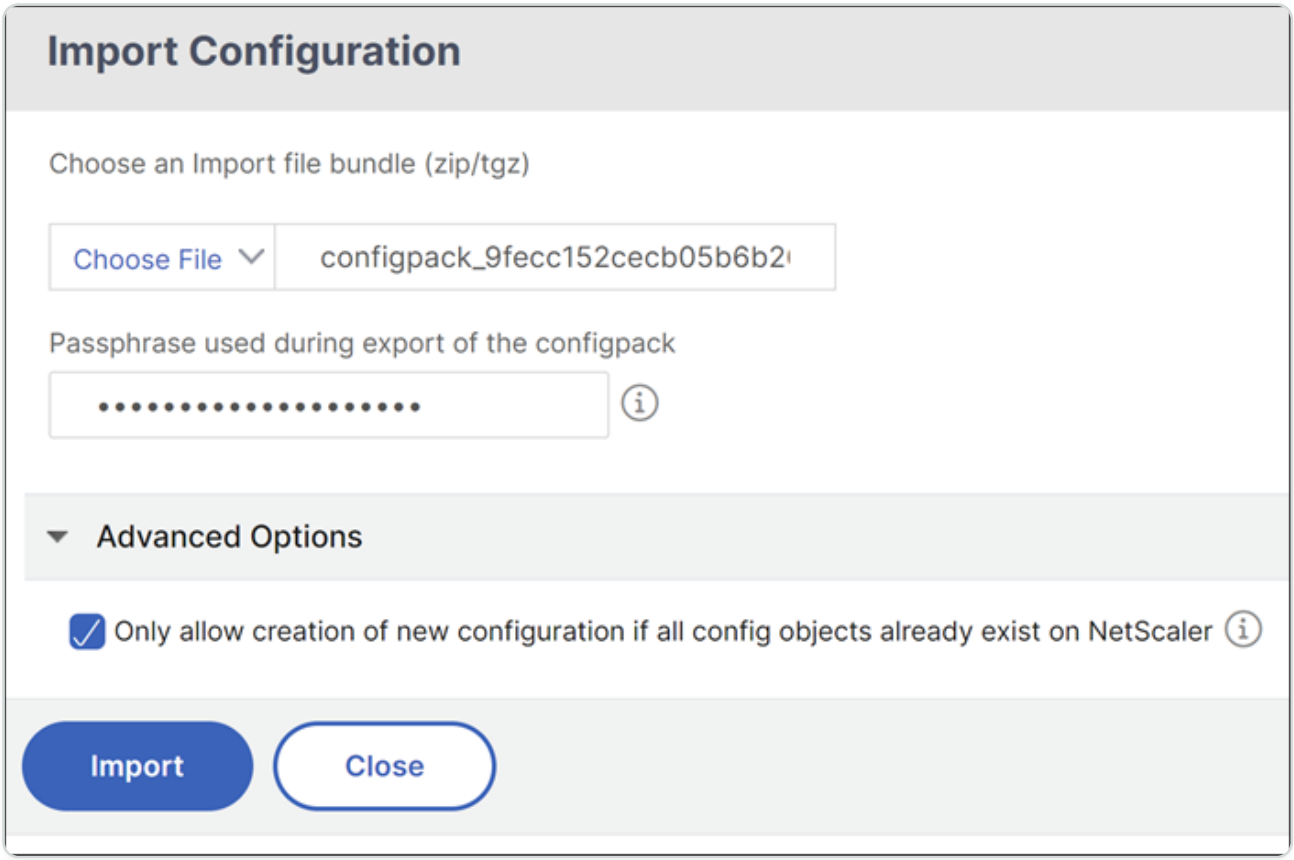
   Consider that you added the same NetScaler instance in two NetScaler Console servers. And, you want to migrate a configuration pack from one NetScaler Console server to another server. Use this option to import a configuration pack without altering its configuration objects on a NetScaler instance.

   IMPORTANT:

   To use this option, make sure that the specified configuration bundle has the target instances information. See, Export configuration.

   This option only migrates the configuration if all the objects are present on the target instance.
6. Click **Import**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



When you import a configuration pack, the NetScaler Console verifies the following:

- **Associated StyleBook**: If the associated StyleBook is not in the NetScaler Console, it imports the StyleBook along with the configuration pack.
- **Target instances**: Check for target instances and deploys the configuration on the specified target instances. If the mentioned NetScaler instances are absent in the NetScaler Console, the configuration pack is imported without target instances.
- **Source NetScaler Console**: If you are importing a configuration pack on the same NetScaler Console server, the selected bundle updates the existing configuration pack.

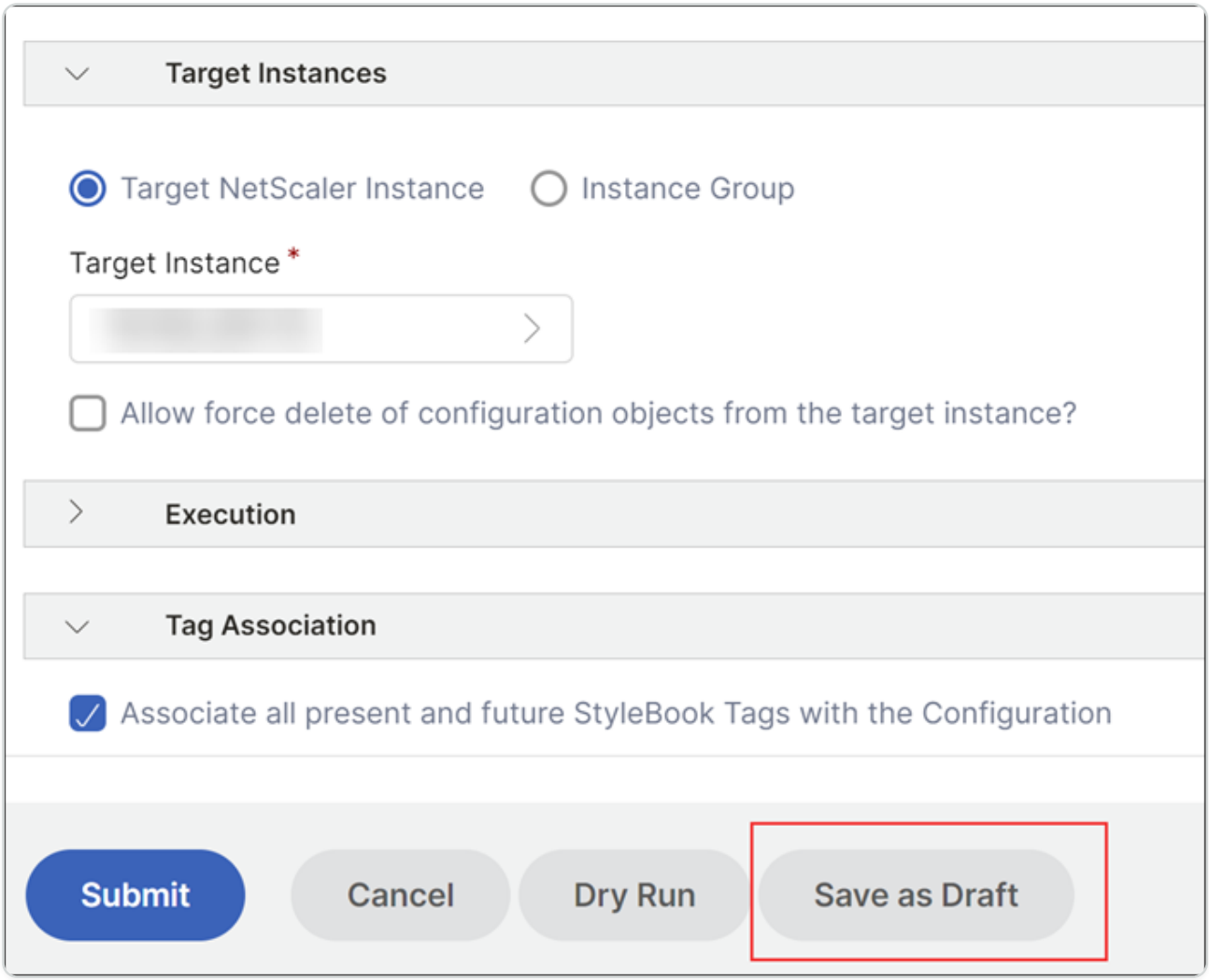
Save a config pack as a draft

The **Save as Draft** option in config packs allows you to save your configuration changes as drafts. This feature saves the changes without immediately deploying them to a NetScaler instance.

To save a config pack as a draft, follow these steps:

1. Navigate to **Applications > Configuration > Config Packs**.
2. On the **Configurations** page, click **Add**.
3. Select your desired stylebook and click **Select**.
4. On the **Create Configuration** page, click **Save as Draft**.

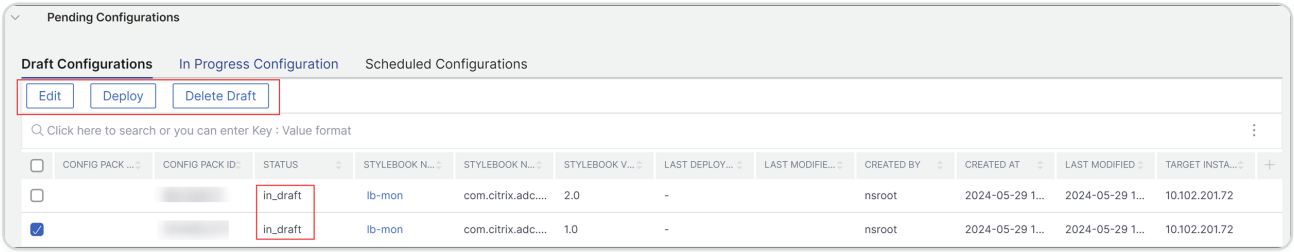
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Once the config pack is saved as a draft, your configuration changes are not deployed directly to NetScaler instance. Instead, the config packs are stored as drafts in the **Draft Configurations** tab under **Pending Configurations**.

In the **Draft Configurations** tab, select the config pack to perform the following operations:

- Edit the configuration of the draft.
- Deploy the configuration to a NetScaler instance.
- Delete the draft.



You can also schedule when to deploy your saved drafts.

For more information, see Create a schedule for a config pack.

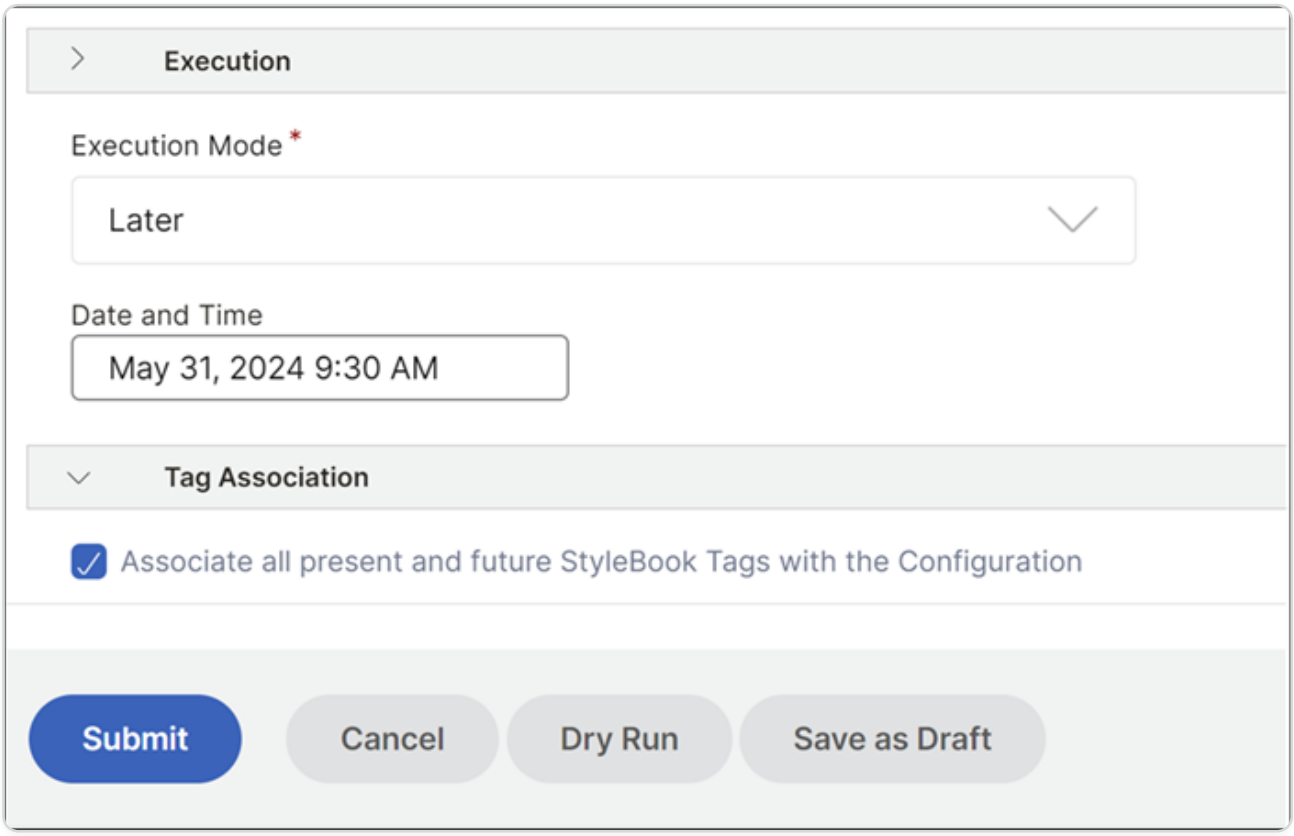
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a schedule for a config pack

When you create a config pack, the config pack is automatically deployed to a NetScaler instance by default. With this feature, you can schedule the deployment of config packs.

To create a schedule for a config pack, follow these steps:

1. Navigate to **Applications > Configuration > Config Packs**.
2. On the **Configurations** page, click **Add**.
3. Select the StyleBook and click **Select**.
4. On the **Create Configuration** page, under **Execution**, select **Later** from the **Execution Mode** list.
5. Select the desired time and date for scheduling and click **Submit**.

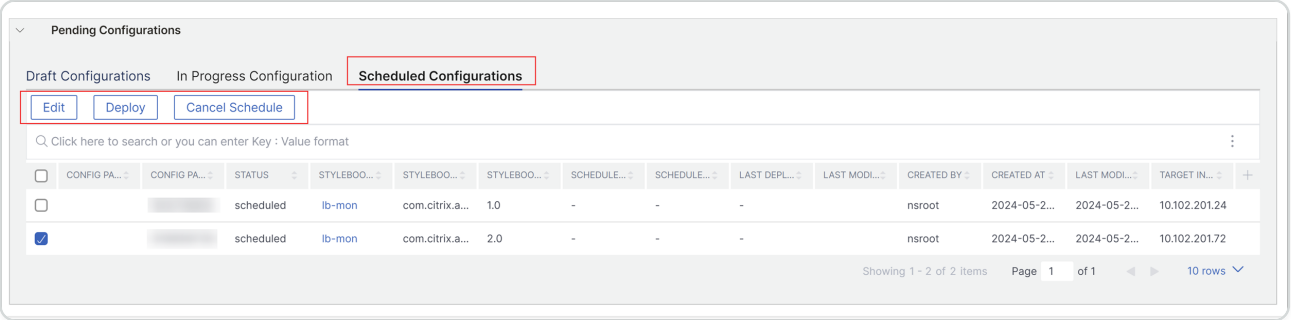


All the scheduled configurations are stored in **Scheduled configurations** tab under **Pending Configurations**. You can select the created schedule to edit the configuration parameters, deploy or cancel the schedule.

NOTE:

Deploying a scheduled config pack cancels the schedule and immediately executes the configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For a deployed config pack

You can also create a schedule to edit and delete a deployed config pack.

SCHEDULE AN EDIT OPERATION FOR A CONFIG PACK

To create a schedule to edit the deployed config pack, follow these steps:

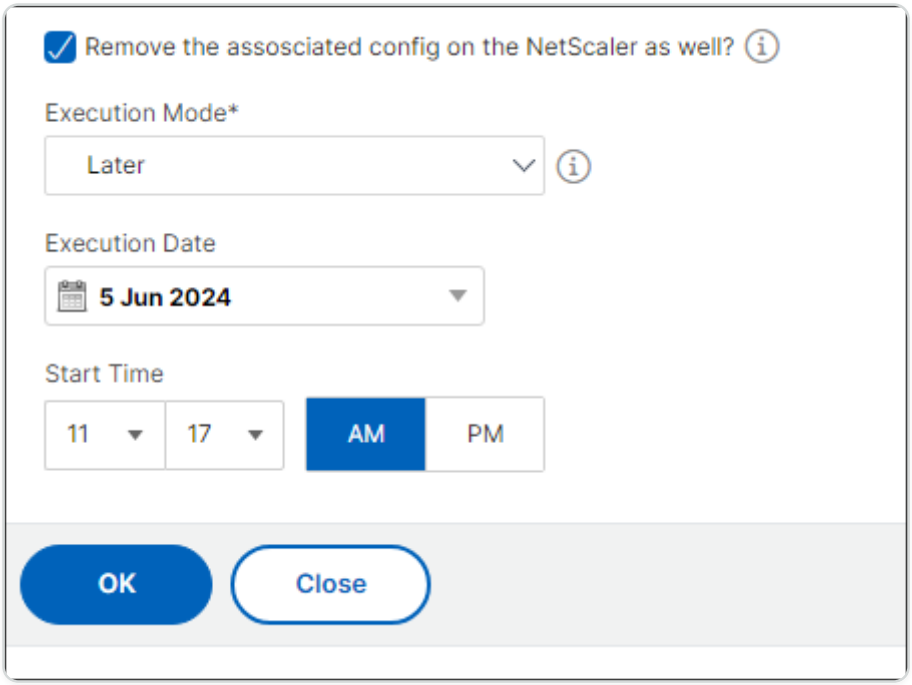
1. Navigate to **Applications > Configuration > Config Packs**.
2. On the **Configurations** page, select a StyleBook and click **Edit**.
3. On the **Edit Configuration** page, edit the config pack.
4. In the **Execution Mode** list, select **Later**.
5. Select the desired time and date for scheduling and click **Submit**.

SCHEDULE A DELETE OPERATION FOR A CONFIG PACK

To create a schedule to delete the deployed config pack, follow these steps:

1. Navigate to **Applications > Configuration > Config Packs**.
2. On the **Configurations** page, select a StyleBook and click **Delete**.
3. In the **Execution Mode** list, select **Later**.
4. Select the desired time and date for scheduling and click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

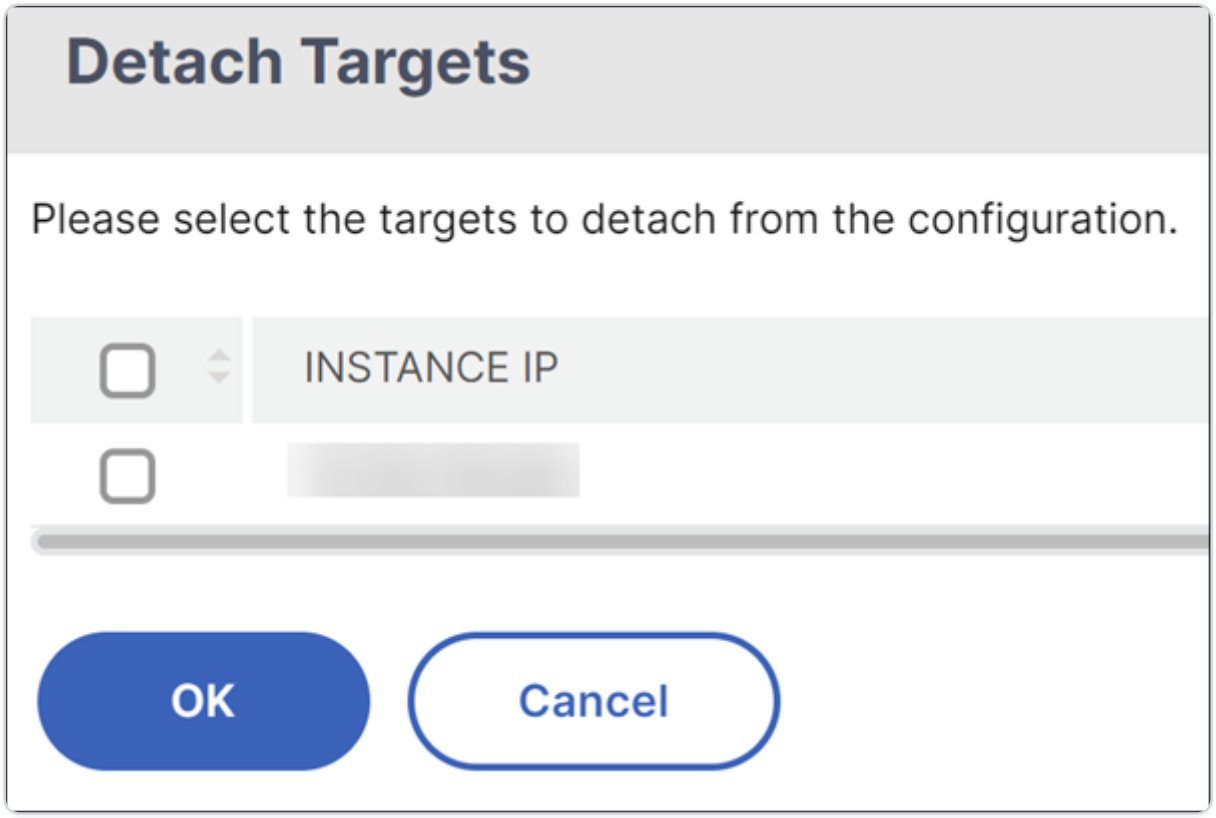


Detach a target instance from a configuration pack

To detach a target instance from a configuration pack, do the following:

1. Navigate to **Applications > Configuration > Config Packs**.
2. Select the configuration pack with a target instance that you want to remove.
3. In **Select Action**, select **Detach Targets**.
4. In the **Detach Targets** pane, select the target instance you want to remove from the configuration pack.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Click **OK**.

A message displays, confirming the creation of a duplicate configuration pack with the target instance now removed.

Build your StyleBooks

The full content of **example-lb** StyleBook is provided for your reference as follows:

```
name: example-lb

namespace: examples.stylebooks

version: "1.0"

display-name: Basic Load Balancer App

description: This is an example StyleBook that creates a load balancer
application

schema-version: "1.0"

import-stylebooks:

  -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    namespace: com.citrix.adc.stylebooks

    prefix: stlb

    version: "1.0"

parameters-default-sources:

  - stlb::lb

components:

  -

    name: lb-comp

    type: stlb::lb

    description: Uses the default lb StyleBook to build the typical lb
configuration objects

    properties-default-sources:

      - $parameters
```

The full content of **example-lb-mon** StyleBook is provided for your reference as follows:

```
name: example-lb-mon

namespace: examples.stylebooks

version: "1.0"

description: This is an example StyleBook that creates a load balancer
application with monitors

display-name: Basic Load Balancer App with Monitors

schema-version: "1.0"

import-stylebooks:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
  -
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: "1.0"
  -
    namespace: com.citrix.adc.commontypes
    prefix: cmtypes
    version: "1.0"
parameters-default-sources:
  - stlb::lb
parameters:
  -
    name: monitors
    label: "List of Monitors"
    description: "List of Monitors to monitor Application Servers"
    type: cmtypes::monitor[]
substitutions:
  mon-name(appname, monname): $appname + "-mon-" + $monname
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
components:

  -

    name: lb-comp

    type: stlb::lb

    description: Uses the default lb StyleBook to build the typical lb
configuration objects

    properties-default-sources:

      - $parameters

  -

    name: monitors-comp

    type: cmtypes::monitor

    condition: $parameters.monitors

    repeat: $parameters.monitors

    repeat-item: mon

    repeat-index: ndx

    description: Builds a list of NetScaler monitor objects and binds them
to the servicegroup of this LB config

    properties-default-sources:

      - $mon

    properties:

        monitorname: $substitutions.mon-name($parameters.lb-appname,
$mon.monitorname)

    components:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      -

        name: monitor-svcg-binding-comp

        condition:  $parameters.svc-servers

        type: ns::servicegroup_lbmonitor_binding

        properties:

          servicegroupname: $components.lb-
comp.outputs.servicegroup.properties.servicegroupname

          monitor_name: $parent.properties.monitorname
```

StyleBook to create a load balancing virtual server

In this example, you design a basic StyleBook that creates a load balancing virtual server of HTTP protocol type and listening on port 80. The virtual server name, IP address, and load balancing method parameters accept user-defined values, that is, they are the parameters of the StyleBook.

Header

The first six lines of a StyleBook comprise the header section. In this example, the header section is written as follows:

```
name: lb-vserver

namespace: com.example.stylebook

version: "1.0"

display-name: Load Balancing Virtual Server (HTTP)

description: "This stylebook defines a very simple load balancing HTTP
virtual server configuration"

schema-version: "1.0"
```

The header section includes the following details:

- **name**: A name for this StyleBook.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **description**: A description defining what this StyleBook does. This description appears on NetScaler Console.
- **display-name**: A descriptive name for the StyleBook that appears on NetScaler Console.
- **namespace**: A namespace forms part of a unique identifier for a StyleBook to avoid name collisions.
- **schema-version**: Always takes the value "1.0" in this release.
- **version**: The version number of the StyleBook. You can change the version number when you update the StyleBook.

The combination of **name**, **namespace**, and **version** uniquely identifies a StyleBook in the system. You cannot have two StyleBooks with the same combination of name, namespace, and version in NetScaler Console. However, you can have two StyleBooks with the same name and version but different namespaces, or with the same namespace and version but different names.

NOTE

Consider that you have updated your StyleBook and you have an updated version number. Now if you are referring to (that is, if you are importing) this StyleBook in other StyleBooks, ensure to update the version number in other StyleBooks too, so that they use the correct version of the imported StyleBook.

Import StyleBooks

The section after header is called "import-stylebooks." In this section, you must declare the namespace and version number of any other StyleBook that you want to refer to in your current StyleBook. This enables you to import and reuse other StyleBooks instead of rebuilding the same configuration in your own StyleBook.

In this example, the import-stylebooks section is written as follows:

```
import-stylebooks:

 -

  namespace: netscaler.nitro.config

  prefix: ns
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
version: "10.5"
```

Every StyleBook must refer to the netscaler.nitro.config namespace if it uses any of the NITRO configuration objects directly. This namespace contains all the NetScaler NITRO types, such as lbvserver.As software versions 10.5 and later are supported, you can use your StyleBook to create and run configurations on any NetScaler instance running release 10.5 and later.

The prefix used in the import-stylebooks section is a shorthand to refer to the combination of namespace and version. In this case, ns refers to netscaler.nitro.config of version 10.5. In the later sections of your StyleBook, instead of using the namespace and version to refer to the imported StyleBook, you can use the prefix string chosen, for example, ns, in the example above.

The version used in the StyleBooks is the NetScaler NITRO version. A StyleBook that is based on NITRO version X can be used to configure any NetScaler that is version X or higher.

NOTE

To ensure that your StyleBooks can be used to configure any NetScaler instance of version 10.5 or later, Citrix recommends that for maximum compatibility, import the NITRO 10.5 namespace in your StyleBooks that directly use NITRO built-in StyleBooks (namespace: netscaler.nitro.config, version: 10.5).

It is important that a StyleBook that imports other StyleBooks need to be based on a NITRO version that is at the same or higher version than the StyleBooks it imports. For example, a StyleBook that is based on NITRO version 10.5 cannot depend on or use or import a StyleBook that is based on 11.1. But a StyleBook based on version 11.1 can import a StyleBook based on any version less than 11.1.

It is also possible that a StyleBook that doesn't import the NITRO namespace at all. That means a StyleBook need not directly define NITRO components but can import (depend on) StyleBooks that defines NITRO components. The StyleBook that imports other StyleBooks always acquires the highest NITRO version in the hierarchy of its dependencies. And, it is used to configure NetScalers that are of that version or higher.

Parameters

The parameters section lets you declare all the parameters that you need in your StyleBook. You, as the StyleBook developer, have to decide what is the input that you want the users of your

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBook to specify. In this example, you have built your StyleBook in a way that requires its users to provide the name of the virtual server, its IP address, and the load balancing method.

The parameters section would look as follows:

```
parameters:

 -

  name: name

  label: "Application Name"

  description: "Give a name to the application configuration."

  type: string

  required: true

 -

  name: vip-ipaddress

  label: "Load Balancer IP Address"

  description: "The Application VIP that clients access"

  type: ipaddress

  required: true

 -

  name: lb-alg

  label: LB Algorithm

  description: Load Balancing Algorithm

  type: string

  default: ROUNDROBIN
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
allowed-values:
 - ROUNDROBIN
 - LEAST-CONNECTION
```

NOTE

If you do not provide the label of a parameter, then NetScaler Console uses the name attribute when displaying this parameter. You must always define a label for your parameters so that you can control how they show up in NetScaler Console.

When using the APIs however, the parameter is designated by its name.
In this section, you have declared three parameters indicated by their **name** attribute values - **name** for virtual server name, **ip** for IP address of the virtual server, and **lb-alg** for the load balancing method.

- **type** refers to the type of value these parameters can take. For example, name and `lb-alg` can take a string value and the IP value has to be of type IP address. Parameters in a StyleBook can be of any of the following built-in types:
- **string**: An array of characters. If a length is not specified, the string value can take any number of characters. However, you can limit the length of a string type by using the attributes min-length and max-length.
- **number**: An integer number. You can specify the minimum and maximum number that this type can take by using the attributes min-value and max-value.
- **boolean**: Can be either true or false. Also, note that all the literals are considered by YAML as booleans (for example, Yes or No).
- **ipaddress**: A string that represents a valid IPv4 or IPv6 address.
- **tcp-port**: A number between 0 and 65535 that represents a TCP or UDP port.
- **password**: An opaque/secret string value. When NetScaler Console displays a value for this parameter, it is shown as asterisks (*****).
- **certfile**: A certificate file.
- **keyfile**: A certificate private key file.
- **file**: A parameter of this type requires the user to upload a file, for example, a certificate or key file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **object**: Consists of multiple elements and each of these elements is a parameter. This type can be used to group multiple related parameters under one parent parameter.
- **required**: States whether a parameter is mandatory or optional. If it is set to true, the parameter is mandatory and the user has to provide a value for this parameter when creating configurations using this StyleBook. By default, all parameters are optional. In this example, **name** and **ip** are mandatory parameters while **lb-alg** is an optional parameter, the default value of which is "ROUNDROBIN."

Use the **default** attribute to assign a default value to an optional parameter. While creating a configuration, if a user does not specify a value, the default value is used. For example, for the **lb-alg** parameter, the default value is ROUNDROBIN.

Use the **allowed-values** attribute to define specific values that a user can choose from when creating a configuration. In this example, you have specified two values for the **lb-alg** parameter - ROUNDROBIN and LEASTCONNECTION.

When you import your StyleBook and use it, NetScaler Console displays a form with these three parameters. The fields displayed for name and IP allow string and `ipaddress` type of value to be entered, and the `lb-alg` field is displayed as a drop-down list with ROUNDROBIN selected as the default value.

NOTE

In addition to built-in types, a parameter can have another StyleBook as its type. This is a way of reusing parameters defined in other StyleBooks.

Components

The last section in this StyleBook is called the components section and is considered as the most important section in the StyleBook. In this section, you define the configuration objects that have to be created by the StyleBook.

For this example, you have to write the components section as follows:

```
components:

 -

  name: lbvserver-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  description: This StyleBook component (a Builtin Nitro StyleBook) builds
a NetScaler lbvserver configuration object.

  type: ns::lbvserver

  properties:

   name: $parameters.name

   ipv46: $parameters.vip-ipaddress

   lbmethod: $parameters.lb-alg

   servicetype: HTTP

   port: 80
```

This example contains only one component. The main attributes of a component are name, type, and properties. The type of a component determines what properties this component provides. Components are of two types:

- **Built-in type**: This type is provided by the system and you do not have to define it, for example, the NITRO entity types `lbvserver` or `servicegroup`. In this example, you are using a built-in component type.
- **Composite type**: This type is the StyleBook that you created and imported into NetScaler Console, or the default StyleBook that is shipped with NetScaler Console. You can learn more about composite StyleBooks in Create a Composite StyleBook.

In this example, you have defined a component called **lbvserver-comp**. This component is of type **ns::lbvserver** (a built-in NITRO type), where "ns" is the prefix that refers to the namespace netscaler.nitro.config and version 10.5 that you had specified in the import-stylebooks section, and `lbvserver` is a NITRO resource in this namespace.

The **properties** defined here are the attributes of the `lbvserver` resource. To learn more about all the available NetScaler NITRO resources and their attributes, see the NetScaler NITRO REST API documentation.

The properties in this section include the mandatory attributes of the `lbvserver` resource and allows you to specify values for these attributes. In this example, you are specifying static values for `servicetype` and port while the name, ipv46, and `lbmethod` properties get their values

© 1997–2026 Citrix Systems, Inc. All rights reserved.

from the input parameters. In the rest of the StyleBook, you can refer to the parameter names defined in the parameters section by using **$parameters.\<parameter-name\>** expression, for example, **$parameters.ip**.

NOTE

By convention, the prefix "ns" is always used to designate a NetScaler NITRO namespace in the "import-stylebooks" section. Though it is not mandatory, Citrix recommends to use the same convention in your own StyleBooks for consistency.

Build your StyleBook

Now that you have defined all the required sections of this StyleBook, bring them all together to build your first StyleBook. Copy and paste the StyleBook content to a text editor, and then save the file as **lb-vserver.yaml**. Citrix recommends that you use the built-in YAML validator in StyleBooks to validate and import the YAML content..

The full content of the file lb-vserver.yaml is reproduced below:

```
name: lb-vserver

namespace: com.example.stylebook

version: "1.0"

display-name: Load Balancing Virtual Server (HTTP)

description: "This stylebook defines a very simple load balancing HTTP
virtual server configuration"

schema-version: "1.0"



import-stylebooks:

 -

  namespace: netscaler.nitro.config

  version: "10.5"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
   prefix: ns
  -
   namespace: com.citrix.adc.stylebooks
   version: "1.0"
   prefix: stlb


parameters:
 -
   name: name
   label: "Application Name"
   description: "Give a name to the application configuration."
   type: string
   required: true
  -
   name: vip-ipaddress
   label: "Load Balancer IP Address"
   description: "The Application VIP that clients access"
   type: ipaddress
   required: true
  -
   name: lb-alg
   label: LB Algorithm
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  description: Load Balancing Algorithm

  type: string

  default: ROUNDROBIN

  allowed-values:

   - ROUNDROBIN

   - LEAST-CONNECTION



components:

 -

  name: lbvserver-comp

  description: This StyleBook component (a Builtin Nitro StyleBook) builds
a NetScaler lbvserver configuration object.

  type: ns::lbvserver

  properties:

   name: $parameters.name

   ipv46: $parameters.vip-ipaddress

   lbmethod: $parameters.lb-alg

   servicetype: HTTP

   port: 80
```

To start using your StyleBook to create configurations, you have to import it to NetScaler Console and then use it. For more information, see How to Use User-Defined StyleBooks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can also import this StyleBook into other StyleBooks (using the import-stylebooks construct.) Or, you can modify this StyleBook to include more parameters and components as described in the next section.

StyleBook to create a basic load balancing configuration

In this section, you design a StyleBook that creates a load balancing configuration which includes a load balancing virtual server, a service group, and a list of services. The StyleBook binds the services to the service group and binds the service group to the virtual server.

To create a basic load balancing configuration, use the example StyleBook, **lb-vserver** that you created in StyleBook to create a load balancing virtual server and save it as **basic-lb-config.yaml**.

Header

To build this StyleBook, update the header section. This section is similar to the header section that you created in StyleBook to create a load balancing virtual server.

Change the value of **name** to basic-lb-config. Update **description** and **display-name** to describe the StyleBook. You do not have to change the **namespace** and **version** values. Because you've changed the name, a unique identifier for this StyleBook is created in the system.

```
name: basic-lb-config

namespace: com.example.stylebooks

version: "0.1"

display-name: Load Balancing Configuration

description: This StyleBook defines a simple load balancing configuration.

schema-version: "1.0"
```

Import StyleBooks

The import-stylebooks section remains the same. It refers to the netscaler.nitro.config namespace to use the NITRO configuration objects.

```
import-stylebooks:

 -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
 namespace: netscaler.nitro.config

 prefix: ns

 version: "10.5"
```

Parameters

Update the parameters section to add two more parameters.

The parameters define the list of services or servers and the port on which the services listen to. The first three parameters `name`, `ip`, and `lb-alg` stay the same.

```
parameters:

 -

  name: name

  type: string

  label: Application Name

  description: Give a name to the application configuration.

  required: true

 -

  name: ip

  type: ipaddress

  label: Application Virtual IP (VIP)

  description: The Application VIP that clients access

  required: true

 -

  name: lb-alg
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  type: string

  label: LoadBalancing Algorithm

  description: Choose the loadbalancing algorithm (method) used for
loadbalancing client requests between the application servers.

  allowed-values:

     - ROUNDROBIN

     - LEASTCONNECTION

  default: ROUNDROBIN

 -

  name: svc-servers

  type: ipaddress[]

  label: Application Server IPs

  description: The IP addresses of all the servers of this application

  required: true

 -

  name: svc-port

  type: tcp-port

  label: Server Port

  description: The TCP port open on the application servers to receive
requests.

  default: 80
```

The parameter, **svc-servers**, is added to accept a list of IP addresses of the back end servers of the application. **svc-servers** is a mandatory parameter as indicated by **required: true**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The second parameter, **svc-port**, denotes the port number on which the servers listen. The default port number is 80 unless specified by the user.

Components

You have to also update the components section to define more components such that they use the two new parameters and build the complete load balancing configuration.

For this example, you have to write the components section as follows:

```
components:
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg


components:
 -
  name: svcg-comp
  type: ns::servicegroup
  properties:
   name: $parameters.name + "-svcgrp"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
 servicetype: HTTP


components:
  -
    name: lbvserver-svg-binding-comp
    type: ns::lbvserver_servicegroup_binding
    properties:
        name: $parent.parent.properties.name
        servicegroupname: $parent.properties.name
  -
    name: members-svcg-comp
    type: ns::servicegroup_servicegroupmember_binding
    repeat: $parameters.svc-servers
    repeat-item: srv
    properties:
       ip: $srv
       port: str($parameters.svc-port)
       servicegroupname: $parent.properties.name
```

In this example, the original component **lbvserver-comp** (from the previous example) now has a child component called **svcg-comp**. The **svcg-comp** component also has two child components within it. Nesting a component within another component allows the nested component to create configuration objects by referring to attributes in the parent component. The nested component can create one or more objects for each object created in the parent component.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The **svcg-comp** component is used to create a service group on the NetScaler instance by using the values provided for the attributes of the resource `servicegroup`. In this example, you are specifying the static value for `servicetype`, while **name** gets its value from the input parameter. Refer to the parameter **name** defined in the parameters section by using the **$parameters.name + "-svcgrp"** notation, where "**-svcgrp**" is appended (concatenated) to the user-defined name.

The component **svcg-comp** has two child components, **lbvserver-svg-binding-comp** and **members-svcg-comp**.

The first child component, **lbvserver-svg-binding-comp**, is used to bind a configuration object between the service group created by its parent component and the load balancing virtual server (`lbvserver`) created by the parent's parent component. The $parent notation, also called the parent reference, is used to refer to entities in the parent components. For example, **servicegroupname: $parent.properties.name** refers to the service group created by the parent component **svcg-comp**, and **name: $parent.parent.properties.name** refers to the virtual server created by the parent's parent component **lbvserver-comp**.

The **members-svcg** component is used to bind configuration objects between the list of services to the service group created by the parent component. The creation of binding configuration objects is achieved by using the **repeat** construct of StyleBook to iterate over the list of servers specified in the parameter **svc-servers**. During the iteration, this StyleBook component creates a NITRO configuration object of type **servicegroup_servicegroupmember_binding** for each service (referred to as `srv` in the **repeat-item** construct) in the service group, and it sets the **ip** attribute in each NITRO configuration object to the IP address of the corresponding server.

Generally, you can use the **repeat** and **repeat-item** constructs in a component to make that component build multiple configuration objects of the same type. You can assign a variable name to the **repeat-item** construct, for example, `srv`, to designate the current value in the iteration. This variable name is referred to in the properties of the same component or in child components as **`$<varname>`**, for example $srv.

In the preceding example, the nesting of components help to easily construct the configuration. You can also build the configuration without nesting as shown in the following example:

```
components:

 -

  name: lbvserver-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
 type: ns::lbvserver
 properties:
  name: $parameters.name + "-lb"
  servicetype: HTTP
  ipv46: $parameters.ip
  port: 80
  lbmethod: $parameters.lb-alg
-
 name: svcg-comp
 type: ns::servicegroup
 properties:
   servicegroupname: $parameters.name + "-svcgrp"
   servicetype: HTTP
-
 name: lbvserver-svg-binding-comp
 type: ns::lbvserver_servicegroup_binding
 properties:
  name: $components.lbvserver-comp.properties.name
  servicegroupname: $components.svcg-comp.properties.servicegroupname
-
 name: members-svcg-comp
 type: ns::servicegroup_servicegroupmember_binding
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  repeat: $parameters.svc-servers

  repeat-item: srv

  properties:

   ip: $srv

   port: 80

   servicegroupname: $components.svcg-comp.properties.servicegroupname
```

Here, even though the components are not nested, the generated NetScaler configuration is the same as that of the nested components used earlier.

The order in which the components are declared in the StyleBook does not impact the order of creation of the configuration objects. In this example, the components **svcg-comp** and **lbvserver-comp**, even though declared last, must be built before building the second component **lbvserver-svg-binding-comp** because there are forward references to these components in the second component.

NOTE

By convention, the names of StyleBooks, parameters, substitutions, components, and outputs are in lowercase. When they contain many words, they are separated by a "-" character. For example `lb-bindings`, `app-name`, `rewrite-config`, and so on. Another convention is to suffix component names with `-comp` string.

Outputs

In this section, you need to specify what the StyleBook exposes to the users (or in other StyleBooks) after it creates a configuration. For example, you can specify to expose the `lbvserver` and the `servicegroup` configuration objects that are created by this StyleBook.

```
outputs:

-

  name: lbvserver-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  value: $components.lbvserver-comp

  description: The component that builds the Nitro lbvserver configuration
object

-

  name: servicegroup-comp

  value: $components.svcg-comp

  description: The component that builds the Nitro servicegroup
configuration object
```

The outputs section of a StyleBook is optional. A StyleBook does not need to return outputs. However, by returning some internal components as outputs, it allows any StyleBooks that import this StyleBook to have more flexibility. This functionality is useful when creating a composite StyleBook.

NOTE

It is a good practice to expose an entire component of the StyleBook in the outputs section, rather than just a single property of a component (for example, expose the whole **$components.lbvserver-comp** rather than just the name, **$components.lbvserver-comp.properties.name**). Also add a description to the output explaining what the specific output represents.

Build your StyleBook

Now that you have defined all the required sections of this StyleBook, bring them all together to build your second StyleBook. You have already saved this StyleBook file as **basic-lb-config.yaml**. Citrix recommends that you use the built-in YAML validator in StyleBooks to validate and import the YAML content.

The full content of the file **basic-lb-config.yaml** is reproduced as follows:

```
name: basic-lb-config

namespace: com.example.stylebooks
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
version: "0.1"

display-name: Load Balancing Configuration

description: This StyleBook defines a simple load balancing configuration.

schema-version: "1.0"



import-stylebooks:

 -

  namespace: netscaler.nitro.config

  version: "10.5"

  prefix: ns

parameters:

 -

  name: name

  type: string

  label: Application Name

  description: Give a name to the application configuration.

  required: true

 -

  name: ip

  type: ipaddress

  label: Application Virtual IP (VIP)

  description: The Application VIP that clients access
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  required: true

 -

  name: lb-alg

  type: string

  label: LoadBalancing Algorithm

  description: Choose the loadbalancing algorithm (method) used for
loadbalancing client requests between the application servers.

  allowed-values:

     - ROUNDROBIN

     - LEASTCONNECTION

  default: ROUNDROBIN

 -

  name: svc-servers

  type: ipaddress[]

  label: Application Server IPs

  description: The IP addresses of all the servers of this application

  required: true

 -

  name: svc-port

  type: tcp-port

  label: Server Port

  description: The TCP port open on the application servers to receive
requests.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  default: 80


components:
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg
 -
  name: svcg-comp
  type: ns::servicegroup
  properties:
    servicegroupname: $parameters.name + "-svcgrp"
    servicetype: HTTP
 -
  name: lbvserver-svg-binding-comp
  type: ns::lbvserver_servicegroup_binding
  properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
   name: $components.lbvserver-comp.properties.name

   servicegroupname: $components.svcg-comp.properties.servicegroupname

 -

  name: members-svcg-comp

  type: ns::servicegroup_servicegroupmember_binding

  repeat: $parameters.svc-servers

  repeat-item: srv

  properties:

   ip: $srv

   port: 80

   servicegroupname: $components.svcg-comp.properties.servicegroupname


outputs:

-

  name: lbvserver-comp

  value: $components.lbvserver-comp

  description: The component that builds the Nitro lbvserver configuration
object

-

  name: servicegroup-comp

  value: $components.svcg-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  description: The component that builds the Nitro servicegroup
configuration object
```

To start using your StyleBook to create configurations, you have to import it to NetScaler Console and then use it. For more information, see How to Use User-Defined StyleBooks.

You can also import this StyleBook into other StyleBooks and use its properties as described in the next section.

Create a composite StyleBook

An important and powerful feature of StyleBooks is that they can be used as building blocks for other StyleBooks. A StyleBook can be imported into another StyleBook and it can be referred to as a **type** that is used by components of the second StyleBook similar to a NITRO built-in StyleBook.

For example, you can use the **basic-lb-config** StyleBook that you built in the previous section, to build another StyleBook called **composite-example**. To use the "basic-lb-config" StyleBook, you have to import it in the new StyleBook in the import-stylebooks section.

Build your StyleBook

The new StyleBook would look as follows:

```
name: composite-example

namespace: com.example.stylebooks

version: "0.1"

display-name: Load Balancing Virtual Server (HTTP/RoundRobin)

description: This StyleBook defines a RoundRobin load balancing
configuration with a monitor.

schema-version: "1.0"

import-stylebooks:

  -

   namespace: netscaler.nitro.config
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    version: "10.5"
    prefix: ns
  -
    namespace: com.example.stylebooks
    version: "0.1"
    prefix: stlb
parameters:
  -
    name: name
    type: string
    label: Application Name
    description: Give a name to the application configuration.
    required: true
  -
    name: ip
    type: ipaddress
    label: Application Virtual IP (VIP)
    description: The Application VIP that clients access
    required: true
  -
    name: svc-servers
    type: ipaddress[]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    label: Application Server IPs

    description: The IP addresses of all the servers of this application

    required: true



  -

    name: response-code

    type: string[]

    label: List of Response Codes

    description: List of Response Codes - Provide a list of response codes
in integer.



components:

  -

    name: basic-lb-comp

    type: stlb::basic-lb-config

    description: This component's type is another StyleBook that builds
the NetScaler lbvserver, servicegroups and services configuration objects.

    properties:

     name: $parameters.name

     ip: $parameters.ip

     svc-servers: $parameters.svc-servers

  -

     name: monit-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: ns::lbmonitor

    description: This component is a basic Nitro type (a Builtin
StyleBook) that builds the NetScaler monitor configuration object.

    properties:

      monitorname: $parameters.name + "-mon"

      type: HTTP

      respcode: $parameters.response-code

      httprequest: "'GET /'"

      lrtm: ENABLED

      secure: "YES"



    components:

       -

         name: monit-svcgrp-bind-comp

         type: ns::servicegroup_lbmonitor_binding

         properties:

           servicegroupname: $components.basic-lb-
comp.outputs.servicegroup-comp.properties.servicegroupname

           monitor_name: $parent.properties.monitorname
```

In the import-stylebooks section, you import the basic-lb-config StyleBook by using its namespace and version, referred to with the prefix `stlb`.

In the components section, two components are defined. The first component is of type **stlb::basic-lb-config**, where "basic-lb-config" is the name of the StyleBook you created in StyleBook to create a basic load balancing configuration. The properties that are defined for this

© 1997–2026 Citrix Systems, Inc. All rights reserved.

component correspond to the mandatory parameters declared in the basic-lb-config StyleBook. You can, however, use any parameter of the StyleBook (both required and optional.) Instead of re-building a `lbvserver`, a service group, and service and service group bindings, you import the StyleBook that does all of this as a component and use it to create these configuration objects in the new StyleBook.

StyleBook adds a second component `monit-comp` that uses the attributes of the NITRO resource `lbmonitor` (a built-in StyleBook) to create a monitor configuration object. It also has a sub-component `monit-svcgrp-bind-comp` to create the binding configuration object that binds the monitor to the `servicegroup` created in the first component. Because the `servicegroup` component created in the "basic-lb-config" StyleBook is exposed as an output, this StyleBook can access it using the expression **$components.basic-lb-comp.outputs.servicegroup-comp**. This is an example of how the outputs section can be used by the importing StyleBooks to have access to components in the imported StyleBooks that they would not have been able to access otherwise.

Next, copy and paste the StyleBook content to a text editor, and then save the file as **composite-example.yaml**. Ensure to validate the YAML content before you import the file in NetScaler Console. Then, import it to NetScaler Console and create one or several configurations by using this StyleBook.

Citrix recommends that you use the built-in YAML validator in StyleBooks to validate and import the YAML content.

Use GUI attributes in a custom StyleBook

You can add GUI attributes in the parameters section of your StyleBook to make the fields intuitive when displayed on NetScaler Console.

Add a label with tooltip for parameters

You can add a descriptive name for the parameter by using the label attribute. Add a tooltip for this parameter by using the description attribute.

Example:

```
name: ip

label: Virtual Server IP Address

description: IP address of the virtual server that represents the load
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
balanced application.

type: ipaddress

required: true
```

Set a collapsible pane for the parameter

If you have a parameter of type object, you can define the layout by using the **gui** attribute.

Example-1:

```
name: svcg-advanced

label: Advanced Application Server Settings

type: object

required: false

gui:

 collapse_pane: true

 columns: 2
```

In this example, the layout is a collapsible object where fields are displayed in two columns.

You can also display a summary view of a parameter of `type: object[]` (list of objects) as a table with the inner parameters representing the columns. To include or exclude an inner parameter from the summary view, you can use the `summary_display` attribute in the `gui` section as follows:

Example-2:

```
name: settings

label: Settings

type: object[]

parameters:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  -

    name: name

    label: Name

    description: Name of this setting

    type: string

    gui:

      summary_display: true
```

Set the user options as radio buttons

You can list the user options as radio buttons using `layout` and `allowed-values` attributes. So, when the user is creating a configuration pack, the parameter values appear as radio buttons.

By default, if the gui attribute is not specified, the parameter values are displayed as a drop-down menu.

```
-

    name: block-by-category-action

    label: Action

    description: Set an action if the bot is detected.

    type: string

    default: RESET

    gui:

        layout: radio

    allowed-values:

        - NONE
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        - DROP

        - REDIRECT

        - RESET

        - MITIGATION
```

In this example, the user options to set an action appear as radio buttons. And, the **RESET** option is selected by default.



Import custom StyleBooks

After you have built your StyleBook, import it to NetScaler Console to use it. NetScaler Console allows you to import a single StyleBook in YAML form or many StyleBook YAML files as a bundle in a .zip, .tgz, or .gz form. The NetScaler Console system validates your StyleBooks on import. The StyleBook is now ready to be used for creating configurations.

NetScaler Console also has a built-in YAML editor that you can use to compose the StyleBook YAML contents. The YAML editor allows you to validate your YAML constructs from the NetScaler Console GUI itself. You do not need to use a separate tool for these validation checks. The content is validated against YAML standards and any deviation is highlighted. You can then correct the content and attempt to import the StyleBook into NetScaler Console. The built-in YAML editor provides two advantages while writing your own StyleBook.

- **Color coded**. The editor displays the StyleBook content parsed as per YAML guidelines. The color coding helps you to differentiate easily between the keys and the values defined in the YAML content.
- **YAML validation**. The content is validated for YAML errors as you type in and any deviation is immediately highlighted. This validation allows you to write text that conforms to YAML guidelines even before you import the StyleBook in NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Currently, the editor validates the content according to YAML guidelines. It does not validate for code correctness and typographical errors.

Use HTML formatting tags in the StyleBook description and header

In the **StyleBook** definition, you can include a header field and use HTML formatting tags for the text. You can also include images as part of the header. The HTML content in the header field is displayed at the top of the configuration page when you are creating or updating a configuration. This feature allows you to add infographics for the StyleBook to help in understanding the StyleBook configuration. If you use images in the header, ensure to use base64 encoded image format in the `<img>` tag.

To use images in your HTML content, the images have to be inline as shown in the following example. You can use online tools to convert your images to their base64 encoded form.

```
name: cs-example

namespace: com.example.stylebooks

version: "1.2"

display-name: Content Switching Configuration

description: Example of a very simple content switching config that
creates and binds an lb to a cs

header:  <img id="b64img" src="…" />

     <h3>Operations performed by this StyleBook:</h3>

     <ul>

      <li style="list-style-type: circle"> Creates a Server </li>

      <li style="list-style-type: circle"> Creates a Service Group </li>

       <li style="list-style-type: circle"> Creates a LBVServer </li>

      <li style="list-style-type: circle"> Creates a CS Policy and Action
</li>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    </ul>

schema-version: "1.0"
```

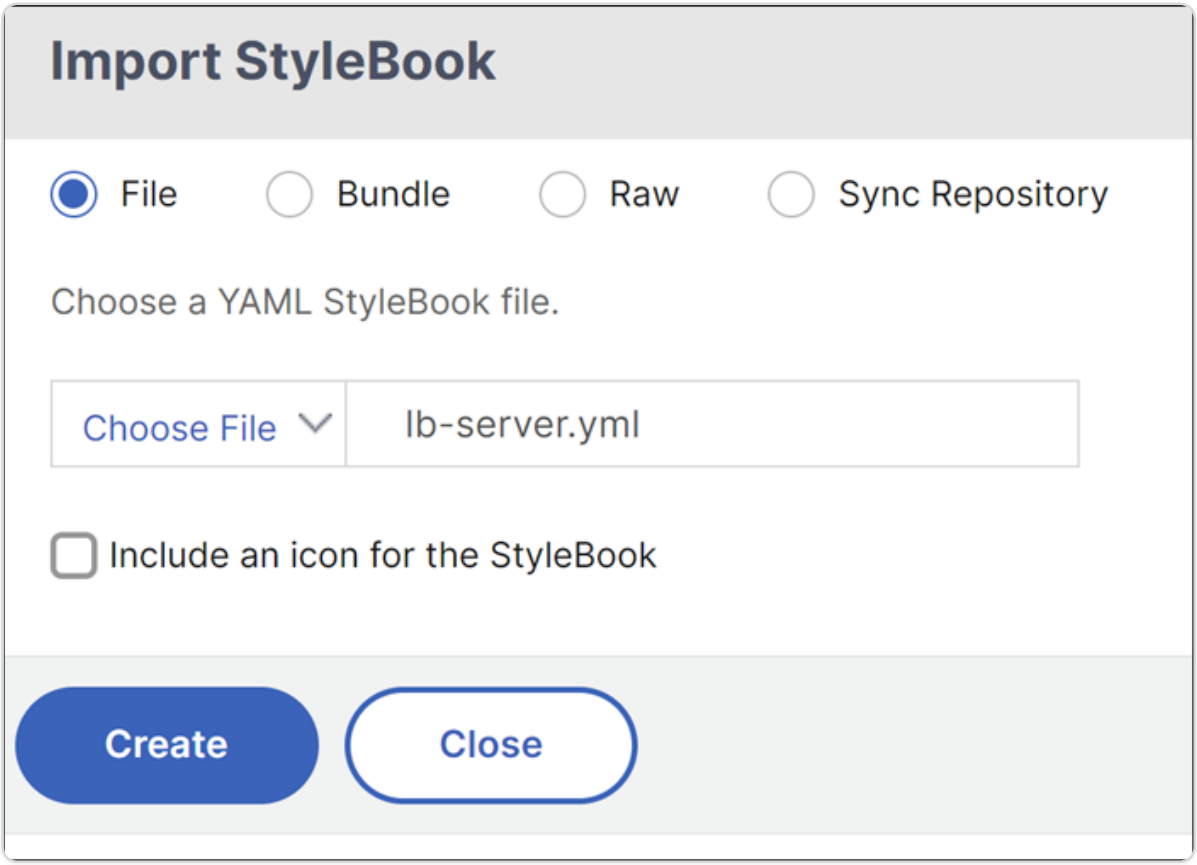
To import your StyleBook

1. In NetScaler Console, navigate to **Applications** > **Configuration** > **StyleBooks**, and then click **Import New StyleBook**.
2. Click one of the following options to import a StyleBook.

   - **File** - select the required file or the bundle of files from your local storage.

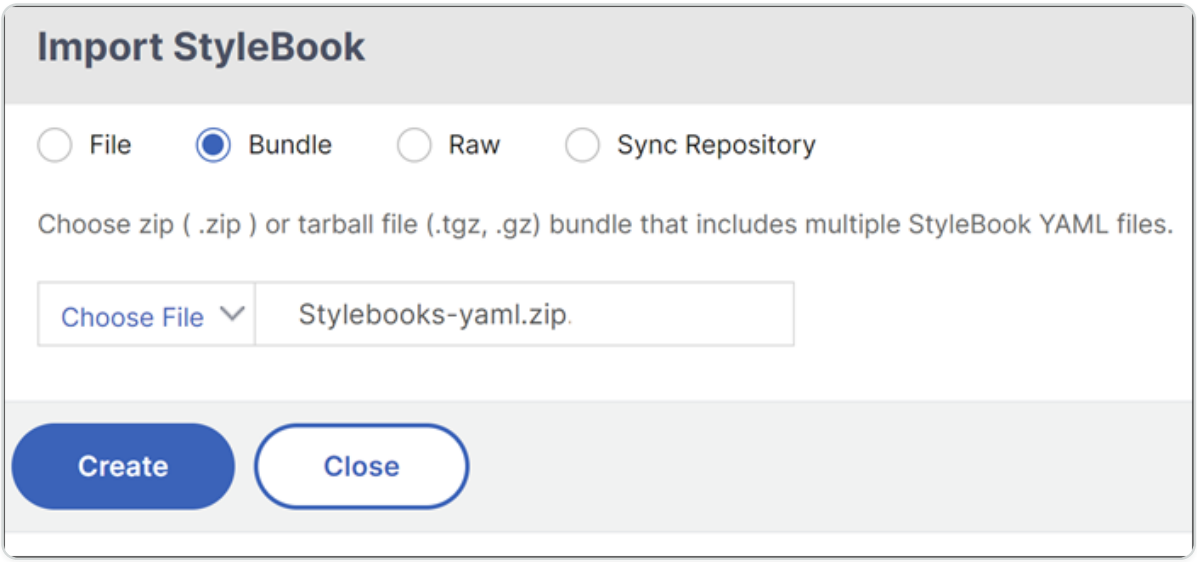
     NOTE:

     In this example, import the `lb-vserver.yml` StyleBook that you created in StyleBook to Create a Load Balancing Virtual Server.

   - **Bundle** - NetScaler Console allows you to import many StyleBooks in YAML format. You can import more than one YAML StyleBook files that are compressed in a zip (.zip) format or tarball (.tgz, .gz) format.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



A StyleBook that is imported into NetScaler Console is displayed with a default icon on the StyleBooks GUI. You can customize these default icons with your own images.

To do so:

- Create a folder named `resources` below the folder that has your StyleBook YAML files.
- Upload your icons to the `resources` folder.

NOTE:

You can't rename the `resources` folder to any other name.

- If the icon file and its corresponding StyleBook file have the same name, the icon is automatically mapped to the StyleBook.
- If the icon file and its corresponding StyleBook file (for example, exchange.yaml and exch.png) do not match, create a JSON file named ‘icon_mapping.json in the `resources` folder as follows:

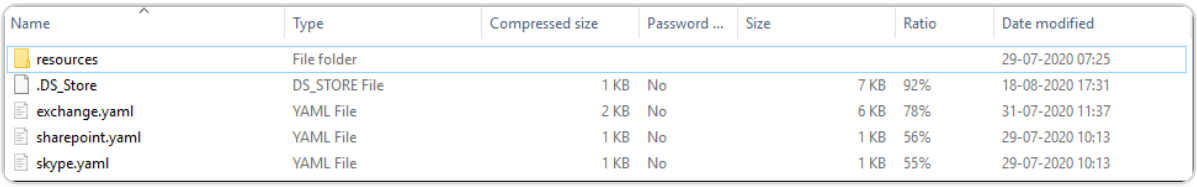
```
<StyleBook file name> : <icon file name>

<StyleBook file1 name> : <icon file1 name>

<StyleBook file2 name> : <icon file2 name>
```

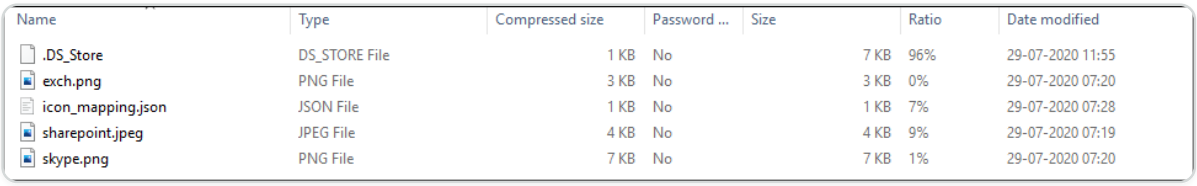
The following is an example StyleBook bundle:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
resources	File folder					29-07-2020 07:25
.DS_Store	DS_STORE File	1 KB	No	7 KB	92%	18-08-2020 17:31
exchange.yaml	YAML File	2 KB	No	6 KB	78%	31-07-2020 11:37
sharepoint.yaml	YAML File	1 KB	No	1 KB	56%	29-07-2020 10:13
skype.yaml	YAML File	1 KB	No	1 KB	55%	29-07-2020 10:13

The `resources` folder has the required icons.



Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
.DS_Store	DS_STORE File	1 KB	No	7 KB	96%	29-07-2020 11:55
exch.png	PNG File	3 KB	No	3 KB	0%	29-07-2020 07:20
icon_mapping.json	JSON File	1 KB	No	1 KB	7%	29-07-2020 07:28
sharepoint.jpeg	JPEG File	4 KB	No	4 KB	9%	29-07-2020 07:19
skype.png	PNG File	7 KB	No	7 KB	1%	29-07-2020 07:20

In this example, `sharepoint.yaml` and `skype.yaml` files are automatically mapped to `sharepoint.jpeg` and `skype.png` respectively.

To map `exchange.yaml` to `exch.png`, specify the following in the `icon_mapping.json` file:

```
{

"exchange.yaml":"exch.png"

}
```

If an icon isn't available in the StyleBook bundle, the default icon is displayed.

- **Raw** - Compose the content of your StyleBook in the YAML editor.

  You can validate the StyleBook contents to check the StyleBook grammar errors. To validate the StyleBook contents, click **Validate Contents**.

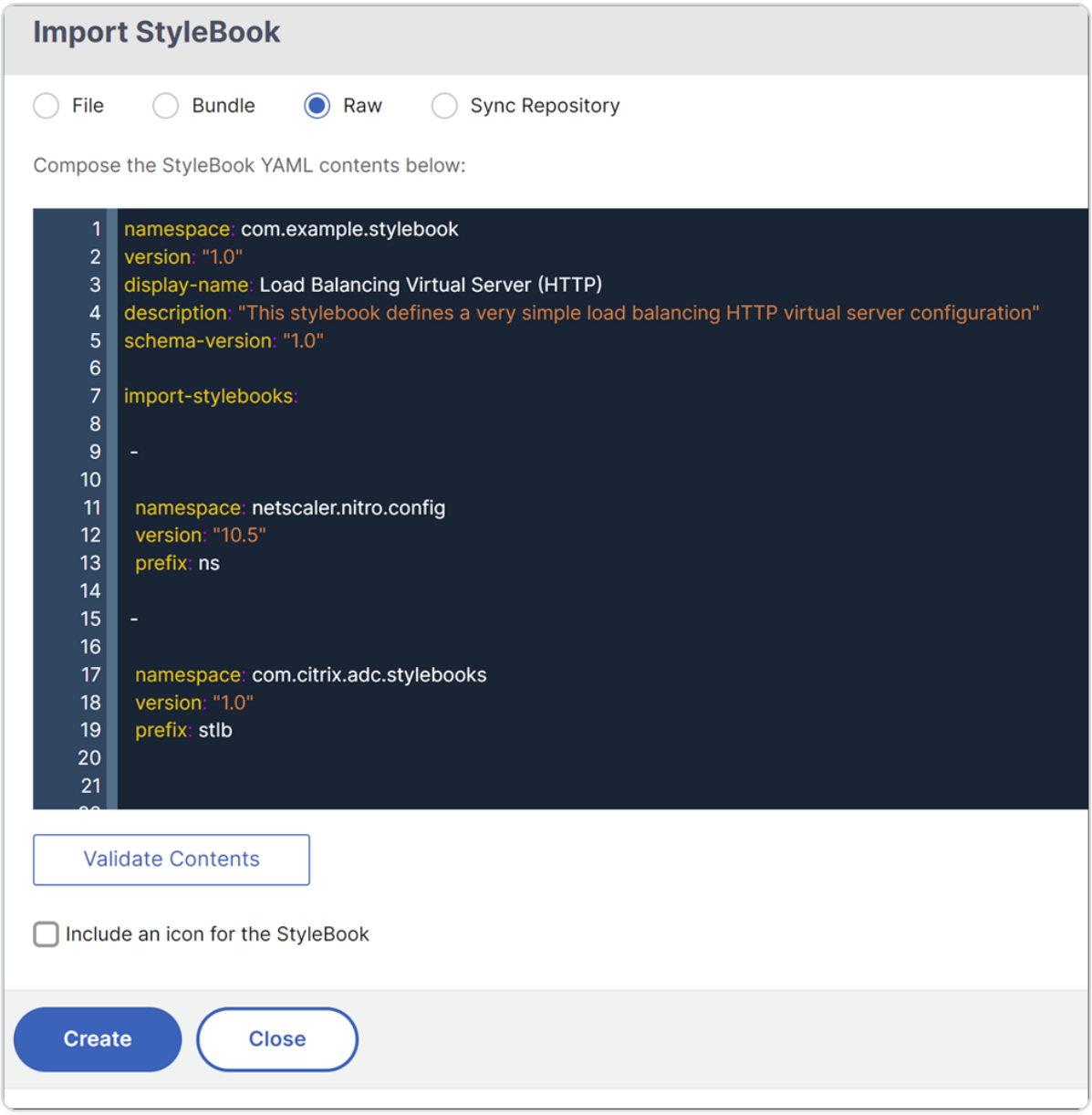
  NOTE:

  While composing a StyleBook, make sure to know the following concepts:

  - NITRO API
  - YAML

  For more information about how to write your own StyleBooks, see How to Create Your Own StyleBooks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE:

You can also create your StyleBook in your favorite editor and then copy and paste the content into the YAML editor for validation and import.

- **Sync Repository** - If you create and maintain your StyleBooks in GitHub, use this option for NetScaler Console to discover new or updated StyleBooks in your repository. Select the repository that you want to synchronize with NetScaler Console.

3. Optional, select an icon to a StyleBook.

   In **Applications > Configuration > StyleBooks**, the imported StyleBook appears with this icon.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Click **Create**.

   NetScaler Console now validates your StyleBook for all syntactic and semantic errors according to the StyleBook grammar. Your StyleBook is not imported into NetScaler Console if there are any errors.

   If there are no errors the StyleBook is successfully imported and listed on the **StyleBooks** page. You can identify the StyleBook by the display name that you defined in the header section of the StyleBook.

   NOTE:

   If you are importing a bundle of files, NetScaler Console decompresses the zipped folder and validates all the StyleBooks. The bundle isn't imported even if one StyleBook file fails the validation test.

   For more information on StyleBook grammar and syntax of the different constructs and attributes, see StyleBook Grammar.

5. Click the **Create Configuration** link to create configurations from this StyleBook.

   The **StyleBook** page opens and you can enter the values for all the parameters defined in this StyleBook.

6. Specify the required values for the parameters.

   In the following example,

   a. Specify the **application name** and **load balancer IP address** mandatory fields.

   b. Select the **LoadBalancing Algorithm** from the list. By default, **ROUNDROBIN** is selected.

7. Under **Target Instances**, select the IP address of the NetScaler instance where you want to deploy the configuration.

   You can also deploy the configuration on more than one NetScaler, by specifying as many target instances as needed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

To add all the recently discovered NetScaler instances in NetScaler Console to **Target Instances**, go to the **StyleBooks** page and click the refresh icon at the right-hand side of the page.

8. If you want to test at the NetScaler (NITRO) configuration objects before you deploy the configuration, click **Dry Run**.

   If the configuration is valid, the configuration objects are created based on the specified values.

   In this example, the StyleBook creates only one object of type `lbvserver`. This load-balancing server was the only component defined in this basic example StyleBook.

   Later, click **Create** to deploy the configuration on the selected NetScaler instances.

After you deploy the configuration successfully, a new configuration pack appears in the **Configurations** page.

Create a StyleBook to upload files

NetScaler Console StyleBooks allow you to create NetScaler configurations that might include among other things while uploading files of any type from your local filesystem to the NetScaler instance, by using the NetScaler Console GUI or the APIs. These files can be the example certificate files or geolocation files. You can also specify the directory to upload these files.

StyleBook configuration

The following is an example StyleBook that describes how to upload a geo-location file on the NetScaler instance. The geo files are used typically in GSLB configurations for defining static-proximity based on the geo location:

Build your StyleBook - 1

```
name: upload-geolocations

namespace: com.citrix.adc.stylebooks.samples

version: "1.0"

display-name: GeoLocation File Upload
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
description: This StyleBook is used to upload a geolocation file to
NetScaler

schema-version: "1.0"



import-stylebooks:

-

 namespace: netscaler.nitro.config

 version: "11.1"

 prefix: ns



parameters:

-

 name: locationfile

 label: Location File

 description: The system file path of the geolocation file on NetScaler
Console

 type: file

 required: true



components:

-

 name: upload-file-comp

 type: ns::systemfile
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
 properties:

    filename: $parameters.locationfile.filename

    filelocation: "/var/netscaler/inbuilt_db/"

    filecontent: base64.encode($parameters.locationfile.contents)
```

NOTE

The parameter used in this example is of a type file. You can import this StyleBook in NetScaler Console and use it to upload geolocation files.

This StyleBook requires the file to be already present in NetScaler Console (for example, you would have already copied it to NetScaler Console using a utility like SCP). If you want to upload a file to NetScalers through NetScaler Console without first copying it to the NetScaler Console filesystem, you can build a StyleBook that has two "string" parameters, one is for specifying the file name to be used on the NetScaler and the other to specify the contents of the file, and use these two parameters in the upload-file-comp components. The following is an alternative StyleBook to upload a geo-location file:

Build your StyleBook - 2

```
name: upload-geolocations-alt

namespace: com.citrix.adc.stylebooks.samples

version: "1.0"

display-name: GeoLocation File Upload

description: This StyleBook is used to upload a geolocation file to
NetScaler

schema-version: "1.0"



import-stylebooks:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
 -
  namespace: netscaler.nitro.config
  version: "11.1"
  prefix: ns


parameters:
 -
  name: filename
  label: Location Filename
  description: The name of the location file on the NetScaler
  type: string
  required: true
 -
  name: filecontents
  label: Location File Contents
  description: The contents of the location file
  type: string
  required: true


components:
 -
  name: upload-file-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
type: ns::systemfile

properties:

 filename: $parameters.filename

 filelocation: "/var/NetScaler/inbuilt_db/"

 filecontent: base64.encode($parameters.filecontents)
```

Creating configurations to upload files

The following procedure creates a configuration on a selected NetScaler instance that would upload a geolocation file using the first StyleBook described above.

To create a configuration for uploading files:

1. In NetScaler Console, navigate to **Applications** > **Configuration**, and click **Create New**. The Choose StyleBook page displays all the StyleBooks that are available in your NetScaler Console. Scroll down and select the StyleBook that you imported.

   The StyleBook parameters appear as a user-interface page that allows you to enter the values for all the parameters defined in this StyleBook.
2. Enter the name of the load balancer and the virtual IP address in the basic load balancer settings section.
3. In **Location File** section, enter the name or location of the file.

   NOTE

   Ensure that in NetScaler Console, the file is located under the current tenant's folder only. Use any FTP to copy the file to NetScaler Console file system.
4. You might be asked to provide your user credentials before you access the target instances.
5. Select the target NetScaler instance on which the configuration needs to be created, and click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

Citrix recommends that you select **Dry Run** to check the configuration objects that are created on the target instance before you run the actual configuration on the instance.

When the creation of the configuration pack is successful, the file is saved on the NetScaler instance file system under the location: /var/netscaler/inbuilt_db/

NOTE

You can also click the refresh icon to add recently discovered NetScaler instances in NetScaler Console to the available list of instances in this window.

Using the NetScaler Console API to create a configuration pack

You can also use the NetScaler Console API to create a configuration pack that uploads files to the selected NetScaler instance. For more information on how to use APIs, see How to Use API to Create Configurations to Upload Any File Type.

Create a StyleBook to upload SSL certificate and certificate key files

When creating a StyleBook configuration that uses the SSL protocol, you must upload the SSL certificate files and certificate key files as required by the StyleBook parameters. StyleBook allows you to directly upload the SSL files and key files from your local system by using the NetScaler Console GUI. You can also use the NetScaler Console APIs to upload certificate files and key files that NetScaler Console already manages.

StyleBook configuration

This document assists you to create your own StyleBook - **Load Balancing Virtual Server (SSL)** with components to upload SSL certificates and key files. The StyleBook provided here as an example creates a basic load balancing virtual server configuration on the selected NetScaler instance. The configuration uses the SSL protocol. To create a configuration using this StyleBook, you must provide the name and IP address of the virtual server, select the load balancing method parameters, and upload the certificate file and the certificate key file for the virtual server, or use a certificate file and certificate key file that are already present in the NetScaler Console. These parameters are specified in the following "parameters" section:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
parameters:
 -
  name: name
  type: string
  required: true
 -
  name: ip
  type: ipaddress
  required: true
 -
  name: lb-alg
  type: string
  allowed-values:
    - ROUNDROBIN
    - LEASTCONNECTION
  default: ROUNDROBIN
 -
  name: certificate
  label: "SSL Certificate File"
  description: "The file name of the SSL certificate file"
  type: certfile
 -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  name: key

  label: "SSL Certificate Key File"

  description: "The file name of the server certificate's private key
file"

  type: keyfile

 -

  name: passphrase

  label: "SSL Certificate Key Passphrase"

  description: "The password used to protect the certificate's private key
file"

  type: password
```

Two components are then created in the components section of the StyleBook. The `my-lbvserver-comp` component is of type `ns::lbvserver`, where:

- "ns" is the prefix that refers to the built-in namespace netscaler.nitro.config and version 10.5 that you specified in the `import-stylebooks` section.
- `lbvserver` is a built-in StyleBook in this namespace. It corresponds to the NetScaler NITRO `lbvserver` resource of the same name.

The second component `lbvserver-certificate-comp` is of type `stlb::vserver-certs-binds`. The prefix `stlb` refers to the namespace "com.citrix.adc.stylebooks" and version 1.0 that is specified in the import-stylebooks section of the StyleBook. If the "com.citrix.adc.stylebooks" namespace can be thought of as a folder, `vserver-certs-binds` is another StyleBook (or a file) in that folder. StyleBooks that are in the namespace "com.citrix.adc.stylebooks" are shipped as part of NetScaler Console.

The `vserver-certs-binds` StyleBook used by user-defined StyleBooks allows you to easily configure the certificates by uploading the certificate and key files to the target NetScaler instance, and by configuring the binding of the certificate and key files to the appropriate virtual servers. The

© 1997–2026 Citrix Systems, Inc. All rights reserved.

properties for this component are - the name of the lb virtual server and the names of the SSL certificates that you provide while creating the configuration pack.

```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name
   servicetype: SSL
   ipv46: $parameters.ip
   port: 443
   lbmethod: $parameters.lb-alg
 -
  name: lbvserver-certificate-comp
  type: stlb::vserver-certs-binds
  description: Binds lbvserver with server certificate
  properties:
   vserver-name: $components.my-lbvserver-comp.properties.name
   certificates:
    -
     cert-name: $parameters.name + "-lb-cert"
     cert-file: $parameters.certificate
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    ssl-inform: PEM

    key-name: $parameters.name + "-key"

    key-file: $parameters.key

    cert-password: $parameters.passphrase
```

When you use the API to create a configuration from such a StyleBook, use just the file names (not the full file path). These files are expected to be already available in the certificate and key file folders on NetScaler Console. The uploaded SSL certificate file is stored on NetScaler Console in the `/var/mps/tenants/.../ns_ssl_certs` directory, and the SSL certificate key file is stored in the `/var/mps/tenants/.../ns_ssl_keys` directory in NetScaler Console.

Creating configurations to upload SSL files

The following procedure creates a basic load balancing virtual server configuration on a selected NetScaler instance using the SSL protocol from the StyleBook example. You can use this procedure to upload the SSL certificate files and the certificate keys files in NetScaler Console.

To create a configuration for uploading files:

1. In NetScaler Console, navigate to **Applications** > **Configuration > StyleBooks**. The **StyleBooks** page displays all the StyleBooks that are available in your NetScaler Console.
2. Scroll down and select **Load Balancing Virtual Server (SSL)** or type **Load Balancing Virtual Server (SSL)** in the search field and press the **Enter** key.
3. Click **Create Configuration** in the StyleBook panel.

   The StyleBook parameters appear as a user-interface page that allows you to enter the values for all the parameters defined in this StyleBook.
4. Enter the name of the load balancer and the virtual IP address in the basic load balancer settings section.
5. In **SSL Certificates Settings**, select the respective files from your local storage folder. You can also select the files present on the NetScaler Console.
6. Select the target NetScaler instance on which the configuration must be created, and click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTES:

You can also click the refresh icon to add recently discovered NetScaler instances in NetScaler Console to the available list of instances in this window.

In NetScaler Console, the following default StyleBooks, which are shipped as part of NetScaler Console, enable you to create SSL support by uploading the SSL certificates and keys.

- HTTP/SSL LoadBalancing StyleBook (lb)
- HTTP/SSL LoadBalancing (with Monitors) StyleBook (`lb-mon`)
- HTTP/SSL Content Switched Application with Monitors (`cs-lb-mon`)
- Sample Application StyleBook using CS, LB, and SSL features (`sample-cs-app`)

Build your StyleBook

The full content of the file lb-vserver-ssl.yaml is shown below:

```
name: lb-vserver-ssl

namespace: com.example.ssl.stylebooks

version: "0.1"

description: "This stylebook defines a load balancing virtual server
configuration."

display-name: "Load Balancing Virtual Server (SSL)"

schema-version: "1.0"



import-stylebooks:

 -

  namespace: netscaler.nitro.config

  prefix: ns

  version: "10.5"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  -
   namespace: com.citrix.adc.stylebooks
   prefix: stlb
   version: "1.0"


parameters:
  -
   name: name
   type: string
   required: true
  -
   name: ip
   type: ipaddress
   required: true
  -
   name: lb-alg
   type: string
   allowed-values:
     - ROUNDROBIN
     - LEASTCONNECTION
   default: ROUNDROBIN
  -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  name: certificate

  label: "SSL Certificate File"

  description: "The file name of the SSL certificate file"

  type: certfile

 -

  name: key

  label: "SSL Certificate Key File"

  description: "The file name of the server certificate's private key
file"

  type: keyfile

 -

  name: key

  label: "SSL Certificate Key Passphrase"

  description: "The password used to protect the certificate's private key
file"

  type: password



components:

 -

  name: my-lbvserver-comp

  type: ns::lbvserver

  properties:

    name: $parameters.name
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    servicetype: SSL

    ipv46: $parameters.ip

    port: 443

    lbmethod: $parameters.lb-alg

-

 name: lbvserver-certificate-comp

 type: stlb::vserver-certs-binds

 description: Binds lbvserver with server certificate

 properties:

  vserver-name: $ components.my-lbvserver-comp.properties.name

  certificates:

   -

    cert-name: $parameters.name + "-lb-cert"

    cert-file: $parameters.certificate

    ssl-inform: PEM

    key-name: $parameters.name + "-key"

    key-file: $parameters.key

    cert-password: $parameters.passphrase
```

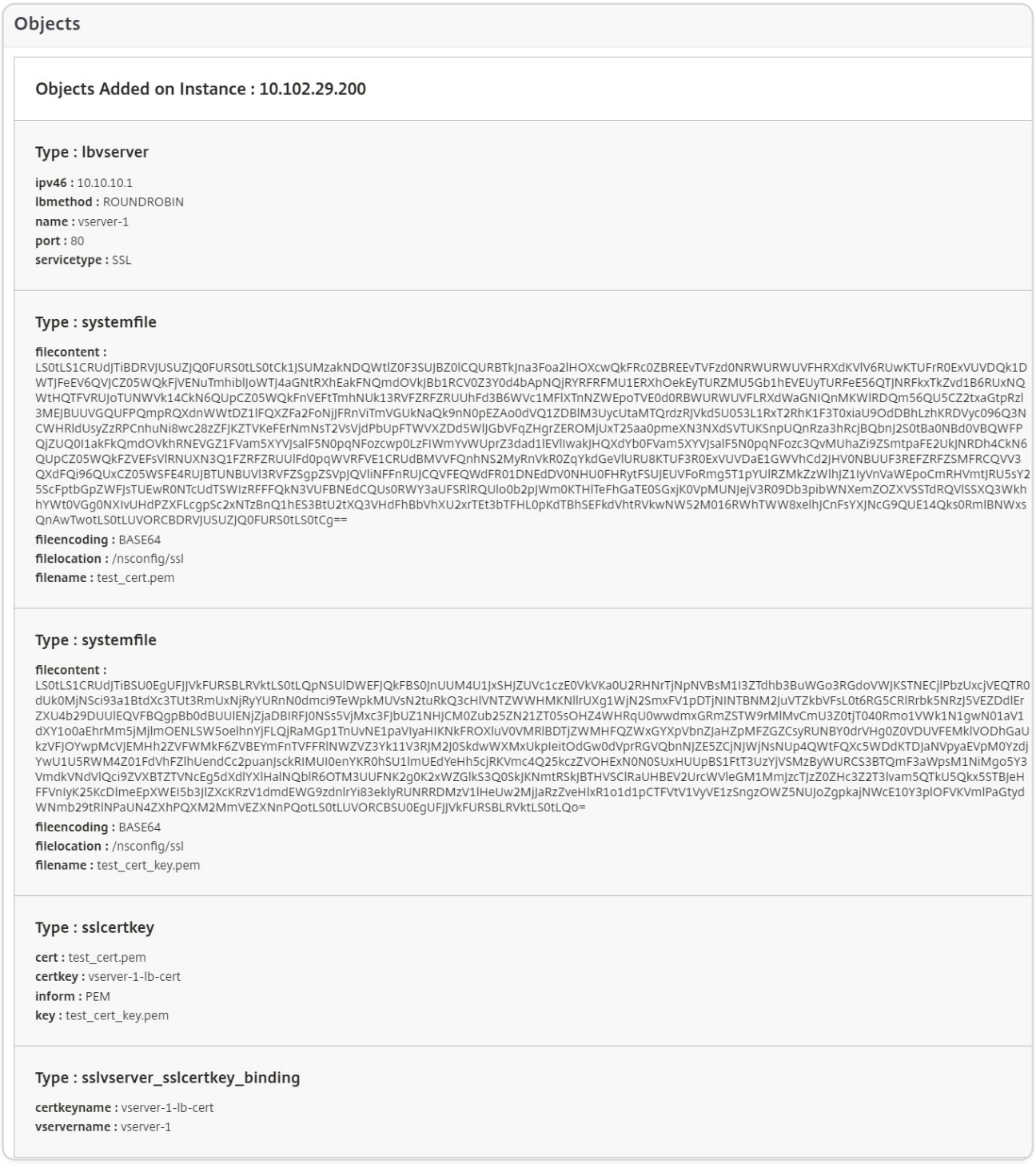
Using the NetScaler Console API to create a configuration pack:

You can also use the NetScaler Console API to create a configuration pack that uploads Cert and Key files to the selected NetScaler instance. For more information on how to use APIs, see How to Use API to Create Configurations to Upload Cert and Key Files.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Viewing the objects defined on the NetScaler instance

After the StyleBook configuration (configuration pack) is created on NetScaler Console, click **View objects created** to display all the NetScaler objects created on the target NetScaler instance



Manage SSL certificates from the certificate store using StyleBooks

NetScaler Console certificate store helps you to store and manage your SSL certificates in one location. So, you can store SSL certificates in NetScaler Console and reuse them during NetScaler configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This article describes how to create a StyleBook definition that allows you to upload and reuse SSL certificates from the NetScaler Console certificate store.

Parameters

The **StyleBook** definition supports `certkey` as a new built-in parameter type. Use this parameter type to reuse SSL certificates from the NetScaler Console certificate store.

```
parameters:

-

    name: certificate

    label: Certificate

    description: "Certificate to be bound to this virtual load balanced
application"

    type: certkey

    required: true
```

In this example, the certificate parameter refers to an SSL certificate or certificate chain from the NetScaler Console certificate store.

In the **StyleBook** definition, you can refer to the following properties for a `certkey` parameter:

- `certkeyname` – A name of SSL certificate key that you want to configure on an instance.
- `cert_filename` – The file name of an SSL certificate.
- `password` – The password required to access an SSL certificate if necessary.
- `key_filename` – The file name of an SSL certificate key.
- `keyfile_contents` – The file contents of an SSL certificate.
- `subject` – Subject mentioned in an SSL certificate.
- `issuer` – It refers to an authority who issued the SSL certificate.
- `certchain_certkeyname` – Sometimes, server certificates are signed by multiple hierarchical Certificate Authorities (CA), which means that the certificates form a chain.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use this property when the certificate store has a certificate chain. It helps you refer and bind the certificates together. While you create a configuration pack, the certificate chain appears as list.

These properties help you create the required components in the **StyleBook** definition.

Components

When a StyleBook has a `type: certkey` parameter, the StyleBook user can provide a certificate for this parameter from the NetScaler Console certificate store. In this workflow, along with viewing and selecting certificates from NetScaler Console certificate store, users can also do the following:

- Upload new certificates.
- Update existing certificates. For example, expired certificates.
- Remove certificates.

NOTES

- You can also manage certificates in NetScaler Console certificate store using NetScaler Console SSL Dashboard.
- When an SSL certificate is updated in the NetScaler Console certificate store, the config packs associated with the SSL certificate are automatically updated.

Build your StyleBook

The following is an example StyleBook definition. It is a complete definition that uses SSL certificates from the NetScaler Console certificate store. This StyleBook includes components that upload the main certificate and key files to the NetScaler instance. If these files are already present on the NetScaler instance, NetScaler Console skips the uploading steps, and these components have no effect.

```
name: lb-with-cert-from-certstore

namespace: com.example.stylebooks

version: "1.0"

display-name: Application using a CertStore certificate
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
description: This StyleBook defines a simple SSL Vserver.

schema-version: "1.0"



import-stylebooks:

 -

    namespace: netscaler.nitro.config

    version: "13.0"

    prefix: ns



parameters:

 -

  name: name

  type: string

  label: Application Name

  description: Give a name to the application configuration.

  required: true

 -

  name: ip

  type: ipaddress

  label: Application Virtual IP (VIP)

  description: The Application VIP that clients access

  required: true
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
 -

  name: certificate

  label: Application Certificate

  description: Certificate chain and key to be bound to this application

  type: certkey

  required: true




components:

 -

    name: pem-cert-files-comp

    type: ns::systemfile

    description: This component uploads the PEM certificate file onto the
NetScaler

    condition: $parameters.certificate

    properties:

      filename: $parameters.certificate.cert_filename

      filelocation: /nsconfig/ssl

      filecontent: base64($parameters.certificate.certfile_contents)

      fileencoding: BASE64

 -

    name: pem-KEY-files-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: ns::systemfile

    description: This component uploads the PEM key file onto the
NetScaler.

    condition: $parameters.certificate

    properties:

      filename: $parameters.certificate.key_filename

      filelocation: /nsconfig/ssl

      filecontent: base64($parameters.certificate.keyfile_contents)

      fileencoding: BASE64

 -

    name: cert-files-comp

    type: ns::sslcertkey

    description: This component creates the certkey on the NetScaler using
the uploaded files.

    condition: $parameters.certificate

    properties:

      certkey:  $parameters.certificate.certkeyname

      cert: $parameters.certificate.cert_filename

      key: $parameters.certificate.key_filename

 -

  name: lbvserver-comp

  type: ns::lbvserver

  description: This component creates the lbvserver of the application.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
properties:
 name: $parameters.name + "-lbvserver"
 servicetype: SSL
 ipv46: $parameters.ip
 port: 443
 lbmethod: ROUNDROBIN
components:
    -
      name: sslvserver-comp
      type: ns::sslvserver
      description: This component configures SSL settings on the vserver
      properties:
        vservername: $parent.properties.name
        ssl3?: ENABLED
        tls1?: ENABLED
        tls11?: ENABLED
    -
     name: cert-bindings-adv-comp
     type: ns::sslvserver_sslcertkey_binding
     description: This component binds the certkey to the vserver
     condition: $parameters.certificate
     properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        vservername: $parent.properties.name

        certkeyname: $parameters.certificate.certkeyname
```

Enable analytics and configure alarms on a virtual server defined in a StyleBook

You can use the operations construct to configure NetScaler Console analytics to collect AppFlow records on all or some of the traffic transactions handled by any virtual server component that is part of a StyleBook. You can also use this construct to configure alarms to get insight into the traffic managed by the virtual server.

The following example shows an operations section of a StyleBook:

```
operations:

  analytics:

   -

    name: lbvserver-ops

    properties:

      target: $components.basic-lb-comp

      filter: HTTP.REQ.URL.CONTAINS("catalog")

  alarms:

   -

    name: lbvserver-alarm

    properties:

      target: $components.basic-lb-comp

      email-profile: $parameters.emailprofile

      sms-profile: "MyProdSMS"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      rules:

       -

         metric: "total_requests"

         operator: "greaterthan"

         value: 25

         period-unit: $parameters.period

       -

         metric: "total_bytes"

         operator: "lessthan"

         value: 60

         period-unit: "day"
```

The attributes in the analytics section are used to instruct NetScaler Console analytics feature to collect AppFlow records on a virtual server component identified by the target property. You can also optionally specify a filter property that accepts a NetScaler Console policy expression to filter requests for which AppFlow records are collected on the virtual server.

When a configuration pack is created from this StyleBook, the NetScaler Console analytics feature is configured to collect AppFlow records on the virtual servers that were specified when these are created in the process of creating a configuration pack.

The attributes in the alarms section are used to set thresholds to generate alarms and send notifications on the virtual server identified by the target property. In the above example, the email-profile and SMS-profile properties are used to specify where the notifications has to be sent. The rules section defines the thresholds. For example, if the total requests handled by the virtual server are greater than 25 and for a period defined by the user, an alarm is set and notification is sent. The "period-unit" specifies how frequently an alarm is triggered. It can take the value of the day, hour, or weekly.

You can use the following operators when comparing the metric value to the threshold value:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `greaterthan` for `>`
- `lessthan` for `<`
- `greaterthanequal` for `>=`
- `lessthanequal` for `<=`

Note that StyleBooks use API names for the metrics and not the names displayed on the NetScaler Console analytics GUI.

To learn how to view and analyze data collected on virtual servers that were created as part of a configuration pack, see the NetScaler Console analytics documentation.

Instance roles

StyleBooks supports the following configurations on NetScaler instances:

- Symmetric configuration - When a configuration pack is applied on multiple NetScaler instances and the configurations deployed on all the instances are the same.
- Asymmetric configuration - When a configuration pack is applied on multiple NetScaler instances and the configurations deployed on all the instances are different. For example, in the default Microsoft Skype for Business StyleBook, a different configuration has to be deployed on each NetScaler instance.

The "instance roles" feature of StyleBooks helps you to create an asymmetric configuration. Here, each NetScaler instance in the configuration pack can be assigned a different role. The role determines the configuration objects of the configuration pack that the NetScaler instance receives.

Points to note:

- The set of instance roles in a StyleBook are defined while creating the StyleBook.
- The roles are assigned to a specific NetScaler instance when creating or updating the configuration pack.

Target-roles section

The "target-roles" is typically placed after the "import-StyleBooks" section and before the "parameters" section in a StyleBook. All the roles supported by the StyleBook are declared in the "target-roles" section.

In the following StyleBook example, two roles are defined within the "target-roles" section - A and B.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
target-roles:



  -

   name: A

   name: B

     min-targets: 2

     max-targets: 5
```

You can see that role B also defines two optional subproperties, `min-targets` and `max-targets`.

`min-targets` specify the minimum mandatory number of NetScaler instances to assign this role when creating a configuration pack from this StyleBook. `max-targets` specify the maximum number of NetScaler instances that can be assigned this role when creating a configuration pack from this StyleBook.

If these subproperties are not specified, then there is no limit to the number of NetScaler instances that can be configured for that role. For min-targets = 0, the configuration associated with the role is optional. For min-targets = 1, the configuration is mandatory and at least one NetScaler instance must be configured for the role.

Role "default"

In addition to explicitly defined roles, there's an implicit role that all StyleBooks have. This implicit role is called the default role and is used like any other role in a StyleBook. When creating a configuration pack, if an NetScaler instance is not assigned with a specific role, the instance gets implicitly assigned to the "default" role. The instance then receives any configuration objects generated by components that have the "default" role.

Components with roles

After the roles that a StyleBook can support (including the role "default") are defined, the roles can be used in the components section of a StyleBook. If you want a component to be deployed only on NetScaler instances that play a certain role, then you can specify the roles attribute as part of the component, as illustrated in the following example of a component:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-

  name: C1

  type: ns::lbvserver

  roles:

    - A

  properties:

    name: lb1

    servicetype: HTTP

    ipv46: 1.1.1.1

    port: 80
```

In this example, the component generates an `lbvserver` is deployed on instances playing the role A. The roles attribute of a component is a `list`, and the component can be assigned multiple roles. These roles would have been declared in the `target-roles` section of the StyleBook.

NOTE

If a component in a StyleBook doesn't specify a role attribute, then the configuration objects generated by the component are created on all NetScaler instances, irrespective of the roles. You can use this feature effectively to create configuration objects that can be applied to all instances of a configuration pack.

Consider a StyleBook with two roles and four components.

- Component C1 has the roles A and B
- Component C2 has the role B
- Component C3 doesn't have any roles defined
- Component C4 has the role "default"

The components section of this StyleBook is as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
components:
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
      - B
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
  -
    name: C2
    type: ns::lbvserver
    roles:
      - B
    properties:
      name: lb2
      servicetype: HTTP
      ipv46: 12.12.12.12
      port: 80
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-
  name: C3
  type: ns::lbvserver
  properties:
    name: lb3
    servicetype: HTTP
    ipv46: 13.13.13.13
    port: 80
-
  name: C4
  type: ns::lbvserver
  roles:
    - default
  properties:
    name: lb4
    servicetype: HTTP
    ipv46: 14.14.14.14
    port: 80
```

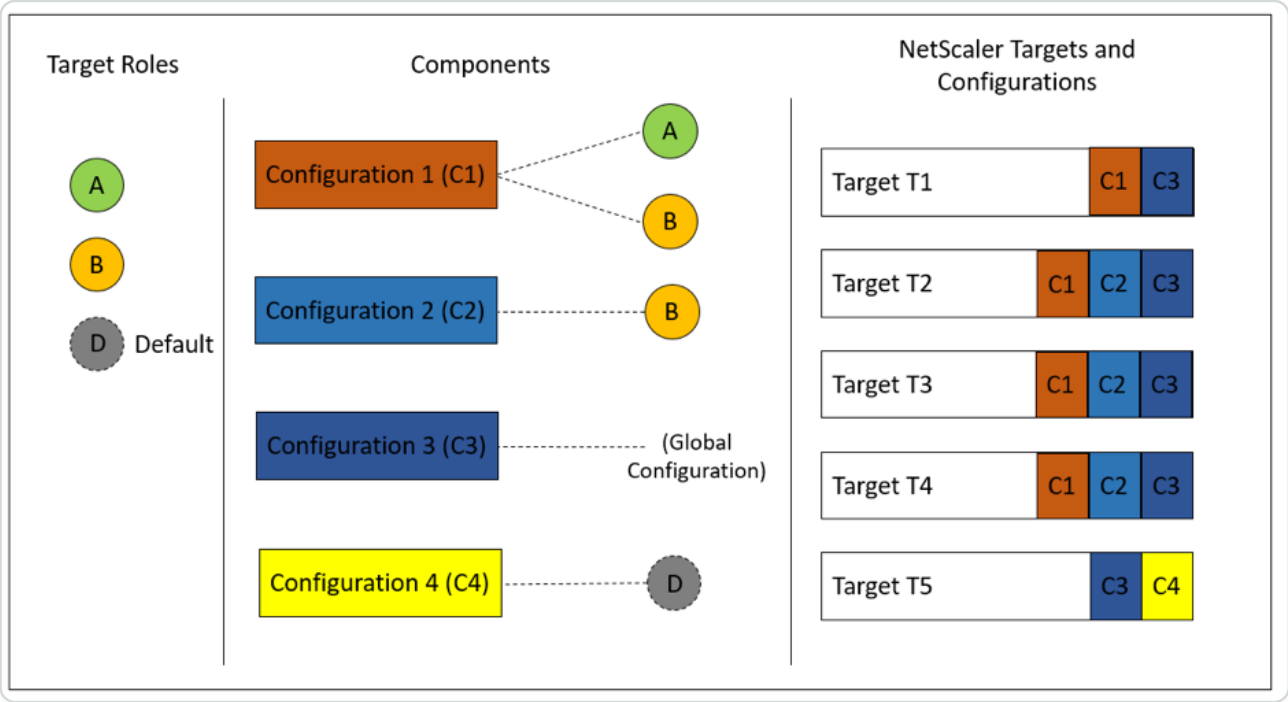
The component C3 doesn't have a role defined, which means the component is deployed on all instances regardless of their role. On the other hand, component C4 has the role "default", which means it is applied to any instance that doesn't have an explicit role assigned to it.

Now, consider that you want to create a configuration pack using this StyleBook, and deploy it on five NetScaler instances. You can assign the roles to the instances in the following manner:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Role A is assigned to Instances T1, T2, T3, and T4
- Role B is assigned to Instances T2, T3, and T4
- Instance T5 isn't assigned any role

The following image summarizes the role assignments, and shows the resulting configuration that each NetScaler instance receives:



The component C3 is deployed on all instances regardless of role, since this component had no `roles` attribute.

Use the "Dry Run" feature to view and verify:

- The assignment of roles
- The configuration objects created on each NetScaler instance

Build your StyleBook

The full content of the StyleBook "demo-target-roles" is as follows:

```
---

name: demo-target-roles

namespace: com.example.stylebooks

version: "1.2"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
parameters:
  -
    name: appname
    type: string
    required: true
    key: true
target-roles:
  -
    name: A
  -
    name: B
    min-targets: 2
    max-targets: 5
components:
  -
    name: C1
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: ns::lbvserver
    roles:
      - A
      - B
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
  -
    name: C2
    type: ns::lbvserver
    roles:
      - B
    properties:
      name: lb2
      servicetype: HTTP
      ipv46: 12.12.12.12
      port: 80
  -
    name: C3
    type: ns::lbvserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    properties:
      name: lb3
      servicetype: HTTP
      ipv46: 13.13.13.13
      port: 80
  -
    name: C4
    type: ns::lbvserver
    roles:
      - default
    properties:
      name: lb4
      servicetype: HTTP
      ipv46: 14.14.14.14
      port: 80
```

The following image shows the objects created for a sample configuration pack:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Objects created (9) ×

Instance : 10.102.102.136 | Roles : B | Count : 3

Type : lbvserver
ipv46 : 1.1.1.1
name : lb1
port : 80
servicetype : HTTP

Type : lbvserver
ipv46 : 12.12.12.12
name : lb2
port : 80
servicetype : HTTP

Type : lbvserver
ipv46 : 13.13.13.13
name : lb3
port : 80
servicetype : HTTP

Instance : 10.102.102.135 | Roles : B | Count : 3

Type : lbvserver
ipv46 : 1.1.1.1
name : lb1
port : 80
servicetype : HTTP

Type : lbvserver
ipv46 : 12.12.12.12
name : lb2
port : 80
servicetype : HTTP

Type : lbvserver
ipv46 : 13.13.13.13
name : lb3
port : 80
servicetype : HTTP

Instance : 10.102.102.62 | Roles : A, default | Count : 3

Type : lbvserver
ipv46 : 1.1.1.1
name : lb1
port : 80
servicetype : HTTP

Type : lbvserver
ipv46 : 13.13.13.13
name : lb3
port : 80
servicetype : HTTP

Type : lbvserver
ipv46 : 14.14.14.14
name : lb4
port : 80
servicetype : HTTP

Using APIs

When using the REST API, you can specify roles for each NetScaler instance when creating or updating the configuration pack as follows. In the "targets" block, specify the UUID of the specific NetScaler instance on which you want to deploy the individual components.

```
"targets": [

           {

            "id": "<ADC-UUID>",

            "roles": ["A"]

           },

          ]
```

A complete sample REST API is provided for your reference.

POST /`<IP`>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/1.2/demo-target-roles/configpacks

```
{

  "configpack": {

     "parameters": {

     "appname": "app1"

    },

     "targets": [

        {

          "id": "f53c35c3-a6bc-4619-b4b4-ad7ab6a94ddb",

        "roles": ["A"]

        },
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        {
          "id": "c08caa1c-1011-48aa-b8c7-9aed1cd38ed0",
          "roles": ["A", "B"]
        },
        {
          "id": "88ac90cb-a5cb-445b-8617-f83d0ef6174e",
          "roles": ["A", "B"]
        },
        {
          "id": "bf7b0f74-7a83-4856-86f4-dcc951d3141e",
          "roles": ["A", "B"]
        },
        {
          "id": "fa5d97ab-ca29-4adf-b451-06e7a234e3da",
          "roles": ["default"]
        }
      ]
    }
}
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a StyleBook to perform non-CRUD operations

StyleBooks manage NetScaler configurations by computing the necessary configuration objects on the NetScaler instances. These objects are added, updated, or removed from the instance each time you create or update a ConfigPack. That is when you specify the "desired state."

However, some NetScaler configuration objects support a few operations other than create, update, or delete (CRUD operations). For example, a load balancer object (`lbvserver`) or a NetScaler feature object (`nsfeature`) can support the "enable" or "disable" operation. Similarly, NetScaler `certkeys` support the "link" and "unlink" operation to link or unlink a certificate to another certificate. These operations on NetScaler objects are called as non-CRUD operations.

This section describes how to perform non-CRUD operations on configuration objects that support them using StyleBooks.

NOTE

The binding between configuration objects (for example, bind a `certkey` to a `lbvserver`) is not a non-CRUD operation because NITRO bindings are represented as configuration objects in their own right. These objects are created and deleted like any other NetScaler configuration object.

Supporting the non-CRUD operations

A construct called `meta-properties` is added in the component at the same level as the `properties` construct. The supported attribute supported in this construct is called `action`. This attribute can take values like `enable`, `disable`, `link`, `unlink`, `import`, `export`, `create`, `archive`, and `apply`.

```
components:

 -

  name: my-lbvserver-comp

  type: ns::lbvserver

  meta-properties

   action: enable
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  properties:

    name: $parameters.name

    servicetype: HTTP

    ipv46: $parameters.ip

    port: 80

    lbmethod: $parameters.lb-alg
```

In this example, the `my-lbvserver-comp` component is of the type `ns::lbvserver`. The "ns" is the prefix that refers to the namespace netscaler.nitro.config and version ** 10.5 that you specified in the import-stylebooks section. The `lbvserver` is a NITRO resource in this namespace. As an implicit action, the StyleBook creates `lbvserver` and then completes the "enable" operation on it.

The `action` in the meta-properties is done on the configuration object only during the creation of the configPack. Updates to the configPack do not perform non-CRUD actions.

You can specify expressions for a meta-property. These expressions dynamically apply the valid meta-property actions for NetScaler objects.

Example:

```
parameters:

-

    name: meta-action-lbvserver

    type: string

    default: disable

    allowed-values:

      - enable

      - disable
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
components:
  -
    name: c1
    type: ns::lbvserver
    meta-properties:
      action: $parameters.meta-action-lbvserver
    properties:
      name: $parameters.lbvserver
      ipv46: $parameters.ip
      port: 80
      servicetype: HTTP
```

In this example, a StyleBook user can specify a valid meta property action while creating a configuration pack.

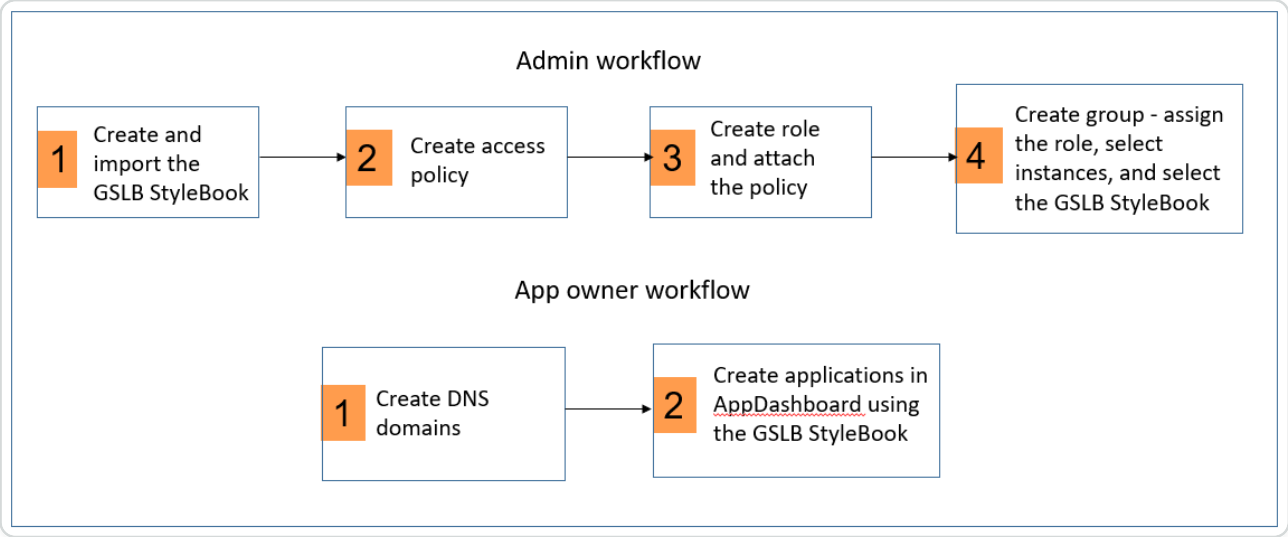
Deploying GSLB configurations using DNS domain names

The new RBAC enhancements in NetScaler Console allow only authorized application owners to create and manage their own DNS domains in NetScaler Console. You can now authorize the app owners to create GSLB configurations from the DNS domains they own, using specific StyleBooks. If the DNS domain name selected is owned by the user, then it can be used when creating GSLB configurations using GSLB StyleBooks in NetScaler Console application dashboard. There are two workflows in NetScaler Console to configure GSLB configurations.

1. **Workflow for the admins**. Set up the RBAC environment in NetScaler Console. That is, to create and import GSLB StyleBooks, you must create user groups, policies and roles, and assign users to the group. As an admin, you must perform this workflow.
2. **Workflow for the application owners**. Application owners must create GSLB configurations using domain names that they own.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The following flowchart depicts both workflows:



Workflow for the admins

As an admin, your workflow to create RBAC environment in NetScaler Console consists of the following steps:

First, create a StyleBook to deploy GSLB configurations on the NetScaler instances. This document provides with a sample YAML content to help you create your own StyleBook - Build your StyleBook.

For more information on how to create custom StyleBooks, see Create and use custom StyleBooks.

NOTE:

NetScaler Console supports a new construct in StyleBooks called "allowed-dynamic-values." This construct can be used to allow the user to list and select from the DNS Domain Values present in NetScaler Console to automatically populates the "domain-name" parameter in the StyleBook in NetScaler Console GUI.

An example "domain-name" parameter section is provided for your reference.

The "domain-name" parameter used here is just an example. The parameter can be different in your custom StyleBook.

```
-

  name: domain-name
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
label: DNS Domain Name

description: GSLB DNS Domain Name

type: string

required: true

allowed-dynamic-values:

   source: local

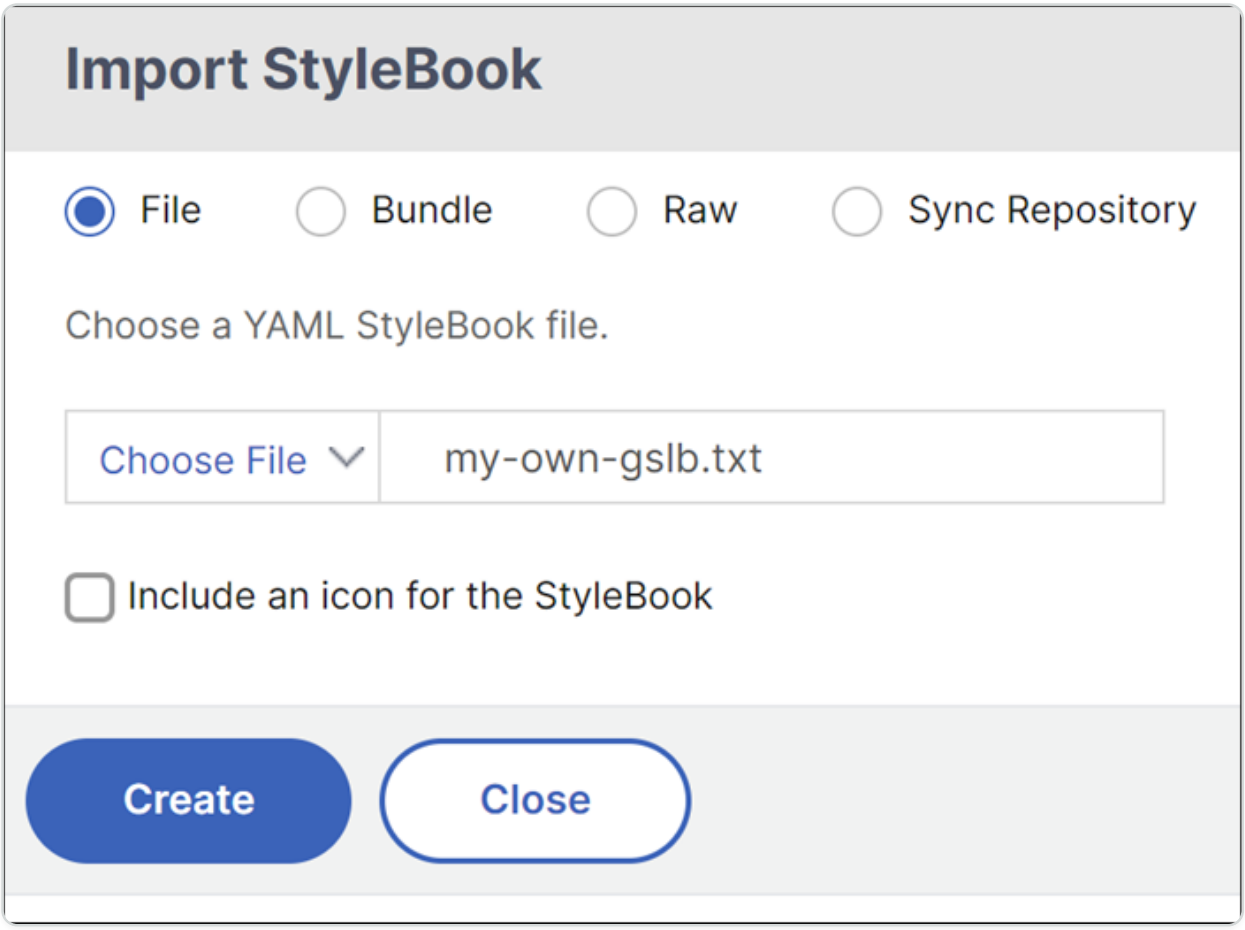
   resource-type: dns_domain_entry
```

NOTE:

Currently in NetScaler Console, the "allowed-dynamic-values" construct is not used in any of the default StyleBooks. Create a new custom GSLB StyleBook by using the default GSLB StyleBook. Replace the part for domain name parameter with the sample provided above. You can use any text editor to create new StyleBooks.

1. Log on to NetScaler Console as admin.
2. Navigate to **Applications** > **Configurations** > **StyleBooks**.
3. Click **Import New StyleBook** and upload the new GSLB StyleBook to NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For more information on how to import StyleBooks in NetScaler Console, see Use custom StyleBooks.

4. Navigate to **System** > **Users** > **Policies** and click **Add** to set up an access policy for the application owners as shown below.

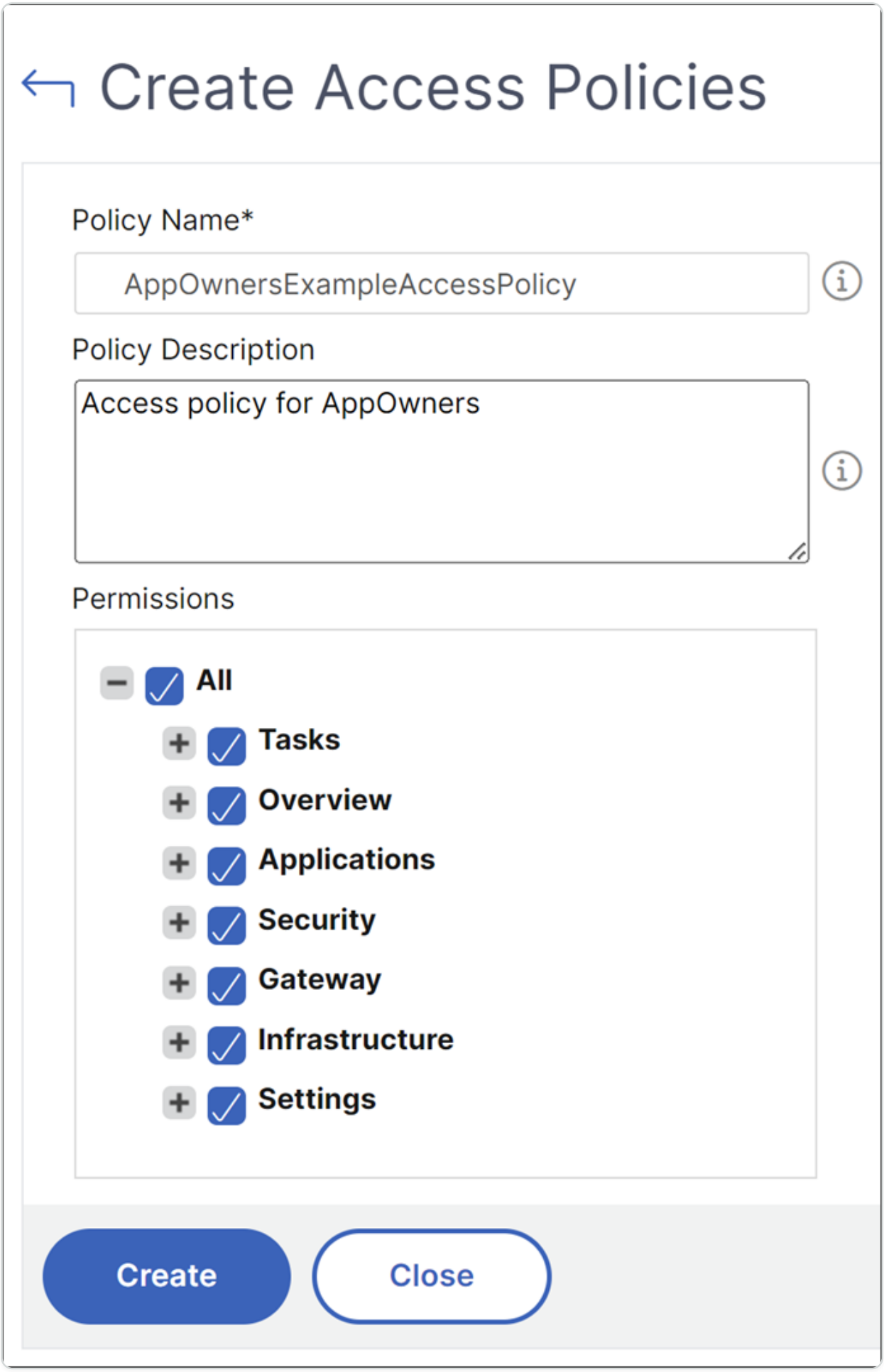
   Citrix recommends that you create an access policy to ensure that the application owners do not evade the RBAC rules set by you.

5. Type a name for the policy and a brief description. In the Permissions section, ensure that the following view-edit permissions are checked mandatorily.

   a. Applications > Dashboard
   b. Applications > Configurations
   c. Infrastructure > Instances
   d. Infrastructure > License Management
   e. Settings > Domain Names

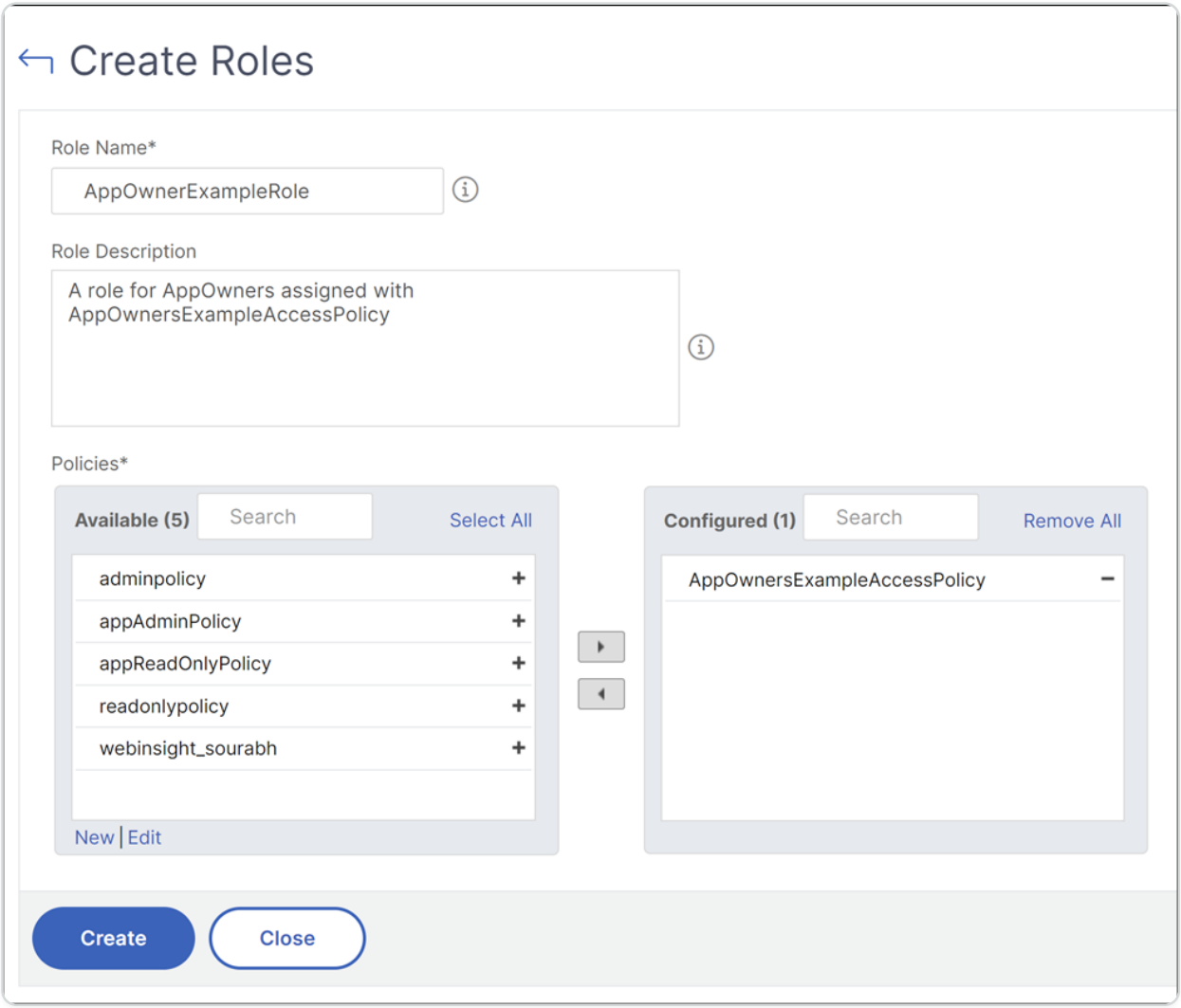
   You can provide other permissions as applicable and click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



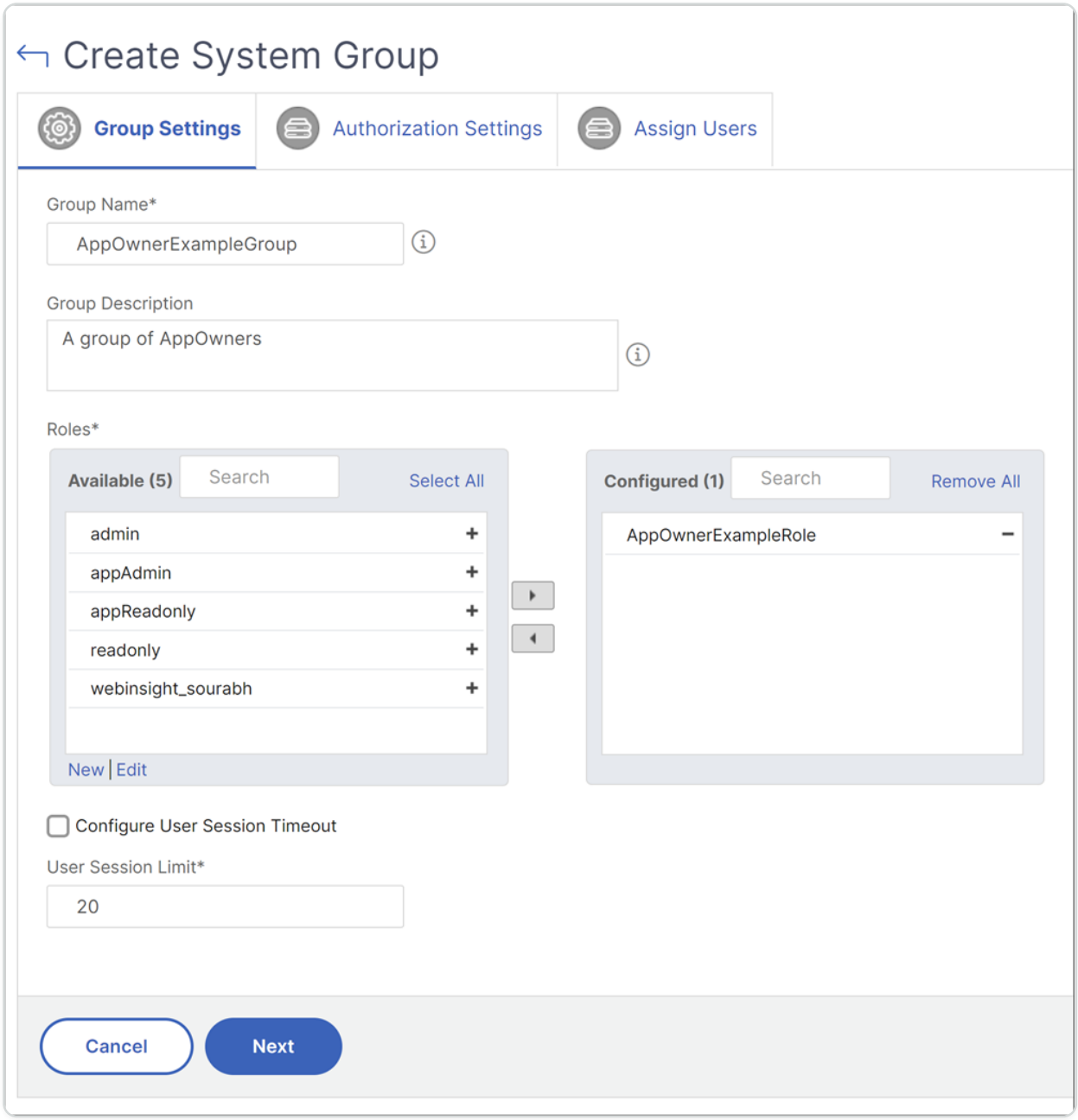
© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Navigate to **System** > **Users** > **Roles** and create a role and assign the policy created in the earlier step.
7. Type a name for the role and provide a brief description. In the Policies section, select **AppOwnerExampleAccessPolicy**.



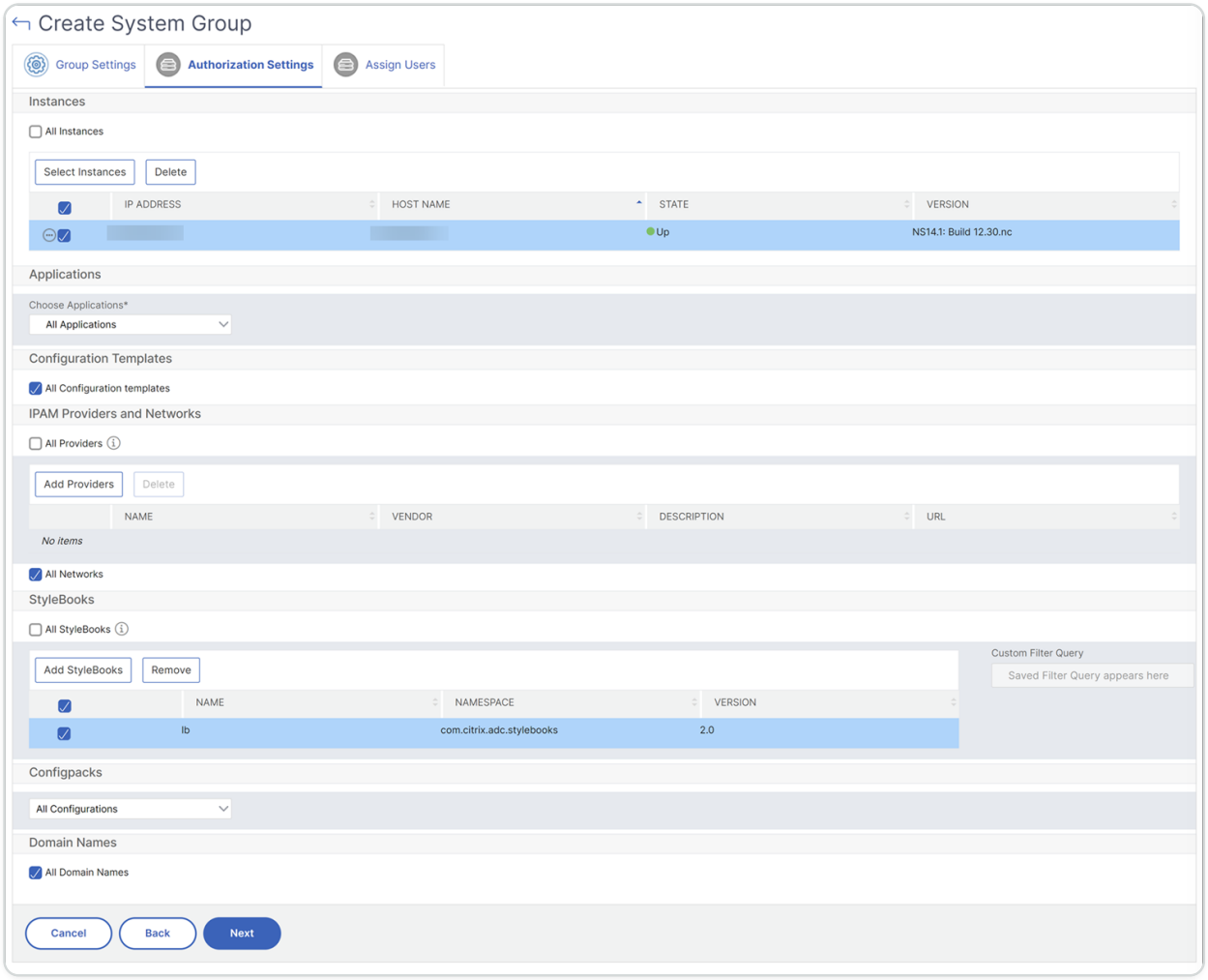
8. Navigate to **System** > **Users** > **Groups** and create a group and associate the role created in the earlier step.
9. Type a name and description, and in the Roles section, select **AppOwnerExampleRole**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



10. Click **Next**.
11. In the **Authorization Settings** tab, select the NetScaler instances that the application owner has access to and the new GSLB StyleBook.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



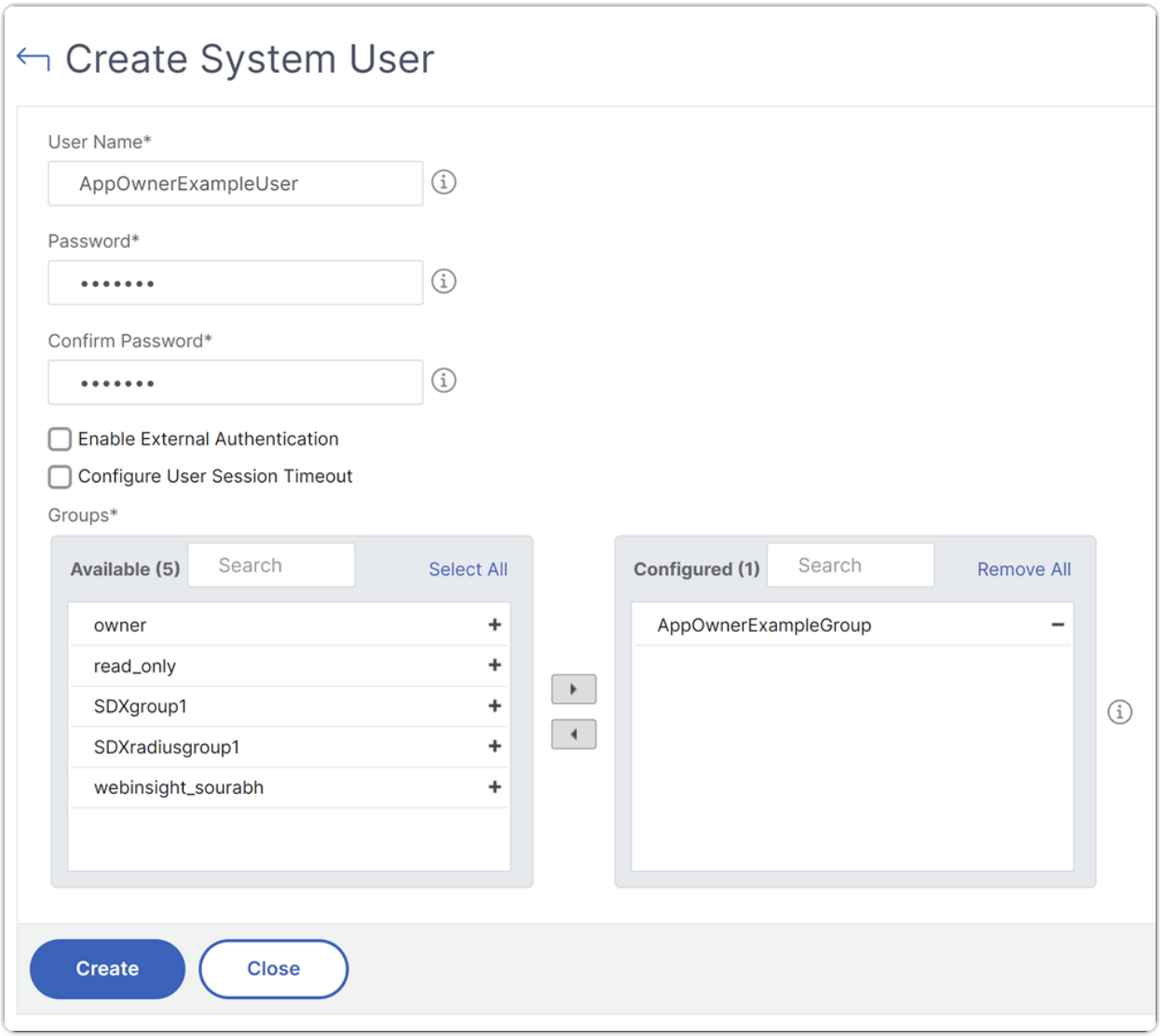
Repeat this step to create as many user groups as you need in your organization. Click **Create Group**.

12. Create a system user and assign the user to a user group. This document refers to only users created locally. You need not create users in user groups if NetScaler Console is set up for using external authentication, for example, LDAP. User mapping to groups is retrieved from the external authentication directory.

    a. Navigate to **System** > **Users** > **User**.

    b. Type a user name and password for the system user and assign the user to the group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE:

Step 12 is optional and is not required if external authentication such as LDAP is used.

NetScaler Console REST API for admin workflow

REST API to log on to NetScaler Console

```
URL: http: //<MAS_IP>/nitro/v2/config/login

HTTPMETHOD: POST



Body Payload:

{
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "login": {
    "username": "<USER_NAME>",
    "password": "<PASSWORD>",
    "session_timeout": 1800
  }
}


The response results in a session cookie header, that can be sent with the rest of the API requests below.


Set-Cookie: SESSID=##ED31F7C886E248CCDCA8F0E0AD2AA511ACCC5F46C48D6D2BCAA719A9DE62;path=/;secure;HttpOnly
```

REST API to create an access policy

```
URL: https://<MAS_IP>/nitro/v2/config/rba_policy

HTTP METHOD: POST


{
  "rba_policy": {
    "name": " AppOwnerAccessPolicy",
    "description": " ExampleCompany AppOwner Access Policy",
    "tenant_id": "7c12ec97-1472-4096-97e7-a5acb453cc5c",
    "statement": [
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      {

        "access_type": true,

        "resource_type": "application",

        "operation_name": "add",

        "dependent_resources":
"mail_profile,slack_profile,smtp_server,app_category"

      },

      {

        "access_type": true,

        "resource_type": "application",

        "operation_name": "get",

        "dependent_resources":
"download,smtp_server,ns_vserver_license,app_category,app_summary,app_heal
th_dashboard_details,haproxy_frontend,haproxy_backend,haproxy_frontend_sta
ts"

      },

      {

        "access_type": true,

        "resource_type": "si_app_unit",

        "operation_name": "get",

        "dependent_resources":
"download,smtp_server,app_summary,si_app_summary,si_device,security_app_da
shboard_details,si_geo_location,si_safety_app_firewall,si_safety_overview,
si_safety_security_check,si_safety_system_security,si_safety_signature"

      },
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      {
        "access_type": true,
        "resource_type": "stylebooks",
        "operation_name": "get",
        "dependent_resources": "download,smtp_server,ns_vserver_license"
      },
      {
        "access_type": true,
        "resource_type": "stylebooks",
        "operation_name": "add",
        "dependent_resources": "mail_profile,slack_profile,smtp_server"
      },
      {
        "access_type": true,
        "resource_type": "configpacks",
        "operation_name": "get",
        "dependent_resources":
"download,smtp_server,stylebooks,ns_vserver_license"
      },
      {
        "access_type": true,
        "resource_type": "configpacks",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "operation_name": "add",
        "dependent_resources": "mail_profile,slack_profile,smtp_server"
      },
      {
        "access_type": true,
        "resource_type": "stylebooks_system_settings",
        "operation_name": "get",
        "dependent_resources": "download,smtp_server"
      },
      {
        "access_type": true,
        "resource_type": "stylebooks_system_settings",
        "operation_name": "add",
        "dependent_resources": "mail_profile,slack_profile,smtp_server"
      },
      {
        "access_type": true,
        "resource_type": "ns_crvserver",
        "operation_name": "get",
        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,perf_cache_redirection_report,poll_ac
tivity_status,ns_emon_poll_policy,lb_export_report"
      },
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      {
        "access_type": true,
        "resource_type": "ns_crvserver",
        "operation_name": "add",
        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,poll_activity_statu
s,ns_emon_poll_policy,lb_export_report"
      },
      {
        "access_type": true,
        "resource_type": "haproxy_frontend",
        "operation_name": "get",
        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,haproxy_backend,haproxy_server"
      },
      {
        "access_type": true,
        "resource_type": "haproxy_frontend",
        "operation_name": "add",
        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server"
      },
      {
        "access_type": true,
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "resource_type": "ns_server",

        "operation_name": "get",

        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,ns_emon_poll_policy,poll_activity_sta
tus,ns_server,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_server",

        "operation_name": "add",

        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,ns_emon_poll_policy
,poll_activity_status,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_lbvserver",

        "operation_name": "get",

        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,perf_lb_vserver_report,ns_emon_poll_p
olicy,poll_activity_status,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_lbvserver",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "operation_name": "add",

        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,ns_emon_poll_policy
,poll_activity_status,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_service",

        "operation_name": "get",

        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,ns_emon_poll_policy,poll_activity_sta
tus,ns_visualizer_lb_bindings,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_service",

        "operation_name": "add",

        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,ns_emon_poll_policy
,poll_activity_status,ns_visualizer_lb_bindings,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_servicegroup",

        "operation_name": "get",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,ns_emon_poll_policy,poll_activity_sta
tus,ns_servicegroupmember_binding,ns_visualizer_lb_bindings,lb_export_repo
rt"

      },

      {

        "access_type": true,

        "resource_type": "ns_servicegroup",

        "operation_name": "add",

        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,ns_emon_poll_policy
,poll_activity_status,ns_servicegroupmember_binding,ns_visualizer_lb_bindi
ngs,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_authenticationvserver",

        "operation_name": "get",

        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,perf_authentication_report,poll_activ
ity_status,ns_emon_poll_policy,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_authenticationvserver",

        "operation_name": "add",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,poll_activity_statu
s,ns_emon_poll_policy,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "syslog_messages",

        "operation_name": "get",

        "dependent_resources": "download,smtp_server"

      },

      {

        "access_type": true,

        "resource_type": "ns_emon_poll_policy",

        "operation_name": "get",

        "dependent_resources": "download,poll_activity_status,smtp_server"

      },

      {

        "access_type": true,

        "resource_type": "ns_emon_poll_policy",

        "operation_name": "add",

        "dependent_resources":
"download,poll_activity_status,mail_profile,slack_profile,smtp_server"

      },
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      {
        "access_type": true,
        "resource_type": "ns_visualizer_gslb_bindings",
        "operation_name": "add",
        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,poll_activity_statu
s,ns_emon_poll_policy,ns_gslbvserver_domain,lb_export_report"
      },
      {
        "access_type": true,
        "resource_type": "ns_visualizer_gslb_bindings",
        "operation_name": "get",
        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,poll_activity_status,ns_emon_poll_pol
icy,ns_gslbvserver_domain,lb_export_report"
      },
      {
        "access_type": true,
        "resource_type": "ns_gslbservice",
        "operation_name": "add",
        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,poll_activity_statu
s,ns_emon_poll_policy,lb_export_report"
      },
      {
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "access_type": true,

        "resource_type": "ns_gslbservice",

        "operation_name": "get",

        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,poll_activity_status,ns_emon_poll_pol
icy,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_gslbvserver",

        "operation_name": "get",

        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,perf_global_server_load_balancing_rep
ort,poll_activity_status,ns_emon_poll_policy,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_gslbvserver",

        "operation_name": "add",

        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,poll_activity_statu
s,ns_emon_poll_policy,lb_export_report"

     },

      {

        "access_type": true,
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "resource_type": "ns_vpnvserver",

        "operation_name": "add",

        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,poll_activity_statu
s,ns_emon_poll_policy,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_vpnvserver",

        "operation_name": "get",

        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,perf_ssl_vpn_report,poll_activity_sta
tus,ns_emon_poll_policy,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_csvserver",

        "operation_name": "get",

        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,perf_content_switching_report,ns_emon
_poll_policy,poll_activity_status,ns_visualizer_cs_bindings,lb_export_repo
rt"

      },

      {

        "access_type": true,
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "resource_type": "ns_csvserver",

        "operation_name": "add",

        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,ns_emon_poll_policy
,poll_activity_status,ns_visualizer_cs_bindings,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "dns_domain_entry",

        "operation_name": "get",

        "dependent_resources": ""

      },

      {

        "access_type": true,

        "resource_type": "dns_domain_entry",

        "operation_name": "add",

        "dependent_resources": ""

      },

      {

        "access_type": true,

        "resource_type": "devicewise_detail_summary",

        "operation_name": "get",

        "dependent_resources":
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"download,mps_user_heatmap,ns_event,mps_agent,active_event,smtp_server,mps
_datacenter,event_severity_report,event_device_report,ns_conf,device_event
_summary"

      },

      {

        "access_type": true,

        "resource_type": "devicewise_detail_summary",

        "operation_name": "add",

        "dependent_resources": "mail_profile,slack_profile,smtp_server"

      },

      {

        "access_type": true,

        "resource_type": "cbwanopt",

        "operation_name": "get",

        "dependent_resources":
"download,device_backup,traceroute,inventory,inventory_status,ping,mps_dat
acenter,cbwanopt_device_profile,sdwanvw_device_profile,sdwanvw_snmp_config
,sdwanvw_appflowconfig,smtp_server,cbwanopt_snmp_config,cbwanopt_appflowco
nfig,sdwanvw,tag"

      },

      {

        "access_type": true,

        "resource_type": "cbwanopt",

        "operation_name": "add",

        "dependent_resources":
"inventory,managed_device,device_backup,upload,cbwanopt_device_profile,mps
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
_datacenter,mail_profile,slack_profile,smtp_server,sdwanvw_device_profile,
sdwanvw_snmp_config,sdwanvw_appflowconfig,cbwanopt_snmp_config,cbwanopt_ap
pflowconfig,sdwanvw,tag"

      },

      {

        "access_type": true,

        "resource_type": "device_login",

        "operation_name": "get",

        "dependent_resources": ""

      },

      {

        "access_type": true,

        "resource_type": "ns",

        "operation_name": "get",

        "dependent_resources":
"download,ns_config_replicate,ns_conf,ns_ns_runningconfig,ns_ns_savedconfi
g,active_event,device_backup,traceroute,inventory,inventory_status,ping,ns
_device_profile,nssdx_device_profile,sdx_snmp_config,sdx_syslog_config,smt
p_server,ns_cluster,ns_snmp_config,ns_syslog_config,ns_l7_latency_config,i
ca_l7_latency_update,af_vserver_policy,ns_vserver_appflow_config,mps_datac
enter,ns_appflow_param_config,ns_ns_license,ns_ns_mode,ns_network_interfac
e,advanced_analytics_config,tag"

      },

      {

        "access_type": true,

        "resource_type": "ns",

        "operation_name": "add",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "dependent_resources":
"inventory,ns_l7_latency_config,ica_l7_latency_update,af_vserver_policy,ns
_config_replicate,managed_device,device_backup,upload,ns_device_profile,ns
sdx_device_profile,mps_datacenter,sdx_snmp_config,sdx_syslog_config,mail_p
rofile,slack_profile,smtp_server,ns_cluster,ns_snmp_config,ns_syslog_confi
g,ns_vserver_appflow_config,ns_appflow_param_config,advanced_analytics_con
fig,tag"

      },

      {

        "access_type": true,

        "resource_type": "haproxyhost",

        "operation_name": "get",

        "dependent_resources":
"download,traceroute,inventory,inventory_status,ping,mps_datacenter,smtp_s
erver,haproxy_device_profile,device_backup,tag"

      },

      {

        "access_type": true,

        "resource_type": "haproxyhost",

        "operation_name": "add",

        "dependent_resources":
"inventory,managed_device,mail_profile,slack_profile,smtp_server,mps_datac
enter,haproxy_device_profile,haproxy,device_backup,tag"

      },

      {

        "access_type": true,

        "resource_type": "docker_host",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "operation_name": "add",

        "dependent_resources":
"inventory,ns_snmp_config,managed_device,ns,upload,mail_profile,slack_prof
ile,smtp_server,mps_datacenter,ns_device_profile,docker_nscpx_image"

      },

      {

        "access_type": true,

        "resource_type": "docker_host",

        "operation_name": "get",

        "dependent_resources":
"download,ns_snmp_config,ns_conf,ns_ns_runningconfig,ns_ns_savedconfig,smt
p_server,mps_datacenter,ns_device_profile,traceroute,inventory,inventory_s
tatus,ping,active_event,ns_ns_license,ns_ns_mode,ns_network_interface"

      },

      {

        "access_type": true,

        "resource_type": "perf_reports",

        "operation_name": "add",

        "dependent_resources":
"mail_profile,slack_profile,smtp_server,perf_custom_dashboard"

      },

      {

        "access_type": true,

        "resource_type": "perf_reports",

        "operation_name": "get",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "dependent_resources":
"download,smtp_server,perf_report_counters,perf_res_util_report,perf_http_
req_tcp_conn_report,perf_lb_ssl_traffic_report,perf_ip_bytes_rxtx_report,p
erf_ip_pkt_rxtx_report,perf_icmp_pkt_rxtx_report,perf_icmp_bytes_rxtx_repo
rt,perf_icmpv6_pkt_rxtx_report,perf_icmpv6_bytes_rxtx_report,perf_ipv6_byt
es_rxtx_report,perf_ipv6_pkt_rxtx_report,perf_udp_bytes_rxtx_report,perf_u
dp_packets_rxtx_report,perf_cmp_bytes_rxtx_report,perf_cmp_tcp_bytes_rxtx_
report,perf_cmp_tcp_ratiosaving_report,perf_cmp_decmp_bytes_rxtx_report,pe
rf_cmp_decmp_ratiosaving_report,perf_tcp_server_conn_report,perf_tcp_surge
len_spareconn_report,perf_http_bytes_rx_report,perf_http_gets_posts_report
,perf_ssl_transactions_hits_report,perf_ssl_client_auth_report,perf_ssl_rs
a_dhkey_report,perf_ssl_frontend_ciphers_report,perf_ssl_backend_ciphers_r
eport,perf_wsdevice_cpu_utilization_report,perf_wsdevice_send_compression_
ratio_report,perf_wsdevice_connected_plugins_report,perf_wsdevice_data_red
uction_report,perf_wsdevice_link_utilization_report,perf_wsserviceclasssta
tstable_pass_through_connection_report,perf_wsserviceclassstatstable_servi
ce_class_report,perf_wsserviceclassstatstable_acceleration_report,perf_wsl
inkstatstable_throughput_report,perf_wslinkstatstable_packet_loss_report,p
erf_wsappstatstable_application_report,perf_wsqosstatstable_qos_report,per
f_ssl_cpu_keyexchange_report,perf_ssl_be_rsa_dhkey_report,perf_custom_dash
board,perf_ns_throughput_report,perf_network_interface_report"

      },

      {

        "access_type": true,

        "resource_type": "perf_threshold",

        "operation_name": "get",

        "dependent_resources":
"download,perf_reports,perf_report_counters,smtp_server,sms_server,sms_pro
file"

      },

      {

        "access_type": true,

        "resource_type": "perf_threshold",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "operation_name": "add",

        "dependent_resources":
"mail_profile,slack_profile,smtp_server,sms_server,sms_profile"

      },

      {

        "access_type": true,

        "resource_type": "perf_poll_config",

        "operation_name": "add",

        "dependent_resources": "mail_profile,slack_profile,smtp_server"

      },

      {

        "access_type": true,

        "resource_type": "perf_poll_config",

        "operation_name": "get",

        "dependent_resources": "smtp_server,download"

      },

      {

        "access_type": true,

        "resource_type": "license_server_info",

        "operation_name": "get",

        "dependent_resources":
"sms_server,license_proxy_server,jazz_license,download,sms_profile,smtp_se
rver,user_managed_tp_vserver,managed_vserver,user_managed_vserver,haproxy_
frontend,haproxy_backend,license_file,device_license_info,license_info,ns_
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
authenticationvserver,ns_gslbvserver,ns_vpnvserver,ns_csvserver,ns_crvserv
er,ns_lbvserver,autoselection_preference,license_threshold,license_expiry_
info"

      },

      {

        "access_type": true,

        "resource_type": "license_server_info",

        "operation_name": "add",

        "dependent_resources":
"sms_server,license_proxy_server,jazz_license,sms_profile,mail_profile,sla
ck_profile,smtp_server,user_managed_tp_vserver,managed_vserver,upload,lice
nse_file,license_info,license_threshold,mas_license,user_managed_vserver,a
utoselection_preference,license_expiry_info"

      }

    ],

    "ui": [

      {

        "access_type": true,

        "name": "ApplicationsDashboard",

        "display_name": "Dashboard"

      },

      {

        "access_type": true,

        "name": "SecurityDashboard",

        "display_name": "App Security Dashboard"
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      },
      {
        "access_type": true,
        "name": "Stylebooks",
        "display_name": "StyleBooks"
      },
      {
        "access_type": true,
        "name": "Stylebooks",
        "display_name": "Configpacks"
      },
      {
        "access_type": true,
        "name": "StylebooksSettings",
        "display_name": "Settings"
      },
      {
        "access_type": true,
        "name": "CacheRedirection",
        "display_name": "Cache Redirection"
      },
      {
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "access_type": true,
        "name": "Servers",
        "display_name": "Servers"
      },
      {
        "access_type": true,
        "name": "VirtualServers",
        "display_name": "Virtual Servers"
      },
      {
        "access_type": true,
        "name": "Services",
        "display_name": "Services"
      },
      {
        "access_type": true,
        "name": "ServiceGroups",
        "display_name": "Service Groups"
      },
      {
        "access_type": true,
       "name": "Authentication",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "display_name": "Authentication"
      },
      {
        "access_type": true,
        "name": "MonitoringAuditing",
        "display_name": "Auditing"
      },
      {
        "access_type": true,
        "name": "MonitoringSettings",
        "display_name": "Settings"
      },
      {
        "access_type": true,
        "name": "GSLBDomains",
        "display_name": "Domains"
      },
      {
        "access_type": true,
        "name": "GSLBServices",
        "display_name": "Services"
      },
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    {
      "access_type": true,
      "name": "GSLBVirtualServer",
      "display_name": "Virtual Server"
    },
    {
      "access_type": true,
      "name": "NetScalerGateway",
      "display_name": "NetScaler Gateway"
    },
    {
      "access_type": true,
      "name": "ContentSwitching",
      "display_name": "Content Switching"
    },
    {
      "access_type": true,
      "name": "DNSDomainNames",
      "display_name": "DNS Domain Names"
    },
    {
      "access_type": true,
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "name": "NetworkDashboard",
        "display_name": "Instances Dashboard"
      },
      {
        "access_type": true,
        "name": "NetScalerSDWANWOInstances",
        "display_name": "NetScaler SD-WAN"
      },
      {
        "access_type": true,
        "name": "InstanceOperations",
        "display_name": "Instance Operations"
      },
      {
        "access_type": true,
        "name": "NetScalerInstances",
        "display_name": "NetScaler ADC"
      },
      {
        "access_type": true,
        "name": "NetScalerCPXDockerHost",
        "display_name": "Docker Hosts"
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    },
    {
      "access_type": true,
      "name": "Reports",
      "display_name": "Reports"
    },
    {
      "access_type": true,
      "name": "Thresholds",
      "display_name": "Thresholds"
    },
    {
      "access_type": true,
      "name": "ReportingSettings",
      "display_name": "Settings"
    },
    {
      "access_type": true,
      "name": "Licenses",
      "display_name": "License Management"
    }
  ]
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  }

}
```

REST API to create an access role

```
URL: https://<MAS_IP>/nitro/v2/config/rba_role

HTTPMETHOD: POST



Payload:

{

  "rba_role": {

    "name": "AppOwnerRole",

    "description": "ExampleCompany App Owner Role",

    "policies": [

      "AppOwnerAccessPolicy"

    ]

  }
```

REST API to upload new GSLB StyleBook

```
URL: https://<MAS_IP>/stylebook/nitro/v2/config/stylebooks

HTTPMETHOD: POST



Payload:

{
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "stylebook": {
      "file_name": "my-own-gslb.yaml",
      "source": "bmFtZTogZ3NsYi1kbnMtZG9tYW...aXRvcm5hbWU=",
      "encoding": "base64"
    }
  }
```

NOTE:

The name of the StyleBook might change on your system.

REST API to create groups and assign selected instances and StyleBooks

```
URL: https://<MAS_IP>/nitro/v2/config/mpsgroup

HTTPMETHOD: POST



Payload:

{
  "mpsgroup": {
    "id": "",
    "name": "AppOwnerGroup1",
    "description": "ExampleCompany App Owner Group",
    "roles": [
      "AppOwnerRole"
    ],
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"enable_session_timeout": false,
"assign_all_devices": false,
"ass ign_all_apps": false,
"application_names_with_regex": [


],
"standalone_instances_id": [
  "72c178da-47df-4426-9acc-cd6316f92506",
  "c948061e-6240-4062-931c-f6988ef36e3b"
],
"application_list": [


],
"permission": "none",
"application_names": [


],
"authscope_props": [
  {
    "propname": "configuration_template_id",
    "propvalues": [
      "NONE"
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        ]
      },
      {
        "propname": "dns_domain_entry_id",
        "propvalues": [
          "cf6631e5-2f56-4bb1-b0a5-90fabfc0e3e2",
          "b268905c-522d-47e3-a2ca-3f8d8a754373"
        ]
      },
      {
        "propname": "stylebook_id",
        "propvalues": [
          "gslbbb963abe85936913035e1d4dd14b56f7",
          "moni72fad4494466d102b19c18ac329fa9f3"
        ]
      }
    ],
    "tenant_id": "6d024111-6636-4571-a250-d47b31aba7a8"
  }
}
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

In order to obtain the IDs for DNS domain names, and GSLB StyleBooks to be used in the API payload above, you can use regular NetScaler Console APIs for querying IDs corresponding to entity names. For example, to obtain the ID for a DNS domain called "app1.acme.com", you can use the following NetScaler Console REST API.

```
URL: https://<MAS_IP>/nitro/v2/config/dns_domain_entry?filter=name:
app1.acme.com

HTTPMETHOD: GET



The ID of this domain can be extracted from the following response.

{

  "errorcode": 0,

  "message": "Done",

  "operation": "get",

  "resourceType": "dns_domain_entry",

  "username": "nsroot",

  "tenant_name": "Owner",

  "tenant_id": "568d8e12-1d88-42b2-8943-cbaa04826fd1",

  "resourceName": "",

  "dns_domain_entry": [

    {

      "tenant_id": "568d8e12-1d88-42b2-8943-cbaa04826fd1",

      "name": "app1.acme.com",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      "id": "3e3d85ea-1c21-49b2-97f4-60fccdbae2e0",

      "description": "app1 domain name"

    }

  ]

}
```

Similarly, to obtain the StyleBook ID for a StyleBook whose namespace is com.citrix.adc.stylebook, version: 1.0, name: `my-own-gslb`, you can use the following API.

```
URL: https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks?filter=name:my-own-gslb,namespace:com.citrix.adc.stylebooks,version:1.0

HTTPMETHOD: GET
```

The response contains the StyleBook details, including its ID attribute.

```
{

  "stylebooks": [

    {

      "author": null,

      "builtin": "false",

      "builtins": "{"netscaler.nitro.config": "10.5"}",

      "deprecate": "false",

      "description": " This StyleBook is used to configure one or a number of NetScalers in different sites into a GSLB setup. It is assumed that the SNIP IP on each NetScaler to be used by this StyleBook as the Site IP is already configured on the appliance.",

      "display_name": "HTTP/SSL LoadBalancing StyleBook",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "filename": "my-own-gslb.yaml",
    "hide": null,
    "id": "gslb5a748d8b7684846cf6c409ad7dea8ccf",
    "imported_by": "",
    "imported_datetime": "2018-05-25 17:20:32.848902",
    "name": "my-own-gslb",
    "namespace": "com.citrix.adc.stylebooks",
    "pkg_id": "gslb5a748d8b7684846cf6c409ad7dea8ccf",
    "primary_keys": "["name"]",
    "private": "false",
    "recompile": "false",
    "schema_version": "1.0",
    "source": "LS0tIApuYW1lOiBsYgpuYW1lc…",
    "system": null,
    "tags": "",
    "tenant_id": null,
    "user_sb": "false",
    "version": "1.0"
  },
  {
    …
  }
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  ]
}
```

NOTE:

The above API returns a list of StyleBooks that match the filter. Ensure that you select the correct StyleBook from the response to retrieve the ID.

REST API to create system user

NOTE:

This step is optional.

```
URL: https://<MAS_IP>/nitro/v2/config/mpsuser

HTTPMETHOD: POST



Payload:

{

  "mpsuser": {

    "name": "John",

    "password": "welcome",

    "external_authentication": false,

    "enable_session_timeout": false,

    "groups": [

      "AppOwnerGroup1"

    ]
```

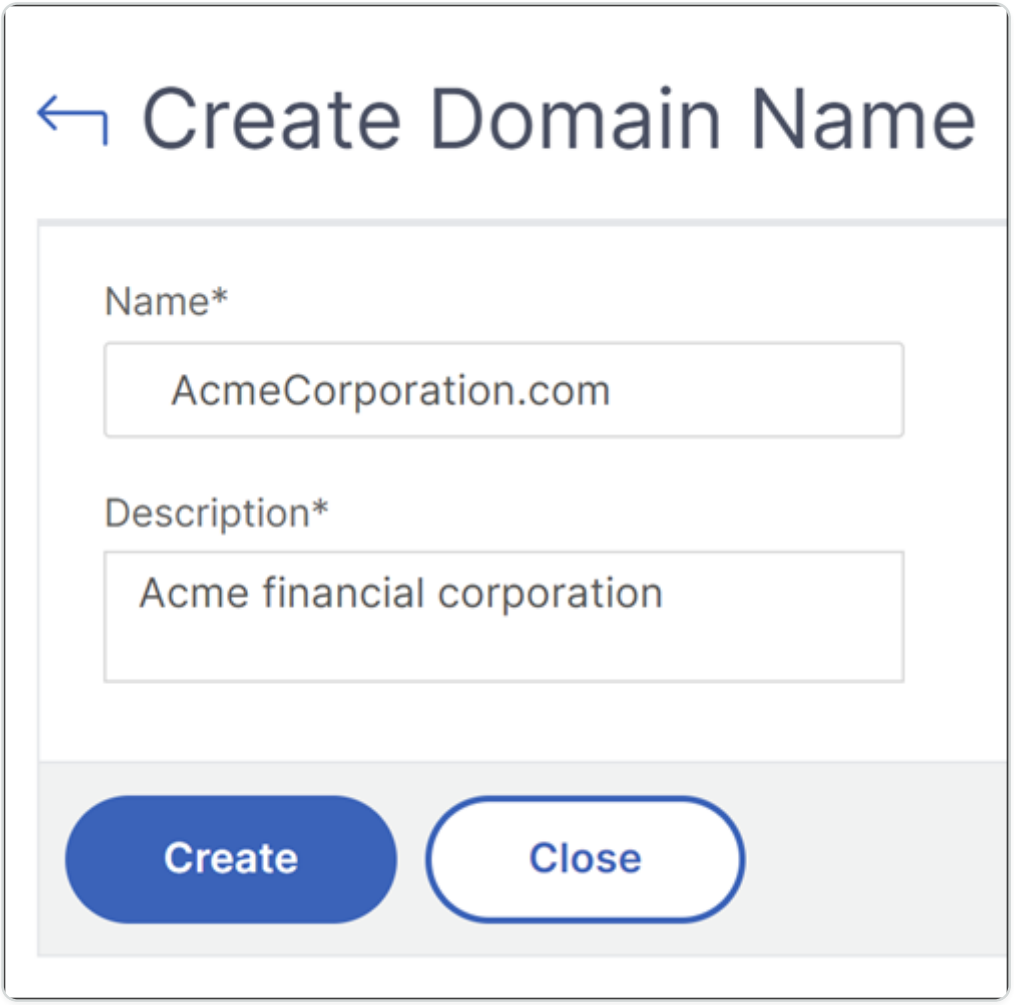
© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    }
}
```

Workflow for the application owners

Your users must log on as application users using their credentials. The users must follow this task to create their own DNS domain names and use the new GSLB StyleBook.

1. In NetScaler Console, navigate to **Settings > Domain Names**.
2. Click **Add** to create a new DNS domain. Create the DNS domains in NetScaler Console.



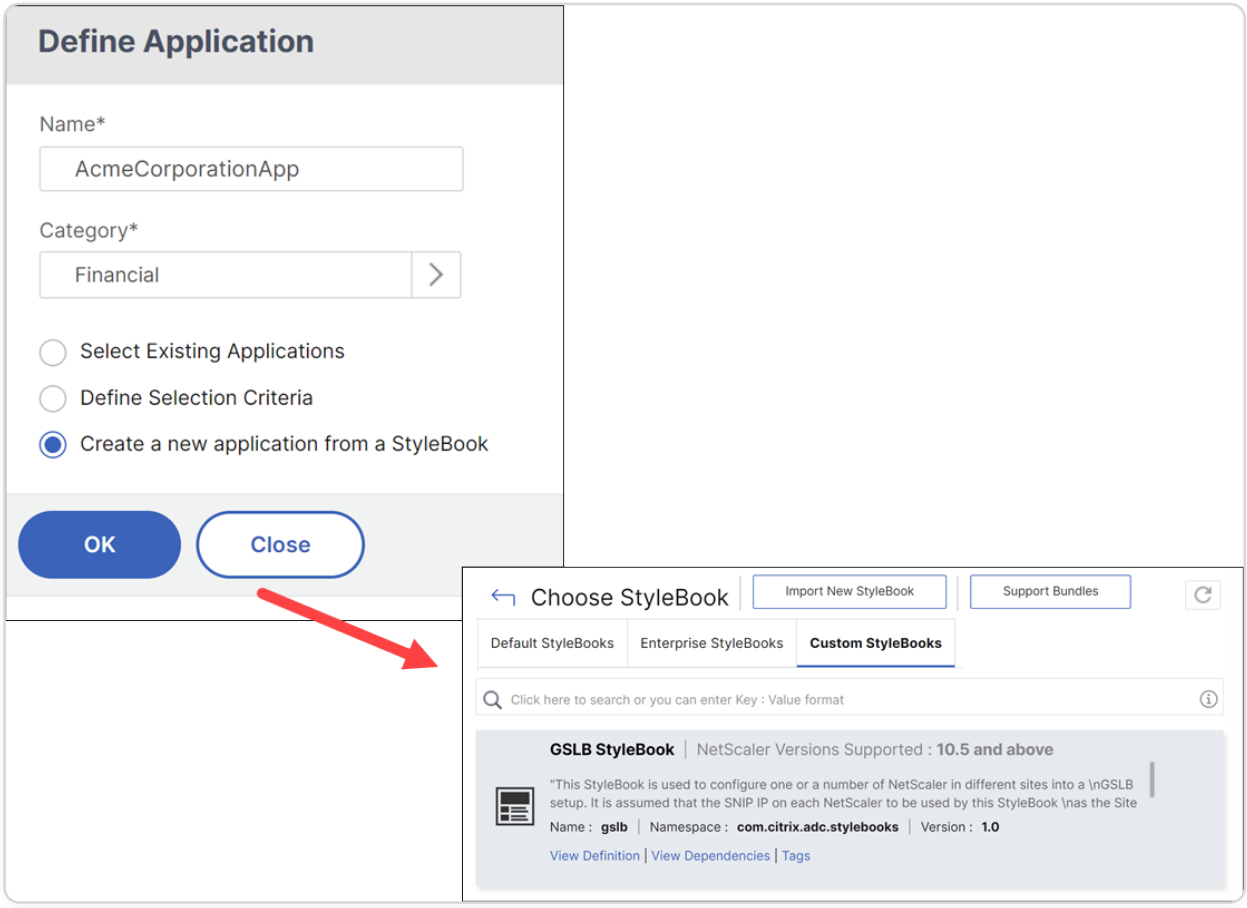
NOTE:

As an admin, you can also create these domain names and assign them to the user groups.

3. Navigate to **Applications** > **Dashboard** and click **Define Custom App**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Type a name for the application and select a category. Select **Create a new application from a StyleBook** and click **OK**. Select **My own GSLB StyleBook** to deploy the configuration on the selected instances.



5. Type the values required for all parameters in the StyleBook.

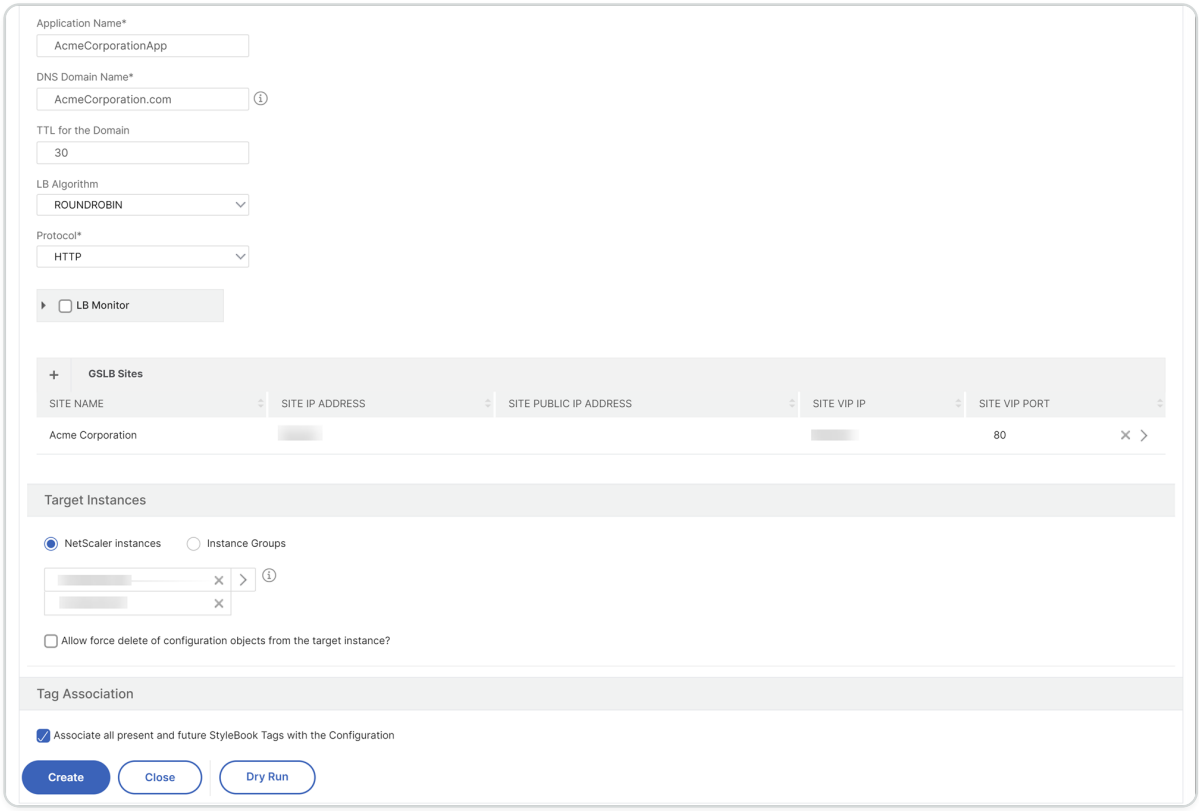
   a. Select the domain name from the list.

   b. Add the GSLB sites of your application as applicable.

   c. Select the target NetScaler instances in all the GSLB sites.

   d. Click **Create** to create a GSLB configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE:

The StyleBook parameter "DNS Domain Name" displays only the list of DNS domains that belong to the user in NetScaler Console.

NetScaler Console REST API for app owner workflow

REST API to log on to NetScaler Console

```
URL: http: //<MAS_IP>/nitro/v2/config/login

HTTPMETHOD: POST



Payload:

{

  "login": {

    "username": "<USER_NAME>",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "password": "<PASSWORD>",
    "session_timeout": 1800
  }
}
```

REST API to create DNS domain names

```
URL: https://<MAS_IP>/nitro/v2/config/dns_domain_entry

HTTP METHOD: POST

PAYLOAD: {"dns_domain_entry":{"name":"app1.acme.com","description":"app1
acme domain"

}

}
```

REST API to create applications using StyleBook

```
URL: https://<MAS_IP>/nitro/v2/config/application

HTTPMETHOD: POST



Payload:

{
  "params": {
    "action": "app_discovery"
  },
  "application": {
    "id": "",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "name": "app1",

    "app_c ategory": "ITOps",

    "stylebook_params": "{"name":"my-own-
gslb","namespace":"com.citrix.adc.stylebooks","version":"1.0","configpack_
payload":{"parameters":{"name":"app1","domain-
name":"app1.acme.com",]"ttl":"30","algorithm":"ROUNDROBIN","protocol":"HTT
P","sites":[{"name":"site1","ipaddress":"6.5.6.77","virtual-
ip":"88.6.5.44","virtual-port":"80"}]},"targets":
[ {"id":"72c178da-47df-4426-9acc-cd6316f92506"}, {"id":"0e4d0789-
bffe-4266-ba1c-09adfc61db4e"}, {"id":"b5af4455-3f06-4f56-
b0cb-3d9f868c1f94"}]}}"

  }

}
```

In the above payload:

- The "stylebook_params" contains the name, namespaces and version of the StyleBook to use.
- The "configpack_payload" contains the filled parameters of the StyleBook as shown in the equivalent GUI form above. NetScaler Console ensures that only DNS domain names that the user has access to, can be used as values for the parameter "domain-name".
- The "targets" contain the list of NetScaler IDs on which the GSLB configuration will be deployed (the NetScaler instances on the GSLB sites).

To obtain the NetScaler ID given a NetScaler's management IP address, you can use the following NetScaler Console API:

```
URL: https://<MAS_IP>/nitro/v2/config/ns?filter=ip_address:
192.168.153.162

HTTPMETHOD: GET
```

The response payload contains information about this NetScaler®, including its ID:

```
{

  "errorcode": 0,
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"message": "Done",
…..."tenant_id": "ec0eb868-0d6b-4729-bfbd-3005dd2694c1",
"resourceName": "",
"ns": [
  {
    "manufacturedate": "9/30/2009",
    "is_grace": "false",
    "hostname": "youcef-ns",
    "std_bw_config": "0",
    "gateway_deployment": "false",
    "gateway_ipv6": "",
    "ha_master_state": "Primary",
    "instance_available": "0",
    "device_finger_print": "",
    "instance_state": "Down",
    "reason": "Device not reachable",
    "name": "",
    "ent_bw_available": "0",
    "description": "",
    "id": "da9ffff2-c100-45f1-a913-c542718338b2",
    "mgmt_ip_address": "192.168.153.162",
    ….
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    }
  ]
}
```

Build your StyleBook

The full content of the file "my-own-gslb.yaml" StyleBook is shown below: You can use this custom StyleBook the way it is or customize it to your needs to generate the required GSLB configuration. The important parameter in this StyleBook called "domain-name" must be present in any StyleBook to make use of the DNS names functionality.

```
name: my-own-gslb

namespace: com.citrix.adc.stylebooks

version: "1.0"

display-name: My own GSLB StyleBook

description: This StyleBook is used to configure one or a number of
NetScalers in different sites into a GSLB setup. It is assumed that the
SNIP IP on each NetScaler to be used by this StyleBook as the Site IP is
already configured on the appliance.

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    version: "10.5"

    prefix: ns

  -

    namespace: com.citrix.adc.commontypes
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    version: "1.0"
    prefix: cmtypes
parameters:
  -
    name: name
    label: Application Name
    type: string
    required: true
    key: true


  -
    name: domain-name
    label: DNS Domain Name
    description: GSLB DNS Domain Name
    type: string
    required: true
    allowed-dynamic-values:
      source: local
      resource-type: dns_domain_entry


  -
    name: ttl
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    label: TTL for the Domain
    description: Time-To-Live value (number of seconds) for the Domain
    type: number
    default: 30


  -
    name: algorithm
    label: LB Algorithm
    description: Global Load Balancing Algorithm
    type: string
    default: ROUNDROBIN
    allowed-values:
      - ROUNDROBIN
      - STATICPROXIMITY
      - SOURCEIPHASH


  -
    name: protocol
    label: Protocol
    description: The protocol of the GSLB VIP
    type: string
    default: HTTP
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    allowed-values:
      - HTTP
      - FTP
      - TCP
      - UDP
      - SSL
      - SSL_BRIDGE
      - SSL_TCP
      - NNTP
      - ANY
      - SIP_UDP
      - SIP_TCP
      - SIP_SSL
      - RADIUS
      - RDP
      - RTSP
      - MYSQL
      - MSSQL
      - ORACLE


  -
    name: monitor
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    label: LB Monitor

    description: Monitor to be bound to the GSLB service

    type: cmtypes::monitor



  -

    name: sites

    label: GSLB Sites

    description: Provide information about the GSLB Sites

    type: object[]

    required: true

    parameters:

      -

        name: name

        label: Site Name

        type: string

        required: true

      -

        name: ipaddress

        label: Site IP Address

        description: The IP Address of this Site. Use a SNIP IP address on
the site's appliance.

        type: ipaddress
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        required: true

      -

        name: public-ipaddress

        label: Site Public IP Address

        description: The Public IP Address of this Site. It NATs to the
Site's IP address

        type: ipaddress

      -

        name: virtual-ip

        label: Site VIP IP

        description: The IP Address for the GSLB Service on this site (The
VIP on this Site)

        type: ipaddress

        required: true

      -

        name: virtual-port

        label: Site VIP Port

        description: The port number for the GSLB Service (VIP) on this
site

        type: tcp-port

        default: 80



components:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  -
    name: enable-gslb-comp
    type: ns::nsfeature
    description: Enables the GSLB feature
    meta-properties:
      action: enable
    properties:
      feature: ["GSLB", "LB"]
  -
    name: gslb-monitor-comp
    type: cmtypes::monitor
    condition: $parameters.monitor
    properties:
      monitorname: $parameters.name + "-" +
$parameters.monitor.monitorname + "-gslbmon"
      type: $parameters.monitor.type
      destip?: $parameters.monitor.destip
      destport?: $parameters.monitor.destport
      httprequest?: $parameters.monitor.httprequest
      send?: $parameters.monitor.send
      customheaders?: $parameters.monitor.customheaders
      respcodes?: $parameters.monitor.respcodes
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      recv?: $parameters.monitor.recv
      lrtm?: $parameters.monitor.lrtm
      secure?: $parameters.monitor.secure
      interval?: $parameters.monitor.interval
      interval_units?: $parameters.monitor.interval_units
      resptimeout?: $parameters.monitor.resptimeout
      retries?: $parameters.monitor.retries
      downtime?: $parameters.monitor.downtime
  -
    name: gslb-vserver-comp
    type: ns::gslbvserver
    description: Creates a GSLB VServer config object
    properties:
      name: $parameters.name + "-gslbvserver"
      servicetype: $parameters.protocol
      lbmethod: $parameters.algorithm
    components:
      -
        name: gslb-domain-comp
        type: ns::gslbvserver_domain_binding
        properties:
          name: $parent.properties.name
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
          domainname: $parameters.domain-name

          ttl: $parameters.ttl

  -

    name: gslb-site-comp

    type: ns::gslbsite

    description: Creates a GSLB Site config object

    repeat: $parameters.sites

    repeat-item: site

    properties:

      sitename: $parameters.name + "-" + $site.name + "-gslbsite"

      siteipaddress: $site.ipaddress

      publicip?: $site.public-ipaddress

    components:

      -

        name: gslb-service-comp

        type: ns::gslbservice

        description: Creates a GSLB Service

        properties:

          servicename: $parameters.name + "-" + $site.name + "-
gslbservice"

          ip: $site.virtual-ip

          servicetype: $parameters.protocol
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
          port: $site.virtual-port

          sitename: $parent.properties.sitename

        components:

          -

            name: gslb-vserver-service-binding-comp

            type: ns::gslbvserver_gslbservice_binding

            description: Creates a Binding between the GSLB vserver and
the GSLB Service

            properties:

              name: $components.gslb-vserver-comp.properties.name

              servicename: $parent.properties.servicename

          -

            name: gslb-service-monitor-binding-comp

            type: ns::gslbservice_lbmonitor_binding

            description: Creates a Binding between the GSLB service and
the GSLB monitor

            condition: $parameters.monitor

            properties:

              servicename: $parent.properties.servicename

              monitor_name: $components.gslb-monitor-
comp.properties.monitorname
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Allow special characters with their literal form in StyleBook

In StyleBook definition, you can use verbatim strings when special characters in a string have to take their literal form. These strings can contain escape characters, backslash, quotes, parentheses, whitespaces, brackets, and so on.

In StyleBooks, you can include NetScaler Policy Expressions in their literal form using verbatim strings. The Policy Expressions typically contain special characters. Without verbatim strings, you have to escape special characters by breaking strings into substrings.

To create a verbatim string, encapsulate a string between special characters as follows:

`~{string}~`

You can use verbatim strings in the StyleBook expressions.

NOTE

Do not use the sequence of characters }~ in an input string because this sequence indicates the end of a verbatim string.

Example:

```
---

name: test-deny-url

namespace: citrix.adc.stylebooks

version: "6.2"

display-name: StyleBook for creating an AppFw profile

description: This Stylebook configures an AppFw config.

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    prefix: ns

    version: "13.0"

parameters:

  -

    name: name

    type: string

    required: true

substitutions:

 default-deny-urls-regex:

     "Command_injection_attack": str("([ /=]|\\t|\\n)(ls|cat)([ ;'" + "\\
\"&].*)?$")

     "Command_injection_attack2": ~{([ /=]|\t|\n)(ls|rm|cat)([ ;'\"&].*)?
$}~

components:

  -

    name: appfw-profile-comp

    type: ns::appfwprofile

    properties:

      name: $parameters.name

      type: ["XML"]

    components:

          -

            name: appfw-profile-denyurl-default-binding-subcomp-all
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            type: ns::appfwprofile_denyurl_binding

            properties:

                name: $parent.properties.name

                denyurl?: $substitutions.default-deny-urls-
regex["Command_injection_attack"]

                state?: "ENABLED"

          -

            name: appfw-profile-denyurl-default-binding-subcomp-all2

            type: ns::appfwprofile_denyurl_binding

            properties:

                name: $parent.properties.name

                denyurl?: $substitutions.default-deny-urls-
regex["Command_injection_attack2"]

                state?: "ENABLED"
```

In this example, the `default-deny-urls-regex` substitutions have a verbatim expression.

- `"Command_injection_attack": str("([ /=]|\\t|\\n)(ls|cat)([ ;'" + "\\\"&].*)?$")`: StyleBook processes it as a regular expression.
- `"Command_injection_attack2": ~{([ /=]|\t|\n)(ls|rm|cat)([ ;'\"&].*)?$}~`: StyleBook processes it as a verbatim expression. The special characters in this string take the literal form.

Concatenate multiple verbatim strings

You can concatenate verbatim strings with the regular strings or strings with interpolations. When you do so, the StyleBook skips the interpretation only for the verbatim strings. Use the plus (+) operator between the strings to concatenate.

Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
value: "~{\"id\": \"}~ + %{$atom.key}% + ~{\", \"value\": \"}~ + %
{$atom.value}% + ~{\"}~"
```

In this example, `%{$atom.key}%` and `%{$atom.value}%` are interpreted. And, the interpretation is skipped for the rest.

Manage data sources

Defining a data source in NetScaler Console helps you to use data from external sources as an input while creating or updating StyleBook configurations. Otherwise, you have to explicitly supply each input required by the StyleBook. In NetScaler Console, you can use any managed NetScaler instance as a data source for the input to a StyleBook configuration. You can also define custom data sources which can serve as input when creating or updating configurations.

Collections: Like how a database can have multiple tables, a data source can contain multiple collections. Each collection has a name and contains a list of similar tuples, where each tuple is a set of key-value pairs. For example, a collection can be made up of tuples where each tuple has (`<name>: <value>, <virtualip>:<value>`).

Data source type: A data source type distinguishes the type of source from which the data is retrieved. NetScaler Console supports two data source types.

- **managed-adc** - It is a built-in data source. And, it is used for retrieving data from any existing NetScaler managed by NetScaler Console. For more information, see Use a NetScaler instance as the data source.

  You can also use the target NetScaler instance as a data source. For more information, see Use target NetScaler instances as data sources.

- **Custom data source type** - You can define custom data source types where data is locally populated on NetScaler® Console.

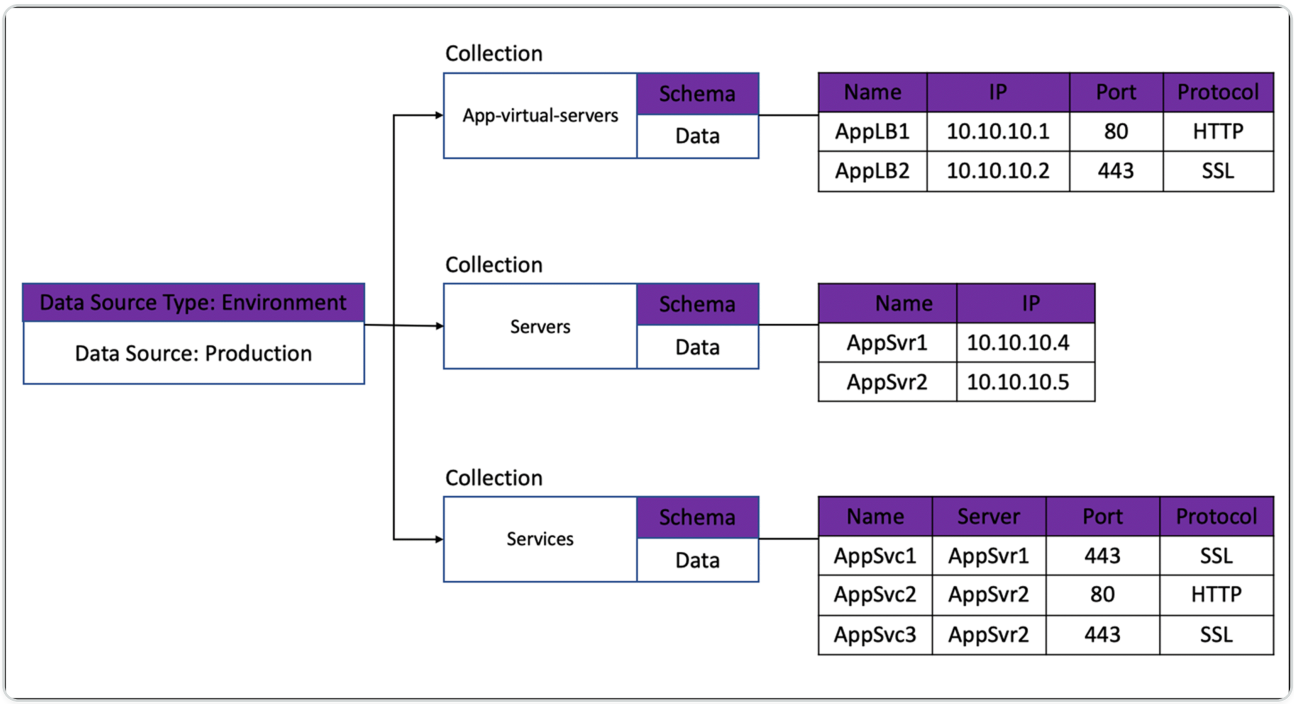
  Consider a data source type `Environment`. This data source type has two data sources `Production` and `Staging`. While creating a StyleBook configuration, the StyleBook user can select any data source of type `Environment`. Depending on the selection the data values from either `Production` or `Staging` are used as input to the StyleBook.

  For more information, see Use custom data sources

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Collection Schema: It describes what type of data that can be stored in a collection tuple. The collection schema describes the name of each key in the tuple and its expected type. In a database analogy, a collection schema is similar to a database schema for a table where each column has a well-defined name and supporting type.

The following diagram is a general representation of the various components of data sources and how they relate to each other:



Use a NetScaler instance as the data source

You can use the managed NetScaler instances as data sources. The `managed-adc` is a built-in data source type that can be readily used as the data sources in NetScaler Console. Each managed NetScaler instance in NetScaler Console is a data source by default. You can start using these data sources in your StyleBooks if you need data from an existing NetScaler managed by NetScaler Console while creating config packs.

In the StyleBook definition, specify the `datum` built-in type parameter. You can use the data source types in your StyleBook. The StyleBook users can select a data source that can be used to retrieve data from that source.

Using the built-in data source without collection

```
parameters:

  - name: selected-adc
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    label: Select an existing NetScaler

    type: datum

    required: true

    data-source:

      type: managed-adc
```

In the example, the `datum` parameter is used to select any NetScaler instance managed by NetScaler Console. The `managed-adc` built-in data source allows you to retrieve data from any NetScaler instance managed by NetScaler Console.

In your StyleBook, you can access any configuration from the selected NetScaler instance. And, you can use that configuration while creating or updating configurations on the same NetScaler or a different NetScaler instance; it depends on the selected target NetScaler instance.

Access the collection from a data source:

In the selected NetScaler instance, to access a collection, use the following expression:

```
$parameters.selected-adc.collections.<collection-name>
```

Example:

```
$parameters.selected-adc.collections.lbvserver
```

This expression returns the list of `lbvserver` entities on the selected NetScaler instance. For example, you can iterate over this list to select a specific `lbvserver` that meets a certain condition.

Example StyleBook without collection

```
name: add-vservers-from-managed-adc-instances

namespace: com.citrix.adc.stylebooks

version: "1.0"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
schema-version: "1.0"


import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"


parameters:
    -
      name: selected-adc
      label: Select a NetScaler instance
      type: datum
      required: true
      data-source:
        type: "managed-adc"


components:
  -
    name: sslvserver-comp
    type: ns::sslvserver
    repeat: $parameters.selected-adc.collections.lbvserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    repeat-item: lbvs

    repeat-condition: $lbvs.attributes.servicetype == "SSL"

    properties:

      name: $lbvs.attributes.name

      ssl2: DISABLED

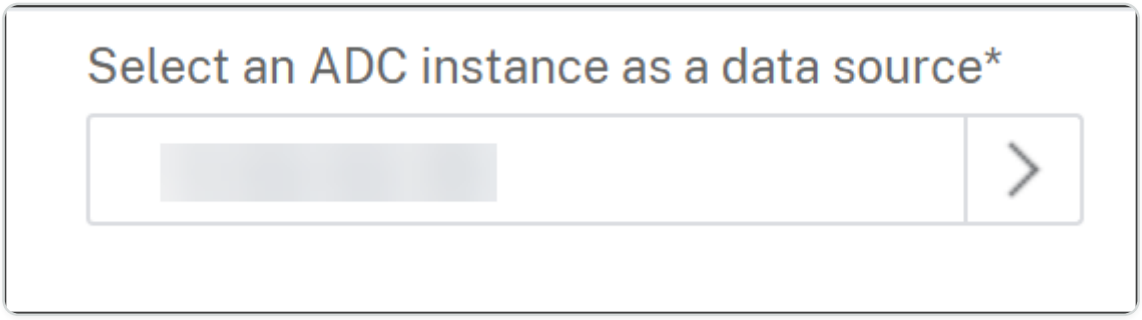
      ssl3: DISABLED

      tls1: DISABLED

      tls11: ENABLED

      tls12: ENABLED
```

The configuration pack GUI displays the managed NetScaler instances by NetScaler Console and StyleBook users can select any NetScaler when creating or updating the configuration pack.



This StyleBook uses the selected NetScaler and iterates over all the `lbvserver` entities. It selects the SSL virtual servers and sets the allowed SSL protocol versions on each virtual server.

The following expression allows you to iterate through the list of `lbvserver` entities in the NetScaler instance.

```
repeat: $parameters.selected-adc.collections.lbvserver
```

- `collections`: Refers to all entity types on the NetScaler instance. For example `csvserver`, `lbmonitor`, `servicegroup`, etc.
- `lbvserver`: Refers to the list of load-balancing virtual server entities in the NetScaler instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Using the built-in data source with collection

```
parameters:

  - name: selected-lbvserver

    label: Select an existing lbvserver

    type: datum

    required: true

    data-source:

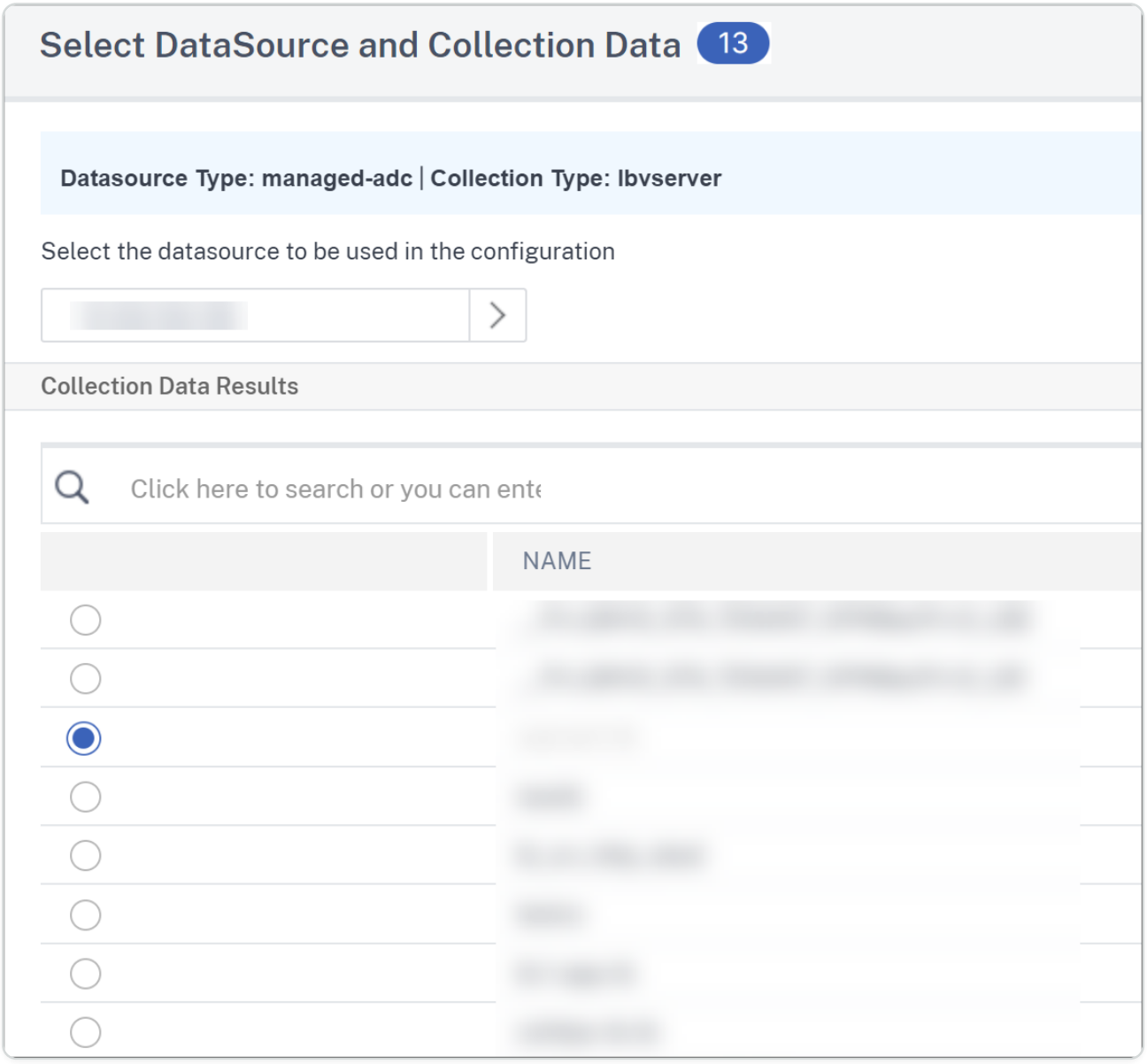
      type: managed-adc

      collection: lbvserver
```

In this example, the `datum` parameter is used to allow a user to select both the NetScaler instance and a specific `lbvserver` from the `managed-adc` data source type.

When you define a collection type in the `parameters` section, the StyleBook users can select the NetScaler instance and a specific entity from a collection on that instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Access an attribute of the selected item:

When the StyleBook user selects a virtual server, the following expression in your StyleBook can access any attribute of the selected item.

```
$parameters.selected-lbvserver.attributes.<attribute-name>
```

In this example, the selected `datum` is `lbvserver`. So, you can access any attribute of the NetScaler entity `lbvserver` such as `name`, `servicetype`, `ipv46`, and so on.

Example:

```
$parameters.selected-lbvserver.attributes.ipv46
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This expression retrieves the IP of the selected load-balancing virtual server. For more information about the NetScaler entities (collections) and their attributes, see NetScaler NITRO API reference.

Select multiple items from a collection:

The following parameters section allows StyleBook users to select multiple items of a collection.

```
parameters:

  - name: selected-lbvservers

    label: Select existing lbvservers

    type: datum[]

    required: true

    data-source:

      type: managed-adc

      collection: lbvserver
```

In this example, the datum parameter is used to define the data source array. User can select one or more lbvservers from a single NetScaler® instance or across NetScaler instances.

The code snippet below depicts the way to access selected items and its attributes.

```
components:

  - name: sslvserver-comp

    type: ns::sslvserver

    repeat:

      repeat-list: $parameters.selected-lbvservers

      repeat-item: vserverObj

    properties:

      name: $vserverObj.attributes.name
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      ssl2: DISABLED

      ssl3: DISABLED

      tls1: DISABLED

      tls11: ENABLED

      tls12: ENABLED
```

Access a collection by selected item's reference:

In addition to allowing a StyleBook user to select a specific entity on a managed NetScaler instance, you can also access any entity from the same or different collections on the selected NetScaler instance. To access another collection on that NetScaler instance, use the following expression in the `components` section:

```
$parameters.selected-lbvserver.datasource.collections.<collection-name>
```

Example:

```
$parameters.selected-lbvserver.datasource.collections.csvserver
```

This expression returns the list of content-switching virtual servers from the selected NetScaler instance.

And, the following expression returns a list of all the bindings between `lbvservers` and `servicegroups`:

```
$parameters.selected-
lbvserver.datasource.collections.lbvserver_servicegroup_binding
```

Example StyleBook with a collection

The following is an example StyleBook to demonstrate how to use the managed NetScaler instance as a data source:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
name: bind-lb-to-servicegroup-using-ADC-as-datasource

namespace: com.citrix.adc.stylebooks

version: "1.1"

display-name: "HTTP/SSL LoadBalancing StyleBook with Service Binding"

description: "This stylebook defines a typical Load Balanced Application
configuration where we allow the user to select an existing lbvserver on
the NetScaler using datum type parameter. Then a servicegroup for the
selected lb is created if it does not exist on the NetScaler. Finally, the
selected lbvserver is bound to the service "

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"



parameters:

  -

    name: selected-vserver

    label: "Select an Existing VServer"

    description: "Load Balancing Application Vservers to be bound to
service on the ADC"

    type: datum

    required: true
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    data-source:

      type: managed-adc

      collection: lbvserver



components:

  -

    name: servicegroup-discovery-comp

    type: object

    repeat: $parameters.selected-
vserver.datasource.collections.servicegroup

    repeat-item: svcgrp

    repeat-condition: $svcgrp.attributes.servicegroupname ==
 $parameters.selected-vserver.attributes.name + "-svcgrp"

    properties:

      servicegroupname: $svcgrp.attributes.servicegroupname

  -

    name: servicegroup-creation-if-not-exists-comp

    type: ns::servicegroup

    condition: not exists($components.servicegroup-discovery-comp)

    properties:

      servicegroupname: $parameters.selected-vserver.attributes.name + "-
svcgrp"

      servicetype: $parameters.selected-vserver.attributes.servicetype
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    components:

      -

        name: lbvserver-servicegroup-binding

        type: ns::lbvserver_servicegroup_binding

        properties:

          name: $parameters.selected-vserver.attributes.name

          servicegroupname: $parent.properties.servicegroupname
```

In this StyleBook, the `components` section checks for the service group name that matches the selected load-balancing virtual server name concatenated with `svcgrp`.

If the name of the selected load-balancing virtual server is `lbv1`, this StyleBook checks for the service group with the name `lbv1-svcgrp`. If it is not found, it creates a service group `lbv1-svcgrp` and binds with the `lbv1` virtual server.

The following expression fetches the list of service groups in the NetScaler instance.

```
repeat: $parameters.selected-vserver.datasource.collections.servicegroup
```

In this expression:

- `datasource`: Refers to the selected NetScaler instance managed by NetScaler Console.
- `collections`: Refers to all the entities in the NetScaler instance.
- `servicegroup`: Refers to the service groups in the NetScaler instance.

Filtering Collection data:

The following parameters section explains how to specify filters on a builtin data source collection in the StyleBook definition. It allows StyleBook users to select a specific item from a filtered collection.

```
parameters:

  - name: selected-lbvserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    label: Select an existing lbvserver

    type: datum

    required: true

    data-source:

      type: managed-adc

      collection: lbvserver

      collection-filters:

        protocol: SSL
```

In this example, the datum parameter is used to allow a user to select both the NetScaler instance and a specific lbvserver having SSL protocol from the managed-adc data source type.

After the StyleBook user selects a virtual server, any attribute of the selected item can be accessed the same way as explained in the previous section.

Use target NetScaler instances as data sources

You can also use the target NetScaler of your configuration itself as a data source input for your configuration. In this scenario, you might want to refer the existing configuration on the target NetScaler to create new configurations on that NetScaler.

To use target instances as data sources, you don't have to use the `datum` built-in type parameter, since no NetScaler instances need to be selected by the StyleBook user. You can directly write expressions in the `components` section of your StyleBook that retrieve data from the target NetScaler instance.

Use the following expression to retrieve the following from the target NetScaler instances:

- Collections:

  ```
  $current-target-as-datasource.collections.<collection-name>
  ```

  Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$current-target-as-datasource.collections.lbvserver
```

- Attributes:

```
$current-target-as-datasource.collections.attributes.<attribute>
```

Example StyleBook to use the target NetScaler instance as a data source

The following is an example StyleBook to demonstrate how to use the target NetScaler instance as a data source:

```
---

name: lb-add-service-with-target-adc

namespace: com.citrix.adc.stylebooks

version: "1.1"

display-name: "HTTP/SSL LoadBalancing StyleBook with Service Binding"

description: "This stylebook defines a typical Load Balanced Application
configuration."

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"



components:

  -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
name: servicegroup-comp

type: ns::servicegroup

properties:

  servicegroupname: "lb-demo-svcgrp"

  servicetype: "HTTP"



components:

  -

    name: lbvserver-svg-binding

    type: ns::lbvserver_servicegroup_binding

    repeat: $current-target-as-datasource.collections.lbvserver

    repeat-item: lbvsrvr

    repeat-condition: $lbvsrvr.attributes.name == "lb-demo-lb"

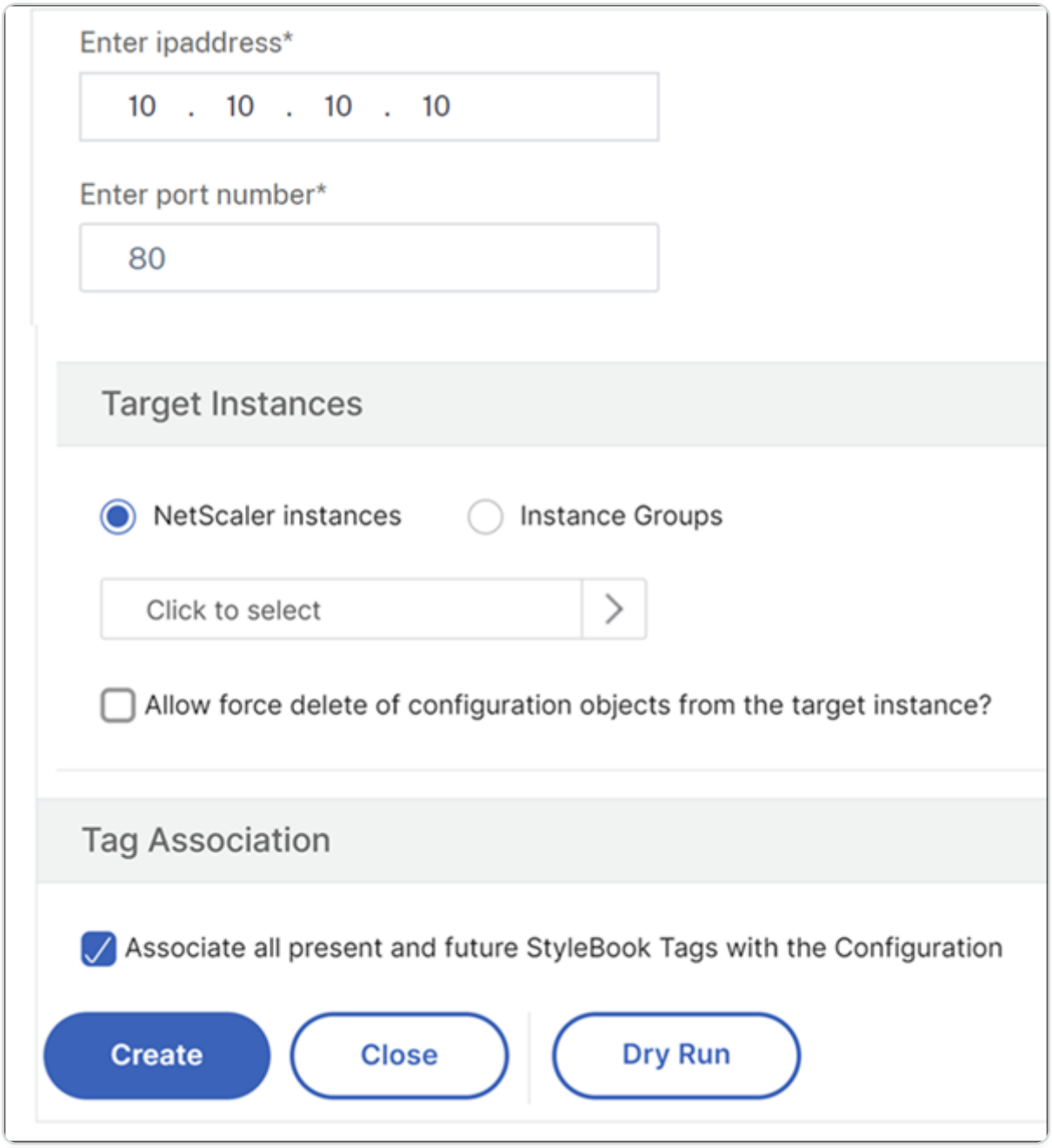
    properties:

      name: $lbvsrvr.attributes.name

      servicegroupname: $parent.properties.servicegroupname
```

In this example, the configuration pack checks for the load-balancing virtual servers in the target NetScaler instances. And, if the given load-balancing virtual server IP address is matched, it retrieves the name and service group name.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Use custom data sources

Along with managed NetScaler instances as a data source, you can define and use custom data sources if the input data is repeatedly used for creating multiple configurations. You can save the input data in NetScaler Console as a data source. And, you can modify StyleBooks to consume this data without requiring StyleBook users to provide inputs repeatedly.

Before using a custom data source in your StyleBook definition, do the following to define a custom data source:

1. Add a data source type.
2. Add collection schema under data source type.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

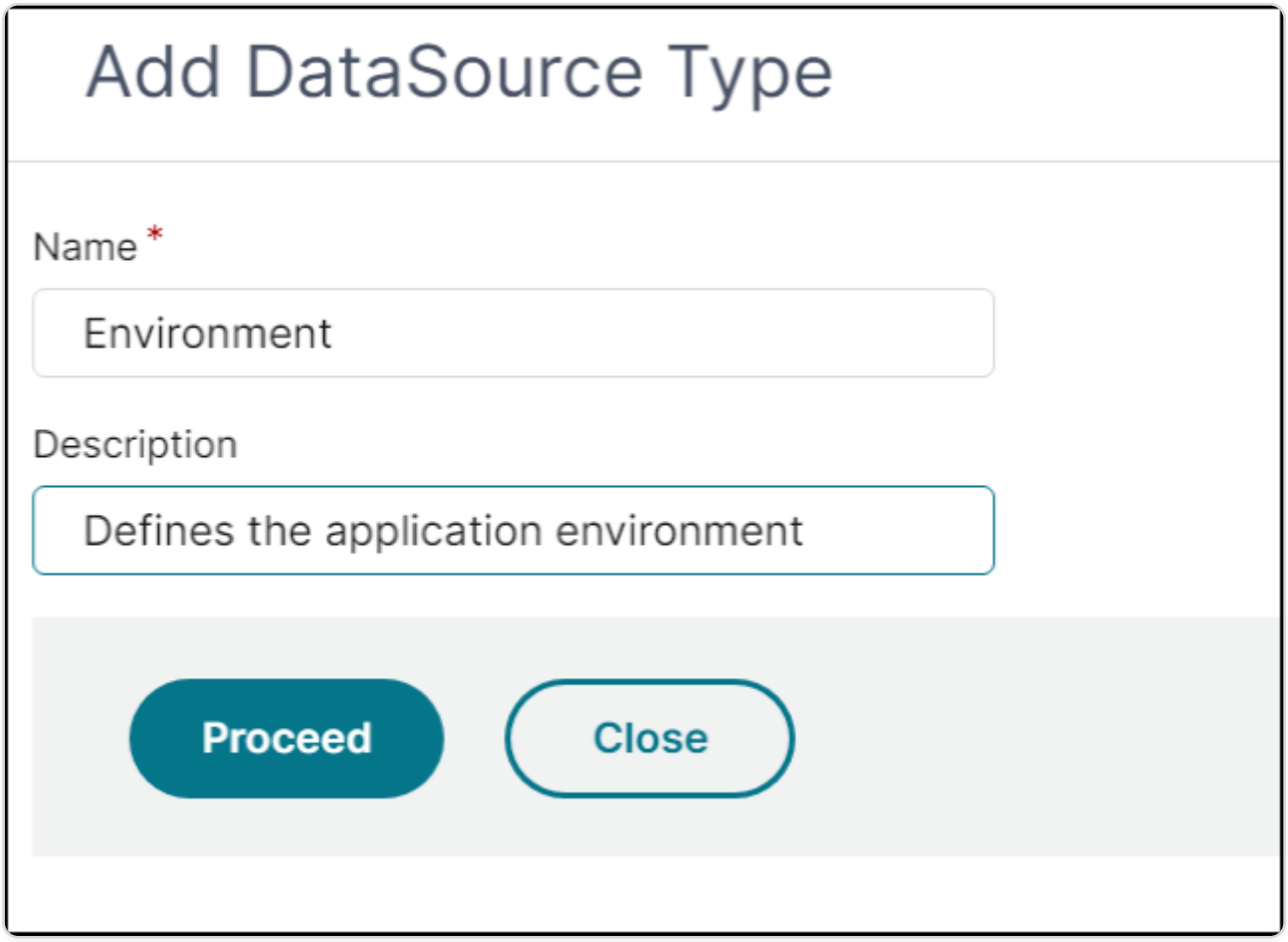
3. Add a data source.
4. Add a collection data.

After adding a data source, you can use this data source to in the StyleBook definition. For more information, see Use custom data sources in the StyleBook definition.

Add a data source type

Specify a data source type to distinguish the source from which data is retrieved.

1. In **Applications > Configuration > Data Sources**.
2. Select **Data Source Type** and click **Add**.
3. Specify the **Name** and **Description** for the data source type.
4. Click **Proceed** to save the **Data Source Type**. Click **Close** to quit the workflow without saving any changes.



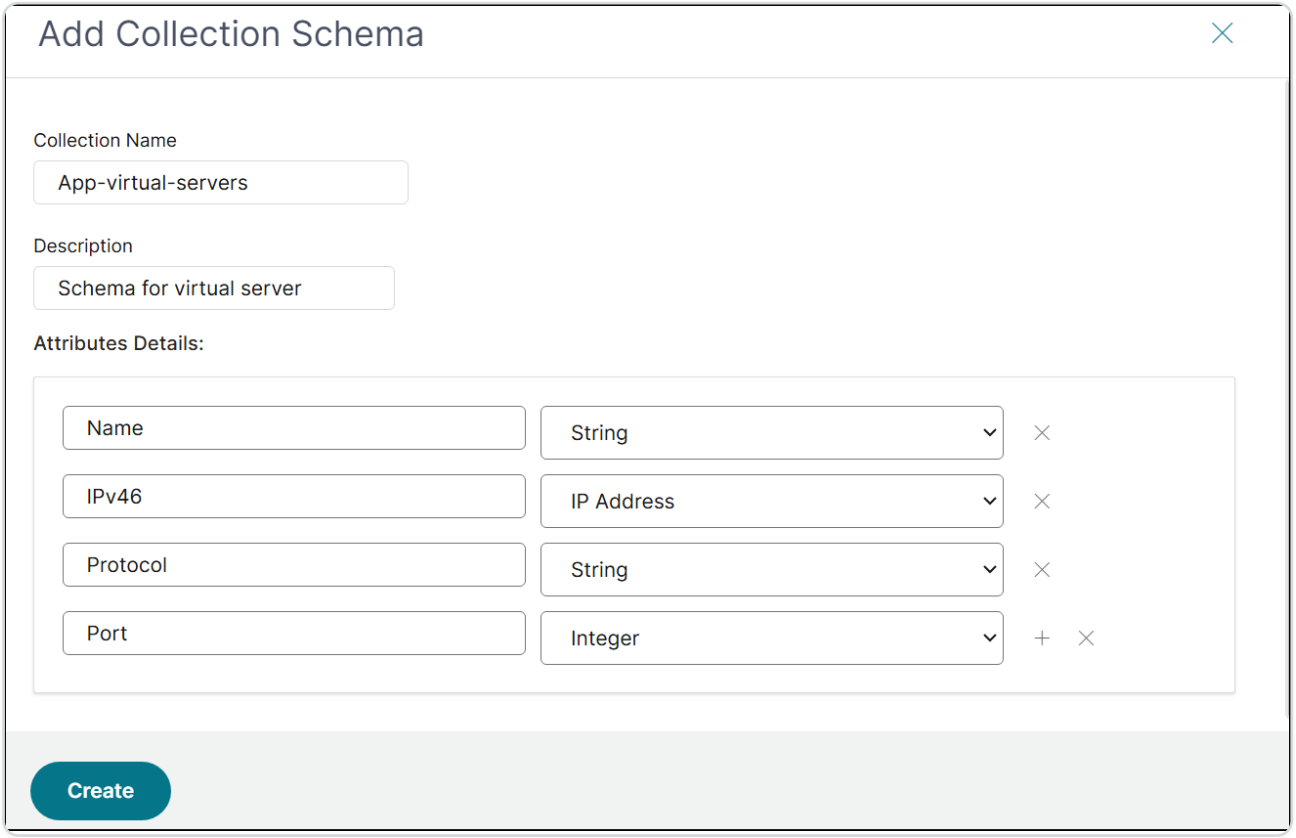
In this example, the data source type is set to **Environment**. This type can be used to define the application environments as data sources.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Add a collection schema under data source type

After adding **Data Source Type**, a screen to add **Collection Schemas** for ""Data Source Type** is displayed.

1. Click **Add**.
2. Specify the **Collection Name** for a collection schema.
3. Enter the **Description**.
4. Add attributes(name and its type) under **Attribute Details** as required.
5. Click **Create**.



In this example, the **App-virtual-servers** collection schema has four attributes. So, the collection that you want to store must have these attributes of the set data types.

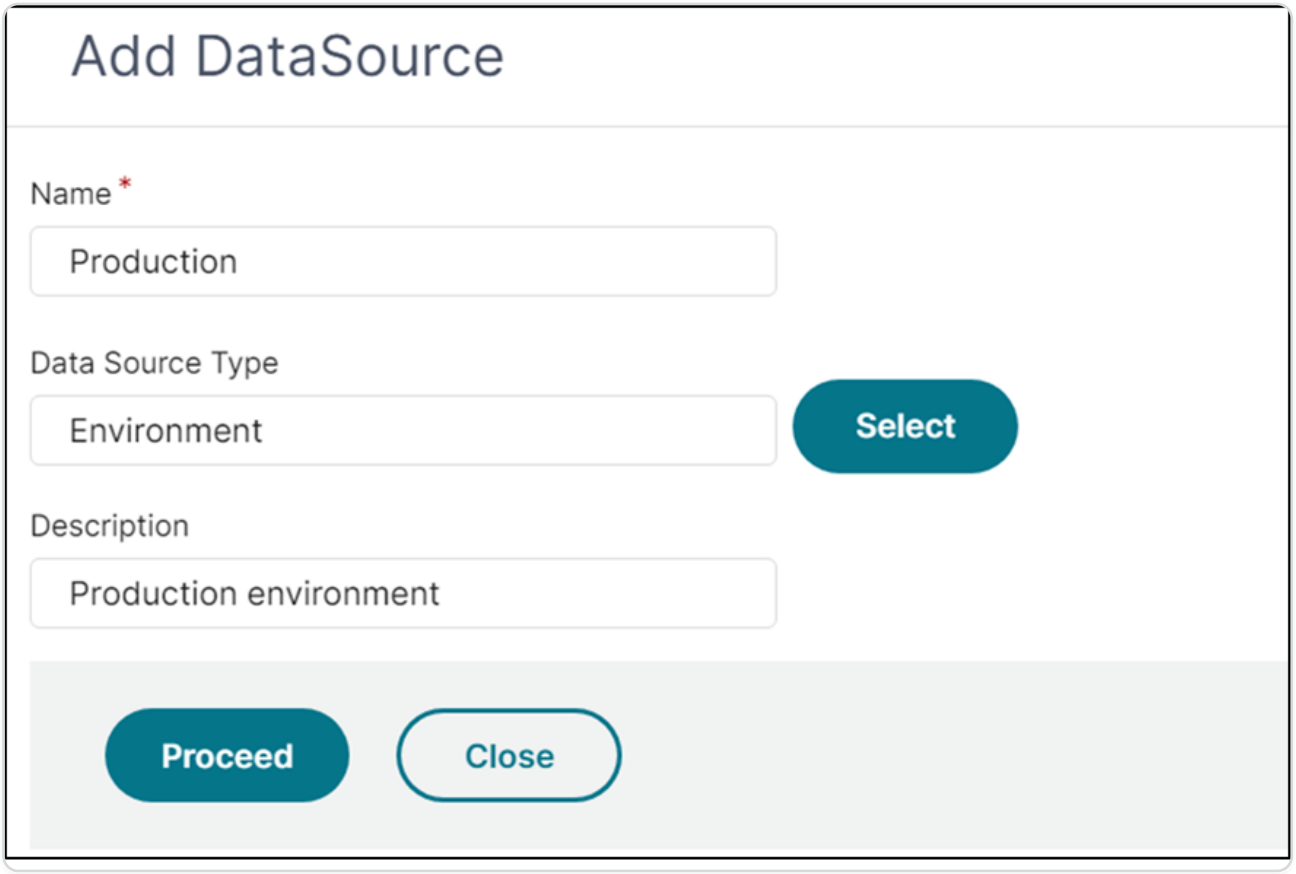
Add a data source

Define a data source for a specific data source type.

1. Go to **Applications > Configuration > Data Sources**.
2. Select the tab **Data Sources** and click **Add**.
3. Specify the **Name**.
4. Select the **Data Source Type**, and enter the **Description**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Click **Proceed** to save the **Data Source**. Click **Close** to quit the workflow without saving any changes.



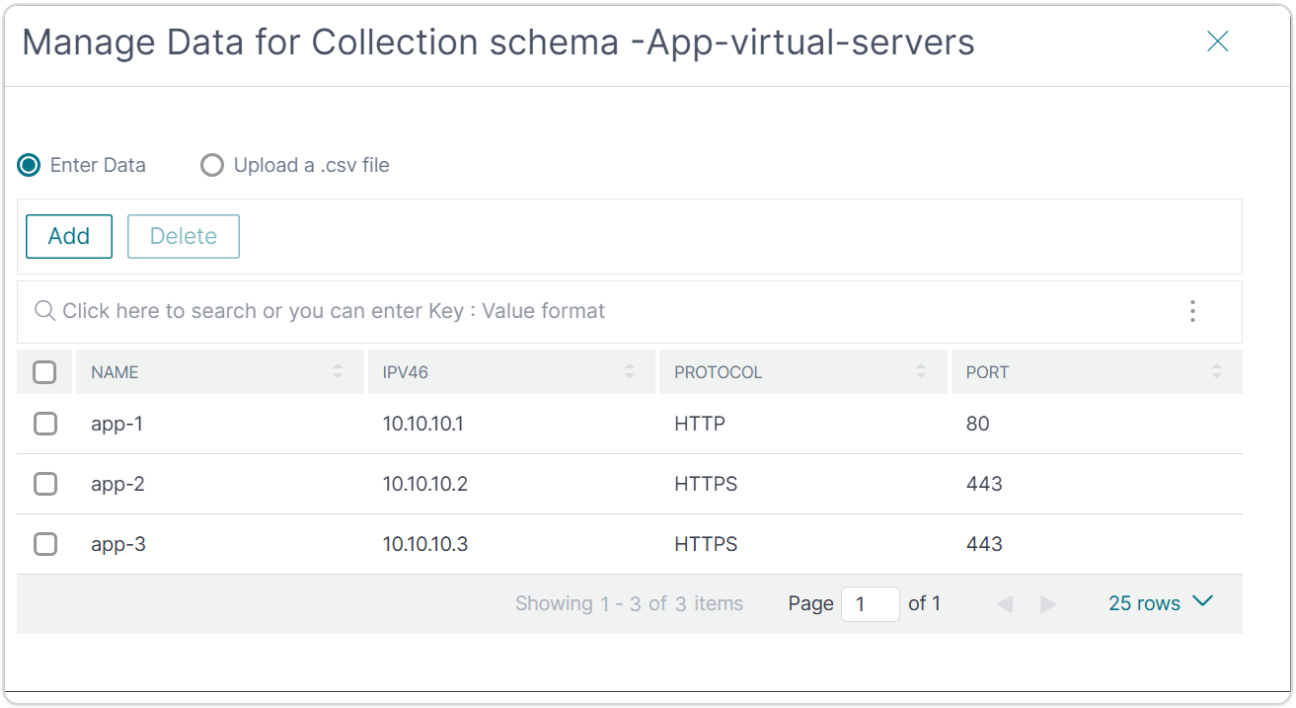
In this example, the **Production environment** is added as a data source.

Add a collection data

After adding **Data Source**, a screen to enter the data for **Data Source** is displayed. You can see a list of **Collection Schemas**.

1. Select the **Collection Schema** to which you want to add collections data.
2. Click **Manage Collection Data**.
3. Add data to the collection. You can either add data one by one or upload a CSV file. When you upload a CSV file, ensure the column names are matching with the attribute names of the collection schema.
4. Click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Use custom data source without collection

The following `parameters` section explains how to define a custom data source in the StyleBook definition without collection.

```
parameters:

    - name: selected-environment

      label: Select a custom datasource environment

      type: datum

      required: true

      data-source:

        type: "Environment"
```

The configuration pack GUI displays the applicable data sources and StyleBook users can select any of them to create a configuration pack.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



In this example, it uses the `Production` data source to retrieve data.

In the `Environment` data source type, to access the `App-virtual-servers` collection type, use the following expression:

```
$parameters.selected-environment.collections.App-virtual-servers
```

Example Snippet:

```
components:

  -

    name: lbvserver-comp

    type: ns::lbvserver

    repeat: $parameters.selected-environment.collections.App-virtual-
servers

    repeat-item: app

    properties:

      name: $app.attributes.Name + "-lb"

      ipv46: ip($app.attributes.IPv46 )

      port: $app.attributes.Port

      servicetype: $app.attributes.Protocol

    components:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    -

      name: servicegroup-comp

      type: ns::servicegroup

      properties:

        servicegroupname: $parent.properties.name + "-svcgrp"

        servicetype: $parent.properties.servicetype



      components:

        -

          name: lbvserver-svg-binding

          type: ns::lbvserver_servicegroup_binding

          properties:

            name: $parent.parent.properties.name

            servicegroupname: $parent.properties.servicegroupname
```

Use custom data sources with collection

The following `parameters` section explains how to define a custom data source in the StyleBook definition. It allows StyleBook users to select a specific item of a collection.

```
parameters:

  - name: selected-app-vserver

    label: Select a collection from the datasource

    type: datum

    required: true
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    data-source:
      type: Environment
      collection: App-virtual-servers
```

In this example, the `datum` parameter is used to define the custom data source. It uses the `Production` data source to retrieve data from the `App-virtual-servers` collection schema.

In the `Environment` data source type, to access the protocol from the `App-virtual-servers` collection, use the following expression:

```
$parameters.selected-app-vserver.attributes.Protocol
```

Example snippet:

```
components:
  - name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: $parameters.selected-app-vserver.attributes.Name
      ipv46: $parameters.selected-app-vserver.attributes.IPv46
      port: $parameters.selected-app-vserver.attributes.Port
      servicetype: $parameters.selected-app-vserver.attributes.Protocol
```

When you define a collection type in the `parameters` section, the StyleBook users can select the data source and collection.

Selecting multiple items from a collection:

The following parameters section allows StyleBook users to select multiple items of a collection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
parameters:

  - name: selected-app-vservers

    label: Select app-vservers from the collection

    type: datum[]

    required: true

    data-source:

      type: Environment

      collection: App-virtual-servers
```

In this example, the datum parameter is used to define the custom data source array. User can select one or more items from ‘App-virtual-servers’ collection from a single data source or across data sources.

The code snippet below depicts the way to access selected items and its attributes.

```
components:

  -

   name: lbvserver-comp

   type: ns::lbvserver

   repeat:

   repeat-list: $parameters.selected-app-vservers

   repeat-item: vserverObj

    properties:

      name: $vserverObj.attributes.Name

      ipv46: $vserverObj.attributes.IPv46
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      port: $vserverObj.attributes.Port

      servicetype: $vserverObj.attributes.Protocol
```

Filtering Collection data:

The following parameters section explains how to specify filters on a custom data source collection in the StyleBook definition. It allows StyleBook users to select a specific item from a filtered collection.

```
parameters:

  - name: selected-app-vserver

    label: Select a collection from the datasource

    type: datum

    required: true

    data-source:

      type: Environment

      collection: App-virtual-servers

      collection-filters:

        Protocol: SSL
```

In this example, the datum parameter is used to define the custom data source. It uses the data source of type Environment to retrieve filtered data from the App-virtual-servers collection schema.

After the StyleBook user selects a virtual server, any attribute of the selected item can be accessed the same way as explained in the previous section.

Use APIs to create configurations from StyleBooks

After you have built your StyleBook, you have to import it either by using the NetScaler Console GUI or by using the NetScaler Console APIs. NetScaler Console validates your StyleBook when

© 1997–2026 Citrix Systems, Inc. All rights reserved.

you import it. If the validation is successful, your StyleBook appears on the NetScaler Console catalog of StyleBooks, ready to be used for creating configurations.

You can now use the StyleBook APIs to create configurations based on this StyleBook. You can use any tool such as the cURL command line tool or the Postman chrome browser extension to send HTTP requests to NetScaler Console.

NOTE:

The StyleBooks APIs are fully documented using the OpenAPI specification on the Developer Portal.

Example 1

Consider the `lb-vserver` StyleBook created in StyleBook to Create a Load Balancing Virtual Server. Use the following REST APIs to create a configuration pack from this StyleBook:

HTTP METHOD: POST

URL: `https://<IP>/stylebook/nitro/v2/config/configpacks`

REQUEST Headers:

Content-Type: application/json

Accept: application/json

REQUEST BODY PAYLOAD:

```
{
  "configpack":
  {
    "parameters": {
      "name": "lb1",
      "vip-ipaddress": "10.102.117.31"
    },
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "targets":
    [
      {
        "instance_id": "deecee30-f478-4446-9741-a85041903410"
      }
    ],
    "stylebook": {
            "name": "lb-vserver",
            "namespace": "com.example.stylebooks",
            "version": "1.0"
        }
  }
}
```

In this HTTP request, the ID, deecee30-f478-4446-9741-a85041903410, is the instance ID of the NetScaler instance on which the load balancing virtual server lb1 with IP address 10.102.117.31 is created. The instance ID of the NetScaler instance is retrieved from NetScaler Console.

To get the ID of an instance managed by NetScaler Console, you can use the NetScaler Console APIs. For example, to retrieve the instance ID or a NetScaler instance whose IP address is 192.168.153.160, you can use the following API:

HTTP METHOD: GET

URL: `https://<IP>/nitro/v2/config/ns?filter=ip_address:192.168.153.160`

REQUEST HEADERS:

Accept: application/json

The response has the ID in the json payload:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EXPECTED RESPONSE HEADERS (on success):

200 OK

Content-Type: application/json

EXPECTED RESPONSE BODY (on success):


```
{
  "errorcode": 0,
  "message": "Done",
  "operation": "get",
  "resourceType": "ns",
  "username": "nsroot",
  "tenant_name": "Owner",
  "resourceName": "",
  "ns":
  [
    {
    "is_grace": "false",
    "hostname": "",
    "std_bw_config": "0",
    "gateway_deployment": "false",
    "id": "deecee30-f478-4446-9741-a85041903410",
   }
 ]
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}
```

If the configuration (configuration pack) is successfully created, you receive the following HTTP response:

EXPECTED RESPONSE HEADERS (on success):

202 OK

Content-Type: application/json

EXPECTED RESPONSE BODY (on success):

```
{
  "job":
  {
    "job_id": "1460806080"
  }
}
```

You have created your first job that is uniquely identified by using the ID, 1460806080. You can use this ID to query, update, or delete the configuration.

You can use the following URL to query the job status:

`https://<IP>/stylebook/nitro/v2/config/jobs/<jobid>`

Example 2

You can use the same StyleBook to create another configuration or configuration pack and run it on the same or different NetScaler instances. In this example, create another configuration and provide a different name and IP address for the virtual server. Specify LEASTCONNECTION as the load balancing method. Deploy this configuration on two NetScaler instances.

The HTTP request is as follows:

HTTP METHOD: POST

© 1997–2026 Citrix Systems, Inc. All rights reserved.

URL: `https://<IP>/stylebook/nitro/v2/config/configpacks`

REQUEST HEADERS:

Content-Type: application/json

Accept: application/json

REQUEST BODY PAYLOAD:

```
{
  "configpack":
  {
    "parameters": {
      "name": "lb1",
      "vip-ipaddress": "10.102.117.31",
      "lb-alg": "LEASTCONNECTION"
    },
    "targets":
    [
      {
        "instance_id": "deecee30-f478-4446-9741-a85041903410"
      },
      {
        "instance_id": "abcdee30-f478-4446-9741-a85041903410"
      }
    ],
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "stylebook": {

            "name": "lb-vserver",

            "namespace": "com.example.stylebooks",

            "version": "1.0"

        }

  }

}
```

In this HTTP request, the load balancing virtual server lb1 with IP address 10.102.117.31 is created on the two NetScaler instances with IDs "deecee30-f478-4446-9741-a85041903410" and "abcdee30-f478-4446-9741-a85041903410".

On successful creation of the configuration pack, the following HTTP response is received:

EXPECTED RESPONSE HEADERS (on success):

202 OK

Content-Type: application/json

EXPECTED RESPONSE BODY (on success):

```
{

    "job": {

        "job_id": "165769629"

    }

}
```

This new configuration pack has a different ID, 165769629. You can update or remove this configuration by using this ID.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example 3

Consider the "basic-lb-config" StyleBook you have created in StyleBook to Create a Basic Load balancing Configuration. Use the REST API to create a configuration pack from this StyleBook as follows:

HTTP METHOD: POST

URL: `https://<IP>/stylebook/nitro/v2/config/configpacks`

REQUEST HEADERS:

Content-Type: application/json

Accept: application/json

REQUEST BODY PAYLOAD:

```
{

  "configpack":

  {

    "parameters":

    {

      "name": "myapp",

      "ip": "10.70.122.25",

      "svc-servers": ["192.168.100.11","192.168.100.12"],

       "svc-port": 8080

    },

    "targets":

    [

     {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      "instance_id": "deecee30-f478-4446-9741-a85041903410"
     },
     {
      "instance_id": "abcdefgi-d589-4557-8632-a74032802412"
     }
    ],
    "stylebook": {
            "name": "basic-lb-config",
            "namespace": "com.example.stylebooks",
            "version": "0.1"
        }
  }
}
```

EXPECTED RESPONSE HEADERS (on success):

202 OK

Content-Type: application/json

EXPECTED RESPONSE BODY (on success):

```
{
    "job": {
        "job_id": "3628681382"
    }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}
```

In this HTTP request, the load balancing configuration is run on two NetScaler instances. You can log on to these NetScaler instances to verify whether a virtual server and a service group with two services bound are created.

Example 4

Consider the composite StyleBook **composite-example** you created in Create a Composite StyleBook. Use REST APIs to create a configuration pack from this StyleBook as follows:

HTTP METHOD: POST

URL: `https://<IP>/stylebook/nitro/v2/config/configpacks`

REQUEST HEADERS:

Content-Type: application/json

Accept: application/json

REQUEST BODY PAYLOAD:

```
{
  "configpack":
  {
    "parameters": {
      "name": "myapp",
      "ip": "2.2.2.2",
      "svc-servers": ["10.102.29.52","10.102.29.53"]
    },
    "targets":
    [
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
     {
      "id": "deecee30-f478-4446-9741-a85041903410"
     },
     {
      "id": "abcdefgg-d589-4557-8632-a74032802412"
     }
    ],
    "stylebook": {
            "name": "composite-example",
            "namespace": "com.example.stylebooks",
            "version": "0.1"
        }
  }
```

In this HTTP request, the configuration is created on two NetScaler instances represented by their IDs. If you log on to the NetScaler instances, you can view the configuration objects created by the "basic-lb-config" StyleBook that was imported into the "composite-example" StyleBook. You can also see a new HTTP monitor called `myapp-mon` that was part of the "composite-example" StyleBook.

On successful creation of the configuration pack, the following HTTP response is received:

EXPECTED RESPONSE HEADERS (on success):

202 OK

Content-Type: application/json

EXPECTED RESPONSE BODY (on success):

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{

    "job": {

        "job_id": "3628681382"

    }

}
```

Updating a configuration

To update the configuration, you can use the following API. Here, a back end server with the IP address 10.102.29.54 is added to the load balancing virtual server `myapp:

HTTP METHOD: PUT

URL: `https://<IP>/stylebook/nitro/v2/config/configpacks/<configpackid>`

REQUEST HEADERS:

Content-Type: application/json

Accept: application/json

REQUEST BODY PAYLOAD:

```
{

  "configpack": {

    "parameters": {

      "name": "myapp",

      "ip": "2.2.2.2",

      "svc-servers": ["10.102.29.52","10.102.29.53","10.102.29.54"]

  },

  "targets":
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    [
      {
       "instance_id": "deecee30-f478-4446-9741-a85041903410"
      },
      {
       "instance_id": "abdcedff-d589-4557-8632-a74032802412"
      }
    ]
  }
}
```

On successful update of the configuration pack, the following HTTP response is received:

EXPECTED RESPONSE HEADERS (on success):

202 OK

Content-Type: application/json

EXPECTED RESPONSE BODY (on success):

```
{
    "job": {
        "job_id": "3628681382"
    }
}
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Deleting a configuration

To delete this configuration (from all the NetScaler instances), you can use the API for deleting a configuration pack as follows:

On successful deletion of the configuration pack, the following HTTP response is received:

HTTP METHOD: DELETE

URL: `https://<DNS-or-IP>//stylebook/nitro/v2/config/configpacks/<configpackid>`

REQUEST HEADERS:

Accept: application/json

EXPECTED RESPONSE HEADERS (on success):

202 OK

Content-Type: application/json

EXPECTED RESPONSE PAYLOAD (on success):

```
{

    "job": {

        "job_id": "3628681382"

    }

}
```

Log on to the NetScaler instance and verify that all the configuration objects that are part of this configuration pack have been removed.

To remove the configuration from specific NetScaler instances instead of from all the instances, use the update configuration pack operation in Updating a configuration. Change the `targets` attribute in the JSON payload to remove the specific NetScaler instance IDs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use APIs to create configurations

Use the StyleBook API to create configurations based on this StyleBook. You can use any tool such as the cURL command line tool or the Postman chrome browser extension to send HTTP requests to NetScaler Console.

Consider the StyleBook example that you created in How to Create a StyleBook to Upload SSL Certificate and Certificate Key Files to NetScaler Console to upload the certificate and key files. Use the REST API to create a configuration pack from the StyleBook as follows:

POST

`https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks?mode=async`

```
{

    "configpack": {

        "stylebook": {

            "name": "lb",

            "namespace": "com.citrix.adc.stylebooks",

            "version": "1.1"

        },

        "parameters": {

            "lb-appname": "lbapp1",

            "lb-virtual-ip": "192.168.1.1",

            "lb-virtual-port": "443",

            "lb-service-type": "SSL",

            "svc-service-type": "HTTP",

            "svc-servers": [

                {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                "ip": "193.1.1.1",
                "port": "80"
            }
        ],
        "certificates": [
            {
                "cert-name": "cert1",
                "cert-file": {
                    "name": "c3.pem",
                    "contents": "<base64 encoded content>",
                    "encoding_type": "base64"
                },
                "ssl-inform": "PEM",
                "key-file": {
                    "name": "c3.key",
                    "contents": "<base64 encoded content>",
                    "encoding_type": "base64"
                }
            }
        ]
    },
    "targets": [
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            {
                "instance_id": "1b322685-3b23-4111-a9ce-56dd1c659e4c"
            }
        ]
        }
    }
}
```

This returns a Job ID that can be used to track the completion of the configuration job:

```
{
    "job": {
        "job_id": "388922985"
    }
}
```

Use the job polling API to find out the status of the job and when the configuration job is complete:

GET

`https://<ADM-endpoint-name>/stylebook/nitro/v2/config/jobs/388922985`

```
200 OK
{
    "job": {
        "job_id": "388922985",
        "status": "completed",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "progress_info": [...],

        "result": {

            "config_key": "388922985",

            "created_by": "nsroot",

            "created_datetime": "2023-01-14 01:46:05.410998",

            "created_datetimestamp": "2023-01-14 01:46:05",

            "id": "388922985",

            "incarnation_number": "0",

            "last_modified_by": "nsroot",

            "last_modified_datetime": "2023-01-14 01:46:05",

            "lock": "Y",

            "name": "sample-dns-stylebook",

            "namespace": "com.citrix.adc.tests",

            "primary_keys": "{}",

            "sb_id": "samp4ed0c4c90aefaadaff6422b0c395f67f",

            "status": "completed",

            "target_devices_json": "[{\"instance_id\": \"49a45044-
ceb3-4e9d-8a5d-e3fe225d90ed\", \"id\": \"1833061454\", \"group_id\": \"\",
\"instance_ip\": \"192.168.153.165\", \"hostname\": \"ctx-adc-dc01-v-
prod-54\", \"instance_role\": \"[\\\"default\\\"]\",
\"incarnation_number\": \"0\"}]",

            "tenant_id": "1a45fd70-7ce3-4bff-8642-1bd7f7e97673",

            "version": "1.0"

        }
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    }
}
```

The job ID (388922985) identifies the configuration pack. You can use this ID to query, update, or delete the configuration.

Use APIs to create configurations to upload any file type

You can also use the NetScaler Console API to create a configuration pack that uploads files to the selected NetScaler instance.

Consider the StyleBook example that you created in How to Create a StyleBook to Upload Files to NetScaler Console to upload files of any type.

Use the following REST API to create a configuration pack from this StyleBook:

POST `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks?mode=async`

```
{
    "configpack": {
        "stylebook": {
        "name": "filetest",
        "namespace": "test.adc.stylebook",
        "version": "1.0"
        },
        "parameters": {
            "nameoffile": "file1",
            "fileupload": {
                "name": "relate.txt",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                "contents": "base64 encoded content",
                "encoding_type": "base64"
            }
        },
        "targets": [
            {
                "instance_id": "9419667d-27b7-495a-b87a-d3b5ee747dd3"
            }
        ],
    }
}
```

Use APIs to import custom StyleBooks

Use the StyleBook API to import custom StyleBooks into NetScaler Console. Use REST APIs to create a configuration pack from this StyleBook in any tool such as the cURL command line tool or the Postman chrome browser extension. For example, you can import a StyleBook named `example-lb` that can be used to create a load balancer configuration on a NetScaler instance.

HTTP Method: POST

URL: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/stylebooks/actions/import?mode=async`

```
{
    "import": {
        "file_name": "add_dnssoarec.yaml",
        "source": "<base 64 encoded content of the sb definition>",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "encoding": "base64"

    }

}
```

Where, the `source` attribute's value is the base64 encoding of the contents of your StyleBook file. You can paste the YAML contents of your StyleBook file in an online tool. For example, use `<https://www.browserling.com/tools/file-to-base64>` to obtain the base64 string that you can then use as a value for the `source` attribute.

Using this API call, you can also upload a compressed tarball file (.tgz file) having multiple StyleBook files in one API operation. Do the following:

- Change the `file_name` attribute to the .tgz file
- Change the `source` attribute to the base64 encoding of the contents of your .tgz file

After the API is run successfully in the tool you get a response with a job ID. Use this job ID to track the operation to completion:

```
200 ACCEPTED
```

Response Body:

```
{

    "job": {

        "job_id": "12345678"

    }

}
```

Use the Job ID to track the status of the operation:

HTTP Method: GET

URL: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/jobs/<job-id>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The status of the job is returned:

```
200 OK
```

Response Body:

```
{
    "job": {
        "job_id": "<job-id>",
        "progress_info": [
            {
                "is_last": "true",
                "message": "No job found",
                "status": "failed"
            }
        ],
        "status": "completed"
    }
}
```

The status value of "completed" indicates that the StyleBook has been successfully imported. Confirm the status of the operations by getting information on the StyleBook:

HTTP Method: GET

URL: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/stylebooks/samples/1.0/demo-helper-object`

The details of the imported StyleBook are displayed:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
200 OK
```

Response Body:


```
{

    "stylebook": {

        "builtin_namespaces": {},

        "created_datetime": "2023-01-14 00:13:59",

        "custom": true,

        "dependencies": [],

        "deprecate": "false",

        "description": "This Stylebook is a test",

        "display_name": "Test StyleBooks",

        "encoding": "BASE64",

        "header": "Test StyleBooks",

        "icon": "''",

        "id": "demo575731aacbfc20b4ff00b3b60ea59855",

        "is_updatable": true,

        "name": "demo-helper-object",

        "namespace": "samples",

        "primary_keys": {},

        "private": false,

        "repository_name": "",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "reverse_dependencies": [],
        "schema_version": "1.0",
        "source": "<base 64 encoded content of the stylebook definition>",
        "tenant_id": "1a45fd70-7ce3-4bff-8642-1bd7f7e97673",
        "username": "abc",
        "version": "1.0"
    }
}
```

Use API to update a custom StyleBook

You can use API to update a custom StyleBook. When you update a StyleBook, you can make changes to the StyleBook without changing its version. You can also update the definitions imported from a StyleBook bundle.

POST: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/stylebooks/<Namespace>/<version>/<Name>/actions/update?mode=async`

Payload:

```
{
    "update": {
        "encoding": "base64",
        "source": "<base 64 encoded content of the stylebook definition>"
}
}
    }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}
```

NOTE

This API is asynchronous and returns a job ID. The job ID can be used to track the update job to completion, similar to the API for importing a StyleBook.

Use APIs to download custom StyleBooks

Use the following StyleBooks REST API to download a custom StyleBook:

POST `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/stylebooks/<NAMESPACE>/<VERSION>/<NAME>/actions/download`

You can run the API in any tool such as the cURL command line tool. You can also use the Postman chrome browser extension after modifying the IP address, name, version, and namespace fields.

When you run this API, the custom StyleBook downloads to your local computer as a zipped file.

Use APIs to download dependent StyleBooks and specify compression type

Use the following API to download the full tree of dependent StyleBooks and to specify a compression format (here, .tgz):

POST `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/stylebooks/<NAMESPACE>/<VERSION>/<NAME>/actions/download?dependencies=true&compress_type=tgz`

The response displays the StyleBook and its dependencies (if any) in a tarball.

```
200 OK

Content-disposition: attachment; filename=samples_1.0_demo-helper-
object.tgz

Content-Type: application/x-zip

....zipped content...
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use API to delete custom StyleBooks

Use the following StyleBooks REST API to delete a custom StyleBook:

DELETE: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/stylebooks/<NAMESPACE>/<VERSION>/<NAME>?dependencies=true`

If the dependencies query parameter in the URL is not provided or its value is set to false, only the StyleBook is deleted. The StyleBook dependencies are not deleted.

When the custom StyleBook and its dependencies are successfully removed from NetScaler Console, you receive an HTTP response status code of 200.

NOTE

You can't delete a custom StyleBook that has dependent StyleBooks.

For example, assume that you created a StyleBook named `lb-virtual-ssl-extended` in NetScaler Console. You later decided to delete that StyleBook.

You can run the API in any tool such as the cURL command line tool. You can also use the Postman chrome browser extension after modifying the IP address, name, version, and namespace fields.

Use APIs to update an existing config pack

You can use the StyleBook API to update the existing config packs in NetScaler Console.

PUT: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/<configpack-ID>?mode=async`

Payload:

```
{

    "configpack": {

        "stylebook": {

            "name": "waf-adv",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "namespace": "com.citrix.adc.stylebooks",
            "version": "1.3"
        },
        "parameters": {
            "name": "TestApp1",
            "lbname": "my-lbv",
            "waf-settings": {
                "rule": "true",
                "type": [
                    "HTML"
                ],
                "profile-settings": {
                    "logeverypolicyhit": false,
                    "enablesignatures": {
                        "signaturename": "waf-sign1"
                    },
                    "sqlinjection-settings": {
                        "sqlinjectionaction": [
                            "log",
                            "stats"
                        ],
                        "sqlinjection-default-settings": {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                        "sqlinjectiontransformspecialchars": true,
                        "sqlinjectionchecksqlwildchars": true,
                        "sqlinjectiontype": "SQLSplCharANDKeyword",
                        "sqlinjectionparsecomments": "checkall",
                        "sqlinjectiongrammar": "OFF"
                    }
                },
                "bufferoverflow-settings": {
                    "bufferoverflowaction": [
                        "log"
                    ],
                    "bufferoverflowmaxurllength": "2048",
                    "bufferoverflowmaxheaderlength": "4096",
                    "bufferoverflowmaxcookielength": "4096",
                    "bufferoverflowmaxquerylength": "65535",
                    "bufferoverflowmaxtotalheaderlength": "65535"
                }
            }
        }
    },
        "targets": [
        {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                "instance_id": "1b322685-3b23-4111-a9ce-56dd1c659e4c"

            }

            ]

    }

}
```

An HTTP Status 202 and a response body with a job ID is returned. You can use the job ID to track the status of the update operation:

```
{

    "job": {

        "job_id": "1092579455"

    }

}
```

You can track this Job ID (in this example, 1092579455) using the jobs polling API:

GET: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/jobs/1092579455`

The update operation is successfully completed if the response contains the status set to "completed". Any other value in this field indicates the failure of the update job. The cause of the failure is available in the **progress_info** object.

```
{

    "job": {

        "job_id": "4268148987",

        "status": "completed",

        "progress_info": [
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            {
                "is_last": "false",
                "message": "Validated the parameters",
                "status": "success"
            },
            {
                "is_last": "false",
                "message": "Configuration audit completed",
                "status": "success"
            },
            {
                "is_last": "false",
                "message": "Computed configuration objects",
                "status": "success"
            },
            {
                "is_last": "false",
                "message": "Prepared objects for applying configuration on
192.168.153.165",
                "status": "success"
            },
            {
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                "is_last": "false",

                "message": "Retrieved existing data for updatable objects
on instance 192.168.153.165",

                "status": "success"

            },

            {

                "is_last": "false",

                "message": "Applied configuration on instance
192.168.153.165",

                "status": "success"

            },

            {

                "is_last": "false",

                "message": "Retrieved data for configuration audit on
instance 192.168.153.165",

                "status": "success"

            },

            {

                "is_last": "false",

                "message": "Logged out from instance 192.168.153.165",

                "status": "success"

            },

            {
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                "is_last": "true",
                "message": "Saved configpack.",
                "status": "completed"
            }
        ],
        "result": {
            "status": "completed",
            "id": "4268148987",
            "config_key": "4268148987",
            "created_by": "nsroot",
            "created_datetime": "2023-01-20 18:57:58.985435",
            "created_datetimestamp": "2023-01-20 18:57:58",
            "last_modified_by": "nsroot",
            "last_modified_datetime": "2023-01-20 19:00:32",
            "name": "sample-dns-stylebook",
            "namespace": "com.citrix.adc.tests",
            "version": "1.0"
        }
    }
}
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use APIs to update target instances

In the update config pack payload, change the `targets` section to add, remove, or replace a NetScaler instance.

Example:

In the following example, the `targets` object in the payload is changed to add a new target NetScaler to the configuration:

```
{

    "targets": [

        {

            "instance_id": "<Existing-ADC-instance-ID>"

        },

        {

            "instance_id": "<New-ADC-instance-ID>"

        }

    ],

}
```

If the update is successful, the configuration is deployed on the new NetScaler instance. Changing the targets of a configuration is useful if you want to move application configurations between NetScalers. For example, modify the `targets` object when a NetScaler needs to be removed from a configuration for maintenance.

NOTE

To remove a configuration from all its current target instances, use an empty `targets` object. The NetScaler Console configuration is retained but it is removed from the all NetScalers on which it was previously deployed. You can update the configuration again to specify one or several targets, if required.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The following API example removes the configuration from all its existing targets:

PUT: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/<configpack-ID>?mode=async`

Payload:

```
{
    "configpack": {
        "stylebook": {
            "name": "waf-adv",
            "namespace": "com.citrix.adc.stylebooks",
            "version": "1.3"
        },
        "parameters": {
            "name": "TestApp1",
            "lbname": "my-lbv",
            "waf-settings": {
                "rule": "true",
                "type": [
                    "HTML"
                ],
                "profile-settings": {
                    "logeverypolicyhit": false,
                    "enablesignatures": {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                    "signaturename": "waf-sign1"
                },
                "sqlinjection-settings": {
                    "sqlinjectionaction": [
                        "log",
                        "stats"
                    ],
                    "sqlinjection-default-settings": {
                        "sqlinjectiontransformspecialchars": true,
                        "sqlinjectionchecksqlwildchars": true,
                        "sqlinjectiontype": "SQLSplCharANDKeyword",
                        "sqlinjectionparsecomments": "checkall",
                        "sqlinjectiongrammar": "OFF"
                    }
                },
                "bufferoverflow-settings": {
                    "bufferoverflowaction": [
                        "log"
                    ],
                    "bufferoverflowmaxurllength": "2048",
                    "bufferoverflowmaxheaderlength": "4096",
                    "bufferoverflowmaxcookielength": "4096",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                        "bufferoverflowmaxquerylength": "65535",
                        "bufferoverflowmaxtotalheaderlength": "65535"
                    }
                }
            }
        },
        "targets": []
    }
}
```

Use API to config audit

You can use API to compare the changes made by a StyleBook configuration pack to the current NetScaler configuration. With this comparison, you can do the following:

- Detect the configuration drift between StyleBook configuration pack and NetScaler configuration.
- Identify any modified and deleted objects on the NetScaler that do not reflect the changes made by the configuration pack.

POST: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/<configpack-ID>/actions/audit?mode=async`

Use API to export a config pack

You can use the StyleBook API to export config packs from NetScaler Console. The export bundle is saved to your local computer. It includes the JSON file with all the parameters defined in a configuration pack and any associated system files.

POST `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/<configpack-ID>/actions/export`

Payload:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{

    "export": {

        "options": {

            "include_stylebook": true,

            "include_targets": false,

            "compress_type": "zip",

            "password_protect": false

        },

        "passphrase": ""

    }

}
```

You can choose to export the config pack along with the associated StyleBook and target instances.

When you export a configuration pack, a `tgz` or `zip` bundle downloads to your local computer. The bundle type depends on the given `compress_type`.

Use APIs to upgrade the configuration pack to a new StyleBook

You can use StyleBook APIs to upgrade the configuration pack from an existing StyleBook to a new StyleBook.

POST `http://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/actions/upgrade?mode=async`

Payload:

```
{

    "upgrade": {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "stylebook": {
            "name": "customer-template",
            "namespace": "neustar.citrix.adc.stylebooks",
            "version": "6.2"
        },
        "configpack_ids": [
            "1644278065",
            "2750234437"
        ]
    }
}
```

In this example payload, the listed config packs are 1644278065 and 2750234437. These config packs are updated to a new StyleBook with name, `customer-template`, and version, 6.2.

To get the status of the configuration pack upgrade job, use the job Polling API:

GET: `https://<ADM-IP-address>/stylebook/nitro/v1/config/jobs/<job-ID>`

NOTE

Repeat the **GET** method until the status field in the response body is set to **completed** (indicating success) or **failed**.

Use API to detach a target instance from a config pack

When you detach a target instance from a config pack, the changes made to the config pack doesn't deploy to that instance. You can use API to detach a target instance.

POST: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/<configpack-ID>/actions/detach_targets`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Payload:

```
{
    "detach_targets": [
        {
            "instance_id": "1b322685-3b23-4111-a9ce-56dd1c659e4c",
            "id": "1b322685-3b23-4111-a9ce-56dd1c659e4c"
        }
    ]
}
```

Use API to forcefully delete a NetScaler instance from the config pack

When the NetScaler instance is removed from NetScaler Console without deleting its configpack, you might get an error. So, you must forcefully delete that instance from the config pack.

You can use the StyleBook API to forcefully delete a NetScaler instance from the config pack.

PUT: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/<configpack-ID>?mode=async&force_targets_delete=true`

```
{
    "configpack": {
        "stylebook": {
            "name": "test-policy-patset",
            "namespace": "com.citrix.adc.stylebooks",
            "version": "1.1"
        },
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "parameters": {
            "lbname": "test11"
        },
        "targets": [
            {
                "instance_id": "f9bdf101-61ec-46a7-bf09-e9ce097b7cfd",
                "instance_ip": "10.106.100.116",
                "roles": [
                    "default"
                ]
            }
        ]
    }
}
```

Use APIs to delete config packs

You can use the following StyleBook API to delete config packs.

DELETE `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/<configpack-ID>?mode=async`

An HTTP Status 202 and a response payload are displayed. The response payload has job ID which you can use to track the status of the delete operation.

The response payload is as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{

    "job": {

        "job_id": "1841028854"

    }

}
```

To track the delete job operation, use the job polling API with the job ID (in this example, the job ID is 1841028854):

GET `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/jobs/1841028854`

If the status field in the response is set to "completed", it means that the delete job operation is successful, as shown in the following example:

```
{

    "job": {

        "job_id": "3920886024",

        "status": "completed",

        "progress_info": [

            {

                "is_last": "false",

                "message": "Validated the parameters",

                "status": "success"

            },

            {

                "is_last": "false",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                "message": "Configuration audit completed",
                "status": "success"
            },
            {
                "is_last": "false",
                "message": "Computed configuration objects",
                "status": "success"
            },
            {
                "is_last": "false",
                "message": "Prepared objects for applying configuration on
192.168.153.165",
                "status": "success"
            },
            {
                "is_last": "false",
                "message": "Retrieved existing data for updatable objects
on instance 192.168.153.165",
                "status": "success"
            },
            {
                "is_last": "false",
                "message": "Applied configuration on instance
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
192.168.153.165",
                "status": "success"
            },
            {
                "is_last": "false",
                "message": "Retrieved data for configuration audit on
instance 192.168.153.165",
                "status": "success"
            },
            {
                "is_last": "false",
                "message": "Logged out from instance 192.168.153.165",
                "status": "success"
            },
            {
                "is_last": "true",
                "message": "Removed configpack.",
                "status": "completed"
            }
        ]
    }
}
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

The delete operation can fail in the following scenarios:

- The NetScaler instance, on which the configuration is present, is down
- The NetScaler instance isn't reachable by the NetScaler Console
- The configuration is no longer available on the NetScaler

You can force the removal of the configuration from NetScaler Console, even if it cannot be removed from NetScaler. In such cases, the NetScaler configuration would need to be restored manually.

To force the removal of the configuration from NetScaler Console, add the query string "force=true" to the API:

DELETE `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/<configpack-ID>?mode=async&force=true`.

StyleBooks grammar

You can design your own StyleBooks, import them to NetScaler Console, and then use them to create configurations either by using the NetScaler Console GUI or by using APIs. To be able to create your own StyleBooks, you must first understand the grammar and syntax of the different constructs and attributes you can use.

This document describes the different constructs and references you can use while creating StyleBooks.

Click a section, construct, or reference name in the following table to view the details.

Header	Import StyleBooks
Parameters	Parameters-default-sources construct
Substitutions	Components
Optional properties	Helper components
Properties default sources	Nested components
Condition construct	Repeat construct
Repeat-condition construct	Outputs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Nested repeats	Parent reference
Parameter reference	Substitutions reference
Components reference	Operations
Variable reference	Alarms
Analytics	Built-in functions
Expressions	Dependency detection
In-place interpolations	

NOTE

While defining `repeat-item`, `repeat-index`, or arguments to substitution functions, do not use the following reserved words to name a user-defined variable, `$<var-name>`

- StyleBook, parameters, substitutions, components, properties, outputs, parent, self, operations, analytics, alarms
- repeat-item, repeat-item-0, repeat-item-1, repeat-item-2
- repeat-index, repeat-index-0, repeat-index-1, repeat-index-2
- default
- roles, role, targets, target
- context, parent-context, parent_context

For information and examples about how to design your own StyleBooks, see How to Create Your Own StyleBooks.

Header

The first six lines of a StyleBook comprise the header section. This section lets you define the identity of a StyleBook and describe what it does. This is a mandatory section.

The following table describes the attributes of the header section:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUTE	DESCRIPTION
name	A name to identify the StyleBook. This attribute is mandatory.
description	A description defining what a StyleBook does. This description appears on the NetScaler Console GUI. This is an optional attribute.
display-name	A descriptive name for the StyleBook. This name appears on the NetScaler Console GUI. This is an optional attribute.
author	The author person or organization who creates the StyleBook. This is an optional attribute.
namespace	A namespace forms part of a unique identifier for a StyleBook to avoid name collisions. A namespace can be any string, but a good practice is to use it for naming the company, department, or unit that created or owns a set of StyleBooks. For example, you can use the following format: `<company>.<department>.<unit>.stylebooks`. This is a mandatory attribute.
version	The version number of the StyleBook. You can change the version number when you update a StyleBook. StyleBooks of different versions can co-exist together. This is a mandatory attribute.
schema-version	The version of the StyleBooks schema. It takes the value "1.0" in the current release of NetScaler Console. This is a mandatory attribute.
private	If this attribute is set to true, the StyleBook is not displayed on the NetScaler Console GUI. This is a useful setting for StyleBooks that are building blocks for other StyleBooks and are not intended to be used by users directly. This

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUTE	DESCRIPTION
	is an optional attribute. Its default value is false.

Example:

```
    name: lb


    description: "This stylebook defines a sample load balancing
configuration."


    display-name: "Load Balancing StyleBook (HTTP)"


    author: Mike Smith (ACME Infra team)


    namespace: com.example.stylebooks


    schema-version: "1.0"


    version: "0.1"
```

The combination of name, namespace, and version uniquely identifies a StyleBook in the system. You cannot have two StyleBooks with the same combination of name, namespace, and version in NetScaler Console. However, you can have two StyleBooks with the same name and version but different namespaces, or with the same namespace and version but different names.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Import StyleBooks

This is the second section of your StyleBook and lets you declare which other StyleBook you want to refer to from your current StyleBook. This enables you to import and reuse other StyleBooks instead of rebuilding the same configuration in your own StyleBook. This is a mandatory section.

You must declare the **namespace** and **version** number of the StyleBook(s) that you want to refer to in your current StyleBook. Every StyleBook must refer to the netscaler.nitro.config namespace if it uses any of the NITRO configuration objects directly. This namespace contains all the NetScaler NITRO types, such as `lbvserver` service or monitor. StyleBooks for NetScaler versions 10.5 and later are supported, which means that you can use your StyleBook to create and run configurations on any NetScaler instance running release 10.5 or later.

The **prefix** attribute used in the import-stylebooks section is a shorthand to refer to the combination of namespace and version. For example, the "ns" prefix can be used to refer to the namespace netscaler.nitro.config with version 10.5. In the later sections of your StyleBook, instead of using the namespace and version each time you want to refer to a StyleBook with this namespace and version, you can simply use the prefix string chosen together with the name of the StyleBook to uniquely identify it.

Example:

```
import-stylebooks:

 -

   namespace: netscaler.nitro.config

   version: "10.5"

   prefix: ns

-

   namespace: com.acme.stylebooks

   version: "0.1"

   prefix: stlb
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In this example, the first prefix defined is called ns and refers to the namespace netscaler.nitro.config and version 10.5. The second prefix that is defined is called `stlb`, and refers to the namespace com.acme.stylebooks and version 0.1.

After you define a prefix, every time you want to refer to a type or a StyleBook that belongs to a certain namespace and version, you can use the notation **\<namespace-shorthand\>::\<type-name\>**. For example, **ns::lbvserver** refers to the type `lbvserver` that is defined in the namespace netscaler.nitro.config, version 10.5.

Similarly, if you want to refer to a StyleBook with version "0.1" in the com.acme.stylebooks namespace , you can use the notation **stlb::\<stylebook-name\>**.

NOTE

By convention, the prefix "ns" is used to refer to the NITRO namespace of NetScaler.

Parameters

This section lets you define all the parameters that you require in your StyleBook to create a configuration. It describes the input that your StyleBook takes. Although this section is optional, most StyleBook might need one. You can consider the parameters section to define the fields for the users who use the StyleBook to create a configuration on a NetScaler instance.

When you import your StyleBook into NetScaler Console and use it to create a configuration, the GUI uses this section of the StyleBook to display a form. This form takes an input for the defined parameter values.

The following section describes the attributes that you need to specify for each parameter in this section:

'name'

The name of the parameter you want to define. You can specify an alphanumeric name.

The name must begin with an alphabet, and can include more alphabets, numbers, hyphen (-), or underscore (_).

When writing a StyleBook, you can use this `name` attribute to refer to the parameter in other sections by using the notation $parameters.\<name>.

Mandatory? Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

'label'

A string that is displayed in the NetScaler Console GUI as the name of this parameter.

Mandatory? No

'description'

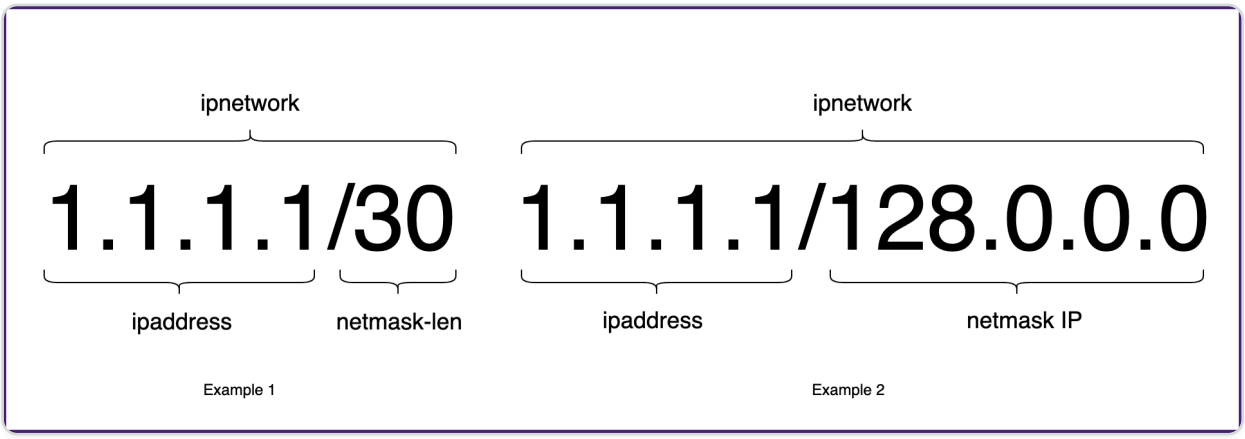
A help string that describes what the parameter is used for. The NetScaler Console GUI displays this text when the user clicks the help icon for this parameter.

Mandatory? No

'type'

The type of value these parameters can take. Parameters can be of any of the following built-in types:

- `string`: An array of characters. If a length is not specified, the string value can take any number of characters. However, you can limit the length of a string type by using the attributes min-length and max-length.
- `number`: An integer number. You can specify the minimum and maximum number that this type can take by using the attributes min-value and max-value.
- `boolean`: Can be either true or false. YAML considers all the literals as booleans (for example, Yes or No).
- `ipaddress`: A string that represents a valid IPv4 or IPv6 address.
- `ipnetwork`: It has two parts. First part is the IP address and second part is the netmask.



The netmask consists of netmask length (`netmask-len`) or netmask IP address (`netmask_ip`). The netmask length is an integer between 0-32 and 0–128 for an IPv6 address. It is used to determine the IP addresses count in a network.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When creating or updating a configuration pack from the NetScaler Console GUI, you can do one of the following actions:

  - Enable Netmask Length and input the IP address and netmask length
  - Disable Netmask Length and input the IP address and netmask IP address

- `tcp-port`: A number between 0 and 65535 that represents a TCP or UDP port.
- `password`: Represents an opaque/secret string value. When the NetScaler Console GUI displays a value for this parameter, it is shown as asterisks (*****).
- `certfile`: Represents a certificate file. This value allows you to upload the files directly from your local system when you are creating a StyleBook configuration using the NetScaler Console GUI. The uploaded certificate file is stored in the directory `/var/mps/tenants/\<tenant_path>/ns_ssl_certs` in NetScaler Console.

  The certificate file is added to the list of certificates managed by NetScaler Console.
- `keyfile`: Represents a certificate key file. This value allows you to upload the file directly from your local system when you are creating a StyleBook configuration using the NetScaler Console GUI. The uploaded certificate file is stored in the directory `/var/mps/tenants/\<tenant_path>/ns_ssl_keys` in NetScaler Console.

  The certificate key file is added to the list of certificate keys managed by NetScaler Console.
- `certkey`: This type is used to select SSL certificates from the NetScaler Console certificate store. This store lists the existing SSL certificates that are uploaded to your NetScaler Console server. So, you can store SSL certificates at one place that is the NetScaler Console certificate store and reuse them whenever required.

  When creating a configuration pack, a user can add or select SSL certificates from the certificate store. Also, the user can select the same certificate for multiple config packs.
- `file`: Represents a file.
- `object`: This type is used to group several related parameters under a parent element. Specify the parent parameter the type as "object". A parameter of type "object" can have a nested "parameters" section to describe the parameters it contains.
- `another StyleBook`: When you use this type of parameter, then this parameter expects its value to be in the form of the parameters defined in the StyleBook denoting its type.

A parameter can also have a `type` that is the list of types. To do so, add `[]` at the end of the type. For example, if the `type` attribute is `string[]`, this parameter takes a list of strings as

© 1997–2026 Citrix Systems, Inc. All rights reserved.

input. You can provide one, two, or several strings for this parameter when creating a configuration from this StyleBook.

Mandatory? Yes

'network'

For `type: ipaddress`, you can specify the `network` attribute to auto-allocate an IP address from an NetScaler Console IPAM network.

NetScaler Console auto-allocates an IP address from the `network` attribute when you create a StyleBook configuration.

Example:

```
name: virtual-ip

label: "Load Balancer IP Address"

type: ipaddress

network: "network-1"

required: true
```

In this example, the `virtual-ip` field auto-allocates an IP address from `network-1`. The IP address is released back to the network when the configuration is deleted.

'dynamic-allocation'

The `dynamic-allocation` attribute is added in the parameter definition of `type:ipaddress`. Use this attribute to dynamically list the NetScaler Console IPAM networks. This attribute can take either `true` or `false` as an input. For `type: ipaddress`, specify the `dynamic-allocation: true` attribute to dynamically list the NetScaler Console IPAM networks that are in NetScaler Console. In the configuration pack creation form, you can do the following:

1. Select the required IPAM network from the list.
2. Specify an IP address that you want to allocate from the selected IPAM network.

   If no IP address is specified, the NetScaler Console auto-allocates an IP address from the selected IPAM network.

Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-

  name: virtual-ip

  label: "Load Balancer IP Address"

  type: ipaddress

  dynamic-allocation: true

  required: true
```

In this example, the `virtual-ip` field lists the NetScaler Console IPAM networks that are in NetScaler Console. Select a network from the list to auto-allocate an IP address from the network. The IP address is released back to the network when the configuration is deleted.

'key'

Specify true or false to indicate if this parameter is a key parameter for the StyleBook.

A StyleBook can have one or more parameters defined as the "key" parameter. The **Configuration > Config Packs** page displays the parameter's value as a **Display Key**.

When you create different config packs from the same StyleBook, each configuration can have a different value for this parameter. This value appears as the display key on the GUI. With this key, you can sort or filter the configuration pack.

Example:

```
parameters:

  - name: example-appname

    type: string

    label: Application Name

    required: true

    key: true
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When a StyleBook user creates a configuration pack, the value for the parameter `example-appname` appears as the display key. The StyleBook user can use this key to identify this configuration pack.

NOTE

The **Config Key** of a configuration pack overwrites the key attribute set on any of its parameters. So, if a user enters a value for the Config Key, this value appears in the **Display Key** column.

Default value is false.

Mandatory? No

'required'

Specify true or false to indicate whether a parameter is mandatory or optional. If it is set to true, the parameter is mandatory and the user has to provide a value for this parameter when creating configurations.

The NetScaler Console GUI forces the user to provide a valid value for this parameter.

Default value is false.

Mandatory? No

'allowed-values'

Use this attribute to define a list of valid values for a parameter, when the type is set to "string."

When creating a configuration from the NetScaler Console GUI, the user is prompted to select a parameter value from this list. This list is static, the user can only select a value from the list. If you want to allow the user to add values to the list, use the `allow-new-values` attribute.

NOTE

If you want to display the list values as radio options, set the `layout` attribute.

Example 1:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-

      name: ipaddress

      type: string

      allowed-values:

            -  SOURCEIP

            -  DEST IP

            -  NONE
```

Example 2:

```
-

      name: TCP Port

      type: tcp-port

      allowed-values:

            -  80

            -  81

            -  8080
```

Example 3:

List of `tcp-ports`, where each element of the list can only have values specified in `allowed-values`.

```
-

      name: tcpports

      type: tcp-port[]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      allowed-values:
            -  80
            -  81
            -  8080
            -  8081
```

Mandatory? No

'allow-new-values'

Use this attribute to add a dynamic list for a parameter. When creating or updating a configuration from the NetScaler Console GUI, the user can add values to the list.

Specify true if you want the user to add a value to the parameter list. You can use the `allow-new-values` and `allowed-values` attributes in a combination. This combination allows you to define a list of suggested values for a parameter and also accept new values.

```
-
      name: port
      type: tcp-port
      allowed-values:
            -  80
            -  81
            -  8080
      allow-new-values: true
```

In this example, a user can either select from 80, 81, 8080, or enter a new value for the parameter `port` while creating or updating a configuration pack.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

'default'

Use this attribute to assign a default value to an optional parameter. When a user creates a configuration without specifying a value, the default value is used.

The parameter takes no value if the following conditions are met:

- The parameter has no default value.
- A user does not provide a value for the parameter.

Example 1:

```
-

      name: timeout

      type: number

      default: 20
```

Example 2:

To list the default values of the parameter:

```
-

      name: protocols

      type: string[]

      default:

            -  TCP

            -  UDP

            -  IP
```

Example 3:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-

      name: timeout

      type: number

      default: 20
```

Example 4:

```
-

      name: tcpport

      type: tcp-port

      default: 20
```

Mandatory? No

'pattern'

Use this attribute to define a pattern (regular expression) for the valid values of this parameter, when the type of the parameter is "string."

Example:

```
-

      name: appname

      type: string

      pattern: "[a-z]+"
```

Mandatory? No

'min-value'

Use this attribute to define the minimum value for parameters of type `number` or `tcp-port`.

Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-

      name: audio-port

      type: tcp-port

      min-value: 5000
```

The `min-value` of numbers can be negative. However, the `min-value` for `tcp-port` must be positive.

Mandatory? No

'max-value'

Use this attribute to define the maximum value for parameters of type `number` or `tcp-port`.

Ensure the maximum value is greater than the minimum value, if defined.

Example:

```
-

      name: audio-port

      type: tcp-port

      min-value: 5000

      max-value: 15000
```

Mandatory? No

'min-length'

Use this attribute to define the minimum length of values accepted for a parameter of type "string."

Ensure the minimum length of the characters defined as values are greater or equal to zero.

Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-

      name: appname

      type: string

      min-length: 3
```

Mandatory? No

'max-length'

Use this attribute to define the maximum length of values accepted for a parameter of type "string."

Ensure the maximum length of the values are greater or equal to the length of the characters defined in `min-length`.

Example:

```
-

      name: appname

      type: string

      max-length: 64
```

Mandatory? No

'min-items'

Use this attribute to define the minimum number of items in a parameter that is a list.

Ensure the minimum number of items are greater or equal to zero.

Example:

```
-

      name: server-ips

      type: ipaddress[]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      min-items: 2
```

Mandatory? No

'max-items'

Use this attribute to define the maximum number of items in a parameter that is a list.

Ensure the maximum number of items are greater than the minimum number of items if defined.

Example:

```
-

      name: server-ips

      type: ipaddress[]

      min-items: 2

      max-items: 250
```

Mandatory? No

'gui'

Use this attribute to customize the layout of the parameter in the NetScaler Console GUI.

Mandatory? No

'columns'

This attribute is a subattribute of the `gui` attribute. Use this attribute to define the number of columns to display the `type: object[]` parameters in the NetScaler Console GUI.

Mandatory? No

'updatable'

This attribute is a subattribute of the `gui` attribute. Use this attribute to specify whether the parameter can be updated after the configuration is created. Set this attribute only on simple parameter types such as string, boolean, or number.

If the value is set to `false`, the parameter field is grayed out when you update the configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mandatory? No

'collapse_pane'

This attribute is a subattribute of the `gui` attribute. Use this attribute to specify whether the pane defining the layout of this object parameter is collapsible.

If the value is set to true, the user can expand or collapse the child parameters under this parent parameter.

Example:

```
gui:


 collapse_pane: true


 columns: 2
```

Example of a complete parameters section:

```


parameters:


   -


      name: name


      label: Name


      description: Name of the application
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      type: string

      required: true

  -

      name: ip

      label: IP Address

      description: The virtual IP address used for this application

      type: ipaddress

      required: true

  -

      name: svc-servers

      label: Servers
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
type: object\[\]

required: true

parameters:

  -

        name: svc-ip

        label: Server IP

        description: The IP address of the server

        type: ipaddress

        required: true

  -

        name: svc-port
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            label: Server Port

            description: The TCP port of the server

            type: tcp-port

            default: 80

        -

            name: lb-alg

            label: LoadBalancing Algorithm

            type: string

            allowed-values:

               - ROUNDROBIN

               - LEASTCONNECTION
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        default: ROUNDROBIN

    -

        name: enable-healthcheck

        label: Enable HealthCheck?

        type: boolean

        default: true
```

The following is an example that defines all the attributes of a list and the values explained in earlier sections:

```
    -

        name: features-list

        type: string[]

        min-length: 1
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            max-length: 3


            min-items: 1


            max-items: 3


            pattern: "\[A-Z\]+"


            allowed-values:


              - SP


              - LB


              - CS


            default:


              - LB
```

'layout'

This attribute is a subattribute of the `gui` attribute. Use this attribute to display the list values as radio buttons. Set the `layout` attribute to `radio` in the parameter section of a StyleBook

© 1997–2026 Citrix Systems, Inc. All rights reserved.

definition. It applies to the parameter that has the `allowed-values` attribute. When you create a configuration pack, the NetScaler Console GUI displays the values in the `allowed-values` list as radio buttons.

Example:

```
-

    gui:

        layout: radio

    allowed-values:

        - One

        - Two

        - Three
```

The One, Two, and Three values appear as radio buttons in the NetScaler Console GUI.

'dependent-parameters'

This attribute is a subattribute of the `gui` attribute. It dynamically controls the parameter's appearance or its initial value in the StyleBook configuration form based on the value specified in another parameter.

Specify this attribute on a source parameter that controls the parameter's behavior on the form. You can include multiple conditions that control other parameters. For example, a source parameter `protocol` can have a dependent-parameter `certificate`, which only appears if the `protocol` parameter value is `SSL`.

Each condition can have the following attributes:

- **target-parameter**: Specify the target parameter to which this condition applies.
- **matching-values**: Specify the list of values of the source parameter that trigger the action.
- **action**: Specify one of the following actions on the targeted parameter:
  - `read-only`: The parameter is made read-only.
  - `show`: The parameter appears in the form if it is hidden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `hide`: The parameter is removed from the form.
- `set-value`: The parameter value is set to the value specified in the value attribute.

- **value**: The value of the target parameter if the action is `set-value`.

When a user input matches the specified values on the source parameter, the target parameter's appearance or value changes according to the specified action.

Example:

```
-

   name: lb-virtual-port

   label: "Load Balanced App Virtual Port"

   description: "TCP port representing the Load Balanced application"

   type: tcp-port

   gui:

     updatable: false

     dependent-parameters:

           -

             matching-values:

               - 80

             target-parameter: $parameters.lb-service-type

             action: set-value

             allowed-values:

             - HTTP

             - TCP

             - UDP
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    default: 80
```

In this example, the dependent parameter is specified under the `lb-virtual-port` parameter (source parameter).

When the source parameter value is set to `80`, the `lb-service-type` parameter triggers the `set-value` action. As a result, a user is allowed to select one of the following options:

- HTTP
- TCP
- UDP

`is_policy_expression`

This attribute is a subattribute of the `gui` attribute. Use this attribute to enable the policy expression editor to compose a policy expression. Set the `is_policy_expression` to `true` in the parameter definition. This attribute can be used only on parameters of type 'string'.

Example:

```
parameters:
  -


    name: expression
    type: string
    label: Expression
    required: true
    gui:
      is_policy_expression: true
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Parameters-default-sources construct

You can use this construct to reuse parameter definitions from other StyleBooks.

Consider a scenario where a parameter or a group of parameters is used repeatedly in multiple StyleBooks. To avoid redefining these parameters, each time you want to create a new StyleBook, you can define them once, and then import their definitions into the StyleBooks that need these parameters by using the **parameters-default-sources** construct.

For example, if many of your StyleBooks need to configure a virtual IP, you might have to define the same parameters related to virtual IPs in each new StyleBook you create. Instead, you can create a separate StyleBook called, for example, `vip-params` where you define all the parameters related to it as shown in the following example:

```
-


name: vip-params


namespace: com.acme.commontypes


version: "1.0"


description: This StyleBook defines a typical virtual IP config.


private: true


schema-version: "1.0"


parameters:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        -

            name: lb-appname

            label: Load Balanced Application Name

           description: Name of the Load Balanced application

            type: string

            required: true

        -

            name: lb-virtual-ip

            label: Load Balanced App Virtual IP address

            description: Virtual IP address representing the Load Balanced
application
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            type: ipaddress


            required: true


        -


            name: lb-virtual-port


            label: Load Balanced App Virtual Port


            description: TCP port representing the Load Balanced
application


            type: tcp-port


            default: 80


        -


            name: lb-service-type


            label: Load Balanced App Protocol
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        description: Protocol used for the Load Balanced application.

        type: string

        default: HTTP

        required: true

        allowed-values:

             - HTTP

             - SSL

             - TCP
```

Then, you can create other StyleBooks that use these parameters

```
    -

    name: acme-biz-app

    namespace: com.acme.stylebooks
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
     version: "1.0"

     description: This stylebook defines the NetScaler configuration for
Biz App

     schema-version: "1.0"

     import-stylebooks:

       -

          namespace: com.acme.commontypes

          prefix: cmtypes

          version: "1.0"

     **parameters-default-sources:**

**            - cmtypes::vip-params**
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    parameters:

        -

          name: monitorname

          label: Monitor Name

          description: Name of the monitor

          type: string

          required: true

        -

          name: type

          label: Monitor Type

          description: Type of the monitor
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            type: string


            required: true


            allowed-values:


              - PING


              - TCP


              - HTTP


              - HTTP-ECV


              - TCP-ECV


              - HTTP-INLINE
```

In the StyleBook, `acme-biz-app`, first, the namespace and version of the `vip-params` StyleBook is imported by using the "import-stylebooks" section. Then the **parameters-default-sources** construct is added, and the StyleBook name, that is, `vip-params` is specified. This parameter has the same effect as defining the parameters of the `vip-params` StyleBook directly in this StyleBook.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can include parameters from multiple StyleBooks because the parameters-default-sources is a list, and each item in the list is expected to be a StyleBook.

In addition to including parameters from other StyleBooks, you can also define your own parameters by using the parameters section. The complete list of parameters of the StyleBook is the combination of parameters included from other StyleBooks and parameters defined in this StyleBook. Therefore, the expression **$parameters** refers to this combination of parameters.

If a parameter is defined both in an imported StyleBook and in the current StyleBook, the definition in the current StyleBook overrides the definition imported from another StyleBook. You can use this approach effectively by customizing a few of the imported parameters if necessary, while using the rest of the imported parameters as they are.

The parameters-default-sources construct can also be used in nested parameters as shown:

```
parameters:

    -

      name: vip-details

      label: Virtual IP details

      description: Details of the Virtual IP

      type: object

      required: true
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      parameters-default-sources:



            - cmtypes::vip-params
```

This approach is similar to having the parameters of the StyleBook `vip-params` added directly as child parameters of the `vip-details` parameter in this StyleBook.

Parameters-source construct

Using the `parameters-source` construct, you can control how the imported parameters appear on the GUI while creating a configuration pack. The following is an example StyleBook to describe this construct:

```
parameters:

  -

    name: appname

    label: "LBVserver Name"

    description: "Name of the Load Balancer"

    type: string

    required: true

  -

   parameters-source: stlb::lb

  -

    name: vip-ipaddress

    label: "Load Balancer IP Address"

    description: "IP Address of the Load Balancer VIP"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: ipaddress

    required: true
```

In this example, the `parameters-source` construct is added in the `parameters` section. The `parameters-source` contains a value equivalent to a list item in the `parameters-default-sources` section. With `parameters-source`, you can import parameters from different StyleBooks in the desired positions and render them on the GUI. Whereas the `parameters-default-sources` section imports the attributes and only renders in the beginning of the GUI.

Parameter conditions

In a StyleBook definition, parameters define the input that StyleBook users provide to create a configuration pack. Sometimes, you might want to modify the parameters behavior like the following:

- Show some parameters to a user only if a condition is met.
- The allowed values of one parameter to depend on another parameter.
- Set a parameter as mandatory only under certain conditions.

In these cases, use the `parameters-conditions` section to define parameter conditions. A parameter condition has the following attributes:

- `target`: Specify the parameter to which you want to apply a condition.
- `action`: Specify what actions to take if the target parameter matches the condition. This feature supports the following actions:
  - Show or hide parameters
  - Set a default value
  - Set as a required field
  - Set allowed values
  - Set the parameter's label
  - Set the parameter's description
  - Collapse or expand parameter's pane
  - Set the parameter's pattern
- `condition`: Specify a condition that has to be met.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `value`: Set the values for the target parameters attribute depending on the action.

NOTE

Currently, the parameter conditions cannot be applied for the parameters within list objects.

'show' or 'hide'

When the action is `show` and the specified condition returns `True`, the target parameter appears on the GUI.

When the action is `hide` and the specified condition returns `True`, the target parameter disappears from the GUI.

Example:

```
parameters-conditions:

  -

   target: $parameters.security-settings.cert-details

   action: show

   condition: $parameters.protocol in ["SSL", "SSL-BRIDGE"]
```

At first, the certificate details are hidden for the `security-settings` parameter. When a user selects SSL or SSL-Bridge protocols, the certificate details appear.

'set-default'

When the action is `set-default` and the specified condition returns `True`, the target parameter's value is set to the default value.

Example 1:

```
parameters-conditions:

  -

   target: $parameters.port
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    action: set-default

    condition: $parameters.protocol == "SSL"

    value: 443

   -

    target: $parameters.port

    action: set-default

    condition: $parameters.protocol != "SSL"

    value: 80
```

Example 2:

```
parameters-conditions:

  -

    target: $parameters.port

    action: set-default

    value: if-then-else($parameters.protocol == "SSL", 443, 80)
```

When a user selects the **SSL** protocol, the default port value is set to `443`. For other protocols, the default port value is set to `80`. Example 1 and 2 gives you the same result.

'set-required'

When the action is `set-required` and the specified condition returns `True`, the target parameter becomes a required field to create a configuration pack.

```
parameters-conditions:

  -

    target: $parameters.security-settings.cert-details
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
   action: set-required

   condition: $parameters.protocol in ["SSL", "SSL-BRIDGE"]
```

At first, the certificate details might not be required for the `security-settings` parameter. When a user selects **SSL** or **SSL-Bridge** protocols, the certificate details become a required field to create a configuration pack.

'set-allowed-values'

When the action is `set-allowed-values` and the specified condition returns `True`, the target parameter allows you to select only specified values.

Example-1:

```
parameters-conditions:

  -

   target: $parameters.app-name

   action: set-allowed-values

   value:

    - "SSL"

   condition: $parameters.lb-virtual-port ==  443
```

When a user specifies `443` as a load-balancer virtual port, the application's name allows only **SSL** option.

Example-2;

```
parameters:

    -

      name: root-certificates

      label: "Root Certificates"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      type: object[]
      parameters:
        -
          name: certkey-name
          label: "SSL Root CertKey Name"
          type: string
          required: true
    -
      name: im-certificates
      label: "Intermediate Certificates"
      type: object[]
      parameters:
        -
          name: certkey-name
          label: "Name of Intermediate CertKey"
          type: string
          required: true
        -
          name: link-options
          label: "Link to Root or Intermediate CertKey?"
          type: string
          allowed-values:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            - Root
            - Intermediate
          default: Root
          required: true
        -
          name: link-certkey
          label: "Linked to Root/Intermediate CertKey Name"
          type: string
          required: true
parameters-conditions:
  -
    repeat: $parameters.im-certificates
    repeat-item: imcert
    parameters-conditions:
    -
      target: $imcert.link-certkey
      action: set-allowed-values
      condition: $imcert.link-options == "Root"
      value: $parameters.root-certificates[*].certkey-name
    -
      target: $imcert.link-certkey
      action: set-allowed-values
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      condition: $imcert.link-options == "Intermediate"

      value: $parameters.im-certificates[*].certkey-name
```

This example is about setting a value for an SSL certificate. The repeat construct in parameter conditions iterates over all the intermediate certificates (`im-certificates`) and checks the `link-options` parameter of each certificate.

If the `link-options` parameter matches a certain value, the allowed values in the `link-certkey` parameter are added to the respective certificate list.

For example, if the `link-options` parameter is `Root`, the allowed values in the `link-certkey` parameter are added to the `root-certificate` list.

The following notations are used to add certificates to the list:

- For root certificates:

  ```
  $parameters.root-certificates[*].certkey-name
  ```

- For intermediate certificates:

  ```
  $parameters.im-certificates[*].certkey-name
  ```

'set-label'

When the action is `set-label` and the specified condition returns `True`, the target parameter's label changes to the specified text.

Example:

```
parameters-conditions:

  -

   target: $parameters.app-name

   action: set-label
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
   value: if-then-else($parameters.lb-service-type == "TCP",
"TCPApp","UDPApp")
```

When a user selects the load-balancer protocol as **TCP**, the application's label changes to **TCPApp**. If the user selects a different option, the application's label changes to **UDPApp**.

'set-description'

When the action is `set-description` and the specified condition returns `True`, the target parameter's description changes to the specified text. This description appears in the tool tip of a target parameter.

Example:

```
parameters-conditions:

  -

   target: $parameters.app-name

   action: set-description

   value: if-then-else($parameters.lb-service-type == "TCP", "Select a TCP
application name","Select a UDP application name")
```

When a user selects the load-balancer protocol as **TCP**, the application's tool tip displays a text: `Select a TCP application name`. If the user selects a different option, the application's description displays `Select a UDP application name`.

'collapse-pane' or 'expand-pane'

When the action is `collapse-pane` and the specified condition returns `True`, the target parameter's pane collapses in the GUI.

When the action is `expand-pane` and the specified condition returns `True`, the target parameter's pane expands in the GUI.

Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
parameters-conditions:

  -

    target: $parameters.security-settings.cert-details

    action: expand-pane

    condition: $parameters.protocol in ["SSL", "SSL-BRIDGE"]
```

At first, the certificate details pane might not be expanded for the `security-settings` parameter. When a user selects **SSL** or **SSL-Bridge** protocols, the certificate details pane expands on the GUI.

'set-pattern'

When the action is `set-pattern` and the specified condition returns `True`, the target parameter field is set to the specified pattern.

Example:

```
parameters-conditions:

  -

    target: $parameters.app-name

    action: set-pattern

    value: "[a-z]+"
```

In this example, the application's name allow only lowercase alphabetical characters.

Nested parameter conditions

In a StyleBook definition, you can specify a parameter condition within a parameter condition. These conditions are called as nested parameter conditions and use a repeat construct to define these conditions. The nested parameter conditions are useful when you want to apply an action for a parameter from another parameter.

Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
parameters-conditions:

  -

    repeat: $parameters.lbvservers

    repeat-item: lbvserver

    parameters-conditions:

      -

        target: $lbvserver.port

        action: set-allowed-values

        condition: $lbvserver.protocol == "HTTPS"

        value: $parameters.ssl-ports
```

In this example, when the user selects the HTTPS protocol for a load balancing virtual server, the port values are dynamically populated. And, it applies for each load balancing virtual servers in the list.

Substitutions

Substitutions are used to define shorthand names that can replace complex expressions in the StyleBook making the StyleBook more readable.

Substitutions are also useful when the same expression or value is used repeatedly in the StyleBook, for example, a constant value. Using a substitution name for a parameter allows you to update only the substitution value instead of updating all occurrences of the parameter in the StyleBook which might be prone to error.

Substitutions are also used for defining mappings between values as described in examples later in this document.

Each substitution in the list is made up of a key and a value. The value can be a simple value, an expression, a function, or a map.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In the following example, two substitutions are defined. The first one is `http-port` that can be used as a shorthand for 8181. By using a substitution, you can refer to this in the rest of the StyleBook as **$substitutions.http-port** instead of 8181.

substitutions:

```
http-port: 8181
```

This allows you to specify a mnemonic name to a port number and define this port number in one place in the StyleBook, irrespective of the number of times it is used. If you want to modify the port number to 8080, you can modify it in the substitution section, and the change takes effect wherever the mnemonic name `http-port` is used. The following example shows how a substitution is used in a component.

```
components:

 -

     name: my-lbvserver-comp

     type: ns::lbvserver

     properties:

          name: $parameters.name + "-lb"

          servicetype: HTTP

          ipv46: $parameters.ip
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
          port: $substitutions.http-port


          lbmethod: $parameters.lb-alg
```

A substitution can also be a complex expression. The following example shows how two substitutions use expressions.

```
substitutions:


  app-rule: HTTP.REQ.HEADER("X-Test-Application").EXISTS


  app-name: str("acme-") + $parameters.name + str("-app")
```

A substitution expression can also use existing substitution expressions as shown in the following example.

```
substitutions:


  http-port: 8181


  app-name: str("acme-") + $parameters.name + str($substitutions.http-
port) + str("-app")
```

Another useful feature of substitutions is maps, where you can map keys to values. The following is an example of a map substitution.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
substitutions:


    secure-port:


        true: int("443")


        false: int("80")


    secure-protocol:


        true: SSL


        false: HTTP
```

The following example shows how to use the maps secure-port and secure-protocol.

```
components:


 -


     name: my-lbvserver-comp


     type: ns::lbvserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
     properties:

          name: $parameters.name + "-lb"

          servicetype: $substitutions.secure-protocol[$parameters.is-
secure]

          ipv46: $parameters.ip

          port: $substitutions.secure-port[$parameters.is-secure]

          lbmethod: $parameters.lb-alg
```

Here, if the user of the StyleBook specifies the Boolean value "true" to the parameter `is-secure`, or selects the check box corresponding to this parameter in the NetScaler Console GUI, the `servicetype` property of this component is assigned the value **SSL** and the port property is assigned the value **443**. However, if the user specifies "false" for this parameter or clears the corresponding check box in the NetScaler Console GUI, the `servicetype` property is assigned the value **HTTP** and the port is assigned the value **80**.

The following example shows how to use substitutions as a function. A substitution function can take one or more arguments. Arguments can be of simple type for example, string, number, `ipaddress`, boolean, and other types.

substitutions:

form-lb-name(name): $name + "-lb"

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In this example, we define a substitution function "form-lb-name" that takes a string argument called "name" and uses it to create a string that suffixes "-lb" to the string in the name argument. An expression using this substitution function can be written as:

`$substitutions.form-lb-name("my")`

It returns `my-lb`

Consider another example:

substitutions:

`cspol-priority(priority): 10100 - 100 * $priority`

The substitution `cspol-priority` is a function that takes an argument called priority and uses it to calculate a value. In the rest of the StyleBook, this substitution can be used as shown in the following example:

```
components:


  -


    name: cspolicy-binding-comp


    type: ns::csvserver_cspolicy_binding


    condition: not $parameters.is-default


    properties:


         name: $parameters.csvserver-name
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        policyname: $components.cspolicy-comp.properties.policyname


        priority: $substitutions.cspol-
priority($parameters.pool.priority)
```

The following is an example of a substitution called `slist` whose value is a list:

```
substitutions:


  slist:


    - a


    - b


    - c
```

The value of a substitution can also be a dictionary of key-value pairs as seen in the following example of a substitution called `sdict` below:

```
substitutions:


  sdict:


    a: 1
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    b: 2

    c: 3
```

You can create more complex attributes by combining the lists and dictionaries. For example, a substitution called `slistofdict` returns a list of key - value pairs.

```
  slistofdict:

    -

      a: $parameters.cs1.lb1.port

      b: $parameters.cs1.lb2.port

    -

      a: $parameters.cs2.lb1.port

      b: $parameters.cs2.lb2.port
```

But, in the following example, a substitution `sdictoflist` returns a key-value pair, where the value itself is another list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
sdictoflist:

  a:

    - 1

    - 2

  b:

    - 3

    - 4
```

In components, these substitutions may be used in condition, properties, repeat, repeat-condition constructs.

The following example of a component shows how a substitution can be used to specify the properties:

```
  properties:

    a: $substitutions.slist

    b: $substitutions.sdict
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    c: $substitutions.slistofdict


    d: $substitutions.sdictoflist
```

A use case for defining a substitution whose value is a list or a dictionary is when you are configuring a content switching virtual server and multiple load balancing virtual servers. Since all lb virtual servers tied to the same cs virtual server might have an identical configuration, you can use the substitution list and dictionary to build this configuration to avoid repeating that configuration for each lb virtual server.

The following example shows the substitution and the component in the `cs-lb-mon` StyleBooks to create a content switching virtual server configuration. While constructing the properties of `cs-lb-mon` StyleBooks, the complex substitution "lb-properties" specifies the properties of the lb virtual servers associated with the cs virtual server. The "lb-properties" substitution is a function that takes the name, service type, virtual IP address, port, and servers as parameters and generates a key-value pair as the value. In `cs-pools` component, we assign the value of this substitution to a lb-pool parameter for each pool.

```
substitutions:


  cs-port[]:


    true: int("80")


    false: int("443")


  lb-properties(name, servicetype, vip, port, servers):
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    lb-appname: $name


    lb-service-type: $servicetype


    lb-virtual-ip: $vip


    lb-virtual-port: $port


    svc-servers: $servers


    svc-service-type: $servicetype


    monitors:


      -


        monitorname: $name


        type: PING


        interval: $parameters.monitor-interval
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        interval_units: SEC


        retries: 3


components:


  -


    name: cs-pools


    type: stlb::cs-lb-mon


    description: | Updates the cs-lb-mon configuration with the different
pools provided. Each pool with rule result in a dummy LB vserver, cs
action, cs policy, and csvserver_cspolicy_binding configuration.


    condition: $parameters.server-pools


    repeat: $parameters.server-pools


    repeat-item: pool


    repeat-condition: $pool.rule
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    repeat-index: ndx

    properties:

      appname: $parameters.appname + "-cs"

      cs-virtual-ip: $parameters.vip

      cs-virtual-port: $substitutions.cs-port($parameters.protocol ==
"HTTP")

      cs-service-type: $parameters.protocol

      pools:

        -

          lb-pool: $substitutions.lb-properties($pool.pool-name, "HTTP",
"0.0.0.0", 0, $pool.servers)

          rule: $pool.rule
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        priority: $ndx + 1
```

Substitution map

You can create substitutions that map keys to values. For example, consider a scenario where you want to define the default port (value) to be used for each protocol (key). For this task, write a substitution map as follows.

```
substitutions:

    port:

        HTTP: 80

        DNS: 53

        SSL: 443
```

In this example, HTTP is mapped to 80, DNS is mapped to 53, and SSL is mapped to 443. To retrieve the port of a certain protocol that is given as a parameter, use the expression

$substitutions.port

The expression returns a value based on the protocol specified by the user.

- If the key is HTTP, the expression returns 80
- If the key is DNS, the expression returns 53
- If the key is SSL, the expression returns 443
- If the key is not present in the map, the expression does not return any value

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Iterate through substitution lists

In the following example, the StyleBook iterates through a substitution list called `apps` to create a set of lbvserver components and their corresponding service groups and bound servers.

```
substitutions:

  apps:

    -

      name: lb1

      vip: 1.2.3.4

      vport: 80

      protocol: HTTP

      servers:

        -

          ip: 10.8.11.11

          port: 8080

        -

          ip: 10.8.11.12

          port: 8080

    -

      name: lb2

      vip: 1.2.3.5

      vport: 81

      protocol: HTTP
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      servers:
        -
          ip: 10.9.11.28
          port: 8080
        -
          ip: 10.9.11.29
          port: 8181
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    repeat: $substitutions.apps
    repeat-item: app
    properties:
      name: $app["name"]
      ipv46: $app["vip"]
      port: $app["vport"]
      servicetype: $app["protocol"]
    components:
      -
        name: servicegroup-comp
        type: ns::servicegroup
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        properties:
          servicegroupname: $parent.properties.name + "-svg"
          servicetype: HTTP
        components:
          -
            name: servers-comp
            type: ns::server
            repeat: $app["servers"]
            repeat-item: server
            properties:
              name: $server["ip"]
              ipaddress: $server["ip"]
            components:
              -
                name: servicegroup-servicegroupmember-binding-comp
                type: ns::servicegroup_servicegroupmember_binding
                properties:
                  servicegroupname:
$parent.parent.properties.servicegroupname
                  servername: $parent.properties.name
                  port: $server["port"]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Components

The Components construct in a StyleBook is considered as the most important section in the StyleBook. In this section, you define the configuration objects that have to be created. Using this construct, you can build one or multiple configuration objects of the same type.

The components construct can use the input provided in the parameters section to adapt the configuration generated by the StyleBook. This is an optional section, although most StyleBooks have a components section.

The following table describes the main attributes of a component.

ATTRIBUTE	DESCRIPTION
`name`	The name of the component. You can specify an alphanumeric name. The name must begin with an alphabet, and can include extra alphabets, numbers, hyphen (-), or underscore (_).
`description`	A description of the role of this component in the StyleBook.
`type`	The type determines what properties this component provides. Components have two kinds of types: **Built-in type**: This type is provided by the system and you do not have to define it, for example, the NITRO entity types `lbvserver` or `servicegroup`. When a component has a built-in type attribute, it creates a configuration object of that type on the NetScaler. For example, if a component refers to the built-in type `lbvserver`, this component creates a load balancing virtual server on the NetScaler instance that is the target of the configuration. **Composite type**: This type refers to an existing StyleBook that you created and imported into NetScaler Console. When a component has a composite type attribute, it creates all the configuration objects, which are specified in the referenced StyleBook, on the NetScaler instance that is the target of the configuration. This enables

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUTE	DESCRIPTION
	you to combine multiple StyleBooks where each StyleBook creates a part of the final configuration. For more information about composite StyleBooks, see Create a Composite StyleBook.
`meta-properties`	Meta-properties define the actions to be taken on NetScaler objects. It can take static or dynamic values as a valid meta-property action. When you specify expressions for a meta-property, it dynamically applies the valid meta-property actions for NetScaler objects. This attribute can be used in a StyleBook when you want do non-CRUD operations on NetScaler objects. For more information, see Create a StyleBook to perform non-CRUD operations.
`properties`	The sub-attributes that can be used for a component type attribute. The properties that are valid for a component are dictated by its type. For a built-in type, these are the properties or attributes of the corresponding NITRO object. For a component whose type is another StyleBook, that is, a composite type, the properties correspond to the parameters defined in that StyleBook.

Example:

```
components:

   -

     name: my-lbvserver-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: ns::lbvserver

    properties:

       name: $parameters.name

       servicetype: HTTP

       ipv46: $parameters.ip

       port: 80

       lbmethod: $parameters.lb-alg
```

In this example, you have defined a component called `my-lbvserver-comp`. This component is of type ns::lbvserver (a built-in type), where "ns" is the prefix that refers to the namespace `netscaler.nitro.config` and version 10.5 that you had specified in the import-stylebooks section, and `lbvserver` is a NITRO resource in this namespace.

The properties in this section include four mandatory and one optional attribute (`lbmethod`) of the `lbvserver` resource and allows you to specify values for these attributes. In this example, you are specifying static values for `servicetype` and port while the name, ipv46, and `lbmethod` properties get their values from the input parameters. You refer to the parameter names defined in the parameters section by using the `$parameters.\<name>` notation, for example, $parameters.ip.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To learn more about all the available NetScaler NITRO resources and their attributes/properties, see the NetScaler NITRO REST API documentation.

NOTE

You have to use lower case for the attribute names of NITRO resource types (its component properties). Otherwise, the import of a StyleBook will fail.

Helper components

The primary use of the components section in a StyleBook is to generate configuration objects through NITRO built-in types or another StyleBook that creates the actual configuration objects. The helper components do not build configuration objects by themselves. Helper components take the inputs from other sections like parameter objects, properties of other components, or outputs of other components and transform them into other forms. This can be later used by other components to generate the actual configuration objects. A helper component can be of two types: object type or another StyleBook that does not contain a component section.

The following example shows a snippet of a StyleBook that is used to create a load balancing server with monitor (`lb-mon-comp`) on a NetScaler instance.

```
parameters:


  -


    name: appname


    type: string


  -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    name: ips

    type: ipaddress[]

  -

    name: vip

    type: ipaddress

components:

  -

    name: help-comp

    type: cmtypes::server-ip-port-params

    repeat:

      repeat-list: $parameters.ips
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      repeat-item: server-ip


    properties:


      ip: $server-ip


      port: 80


-


    name: lb-mon-comp


    type: stlb::lb-mon


    properties:


      lb-appname: $parameters.appname


      lb-virtual-ip: $parameters.vip


      lb-virtual-port: 80
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    lb-service-type: HTTP


    svc-service-type: HTTP


    svc-servers: $components.help-comp.properties
```

The parameters section allows you to enter the name of the application and the IP addresses of the load balancing servers. In the `lb-mon-comp` component section, the `svc-servers` parameter of `lb-mon` StyleBook expects a list of objects where each item has two sub-parameters `ip` and port.

However, the parameters section of this StyleBook only accepts the server IPs through $parameters.ips. The StyleBook assumes that all servers are running on port 80. To create the load balancing configuration using `lb-mon` StyleBook, you must transform the $parameters.ips to a list of objects. This is achieved using the helper component, help-comp in the above example. The help-comp component is of type `server-ip-port-params` StyleBook. This StyleBook does not have any components. As a result, it does not create any configuration objects. The help-comp creates a repeat list over $parameters.ips and constructs an object which consists of `ip` and port (that is set to a static 80) for each item of $parameters.ips. Thus, help-comp transforms a list of IP addresses into a list of objects that can be later used in `lb-mon-comp` to assign `svc-servers` property. The result of the help-comp is assigned to the `svc-servers` property of `lb-mon-comp`.

Optional properties

Sometimes, a property of a component takes its value from an expression, which can be a simple expression such as a parameter reference, or a more complex one. Setting this property value is optional in the component. You can choose to set the property value only if the expression returns an actual value, else you can choose not to set this property.

For example, consider that one of the properties you want to set is the `lbmethod` (load balancing algorithm) of a component whose type is ns::lbvserver. The value of the property `lbmethod` is taken from a parameter value provided by the user, as shown below:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
components


  -


      name: lbvserver_comp


      type: ns::lbvserver


      properties:


        name: $parameters.lb-appname + "-lb"


        servicetype: $parameters.lb-service-type


        ipv46: $parameters.lb-virtual-ip


        port: 80


        lbmethod: $parameters.lb-advanced.algorithm
```

Now, consider that the parameter **lb-advanced.algorithm** is an optional parameter. And, if the user does not provide a value for this parameter because it is optional, the expression **$parameters.lb-advanced.algorithm** evaluates to blank value. Therefore, an invalid value is

© 1997–2026 Citrix Systems, Inc. All rights reserved.

passed for the `lbmethod` property. In order to avoid such a situation, you can annotate the property as optional by suffixing its name with "?" as follows:

```
components


   -


     name: lbvserver_comp


     type: ns::lbvserver


     properties:


       name: $parameters.lb-appname + "-lb"


       servicetype: $parameters.lb-service-type


       ipv46: $parameters.lb-virtual-ip


       port: 80


       lbmethod?: $parameters.lb-advanced.algorithm
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The use of "?" omits the property if the expression on the right evaluates to nothing, which would be equivalent, in this case, to a component defined as follows:

```
components


  -


    name: lbvserver_comp


    type: ns::lbvserver


    properties:


      name: $parameters.lb-appname + "-lb"


      servicetype: $parameters.lb-service-type


      ipv46: $parameters.lb-virtual-ip


      port: 80
```

Because **lbmethod** is optional, omitting it still makes a valid component. Note that `lbmethod` might take its default value if one is defined in its type "ns::lbvserver."

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Properties-default-sources construct

The properties-default-sources construct is analogous to the parameters-default-sources construct. While the parameters-default-sources construct allows the reuse of existing parameters (from other StyleBooks) in a StyleBook, properties-default-sources construct allows the user to specify properties of a component based on existing sources.

The properties of a component may be distributed across various sections of the StyleBook. For example, the properties may come from object parameters, substitutions that return an object, properties of other components, or outputs of other components. In such cases, you need to redefine the properties that occur in other sections of the StyleBook in the definition of the component. Clearly, this is redundant and can lead to errors. To deal with this problem, properties-default-sources construct can be used. The properties-default-sources construct is a list where each item identifies a source for some properties of the component.

For example, consider a component that creates an `lbvserver` configuration. This component defines the properties of the `lbvserver` as follows.

```
parameters:


  -


    name: lb


    type: ns::lbvserver


components:


  -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    name: lb-comp


    type: ns::lbvserver


    properties:


      name: $parameters.lb.name


      ipv46: $parameters.lb.ipv46


      port: $parameters.lb.port


      servicetype: $parameters.lb.servicetype


      lbmethod: $parameters.lb.lbmethod
```

In the above example, observe that the values for all properties defined in the components section are taken from $parameters.lb object. Though they are taken from a single source, the properties are again defined in the StyleBook. In addition, if a new sub-parameter to $parameters.lb object that is relevant to the configuration of the `lbvserver` is added, you need to update the lb-comp component to add the new property that corresponds to the new sub-parameter.

To avoid redefining properties and to fetch all relevant properties of a component without explicitly list them in the properties section, properties-default-sources construct can be used. The above example can be written as follows.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
parameters:

  -

    name: lb

    type: ns::lbvserver

components:

  -

    name: lb-comp

    type: ns::lbvserver

    properties-default-sources:

      - $parameters.lb
```

In the above example, the use of properties-default-sources construct leads to a reduction in the size of the component definition, and this allows you to concisely define a component. In addition, each time the source of the properties of the component changes, the changes are reflected automatically. For example, when a new property, say `persistencetype`, is added in the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

$parameters.lb object, this property is added to the configuration of lb-comp by default since `persistencetype` is a property of `lbvserver`. Thus, properties-default-sources construct provides a dynamic interface to define the components without worrying about changes happening to the sources of the properties of the component.

Computation of the Properties of the Component

This section discusses on how the properties are fetched if properties-default-sources construct is used in a component. First, the StyleBooks compiler identifies the list of properties for a component based on its type (in the above example, `lbvserver`.) Next, the compiler fetches these properties from the multiple sources in the order that they are defined (in properties-default-sources section of the component). If a property exists in multiple sources then the property appearing in the last source takes precedence over others. Finally, a property fetched by using properties-default-sources construct can be overridden in the properties section of the component. It is important to note that the definition of a component section at least have a properties-default-sources section or a properties section. It may have both.

Nested components

Nesting a component within another component allows the nested component to create its configuration objects by referring to configuration objects or the context created by the parent component. The nested component can create one or more objects for each object created in the parent component. Nesting a component within another component does not indicate any relationship between the configuration objects created. Nesting is a way to facilitate the task of components to construct configuration objects within an existing context of the parent components.

Example:

```
components:


 -


  name: my-lbvserver-comp


  type: ns::lbvserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
properties:

   name: $parameters.name + "-lb"

   servicetype: HTTP

   ipv46: $parameters.ip

   port: 80

   lbmethod: $parameters.lb-alg

   components:

     -

      name: my-svcg-comp

      type: ns::servicegroup

      properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    name: $parameters.name + "-svcgrp"

    servicetype: HTTP

  components:

    -

      name: lbvserver-svg-binding-comp

      type: ns::lbvserver_servicegroup_binding

      properties:

        name: $parent.parent.properties.name

        servicegroupname: $parent.properties.name

          -

            name: members-svcg-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                type: ns::servicegroup_servicegroupmember_binding

                repeat:

                  repeat-list: $parameters.svc-servers

                  repeat-item: srv

                properties:

                  ip: $srv

                  port: str($parameters.svc-port)

                  servicegroupname: $parent.properties.name
```

In this example, multi-level nesting is used. The component `my-lbvserver-comp` has a child component called `my-svcg-comp`. And, the `my-svcg-comp` component has two child components within it. The `my-svcg-comp` component is used to create a service group configuration object on the NetScaler instance by providing values to the attributes of the built-in NITRO resource type "`servicegroup`." The first child component of the `my-svcg` component, `lbvserver-svg-binding-comp`, is used to bind the service group created by its parent component to the load balancing virtual server (`lbvserver`) created by the parent's parent component. The $parent notation, also called the parent reference, is used to refer to entities in the parent components. The second child component, `members-svcg-comp`, is used to bind the list of

© 1997–2026 Citrix Systems, Inc. All rights reserved.

services to the service group created by the parent component. The binding is achieved by using the repeat construct of a StyleBook to iterate over the list of services specified for the parameter `svc-servers`. For information on repeat constructs, see Repeat Construct.

You can also create the same configuration objects without using nesting of components. For more information and examples, see StyleBook to Create a Basic Load Balancing Configuration.

Condition construct

You can make a component conditional by using a condition construct. The value of a conditional construct is a boolean expression that evaluates to true or false. If the condition is true, the component is used to build its configuration objects. If the condition is false, the component is skipped, and no configuration objects are created through it. The boolean expression is often based on parameter values.

Example:

```
components:

      -

        name: servicegroup-comp

        type: ns::servicegroup

        condition: $parameters.svc-server-ips

        properties:

             name: $parameters.name + "-svcgrp"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
              servicetype: HTTP
```

In this example, if the user specifies a value for the optional parameter `svc-server-ips`, then the component, `servicegroup-comp`, is processed by the StyleBook engine. If the condition is false, that is, if the user does not provide a value to this parameter, a null value is assigned to this parameter and evaluates to false, then the StyleBook engine ignores the presence of this component, and no `servicegroup` is created.

Note that the boolean expression can be based on any valid expression supported in StyleBooks (for example, whether another component is present, or whether a parameter has a certain value).

The following example builds the configuration object of NITRO type ns::systemfile if the condition is evaluated to true.

Example:

```
     components

          -

            name: pem_key_files

            type: ns::systemfile

            condition: "$components.der-certificate-files-comp or
$components.pem-certificate-files-comp"

            properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                filecontent: $certificate.keyfile.contents


                fileencoding: "BASE64"


                filelocation: "/nsconfig/ssl"


                filename: $certificate.keyfile.filename
```

In this example, the condition is a complex "or" expression, where you want this configuration object to be created by the StyleBook only if two other components in the StyleBook have been processed (not skipped), therefore, creating a dependency between components.

Repeat construct

You can use the **repeat** construct of a component to build multiple configuration objects of the same type.

In the following example, the **members-svcg-comp** component is used to bind the list of services to the service group created by the parent component. To create a configuration object that binds each server to the service group, use the **repeat** construct to iterate over the list of services specified for the parameter **svc-servers**. During the iteration, the component creates a NITRO object of the type **servicegroup_servicegroupmember_binding** for each service (referred to as **srv** in the **repeat-item** construct) in the service group, and it sets the **ip** attribute in each NITRO object to the IP address of the corresponding service.

Example:

```
components:

  -

      name: my-lbvserver-comp

      type: ns::lbvserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    properties:
        name: $parameters.name + "-lb"
        servicetype: HTTP
        ipv46: $parameters.ip
        port: 80
        lbmethod: $parameters.lb-alg
        components:
            -
               name: my-svcg-comp
               type: ns::servicegroup
               properties:
                    name: $parameters.name + "-svcgrp"
                    servicetype: HTTP
               components:
                     -
                     name: lbvserver-svg-binding-comp
                     type: ns::lbvserver\servicegroup\binding
                     properties:
                           name: $parent.parent.properties.name
                           servicegroupname: $parent.properties.name
                     -
                     name: members-svcg-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                    type: ns::servicegroup\servicegroupmember\binding

                    repeat:

                      repeat-list: $parameters.svc-servers

                      repeat-item: srv

                    properties:

                          ip: $srv

                          port: $parameters.svc-port

                          servicegroupname: $parent.properties.name
```

The **repeat** is an object by itself, and **repeat-list** and **repeat-item** are attributes for the repeat object.

- repeat-list is a mandatory attribute that identifies the list that the component iterates on.
- repeat-item is optional, and is used to give a friendly name to the current item in the iteration.

If not specified, the current item can be accessed using the expression **$repeat-item**. The last component in the above example can also be written as follows:

```
          -


          name: members-svcg-comp


          type: ns::servicegroup_servicegroupmember_binding


          repeat:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            repeat-list: $parameters.svc-servers


        properties:


              ip: $repeat-item


              port: $parameters.svc-port


              servicegroupname: $parent.properties.name
```

In addition to being able to refer to the current item white iterating over a list, it is also possible to refer to the current index of the item in the list using **repeat-index**. In the following example, **repeat-index** is used to calculate a port number based on the current index:

```
            name: services


            type: ns::service


            repeat:


               repeat-list: $parameters.app-services


               repeat-item: srv
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            properties:

                ip: $parameters.app-ip

                port: $parameters.base-port + repeat-index

                servicegroupname: $parent.properties.name
```

Similar to the **repeat-item** construct, you can assign a different variable name to refer to the current index of the iteration. The previous example is equivalent to the following example:

```
    -

            name: services

            type: ns::service

            repeat:

               repeat-list: $parameters.app-services

               repeat-item: srv

               repeat-index: idx
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            properties:

                ip: $parameters.app-ip

                port: $parameters.base-port + $idx

                servicegroupname: $parent.properties.name
```

Repeat-condition construct

The repeat-condition construct is evaluated in each iteration of a repeat construct and the result determines whether to build the configuration object in that iteration or to move to the next iteration. The following example shows the use of the repeat-condition construct:

Example:

```
components

   -

      name: der-key-files-comp

      type: ns::systemfile

      repeat:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
repeat-list: $parameters.certificates

repeat-item: certificate

  repeat-condition: $certificate.ssl-inform == DER

  properties:

   filecontent: base64($certificate.keyfile.contents)

   fileencoding: BASE64

   filelocation: /nsconfig/ssl

   filename: $certificate.keyfile.file
```

In this example, the `der-key-files-comp` component iterates over all the certificates given by the user but it only builds configuration objects that correspond to certificates with DER encoding. In each iteration, the repeat-condition expression is evaluated to test whether the certificate encoding is of type DER. If it is not of type DER, no configuration object is built in the current iteration, and the iteration moves to the next certificate in the list.

Nested repeats

With the nested repeat construct you can have more than one repeat construct in each component depending on the definition of the component. Consider a nested repeat of two levels. For each

© 1997–2026 Citrix Systems, Inc. All rights reserved.

element in the outer list (first repeat-list), you can create a repeat list for all elements of the inner list (second repeat-list). The StyleBook compiler supports up to three nested repeats. Each repeat level has repeat-item and repeat-index attributes associated with it. Both repeat-item and repeat-index attributes are optional. In addition, each repeat can also specify a repeat-condition.

Example:

```
parameters:

  -

      name: vips

      type: ipaddress[]

  -

      name: vip-ports

      type: tcp-port[]

components:

  -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
name: lbvservers-comp

type: ns::lbvserver

repeat:

   repeat-list: $parameters.vips

   repeat-item: ip

   repeat:

        repeat-list: $parameters.vip-ports

        repeat-item: port

properties:

   name: str("lb-") + str($ip) + '-' + str($port)

   servicetype: HTTP
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        ipv46: $ip


        port: $port
```

In this example, for each item in `$parameters.vips`, we iterate over all the items of `$parameters.vip-ports`. Thus, for each `ipaddress` specified in `$parameters.vips`, we create `lbvserver` configuration objects for all ports specified in $parameters.vip-ports. The properties section defines the name of the object with "lb" as a prefix for the combination of the IP address and the port. Therefore, for each iteration, `$ip + $port` defines a unique combination of the IP address and the port number.

If the `repeat-item` attribute is not provided, the compiler generates a default value for it. The default values for repeat-item are: `$repeat-item`, `$repeat-item-1`, `$repeat-item-2` respectively for each repeat level. Similarly, if the `repeat-index` attribute is not provided, the compiler generates a default value for it. The default values for repeat-index are: $repeat-index, $repeat-index-1, and $repeat-index-2 respectively for each repeat level.

The following example describes the naming convention in the absence of repeat-item and repeat-index attributes in a nested repeat object.

Example:

```
components:


-


    name: lbvservers-comp


    type: ns::lbvserver


    repeat:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        repeat-list: $parameters.vips

        repeat:

           repeat-list: $parameters.vip-ports

    properties:

       name: str("lb-") + str($repeat-item) + '-' + str($repeat-item-1)

       servicetype: HTTP

       ipv46: $repeat-item

       port: $repeat-item-1
```

Outputs

In the outputs section, you specify what a StyleBook exposes to its users after it has completed creating all the configuration objects successfully. The outputs section of a StyleBook is optional. A StyleBook does not need to return outputs. However, by returning some internal components as outputs, it allows any StyleBooks that import it more flexibility as you can see when creating a composite StyleBook.

The following table describes the attributes used in the outputs section.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUTE	DESCRIPTION	MANDATORY
name	The name of the output corresponding to the configuration object you want to expose.	Yes
description	A text string describing the output.	No
value	This attribute specifies how to extract the value that is returned by a StyleBook.	Yes

Example:

```
outputs:

 -

   name: lbvserver

   description: LBVServer component

   value: $components.my-lbvserver-comp

 -

   name: svc-grp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    description: ServiceGroup name


    value: $components.my-svcg.properties.name
```

In this example, you expose the **lbvserver** component and the `servicegroup` **name** that would be created by the StyleBook. The value of the output called **lbvserver** is the component **my-lbvserver-comp**. Similarly, the value of the output called **svc-grp** is the name of the `servicegroup` created by the component **my-svcg**.

Parameter reference

In the components construct, you refer to the parameters defined in the parameters section by using `$parameters.<parametername>` notation. If `<parametername>` itself contains parameters (when type is object), then you must use the notation `$parameters.<parametername>.<sub-parametername>`, and so on.

Example:

```
parameters:


  -


    name: name


    label: Name


    type: string


    required: true
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-

 name: vip

 label: Virtual IP and Port

 type: object

 required: true

 parameters:

   -

     name: ip

     label: Virtual IP

     description: The Virtual IP Address

     type: ipaddress
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
          required: true

            -

              name: port

              label: The Virtual Port

              description: The TCP port for the Virtual IP

              type: tcp-port

              default: 80

components:

  -

    name: my-lbvserver-comp

    type: ns::lbvserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    properties:

       name: $parameters.name

       servicetype: HTTP

       ipv46: $parameters.vip.ip

       port: $parameters.vip.port
```

Parent reference

If you are using nested components, you can refer to the parent component using the $parent notation. If the parent component builds multiple configuration objects using the repeat construct, and within each iteration, child components build other configuration objects, then the $parent notation always refers to the current iteration of the parent component. For example, $parent.properties.name refers to the name property of the configuration object built in the current iteration by the parent.

Example:

```
components:

 -

   name: my-lbvserver-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
type: ns::lbvserver

properties:

  name: $parameters.name + "-lb"

  servicetype: HTTP

  ipv46: $parameters.ip

  port: 80

  lbmethod: $parameters.lb-alg

  components:

    -

      name: my-svcg-comp

      type: ns::servicegroup
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        properties:

          name: $parameters.name + "-svcgrp"

          servicetype: HTTP

          components:

           -

             name: lbvserver-svg-binding-comp

             type: ns::lbvserver_servicegroup_binding

             properties:

                name: $parent.parent.properties.name

                servicegroupname: $parent.properties.name

                  -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                name: members-svcg-comp


                type: ns::servicegroup_servicegroupmember_binding


                repeat: $parameters.svc-servers


                repeat-item: srv


                properties:


                  ip: $srv


                  port: str($parameters.svc-port)


                  servicegroupname: $parent.properties.name
```

You can also navigate upward through the hierarchy of components by accessing the properties of the parents of parents all the way to the top-level components. For example, the property name of the component **lbvserver-svg-binding-comp** takes its value from the property name of the parent of its parent, the **my-lbvserver-comp** component, by using the **$parent.parent** notation.

Components reference

In the components construct, you refer to a top-level component in the StyleBook by using the `$components.<componentname>` notation. If there are nested components within a top-level

© 1997–2026 Citrix Systems, Inc. All rights reserved.

component, then the notation used is `$components.<componentname>.components.<component-name>` to refer to them, and so on.

Example:

```
components:

 -

    name: my-lbvserver-comp

    type: ns::lbvserver

    properties:

       name: $parameters.name + "-lb"

       servicetype: HTTP

       ipv46: $parameters.ip

       port: 80

       lbmethod: $parameters.lb-alg
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
 -

    name: my-svcg-comp

    type: ns::servicegroup

    properties:

       name: $parameters.name + "-svcgrp"

       servicetype: HTTP

-

    name: members-svcg-comp

    type: ns::servicegroup_servicegroupmember_binding

    repeat: $parameters.svc-servers

    repeat-item: srv
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    properties:

       ip: $srv

       port: str($parameters.svc-port)

       servicegroupname: $components.my-svcg-comp.properties.name

-

    name: lbvserver-svg-binding-comp

    type: ns::lbvserver_servicegroup_binding

    properties:

        name: $components.my-lbvserver-comp.properties.name

        servicegroupname: $components.my-svcg-comp.properties.name
```

In this example, the components **my-svcg-comp** and **my-lbvserver-comp** have to be built before building the last component **lbvserver-svg-binding-comp** because there are references to these

© 1997–2026 Citrix Systems, Inc. All rights reserved.

components in this last component. These references are provided by using the components references denoted by `$components.<componentname>`.

Substitutions reference

In the components section or operations section, you refer to substitutions defined in the substitutions section by using the **`$substitutions.<substitution-name>`** notation. For example, **$substitutions.http-port**.

If a substitution is a map, you can refer to an element in the map as **`$substitutions.<substitutions-name>[<map-key>]`**. For example, **`$substitutions.protocol-map[$parameters.port]`**.

Variable reference

When you use the repeat and repeat-item constructs in components to build multiple configuration objects, you can assign a variable name to the repeat-item construct. This variable can be then referenced in the properties of that component or in child components by using the notation `$<varname>`. Note that when the repeat construct is used without the repeat-item construct in a component, a default variable called $repeat-item can be used to access the iteration items.

Example:

```
components:


  -


    name: server-members-comp


    type: ns::server


    condition: $parameters.svc-server-domain-names
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
repeat: $parameters.svc-server-domain-names

repeat-item: server-name

properties:

  name: $server-name + "-server"

  domain: $server-name

components:

  -

     name: service-members-comp

     type: ns::service

     properties:

       name: $server-name + "-service"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            servername: $parent.properties.name


            servicetype: $parameters.svc-service-type


            port: $parameters.svc-server-port
```

In the above example, a variable name, server-name, is assigned to the repeat-item construct. This variable name is referred to in the properties of the same component and in the child components `$<varname>`.

Operations

The `Operations` is an optional section in a StyleBook. In this section, you can configure NetScaler Console Analytics to collect AppFlow records on all or some of the traffic transactions. The virtual server created on a NetScaler instance, by using the StyleBook, handles the traffic transactions. You can also configure NetScaler Console to trigger alarms when certain traffic conditions are met on a virtual server.

You can configure NetScaler Console through StyleBooks to collect traffic statistics from the various NetScaler Console insights that are listed as follows:

- Bot Insight
- Web Insight
- Security Insight
- HDX™ Insight
- NetScaler Gateway Insight

The virtual servers supported are load balancing, content switching, and VPN virtual servers.

Enable both Web Insight and Security Insight or one of them for analytics on a load balancing or content switching virtual server. For VPN virtual servers, however, you must enable both HDX Insight and NetScaler Gateway Insight or one of them.

Any NetScaler Console insight enabled on NetScaler instances through StyleBooks uses an IPFIX protocol (AppFlow) to send the data from the instances to NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Also, when you enable Web Insight, "Client-Side Measurements" is enabled on the load balancing and the content switching virtual servers. With this feature enabled, NetScaler Console captures load time and render time metrics for HTML pages, through HTML injection. Using these metrics, admins can identify L7 latency issues.

After you enable a particular NetScaler Console insight, view the **Application Overview** page to see the threat details associated with that insight.

Example 1:

The following example shows how to write the operations section in a StyleBook to enable both HDX Insight and NetScaler Gateway Insight on a VPN virtual server:

```
name: simple-vpn-ops


namespace: com.example.stylebooks


schema-version: "1.0"


version: "0.1"


description: Test StyleBook to enable hdxinsight and gatewayinsight on a
VPN vserver


import-stylebooks:


  -


    namespace: netscaler.nitro.config
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    version: "10.5"

    prefix: ns

components:

  -

    name: vpnvserver-comp

    type: ns::vpnvserver

    properties:

      name: str("vpn-") + str($current-target.ip)

      servicetype: SSL

      ipv46: 1.1.21.37

      port: 443
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
operations:

    analytics:

      -

        name: comp-ops

        properties:

          target: $components.vpnvserver-comp

          filter: "true"

          insights:

            -

              type: hdxinsight

            -

              type: gatewayinsight
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
outputs:

  -

    name: myvpns

    value: $components.vpnvserver-comp
```

Example 2:

The following example shows how to write the operations section in a StyleBook to enable Web Insight, Security Insight, and Bot Insight on a load balancing virtual server:

```
---

name: enable-insights

namespace: com.acme.stylebooks

description: "This StyleBook enables Web,Security & Bot Insight on Load
Balancing Vserver"

display-name: "SB Operations"

schema-version: "1.0"

version: "1.0"

import-stylebooks:

  -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"


parameters:




 -
    name: lbname
    type: string
    required: true
  -
    name: vip
    type: ipaddress
    required: true
  -
    name: appflowfilter
    type: string
    required: true


components:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  -
    name: my-lbvserver-comp
    type: ns::lbvserver
    properties:
      name: $parameters.lbname
      servicetype: HTTP
      ipv46: $parameters.vip
      port: 80


outputs:
  -
    name: mylb
    value: $components.my-lbvserver-comp


operations:
  analytics:
    -
      name: lbvserver-op
      properties:
        target: $outputs.mylb
        filter: $parameters.appflowfilter
        insights:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        -
          type: webinsight
        -
          type: securityinsight
        -
          type: botinsight
```

Analytics

Each element in the analytics section is used to configure the NetScaler Console analytics feature for one or more virtual servers created in StyleBooks.

An element in the analytics section has the following attributes:

ATTRIBUTE	DESCRIPTION	MANDATORY
name	Name of the analytics element.	Yes
description	A text string describing what this element is.	No
condition	A boolean expression. When this condition evaluates to false, the entire analytics element is skipped.	No
repeat	Iterates over a list.	No
repeat-condition	A boolean expression. If the expression evaluates to false, the current iteration is skipped.	No
repeat-item	Name of the item in the current iteration.	No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUTE	DESCRIPTION	MANDATORY
repeat-index	Name of the index value of the current iteration.	No
properties	A list of analytics operation properties.	Yes
target	One of the properties in the list. The target expression is the name of a virtual server, configured on the NetScaler, for which analytics is collected.	Yes
filter	One of the properties in the list. The value of this attribute is a NetScaler advanced policy expression that is used to filter the requests on the virtual server for which analytics is collected. By default, the analytics data is collected on all the traffic passing through the virtual server.	No
insights	One of the properties in the list. The value of this attribute is the type of insight data to be collected from the target virtual server. By default, all the allowed insights are configured on the target virtual servers based on virtual server type as specified in Target virtual servers and insight types.	No
transport-mode	One of the properties in the list. The value of this attribute is either `logstream` or	No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUTE	DESCRIPTION	MANDATORY
	`ipfix`. `logstream` is the default value.	
client-side-measurements	One of the properties in the list. The value of this attribute is either ENABLED or DISBALED. DISABLED is the default value.	No
http-x-forwarded-for	One of the properties in the list. The value of this attribute is either ENABLED or DISBALED. The attribute enables or disables the X-Forwarded-For header insertion to pass the client IP information to the back end server. DISABLED is the default value.	No
enable-hdxinsight-for	One of the properties in the list. The value of this attribute is either ICA or TCP. This attribute enables `hdxinsight` for specific traffic data. ICA is the default value.	No

Example 1: Configure analytics for a single virtual server

```
operations:


  analytics:

    -

    name: lbvserver-ops-comp

    properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        target: $components-basic-lb-comp.outputs.lbvserver-name

        filter: HTTP.REQ.URL.CONTAINS("catalog")

        transport-mode: logstream

        client-side-measurements: ENABLED

        insights:

          -

            type: webinsight

          -

            type: securityinsight
```

Example 2: Configure analytics for a list of VPN virtual servers

```
operations:



    analytics:

    -

      name: vpnvserver-ops-comp

      repeat: $outputs.staging-vpnvservers

      repeat-item: vpnvsvr

      properties:

        target: $vpnvsvr.outputs.vpnvserver

        filter: HTTP.REQ.URL.CONTAINS("catalog")

        http-x-forwarded-for: ENABLED
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        insights:
          -
            type: hdxinsight
            enable-hdxinsight-for: TCP
```

Each attribute in the analytics section configures the NetScaler instances to collect AppFlow records on the virtual server identified by the target property.

Target virtual servers and insight types

The target virtual servers and the corresponding allowed insight types are as follows:

TARGET VIRTUAL SERVER	INSIGHT TYPE
lbvserver	webinsight, securityinsight, botinsight
csvserver	webinsight, securityinsight, botinsight
vpnserver	hdxinsight, gatewayinsight

NOTE

IPFIX is the default transport mode used to configure analytics for virtual servers in StyleBooks.

Alarms

The alarms subsection of the operations section has a similar structure and the same attributes as in the analytics subsection. The only difference is in the properties attribute. For a list of all the attributes (other than the properties attribute), see Analytics.

The following properties are available in an alarm subsection:

ATTRIBUTE	DESCRIPTION	MANDATORY
`target`	An expression that evaluates to the name of a virtual server, configured on the	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUTE	DESCRIPTION	MANDATORY
	NetScaler, for which alarms are configured.	
`email-profile`	Name of an email profile that is defined in the NetScaler Console Analytics feature and contains a list of email addresses that you want to notify when the alarm is triggered.	No (either an `email-profile` or an `sms-profile` must be defined)
`sms-profile`	Name of an SMS profile that is defined in the NetScaler Console Analytics feature and contains a list of phone numbers that you want to notify when the alarm is triggered.	No (either an `email-profile` or an `sms-profile` must be defined)
`rules`	A list of rules that define the conditions that would trigger an alarm for the virtual server defined by the target property.	Yes
`metric`	An attribute of rule. The name of a metric you want to track pertaining to the NetScaler virtual server.	Yes
`operator`	An attribute of rule. The operator to use to compare the metric to the value. Valid operators are `greaterthan` and `lessthan`.	Yes
`value`	An attribute of rule. The threshold value that the metric is compared to by using the operator. If the metric value exceeds this	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUTE	DESCRIPTION	MANDATORY
	threshold, the associated alarms are triggered.	
`period-unit`	An attribute of a rule. The frequency at which to alert users if the alarm rule is met. This attribute can contain the value day, hour, or weekly. It means that if the rule is met, an alarm is sent once a period-unit (for example, once a day).	Yes

The following table provides a list of metrics that are tracked pertaining to the NetScaler virtual server.

COUNTERS	DESCRIPTION	DETAILED DESCRIPTION	NETSCALER CONSOLE CALCULATION
For a VPN virtual server			
total_requests	Total VPN Session Launch Count	Total number of active sessions on this VPN virtual server started during a time interval specified by the user.	Monotonically increasing counter, incremented on each new session launch
app_count	VPN App Launch Count	Total number of unique VPN applications on this VPN virtual server launched during a time interval specified by the user.	Monotonically increasing counter on each new application launch
app_launch_duration	VPN App Launch Duration	Average time taken to launch an	Average value calculated across the launch time

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COUNTERS	DESCRIPTION	DETAILED DESCRIPTION	NETSCALER CONSOLE CALCULATION
		application (in milliseconds)	durations of all VPN applications launched on this VPN virtual server
Other virtual servers (`CS`, `LB`, `Auth`, `GSLB`)			
total_requests	Number of requests	Number of client requests on this virtual server since the last appliance reboot, or since the creation of the virtual server, whichever is more recent.	Monotonically increasing counter, incremented on each new request to this virtual server.
total_bytes	Bytes	Total bytes transferred from the virtual server to NetScaler Console over the specified time interval.	Monotonically increasing counter to account for the total number of bytes served by this virtual server.
application_response_time	Response Time	Average response time of the virtual server.	The average value of the response times of all requests received by this virtual server since the last reboot of the appliance (or since the creation of the virtual server), whichever is the last.

Example of an alarms section in a StyleBook:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
operations:

alarms:

 -

  name:lbvserver_alarm

  properties:

      target: $outputs.lbvserver

      email-profile: $parameters.emailprofile

      sms-profile: "NetScalerSMS"

      rules:

      -

        metric: "total_requests"

        operator: "greaterthan"

        value: 25

        period-unit: weekly

        -

          metric: "total_bytes"

          operator: "lessthan"

          value: 1024

          period-unit: day
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Expressions

One of the most powerful features of a StyleBook is the use of expressions. You can use StyleBooks expressions in various scenarios to compute dynamic values. The following example is an expression to concatenate a parameter value with a literal string.

Example:

```
$parameters.appname + "-mon"
```

This expression retrieves the parameter named `appname`, and concatenates it with the string `-mon`.

NOTE

StyleBook supports using the reserved keywords when you define parameters and expressions in a StyleBook definition. The reserved keywords are - `and`, `false`, `in`, `not`, `true`, and `or`.

The following types of expressions are supported:

Arithmetic expressions

- Addition (+)
- Subtraction (-)
- Multiplication (*)
- Division (/)
- Modulo (%)

Examples:

- Adding two numbers: $parameters.a + $parameters.b
- Multiplying two numbers: $parameters.a * 10
- Finding the remainder after division of one number by another:

`15%10` Results in `5`

String expressions

- Concatenate two strings (+)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example:

Concatenate two strings: str("app-") + $parameters.appname

List expressions

Merges two lists (+)

Example:

- Concatenate two lists: $parameters.external-servers + $parameters.internal-servers
- If `$parameters.ports-1` is and `$parameters.port-2` is , the `$parameters.ports-1 + $parameters.ports-2` displays as a list .

Relational expressions

- **==** : Tests if two operands are equal and returns true if they are equal, else returns false.
- **!=** : Tests if two operands are different and returns true if they are different, else returns false.
- **\>** : Returns true if the first operand is greater than the second operand, else returns false.
- **\>=** : Returns true if the first operand is greater than or equal to the second operand, else returns false.
- **\<** : Returns true if the first operand is lesser than the second operand, else returns false.
- **\<=** : Returns true if the first operand is lesser than or equal to the second operand, else returns false.

Example:

- Use of Equality operator: `$parameters.name = = "abcd"`
- Use of Inequality operator: `$parameters.name != "default"`
- Examples for other relational operators
  - `10 > 9`
  - `10 >= 10`
  - `0 < 9`
  - `10 <= 9`
  - `10 == 10`
  - `10 != 1`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Logical expressions - boolean

- **and**: The logical 'and' operator. If both operands are true, the result is true, else it is false.
- **or**: The logical 'or' operator. If one of the operands is true, the result is true, else it is false.
- **not**: The unary operator. If the operand is true, the result is false, and the opposite way.
- **in**: Tests whether the first argument is a substring of the second argument
- **in**: Tests if an item is part of a list

NOTE

You can type-cast expressions where strings are converted into numbers (using int() builtin function) and numbers are converted to strings (using str() builtin function). Similarly, you can cast `tcp-port` to a number (using the `int()` builtin function), and an IP address can be cast to a string (using the str() builtin function).

Use a delimiter before and after any operator. You can use the following delimiters:

- Before an operator: `space`, `tab`, `comma`, `(`, `)`, `[`, `]`
- After an operator: `space`, `tab`, `(`, `[`

For example:

- `abc + def`
- `100 % 10`
- `10 > 9`
- `$item in $parameters.some-list`

Splat expressions

A splat expression `[*]` provides a simpler way to retrieve a certain attribute from a complex list for all the iterations. You can now include splat expressions in a StyleBook definition.

Syntax:

```
list[*].attribute
```

This expression iterates over all the items of the list specified to its left and returns the attribute value specified to its right.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When you want to retrieve an IP address or host name of each virtual server from the list, you can use the following splat expressions:

Example 1:

```
$parameters.server-members[*].hostname
```

This expression returns a list of host names from all the server-members.

Example 2:

```
$parameters.server-members[*].sub-domains[*].name
```

This expression returns a list of all names under the subdomains of each server-members.

These expressions always return the right-most element type's list.

Verbatim string expressions

You can use verbatim strings when special characters in a string have to take their literal form. These strings can contain escape characters, backslash, quotes, parentheses, whitespaces, brackets, and so on. In verbatim strings, the special characters' usual interpretation is skipped. All the characters in the string are preserved in their literal form.

In StyleBooks, you can include NetScaler Policy Expressions in their literal form using verbatim strings. The Policy Expressions typically contain special characters. Without verbatim strings, you have to escape special characters by breaking strings into substrings.

To create a verbatim string, encapsulate a string between special characters as follows:

```
~{string}~
```

You can use verbatim strings in the StyleBook expressions.

NOTE

Do not use the sequence of characters `}~` in an input string because this sequence indicates the end of a verbatim string.

Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
~{HTTP.REQ.COOKIE.VALUE("jsessionid") ALT
HTTP.REQ.URL.BEFORE_STR("=").AFTER_STR(";jsessionid=") ALT
HTTP.REQ.URL.AFTER_STR(";jsessionid=")}~
```

For more informtion, see Allow special characters with their literal form in StyleBooks.

Target expressions

In a StyleBook definition, you can use the `$current-target` expression to refer the current target NetScaler instance. To specifically refer an IP address of the target NetScaler instance, use this expression as follows:

```
$current-target.ip
```

Example:

```
components:

 -

  name: lb-comp

  type: ns::lbvserver

  properties:

    name: $current-target.ip + "-lbvserver"
```

In this example, the name of the `lbvserver` uses the IP address of the target NetScaler instance.

Expression Type Validation

StyleBook engine now allows for stronger type checking during compile time, that is, the expressions used while writing the StyleBook are validated during the import of a StyleBook itself rather than while creating the configuration pack.

All references to parameters, substitutions, components, properties of components, outputs of components, user-defined variables (repeat-item, repeat-index, arguments to substitution functions) and so on are all validated for their existence and types.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example of Type Checks:

In the following example, the expected type of port property of `lbvserver` StyleBook is `tcp-port`. In NetScaler Console, the type validations happen at compile-time (import-time). The compiler finds that string and `tcp-port` are not compatible types and therefore, the StyleBook compiler displays an error and fails to import or migrate a StyleBook.

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: str("80")
      servicetype: HTTP
```

To successfully compile this StyleBook, declare the following as a number in the compiler:

`port: 80`

Example of Flagging Invalid Expressions:

When you import a StyleBook to NetScaler Console, the compiler identifies the invalid expressions and flag it. As a result, the StyleBook fails to import to NetScaler Console.

In the following example, the expression assigned to the name property in the `lb-sg-binding-comp` component is: `$components.lbvserver-comp.properties.lbvservername`. However, there is no property called `lbvservername` in component `lbvserver-comp`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Components:

  -

    name: lbvserver-comp

    type: ns::lbvserver

    properties:

      name: mylb

      ipv46: 10.102.190.15

      port: 80

      servicetype: HTTP

  -

    name: sg-comp

    type: ns::servicegroup

    properties:

      servicegroupname: mysg

      servicetype: HTTP

  -

    name: lb-sg-binding-comp

    type: ns::lbvserver_servicegroup_binding

    condition: $parameters.create-binding

    properties:

      name: $components.lbvserver-comp.properties.lbvservername
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
servicegroupname: $components.sg-comp.properties.servicegroupname
```

Implicit typecasting of datatypes

When you use StyleBook expressions for different datatypes, the StyleBook engine now implicitly typecasts the output to an appropriate datatype. The implicit typecasting of datatypes supports binary operations and value assignments.

Examples for binary operations:

- Adding (+) two variables of type `string` and `number`, sets the output datatype to `string`.

```
$parameters.appname + '_' + $parameters.app_instance_num
```

- Adding (+) two variables of type `string` and `ipaddress`, sets the output datatype to `string`.

```
$parameters.appname + '_' + $parameters.instance_ip
```

- Adding (+) two variables of type `ipaddress` and `number`, sets the output datatype to `ipaddress`.

```
$parameters.instance_ip + $parameters.number
```

- Subtracting (-) two variables of type `ipaddress` and `number`, sets the output datatype to `ipaddress`.

```
$parameters.instance_ip - $parameters.number
```

- Multiplying (*) two variables of type `string` and `number`, sets the output datatype to `string`.

```
$parameters.dummy_str * $parameters.count
```

Examples for value assignments:

- If a variable is defined as the `string` datatype, the assigned value is converted to the defined datatype.

```
name: $parameters.port * 3
```

- If a variable is defined as the `portnumber` datatype, the assigned value converted to the `portnumber` datatype with exceptions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
port: $index + $parameters.lower_limit
```

Indexing Lists

Items of a list can be accessed now by indexing them directly:

Expression	Description
`$components.test-lbs[0]`	Refers to the first item in `thetest-lbs` component
`$components.test-lbs[0].properties.p1`	Refers to property p1 of the first item in the test-lbs component
`$components.lbcomps[0].outputs.servicegroups[1].properties.servicegroupname`	Refers to the property `servicegroupname` of the second item in the `servicegroups` component, which is an output from the first item of the `lbcomps` component

Policy expressions in StyleBooks

The StyleBooks GUI allows you to build NetScaler® policy expressions by selecting items from lists, helping you to create expressions faster and more accurately.

Policy expressions in StyleBooks allow you to create flexible and customizable configurations. You can specify conditions based on various parameters, attributes, or variables. Policy expressions are commonly used to implement NetScaler policy configurations.

ENABLE POLICY EXPRESSION EDITOR IN STYLEBOOKS GUI

To make the EPA or expression editor available for a parameter, specify the `is_policy_expression` GUI attribute in the parameter definition. When enabled (set to true) this setting allows you the invoke the **Expressions Editor** when entering a value for this parameter.

```
parameters:

  -

    name: expression

    type: string

    label: Expression
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

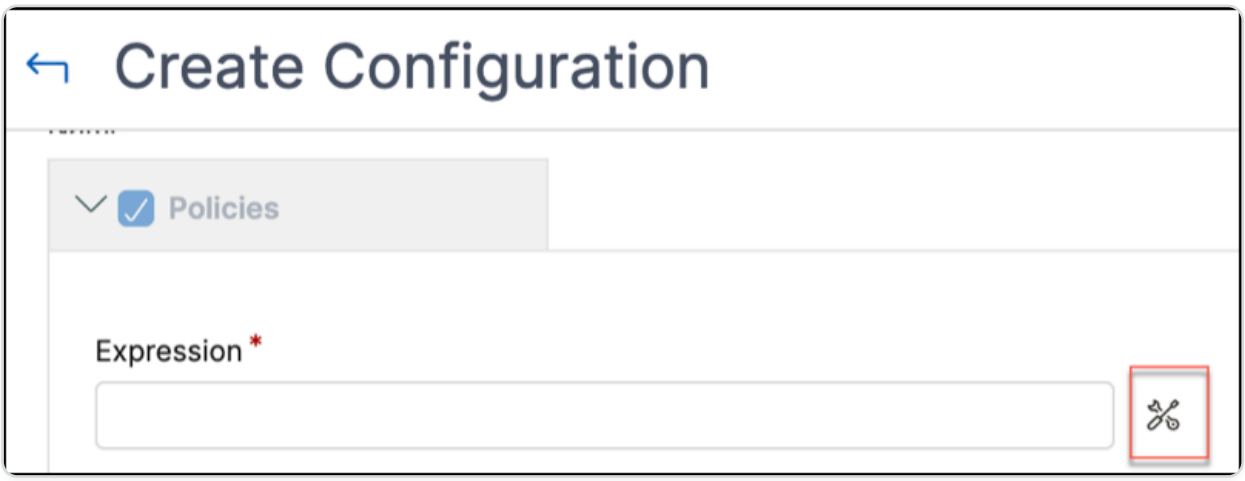
```
    required: true

    gui:

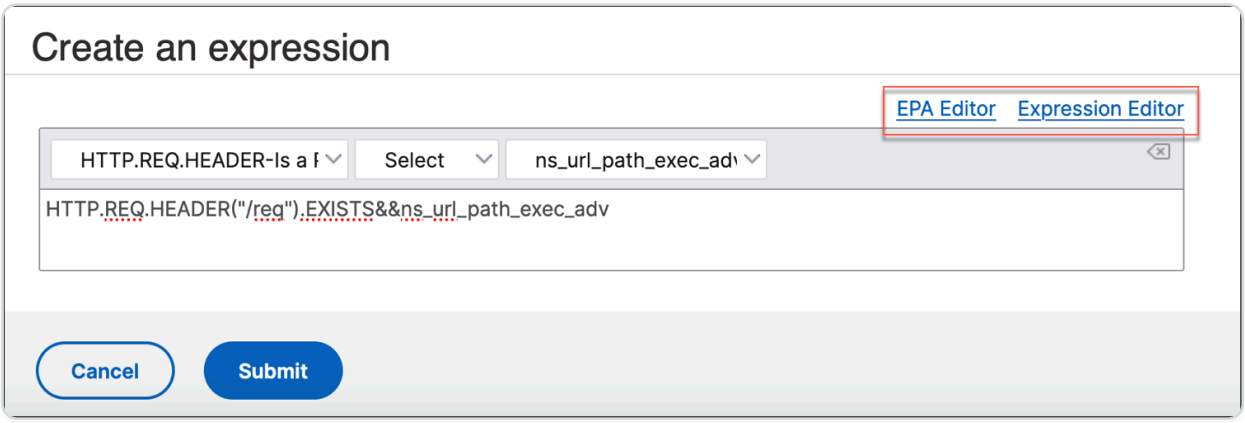
      is_policy_expression: true
```

CREATE AND BUILD POLICY EXPRESSIONS

1. Navigate to **Applications > Configurations > StyleBooks**. The **StyleBooks** page displays all the StyleBooks that are available in your NetScaler Console.
2. Select a StyleBook that includes policy expressions in its parameters.
3. Click **Create Configuration**. In the **Create Configuration** page, enter values for all the parameters defined in this StyleBook.
4. Click the icon next to the **Expressions** field. The **Create an expression** page appears.



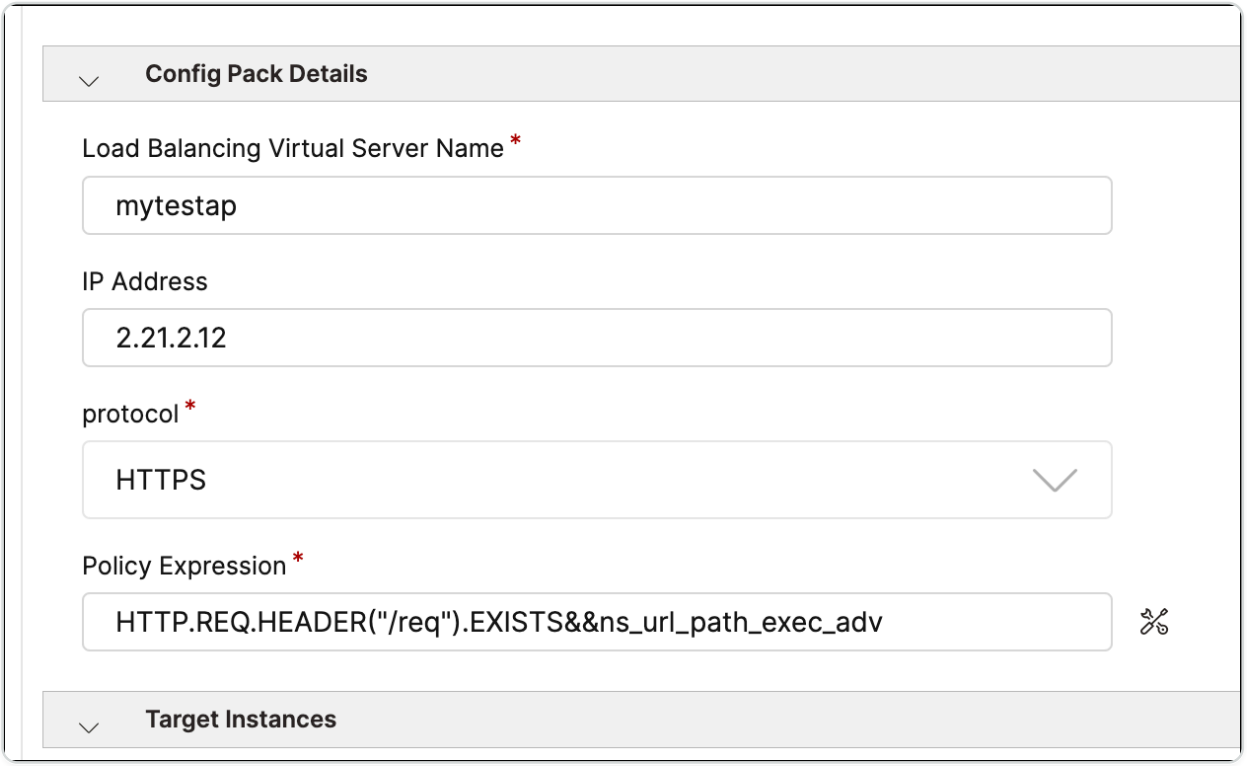
5. In **Create an expression**, use the intuitive drop-downs to construct your policy expression. Click **Submit**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you want to create a custom policy expression, click on **EPA Editor** or **Expression Editor** to build your expressions. Review your expressions in **Preview Expressions** and then click **Submit**.

6. Select the target NetScaler instance on which the configuration should be deployed and click **Submit**.



In-place interpolations

It is now possible to replace parts of a string using a StyleBook expression. When these string expressions are evaluated by the StyleBook compiler, the part of the string that uses a StyleBook expression will be replaced by a value of the expression. To include StyleBook expressions in a string, we use the following notation:

```
"...%{...}%..."
```

Where the characters enclosed between" %{ " and "}%" form a StyleBook expression. These expressions are known as "in-place interpolations. "

For example, the string `lb-%{$parameters.appname}%-svc` is a string expression with an in-place interpolation of a StyleBook expression. The value of the string expression depends on the value of the interpolation expression. Consider that **$parameters.appname** is assigned with

© 1997–2026 Citrix Systems, Inc. All rights reserved.

"app1." Then, the string expression evaluates to **lb-app1-svc**. This allows the values to be not hard-coded in string expressions, but rather be evaluated based on the user-defined values.

A practical use case of in-place interpolations is to parameterize policy expressions in StyleBooks. Consider a scenario where you want to write a policy expression that checks if the HTTP URL contains a specific word, say, "jpeg".

For this, you write a policy expression as follows: "HTTP.REQ.URL.CONTAINS(\\"jpeg\\")".

Now, if you want to parameterize the object in the HTTP URL, you can add a string parameter in the StyleBook, say, `$parameters.url-object`. The policy expression is written based on this parameter. To do that, you use string concatenation to achieve the result. The expression would look like:

```
str("HTTP.REQ.URL.CONTAINS(\\"" + $parameters.url-object + "\\")")
```

If `$parameter.url-object` is assigned "csv", the above expression evaluates to "HTTP.REQ.URL.CONTAINS(\\"csv\\")". However, this expression is not easy to read. To make this parameterization easy to read and understand, you can use in-place interpolations.

The expression with in-place interpolation is now:

```
str("HTTP.REQ.URL.CONTAINS(%{quotewrap($parameters.url-object)}%)")
```

In the above expression, you used an interpolation expression that adds the inner-quotes around the value of the $parameters.url-object. The result of this expression is the same as the above, but, it looks more intuitive and closer to the actual result.

Allowed Types Inside Interpolations

You can use expressions that generate a value of the following types inside interpolations: boolean, number, `tcp-port`, `ipaddress`, and string. The generated value is automatically transformed to a string when the interpolations are replaced with the result.

String expressions can have 0, 1, or more interpolations. In a sequential interpolation, different parts of the string expression can be replaced by different StyleBook expressions. For example, the string lb-%{$parameters.appname}%-%{$parameters.vip}% returns "lb-app1-1.1.1.1", if $parameters.appname is "app1" and $parameters.vip is "1.1.1.1"

© 1997–2026 Citrix Systems, Inc. All rights reserved.

String expressions also support nested interpolations. That is, an interpolation expression can be nested inside another interpolation expression so that the value of one expression can become an input to the second expression.

For example, consider a string "%{lb-%{$parameters.port + 1}%}%"

The internal string, "**%{$parameters.port + 1}%**" returns "lb-81" if $parameters.port is 80. Here this expression is nested inside another interpolation expression.

The following table describes the different types of interpolations with examples and corresponding results. The value of the parameters used in the examples is:

- $parameters.appname: "lb1"
- $parameters.vip: "1.1.1.1"
- $parameters.n1: 1
- $parameters.n2: 3

Simple interpolations

EXPRESSION	RESULT
`lb-%{$parameters.appname}%-def`	`lb-lb1-def`

Automatic type conversions

EXPRESSION	RESULT
lb-%{1}%	lb-1
lb-%{$parameters.vip}%	lb-1.1.1.1
lb-%{true}%	lb-True

Sequential interpolations

EXPRESSION	RESULT
%{$parameters.appname}%-%{str($parameters.appname)}%	lb1-lb1
lb-%{1}%-%{2}%	lb-1-2

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Nested interpolations

EXPRESSION	RESULT
`%{abc-%{$parameters.n1 + 1}%}%`	`abc-2`
`str("%{abc-%{$parameters.n1}%}%-%{$parameters.n2}%")`	`bc-1-3`

Interpolations with `quotewrap`

EXPRESSION	RESULT
`str("%{quotewrap(abcd)}%")`	`\"abcd`
`str("%{quotewrap(https://)}%+HTTP.REQ.HOSTNAME+HTTP.REQ.URL")`	`<https://"+HTTP.REQ.HOSTNAME+HTTP.REQ.URL`

Escape Characters in Interpolations

If the characters "%{" or "}%" are part of the string, you must provide "`\`" as an escape character so that the StyleBook compiler does not evaluate these as interpolation tags.

Example:

`str("%{\%\{ + str($parameters.vip) + \}\%}%") returns "%{1.1.1.1}%" if $parameters.vip is 1.1.1.1`

The following table describes a few more expressions and their results:

CATEGORY	EXPRESSION	RESULT
Escaping interpolations	`str("%{str($parameters.n1) + \}\%}%")`	`1}%`
	`lb-%{str($parameters.n1) + \}\%}%`	`lb-1}%`
	`"%{str($parameters.n1) + \"\}\%\"}%"	1}%`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Built-in functions

Expressions in StyleBooks can use built-in functions.

For example, you can use the built-in function, `str()` to transform a number to a string.

```
str($parameters.order)
```

Or, you can use the built-in function, `int()` to transform a string into an integer.

```
int($parameters.priority)
```

The following is the list of built-in functions supported in StyleBook expressions with examples of how they can be used:

str()

The `str()` function transforms the input argument to a string value.

Allowed argument types:

- `string`
- `number`
- `tcp-port`
- `boolean`
- `ipaddress`

Examples:

- The `"set-" + str(10)` function returns `"set-10"`.
- The `str(10)` function returns `10`.
- The `str(1.1.1.1)` function returns `1.1.1.1`.
- The `str(True)` function returns `"True"`.
- The `str(NetScaler Console)` function returns `"NetScaler Console"`.

int()

The `int()` function takes a string, number, IP address, or `tcpport` as an argument and returns an integer.

Examples:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The `int("10")` function returns `10`.
- The `int(10)` function returns `10`.
- The `int(ip('0.0.4.1'))` function returns `1025`.

bool()

The `bool()` function takes any type as an argument. If the argument value is `false`, empty, or absent, this function returns `false`.

Otherwise, it returns `true`.

Examples:

- The `bool(true)` function returns `true`.
- The `bool(false)` function returns `false`.
- The `bool($parameters.a)` function returns `false` if the `$parameters.a` is `false`, empty, or absent.

len()

The `len()` function takes a string or a list as an argument, and returns the number of characters in a string or the number of items in a list.

Example 1:

If you define a substitution as follows:

```
items: ["123", "abc", "xyz"]
```

The `len($substitutions.items)` function returns `3`

Example 2:

The `len("NetScaler Console")` function returns `10`.

Example 3:

If `$parameters.vips` has values `['1.1.1.1', '1.1.1.2', '1.1.1.3']`, the `len($parameters.vips)` function returns `3`.

min()

The `min()` function takes either a list or a series of numbers or TCP ports as arguments, and returns the smallest item.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Examples with a series of numbers/TCP ports:

- The `min(80, 100, 1000)` function returns `80`.
- The `min(-20, 100, 400)` function returns `-20`.
- The `min(-80, -20, -10)` function returns `-80`.
- The `min(0, 100, -400)` function returns `-400`.

Examples with a list of numbers/TCP ports:

- Support `$parameters.ports` is a list of TCP ports and has values: `[80, 81, 8080]`.

  The `min($parameters.ports)` function returns `80`.

max()

The `max()` function takes either a list or a series of numbers or TCP ports as arguments, and returns the largest item.

Examples with a series of numbers/TCP ports:

- The `max(80, 100, 1000)` function returns `1000`.
- The `max(-20, 100, 400)` function returns `400`.
- The `max(-80, -20, -10)` function returns `-10`.
- The `max(0, 100, -400)` function returns `100`.

Examples with a list of numbers/TCP ports:

- Support `$parameters.ports` is list of TCP ports and has values: `[80, 81, 8080]`.

  The `max($parameters.ports)` function returns `8080`.

bin()

The `bin()` function takes a number as an argument, and returns a string that represents the number in binary format.

Examples of expressions:

The `bin(100)` function returns `0b1100100`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

oct()

The `oct()` function takes a number as an argument, and returns a string that represents the number in octal format.

Examples of expressions:

The `oct(100)` function returns `0144`.

hex()

The `hex()` function takes a number as an argument, and returns a lowercase string that represents the number in hexadecimal format.

Examples of expressions:

The `hex(100)` function returns `0x64`.

lower()

The `lower()` function takes a string as an argument and returns the same string in the lowercase.

Example:

The `lower("NetScaler Console")` function returns `NetScaler Console`.

upper()

The `upper()` function takes a string as an argument and returns the same string in uppercase.

Example:

The `upper("NetScaler Console")` function returns `NetScaler Console`.

sum()

The `sum()` function takes a list of numbers or `tcpports` as arguments and returns the sum of the numbers in the list.

Example 1:

If you define a substitution as follows: substitutions:

```
list-of-numbers = [11, 22, 55]
```

The `sum($substitutions.list-of-numbers)` function returns `88`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example 2:

If `$parameters.ports` is `[80, 81, 82]`, the `sum($parameters.ports)` function returns `243`.

pow()

The `pow()` function takes two numbers as arguments and returns a number that represents the first argument raised to the power of the second one.

Example:

The `pow(3,2)` function returns `9`.

ip()

The `ip()` function takes an integer, string, or an IP address as an argument and returns the IP address based on the input value.

Examples:

- Specify an IP address in the `ip` function:

  The `ip(3.1.1.1)` function returns `3.1.1.1`.
- Specify a string in the `ip` function:

  The `ip('2.1.1.1')` function returns `2.1.1.1`
- Specify an integer in the `ip` function:
  - The `ip(12)` function returns `0.0.0.12`.
  - When you specify an integer as string in the `ip` function, it returns an equivalent IP address of the input.

    The `ip('1025')` function returns `0.0.4.1`.

  This function also supports the integer addition and subtraction operations and returns a resultant IP address.

  - Addition: The `ip(1025) + ip(12)` function returns `0.0.4.13`.
  - Subtraction: The `ip('1025') - ip(12)` function returns `0.0.3.245`.
  - Combine addition and subtraction: The `ip('1.1.1.1') + ip('1.1.1.1') – ip(2)` returns `2.2.2.0`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ip_network()

The `ip_network` function takes IP address and netmask length as arguments and returns an IP network notation.

Example-1:

The `ip_network(1.1.1.1, 28)` function returns `1.1.1.1/28`.

Example-2:

Consider the value `1.1.1.1` for `$parameters.ipaddr`. The `ip_network($parameters.ipaddr, 30)` function returns `1.1.1.1/30`.

Example-3:

Consider the value `24` for `$parameters.netmask-len`. The `ip_network(23.1.12.76, $parameters.netmask-len)` function returns `23.1.12.76/24`.

network_ip()

The `network_ip()` function returns the first IP address of the specified IP network.

Example:

The `network_ip(1.1.1.1/28)` function returns `1.1.1.0`. In this example, `1.1.1.0` is the first IP address in the given network.

subnets()

The `subnets()` function returns the list of subnets from the specified IP network and netmask length.

Example:

The `subnets(1.1.1.1/28, 30)` function returns the subnets list from the given IP network and netmask length. The output can be as follows:

```
[1.1.1.0/30', '1.1.1.4/30', '1.1.1.8/30', '1.1.1.12/30']
```

netmask_ip()

The `netmask_ip()` function returns the netmask IP address for the specified IP network.

Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The `netmask_ip(1.1.1.1/28)` function returns `255.255.255.240`. For the given IP network, `255.255.255.240` is the netmask IP address.

is_netmask_ip()

The `is_netmask_ip()` function accepts an `ipaddress` as an input. And, it returns `True` if the specified value is a valid netmask IP address.

Example 1:

The `is_netmask_ip(255.255.255.240)` function returns `True` because the specified value is a valid netmask IP address.

Example 2:

The `is_netmask_ip(255.255.255.232)` function returns `False` because the specified value is not a valid netmask IP address.

broadcast_ip()

The `broadcast_ip()` function returns the broadcast IP address for the specified IP network.

Example:

The `broadcast_ip(1.1.1.1/28)` function returns `1.1.1.15`. For the given IP network, `1.1.1.15` is the broadcast IP address.

cidr()

The `cidr()` function returns the CIDR notation for the specified IP network.

Example:

The `cidr(1.1.1.1/28)` function returns the `1.1.1.0/28`. For the given IP network, `1.1.1.0/28` is the CIDR notation.

is_cidr()

The `is_cidr()` function accepts an `ipnetwork` as an input. And, it returns `True` if the specified value matches the CIDR notation of the IP network.

Example-1:

The `is_cidr(1.1.1.0/24)` function returns `True` because the specified value is the CIDR notation of the given network.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example-2:

The `is_cidr(1.1.1.1/28)` function returns `False` because the CIDR notation of the given network is different than the specified value.

is_in_network()

The `is_in_network()` function accepts `ipnetwork` and `ipaddress` values. And, it returns `True` if the specified IP address exists in the specified IP network.

Example-1:

The `is_in_network(1.1.1.1/24, 1.1.1.121)` function returns `True` because the `1.1.1.121` address is part of the `1.1.1.1/24` network.

Example-2:

The `is_in_network(1.1.1.1/28, 2.1.1.1)` function returns `Fasle` because the `2.1.1.1` address is not part of the `1.1.1.1/28` network.

base64.encode()

The `base64.encode()` function takes a string argument and returns the base64 encoded string.

Example:

The `base64.encode("abcd")` function returns `YWJjZA==`.

base64.decode()

The `base64.decode` function takes a base64 encoded string as an argument and returns the decoded string.

Example:

The `base64.decode("YWJjZA==")` function returns `abcd`.

exists()

The `exists()` function takes an argument of any type and returns a boolean. The return value is `True` if the input has any value. The return value is `False` If the input argument does not have a value (that is, no value).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Consider that the `$parameters.monitor` is an optional parameter. If you provide a value to this parameter when creating a configuration pack, exist the `($parameters.monitor)` function returns `True`.

Otherwise, it returns `False`.

filter()

The `filter()` function takes two arguments.

Argument 1: a substitution function that takes one argument and returns a Boolean value.

Argument 2: a list.

The function returns a subset of the original list where each element evaluates to `True` when passed to the substitution function in the first argument.

Example:

Suppose we have defined a substitution function as follows.

Substitutions:

```
x(a): $a != 81
```

This function returns True if the input value is not equal to `81`. Otherwise, it returns `False`.

Suppose, `$parameters.ports` is `[81, 80, 81, 89]`.

The `filter($substitutions.x, $parameters.ports)` returns `[80, 89]` by removing all occurrences of `81` from the list.

if-then-else()

The function `if-then-else()` takes three arguments.

Argument 1: a Boolean expression

Argument 2: any expression

Argument 3: any expression (optional)

If the expression in argument 1 evaluates to `True`, the function returns the value of the expression provided as argument 2.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Otherwise, if argument 3 is provided, the function returns the value of the expression in argument 3.

If argument 3 is not provided, the function returns `no`.

Example 1:

The `if-then-else($parameters.servicetype == HTTP, 80, 443)` function returns `80` if `$parameters.servicetype` has value `HTTP`. Otherwise, the function returns `443`.

Example 2:

The `if-then-else($parameters.servicetype == HTTP, $parameters.hport, $parameters.sport)` function returns the value of `$parameters.hport` if `$parameters.servicetype` has value `HTTP`.

Otherwise, the function returns the value of `$parameters.sport`.

Example 3:

The `if-then-else($parameters.servicetype == HTTP, 80)` returns `80` if `$parameters.servicetype` has value `HTTP`.

Otherwise, the function does not return any value.

join()

The `join()` function takes two arguments:

Argument 1: a list of `number`, `tcp-port`, `string`, `ipaddress`

Argument 2: a delimiter string (optional)

This function joins the elements of the list provided as argument 1 into a string, where each element is separated by the delimiter string provided as argument 2. If argument 2 is not provided, then the elements in the list are joined as one string.

Example:

- `$parameters.ports` is `[81, 82, 83]`.
    - With delimiter argument:

      The `join($parameters.ports, '-')` function returns `81-82-83`.
    - Without delimiter argument:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The `join($parameters.ports)` function returns `818283`.

split()

The `split()` function splits an input string into multiple lists depending on the specified separators. If no or blank (`''`) separator is specified, this function considers space as a separator and splits the string into lists.

Examples:

- The `split('Example_string_split', 's')` function returns `['Example_','tring_','plit']`.
- The `split('Example string split')` function returns `['Example','string','split']`.
- The `split('Example string split', '')` function returns `['Example','string','split']`.
- The `split('Example string')` function returns `['Example','string']`.

  This function considers continuous spaces as one space.

map()

The `map()` function takes two arguments;

Argument 1: any function

Argument 2: a list of elements

The function returns a list where each element in the list is the result of applying the `map()` function (argument 1) to the corresponding element in argument 2.

Allowed functions in argument 1:

- Built-in functions that take one argument:

  `base64.encode, base64.decode, bin, bool, exists, hex, int, ip, len, lower, upper, oct, quotewrap, str, trim, upper, url.encode, url.decode`
- Substitution functions that take at least one argument.

Example:

Suppose $parameters.nums is `[81, 82, 83]`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Map using a built-in function, str

  The `map(str, $parameters.nums)` function returns `["81", "82", "83"]`

  The result of the map function is the list of strings where each element is string is computed by applying the str function on the corresponding element in the input list ($parameters.nums).

- Map using a substitution function

  - Substitutions:

    `add-10(port): $port + 10`

  - Expression:

    The `map($substitutions.add-10, $parameters.nums)` function returns a list of numbers: `[ 91, 92, 93 ]`

The result of this map function is a list of numbers. Each element is computed by applying the substitution function `$substitutions.add-10` on the corresponding element in the input list `($parameters.nums)`.

quotewrap()

The `quotewrap()` function takes a string as an argument and returns a string after adding a double quote character before and after the input value.

Example:

The `quotewrap("NetScaler Console")` function returns `"NetScaler Console"`

replace()

The `replace()` function takes three arguments:

Argument 1: a `string` or list of the following built-in types:

- `string`
- `number`
- `ipaddress`
- `tcp-port`
- `boolean`

Argument 2: a single value or a list of values whose type matches the type specified in argument 1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Argument 3: a single value of the same type as specified in argument 1 (optional)

The `replace()` function replaces all occurrences of argument 2 with argument 3 in argument 1.

If argument 3 is not provided, all occurrences of argument 2 are removed from argument 1.

Example:

- `replace('abcdef', 'def', 'xyz')` function returns `abcxyz`.

  All occurrences of `def` are replaced with `xyz`.
- `replace('abcdefabc', 'def')` returns `abcabc`.

  As there is no argument 3, `def` is removed from the resulting string.
- `replace('An#example@to%replace!characters', ['@', '#', '!', '%'], '_')` function returns `An_example_to_replace_characters`.

  The output string has underscore (_) instead of the characters specified in `['@', '#', '!', '%']`.
- `replace([10.10.10.1, 10.10.10.2, 10.10.10.3, 10.10.10.4], [10.10.10.2, 10.10.10.4])` function returns `[10.10.10.1, 10.10.10.3]`.

  As there is no argument 3, `10.10.10.2` and `10.10.10.4` are removed from the resulting list of IP addresses.
- `replace([8080, 8081, 8082, 8083, 8084], 8083, 80)` function returns `[8080, 8081, 8082, 80, 8084]`.

  All occurrences of `8083` are replaced with `80`.

trim()

The `trim()` function returns a string where the leading and trailing whitespaces are stripped from the input string.

Example:

The `trim(' abc ')` function returns `abc`.

truncate()

The `truncate()` function takes two arguments:

Argument 1: a string

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Argument 2: a number

The function returns a string where the input string in argument 1 is truncated to the length specified by argument 2.

Example:

The `truncate('Stylebooks', 6)` returns `Styleb`.

distinct()

The `distinct()` function extracts unique items from a list input.

Examples: If `$parameters.input_list` is `['ADC', 'VPX', 'ADC', 'CPX']`, the `distinct($parameters.input_list)` function returns `['ADC', 'VPX', 'CPX']`.

url.encode()

The `url.encode()` function returns a string where characters are transformed using the ASCII character set according to RFC 3986.

Example:

The `url.encode("a/b/c")` function returns `a%2Fb%2Fc`.

url.decode()

The `url.decode()` function returns a string where the URL encoded argument is decoded in to a regular string according to RFC 3986.

Example:

The `url.decode("a%2Fb%2Fc")` function returns `a/b/c`.

is-ipv4()

The `is-ipv4()` function takes an IP address as an argument and returns the boolean `True` if the IP address is of the IPv4 format.

The `is-ipv4(10.10.10.10)` function returns `True`

is-ipv6()

The `is-ipv6()` function takes an IP address as an argument and returns the boolean `True` if the IP address is of the IPv6 format.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The `is-ipv6(2001:DB8::)` function returns `True`

startswith()

The `startswith()` function determines whether a string begins with a given prefix. This function requires two mandatory string arguments.

`startswith(str, sub_str)`

This function returns `True` when the string (`str`) starts with the substring (`sub_str`).

Examples:

- The `startswith('Citrix', 'Ci')` function returns `True`.
- The `startswith('Citrix', 'iC')` function returns `False`
- The `startswith('Citrix', 'Ab')` function returns `False`

endswith()

The `endswith()` function determines whether a string ends with a given suffix. This function requires two mandatory string arguments.

`endswith(str, sub_str)`

This function returns `True` when the string (`str`) ends with the substring (`sub_str`).

Examples:

- The `endswith('Citrix', 'ix')` function returns `True`.
- The `endswith('Citrix', 'Ix')` function returns `False`.
- The `endswith('Citrix', 'ab')` function returns `False`.

contains()

The `contains()` function determines whether a string contains a given substring. This function requires two mandatory string arguments.

Allowed argument types:

- `string`
- `number`
- `tcp-port`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `boolean`
- `ipaddress`

`contains(str, sub_str)`

This function returns `True` when the substring (`sub_str`) is contained anywhere inside the string (`str`).

Examples:

- The `contains('Citrix', 'tri')` function returns `True`.
- The `contains('Citrix', 'Ci')` function returns `True`.
- The `contains('Citrix', 'ti')` function returns `False`

You can also use this function to check whether a given item belongs to the list.

Example:

```
list_of_strings = [“Citrix”, “Core”, ”Values”, ”Integrity”]



contains($parameters.list_of_strings, “Values”)
```

In this example, the `contains()` function returns `True` because the list has the `Values` item in it.

substring()

Use the `substring()` function to extract a substring from a string.

`substring(str, start_index, end_index)`

This function requires the two mandatory arguments and one optional integer argument.

- `str` (Mandatory)
- `start_index` (Mandatory)
- `end_index` (Optional)

This function returns the substring from the string (`str`) that is between the specified index positions. If you do not specify the end index position, the function extracts the substring from the start index to the end of the string.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

When you specify `end_index`, the substring excludes the character at the `end_index` position.

Example:

- The `substring('Citrix', 2)` function returns `trix`
- The `substring('Citrix', 10)` function returns (`''`)

  In this example, the function returns a blank string because it has an invalid `start_index` position.
- The `substring('Citrix', 2, 4)` function returns `tr`

  In this example, the function extracts the characters between 2 and 4 index positions.
- The `substring('Citrix', -3)` function returns `rix`

  If you want to extract characters that are at the end of the string, specify a negative value for the `start_index` argument.

  In this example, the function extracts the substring that includes the last three characters in the string.

match()

The `match()` function checks whether an input string matches the defined regular expression pattern. This function accepts regular expression pattern and search strings as arguments. Optional, you can also specify a Boolean type to ignore case sensitive patterns.

Examples:

- The `match("\^[A-Z0-9]{2}_[A-Z0-9]{2,10}$", "A2_B2")` returns `True`.
- The `match("\^[A-Z0-9]{2}_[A-Z0-9]{2,10}$", "a2_b2")` returns `False`.
- The `match("\^[A-Z0-9]{2}_[A-Z0-9]{2,10}$", "a2_B2", $parameters.ignore_case)` returns `True`.

sha256()

Use this function to compute the SHA-256 hash for any string. This function accepts a string input of any length and returns a hash string of fixed length (64 characters).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example:

```
components:

    -

        name: lbvserver-comp

        type: ns::lbvserver

        properties:

            name: sha256(lbserver-name)

            servicetype: SSL

            ipv46: 10.10.10.10
```

In this example, `lbserver-name` appears as a hash string on the NetScaler object.

This function can also accept expressions as an input.

Example:

```
components:

    -

        name: lbvserver-comp

        type: ns::lbvserver

        properties:

            name: sha256($parameters.lb-appname)

            servicetype: SSL

            ipv46: 10.10.10.10
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

relate()

The `relate()` function forms a list of dictionary objects from a set of lists.

It takes two arguments:

Argument 1: A list of strings which represent key names.

Argument 2: A list of lists, where each list has the values of the corresponding key names in argument 1. Each list in argument 2 must be of the same length. The number of lists in argument 2 should be equal to the number of strings in argument 1.

Example:

```
name: test_relate_3

description: "Hello World StyleBook."

namespace: com.citrix.adc.stylebooks

schema-version: "1.0"

version: "1.1"



import-stylebooks:

    -

        namespace: netscaler.nitro.config

        prefix: ns

        version: "10.5"

    -

        namespace: com.citrix.adc.stylebooks

        prefix: stlb

        version: "1.0"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        parameters:
    -
        name: namesofservers
        description: "Provide the names of LB VServers"
        type: string[]
    -
        name: listofips
        description: "Provide the list of IP Addresses"
        type: string[]
    -
        name: list_of_keys
        type: string[]
        default:
        - "name"
        - "ip"


    substitutions:
        list_of_values: [$parameters.namesofservers,$parameters.listofips]
    components:
    -
        name: svc-comp
        type: object
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        properties:

        svcdetails: relate($parameters.list_of_keys,
$substitutions.list_of_values)



    -

        name: lb-comp

        type: ns::lbvserver

        repeat: $components.svc-comp.properties.svcdetails

        repeat-item: svcd

        properties:

            name: $svcd['name']

            servicetype: HTTP

            ipv46: $svcd['ip']

            port: 80
```

In this example:

- The `parameters` section has a list called `list_of_keys` which has `name` and `ip`.
- The `substitutions` section has a list called `list_of_values` which has the following two lists:
  - A list of virtual server names (`string`)
  - A list of IP addresses (`string`).

The `relate()` built-in function accepts the `list_of_keys` and `list_of_values` as the arguments. The function then creates a list of dictionary objects where each object has a name from the first list and an IP address from the second list.

If you provide the following list of virtual servers:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
["lb1","lb2"]
```

and a list of virtual server IP addresses as:

```
["1.1.1.1","2.2.3.3"]
```

The `relate()` function then returns the following lists:

```
[\{"name": "lb1", "ip": "1.1.1.1"},\{"name": "lb2", "ip": "2.2.3.3"}]
```

The StyleBook iterates over this list of dictionary objects, in the `components` section, to create the corresponding virtual servers.

multiple()

The `multiple()` function takes two arguments:

Argument 1: a `number`, `string`, `boolean`, `ipaddress`, `tcp-port`, or `password`

Argument 2: a `number`

The `multiple(argument1, argument2)` function returns a list with many copies of argument 1. The number of copies is equal to the number passed to argument 2.

Examples:

- The `multiple(10.10.10.10, 3)` function returns `[10.10.10.10, 10.10.10.10, 10.10.10.10]`.
- The `multiple(8080, 4)` function returns `[8080, 8080, 8080, 8080]`.

reverse()

The reverse() function takes a list of items as an argument and returns a list with the same items but listed in the reverse order.

Argument can be a list of the following built-in types:

- string
- number
- ipaddress

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ipnetwork
- tcp-port
- boolean
- password
- object
- file
- certfile
- keyfile
- certkey

Examples:

- reverse() returns .
- reverse() returns .
- reverse() returns .

Dependency detection

Components in a StyleBook can refer to properties or sections of other components in the same StyleBook. Components are complete blocks by themselves and they may not be written in the same order that they have to be ran. The StyleBook compiler checks the order in which the components are written and then runs them in a logical order.

Example:

```
components:

  -

    name: lbvserver-comp

    type: ns::lbvserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    properties:

      name: mylb

      ipv46: 10.102.190.15

      port: 80

      servicetype: HTTP

-
   name: lb-sg-binding-comp

   type: ns::lbvserver_servicegroup_binding

   condition: $parameters.create-binding

   properties:

     name: $components.lbvserver-comp.properties.name
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      servicegroupname: $components.sg-comp.properties.servicegroupname


-

    name: sg-comp


    type: ns::servicegroup


    properties:


      servicegroupname: mysg


      servicetype: HTTP
```

In the above example, there are three components defined - **lbvserver-comp**, **lb-sg-binding-comp**, and **sg-comp**. When you run this StyleBook, the `lbvserver-comp` is first created. The `lb-sg-binding-comp` refers to `lbvserver-comp` properties, but it cannot be created next though it is the second component defined in the StyleBook. This is because the `lb-sg-binding-comp` also has a dependency on the `sg-comp` which is yet to be created. As a result, the compiler reorders the components so that the dependencies of a component are resolved by the time a component is created, and runs this reordered list of components. The order of execution of the above StyleBook is: `lbvserver-comp`, `sg-comp`, and `lb-sg-binding-comp`.

Thus, the author of a StyleBook need not worry about the correct order of the components. The components may appear in any order. The compiler computes the correct order of execution of the components based on how the components refer each other. Note that this applies to substitutions and outputs sections as well.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cyclic Dependencies

Since a component may refer another component, it is possible that the cycle of dependencies may be introduced in the definition of the StyleBook. For example, if component A refers to a property defined in component B, which again refers to a property defined in component A. This kind of dependency is called cyclic dependencies. Cyclic dependencies cannot be resolved automatically. The author of the StyleBook manually corrects the StyleBook definition to eliminate such cyclic dependencies. The compiler will be able to identify cyclic dependencies - if they exist, and report it.

The following example shows a cyclic dependency of components:

```
components:

  -

    name: lbvserver-comp

    type: ns::lbvserver

    properties:

      name: $components.lb-sg-binding-comp.properties.name

      ipv46: 10.102.190.15

      port: 80
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    servicetype: HTTP

-

  name: lb-sg-binding-comp

  type: ns::lbvserver_servicegroup_binding

  condition: $parameters.create-binding

  properties:

    name: mylb

    servicegroupname: $components.sg-comp.properties.servicegroupname

-

  name: sg-comp

  type: ns::servicegroup
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    properties:


      servicegroupname: mysg


      servicetype: $components.lbvserver-comp.properties.servicetype
```

In the above example, there are three components: **lbvserver-comp**, **lb-sg-binding-comp**, and **sg-comp**. The `lbvserver-comp` component depends on `lb-sg-binding-comp`, `lb-sg-binding` components. And, these components depend on `sg-comp`. The `sg-comp` component depends on `lbvserver-comp`. Here, a cycle of dependencies among these components is formed and this cannot be resolved automatically. As a result, this StyleBook cannot be ran. The StyleBook compiler detects this and prevents the StyleBook from being imported into NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Security

The NetScaler Console security features provide visibility into the security posture of your applications. You can monitor security metrics, investigate security violations, protect your APIs, and use web application firewall (WAF) learning and recommendations to strengthen your security configuration.

The following topics help you monitor and manage application security:

- Application security dashboard
  - Unified security dashboard
- Security violations
  - Application overview
  - All violations
- API Security
- WAF learning
- WAF recommendations

Application Security Dashboard

The **App Security** dashboard provides you the overview of security metrics for the discovered applications. This dashboard displays the security attack information for the discovered applications, such as sync attacks, small window attacks, DNS flood attacks.

To view the security metrics on app security dashboard:

1. Navigate to **Security > Security Dashboard**.
2. Select the instance IP address from the Instance list.

   The reports include the following information for each application:

   - **Threat index**. A single-digit rating system that indicates the criticality of attacks on the application. The more critical the attacks on an application, the higher the threat index for that application. The values range from 1 through 7.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

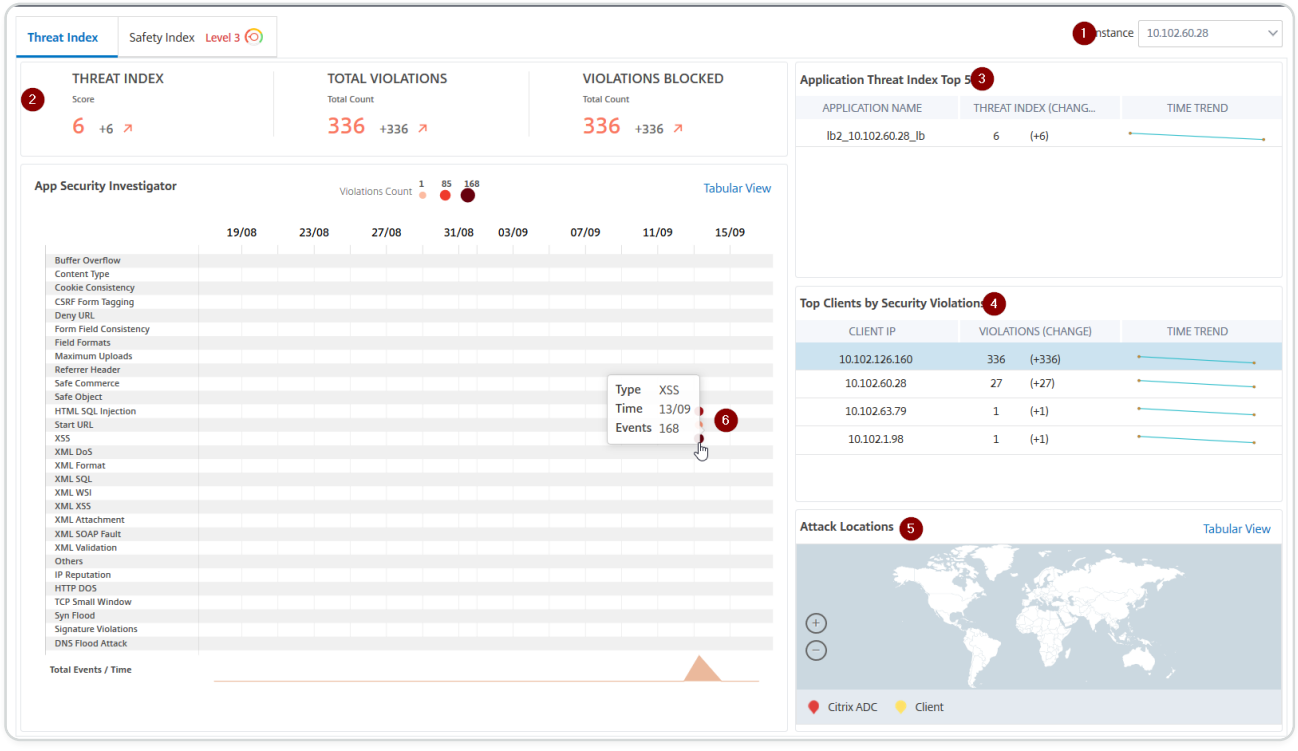
The threat index is based on attack information. The attack-related information, such as violation type, attack category, location, and client details, gives an insight into the attacks on the application. Violation information is sent to NetScaler Console only when a violation or attack occurs. Many breaches and vulnerabilities lead to a high threat index value.

- **Safety index**. A single-digit rating system that indicates how securely you have configured the NetScaler instances to protect applications from external threats and vulnerabilities. The lower the security risks for an application, the higher the safety index. The values range from 1 through 7.

  The safety index considers both the application firewall configuration and the NetScaler system security configuration. For a high safety index value, both configurations must be strong. For example, if rigorous application firewall checks are in place, but NetScaler system security measures, such as a strong password for the nsroot user is not provided, then applications are assigned a low safety index value.

You can view discrepancies reported on the **App Security Investigator**.

Threat index details



1 - Displays the NetScaler instance IP address for which you can view details.

2 - Displays details such as threat index score, total violations occurred, and total violations blocked.

3 - Displays the virtual server of the selected instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

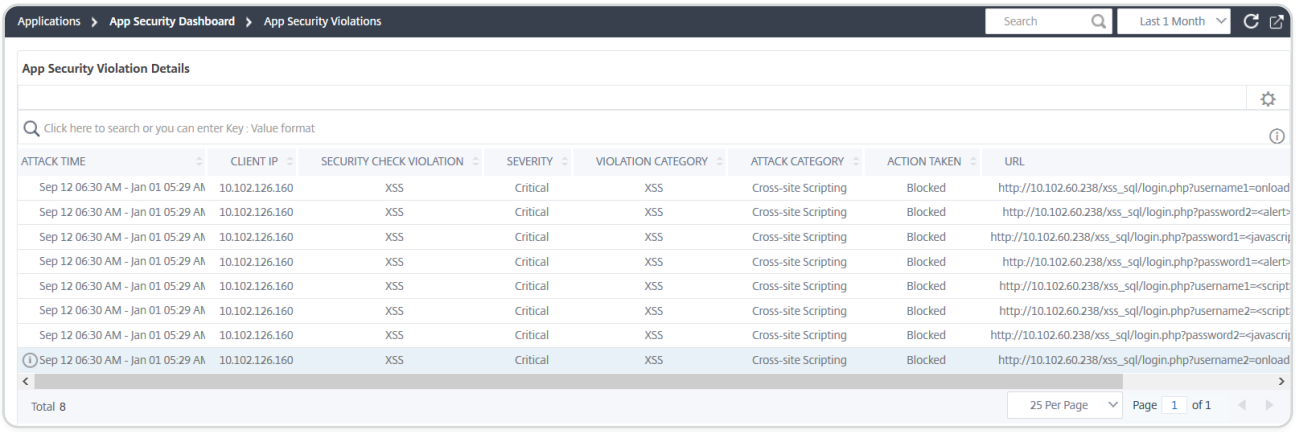
4 - Displays the security violations based on clients. The App Security Investigator graph is displayed for each client. You can click each client IP to view results.

5 - Displays the violations in map view and tabular view.

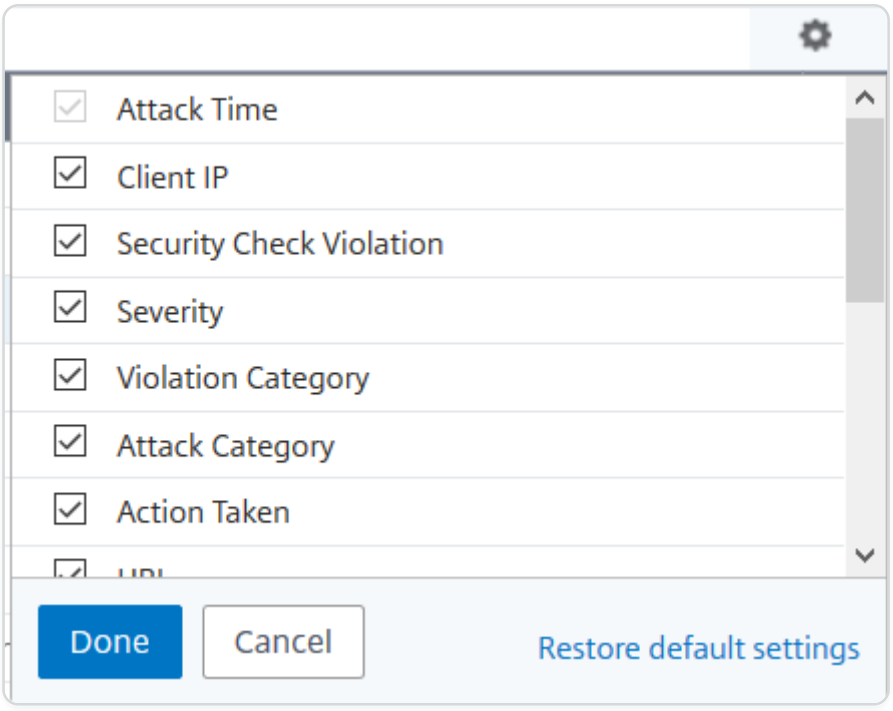
6 - Displays the violation details. When you hover the mouse pointer on the graph, the details such as violation type, time of the attack, and total events are displayed.

When you click a bubble graph, the details are displayed in the **App Security Violation Details** page. For example, if you want to further view details for cross-site script violation, click the graph populated for **XSS** in **App Security Investigator**.

The **App Security Violation Details** is displayed with violation details such as attack time, attack category, severity, URL, and so on.



You can also click the **Settings** option to select the options that you want to get it displayed.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Safety index details

After reviewing the threat exposure of an application, you want to determine what application security configurations are in place and what configurations are missing for that application. You can obtain this information by drilling down into the application safety index summary.

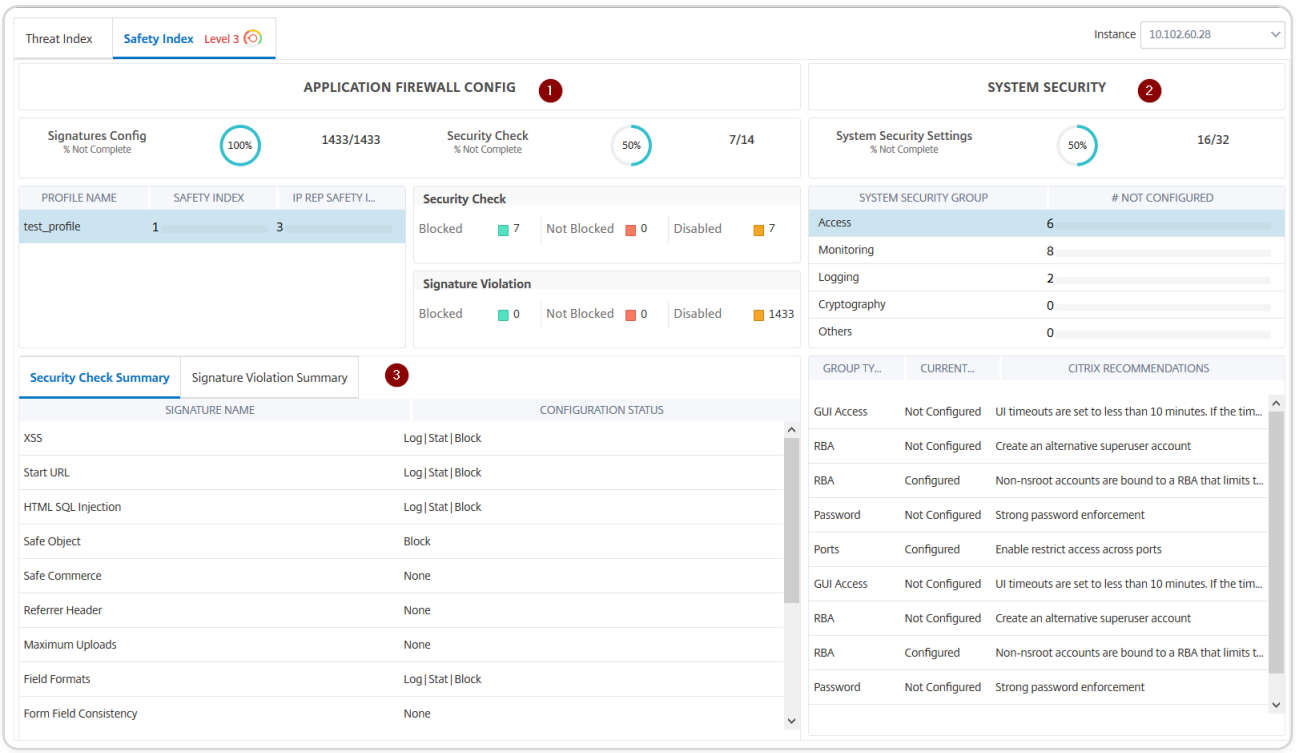
The safety index summary gives you information about the effectiveness of the following security configurations:

- **Application Firewall Configuration**. Shows how many signature and security entities are not configured.
- **NetScaler Console System Security**. Shows how many system security settings are not configured.

To view the **Safety Index** details, select a virtual server/application and click the **Safety Index** tab.



The details are displayed.



1 - Displays the detailed information for Application Firewall configurations.

2 - Displays the detailed information for System Security. Click each security group to get details on status and Citrix recommendations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3 - Displays the summary for Security Check and Signature Violation.

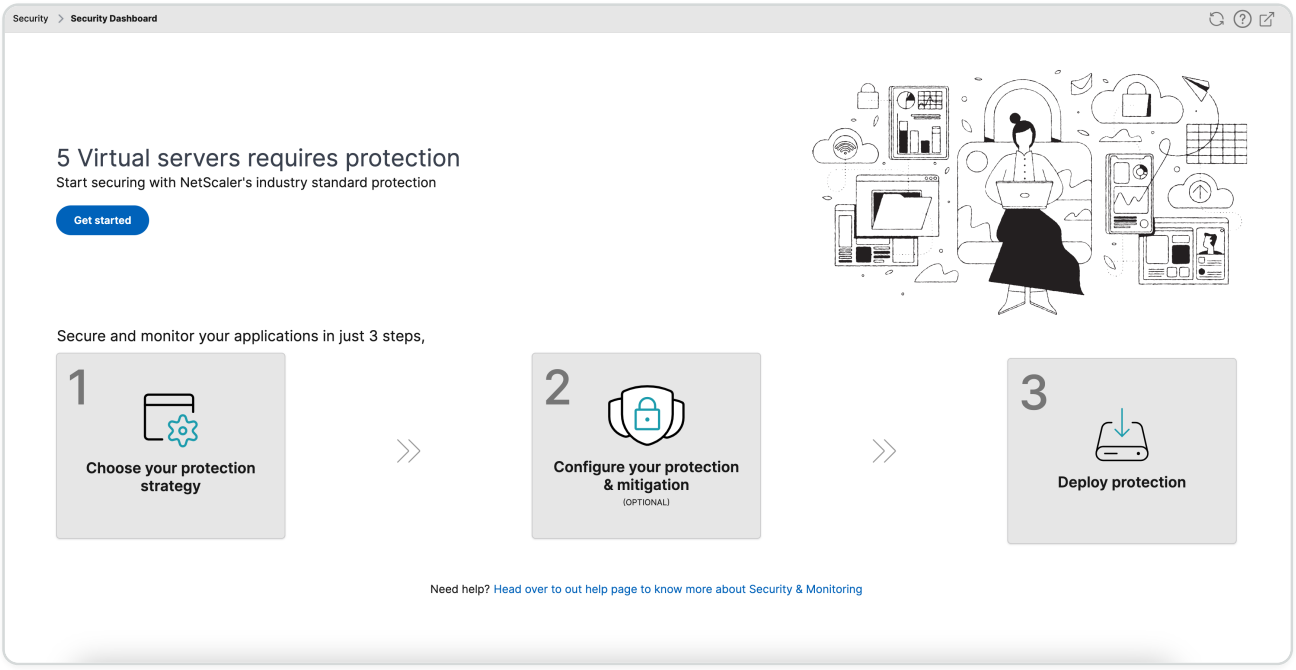
You can also view summary of the threat environment by enabling the security insight for virtual servers and then navigating to **Security > Security violations**. For more information on safety index use case, see security insight.

Unified Security dashboard

The **Unified Security** dashboard is a single-pane dashboard where you can configure protections, enable analytics, and deploy the protections on your application. In this dashboard, you can choose from various template options and complete the entire configuration process in a single workflow. To get started, navigate to **Security > Security Dashboard** and then click **Manage Application**. In the **Manage Application** page, you can view details of your secured and unsecured applications.

NOTE:

- If you are a new user or if you have not configured any protections either through StyleBooks or directly on NetScaler® instances, the following page appears after you click **Security > Security Dashboard**.



- You can view the total number of virtual servers that require protection. Click **Get Started** to view details in **Unsecured Applications**.

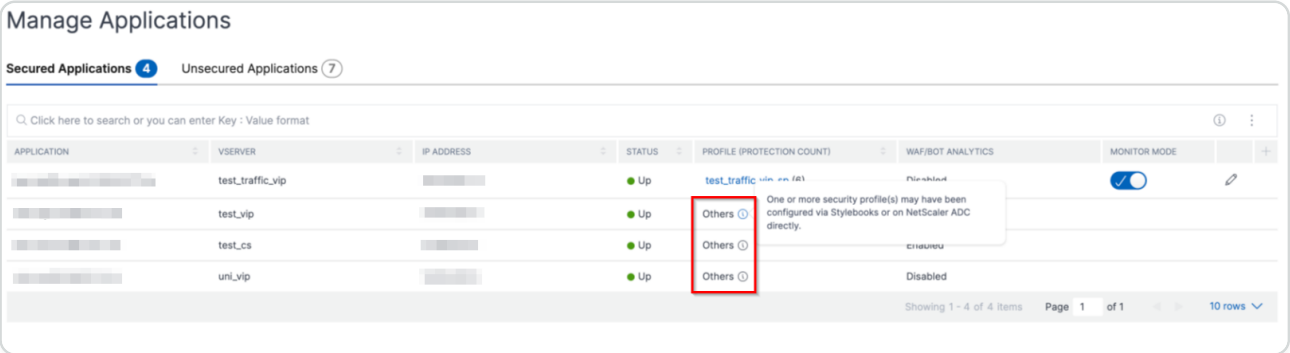
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The eligible virtual server types for configuring protections are load balancing and content switching.

Secured applications

You can view details after you configure protections using the unified security dashboard. For more information, see Configure protections for unsecured applications.

If you have already configured protections directly on the NetScaler instances or through StyleBooks, you can view the applications in the **Secured Applications** tab marked as **Others** under **Profile**.



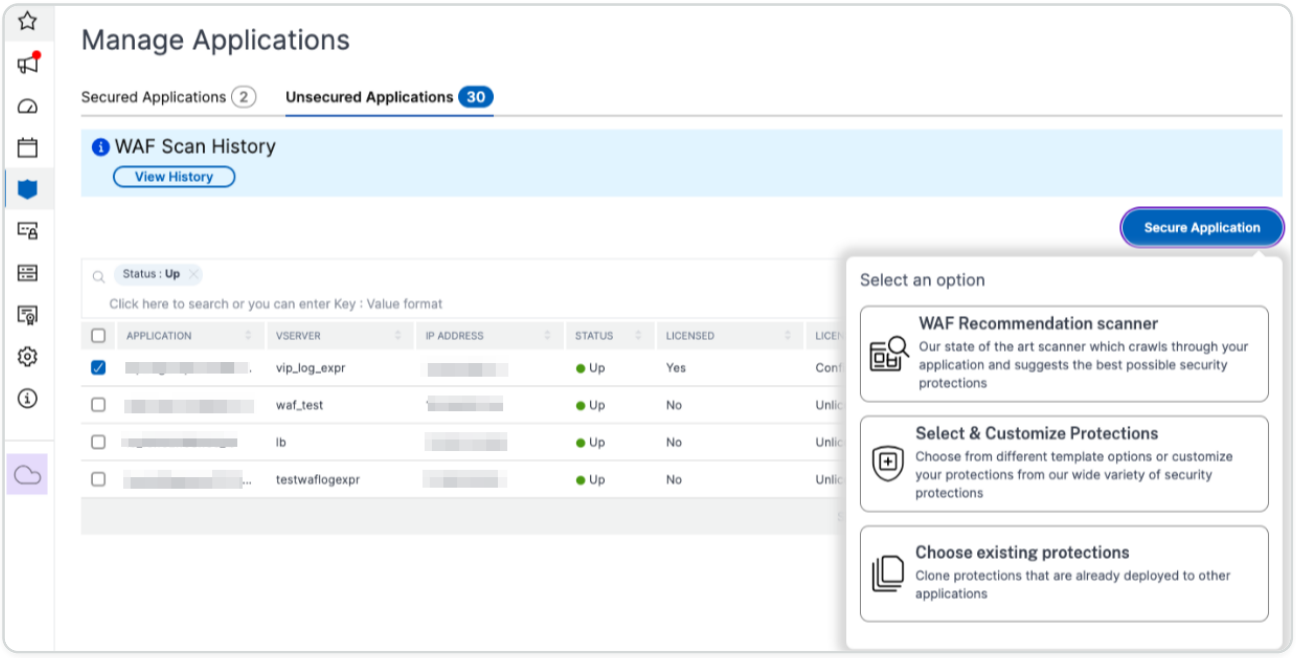
Configure protections for unsecured applications

NOTE:

The maximum supported configuration entities (rules) in Block list is 32.

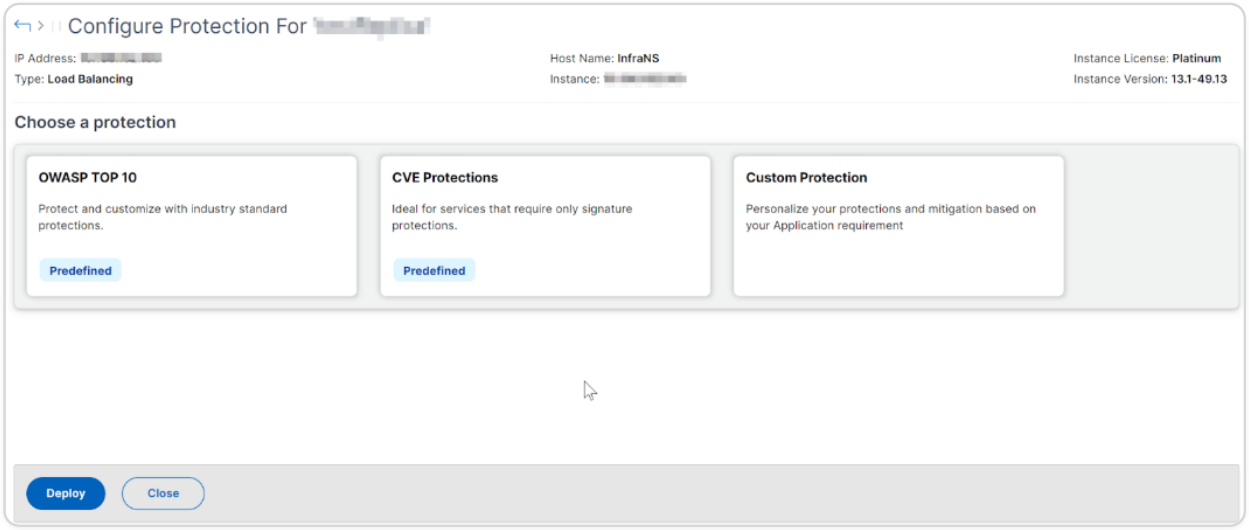
In the **Unsecured Applications** tab, select an application, and click **Secure Application**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can select either of the following options to protect your application:

- WAF Recommendation scanner - This option enables you to run a scan on your application. Based on certain parameters of the scan, the result suggests you the protections for your application. You might consider applying those recommendations.
- Select & Customize Protections - This option enables you to choose from different template options or customize your protections and deploy.



  - **OWASP Top 10** - A predefined template that has the industry-standard protections against the OWASP top-10 security risks. For more information, see `https://owasp.org/www-project-top-ten/`.
  - **CVE Protections** - You can create the signature set from the list of pre-configured signature rules classified under known vulnerability categories. You can select signatures to

© 1997–2026 Citrix Systems, Inc. All rights reserved.

configure log or block action when a signature pattern matches the incoming traffic. The log message contains the vulnerability details.

- **Custom Protections** - Select the protections and deploy them based on your requirements.

- Choose existing protections - This option clones the protections that are deployed in an existing application. If you want to deploy those same protections to another application, you can select this option and deploy it to another application as it is. You can also select this option as a template, modify the protections, and then deploy.

WAF recommendation scanner

NOTE:

- You can run only one scan at a time for an application. To start a new scan for the same application or a different application, you must wait until the previous scan gets completed.
- You can click **View History** to view the history and status of the past scans. You can also click **View Report** and then apply recommendations later.

Prerequisites:

- The NetScaler instance must be 13.0 41.28 or later (for security checks) and 13.0 or later (for signatures).
- Must have the premium license.
- Must be the load balancing virtual server.

To get started with WAF recommendation scan, you must provide the following information:

1. Under **Scan Parameters**:
   - **Domain Name** – Specify a valid accessible IP address or the publicly reachable domain name that is associated with the application. For example: `www.example.com`.
   - **HTTP/HTTPS Protocol** – Select the protocol of the application.
   - **Traffic Timeout** – The wait time (in seconds) for a single request during the scan. The value must be greater than 0.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **URL to start scan from** – The home page of the application to initiate the scan. For example, `https://www.example.com/home`. The URL must be a valid IPv4 address. If the IP addresses are private, then you must ensure that the private IP address is accessible from the NetScaler Console management IP.
- **Login URL** – The URL to which the login data is sent for authentication. In HTML, this URL is commonly known as the action URL.
- **Authentication Method** – Select the supported authentication method (form based or header based) for your application.
    - Form-based authentication requires submitting a form to the login URL with the login credentials. These credentials must be in the form of form fields and their values. The application then shares the session cookie that is used to maintain sessions during the scan.
    - Header-based authentication requires the Authentication header and its value in the headers section. The Authentication header must have a valid value and is used to maintain sessions during the scan. The form-fields should be left empty for Header-based.
- **Request Method** – Select the HTTP method used when submitting form data to the login URL. The allowed request method is **POST**, **GET**, and **PUT**.
- **Form Fields** – Specify the form data to be submitted to the login URL. Form Fields are required only if you select the form-based authentication. You must specify in the key-value pairs, where **Field Name** is the Key and **Field Value** is the Value. Ensure that all form fields needed for login to work are added correctly, including passwords. The values are encrypted before storing it in the database. You can click **Add** to add multiple form fields. For example, **Field Name** – user name and **Field Value** – admin.
- **Logout URL** – Specify the URL that terminates the session after accessing. For example: `https://www.example.com/customer/logout`.

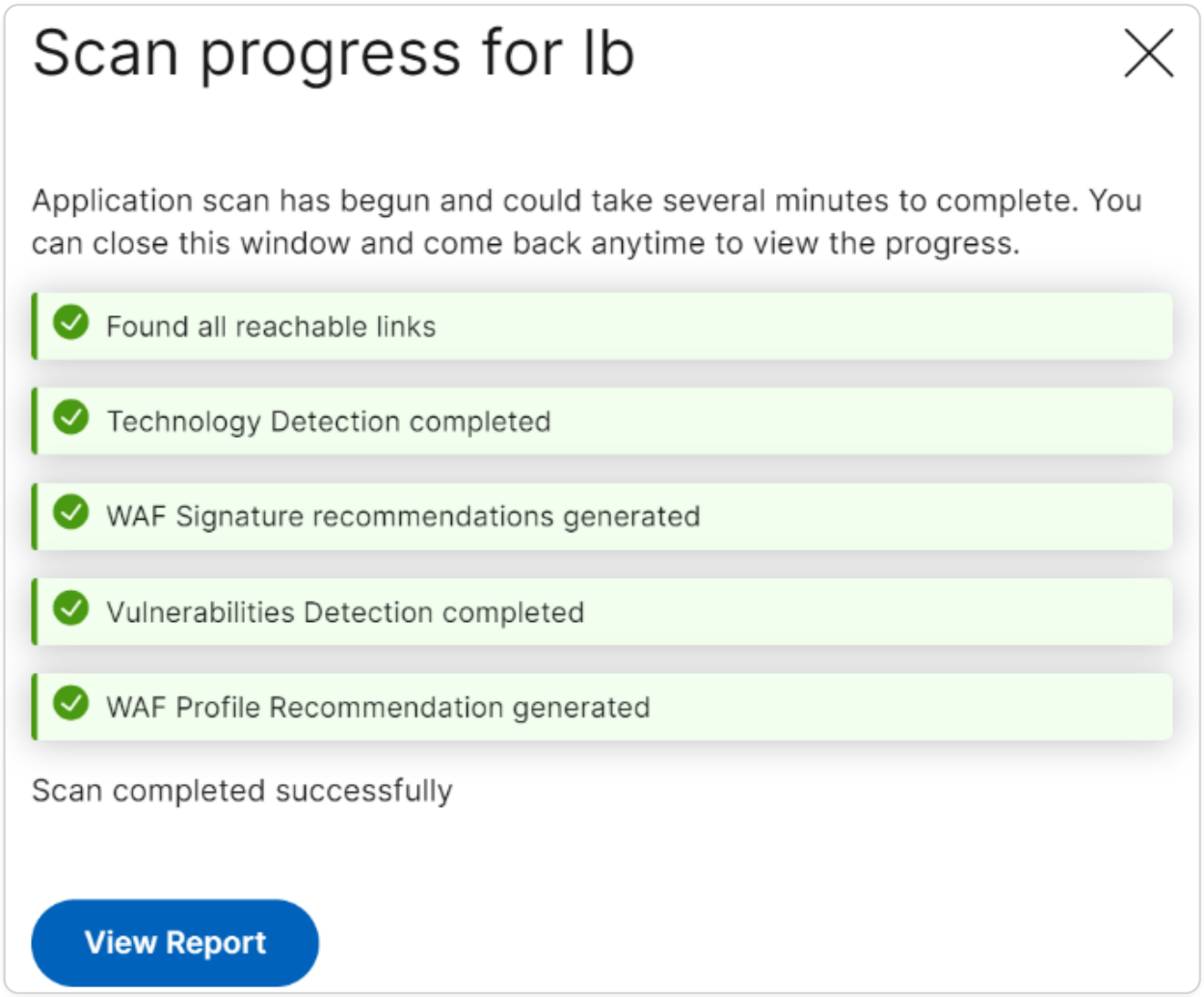
2. Under **Scan Configurations**:

- **Vulnerabilities to check** – Select the vulnerabilities for the scanner to detect them. Currently, this is done for SQL Injection and Cross-site scripting violations. By default, all the violations are selected. After selecting the vulnerabilities, it simulates these attacks on the application to report the potential vulnerability. It is recommended to enable this detection that is not in the production environment. All other vulnerabilities are also reported, without simulating these attacks on the application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

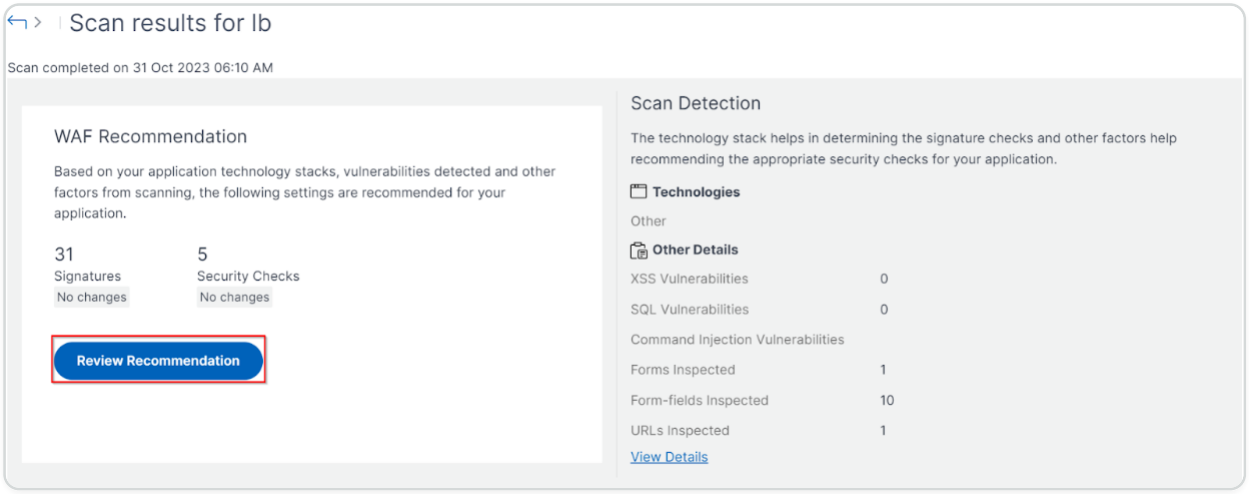
- **Response size limit** – The maximum limit on the response size. Any responses beyond the mentioned value are not scanned. The recommended limit is 10 MB (1000000 bytes).
- **Requests Concurrency** – The total requests sent to the web application in parallel.

3. The WAF scan settings configuration is complete. You can click **Start Scan** to begin the scanning process and wait for the progress to complete. After the scan is complete, click **View Report**.

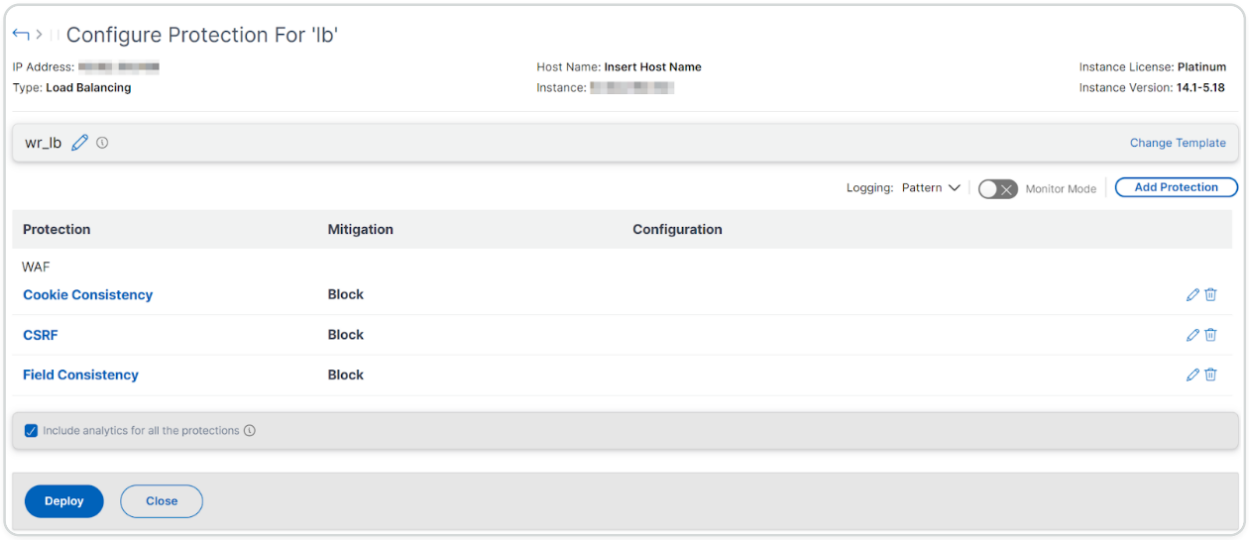


4. In the scan results page, click **Review Recommendation**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Review the protections or edit/add any other protections, and click **Deploy**.



When you apply security checks successfully:

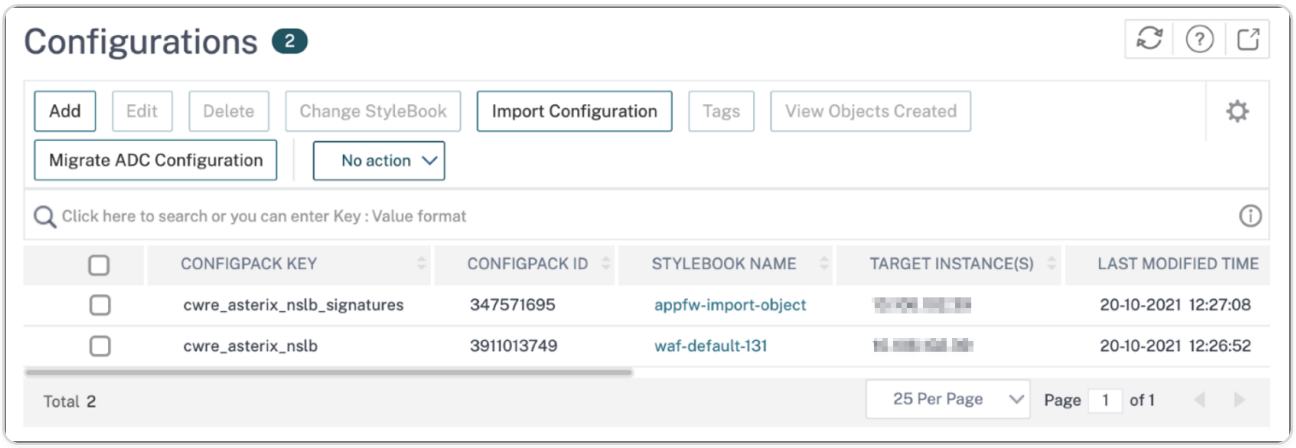
- The configuration is applied on the NetScaler instance through StyleBooks, depending upon the version.
  - For NetScaler 13.0, `unified-appsec-protection-130` StyleBook is used.
  - For NetScaler 13.1, `unified-appsec-protection-131` StyleBook is used.
  - For NetScaler 14.1, `unified-appsec-protection-141` StyleBook is used.
- The `Appfw` profile is created on your NetScaler and bound to the application using the `policylabel`.
- The signatures are bound to the appfw profile, if the recommended signatures are already applied.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

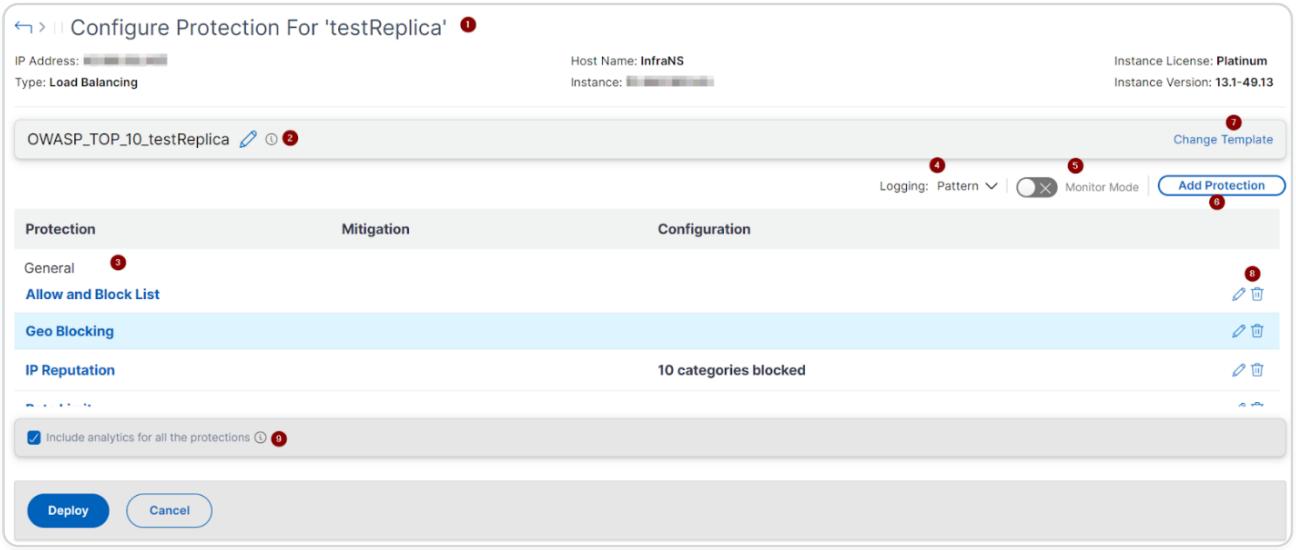
Security checks are supported in NetScaler 13.0 41.28 or later version.

You can verify the WAF profiles and signatures are applied through the default StyleBooks by navigating to **Applications > Configuration > Config Packs**.



Select and customize protections

OWASP TOP 10



1 - Provides information about the application such as IP address, virtual server type, license type, from which instance the application is configured, and so on.

2 - Displays the selected template. You can rename it based on your choice.

3 - Displays the protections. Some protections require additional information.

4 - Displays the verbose log type. You can select the following options:

- **Pattern**. Logs only violation pattern.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Pattern payload**. Logs violation pattern and 150 bytes of extra JSON payload.
- **Pattern, payload, header**. Logs violation pattern, 150 bytes of extra JSON payload and HTTP header information.

5 - Allows you to enable the Monitor Mode. If you enable Monitor Mode, the traffic is only logged and mitigations are not activated.

6 - Enables you to add more protections. Click **Add Protections** and review them to add.

7 - Allows you to choose a new template by using the Change Template option.

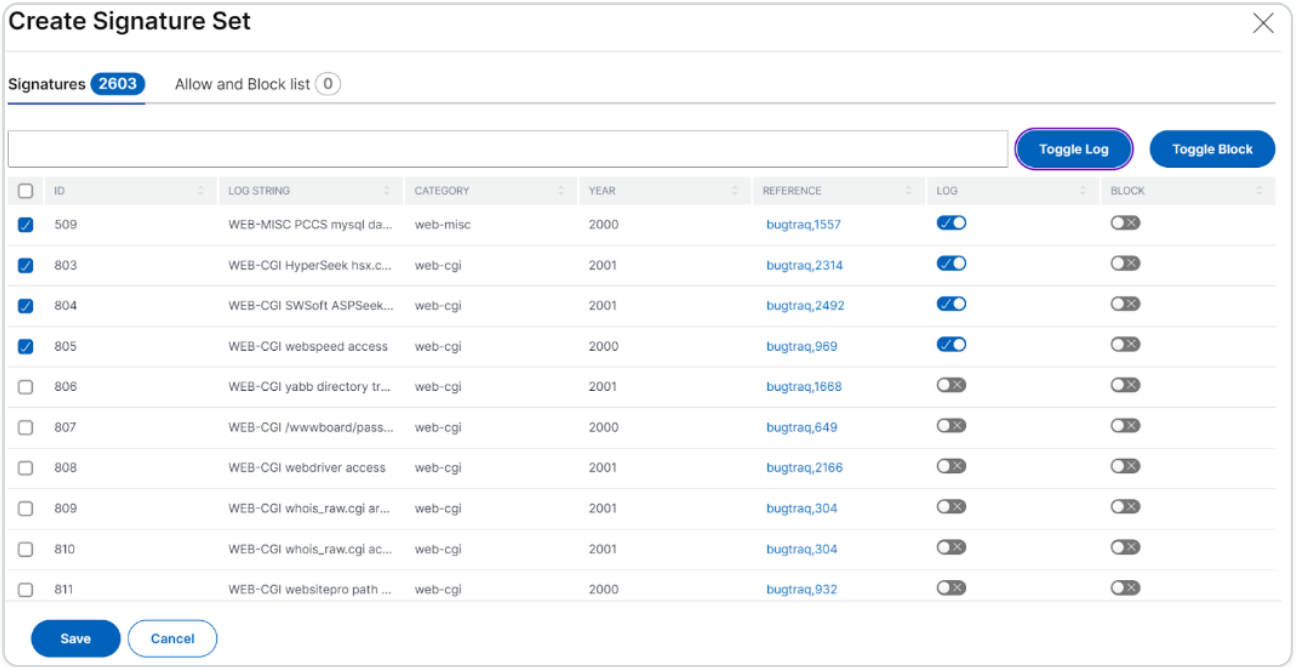
8 - Enables you to edit or delete the protection.

9 - Enables analytics for the protections that you select. This option is selected by default. You can view analytics for the configured protections at **Security > Security Violations**.

After you configure the protections, click **Deploy**.

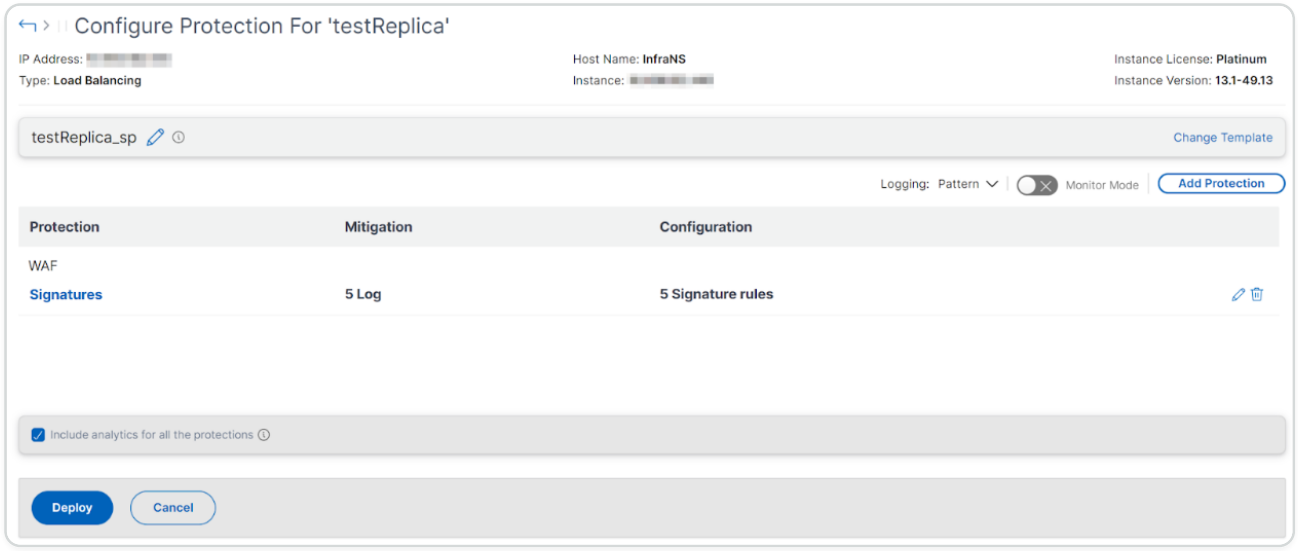
CVE PROTECTIONS

To deploy the CVE protections, click **Create CVE Protection**. In the **Create Signature Set** page, select the signatures from the list to configure the log or block action, and then click **Save**.



After you click **Save**, you can view the signatures added to the configuration page.

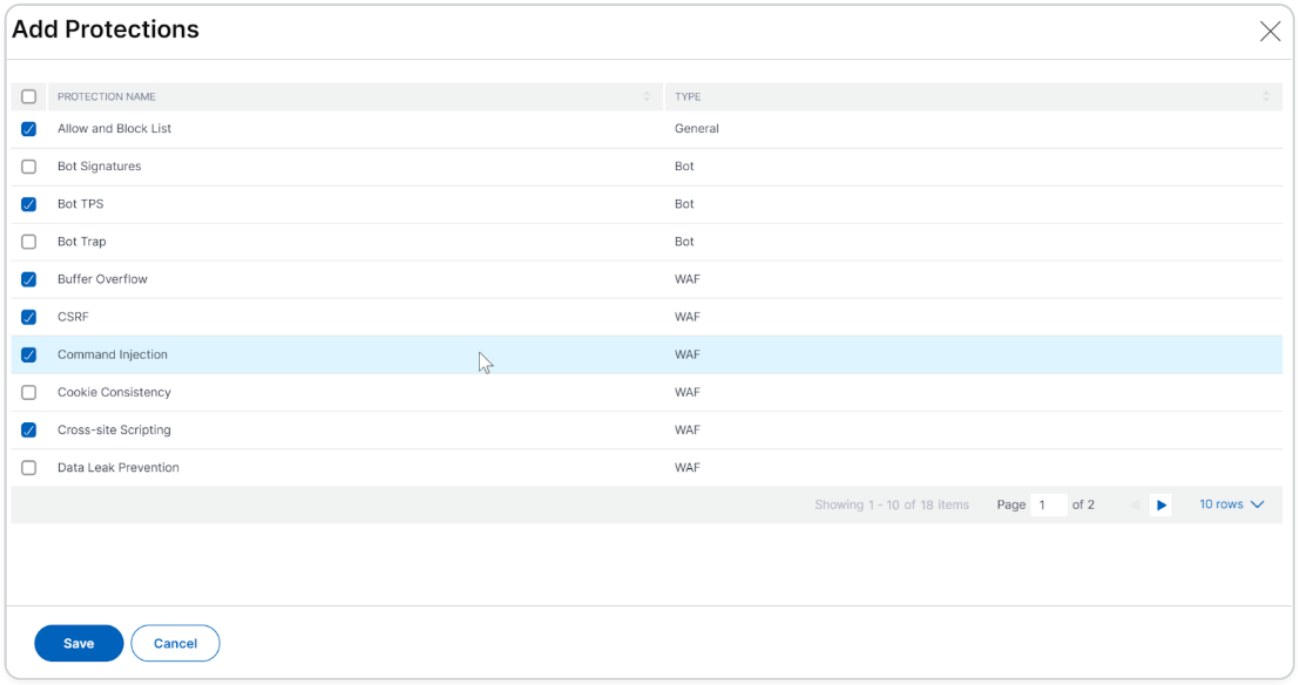
© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can also click **Add Protection** to add more protections to the application. After you configure all protections, click **Deploy**.

CUSTOM PROTECTION

To deploy with protections based on your requirement, click **Create new protection**. In the **Add Protections** page, select the protections that you want to deploy and click **Save**.

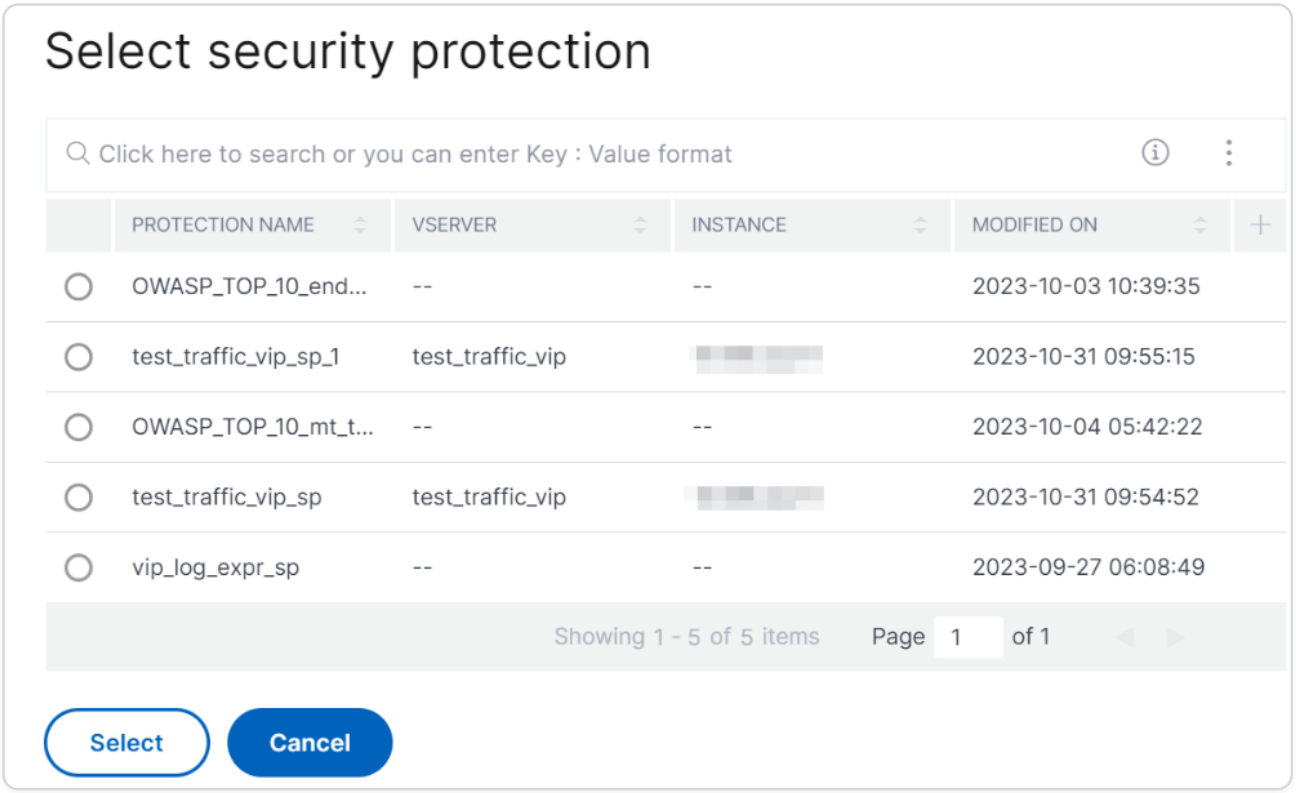


After you click **Save**, review the selected protections in the configuration page, and then click **Deploy**.

Choose existing protections

To deploy existing protections from one application to another, select an existing protection from the list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



After you select a protection, the existing protections are cloned and displayed in the configuration page. You can modify based on your requirement and then click **Deploy**.

View application security violation details

Web applications that are exposed to the internet have become vulnerable to attacks drastically. NetScaler Console enables you to visualize actionable violation details to protect applications from attacks. Navigate to **Security** > **Security Violations** for a single-pane solution to:

- Visualize applications with full visibility into the threat details associated in both WAF insight and bot insight. For more information, see Unified Security dashboard.
- Access the application security violations based on its categories such as **Network**, **Bot**, and **WAF**.
- Take corrective actions to secure the applications.

The **Security Violations** page has the following options:

- **Application Overview** – Displays an overview with applications that have total violations, total WAF and Bot violations, violation by country, and so on. For more information, see Application overview.
- **All Violations** – Displays the application security violation details. For more information, see All violations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Setting up

To view the violations, you must ensure:

- To get started with configuring protections and enabling analytics in your applications. For more information, see Unified Security dashboard.

  If you have configured protections either through StyleBook or directly on the NetScaler instance, you can follow the procedure to enable **WAF Security Violations** and **Bot Security Violations**:

  a. Navigate to **Infrastructure > Instances > NetScaler** and select the instance type. For example, VPX.
  b. Select the instance and from the **Select Action** list, select **Configure Analytics**.
  c. Select the virtual servers and click **Enable Security & Analytics**.
  d. On the **Enable Analytics** window, select **WAF Security Violations** and **Bot Security Violations**, and then click **OK**.

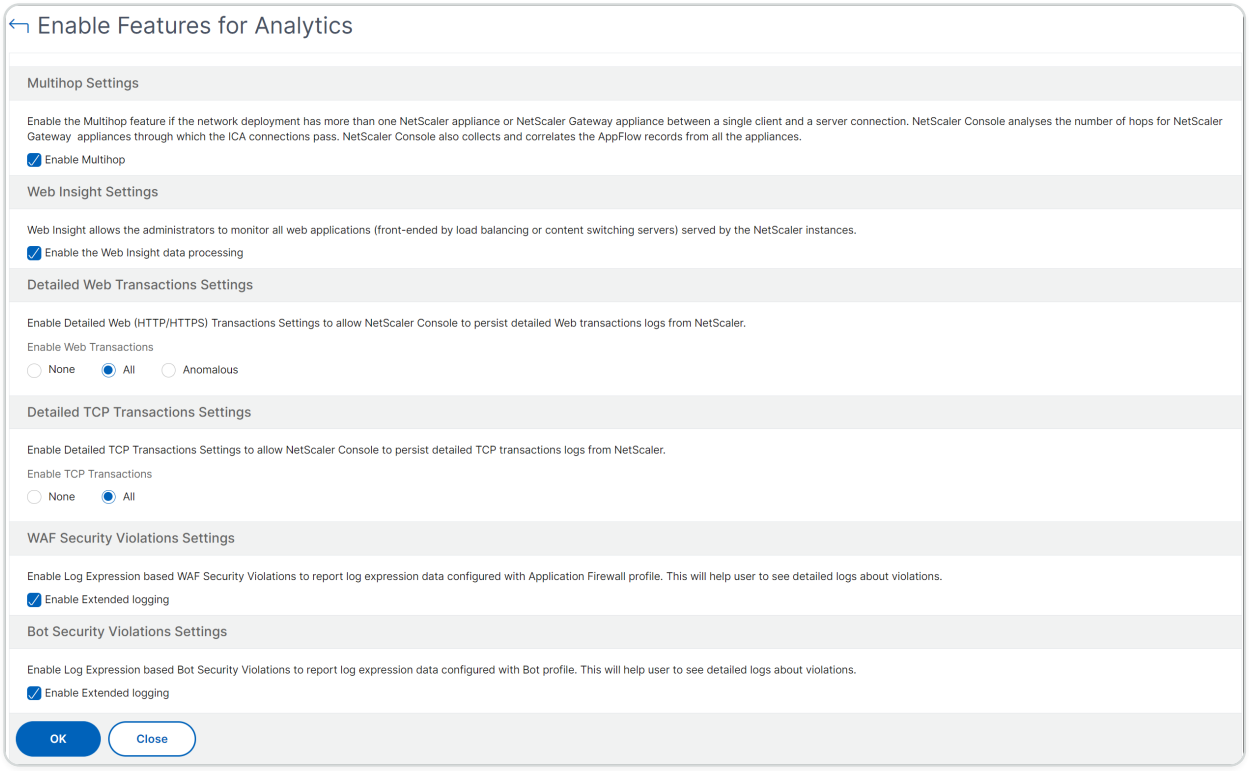
- To configure Detailed Web Transaction Settings.
- If **Metrics Collector** is enabled. For more information, see Configure Intelligent App Analytics.

Enable Web Transaction settings

1. Navigate to **Settings > Analytics Settings**.

   The **Analytics Settings** page is displayed.
2. Click **Enable Features for Analytics**.
3. Under **Detailed Web Transaction Settings**, select **All**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

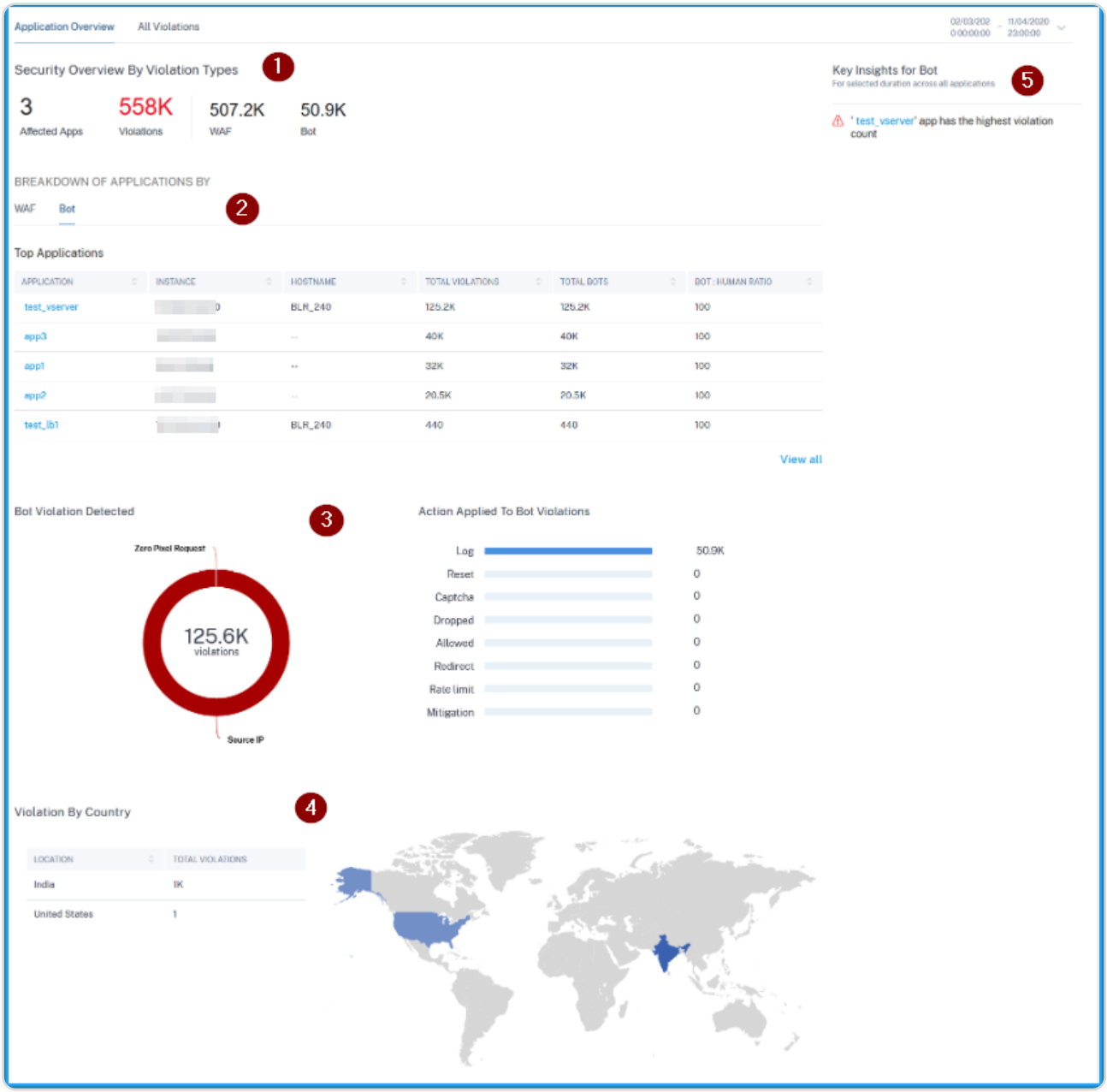


4. Click **Ok**.

Application overview

The **Application Overview** page displays applications with full visibility into the threat details associated in both security insight and bot insight. You can also view information such as total violations, total WAF and Bot violations, violation by country, and so on.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1 – Displays the total affected applications, total violations, total WAF violations, and total Bot violations for the selected duration.

2 – Displays the WAF and Bot violation details. Click the **WAF** and **Bot** tab to view the top 5 custom or discrete applications based on the total violations occurred. Click **View All** to view all application details.

3 – Displays the top violations based on the occurrences and the actions applied.

4 – Displays a geo map view that provides visibility from which locations the violations have occurred.

5 – Provides information based on the violations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Violation categories

WAF	BOT
Cookie Hijack	Scraper
Infer Content Type XML	Screenshot Creator
Buffer Overflow	Search Engine
Content Type	Service Agent
Cookie Consistency	Site Monitor
CSRF Form Tagging	Speed Tester
Deny URL	Uncategorized
Form Field Consistency	Virus Scanner
Field Formats	Vulnerability Scanner
Maximum Uploads	DeviceFP Wait Exceeded
Referrer Header	Invalid DeviceFP
Safe Commerce	Invalid Captcha Response
Safe Object	Tool
HTML SQL Inject	Captcha Attempts Exceeded
Start URL	Valid Captcha Response
Cross-site scripting	Captcha Client Muted
XML DoS	Captcha Wait Time Exceeded
XML Format	Request Size Limit Exceeded
XML WSI	Rate Limit Exceeded
XML SSL	Block list (IP, subnet, policy expression)
XML Attachment	Allow list (IP, subnet, policy expression)

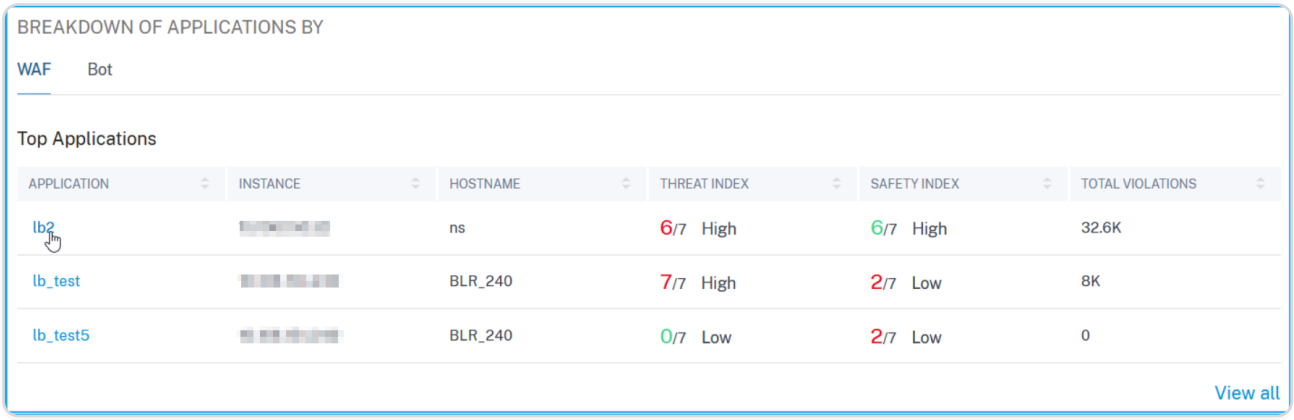
© 1997–2026 Citrix Systems, Inc. All rights reserved.

WAF	BOT
XML SOAP Fault	Zero Pixel Request
XML Validation	Source IP
Others	Host
IP Reputation	Crawler
HTTP DOS	Feed Fetcher
TCP Small Window	Link Checker
Signature Violation	Marketing
File Upload Type	Geo Location
JSON cross-site scripting	URL
JSON SQL	
JSON DOS	
Command Injection	
Block Keyword	
JSON Block Keyword	
Command Injection Grammar	

View WAF violation details

Click an application from the **Top Applications** or from the **View All** option to view the WAF details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

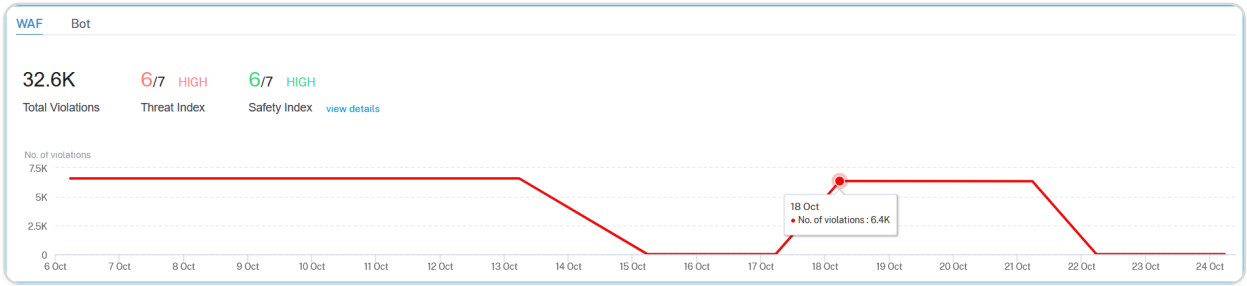


NOTE:

If you select a custom app, you can view the consolidated applications details in the **Security Overview** page. From the list, select an application to view details for the selected application.

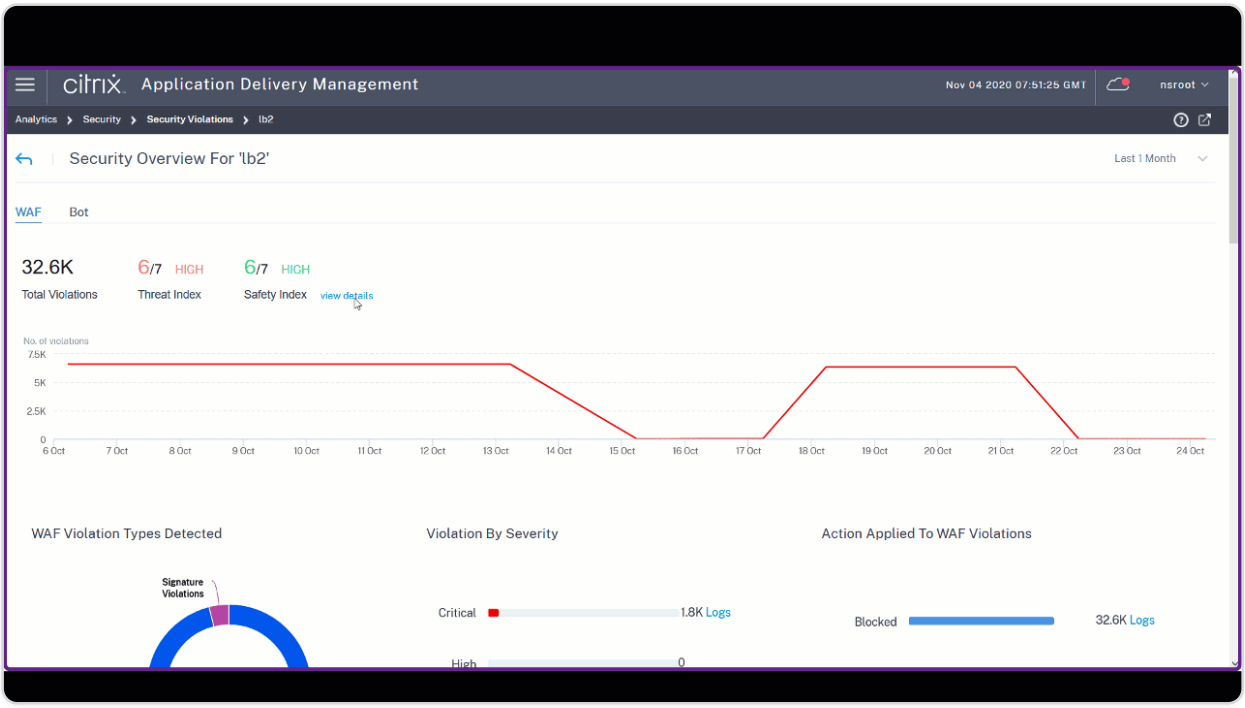
The **Security Overview** page for the selected application is displayed. Under **WAF**, you can view:

- A graph view that indicates the total violations, threat index score, safety index score for the application.

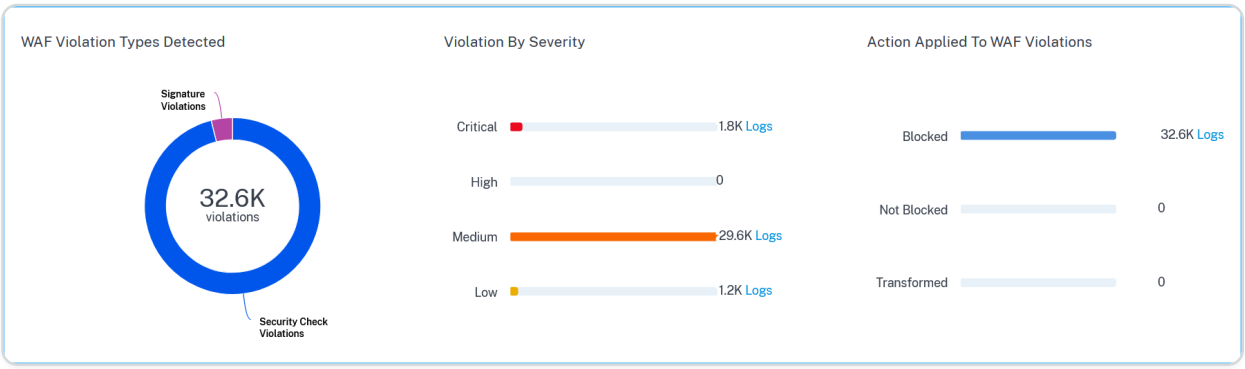


  Click **View Details** to see the Application Firewall and NetScaler System Security configuration details.

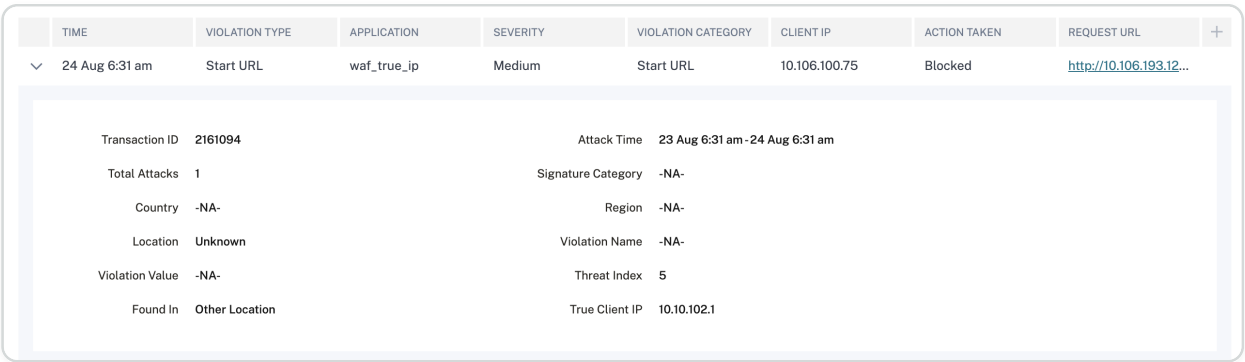
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- The violations based on types, severity, and actions applied.



Click **Logs** to view details based on the severity or action taken. You can also view the client IP address.



You can also use the search text box where you can view details as per your requirement. When you click the search box, the search box gives you the list of search suggestions.

- The violations affected on the application. Under **Violation Details**, you can view the affected violation details.

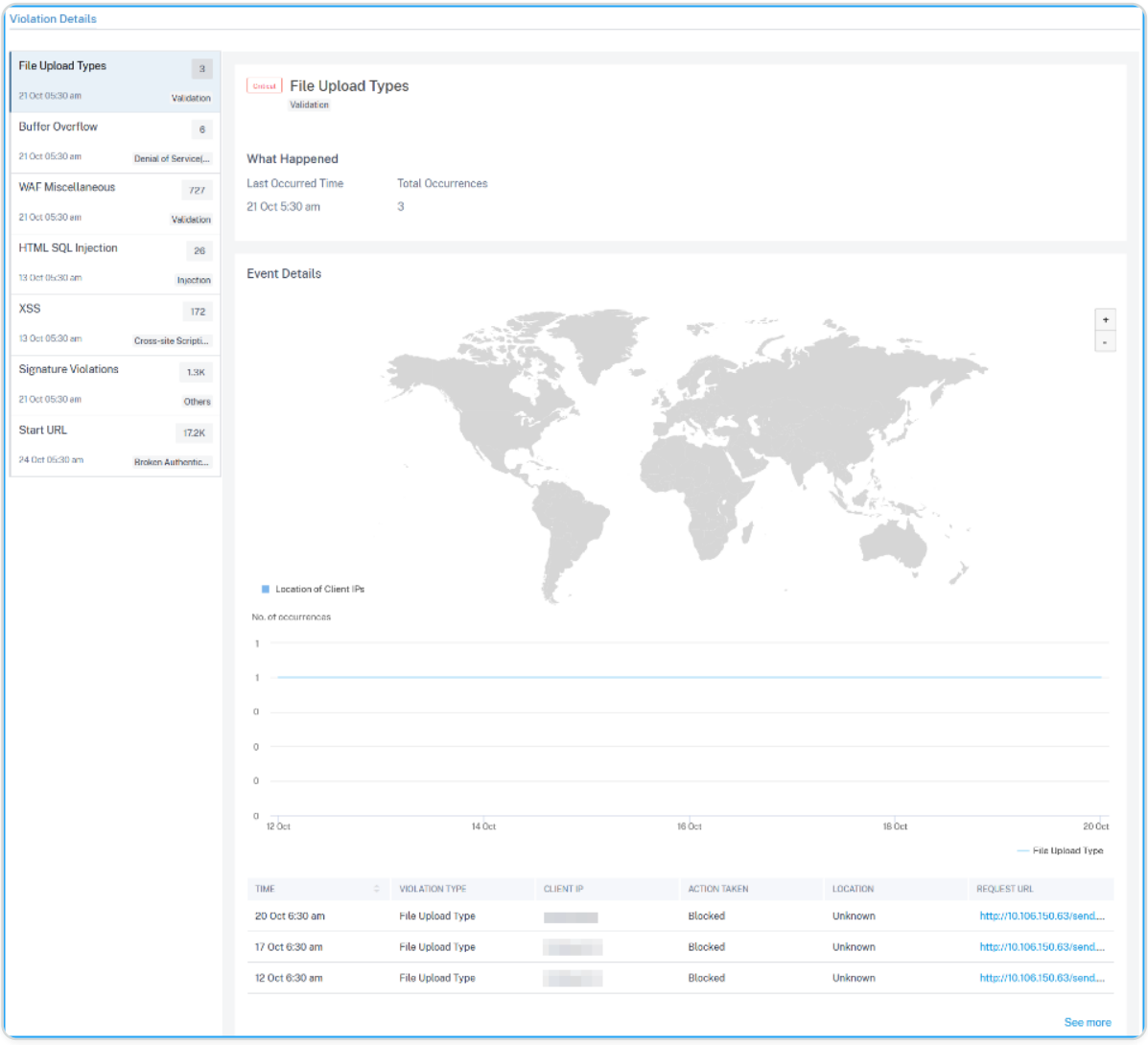
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

For a custom app, violations that are applicable for all applications are displayed. You can click an application from the list to view the violations affected for the selected application.

Click each violation to view details such as:

- **What Happened** – Indicates the total occurrences and the last occurred date and time.
- **Event Details** – Displays a geo map that indicates the client IP and other violation details such as violation type, client IP, location, and so on.



View bot violation details

From the **Bot** tab, click an application from the **Top Applications** or from the **View All** option to view the bot details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

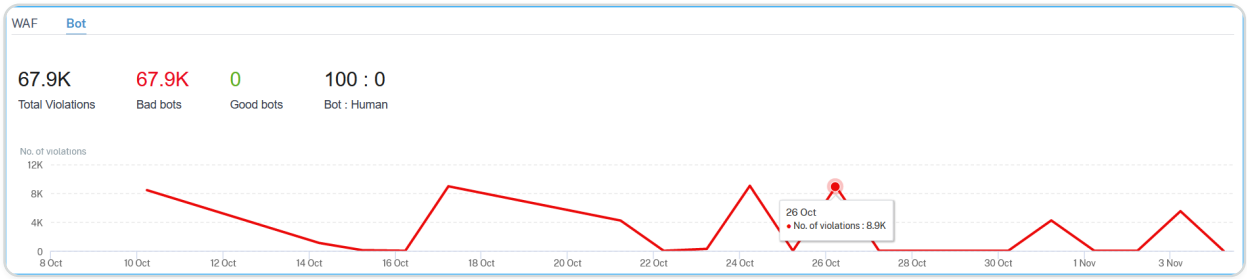


NOTE

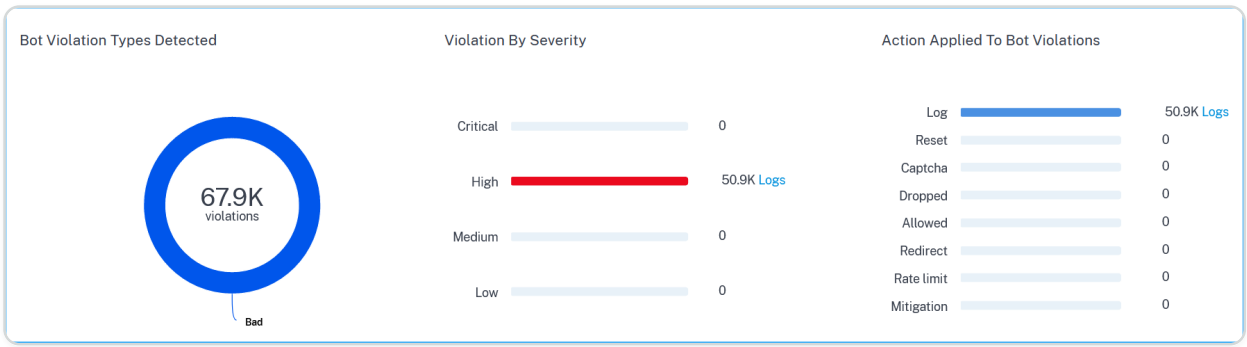
If you select a custom app, you can view the consolidated applications details in the **Security Overview** page. From the list, select an application to view details for the selected application.

The **Security Overview** page for the selected application is displayed. Under **Bot**, you can view:

- A graph indicating total bots, total bad bots, total good bots, and total ratio between human users and bots accessing the application.

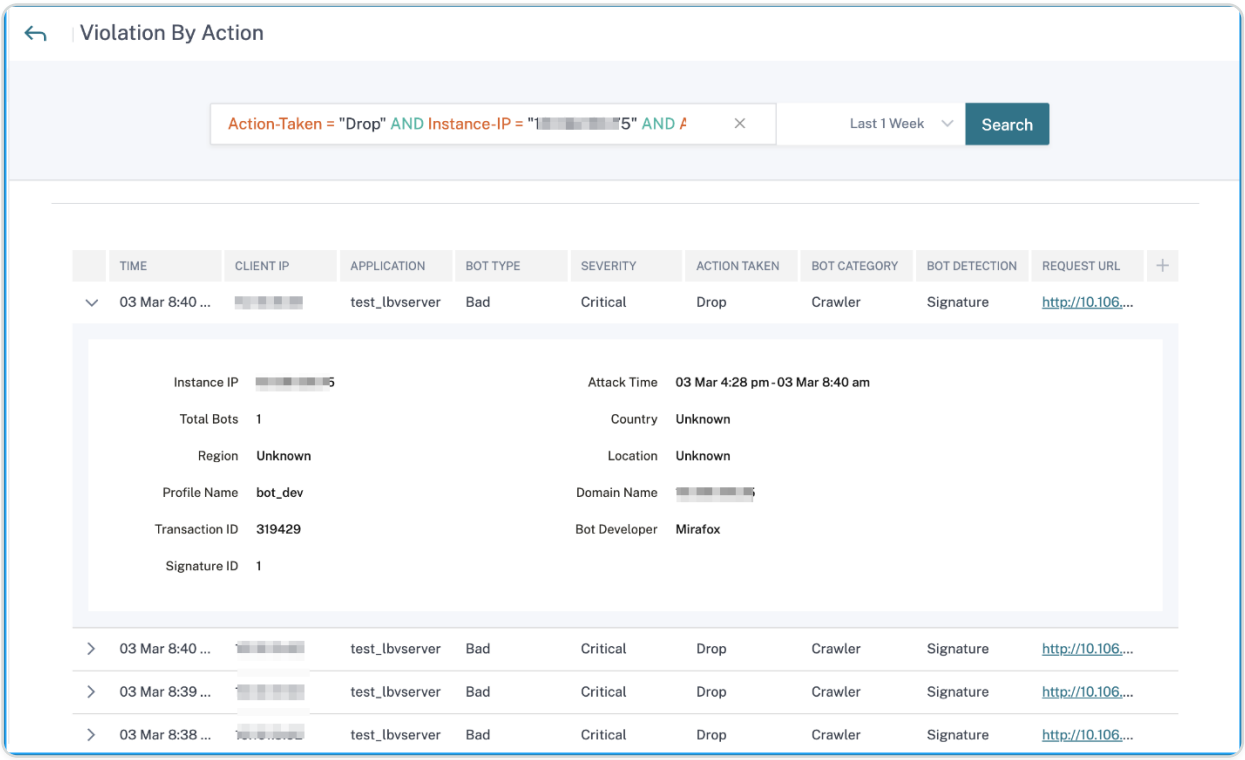


- The violations based on the bot types, severity, and actions applied.



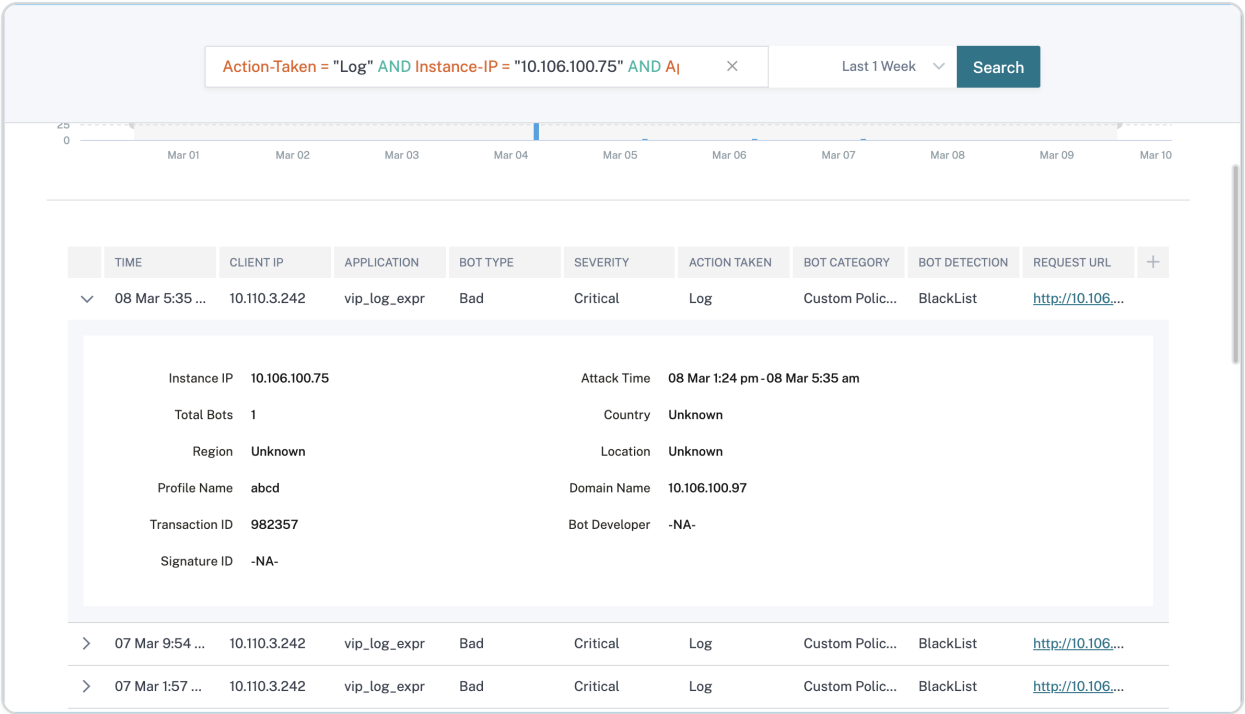
Click **Logs** to view details based on severity or actions taken. If a detected bot is a Signature type bot, you can view more details such as Bot developer and Signature ID. The Signature ID enables you to identify if the detected bot is a good bot or a bad bot.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE:

If a detected bot is any other bot type apart from Signature bot, the Signature ID and Bot developer are displayed as N/A.



You can also use the search text box where you can view bot details as per your requirement. When you click the search box, the search box gives you the list of search suggestions.

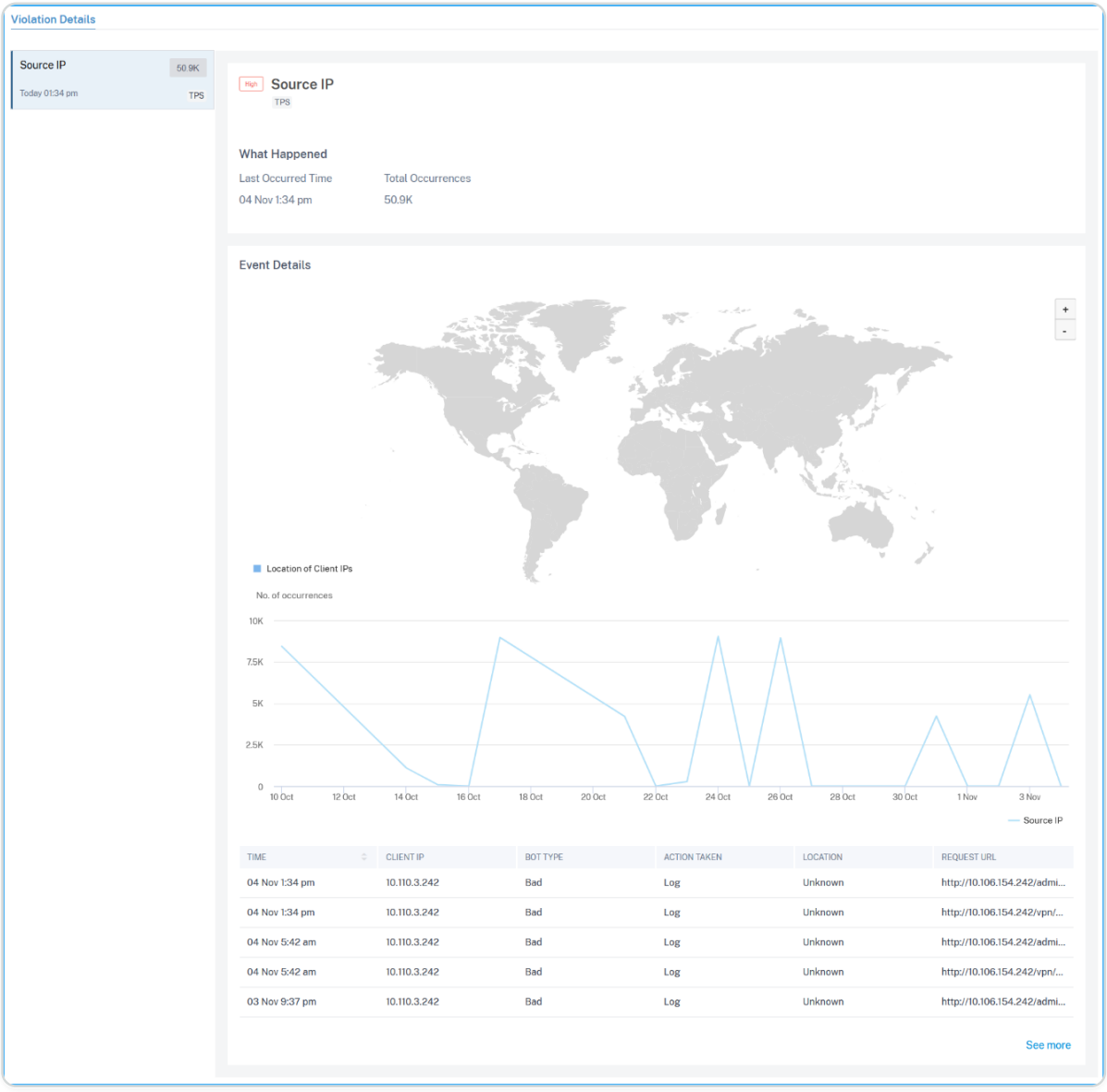
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The violations affected on the application. Under **Violation Details**, you can view the affected violation details.

> **NOTE:**
>
> For a custom app, violations that are applicable for all applications are displayed. You can click an application from the list to view the violations affected for the selected application.

Click each violation to view details such as:

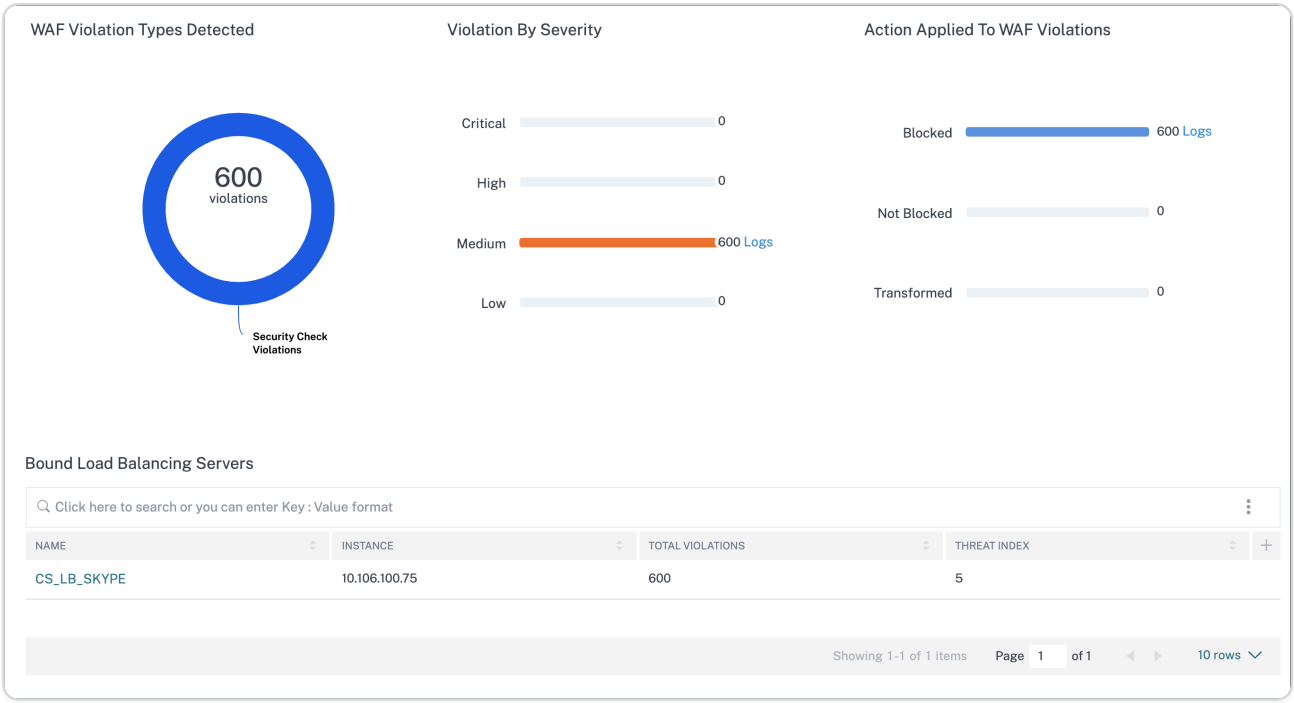
- **What Happened** – Indicates the total occurrences and the last occurred date and time.
- **Event Details** – Displays a geo map that indicates the client IP and other violation details such as violation type, client IP, location, and so on.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Under **WAF** and **Bot**, you can view analytics for content switching virtual server that is bound with load balancing virtual servers. Click the content switching virtual server and under **Bound Load Balancing Server**, you can view the list of load balancing servers bound to the content switching virtual server.



View events history

You can view the signature updates in **Events**, when:

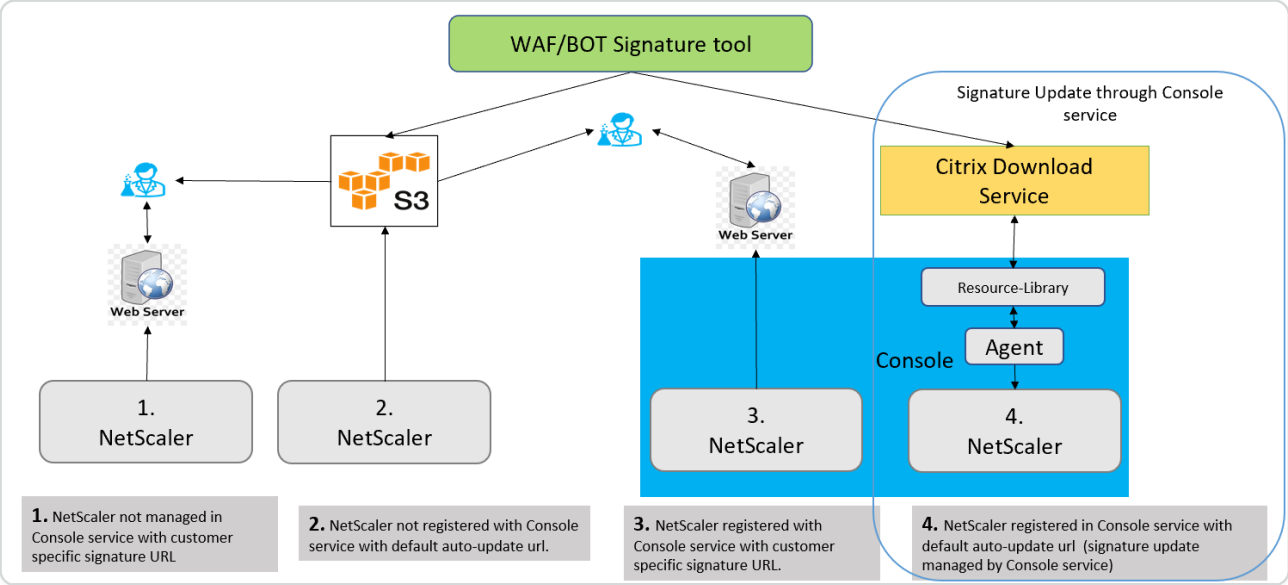
- New signatures are added in NetScaler instances.
- Existing signatures are updated in NetScaler instances.

Signature auto update

NetScaler Console automatically checks for new signature updates and applies to the managed NetScaler instances.

The following diagram shows how the signatures are retrieved from AWS cloud, updated on NetScaler and view signature update summary on NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



All Violations

The **All Violations** page displays the application security violation details based on the **Network**, **WAF**, and **Bot** categories. To view the security violations in NetScaler Console, ensure that you enabled all the required settings. For more information, see the procedure available at Setting up.

Violation categories

NetScaler Console enables you to view the following violations. Under **Violation Details**, you can click each violation tab to view the violation details.

NETWORK	WAF	BOT
HTTP Slow Loris	Infer Content Type XML	Scraper
DNS Slow Loris	Buffer Overflow	Screenshot Creator
HTTP Slow Post	Content Type	Search Engine
NXDomain Flood Attack	Cookie Consistency	Service Agent
HTTP desync attack	CSRF Form Tagging	Site Monitor
Bleichenbacher Attack	Deny URL	Speed Tester
Segment smack Attack	Form Field Consistency	Tool
SYN Flood Attack	Field Formats	Uncategorized
Small Window Attack	Referrer Header	Virus Scanner

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETWORK	WAF	BOT
	Cross-site scripting	Vulnerability Scanner
	XML DoS	DeviceFP Wait Exceeded
	XML Format	Invalid DeviceFP
	XML WSI	Invalid Captcha Response
	XML SSL	Captcha Attempts Exceeded
	XML Attachment	Valid Captcha Response
	XML SOAP Fault	Captcha Client Muted
	XML Validation	Captcha Wait Time Exceeded
	Others	Request Size Limit Exceeded
	IP Reputation	Rate Limit Exceeded
	HTTP DOS	Block list (IP, subnet, policy expression)
	TCP Small Window	Allow list (IP, subnet, policy expression)
	Signature Violation	Zero Pixel Request
	File Upload Type	Source IP
	JSON cross-site scripting	Host
	JSON SQL	Geo Location
	JSON DOS	URL
	Command Injection	Crawler
	Cookie Hijack	Feed Fetcher
	Block Keyword	Link Checker

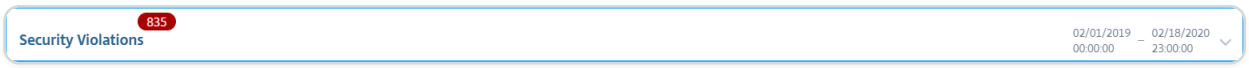
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETWORK	WAF	BOT
	JSON Block Keyword	Marketing
	Safe Commerce	
	Safe Object	
	HTML SQL Inject	
	Start URL	
	Command Injection Grammar	
	JSON SQL Injection Grammar	

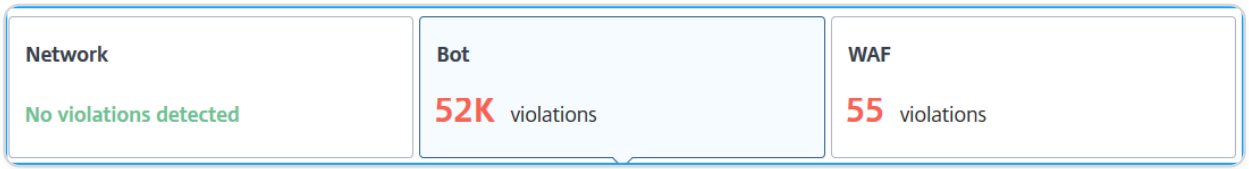
Security violations dashboard

In the security violations dashboard, you can view:

- Total violations occurred across all NetScaler instances and applications. The total violations are displayed based on the selected time duration.

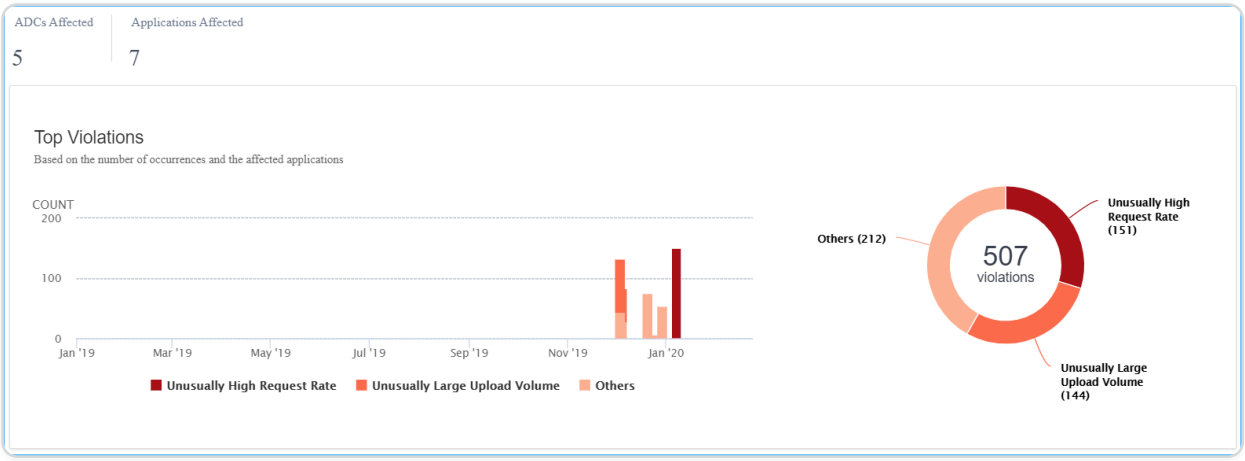


- Total violations under each category.



- Total NetScaler instances affected, total applications affected, and top violations based on the total occurrences and the affected applications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Violation details

For each violation, NetScaler Console monitors the behavior for a specific time duration and detects violations for unusual behaviors. Click each tab to view the violation details. You can view details such as:

- The total occurrences, last occurred, and total applications affected
- Under event details, you can view:
  - The affected application. You can also select the application from the list if two or more applications are affected with violations.
  - The graph indicating violations.
  - **Recommended Actions** that suggest you troubleshoot the issue.
  - Other violation details such as violence occurrence time and detection message.

WAF learning

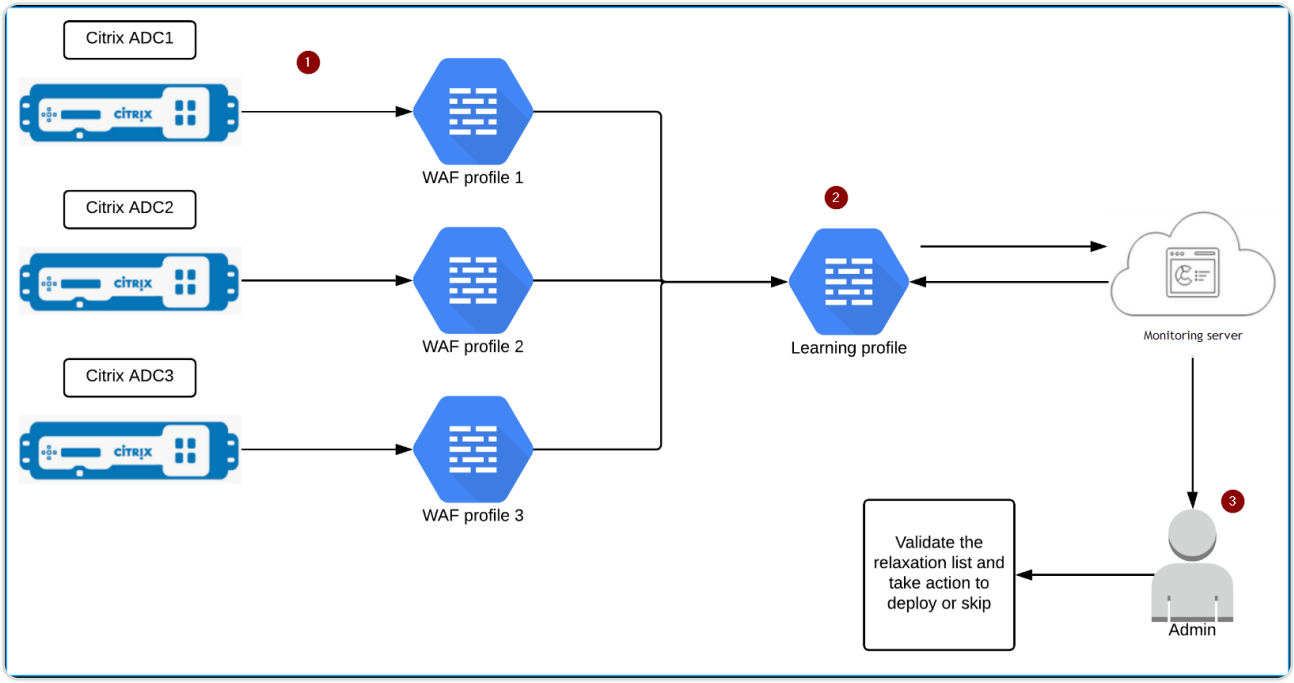
NetScaler Web App Firewall (WAF) protects your web applications from malicious attacks such as SQL injection and cross-site scripting. To prevent data breaches and provide the right security protection, you must monitor your traffic for threats and real-time actionable data on attacks. Sometimes, the attacks reported might be false-positive and those need to be provided as an exception.

The Learning engine on NetScaler Console is a repetitive pattern filter that enables WAF to learn the behavior (the normal activities) of your web applications. Based on monitoring, the engine generates a list of suggested rules or exceptions for each security check applied on the HTTP traffic.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

It is much easier to deploy relaxation rules using the Learning engine than manually deploy it as necessary relaxations.

The following image explains the high-level information on how the WAF learning in NetScaler Console works:



1 – NetScaler instances with its WAF profiles

2 – Configure a learning profile in NetScaler Console, add the WAF profiles, and select to auto deploy or manually deploy the relaxation rules

3 – Administrator can validate the relaxation rules in NetScaler Console and decide to deploy or skip

Get started

To deploy the learning feature, you must:

- Enable the centralized learning in the NetScaler instance. Run the following command in the NetScaler instance:

  ```
  set appfw settings -centralizedLearning ON
  ```

- Ensure that the NetScaler instance version is **13.0-76.6** or later.
- Configure a Web App Firewall profile (set of security settings) on your NetScaler appliance. For more information, see Creating Web App Firewall profiles.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After you enable the centralized learning and configure the WAF profile, NetScaler Console generates a list of exceptions (relaxations) for the configured security check. As an administrator, you can review the list of exceptions in NetScaler Console and decide to deploy or skip.

Using the WAF learning feature in NetScaler Console, you can:

- Configure a learning profile with the following security checks:
  - Start URL
  - Cookie Consistency
  - Credit Card

    NOTE

    For the credit card security check, you must configure the `doSecureCreditCardLogging` in NetScaler instance and ensure the setting is **OFF**.
  - Content Type
  - Form Field Consistency
  - Field Formats
  - CSRF Form Tagging
  - HTML Cross-Site Scripting
  - HTML SQL Injection

    NOTE

    For the HTML SQL Injection check, you must configure `set -sqlinjectionTransformSpecialChars ON` and `set -sqlinjectiontype sqlspclcharorkeywords` in NetScaler instance.
  - HTML Command Injection

    NOTE

    Supported only in NetScaler instance 13.0-72.12 or later.
  - JSON SQL

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **NOTE**
>
> Supported only in NetScaler instance 13.1-14.10 or later.

- JSON Command Injection

> **NOTE**
>
> Supported only in NetScaler instance 13.1-14.10 or later.

- JSON XSS

> **NOTE**
>
> Supported only in NetScaler instance 13.1-14.10 or later.

- Check the relaxation rules in NetScaler Console and decide to take necessary action (deploy or skip)
- Get the notifications through email, slack, and ServiceNow
- Use the **Action Summary** page to view relaxation details

To use the WAF learning in NetScaler Console:

1. Configure the learning profile
2. Manage the relaxation rules
3. Use the WAF learning Action Summary page

WAF recommendations

NetScaler Web App Firewall (WAF) Profile and WAF Signatures protect your web applications from malicious attacks. WAF signatures provide specific, configurable rules to simplify the task of protecting your websites against known attacks. A signature represents a pattern that is a component of a known attack on an operating system, web server, website, XML-based web service, or other resource. To protect your application using signatures, you must review the rules, enable, and configure the ones that you want to apply.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Similarly, to prevent data breaches and provide the right security protection in the application, you must create a WAF profile with security checks. When you create a WAF profile in the NetScaler instance, the traffic might:

- Get generated with the mentioned security checks
- Not get generated with the mentioned security checks

The instance might be receiving other attacks, but you might not have enabled that security check in the WAF profiles.

As an administrator, you must understand to enable the right signatures and create the right WAF profiles to protect the web application. Identifying the right signatures and the WAF profiles might be a difficult task at some scenarios.

NetScaler Console WAF recommendation scans the application for vulnerabilities and generates the following recommendations:

- WAF Profile
- WAF Signature

For more information, see WAF profile and WAF Signatures.

WAF recommendation database is updated on a frequent duration to include any new vulnerabilities. You can scan and then select to enable the required recommendations. You can enable all signatures and security checks, but it might result in false positives and affect the NetScaler instance performance. Hence, it is recommended to select only the required security checks and signatures. WAF recommendation engine also automatically detects which signatures and security checks must be enabled for the application.

NOTE

The NetScaler instance must be **13.0 41.28 or later** (for security checks) and **13.0 or later** (for signatures).

Prerequisites

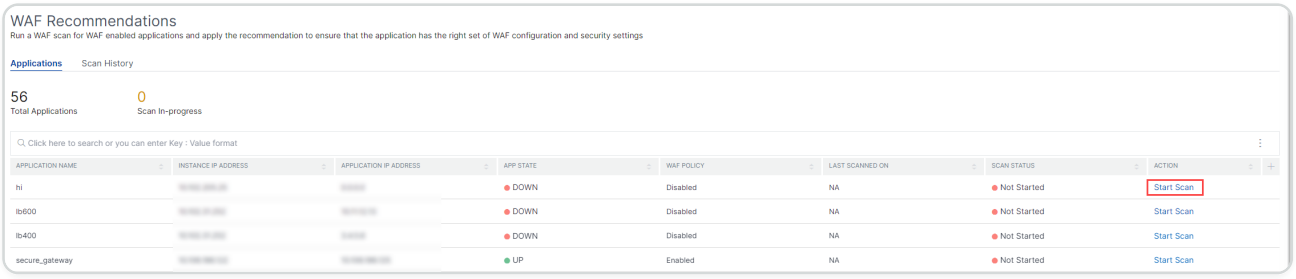
The applications:

- Must have the premium license.
- Must be the load balancing virtual server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure the WAF scan settings

In NetScaler Console, navigate to **Security > WAF Recommendation** and under **Applications**, click **Start Scan** to configure the WAF scan settings for an application.



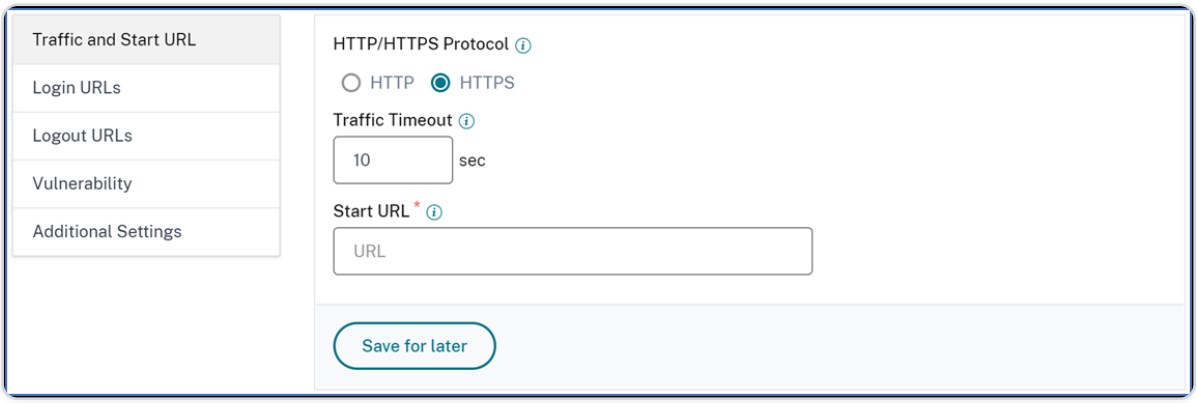
In the WAF Recommendations page:

- **Domain Name** – Specify the publicly accessible/publicly reachable domain name that is associated with the application VIP. For example: `www.example.com`.

  Note

  > Start URL, Login URL and Logout URL must match the specified domain.

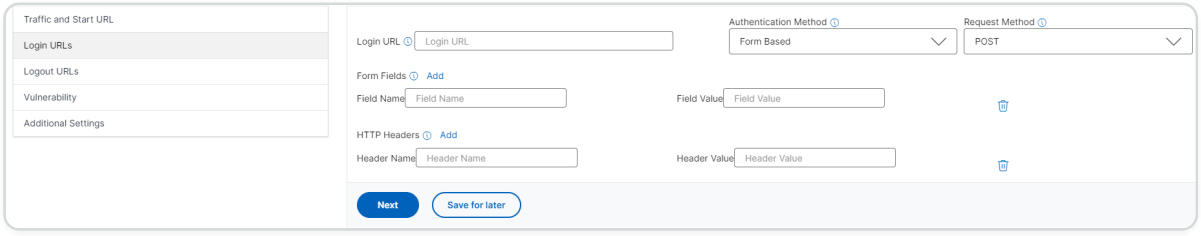
- **Traffic and Start URL** – Provide the URL details of the application (server).
  - **HTTP/HTTPS Protocol** – Select the protocol of the application.
  - **Traffic Timeout** – The wait time (in seconds) for a single request during the scan. The value must be greater than 0.
  - **Start URL** – The home page of the application to initiate the scan. For example, `https://www.example.com/home`. The URL must be a valid IPv4 address. If the IP addresses are private, then you must ensure that the private IP address is accessible from the NetScaler Console management IP.



- **Login URLs** – Specify the login credentials, URLs, if any, to access the application.

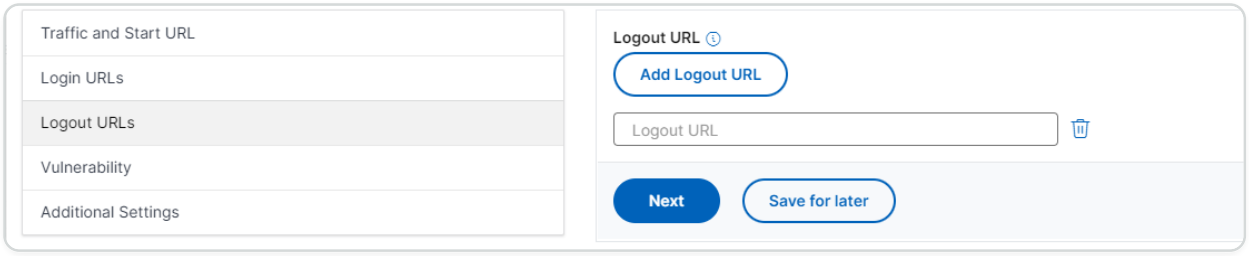
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Login URL** – The URL to which the login data is sent for authentication. In HTML, this URL is commonly known as the action URL.
- **Authentication Method** – Select the supported authentication method (form based or header based) for your application.
  - Form-based authentication requires submitting a form to the login URL with the login credentials. These credentials must be in the form of form fields and their values. The application then shares the session cookie that is used to maintain sessions during the scan.
  - Header-based authentication requires the Authentication header and its value in the headers section. The Authentication header must have a valid value and is used to maintain sessions during the scan. The form-fields should be left empty for Header-based.
- **Request Method** – Select the HTTP method used when submitting form data to the login URL. The allowed request method is POST, GET, and PUT.
- **Form Fields** – Specify the form data to be submitted to the login URL. Form Fields are required only if you select the form-based authentication. You must specify in the key-value pairs, where Field Name is the Key and Field Value is the Value. Ensure that all form fields needed for login to work are added correctly, including passwords. The values are encrypted before storing it in the database. You can click the Add button to add multiple form fields. For example, Field Name – user name and Field Value – admin.
- **HTTP Headers** – The HTTP headers maybe required for the login to succeed. You must specify in the key-value pairs, where Header Name is the Key and Header Value is the Value. You can click the Add button to add multiple HTTP headers. One of the most common required HTTP headers is Content-Type header.

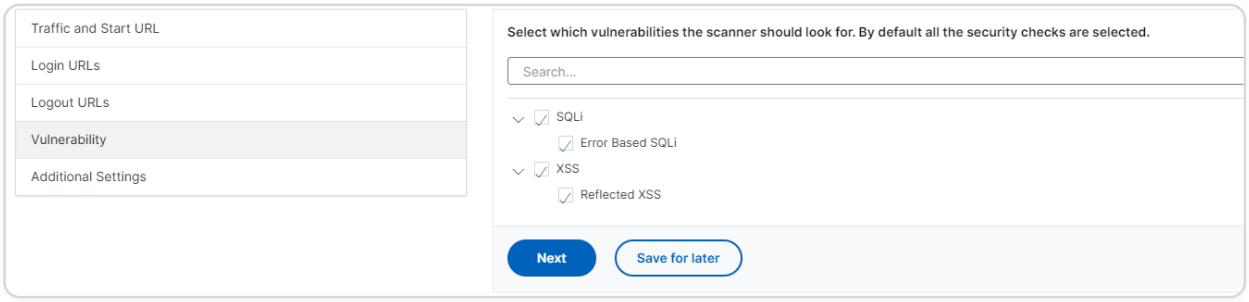


- **Logout URLs** – Specify the URL that terminates the session after accessing. For example: `https://www.example.com/customer/logout`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

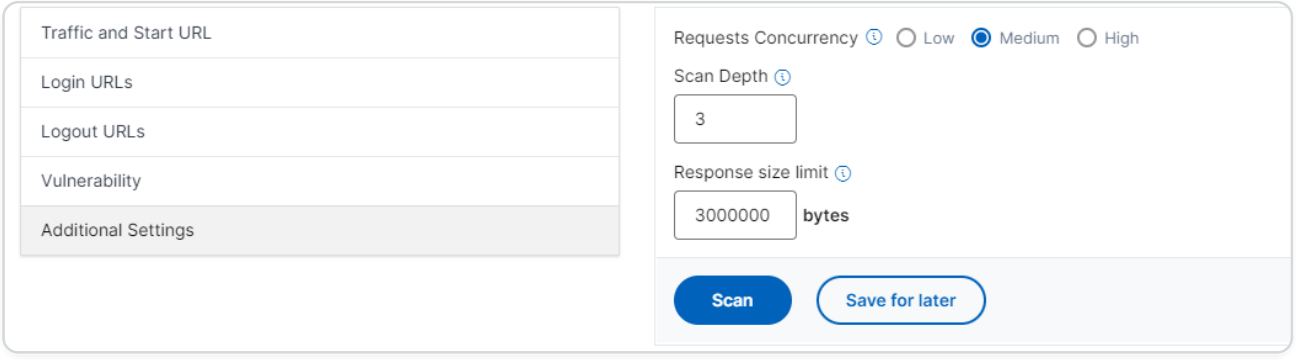


- **Vulnerability** – Select the vulnerabilities for the scanner to detect them. Currently, this is done for SQL Injection and Cross-site scripting violations. By default, all the violations are selected. After selecting the vulnerabilities, it simulates these attacks on the application to report the potential vulnerability. It is recommended to enable this detection that is not in the production environment. All other vulnerabilities are also reported, without simulating these attacks on the application.



- **Additional Settings**
  - **Requests Concurrency** – The total requests sent to the web application in parallel.
  - **Scan Depth** - The depth of the web application up to which the scan must go on. For example, for a scan depth of value 2, the Start URL and all the links found in this URL are scanned. You must specify a value greater than or equal to 1.
  - **Response size limit** – The maximum limit on the response size. Any responses beyond the mentioned value are not scanned. The recommended limit is 3 MB (300000 bytes).

The WAF scan settings configuration is complete. You can click **Scan** to start the scanning process or you can click **Save for later** to save the configurations and scan later.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

WAF scan recommendation process

When you start the scan, the WAF recommendation engine:

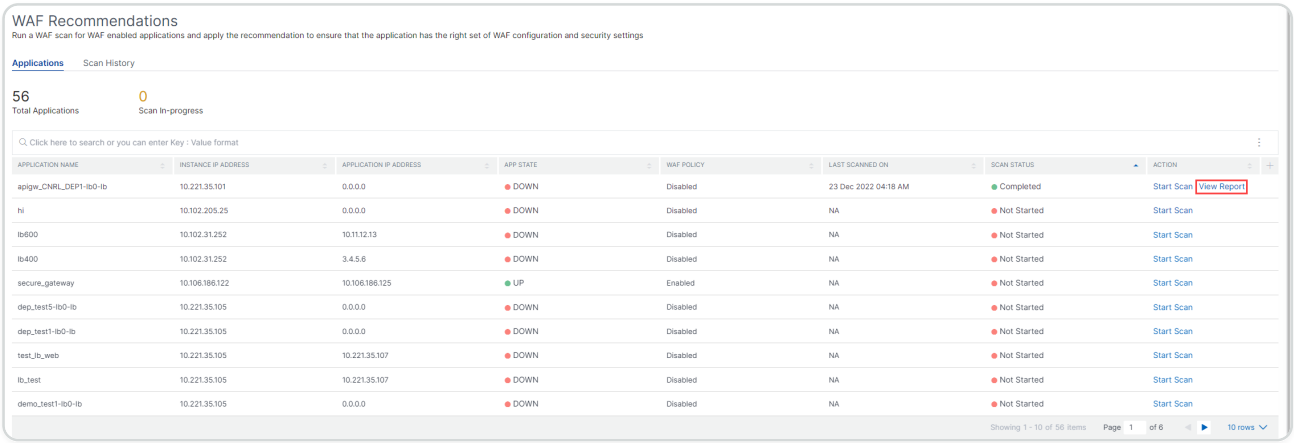
- Scans the provided web application through the provided URL.
- Inspects the web application to discover the technologies used by the web application.
- Simulates security attacks on the web application to detect potential vulnerabilities.
- Recommends signatures based on the web technologies detected.
- Recommends security checks based on vulnerabilities found and the analysis of the traffic.
- Analyzes the web application responses to generate more granular settings.

The following security checks are supported:

- Buffer Overflow
- Field Formats
- Credit Card
- Cookie Consistency
- HTML SQL Injection
- HTML Cross Site Scripting
- Form Field Consistency
- CSRF Form Tagging

View scan report

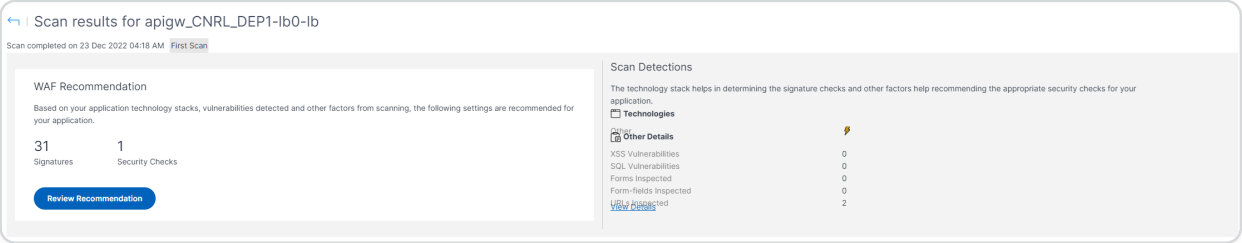
After the scan is complete, click **View Report** to view the results.



The scan result provides:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

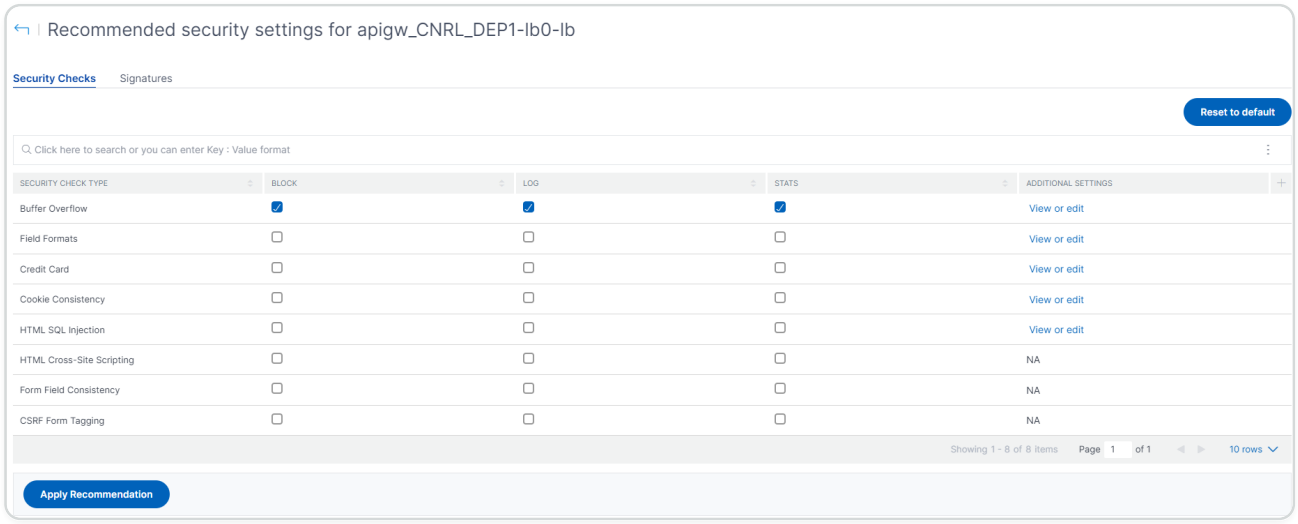
- **WAF Recommendation** – Enables you to view the summary of the total signatures and security checks recommended for the application.
- **Scan Detections** – Enables you to view the collection of information such as technologies and violation details performed on the application. Click **View Details** to see the information about the detections and other details of the scan.



Under **WAF Recommendation**, click **Review Recommendation** to view the details for **Security Checks** and **Signatures**.

The recommended security settings suggest the recommended security checks and signatures for the application. You can edit the recommendations from the list and click **view or edit** to view details or edit changes according to the requirement. The Reset to default resets all changes made and brings back to the original recommendations.

After reviewing details, click **Apply Recommendation**. The recommendations are configured using the StyleBooks. You must ensure to apply recommendation in the **Security Checks** and **Signature** tabs separately.



It is recommended to apply the signatures first and then the security checks. This binds the signatures to the profile automatically.

When you apply signatures successfully:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The configuration is applied on the NetScaler instance through the `appfw-import-object` StyleBook.
- The signatures file with recommendations configured is imported in the NetScaler instance.

NOTE

Signatures are supported in NetScaler 13.0 or later version.

Before you proceed to apply the **Security Check** recommendations, navigate to **Applications > Configuration > Config Packs** and ensure that the signatures configpack is successfully created.

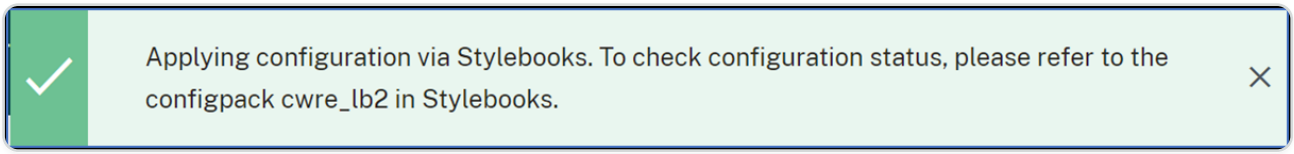
When you apply security checks successfully:

- The configuration is applied on the NetScaler instance through StyleBooks, depending upon the NetScaler version. For NetScaler 13.0, `waf-default-130` StyleBook is used and for NetScaler 13.1, `waf-default-131` stylebook is used.
- The `Appfw` profile is created on your NetScaler and bound to the application using the `policylabel`.
- The signatures are bound to the appfw profile, if the recommended signatures are already applied.

NOTE

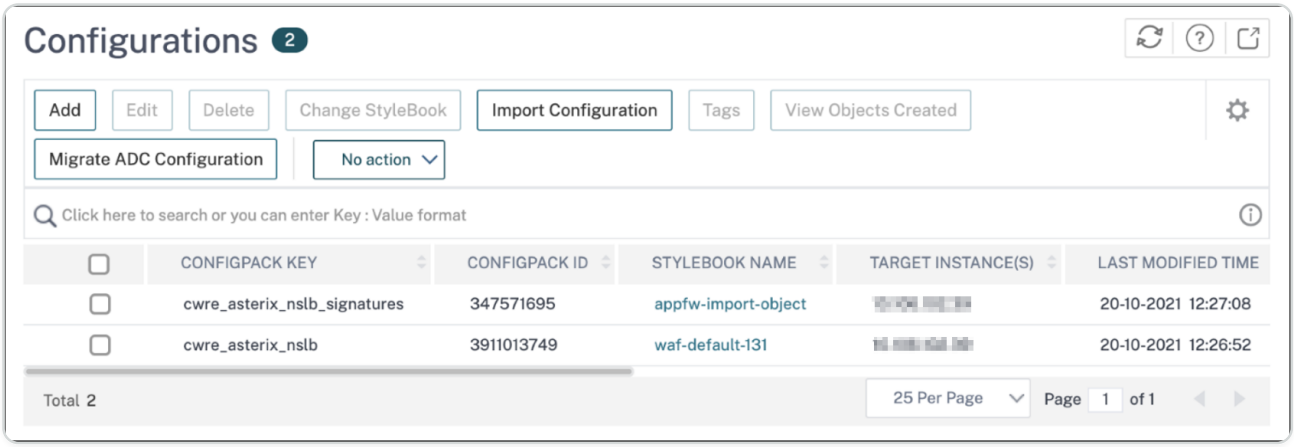
Security checks are supported in NetScaler 13.0 41.28 or later version.

After you apply the recommendation (security checks and signatures), you can view the following confirmation message:



You can verify the WAF profiles and signatures are applied through the default StyleBooks by navigating to **Applications > Configuration > Config Packs**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gateway

The NetScaler Console gateway features provide visibility into the user access and virtual desktop experience across your NetScaler Gateway deployments. You can troubleshoot logon and access failures, monitor the HDX™ virtual desktop experience, and configure thresholds and alerts.

The following topics help you monitor and manage gateway analytics:

- Gateway Insight
  - Troubleshoot Gateway Insight issues
- HDX Insight
  - Enable HDX Insight data collection
  - Create thresholds and configure alerts for HDX Insight
  - View HDX Insight reports and metrics
  - Troubleshoot HDX Insight issues
- Metrics information for thresholds

Gateway Insight

In a NetScaler Gateway deployment, visibility into a user access detail is essential for troubleshooting access failure issues. As the network administrator, you want to know when a user is not able to log on to NetScaler Gateway, and you want to know the user activity and the reasons for logon failure, but that information is typically not available unless the user sends a request for resolution.

Gateway Insight provides visibility into the failures encountered by all users, regardless of the access mode, at the time of logging on to NetScaler Gateway. You can view a list of all available users, number of active users, number of active sessions, and bytes and licenses used by all users at any given time. You can view the end-point analysis (EPA), authentication, single sign-on (SSO), and application launch failures for a user. You can also view the details of active and terminated sessions for a user.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gateway Insight also provides visibility into the reasons for application launch failure for virtual applications. This enhances your ability to troubleshoot any kind of logon or application launch failure issues. You can view the number of applications launched, number of total and active sessions, the number of total bytes and bandwidth consumed by the applications. You can view details of the users, sessions, bandwidth, and launch errors for an application.

You can view the number of gateways, number of active sessions, total bytes, and bandwidth used by all gateways associated with an NetScaler Gateway appliance at any given time. You can view the EPA, authentication, single sign-on, and application launch failures for a gateway. You can also view the details of all users associated with a gateway and their logon activity.

All log messages are stored in the NetScaler Console database, so you can view error details for any time period. You can also view a summary of the logon failures and determine at what stage of the logon process a failure has occurred.

Points to Note:

- Gateway Insight is supported on the following deployments:
  - Access Gateway
  - Unified Gateway
- The NetScaler Console release and build must be same or later than that of the NetScaler Gateway appliance.
- One hour of Gateway Insight reports can be viewed for NetScaler instances with Advanced license. A Premium license is required to view Gateway Insight reports beyond one hour.

Limitations:

- NetScaler Gateway does not support Gateway Insight when the authentication method is configured as certificate-based authentication.
- Successful user logons, latency, and application-level details for virtual ICA applications and desktops are visible only on the HDX™ Insight Users dashboard.
- In a double-hop mode, visibility into failures on the NetScaler Gateway appliance in the second DMZ is not available.
- Remote Desktop Protocol (RDP) desktop access issues are not reported.
- The Gateway Insight records for the SAML authentication are not reported.
- Gateway Insight is supported for the following authentication types. If other authentication type is used other than these, you might see some discrepancies in Gateway Insight.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Local
- LDAP
- RADIUS
- TACACS
- SAML
- Native OTP
- OAuth

Enable Gateway Insight

To enable Gateway Insight for your NetScaler Gateway appliance, you must first add the NetScaler Gateway appliance to NetScaler Console. You must then enable AppFlow for the virtual server representing the VPN application. For information about adding device to NetScaler Console, see Adding Instances.

NOTE

To view end-point analysis (EPA) failures in NetScaler Console, you must enable AppFlow authentication, authorization, and access control user name logging on the NetScaler Gateway appliance.

Enable AppFlow for a virtual server in NetScaler Console

1. Navigate to **Settings > Licensing & Analytics Configuration**.
2. Under **Virtual Server Analytics Summary**, click **Configure Analytics**.
3. In the **All Virtual Servers** page, select the NetScaler Gateway virtual server, and click **Enable Security & Analytics**.
4. Select **Gateway Insight**.
5. Click **Save**.

Enable AppFlow user name logging on an NetScaler Gateway appliance by using the GUI

1. Navigate to **Configuration > System > AppFlow® > Settings**, and then click **Change AppFlow Settings**.
2. In the **Configure AppFlow Settings** screen, select **AAA Username**, and then click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View Gateway Insight reports

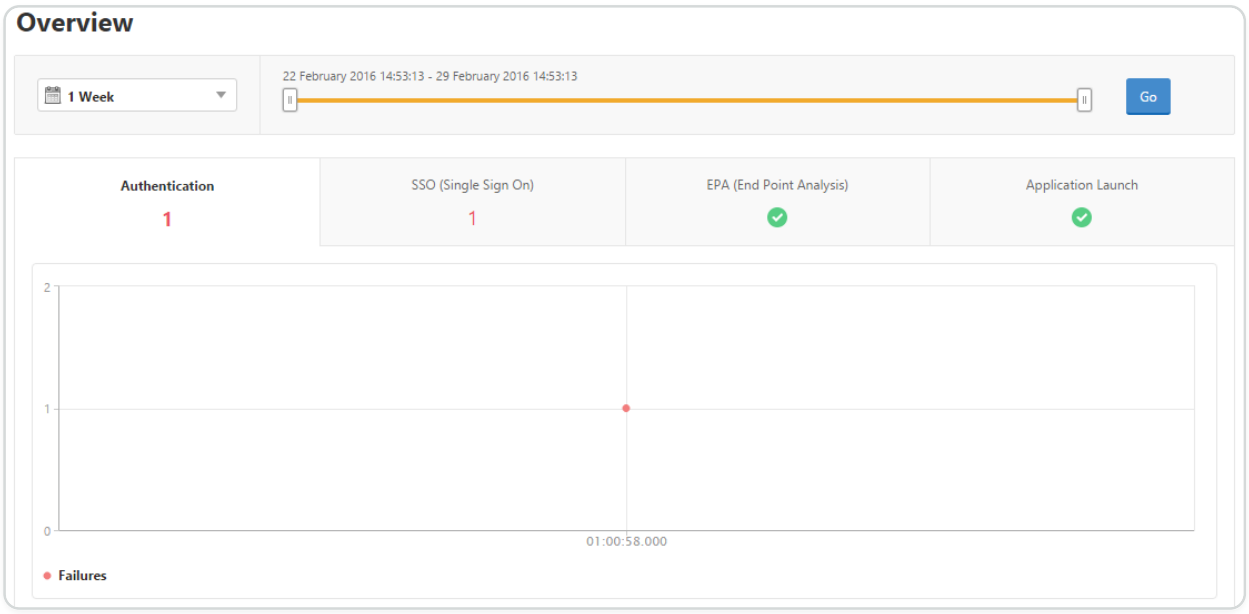
In NetScaler Console, you can view reports for all users, applications, and gateways associated with the NetScaler Gateway appliances, and you can view details for a particular user, application, or gateway. In the **Overview** section, you can view the EPA, SSO, Authentication, and Application Launch failures. You can also view a summary of the different session modes used by users to log on, the types of clients, and the number of users logged on every hour.

NOTE:

When you create a group, you can assign roles to the group, provide application-level access to the group, and assign users to the group. NetScaler Console analytics now supports virtual IP address-based authorization. Your users can now see reports for all Insights for only the applications (virtual servers) that they are authorized to. For more information on groups and assigning users to the group, see Configure Groups on NetScaler Console.

View EPA, SSO, authentication, authorization, and application launch failures

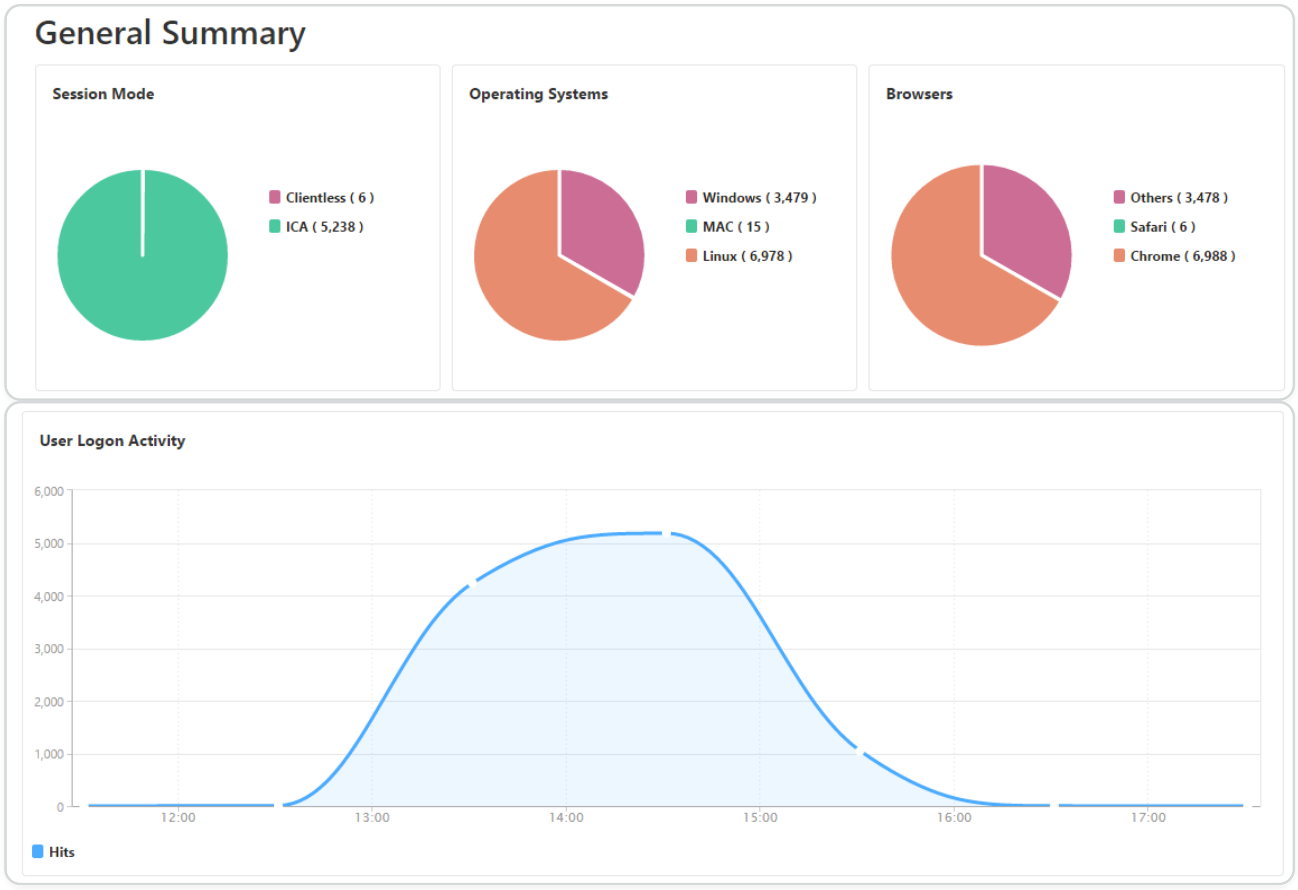
1. In NetScaler Console, navigate to **Gateway > Gateway Insight**.
2. Select the time period for which you want to view the user details. You can use the time slider to further customize the selected period. Click **Go**.
3. Click the EPA (End Point Analysis), Authentication, Authorization, SSO (Single Sign On), or Application Launch tabs to display the failure details.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

View summary of session modes, clients, and the number of users

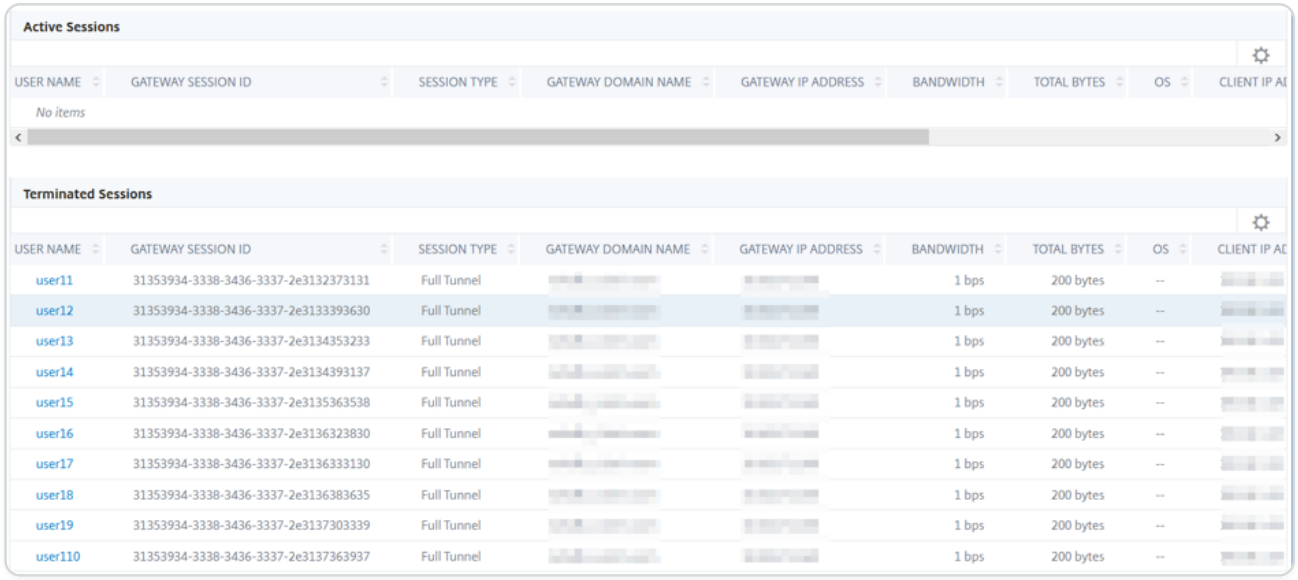
In NetScaler Console, navigate to **Gateway > Gateway Insight**, scroll down to view the reports.



Users

You can view a complete report for the users associated with the NetScaler Gateway appliances. You can view the EPA, authentication, SSO, application launch failures, and so on for a user.

You can also visualize a consolidated view of all users active and terminated sessions.



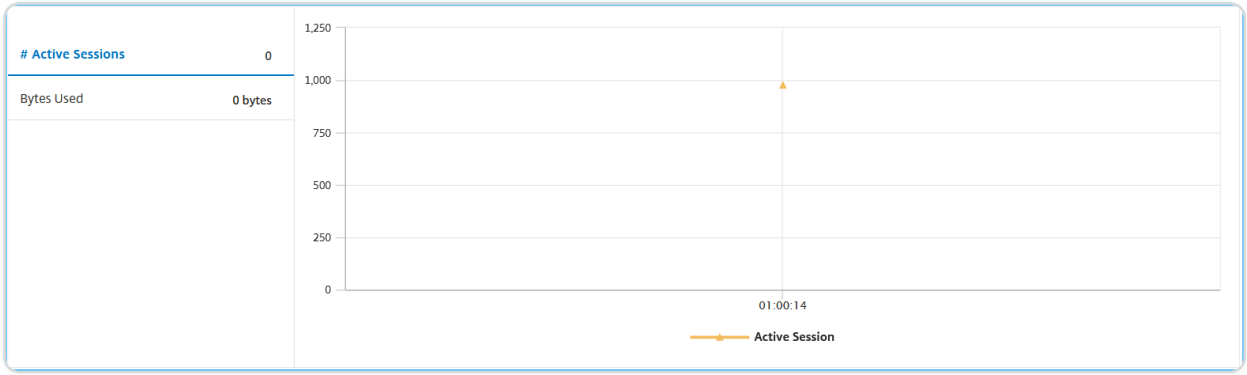
© 1997–2026 Citrix Systems, Inc. All rights reserved.

As an administrator, this view enables you to:

- View all users details in a single-pane visualization
- Eliminate the complexity in selecting each user and seeing the active and terminated sessions

View user details

1. In NetScaler Console, navigate to **Gateway > Gateway Insight > Users**.
2. Select the time period for which you want to view the user details. You can use the time slider to further customize the selected period. Click **Go**.
3. You can view the number of active users, number of active sessions, and bytes by all users during the time period.



Scroll down to view a list of available users and active users.

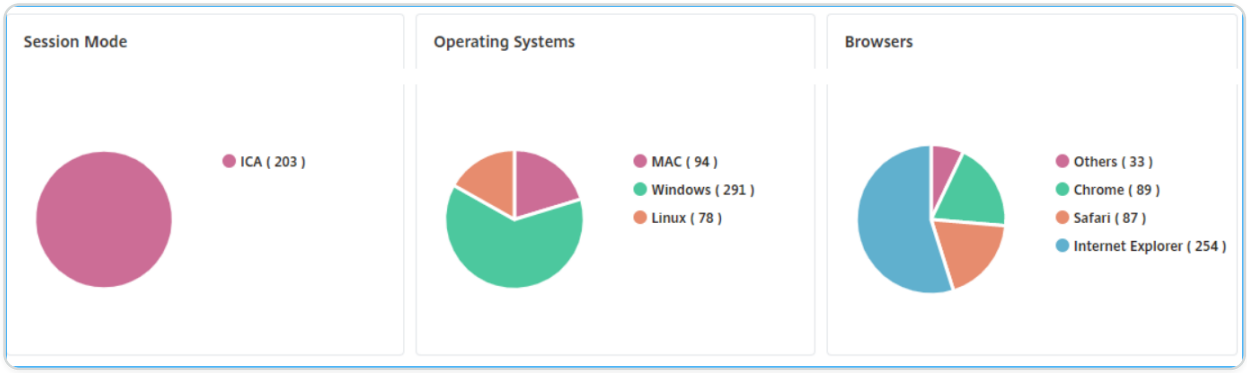


User Name	Total Bytes	# Sessions Used
user1	191.94 KB	11
user10	0	4
user100	2.81 KB	4
user1000	42.66 KB	5
user1001	2.11 KB	4
user1002	4.22 KB	4
user1003	4.22 KB	4

On the **Users** or **Active Users** tab, click a user to view the following user details:

- **User details** - You can view insights for each user associated with the NetScaler Gateway appliances. Navigate to **Gateway** > **Gateway Insight** > **Users** and click a user to view insights for the selected user such as Session Mode, Operating System, and Browsers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

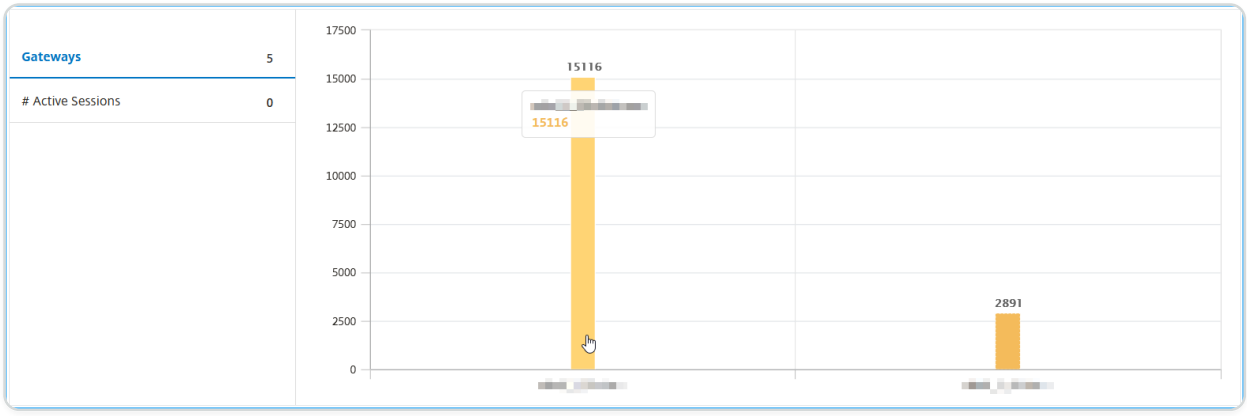


- **Users and applications for the selected gateway** - Navigate to **Gateway** > **Gateway Insight** > **Gateway** and click a gateway domain name to view the top 10 applications and top 10 users that are associated with the selected gateway.

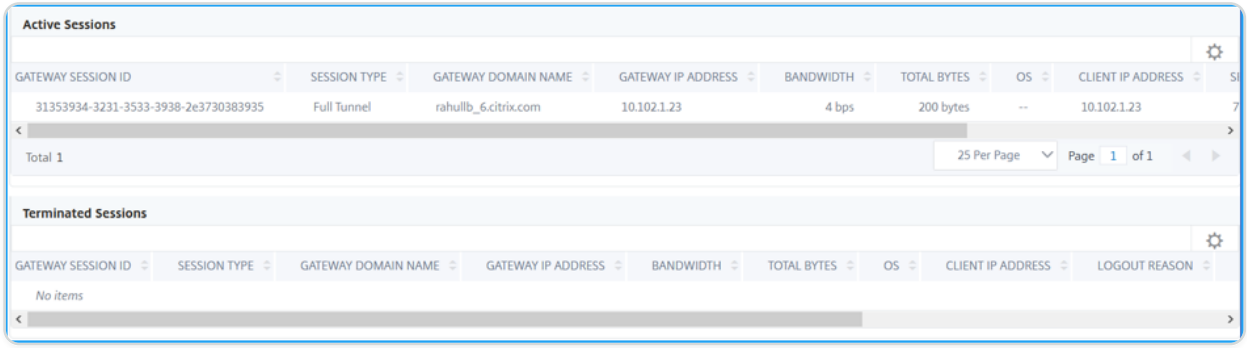


- **View more option for applications and users** – For more than 10 applications and users, you can click the more icon in Applications and Users to view all users and applications details that are associated with the selected gateway.
- **View details by clicking the bar graph** – When you click a bar graph, you can view the relevant details. For example, navigate to **Gateway > Gateway Insight > Gateway** and click the gateway bar graph to view the gateway details.

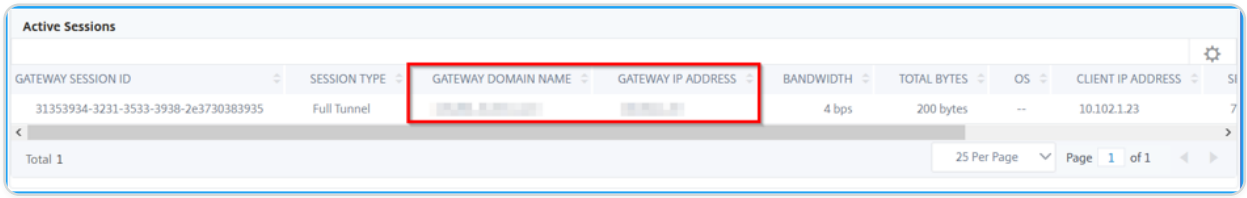
© 1997–2026 Citrix Systems, Inc. All rights reserved.



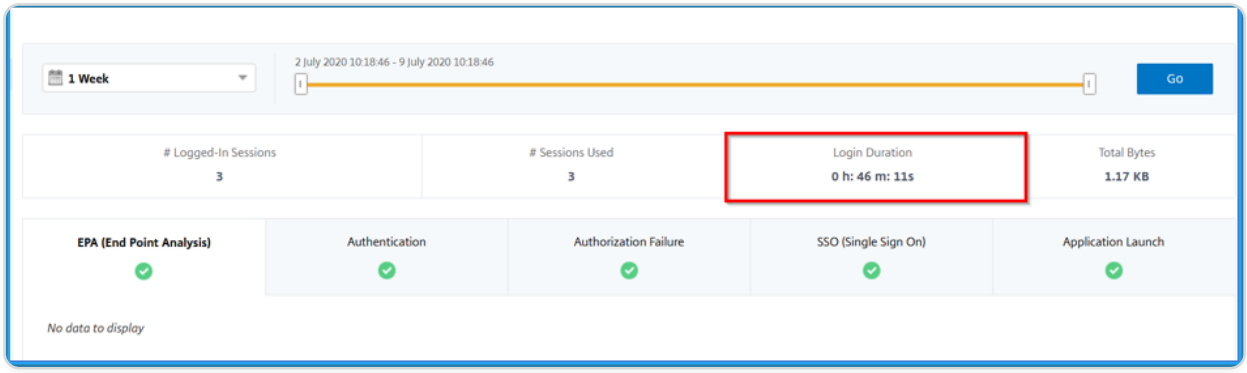
- The user **Active Sessions** and **Terminated Sessions**.



- The gateway domain name and gateway IP address in **Active Sessions**.



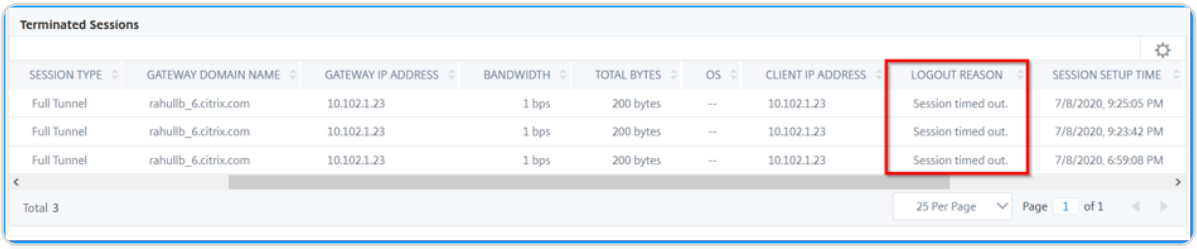
- The user login duration.



- The reason for the user logout session. The logout reasons can be:
  - Session timed out
  - Logged out because of internal error
  - Logged out because of inactive session timed out
  - User has logged out

© 1997–2026 Citrix Systems, Inc. All rights reserved.

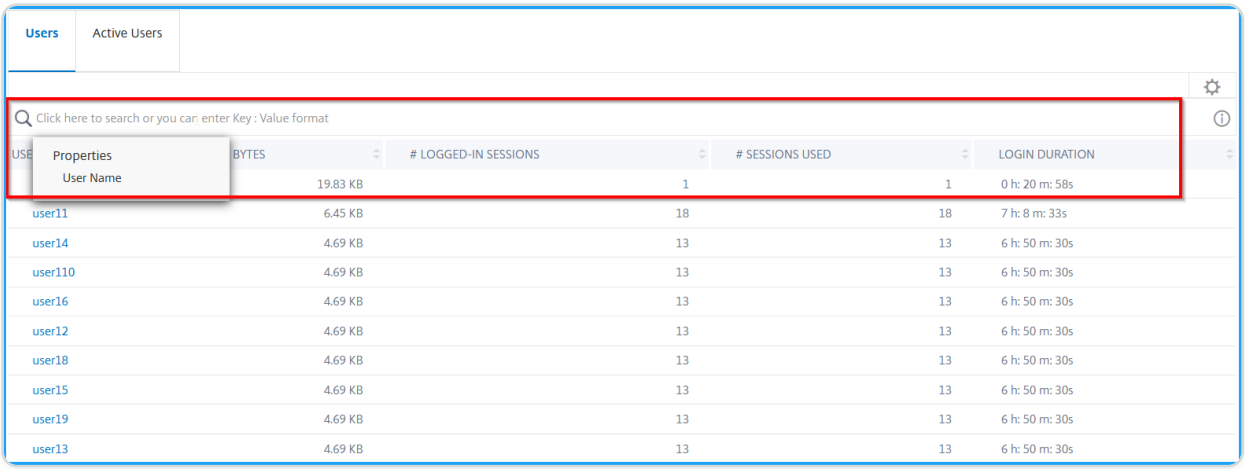
- Administrator has stopped the session



Search bar and Geo map view

You can view:

- A search bar that enables you to filter results based on the user name. Navigate to **Gateway > Gateway Insight > Users** to view the search bar for **Users** and **Active Users**. Place the mouse pointer on the search bar, select **User Name**, and type a user name to filter results.



- A geo map that displays the users information based on the users geographical location. As an administrator, this geo map enables you to view the summary of total users, total apps, and total sessions for a specific location.

  a. Navigate to **Gateway > Gateway Insight** to view the geo map

  b. Click a country. For example, United States

     The geo map displays the details such as users list, active sessions, terminated sessions, applications for the selected country.

Applications

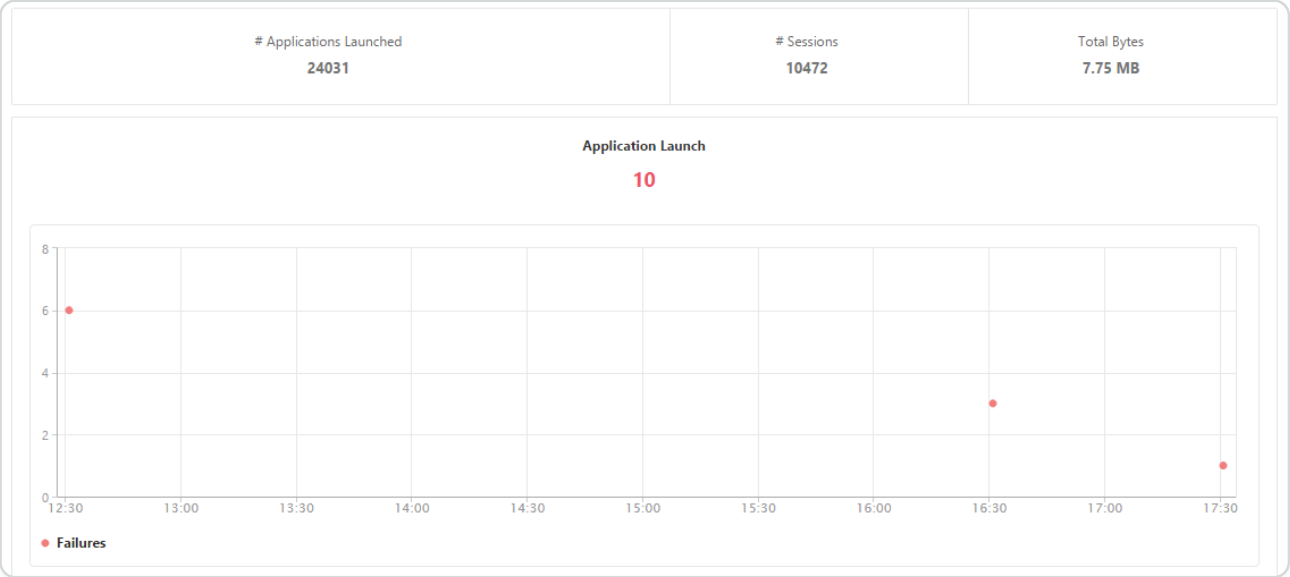
You can view the number of applications launched, number of total and active sessions, the number of total bytes and bandwidth consumed by the applications. You can view details of the users, sessions, bandwidth, and launch errors for an application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

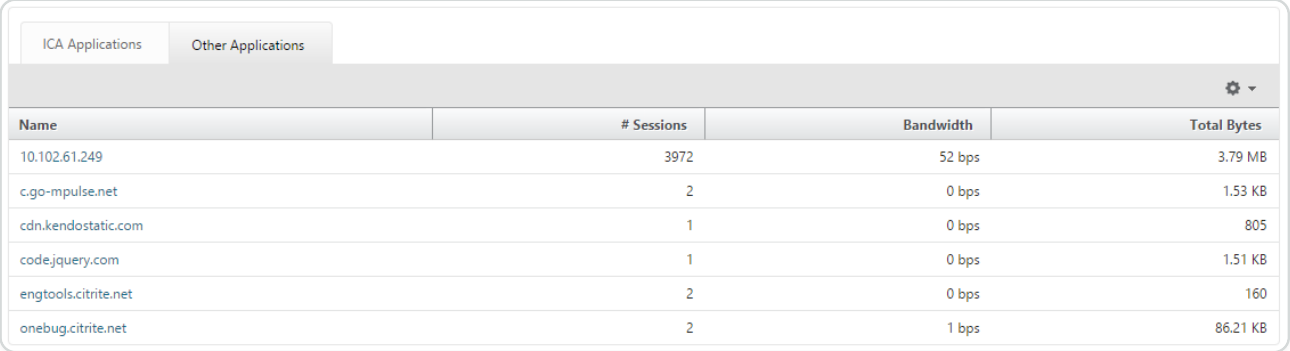
View application details

1. In NetScaler Console, navigate to **Gateway > Gateway Insight > Applications**.
2. Select the time period for which you want to view the application details. You can use the time slider to further customize the selected time period. Click **Go**.

You can now view the number of applications launched, number of total and active sessions, the number of total bytes and bandwidth consumed by the applications.



Scroll down to view the numbers of sessions, bandwidth, and total bytes consumed by ICA® and other applications.



Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	3972	52 bps	3.79 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB

On the **Other Applications** tab, you can click an application in the **Name** column to display details of that application.

Gateways

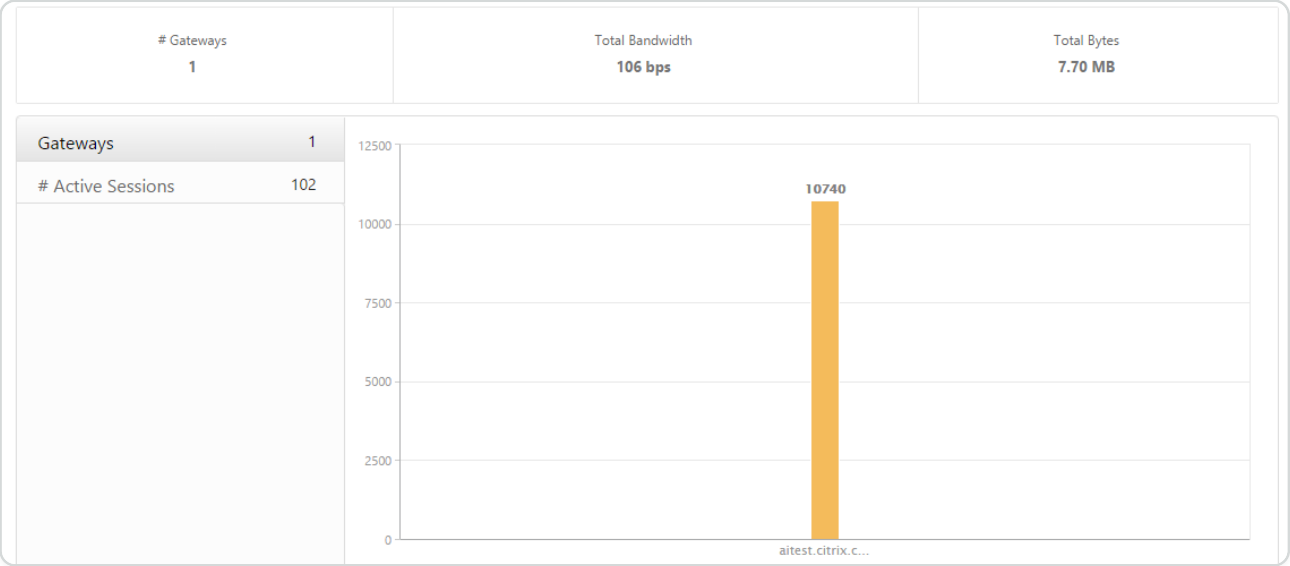
You can view the number of gateways, number of active sessions, total bytes and bandwidth used by all gateways associated with a NetScaler Gateway appliance at any given time. You can view the EPA, authentication, single sign-on, and application launch failures for a gateway. You can also view the details of all users associated with a gateway and their logon activity.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

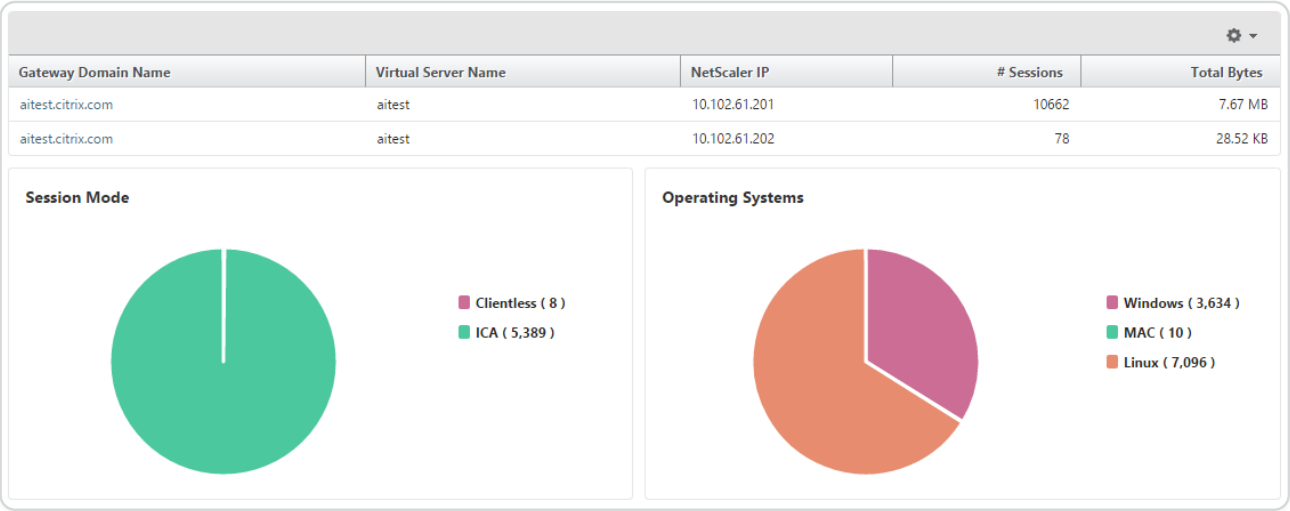
View gateway details

1. In NetScaler Console, navigate to **Gateway > Gateway Insight > Gateways**.
2. Select the time period for which you want to view the gateway details. You can use the time slider to further customize the selected time period. Click **Go**.

You can now view the number of gateways, number of active sessions, total bytes and bandwidth used by all gateways associated with a NetScaler Gateway appliance at any given time.



Scroll down to view the gateway details such as Gateway Domain Name, Virtual Server Name, NetScaler IP address, session modes, and Total Bytes.



You can click a gateway in the **Gateway Domain Name** column to display the EPA, authentication, single sign-on, and application launch failures and other details for a gateway.

You can also view a geo map for gateways that enables you to filter users based on a particular location.

1. Navigate to **Gateway > Gateway Insight > Gateways**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Select a gateway domain name to view the geo map
3. Click a country. For example, United States

   The geo map displays the details such as users list, active sessions, terminated sessions, applications for the selected country.

Exporting reports

You can save the Gateway Insight reports with all the details shown in the GUI in PDF, JPEG, PNG, or CSV format on your local computer. You can also schedule the export of the reports to specified email addresses at various intervals.

NOTE

- Users with read only access cannot export reports.
- Geo map reports are exported only if the NetScaler Console has internet connectivity.

Export a report

1. On the **Dashboard** tab, in the right pane, click the **export** button.
2. Under **Export Now**, select the required format, and then click **Export**.

To schedule export:

1. On the **Dashboard** tab, in the right pane, click the **export** button.
2. Under **Schedule Export**, specify the details and click **Schedule**.

NOTE

Configure the email server settings before scheduling the report by navigating to **System** > **Notifications** > **Email** and by clicking **Add**.

To add an email server or an email distribution list:

1. On the **Configuration** tab, navigate to **System** > **Notifications** > **Email**.
2. In the right pane, select **Email Server**, to add an email server or select **Email Distribution list** to create an email distribution list.
3. Specify the details and click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To export the entire Gateway Insight dashboard:

1. On the **Dashboard** tab, in the right pane, click the **export** button.
2. Under **Export Now**, select **PDF** format, and then click **Export**.

Gateway Insight Use Cases

The following use cases show how you can use Gateway Insight to gain visibility into users' access details, applications, and gateways on NetScaler Gateway appliances.

1. User is not able to log on to the NetScaler Gateway appliance or to the internal web servers

You are a NetScaler Gateway administrator monitoring NetScaler Gateway appliances through NetScaler Console, and you want to see why a user is unable to log in, or at what stage of the login process the failure has occurred.

NetScaler Console enables you to view the user login error details in the following stages of the login process:

- Authentication
- End-point analysis (EPA)
- Single sign-on

In NetScaler Console, you can search for a particular user and then view all the details for that user.

To search for a user:

In NetScaler Console, navigate to **Gateway > Gateway Insight** and, in the **Search for Users** text box, specify the user you want to search.

Authentication Failures

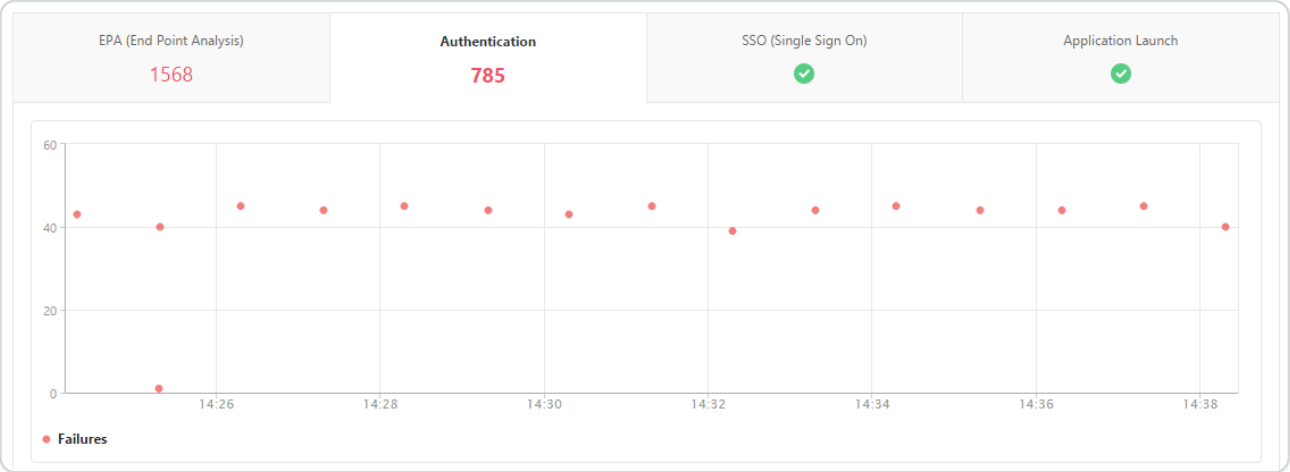
You can view authentication errors such as incorrect credentials or no response from the authentication server. If you have set up two-stage authentication, you can see whether the primary, secondary, or both stages of the authentication have failed.

View the authentication failure details

1. In NetScaler Console, navigate to **Gateway > Gateway Insight**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

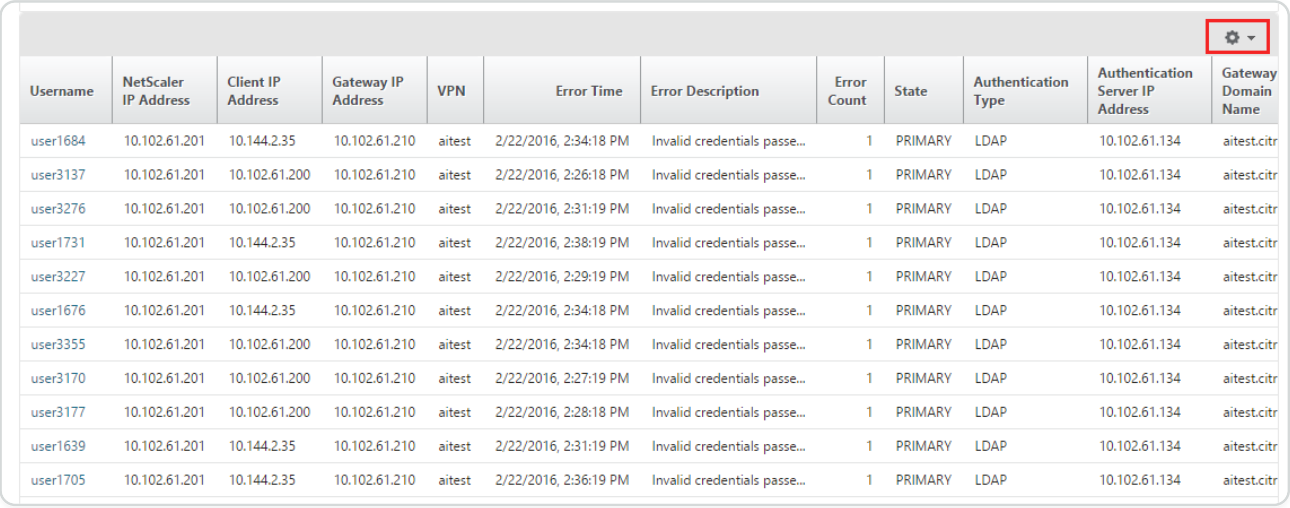
2. In the **Overview** section, select the time period for which you want to view the authentication errors. You can use the time slider to further customize the selected time period. Click **Go**.
3. Click the **Authentication** tab. You can view the number of authentication errors at any given time in the **Failures** graph.



Scroll down to view details of each authentication error such as **Username, Client IP Address, Error Time, Authentication type, Authentication Server IP Address**, and more from the table on the same tab. The **Error Description** column in the table displays the reason for the logon failure, and the **State** column displays at what stage of a two-stage authentication the failure occurred.

You can click a user in the **Username** column to display the authentication errors and other details for that user.

You can customize the table to add or delete columns by using the settings option.



Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	State	Authentication Type	Authentication Server IP Address	Gateway Domain Name
user1684	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3137	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:26:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3276	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1731	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:38:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3227	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:29:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1676	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3355	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3170	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:27:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3177	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:28:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1639	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1705	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:36:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr

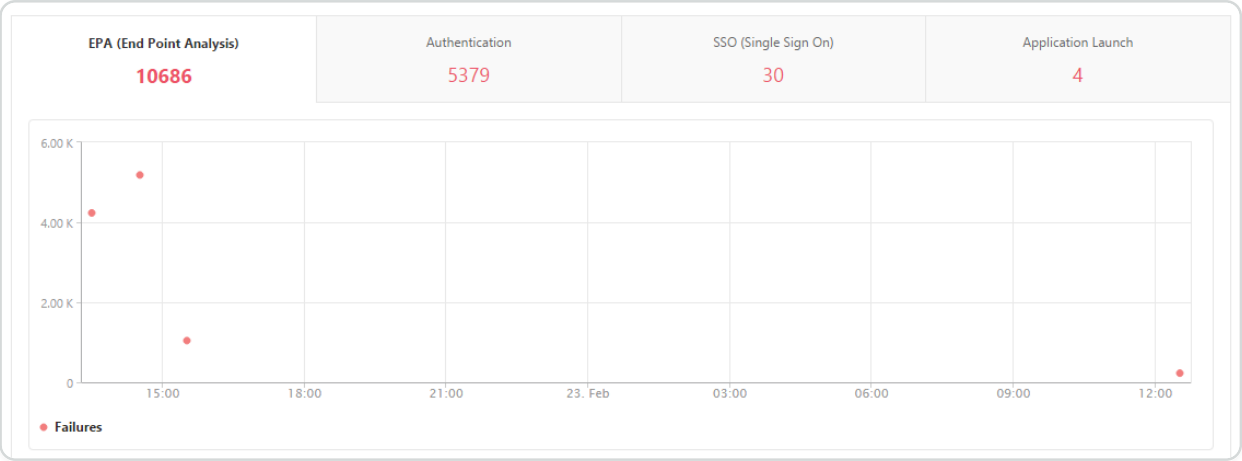
EPA Failures

You can view EPA failures at pre- or post-authentication stage.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View EPA failure details

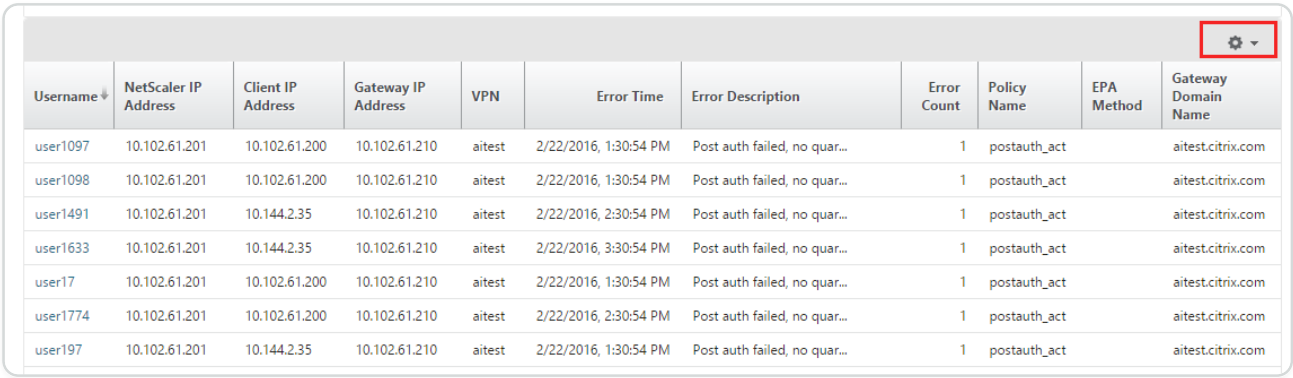
1. In NetScaler Console, navigate to **Gateway > Gateway Insight**.
2. In the Overview section, select the time period for which you want to view the EPA errors. You can use the time slider to further customize the selected time period. Click **Go**.
3. Click the **EPA (End Point Analysis)** tab. You can view the number of EPA errors at any given time in the **Failures** graph.



Scroll down to view details of each EPA error such as **Username, NetScaler IP Address, Gateway IP Address, VPN, Error Time, Policy Name, Gateway Domain Name** and more from the table on the same tab. The **Error Description** column in the table displays the reason for the EPA failure, and the **Policy Name** column displays the policy that resulted in the failure.

You can click a user in the **Username** column to display the EPA errors and other details for that user.

You can customize the table to add or delete columns by using the settings option.



Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	Policy Name	EPA Method	Gateway Domain Name
user1097	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1098	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1491	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1633	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 3:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user17	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1774	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user197	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

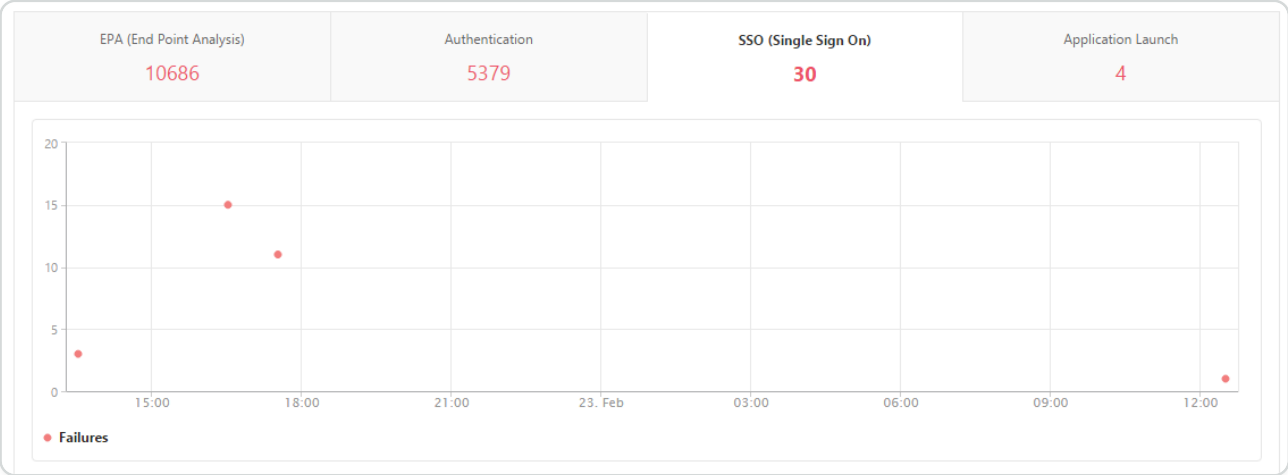
NetScaler Gateway doesn't report the EPA failures when the "clientSecurity" expression is configured as a VPN session policy rule.

SSO Failures

You can view the all the SSO failures at any stage for a user accessing any applications through the NetScaler Gateway appliance.

View SSO failure details

1. In NetScaler Console, navigate to **Gateway > Gateway Insight**.
2. In the Overview section, select the time period for which you want to view the SSO errors. You can use the time slider to further customize the selected time period. Click **Go**.
3. Click the **SSO (Single Sign On)** tab. You can view the number of SSO errors at any given time in the Failures graph.

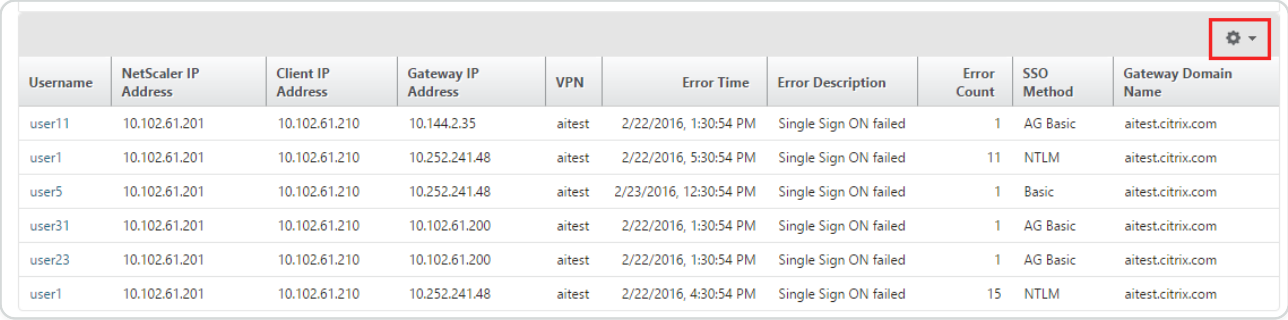


Scroll down to view details of each SSO error such as **Username, NetScaler IP Address, Error Time, Error Description, Resource Name** and more from the table on the same tab.

You can click a user in the **Username** column to display the SSO errors and other details for that user.

You can customize the table to add or delete columns by using the settings option.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



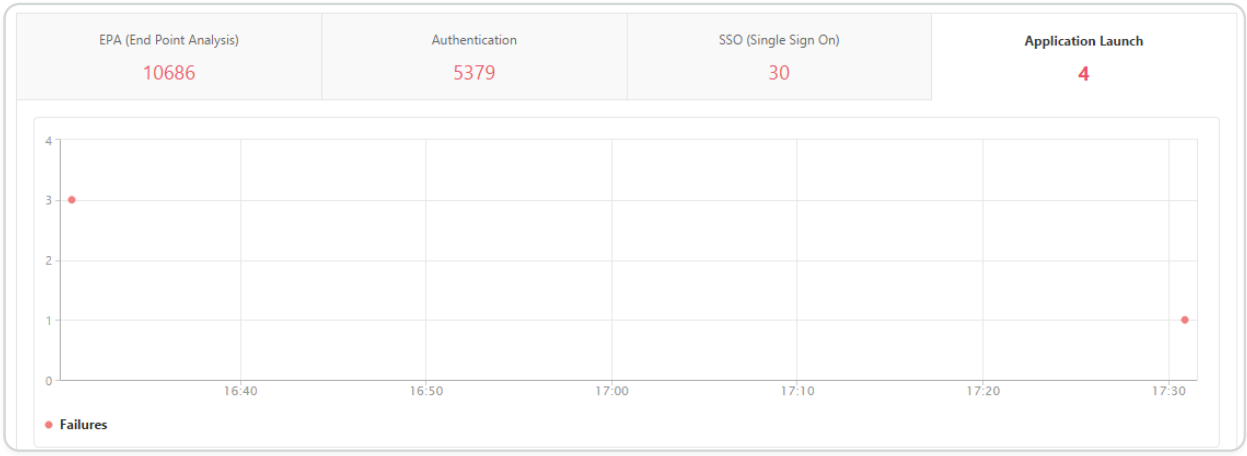
Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	SSO Method	Gateway Domain Name
user11	10.102.61.201	10.102.61.210	10.144.2.35	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 5:30:54 PM	Single Sign ON failed	11	NTLM	aitest.citrix.com
user5	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/23/2016, 12:30:54 PM	Single Sign ON failed	1	Basic	aitest.citrix.com
user31	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user23	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 4:30:54 PM	Single Sign ON failed	15	NTLM	aitest.citrix.com

2. After successfully logging on to NetScaler Gateway, a user is not able to launch any virtual application

For an application-launch failure, you can gain visibility into the reasons, such as inaccessible Secure Ticket Authority (STA) or Citrix Virtual App server, or invalid STA ticket. You can view the time the error occurred, details of the error, and the resource for which STA validation failed.

View application launch failure details

1. In NetScaler Console, navigate to **Gateway > Gateway Insight**.
2. In the **Overview** section, select the time period for which you want to view the SSO errors. You can use the time slider to further customize the selected time period. Click **Go**.
3. Click the **Application Launch** tab. You can view the number of application launch failures at any given time in the **Failures** graph.

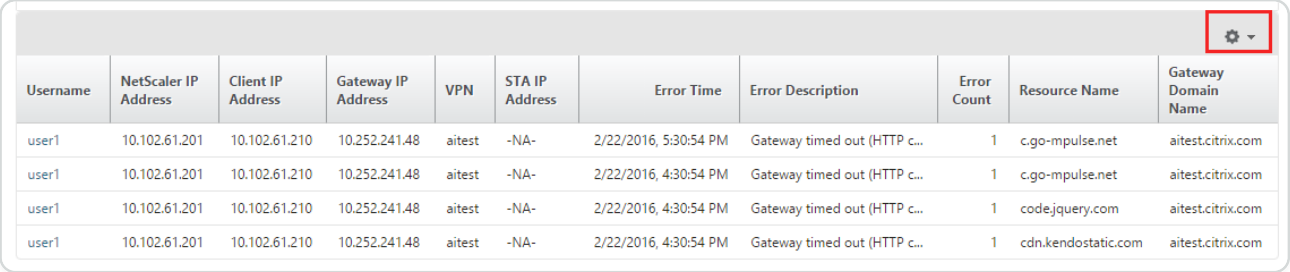


Scroll down to view details of each application launch error, such as **NetScaler IP Address, Error Time, Error Description, Resource Name, Gateway Domain Name**, and more, from the table on the same tab. The **Error Description** column in the table displays the IP address of the STA server and the **Resource Name** column displays the details of the resource for which the STA validation has failed.

You can click a user in the **Username** column to display the application launch errors and other details for that user.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can customize the table to add or delete columns by using the settings option.



Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	STA IP Address	Error Time	Error Description	Error Count	Resource Name	Gateway Domain Name
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 5:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	code.jquery.com	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	cdn.kendostatic.com	aitest.citrix.com

3. After successfully launching a new application, a user wants to view the total bytes and bandwidth consumed by that application

After you have successfully launched a new application, in NetScaler Console, you can view the total bytes and bandwidth consumed by that application.

View total bytes and bandwidth consumed by an application

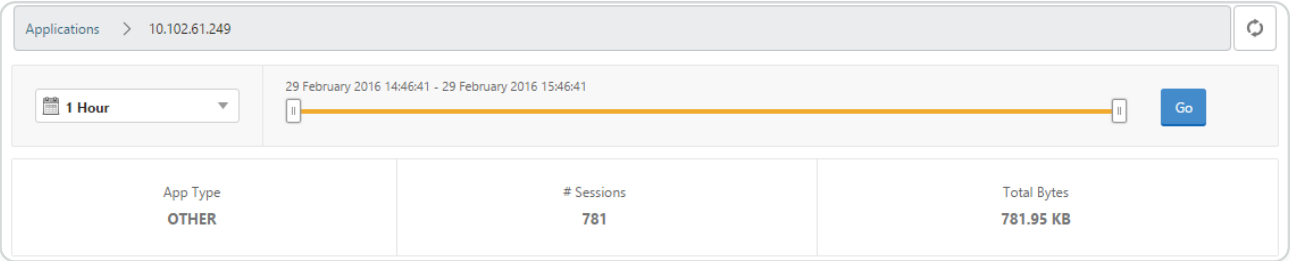
In NetScaler Console, navigate to **Gateway > Gateway Insight > Applications**, scroll down and, on the **Other Applications** tab, click the application for which you want to view the details.



ICA Applications | Other Applications

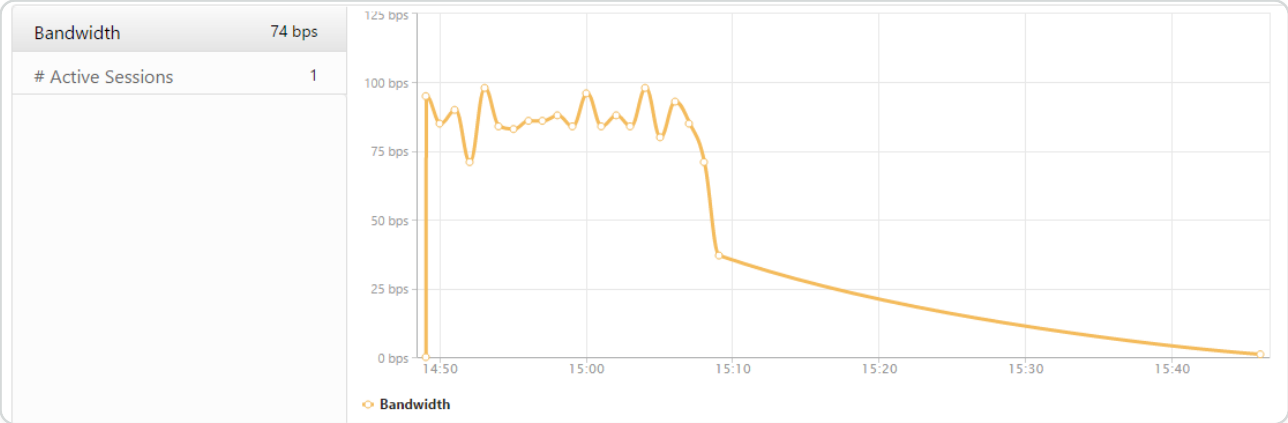
Name	# Sessions	Bandwidth	Total Bytes
10.102.61.134	1	0 bps	12.19 KB
10.102.61.249	4	0 bps	82.32 KB
alt1-safebrowsing.google.com	1	0 bps	1.04 KB
bcwhwkevnw	1	0 bps	1.98 KB
bcwhwkevnw.citrite.net	1	0 bps	1.01 KB

You can view the number of sessions and the total number of bytes consumed by that application.



You can also view the bandwidth consumed by that application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. A user has logged on to NetScaler Gateway successfully, but is unable to access certain network resources in the internal network

With Gateway Insight, you can determine whether the user has access to the network resources or not. You can also view the name of the policy that resulted in the failure.

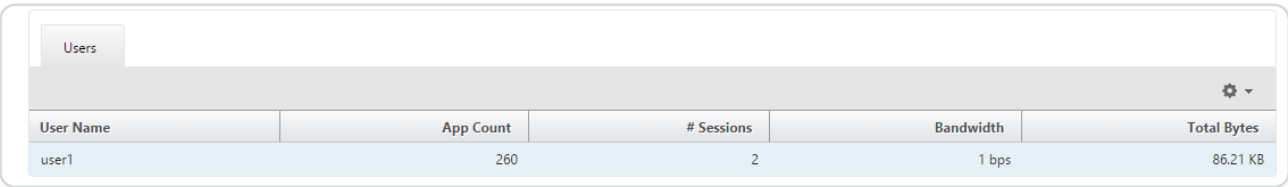
View user access for resources

1. In NetScaler Console, navigate to **Gateway > Gateway Insight > Applications**.
2. On the screen that appears, scroll down, and on the **Other Applications** tab, select the application to which the user was unable to log on to.



Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	2499	32 bps	2.36 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB
rock.citrite.net	1	0 bps	120

On the screen that appears, scroll down, and in the **Users** table, all the users that have access to that application are displayed.



User Name	App Count	# Sessions	Bandwidth	Total Bytes
user1	260	2	1 bps	86.21 KB

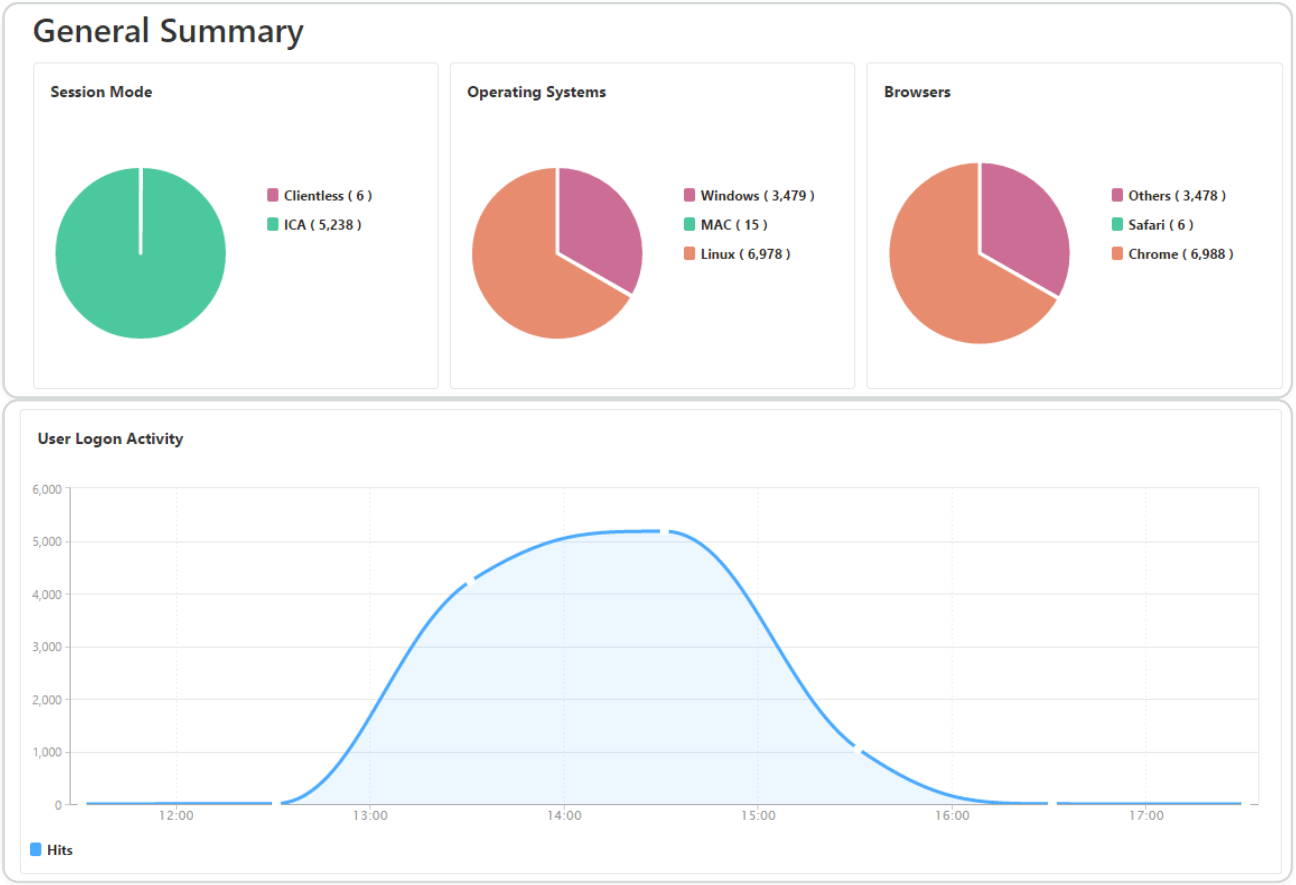
© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Different users might be using different NetScaler Gateway deployments or might log on to NetScaler Gateway through different access modes. The administrator must be able to view details about the deployment types and access modes

With Gateway Insight, you can view a summary of the different session modes used by users to log on, the types of clients, and the number of users logged on every hour. You can also determine whether a user's deployment is a unified gateway or classic NetScaler Gateway deployment. For unified gateway deployments, you can view the content switching virtual server name and IP address and the VPN virtual server name.

View summary of session modes, type of clients, and number of users logged on

1. In NetScaler Console, navigate to **Gateway > Gateway Insight**.
2. In the **Overview** section, scroll down to view the **Session Mode, Operating Systems, Browsers**, and **User Logon Activity** charts display the different session modes used by users to log on, the types of clients, and the number of users logged on every hour.



Troubleshoot Gateway Insight issues

If the Gateway Insight solution is not functioning as expected, the issue might be with one of the following. Refer to the checklists in the respective sections for troubleshooting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Gateway Insight configuration.
- Connectivity issue between NetScaler and NetScaler Console.
- Record generation in NetScaler.
- Validations in NetScaler Console.

Gateway Insight configuration checklist

- Make sure that the AppFlow feature is enabled in NetScaler. For details, see Enabling AppFlow.
- Check Gateway Insight configuration in the NetScaler running configuration.

  Run the `show running | grep -i <appflow_policy>` command to check the Gateway Insight configuration. Make sure that the bind type is REQUEST. For example;

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

- For single-hop, Access Gateway, or Unified Gateway deployment, make sure that Gateway Insight AppFlow policy is bound to the VPN virtual server, where VPN traffic is flowing. For details, see Enabling HDX Insight data collection.
- Check `appflowlog` parameter in NetScaler Gateway/VPN virtual server. For details, see Enabling AppFlow for Virtual Servers.

Connectivity between NetScaler and NetScaler Console checklist

- Check AppFlow collector status in NetScaler. For details, see How to check the status of connectivity between NetScaler and AppFlow Collector.
- Check Gateway Insight AppFlow® policy hits.

  Run the command `show appflow policy <policy_name>` to check the AppFlow policy hits.

  You can also navigate to **System > AppFlow > Policies** in the GUI to check the AppFlow policy hits.
- Validate any firewall blocking AppFlow ports 4739 or 5557.

Record generation in NetScaler checklist

- Run the `nsconmsg -d stats -g ai_tot` command and check for the stats increments in NetScaler.
- Capture `nstrace` logs and check for CFLOW packets to confirm NetScaler exports AppFlow records.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Validations in NetScaler Console

- Run the `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: vpn_"` command to check the logs to confirm NetScaler Console is receiving AppFlow records.
- Make sure that the NetScaler instance is added to NetScaler Console.
- Make sure that the NetScaler Gateway/VPN virtual server is licensed in NetScaler Console.

Gateway Insight stats

The following Gateway Insight stats are available.

- ai_tot_preauth_epa_export
- ai_tot_auth_export
- ai_tot_auth_session_id_update_export
- ai_tot_postauth_epa_export
- ai_tot_vpn_update_export
- ai_tot_ica_fileinfo_export
- ai_tot_app_launch_failure
- ai_tot_logout_export
- ai_tot_skip_appflow_export
- ai_tot_sso_appflow_export
- ai_tot_authz_appflow_export
- ai_tot_appflow_pol_eval_failure
- ai_tot_vpn_export_state_mismatch
- ai_tot_appflow_disabled

Contact Citrix technical support

For a speedy resolution, make sure that you have the following information before contacting Citrix technical support:

- Details of the deployment and network topology.
- NetScaler and NetScaler Console versions.
- Tech support bundle for NetScaler and NetScaler Console.
- `nstrace` capture during the issue.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Known Issues

Refer NetScaler release notes for known issues on Gateway Insight.

HDX™ Insight

HDX Insight provides end-to-end visibility for HDX traffic to Citrix Virtual Apps and Desktops passing through NetScaler. It also enables administrators to view real-time client and network latency metrics, historical reports, End-to-end performance data, and troubleshoot performance issues. Availability of both real-time and historical visibility data enables NetScaler Console to support a wide variety of use cases.

For any data to appear you need to enable AppFlow on your NetScaler Gateway virtual servers. AppFlow can be delivered by the **IPFIX** protocol or the **Logstream** method.

NOTE

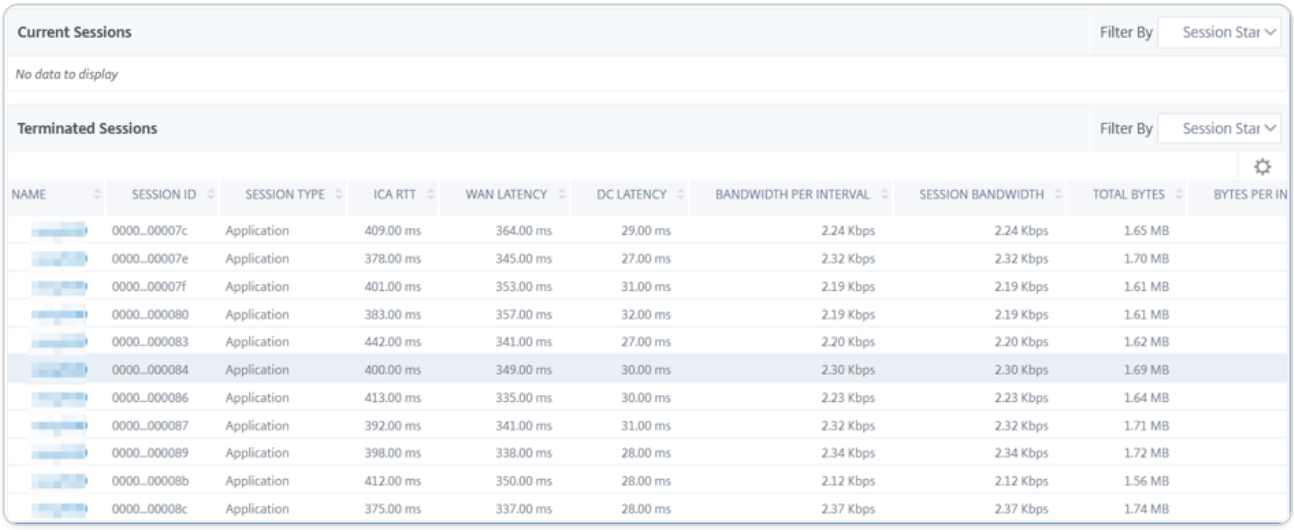
To allow ICA® round trip time calculations to be logged, enable the following policy settings:

- ICA Round Trip Calculation
- ICA Round Trip Calculation Interval
- ICA Round Trip Calculation for Idle Connections

If you click an individual user, you can see each HDX session, active or terminated, that the user made within the selected time frame. Other information includes several latency statistics and bandwidth consumed during the session. You can also get bandwidth information from individual virtual channels such as audio, printer mapping and client drive mapping.

You can also visualize a consolidated view of all users active and terminated sessions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



As an administrator, this view enables you to:

- View all users details in a single-pane visualization
- Eliminate the complexity in selecting each user and seeing the active and terminated sessions

NOTE

When you create a group, you can assign roles to the group, provide application-level access to the group, and assign users to the group. NetScaler Console analytics now supports virtual IP address based authorization. Your users can now see reports for all Insights for only the applications (virtual servers) that they are authorized to. For more information on groups and assigning users to the group, see Configuring Groups on NetScaler Console.

You can also navigate to **HDX Insight** > **Applications** and click **Launch Duration** to view the time taken for the application to launch. You can also view the user agent of all connected users by navigating to **HDX Insight > Users**.

NOTE

HDX insight supports Admin Partitions configured in NetScaler instances running on software version 12.0.

The following Thin Clients support HDX Insight:

- WYSE Windows-based Thin Clients
- WYSE Linux-based Thin Clients
- WYSE ThinOS-based Thin Clients

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 10ZiG Ubuntu-based Thin Clients

Identifying the root cause of slow performance issues

Scenario 1

User is experiencing delays while accessing Citrix Virtual Apps and Desktops

The delays might be due to latency on the server network, ICA traffic delays caused by the server network, or latency on the client network.

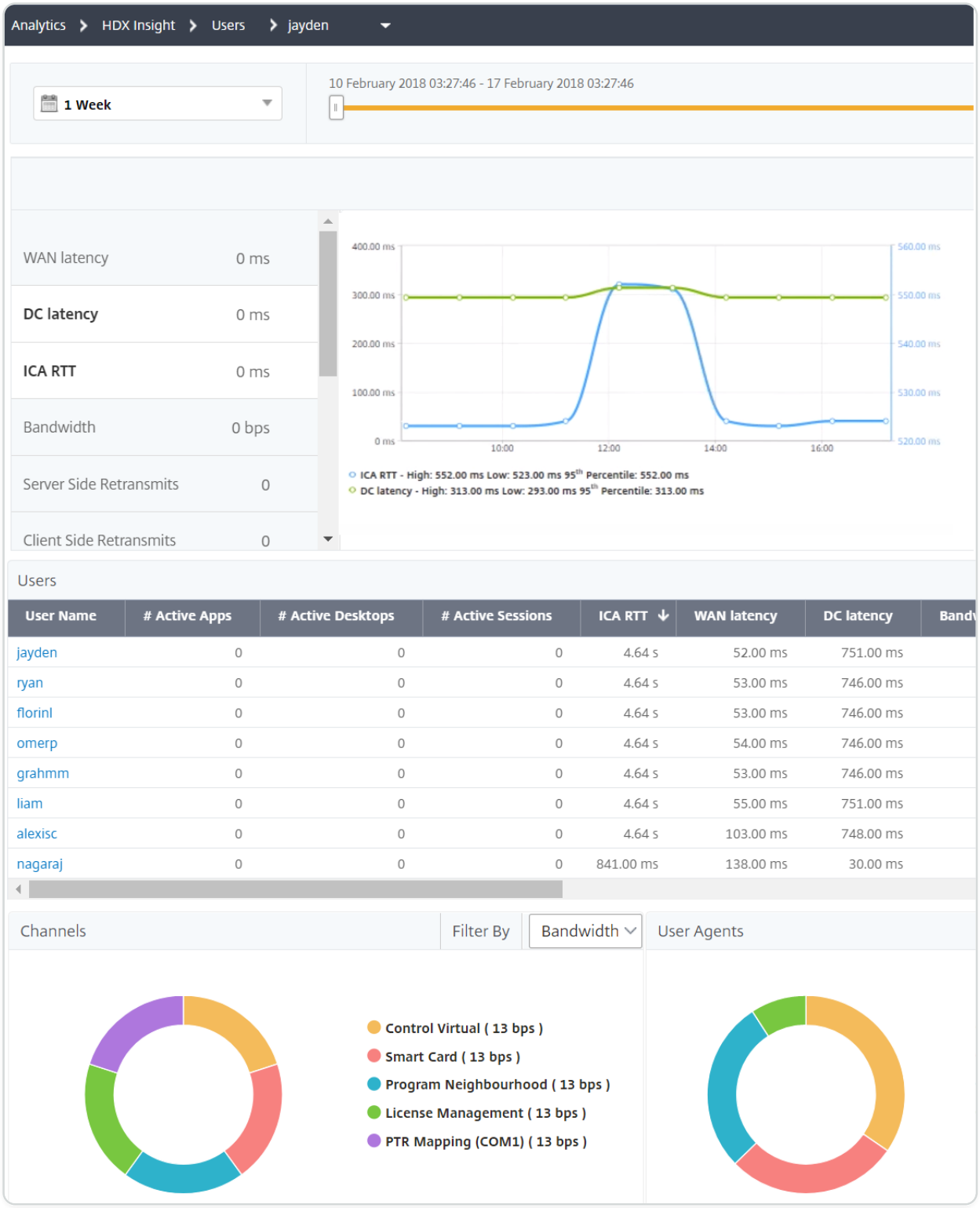
To identify the root cause of the issue, analyze the following metrics:

- WAN Latency
- DC Latency
- Host Delay

To view the client metrics:

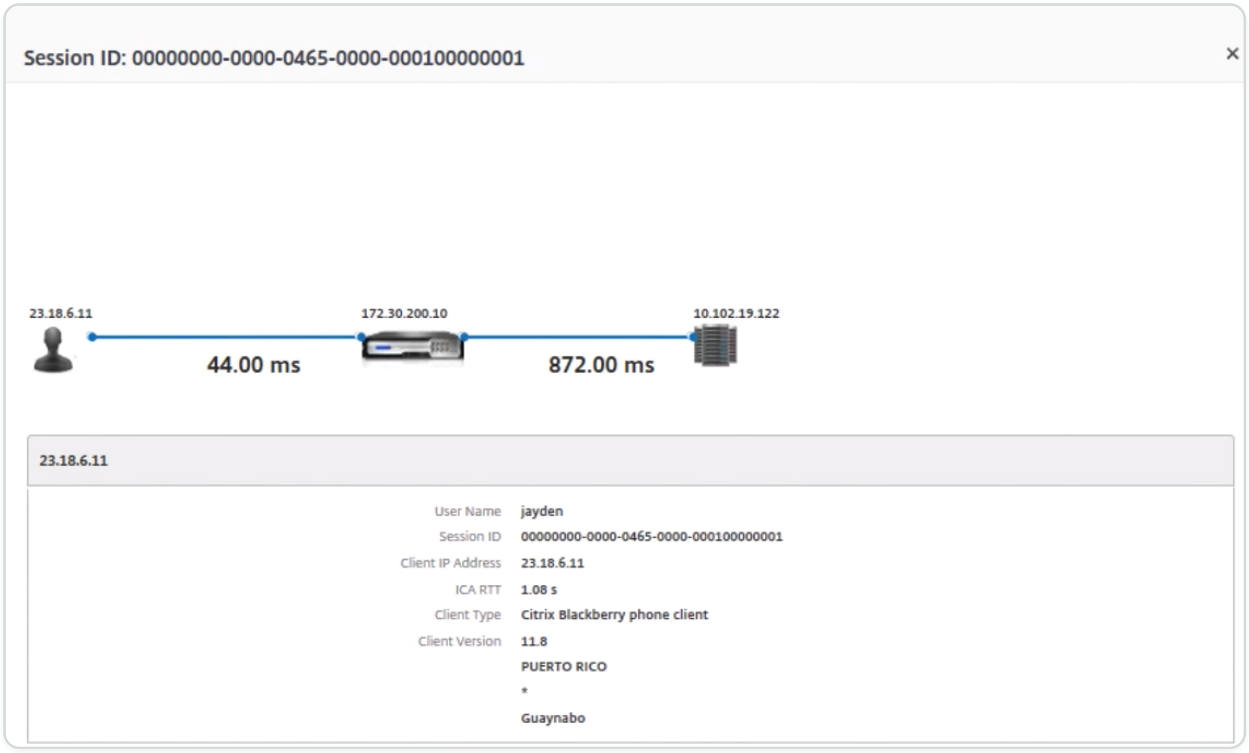
1. On the **Analytics** tab, navigate to **HDX Insight** > **Users**.
2. Scroll down and select the user name and select the period from the list. The period can be one day, one week, one month, or you can even customize the period for which you want to see the data.
3. The chart displays the ICA RTT and DC latency values of the user for the specified period as a graph.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. On the **Current Application Sessions** table, hover the mouse over the **RTT** value and note the host delay, DC latency, and WAN latency values.
5. On the **Current Application Sessions** table, click the hop diagram symbol to display information about the connection between the client and the server, including latency values.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Summary:

In this example, the **DC Latency** is 751 milliseconds, the **WAN latency** is 52 milliseconds and **Host Delays** is 6 seconds. This indicates that the user is experiencing delay due to average latency caused by the server network.

Scenario 2

User is experiencing delay while launching an application on Citrix Virtual Apps™ or Desktops

The delay might be due to latency on the server network, ICA-traffic delays caused by the server network, latency on the client network, or time taken to launch an application.

To identify the root cause of the issue, analyze the following metrics:

- WAN latency
- DC latency
- Host delay

To view the user metrics:

1. Navigate to **Gateway** > **HDX Insight** > **Users**.
2. Scroll down and click the user name.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. In the graphical representation, note the WAN Latency, DC Latency and RTT values for the particular session.
4. In the **Current Application Sessions** table, note that the host delay is high.

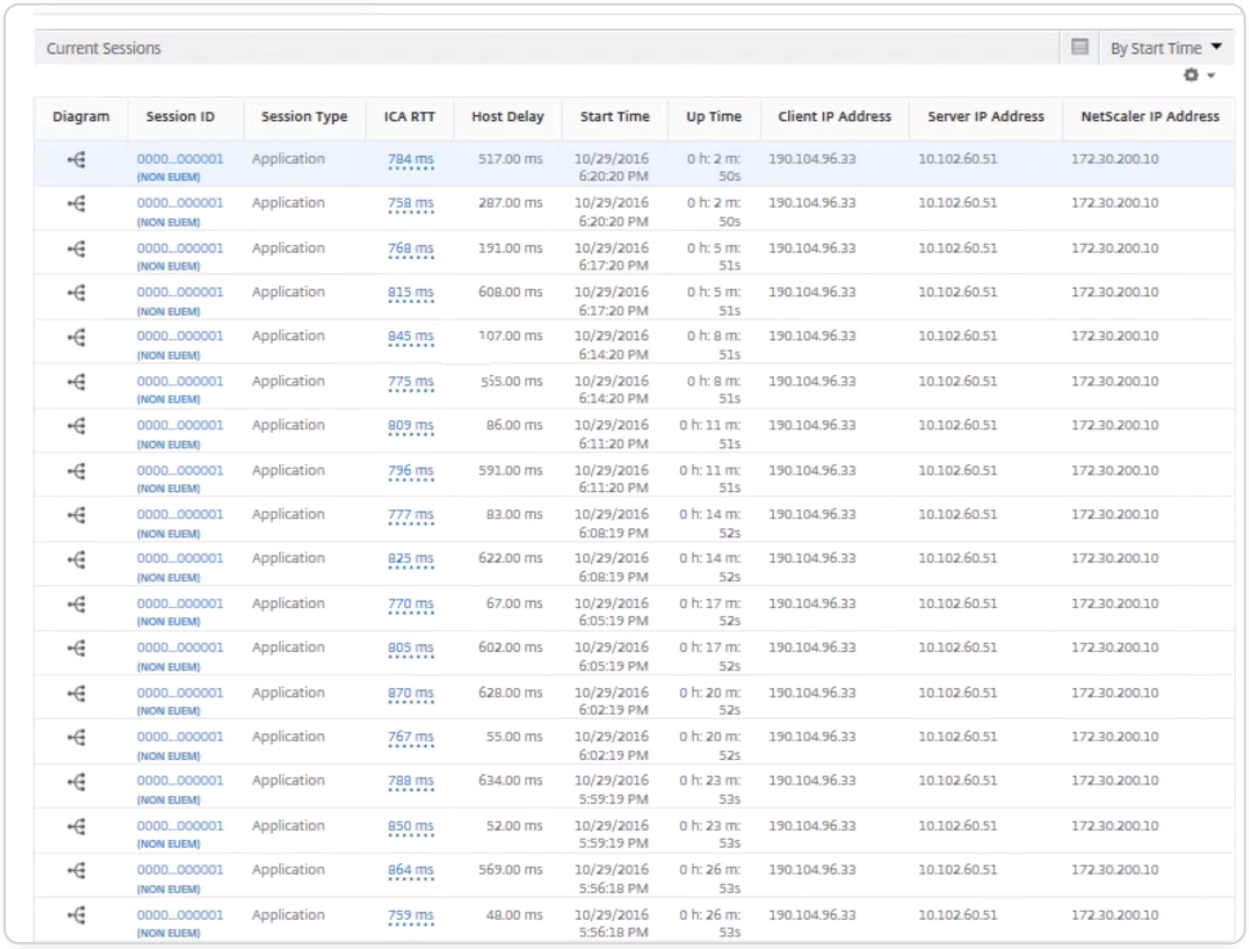


Diagram	Session ID	Session Type	ICA RTT	Host Delay	Start Time	Up Time	Client IP Address	Server IP Address	NetScaler IP Address
	0000...000001 (NON EUEM)	Application	784 ms	517.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	758 ms	287.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	768 ms	191.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	815 ms	608.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	845 ms	107.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	775 ms	555.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	809 ms	86.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	796 ms	591.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	777 ms	83.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	825 ms	622.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	770 ms	67.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	805 ms	602.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	870 ms	628.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	767 ms	55.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	788 ms	634.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	850 ms	52.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	864 ms	569.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	759 ms	48.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10

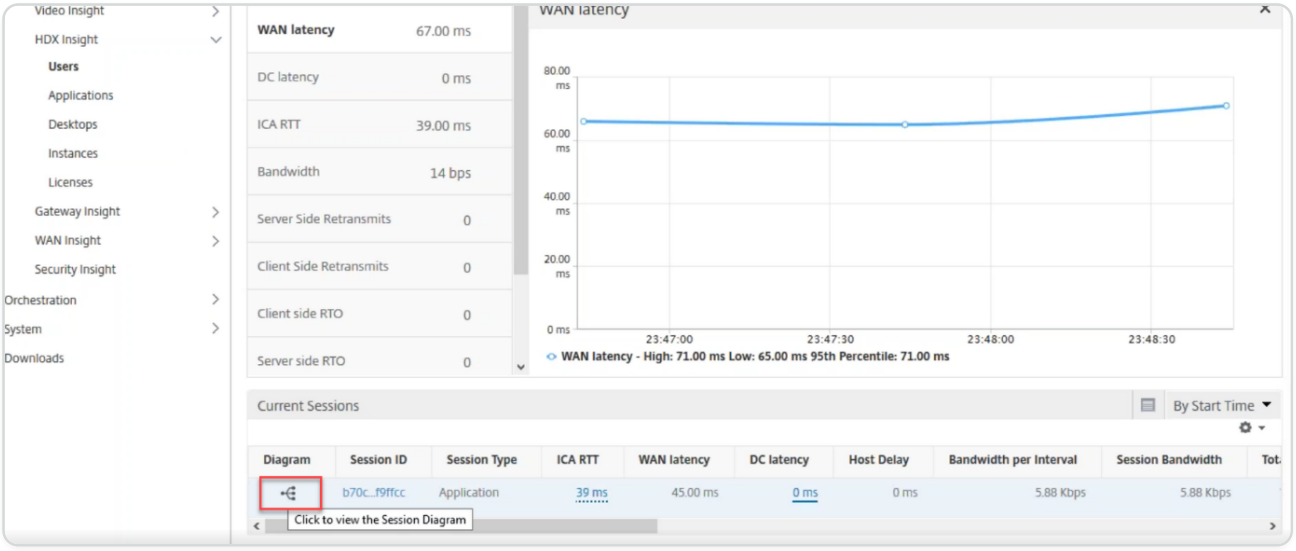
Summary:

In this example, the **DC Latency** is 1 millisecond, the **WAN latency** is 12 milliseconds, but the **Host Delay** is 517 milliseconds. High RTT with low DC and WAN latencies indicates an application error on the host server.

NOTE

HDX Insight also displays more user metrics, such as WAN jitter and Server Side Retransmits if you are using NetScaler Console running software 11.1 build 51.21 or later. To view these metrics, navigate to **Gateway** > **HDX Insight** > **Users**, and select a user name. The user metrics appear in the table next to the graph.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Geo map for HDX Insight

Geo map feature in NetScaler Console displays the usage of web applications across different geographical locations on a map. As an administrator, you can use this information to understand the trends in application usage and for capacity planning.

Geo map provides information about the following metrics specific to a country, state, and city:

- Total Hits: Total number of times an application is accessed.
- Bandwidth: Total bandwidth consumed while serving client requests
- Response Time: Average time taken to send responses to client requests.

Geo map provides information which can be used to address several use cases such as the following:

- Region that has the maximum number of clients accessing an application
- Region that has the highest response time
- Region that consumes the most bandwidth

NetScaler Console **automatically enables** geomaps for private IP addresses or public IP addresses, when you enable **Web insight**.

Create a private IP block

NetScaler Console can recognize the location of a client when the client private IP address is added to the NetScaler Console server. For example, if the IP address of a client falls within the range of a private IP address block associated with City A, NetScaler Console recognizes that the traffic is originating from City A for this client.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To create an IP block:

1. In NetScaler Console, navigate to **Settings > Analytics Settings > IP Blocks**, and then click **Add**.
2. In **Create IP Blocks** page, specify the following parameters:
    - **Name**. Specify a name for the private IP block
    - **Start IP address**. Specify the lowest IP address range for the IP block.
    - **End IP address**. Specify the highest IP address range for the IP block.
    - **Country**. Select the country from the list.
    - **Region**. Based on the country, the region is auto-populated, but you can select your region.
    - **City**. Based on the region, the city is auto-populated, but you can select your city.
    - **City Latitude** and **City Longitude**. Based on the city you select, the latitude and longitude are auto-populated.
3. Click **Create** to finish.

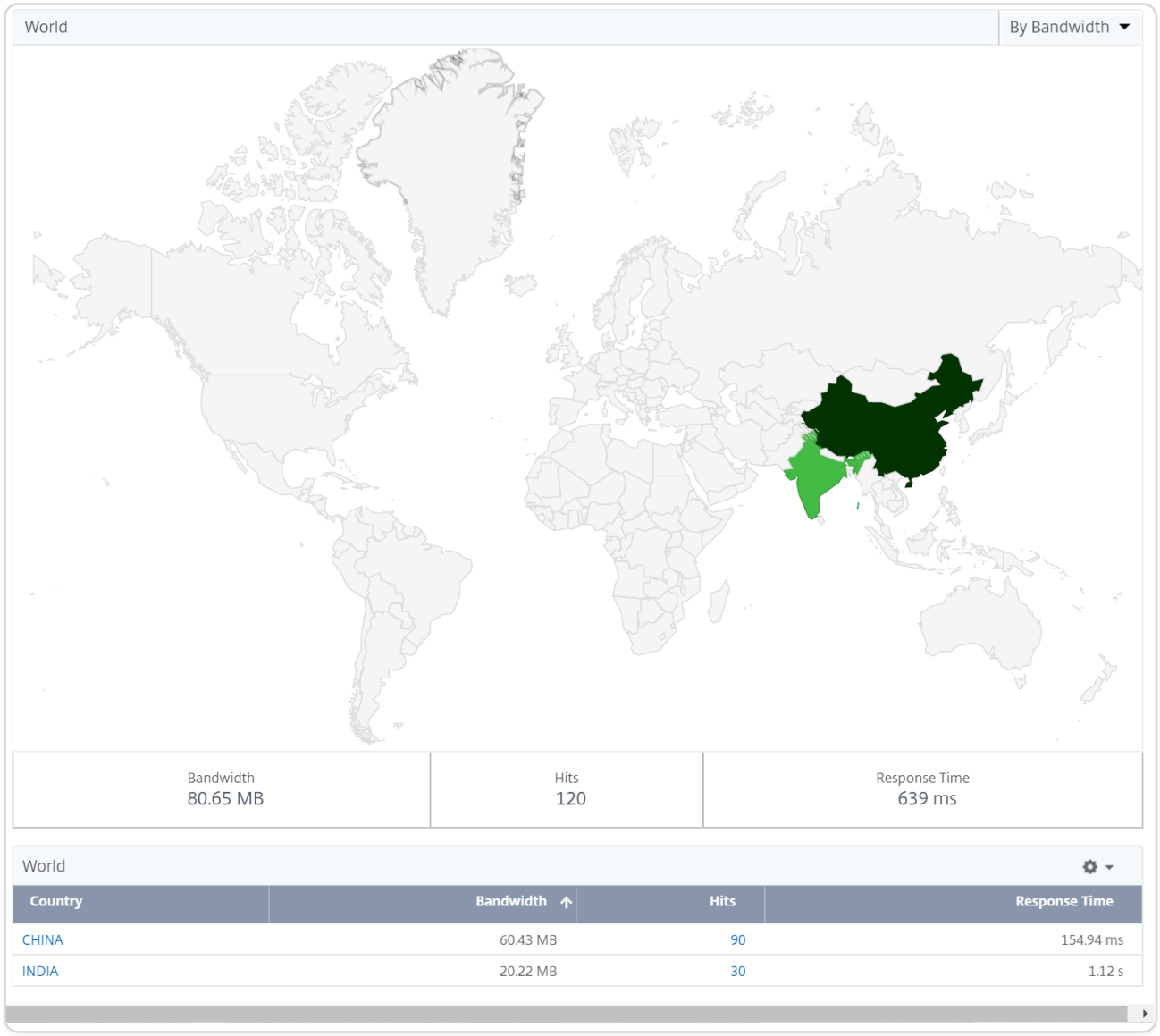
Public IP blocks

NetScaler Console can also recognize the client location if the client uses public IP address. NetScaler Console has its built-in location CSV file that matches the location based on the client IP address range. For using public IP block, the only requirement is that you have to enable the **Enable geo data** collection from the Configure Insight page.

Note

> NetScaler Console requires an internet connection to display the geomaps for a particular geographical location. Internet connection is also required to export the GeoMap in .pdf, .png, or .jpg formats.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



To export the report of this dashboard:

To export the report of this page, click the **Export** icon on the top right side of this page. On the **Export** page, you can do one of the following:

1. Select **Export Now** tab. To view and save the report in PDF, JPEG, PNG, or CSV format.
2. Select **Schedule Export** tab. To schedule the report daily, weekly, or monthly and send the report over email or slack message.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

- If you select **Weekly** recurrence, ensure that you select the weekdays on which you want the report to be scheduled.
- If you select **Monthly** recurrence, ensure that you enter all the days that you want the report to be scheduled separated by commas.

To configure a geomap for data centers:

On the **Infrastructure** tab, navigate to **Sites** > **Private IP Blocks** to configure geomaps for a particular location.

Use Case

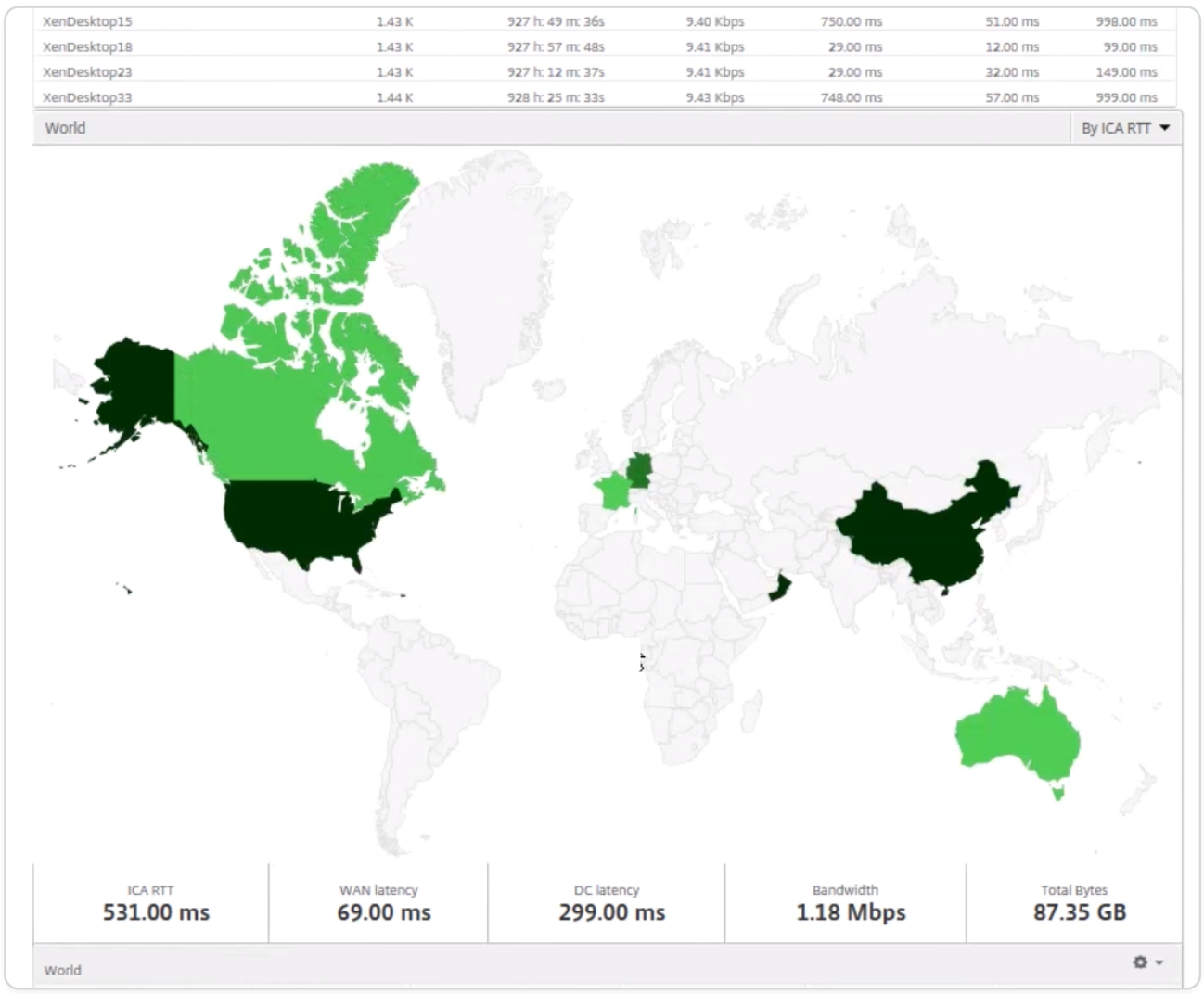
Consider a scenario in which organization ABC has 2 branch offices, one in Santa Clara and the other in India.

The Santa Clara users use the NetScaler Gateway appliance at SClara.x.com to access VPN traffic. The Indian users use the NetScaler Gateway appliance at India.x.com to access VPN traffic.

During a particular time-interval, say 10 AM to 5 PM, the users in Santa Clara connect to SClara.x.com to access VPN traffic. Most of the users access the same NetScaler Gateway, causing a delay in connecting to the VPN, so some users connect to India.x.com instead of SClara.x.com.

A NetScaler administrator analyzing the traffic can use the geo map functionality to show the traffic in Santa Clara office. The map shows that the response time in the Santa Clara office is high, because the Santa Clara office has only one NetScaler Gateway appliance through which users can access VPN traffic. The administrator might therefore decide to install another NetScaler Gateway, so that users have two local NetScaler Gateway appliances through which to access the VPN.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Limitations

If NetScaler instances have Advanced license, thresholds set on NetScaler Console for HDX Insight will not be triggered since analytical data is collected for only 1 hour.

To export the report of this dashboard:

To export the report of this page, click the **Export** icon on the top right side of this page. On the **Export** page, you can do one of the following:

1. Select **Export Now** tab. To view and save the report in PDF, JPEG, PNG, or CSV format.
2. Select **Schedule Export** tab. To schedule the report daily, weekly, or monthly and send the report over email or slack message.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

- If you select **Weekly** recurrence, ensure that you select the weekdays on which you want the report to be scheduled.
- If you select **Monthly** recurrence, ensure that you enter all the days that you want the report to be scheduled separated by commas.

Enable HDX™ Insight data collection

HDX Insight enables the administrator to deliver an exceptional user experience by providing end-to-end visibility into the ICA traffic that passes through the NetScaler appliance.

HDX Insight delivers compelling and powerful business intelligence and failure analysis capabilities for the network, virtual desktops, applications, and application fabric. HDX Insight can both instantly triage on user issues, collects data about virtual desktop connections, and generates AppFlow® records and presents them as visual reports.

The configuration to enable data collection in the NetScaler instances differs with the position of the appliance in the deployment topology. This topic includes the following details:

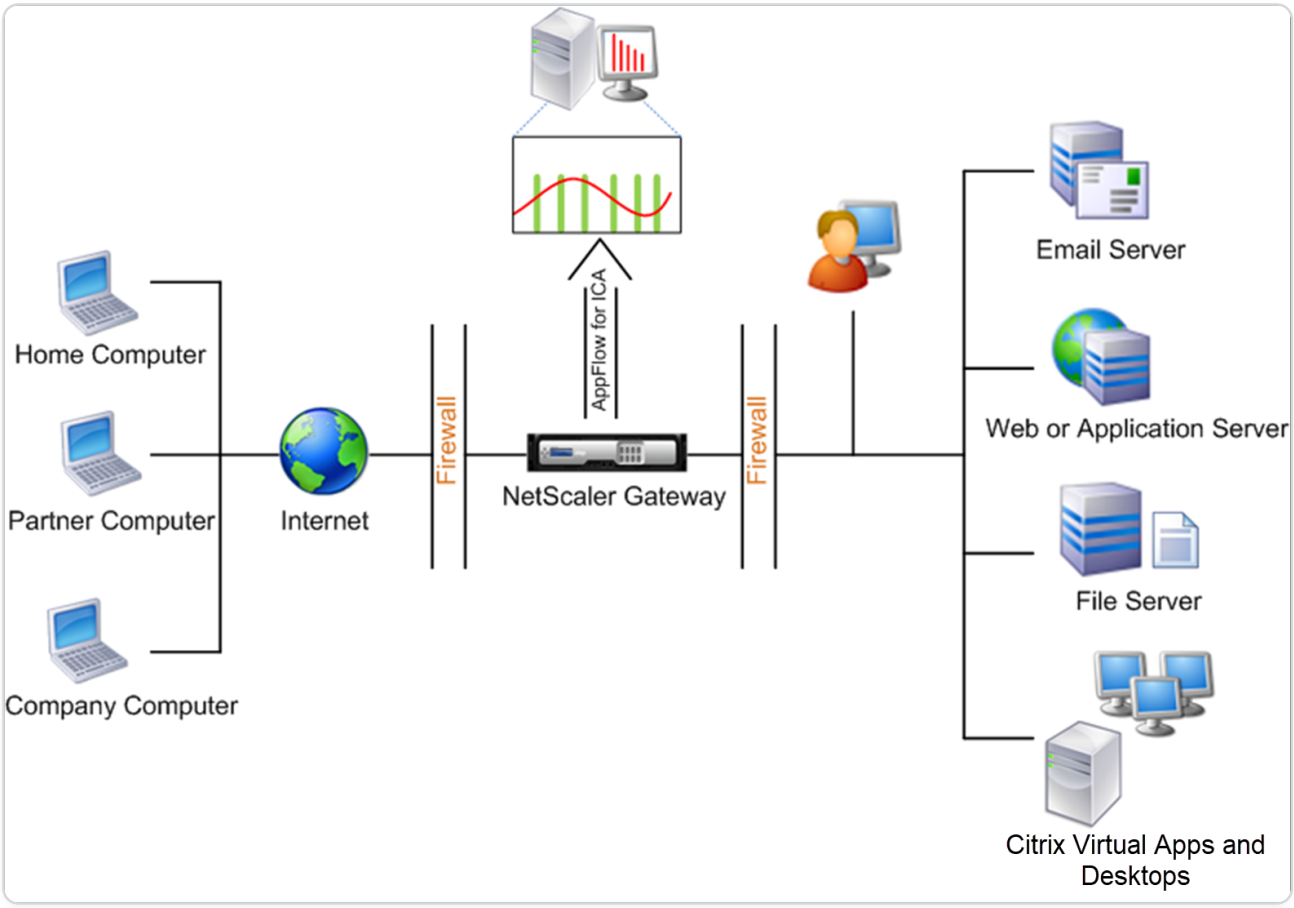
- Enabling data collection for monitoring NetScaler instances deployed in transparent mode
- Enabling data collection for NetScaler Gateway appliances deployed in single-hop mode
- Enabling data collection for NetScaler Gateway appliances deployed in double-hop mode
- Enabling data collection for monitoring NetScalers deployed in LAN user mode

Enable data collection for NetScaler Gateway appliances deployed in single-hop mode

When NetScaler Gateway is deployed in single-hop mode, the NetScaler Gateway is at the edge of the network and proxies ICA connections to the desktop delivery infrastructure. This deployment is the simplest and most common deployment. This mode provides security if an external user tries to access the internal network in an organization. In single-hop mode, users access the NetScaler appliances through a virtual private network (VPN).

To start collecting the reports, you must add the NetScaler Gateway appliance to the NetScaler Console inventory and enable AppFlow on NetScaler Console. The following image illustrates a NetScaler Console deployed in single-hop mode

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Enable the AppFlow feature from NetScaler Console

1. Navigate to **Infrastructure** > **Instances**, and select the NetScaler instance you want to enable analytics.
2. From the **Select Action** list, select **Configure Analytics**.
3. Select the VPN virtual servers, and click **Enable Analytics**.
4. Select **Web Insight**.
5. Click **OK**.

NOTE

The following commands start to run in the background when you enable AppFlow® in single-hop mode. These commands are explicitly specified here for troubleshooting purposes.

- `add appflow collector \<name\> -IPAddress \<ip\_addr\>`
- `add appflow action \<name\> -collectors \<string\>`
- `set appflow param -flowRecordInterval \<secs\>`
- `disable ns feature AppFlow`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `enable ns feature AppFlow`
- `add appflow policy \<name\> \<rule\> \<expression\>`
- `set appflow policy \<name\> -rule \<expression\>`
- `bind vpn vserver \<vsname\> -policy \<string\> -type \<type\> >-priority \<positive\_integer\>`
- `set vpn vserver \<name\> -appflowLog ENABLED`
- `save ns config`

Enable data collection to monitor NetScalers deployed in transparent mode

When a NetScaler is deployed in transparent mode the clients can access the servers directly, with no intervening virtual server. If a NetScaler appliance is deployed in transparent mode in a Citrix Virtual Apps and Desktops environment, the ICA traffic is not transmitted over a VPN.

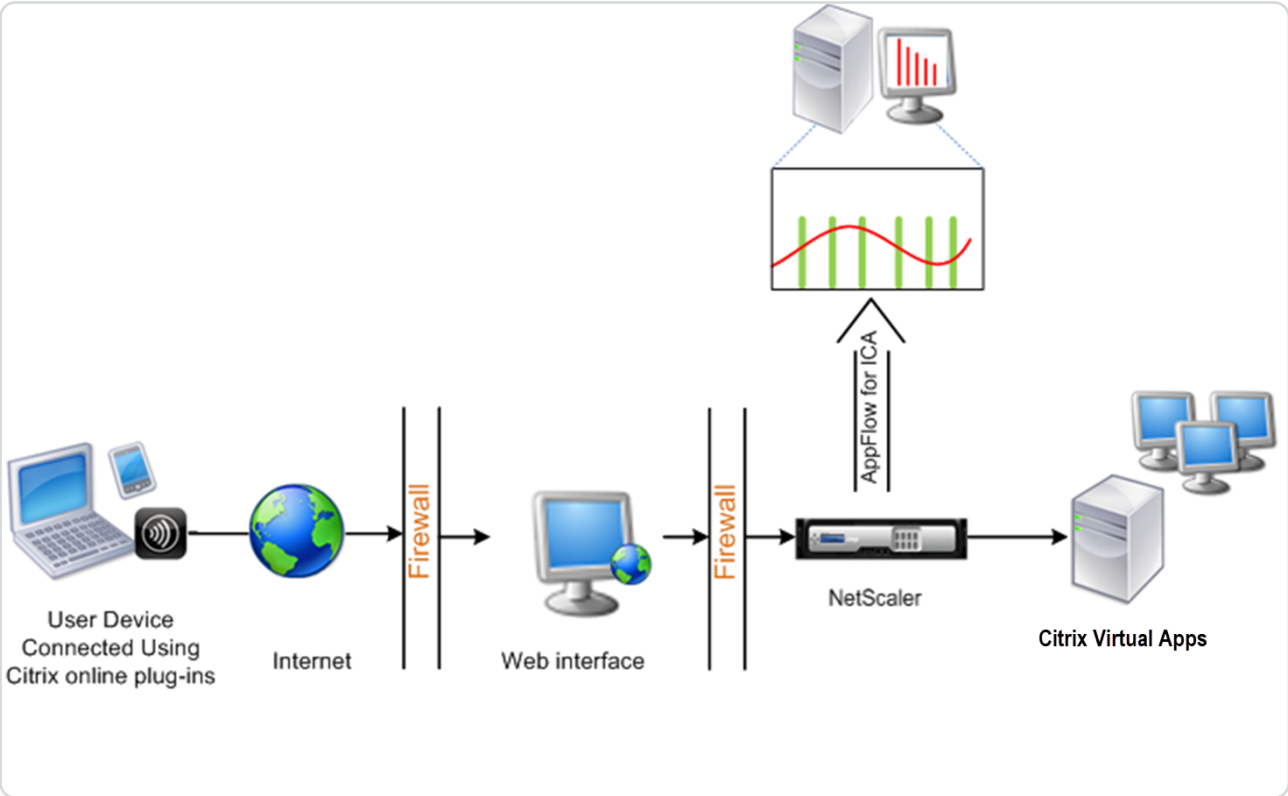
After you add the NetScaler to the NetScaler Console inventory, you must enable AppFlow for data collection. Enabling data collection depends on the device and the mode. In that case, you have to add NetScaler Console as an AppFlow collector on each NetScaler appliance, and you must configure an AppFlow policy to collect all or specific ICA traffic that flows through the appliance.

NOTE

- You cannot enable data collection on a NetScaler deployed in transparent mode by using the NetScaler Console configuration utility.
- For detailed information about the commands and their usage, see Command Reference.
- For information on policy expressions, see Policies and Expressions.

The following image shows the network deployment of a NetScaler Console when a NetScaler is deployed in a transparent mode:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



To configure data collection on a NetScaler appliance by using the command line interface:

At the command prompt, do the following:

1. Log on to an appliance.
2. Specify the ICA ports at which the NetScaler appliance listens for traffic.

   ```
   set ns param --icaPorts \<port\>...
   ```

   Example:

   ```
   set ns param -icaPorts 2598 1494
   ```

   NOTE

   - You can specify up to 10 ports with this command.
   - The default port number is 2598. You can modify the port number as required.

3. Add NetScaler Insight Center as an AppFlow collector on the NetScaler appliance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add appflow collector <name> -IPAddress <ip_addr>
```

Example:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

NOTE

To view the AppFlow collectors configured on the NetScaler appliance, use the **show appflow collector** command.

4. Create an AppFlow® action and associate the collector with the action.

```
add appflow action <name> -collectors <string> ...
```

Example:

```
add appflow action act -collectors MyInsight
```

5. Create an AppFlow policy to specify the rule for generating the traffic.

```
add appflow policy <policyname> <rule> <action>
```

Example:

```
add appflow policy pol true act
```

6. Bind the AppFlow policy to a global bind point.

```
bind appflow global <policyname> <priority> -type <type>
```

Example:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

The value of **type** must be ICA_REQ_OVERRIDE or ICA_REQ_DEFAULT to apply to ICA® traffic.

7. Set the value of the flowRecordInterval parameter for AppFlow to 60 seconds.

```
set appflow param -flowRecordInterval 60
```

8. Save the configuration.

```
save ns config
```

Enable data collection for NetScaler Gateway appliances deployed in double-hop mode

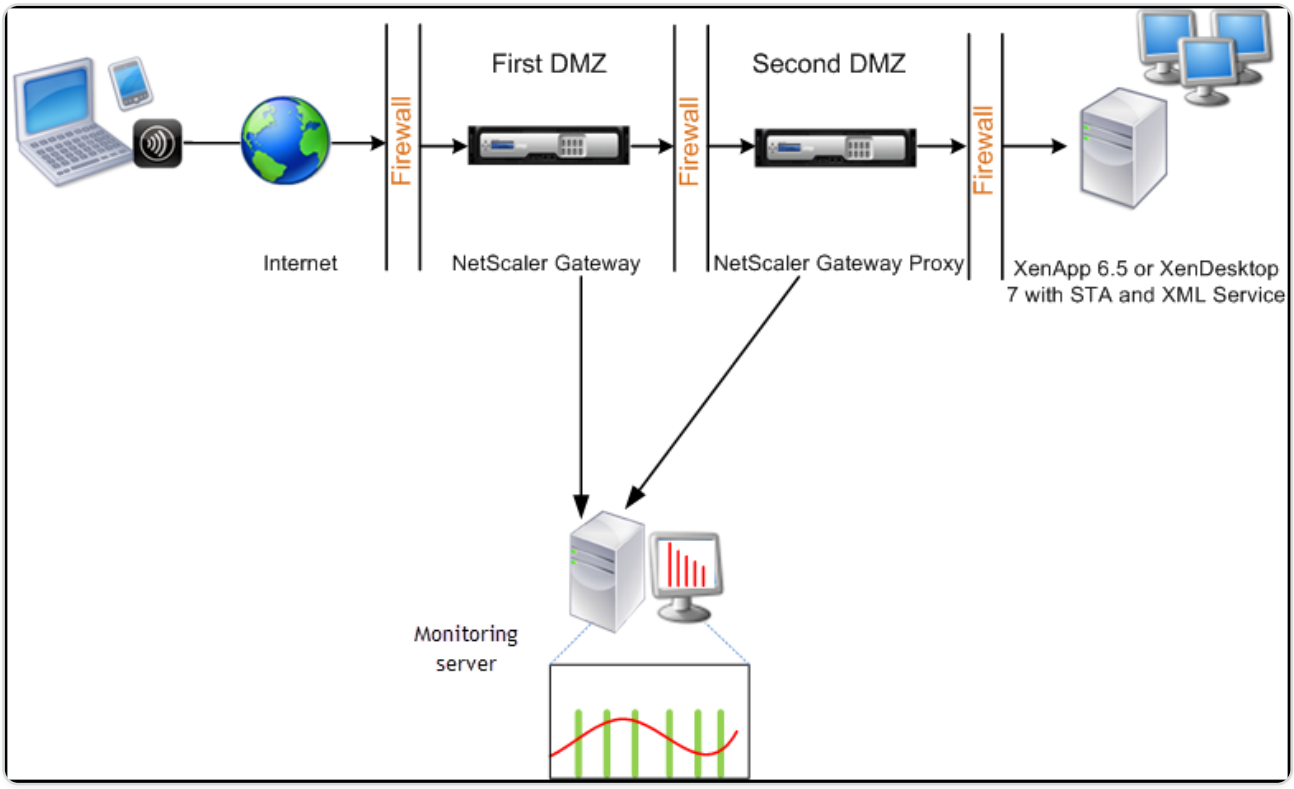
The NetScaler Gateway double-hop mode provides extra protection to an organization internal network because an attacker would need to penetrate multiple security zones or Demilitarized zones (DMZ) to reach the servers in the secure network.

As an administrator, using NetScaler Console, you can analyze:

- The number of hops (NetScaler Gateway appliances) through which the ICA connections pass
- The details about the latency on each TCP connection and how it fairs against the total ICA® latency perceived by the client

The following image indicates that the NetScaler Console and NetScaler Gateway in the first DMZ are deployed in the same subnet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The NetScaler Gateway in the first DMZ handles user connections and performs the security functions of an SSL VPN. This NetScaler Gateway encrypts user connections, determines how the users are authenticated, and controls access to the servers in the internal network.

The NetScaler Gateway in the second DMZ serves as a NetScaler Gateway proxy device. This NetScaler Gateway enables the ICA traffic to traverse the second DMZ to complete user connections to the server farm.

The NetScaler Console can be deployed either in the subnet belonging to the NetScaler Gateway appliance in the first DMZ or the subnet belonging to the NetScaler Gateway appliance second DMZ.

In a double-hop mode, NetScaler Console collects TCP records from one appliance and ICA records from the other appliance. After you add the NetScaler Gateway appliances to the NetScaler Console inventory and enable data collection, each appliance export the reports by keeping track of the hop count and connection chain ID.

For NetScaler Console to identify which appliance is exporting records, each appliance is specified with a hop count and each connection is specified with a connection chain ID. Hop count represents the number of NetScaler Gateway appliances through which the traffic flows from a client to the servers. The connection chain ID represents the end- to end connections between the client and server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console uses the hop count and connection chain ID to co-relate the data from both the NetScaler Gateway appliances and generates the reports.

To monitor NetScaler Gateway appliances deployed in this mode, you must first add the NetScaler Gateway to NetScaler Console inventory, enable AppFlow on NetScaler Console, and then view the reports on the NetScaler Console dashboard.

Enabling data collection on NetScaler Console

If you enable NetScaler Console to start collecting the ICA details from both the appliances, the details collected are redundant. To overcome this situation, you must enable AppFlow for TCP on the first NetScaler Gateway appliance, and then enable AppFlow for ICA on the second appliance. By doing so, one of the appliances exports ICA AppFlow records and the other appliance exports TCP AppFlow records. This also saves the processing time on parsing the ICA traffic.

To enable the AppFlow feature from NetScaler Console:

1. Navigate to **Infrastructure** > **Instances**, and select the NetScaler instance you want to enable analytics.
2. From the **Select Action** list, select **Configure Analytics**.
3. Select the virtual servers, and click **Enable Security & Analytics**.
4. Select Web **Insight**
5. Click **OK**.

Configure NetScaler Gateway appliances to export data

After you install the NetScaler Gateway appliances, you must configure the following settings on the NetScaler gateway appliances to export the reports to NetScaler Console:

- Configure virtual servers of the NetScaler Gateway appliances in the first and second DMZ to communicate with each other.
- Bind the NetScaler Gateway virtual server in the second DMZ to the NetScaler Gateway virtual server in the first DMZ.
- Enable double hop on the NetScaler Gateway in the second DMZ.
- Disable authentication on the NetScaler Gateway virtual server in the second DMZ.
- Enable one of the NetScaler Gateway appliances to export ICA records
- Enable the other NetScaler Gateway appliance to export TCP records:
- Enable connection chaining on both the NetScaler Gateway appliances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure NetScaler Gateway using the command line interface:

1. Configure the NetScaler Gateway virtual server in the first DMZ to communicate with the NetScaler Gateway virtual server in the second DMZ.

   add vpn nextHopServer \<name\> \<nextHopIP\> \<nextHopPort\> \[**-secure** (ON|OFF)\] \[**-imgGifToPng**\] ...

   ```
   add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON
   ```

2. Bind the NetScaler Gateway virtual server in the second DMZ to the NetScaler Gateway virtual server in the first DMZ. Run the following command on the NetScaler Gateway in the first DMZ:

   bind vpn vserver \<name\> **-nextHopServer** \<name\>

   ```
   bind vpn vserver vs1 -nextHopServer nh1
   ```

3. Enable double hop and AppFlow on the NetScaler Gateway in the second DMZ.

   set vpn vserver \<name\> \[**- doubleHop** (ENABLED |DISABLED)\] \[**- appflowLog** (ENABLED |DISABLED)\]

   ```
   set vpn vserver vpnhop2 –doubleHop ENABLED –appFlowLog ENABLED
   ```

4. Disable authentication on the NetScaler Gateway virtual server in the second DMZ.

   set vpn vserver\<name\> \[**-authentication** (ON|OFF)\]

   ```
   set vpn vserver vs -authentication OFF
   ```

5. Enable one of the NetScaler Gateway appliances to export TCP records.

   bind vpn vserver\<name\> \[**-policy**\<string\> **-priority**\<positive_integer\>\] \ [**-type**\<type\>\]

   ```
   bind vpn vserver vpn1 -policy appflowpol1 -priority 101 –type
   OTHERTCP\_REQUEST
   ```

6. Enable the other NetScaler Gateway appliance to export ICA records:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

bind vpn vserver\<name\> \[**-policy**\<string\> **-priority**\<positive_integer\>\] \
[**-type**\<type\>\]

```
bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
ICA\_REQUEST
```

7. Enable connection chaining on both the NetScaler Gateway appliances:

   set appFlow param \[**-connectionChaining** (ENABLED|DISABLED)\]

```
set appflow param -connectionChaining ENABLED
```

Configuring NetScaler Gateway using configuration utility:

1. Configure the NetScaler Gateway in the first DMZ to communicate with the NetScaler Gateway in the second DMZ and bind the NetScaler Gateway in the second DMZ to the NetScaler Gateway in the first DMZ.
   a. On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.
   b. In the right pane, double-click the virtual server, and in the Advanced group, expand **Published Applications**.
   c. Click **Next Hop Server** and bind a next hop server to the second NetScaler Gateway appliance.
2. Enable double hop on the NetScaler Gateway in the second DMZ.
   a. On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.
   b. In the right pane, double-click the virtual server, and in the **Basic Settings** group, click the edit icon.
   c. Expand **More** , select **Double Hop** and click **OK**.
3. Disable authentication on the virtual server on the NetScaler Gateway in the second DMZ.
   a. On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.
   b. In the right pane, double-click the virtual server, and in the **Basic Settings** group, click the edit icon.
   c. Expand **More**, and clear **Enable Authentication**.
4. Enable one of the NetScaler Gateway appliances to export TCP records.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.
b. In the right pane, double-click the virtual server, and in the Advanced group, expand Policies.
c. Click the + icon and from the **Choose Policy** list, select **AppFlow®** and from the **Choose Type** list, select **Other TCP Request**.
d. Click **Continue**.
e. Add a policy binding, and click **Close**.

5. Enable the other NetScaler Gateway appliance to export ICA records:

a. On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.
b. In the right pane, double-click the virtual server, and in the **Advanced** group, expand **Policies**.
c. Click the + icon and from the **Choose Policy** list, select **AppFlow** and from the **Choose Type** list, select **Other TCP Request**.
d. Click **Continue**.
e. Add a policy binding, and click **Close**.

6. Enable connection chaining on both the NetScaler Gateway appliances.

a. On the **Configuration** tab, navigate to **System** > **Appflow**.
b. In the right Pane, in the **Settings** group, click **Change Appflow Settings**.
c. Select **Connection Chaining** and Click **OK**.

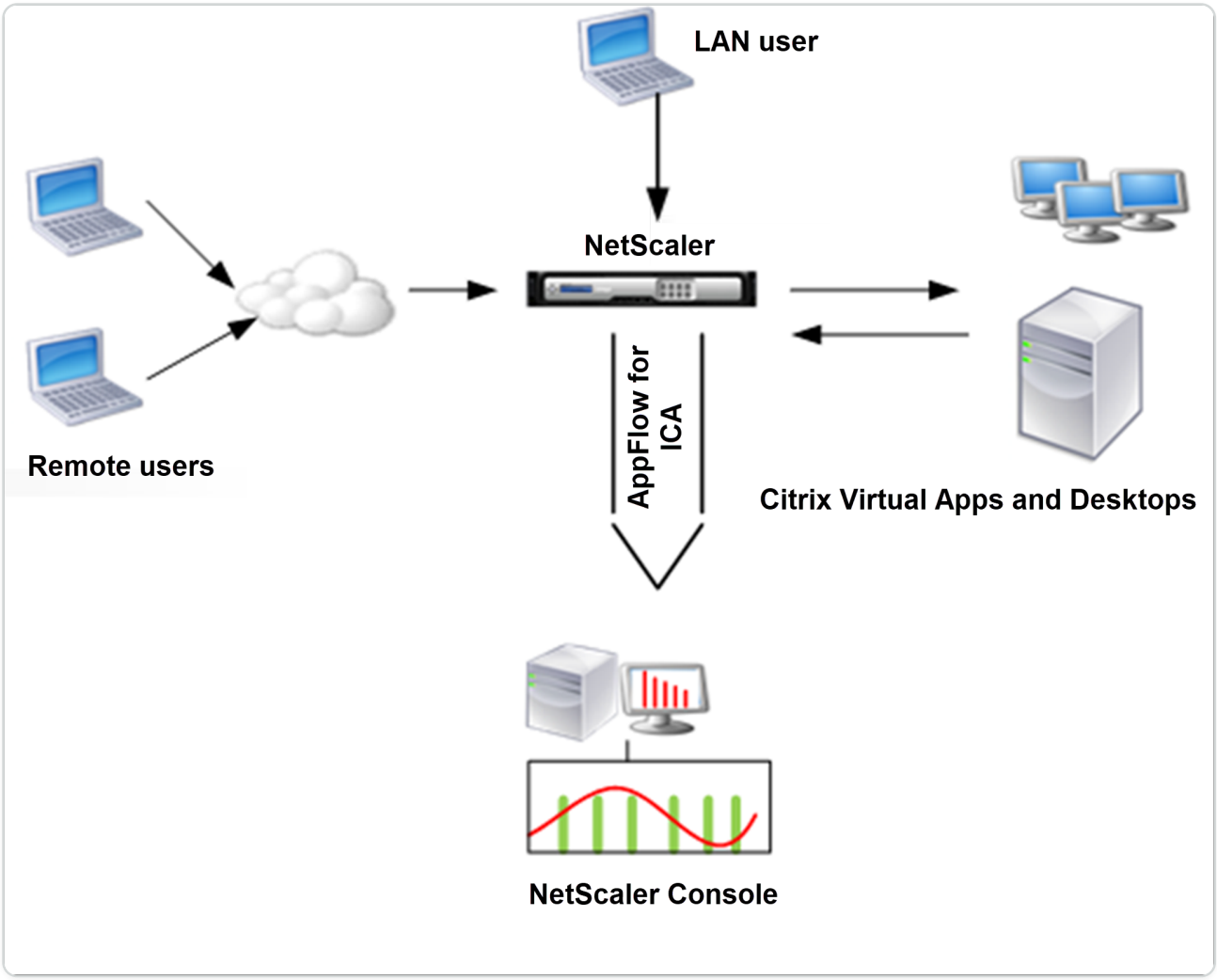
Enable data collection to monitor NetScalers deployed in LAN user mode

External users who access Citrix Virtual App or Desktop applications must authenticate themselves on the NetScaler Gateway. Internal users, however, might not require to be redirected to the NetScaler Gateway. Also, in a transparent mode deployment, the administrator must manually apply the routing policies, so that the requests are redirected to the NetScaler appliance.

To overcome these challenges, and for LAN users to directly connect to Citrix Virtual Apps and Desktops applications, you can deploy the NetScaler appliance in a LAN user mode by configuring a cache redirection virtual server. The cache redirection virtual server acts as a SOCKS proxy on the NetScaler Gateway appliance.

The following image illustrates NetScaler Console deployed in **LAN User Mode**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE

NetScaler Gateway appliance must be able to reach the agent.

To monitor NetScaler appliances deployed in this mode, first add the NetScaler appliance to the NetScaler Insight inventory, enable AppFlow, and then view the reports on the dashboard.

After you add the NetScaler appliance to the NetScaler Console inventory, you must enable AppFlow for data collection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

- You cannot enable data collection on a NetScaler deployed in LAN User mode by using the NetScaler Console configuration utility.
- For detailed information about the commands and their usage, see Command Reference.
- For information on policy expressions, see Policies and Expressions.

To configure data collection on a NetScaler appliance by using the command line interface:

At the command prompt, do the following:

1. Log on to NetScaler appliance.
2. Add a forward proxy cache redirection virtual server with the proxy IP and port, and specify the service type as HDX.

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-cacheType
<cachetype>] [ - cltTimeout <secs>]
```

Example:

```
add cr vserver cr1 HDX 10.12.2.2 443 –cacheType FORWARD –cltTimeout 180
```

NOTE

If you are accessing the LAN network by using a NetScaler Gateway appliance, add an action to apply a policy that matches the VPN traffic.

```
add vpn trafficAction** \<name\> \<qual\> \[-HDX ( ON | OFF )\]



add vpn trafficPolicy** \<name\> \<rule\> \<action\>
```

Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add vpn trafficAction act1 tcp -HDX ON



add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
```

3. Add NetScaler Console as an AppFlow collector on the NetScaler appliance.

```
add appflow collector** \<name\> **-IPAddress** \<ip\_addr\>
```

Example:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

4. Create an AppFlow® action and associate the collector with the action.

```
add appflow action** \<name\> **-collectors** \<string\> ...
```

Example:

```
add appflow action act -collectors MyInsight
```

5. Create an AppFlow policy to specify the rule for generating the traffic.

```
add appflow policy** \<policyname\> \<rule\> \<action\>
```

Example:

```
add appflow policy pol true act
```

6. Bind the AppFlow policy to a global bind point.

```
bind appflow global** \<policyname\> \<priority\> **-type** \<type\>
```

Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

NOTE

The value of type must be ICA_REQ_OVERRIDE or ICA_REQ_DEFAULT to apply to ICA® traffic.

7. Set the value of the flowRecordInterval parameter for AppFlow to 60 seconds.

```
set appflow param -flowRecordInterval 60
```

Example:

```
set appflow param -flowRecordInterval 60
```

8. Save the configuration.

```
save ns config
```

Create thresholds and configure alerts for HDX™ Insight

HDX Insight on NetScaler Console allows you to monitor the HDX traffic passing through the NetScaler instances. NetScaler Console allows you to set thresholds on various counters used to monitor the Insight traffic. You can also configure rules and create alerts in NetScaler Console.

HDX traffic type is associated with various entities such as applications, desktops, gateways, licenses, and users. Every entity can contain different metrics associated with them. For example, application entity is associated with several hits, bandwidth consumed by the application, and response time of the server. A user entity can be associated with WAN latency, DC latency, ICA® RTT, and bandwidth consumed by a user.

The threshold management for HDX Insight in NetScaler Console allowed you to proactively create rules and configure alerts whenever the thresholds set are breached. Now, this threshold management is extended to configure a group of threshold rules. You can now monitor the group instead of individual rules. A threshold rule group comprises one or more user-defined threshold rules for metrics chosen from entities such as users, applications, and desktops. Each rule is

© 1997–2026 Citrix Systems, Inc. All rights reserved.

monitored against an expected value that you enter when you create the rule. In users entity, the threshold group can be associated with a geolocation as well.

An alert is generated on NetScaler Console only if all the rules in the configured threshold group are breached. For example, you can monitor an application on total session launch count and also on application launch count as one threshold group. An alert is generated only if both rules are breached. This allows you to set more realistic thresholds on an entity.

A few examples are listed as follows:

- Threshold rule1: ICA RTT(metric) for users(entity) must be \<= 100 ms
- Threshold rule2: WAN Latency (metric) for users(entity) must be \<= 100 ms

An example of threshold group can be: {Threshold rule 1 + Threshold rule 2}

To create a rule, you must first select the entity that you want to monitor. Then choose a metric while creating a rule. For example, you can select applications entity and then select **Total Session Launch count or App Launch Count**. You can create one rule for every combination of an entity and a metric. Use the comparators provided (\>, \<, \>=, and \<=) and type a threshold value for each metric.

NOTE

If you do not want to monitor multiple entities in a single group, you must create a separate threshold rule group for each entity.

When the value of a counter exceeds the value of a threshold, NetScaler Console generates an event to signify a threshold breach, and an alert is created for every event.

You must configure how you receive the alert. You can enable the alert to be displayed on NetScaler Console or receive the alert as an email or both, or as an SMS on your mobile device. For the last two actions, you must configure the email server or the SMS server on NetScaler Console.

Threshold groups can also be bound to Geolocations for geo-specific monitoring for user entity.

Example Use Cases

ABC Inc. is a global firm and has offices in over 50 countries. The firm has two data centers, one in Singapore and other in California that host the Citrix Virtual Apps and Desktops. Employees of the firm access the Citrix Virtual Apps and Desktops throughout the globe using the NetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gateway and GSLB based redirection. Eric, the Citrix Virtual Apps and Desktops admin for ABC Inc. wants to track the user experience for all their offices to optimize the apps and desktop delivery for anywhere, anytime access. Eric also wants to check the user-experience-metrics like ICA RTTs, latencies, and raise any deviations proactively.

The users of ABC Inc. have a distributed presence. Some users are located close to the data center, while a few are located at further away from the data center. As the user base is distributed widely, the metrics and the corresponding thresholds also vary among these locations. For example, the ICA RTT for a location near to the data center can be 5–10 ms whereas the same for a remote location can be around 100 ms.

With threshold rule group management for HDX Insight, Eric can set geo-specific threshold rule groups for each location and be alerted through email or SMS for breaches per area. Eric is also able to combine tracking of more than one metric within a threshold rule group and narrow down the root cause to capacity issues if any. Eric is now able to proactively track any deviation without having to worry about the complexity of manually looking through all Citrix Virtual Apps and Desktops for HDX Insight portfolio metrics.

Create a threshold rule group and configure alerts for HDX Insight using NetScaler Console

1. In NetScaler Console, navigate to **Settings> Analytics Settings > Thresholds**. On **Thresholds** page that opens, click **Add**.
2. On the **Create Thresholds and Alerts** page, specify the following details:

    a. **Name**. Type in a name for creating an event for which NetScaler Console generates an alert.

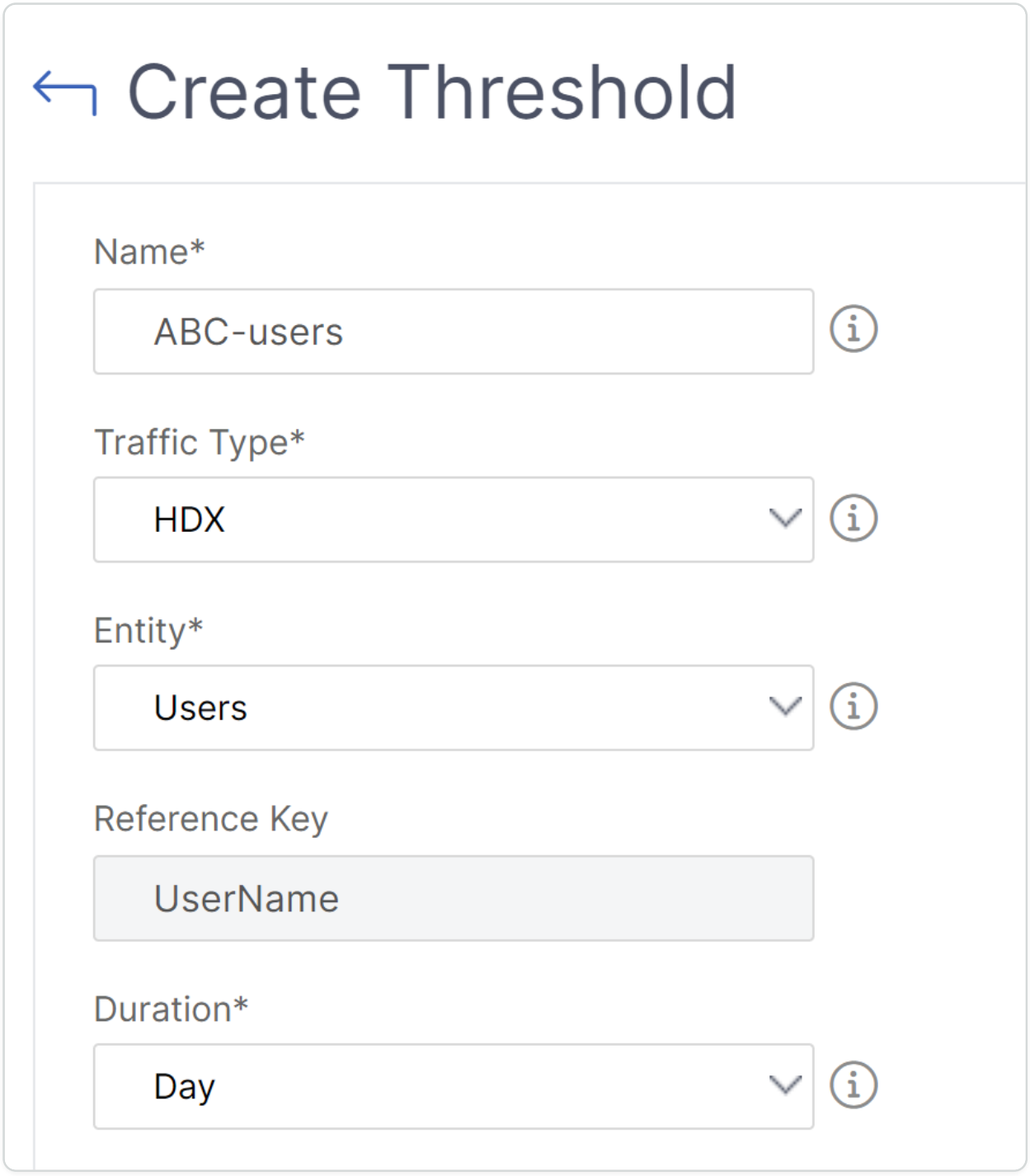
    b. **Traffic Type**. From the list, select **HDX**.

    c. **Entity**. From the list, select the category or the resource type. The entities differ for each traffic type that you have selected earlier.

    d. **Reference Key**. A reference key is automatically generated based on the traffic type and entity that you have selected.

    e. **Duration**. From the list, select the time interval for which you want to monitor the entity. You can monitor the entities for an hour, or for a day, or for a week's duration.

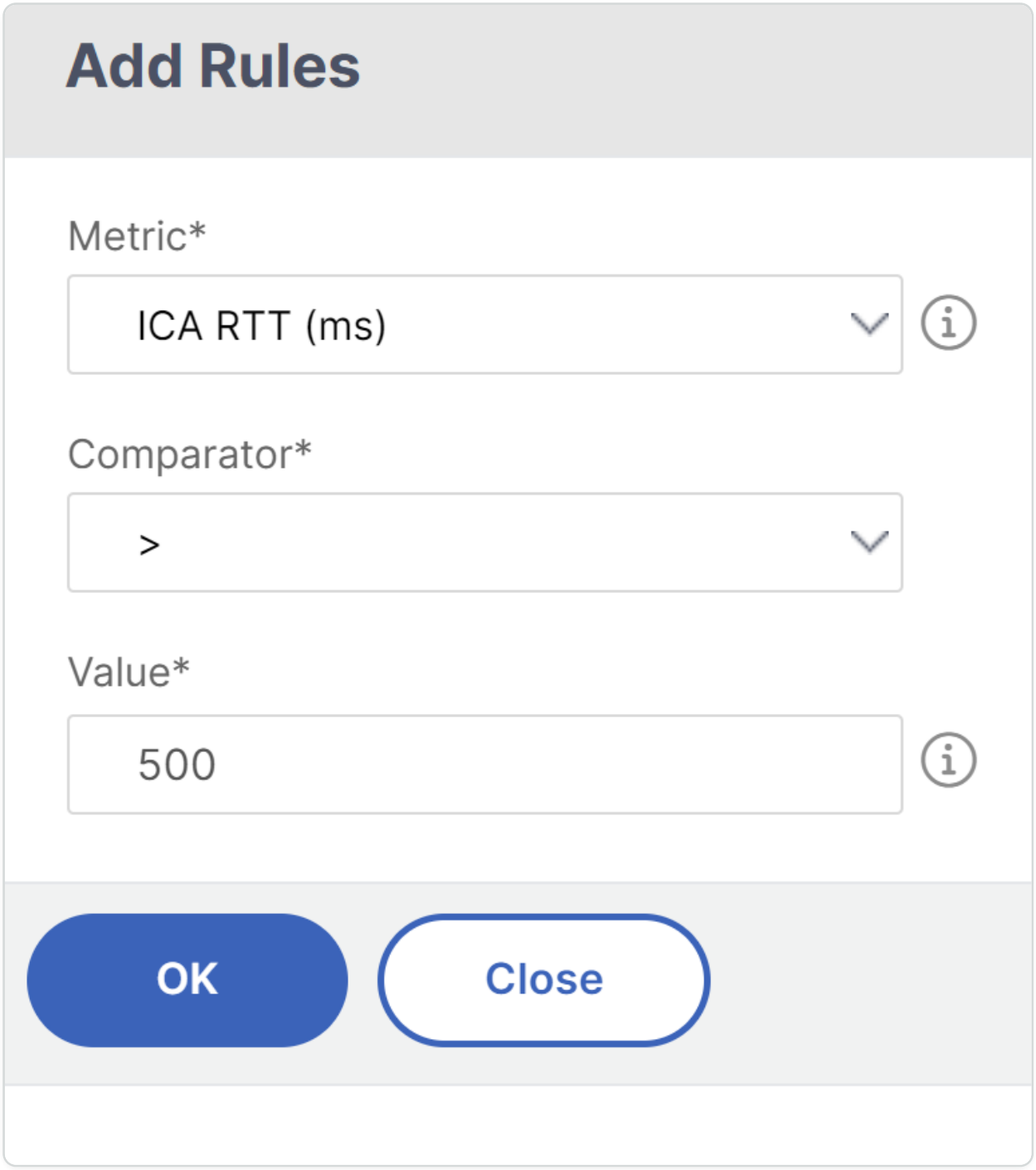
© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. **Creating threshold rules group for all entities:**

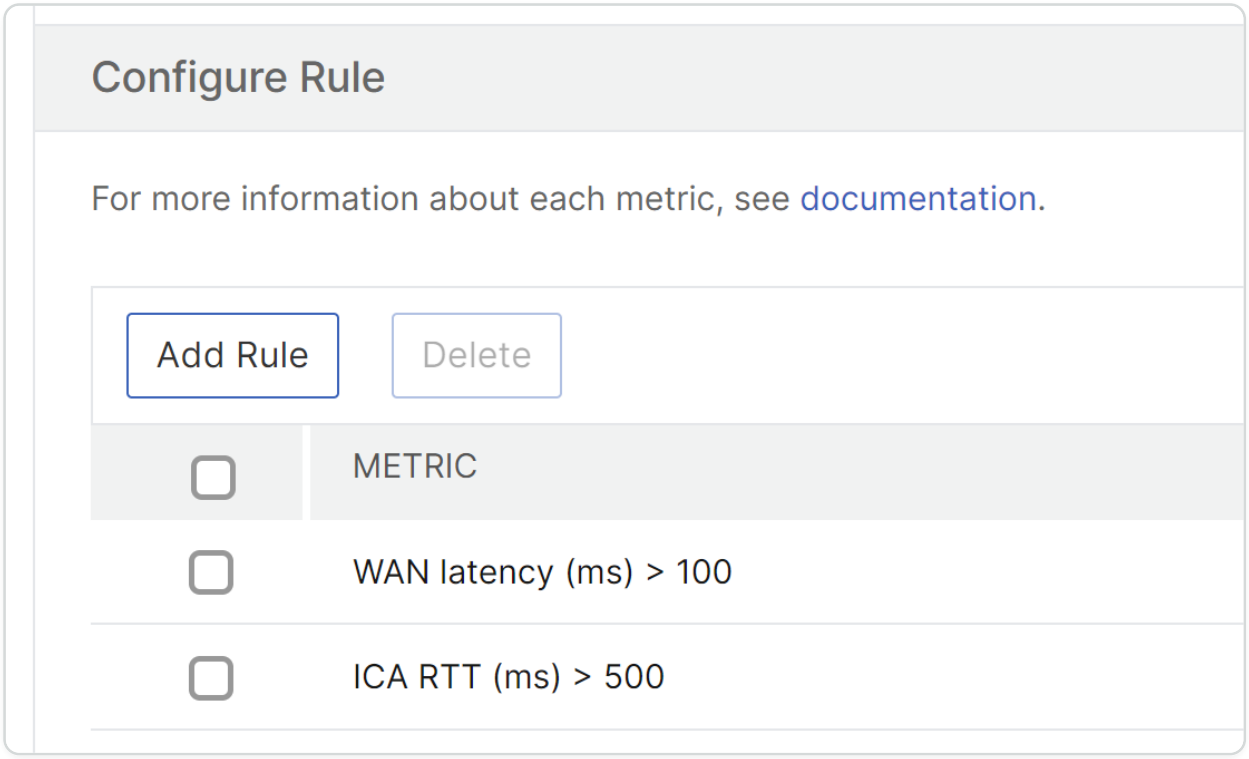
   For HDX traffic, you must create a rule by clicking **Add Rule**. Enter the values in the **Add Rules** pop-up window that opens.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



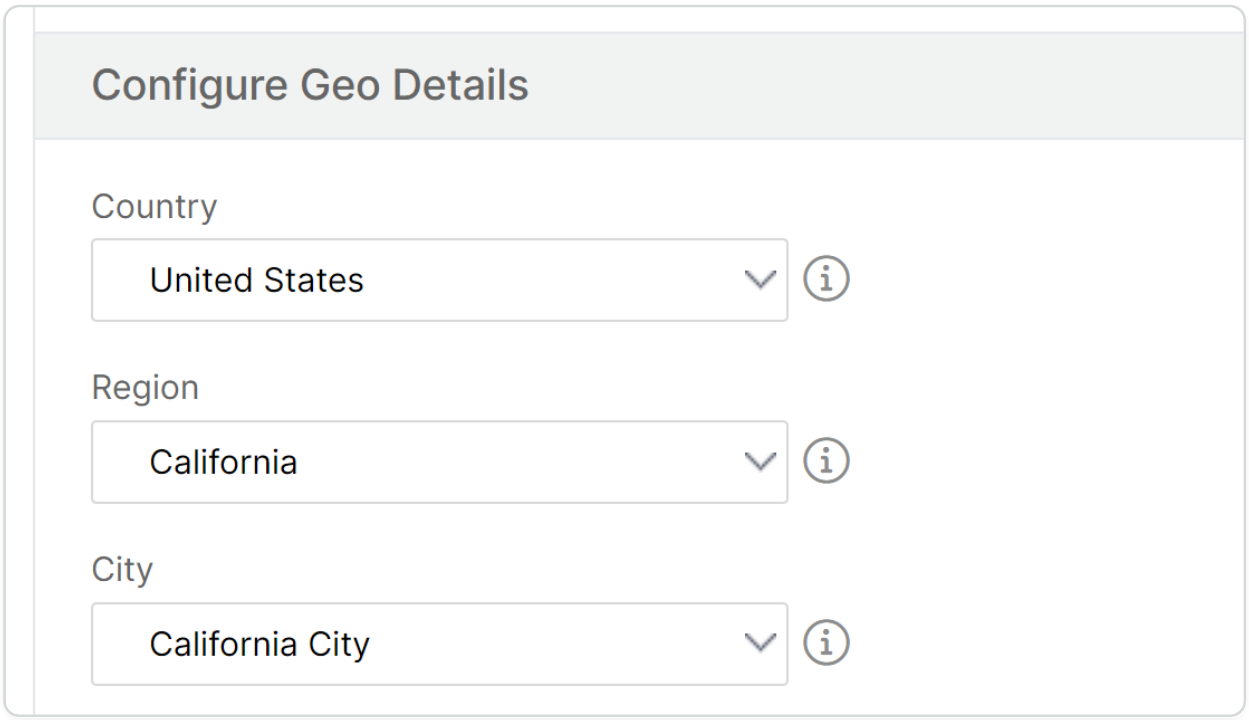
You can create multiple rules to monitor each entity. Creating multiple rules in one single group allows you to monitor the entities as a group of threshold rules instead of individual rules. Click **OK** to close the window.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. **Configuring Geolocation tagging for Users entity:**

   Optionally, you can create a location-based alert for the user entity in the **Configure Geo Details** section. The following image shows an example of creating a geolocation based tagging to monitor WAN latency performance for users on the west coast of the United States.



5. Click **Enable Thresholds** to allow NetScaler Console to start monitoring the entities.
6. Optionally, configure actions such as email and Slack notifications.
7. Click **Create** to create a threshold rule group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

View HDX™ Insight reports and metrics

HDX insight provides complete visibility of the reports and metrics pertaining to HDX traffic on your NetScaler instances.

You can view the HDX metrics for any selected entity. The views include the following categories of entities:

- **Users**: Displays the reports for all the users accessing the Citrix Virtual Apps and Desktops within the selected time interval.
- **Applications:** Displays the reports for total number of applications, and all related relevant information like the total number of times the applications were launched within the specified time interval.
- **Instances**: Displays the reports on the NetScaler instances that act as gateways for incoming traffic.
- **Gateway Virtual Servers**: Displays the reports for all virtual servers.
- **Desktops**: Displays the reports for the desktops used in the selected time frame.
- **Licenses**: Displays the reports for total SSL VPN licenses used within the specified time slot.

NOTE:

Starting from **14.1-51.x** or later release, you can monitor key metrics such as active sessions, desktops, and launched applications at the VPN virtual server level. You can view a list of all virtual servers under **Gateway > HDX Insight > Gateway Virtual Servers**.

This document includes the following:

- User View Reports and Metrics
- Application View Reports and Metrics
- Desktop View Reports and Metrics
- Instance View Reports and Metrics
- License View Reports and Metrics

Application View Reports and Metrics

The reports and metrics in this view are focused on the Citrix Virtual Apps. Navigate to **Gateway** > **HDX Insight** > **Applications**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

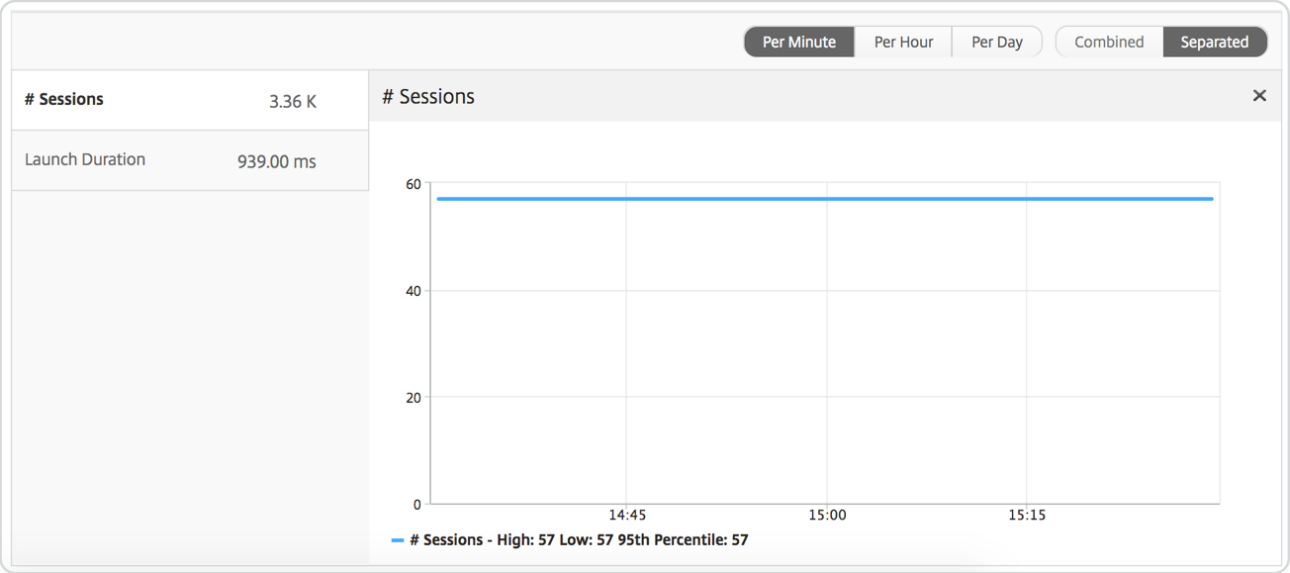
Summary View

The summary view displays the reports for all the applications that are logged in during the selected timeline.

All the metrics/reports, unless explicitly mentioned will have the values corresponding to them for the select time period.

LINE CHART

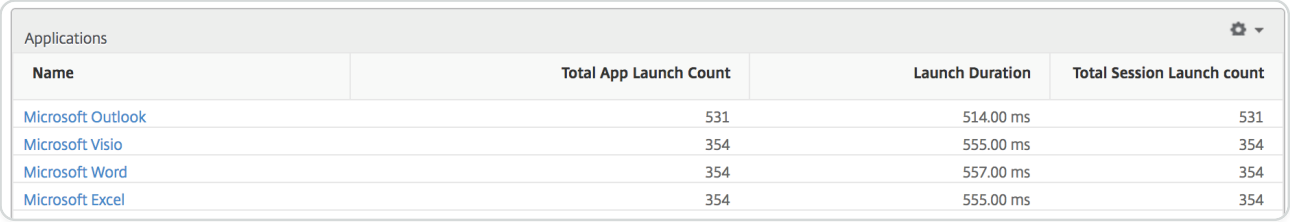
METRICS	DESCRIPTION
Sessions	Total number of sessions during a given time interval.
Launch duration	Average time taken to launch an application.



APPLICATIONS SUMMARY REPORT

METRICS	DESCRIPTION
Name	Name of the Citrix Virtual App.
Total Session Launch count	Total number of active Citrix Virtual App sessions during the given time interval.
Total App Launch Count	Total number of Citrix Virtual App applications launched during the given time interval.
Launch Duration	Average time taken to launch the Citrix Virtual App.

© 1997–2026 Citrix Systems, Inc. All rights reserved.


Applications

Name	Total App Launch Count	Launch Duration	Total Session Launch count
Microsoft Outlook	531	514.00 ms	531
Microsoft Visio	354	555.00 ms	354
Microsoft Word	354	557.00 ms	354
Microsoft Excel	354	555.00 ms	354

ACTIVE APPLICATION REPORT

METRICS	DESCRIPTION
Name	Name of the Citrix Virtual App.
State	Displays the state of the application: Green-Active, Red-Inactive
#Active Sessions	Number of active user sessions using this app during a given time interval.
#Active Apps	Number of active sessions for this application.


Active Applications

Name	State	# Active Sessions	# Active Apps
Communicator		60	60
Fidelity		60	60
GoToMeeting		60	60

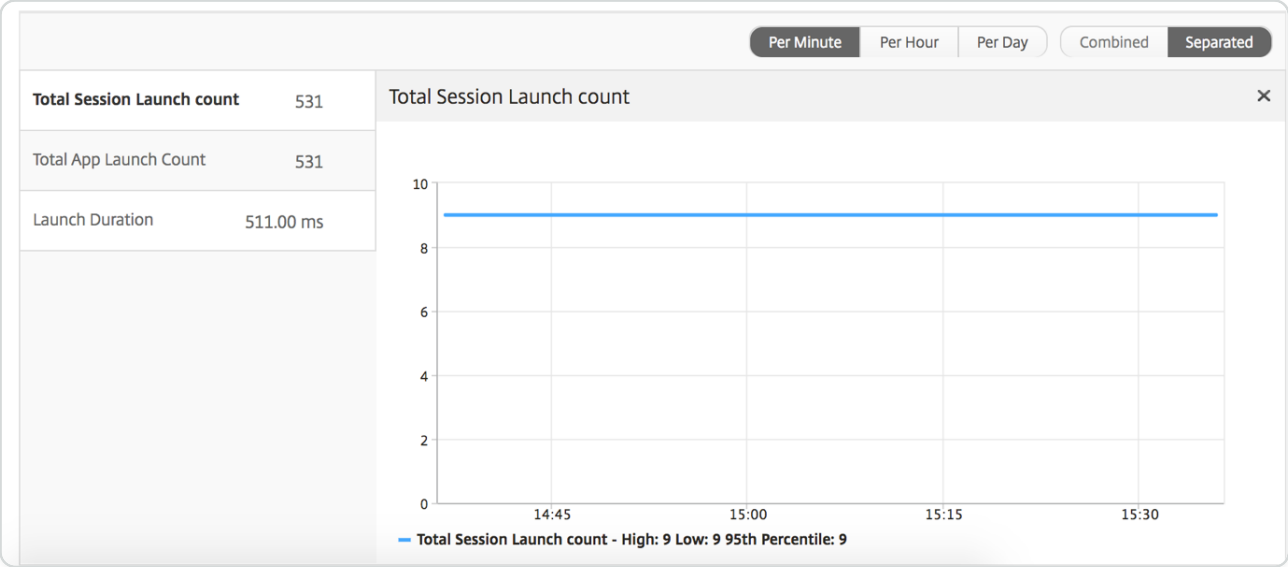
THRESHOLD REPORT

The Threshold Report represents the count of thresholds breached where the *entity* is selected as Application in the selected period.

LINE CHART

METRICS	DESCRIPTION
Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
Launch duration	Average time taken to launch an application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



CURRENT SESSIONS REPORT

METRICS	DESCRIPTION
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScalers caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.
Server IP Address	Backend/ Citrix Virtual App server IP.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

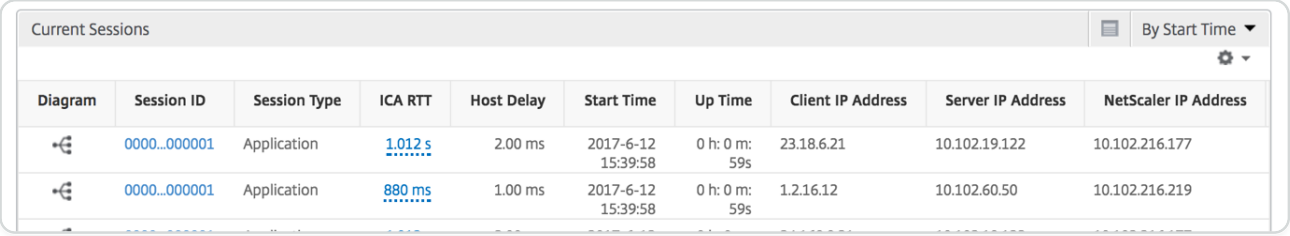
METRICS	DESCRIPTION
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Citrix Workspace type- Citrix Windows Client.
Client Version	Citrix Workspace version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.
Country	Country from which the session was established.
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back-end servers.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back-end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back-end server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
User Name	The user name of the user accessing this particular Citrix Virtual App.
Session ID	Unique identifier for the Citrix Virtual App session.
Session Type	Will be "Application".
State	Session state: Green for active, Red for in-active.
Maximum Breach Latency	The highest value of the L7 latency when a breach of a defined threshold for a set time interval occurs.
Average Breach Latency	The average value of L7 latency when the system is in a "L7 latency breached" state.
L7 Threshold Breach Count	The number of times a L7 threshold breach has occurred.
L7 Client-side Latency	The average L7 latency observed between the ICA client and the NetScaler instance. This metric is useful in non-Citrix devices being present in the delivery path.
L7 Server-side Latency	The average L7 latency observed between the NetScaler device and the Citrix Virtual App. This metric is useful in non-Citrix devices being present in the delivery path.



PER APPLICATION SESSION VIEW

The per application session view displays reports for a particular selected application session.

To view the Session reports:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

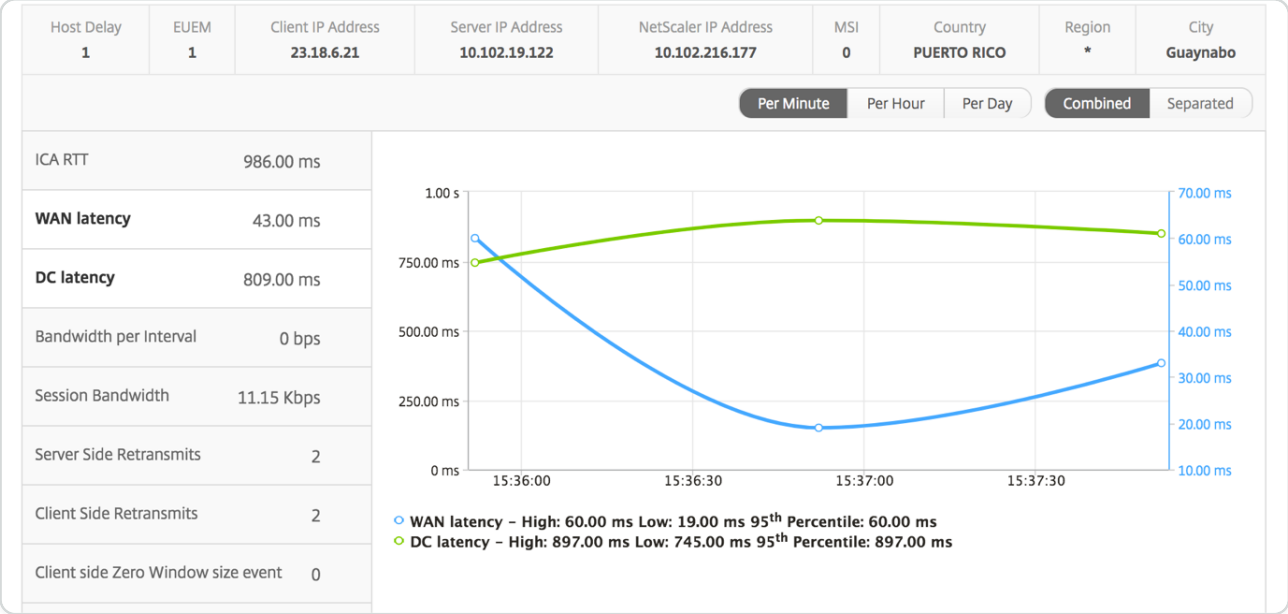
1. Navigate to **Gateway** > **HDX™ Insight** > **Applications**.
2. Select a particular user from the **Application Summary Report**.
3. Selected a session from current sessions report.

LINE CHART

METRICS	DESCRIPTION
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
Server side Zero Window size event	Latency caused by the server side of the network. That is, from NetScaler to back-end servers.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back-end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.

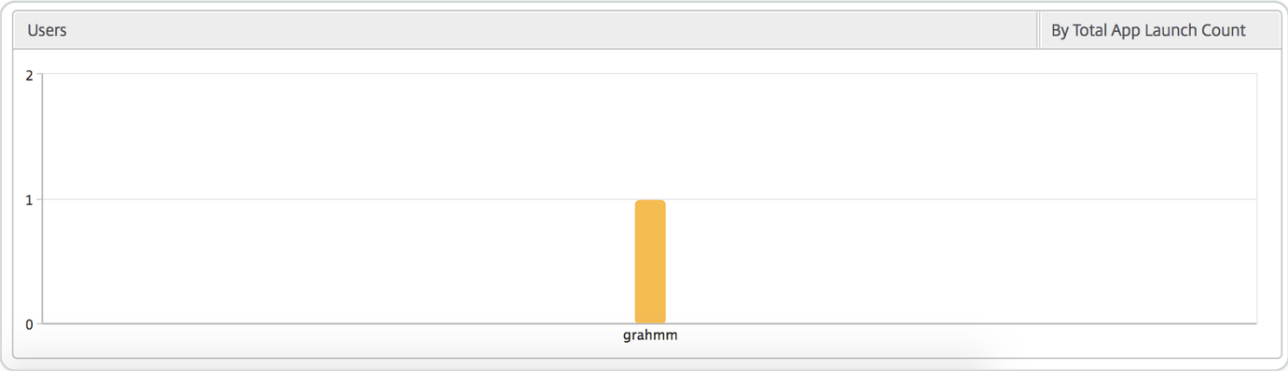
© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back-end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.



USER BAR GRAPH

The **User** bar graph represents the users logged into this particular app.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Desktop View Reports and Metrics

The reports and metrics in this view are focused on the Citrix Virtual Desktop. Navigate to **Gateway** > **HDX™ Insight** > **Desktop**

Summary View

The summary view displays the reports for all the Citrix Virtual Desktops™ that are logged in during the selected timeline.

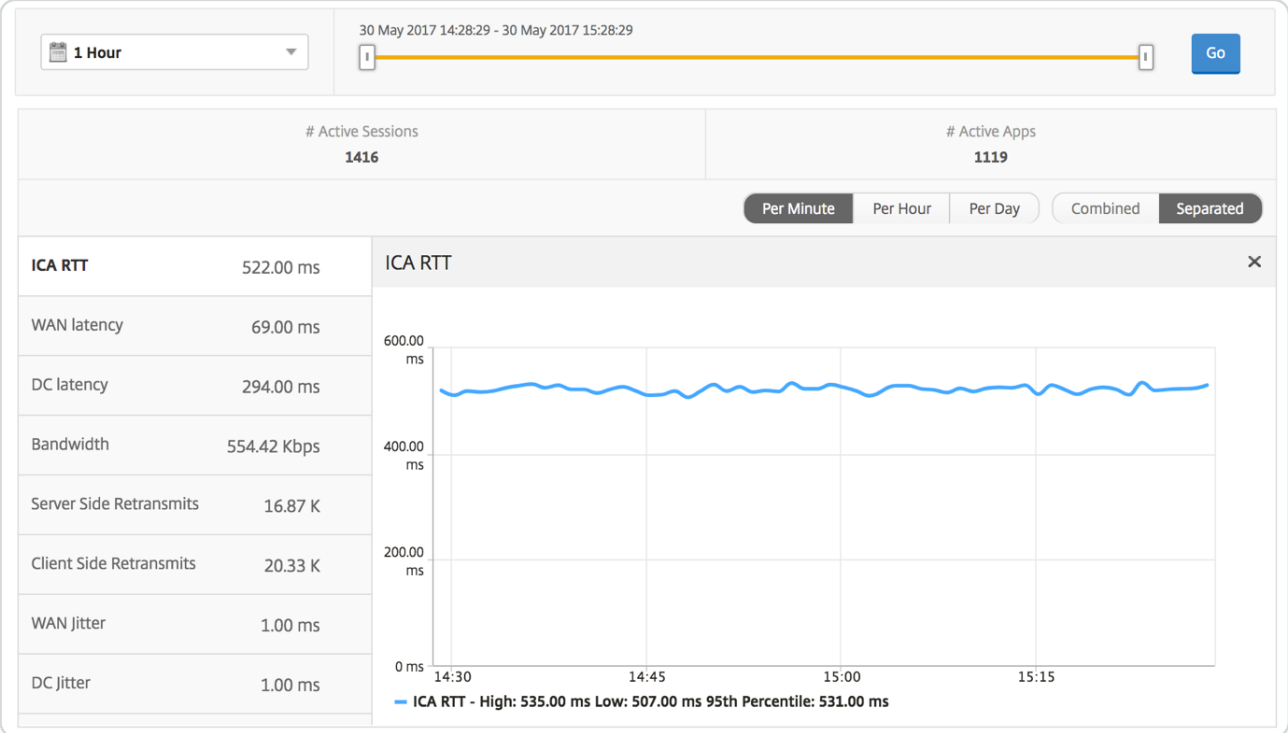
All the below metrics/reports, unless explicitly mentioned will have the values corresponding to them for the select time period.

LINE CHART

METRICS	DESCRIPTION
Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back-end servers.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back-end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end

© 1997–2026 Citrix Systems, Inc. All rights reserved.

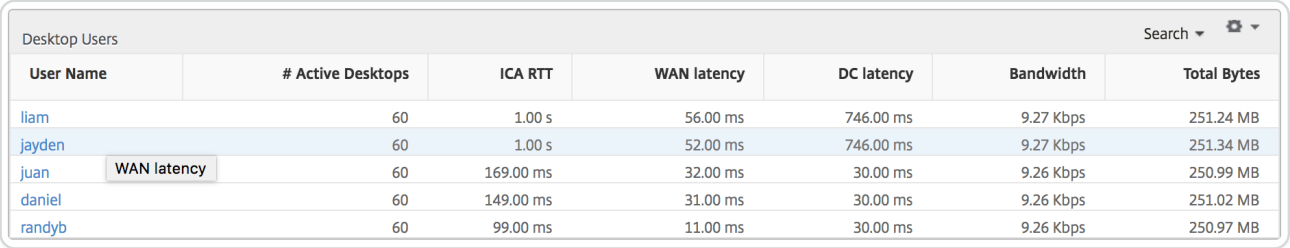
METRICS	DESCRIPTION
	user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back-end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

DESKTOP SUMMARY REPORT

METRICS	DESCRIPTION
Active Sessions	Total number of active Citrix Virtual Desktop sessions during a given time interval.
Active Desktops	Total number of active Citrix Virtual Desktops during a given time interval.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back-end servers.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
Total Bytes	Total Bytes consumed by the user during the selected time period.



THRESHOLD REPORT

The threshold report represents the count of thresholds breached where the *entity* is selected as Desktop in the selected period.

Per Desktop View

Per desktop view provides detailed end user experience reporting for a selected Citrix Virtual Desktop.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To navigate to the particular Desktop view:

1. Navigate to **Gateway > HDX Insight > Desktop**.
2. Select a particular **Desktop** from the **Desktop Summary Report**.

LINE CHART

METRICS	DESCRIPTION
Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back-end servers.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back-end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back-end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.



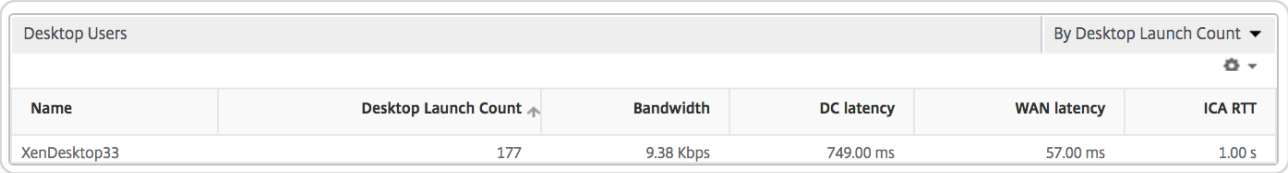
DESKTOP USERS REPORT

This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

METRICS	DESCRIPTION
Name	Name of the Citrix Virtual Desktop.
Desktop Launch Count	Number of times the desktop has launched.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back-end servers.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.



USER DESKTOPS ACTIVE/INACTIVE REPORT

These following metrics can be sorted by Bandwidth per interval, session reconnects, and ACR counts.

METRICS	DESCRIPTION
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScalers caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

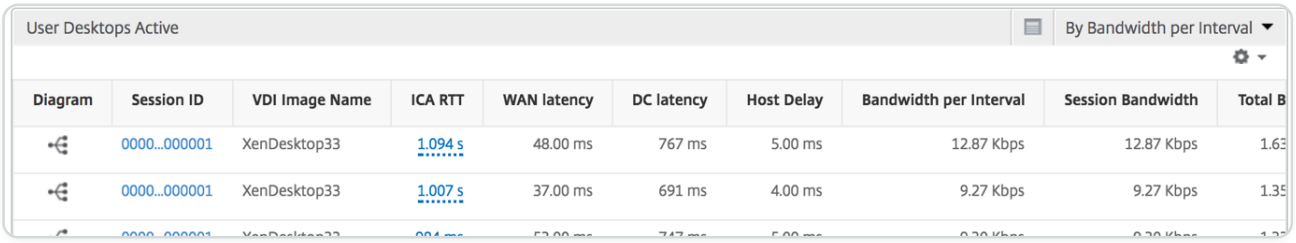
METRICS	DESCRIPTION
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.
Server IP Address	Backend/ Citrix Virtual App server IP.
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Citrix Workspace type- Citrix Windows Client
Client Version	Citrix Workspace version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.
Country	Country from which the session was established.
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back-end servers.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back-end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back-end server.
VDI Image Name	Name of the Citrix Virtual Desktop to which the user is connected
Diagram	



Per Desktop Session View

Per desktop session view provides reporting for a particular selected Citrix Virtual Desktop session.

To navigate to the Desktop session view:

1. Navigate to **Gateway** > **HDX Insight** > **Desktop**.
2. Select a particular desktop from the **Desktop Summary Report**.
3. Select a session from current sessions report.

TIMELINE CHART

The per user session view provides reporting for a particular selected user's session.

To view the metrics for a selected user's session:

1. Navigate to **Gateway** > **HDX Insight** > **Users**.

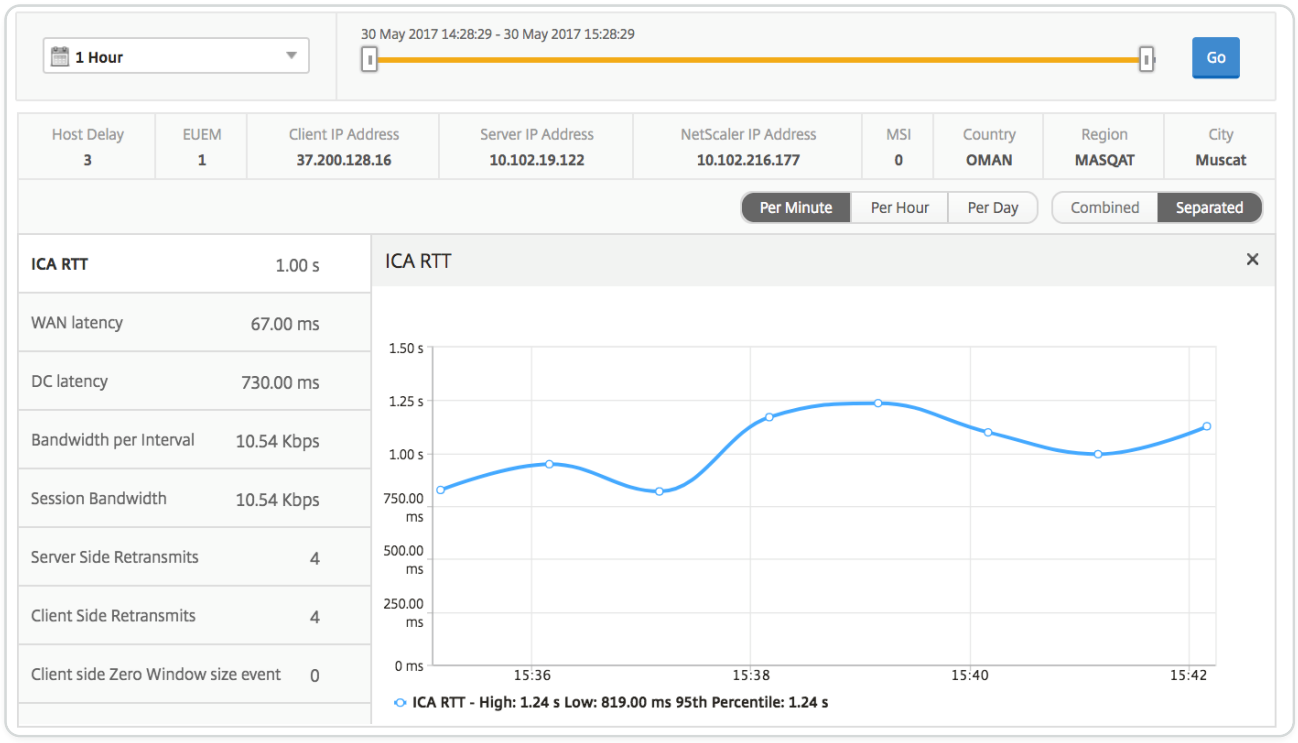
© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Select a particular user from the **User Summary Report** section.
3. Select a session from **Current Sessions** or **Terminated Sessions** column.

METRICS	DESCRIPTION
Session Reconnects	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
ACR Counts	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back-end servers.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back-end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back-end server.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.



RELATED DESKTOP SESSIONS REPORT

These following metrics can be sorted by Bandwidth per interval, session reconnects, and ACR counts.

METRICS	DESCRIPTION
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

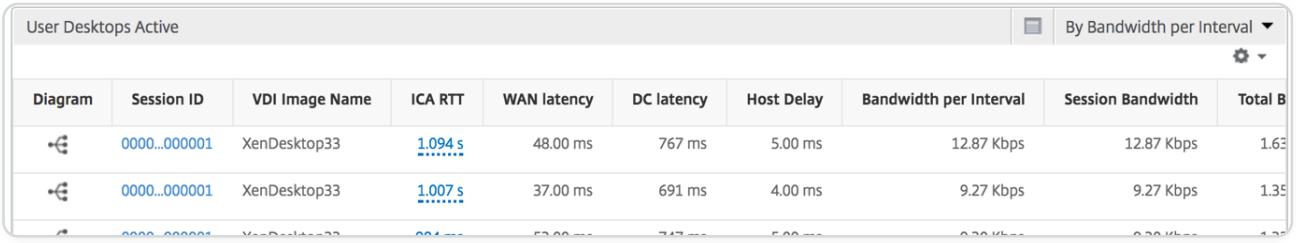
METRICS	DESCRIPTION
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScalers caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.
Server IP Address	Backend/ Citrix Virtual App server IP.
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Workspace type- Citrix Windows Client
Client Version	Citrix Workspace version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Country	Country from which the session was established.
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back-end servers.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back-end server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back-end server.
VDI Image Name	Name of the Citrix Virtual Desktop to which the user is connected

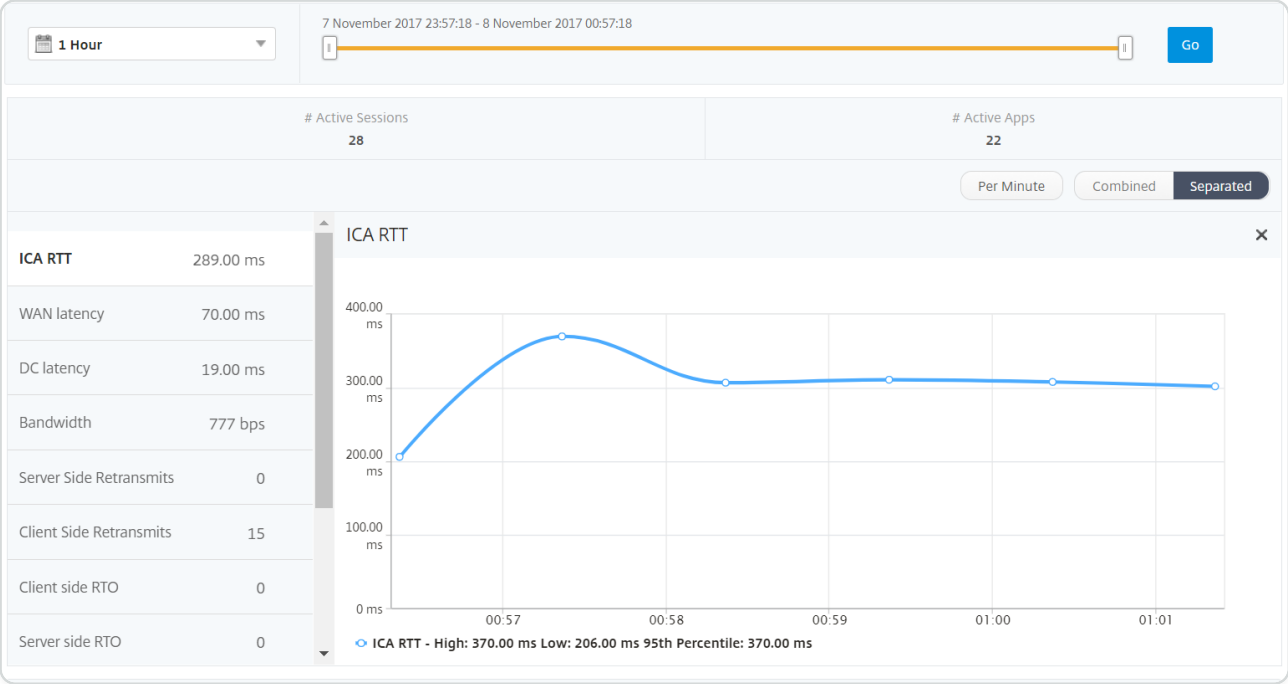


User View Reports and Metrics

The reports and metrics in this view are displayed per Citrix Virtual App or Desktop users.

Navigate to **Gateway** > **HDX™ Insight** > **Users**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Summary view

The summary view displays the reports for all the users that have logged in during the selected timeline. All the metrics/reports in this view display the values corresponding to them for the selected time period unless specified otherwise.

To change the selected time period:

1. Use the time period list or the time slider to set the desired time interval.
2. Click **Go**.

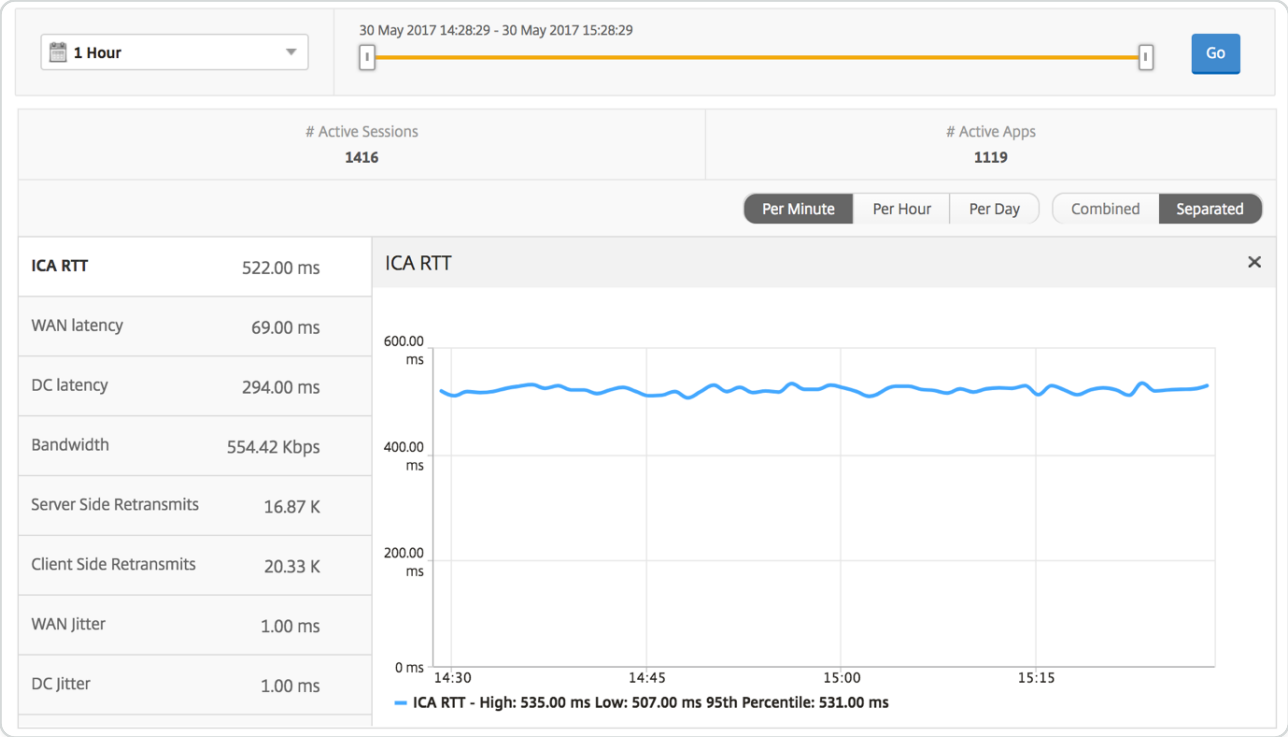
LINE CHART

METRICS	DESCRIPTION
Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back-end servers.
Bandwidth	Total bits per second taken for end to end communication during the selected time interval.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back-end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back-end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



USER SUMMARY REPORT

Following are the metrics that are specific to this report.

METRICS	DESCRIPTION
# Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
# Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back-end servers.
Bandwidth	Total bits per second taken for end to end communication during the selected time interval.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back-end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back-end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Total App Launch Count	Total Apps launched by the user during the selected time period.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Active Desktops	Total number of active Citrix Virtual Desktops during a given time interval.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

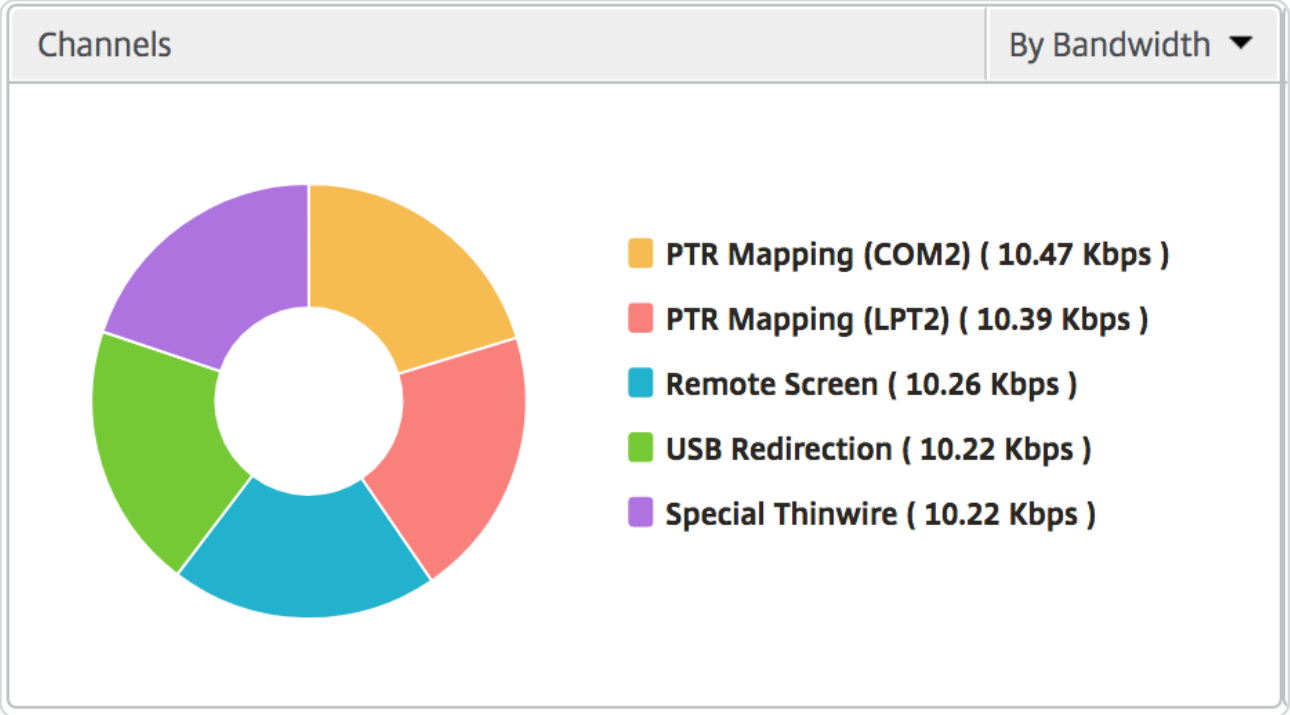
Users

Search

User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Cl
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	23.66 Kbps	1.88 K	
ramas	59	0	59	997.00 ms	778.00 ms	1.00 ms	7.03 Kbps	0	
omerp	59	0	59	997.00 ms	57.00 ms	754.00 ms	23.80 Kbps	1.89 K	
grahmm	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.80 Kbps	1.89 K	
ryan	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.69 Kbps	1.88 K	
rajivs	59	0	59	801.00 ms	11.00 ms	1.00 ms	23.97 Kbps	0	
alexisc	117	0	118	622.00 ms	56.00 ms	392.00 ms	47.67 Kbps	1.88 K	
juan	59	59	118	169.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
lennoxl	59	0	59	169.00 ms	31.00 ms	30.00 ms	23.86 Kbps	0	
daniel	59	59	118	149.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
woojunek	58	0	59	149.00 ms	31.00 ms	30.00 ms	23.85 Kbps	0	
parkerf	59	0	59	149.00 ms	31.00 ms	30.00 ms	23.88 Kbps	0	
randyb	59	59	118	99.00 ms	11.00 ms	29.00 ms	47.71 Kbps	0	
bradp	177	0	177	74.00 ms	27.00 ms	1.00 ms	71.75 Kbps	0	

CHANNELS

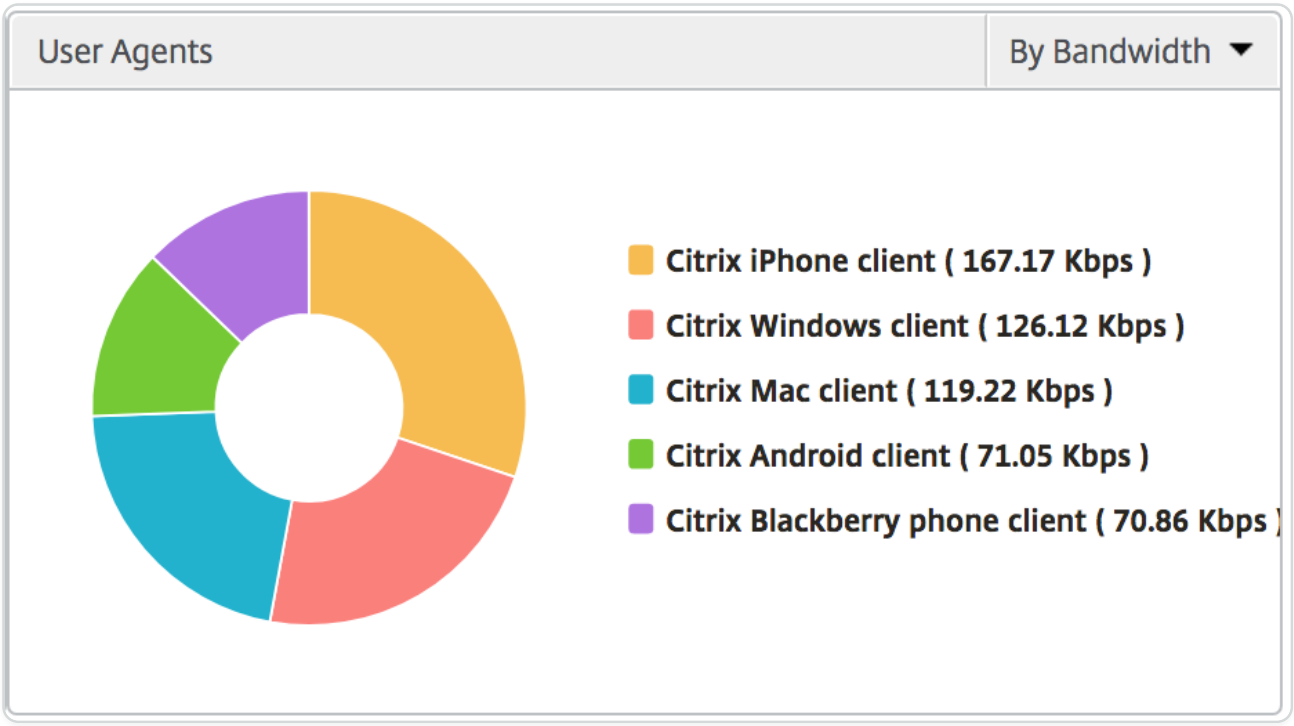
Channels represent the overall bandwidth or the total bytes consumed by each ICA® virtual channel in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.



USER AGENTS

User Agents represent the overall bandwidth/total bits consumed by each end point in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



THRESHOLDS BREACH COUNT

The Thresholds breach count metrics represent the count of thresholds breached in the selected time period.

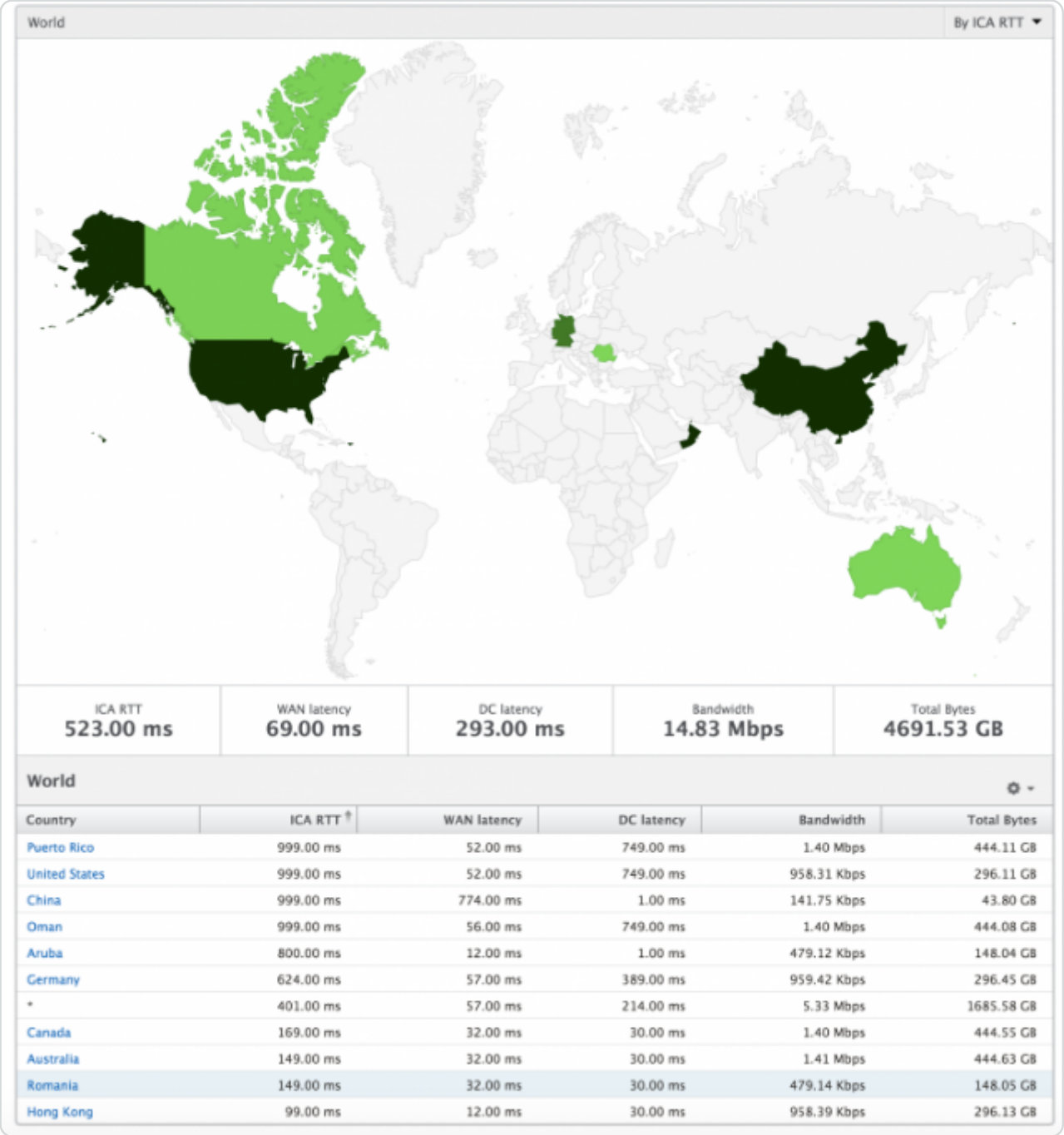
WORLD MAP

The World map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill-down to a particular country and further into cities as well by simply clicking the region. The administrators can further drill down to view information by city and state. From NetScaler Console version 12.0 and later, you can drill down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metric is displayed in the form of a heat map:

- ICA RTT
- WAN Latency
- DC Latency
- Bandwidth
- Total Bytes

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Per User View

The per user view provides detailed end user experience reporting for any particular selected user.

To navigate to specific user's metrics:

1. Navigate to **Gateway** > **HDX Insight** > **Users**.
2. Select a particular user from the Users summary report.

LINE CHART

Line chart displays the summary of all the metrics for the particular selected user during the selected time period.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CURRENT/TERMINATED SESSIONS REPORT

This report is pertinent to all current/terminated user sessions for the selected user. These metrics can be sorted by start time, session reconnects and ACR count.

METRICS	DESCRIPTION
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScalers caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.
Server IP Address	Back end/ Citrix Virtual App server IP.
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Workspace type- Citrix Windows Client
Client Version	Workspace version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.
Country	Country from which the session was established.
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back-end servers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

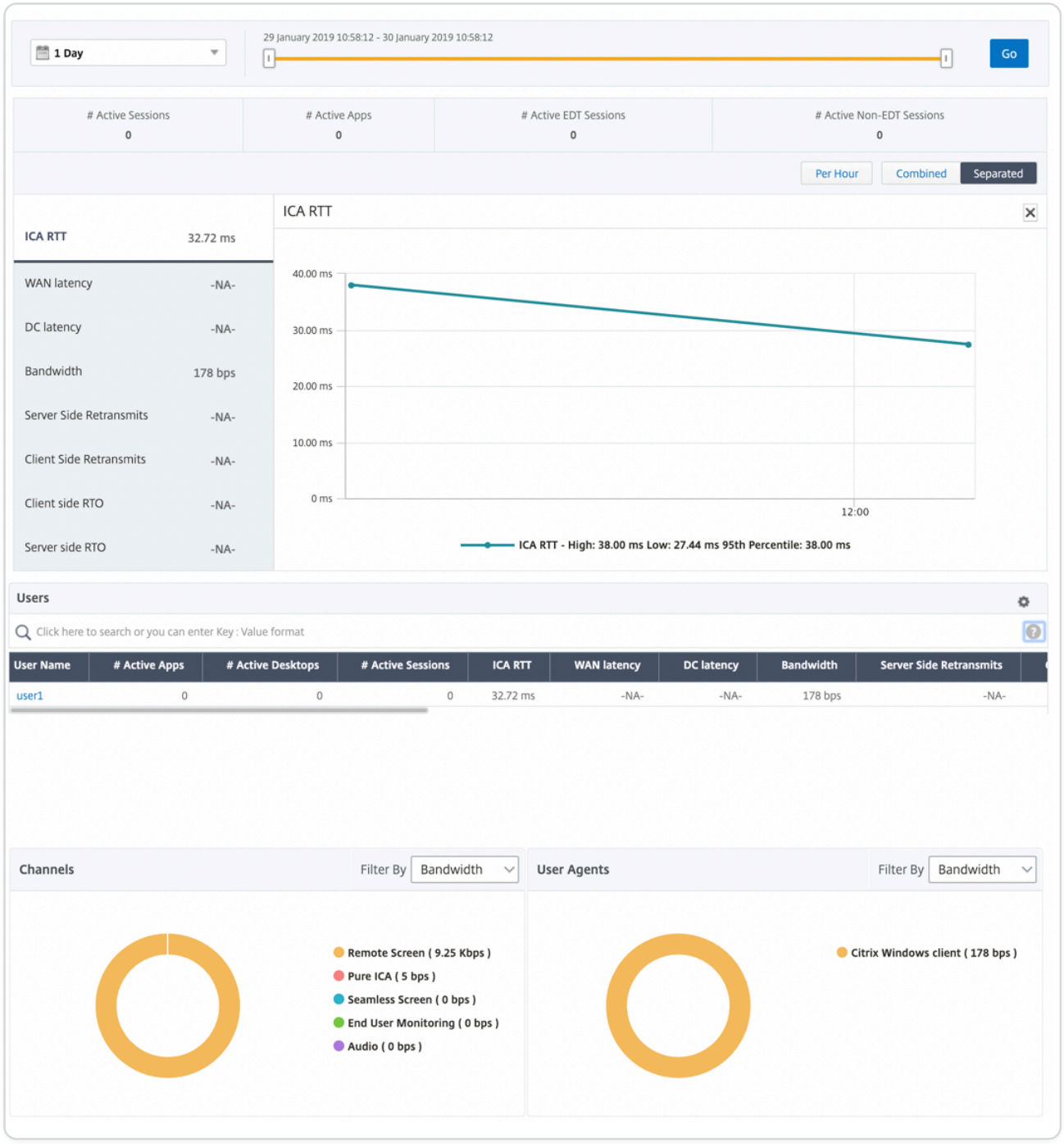
METRICS	DESCRIPTION
Total Bytes	Total Bytes consumed by the user during the selected time period.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back-end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between the NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between the NetScaler and back-end server.

SUPPORT FOR EDT IN HDX INSIGHT

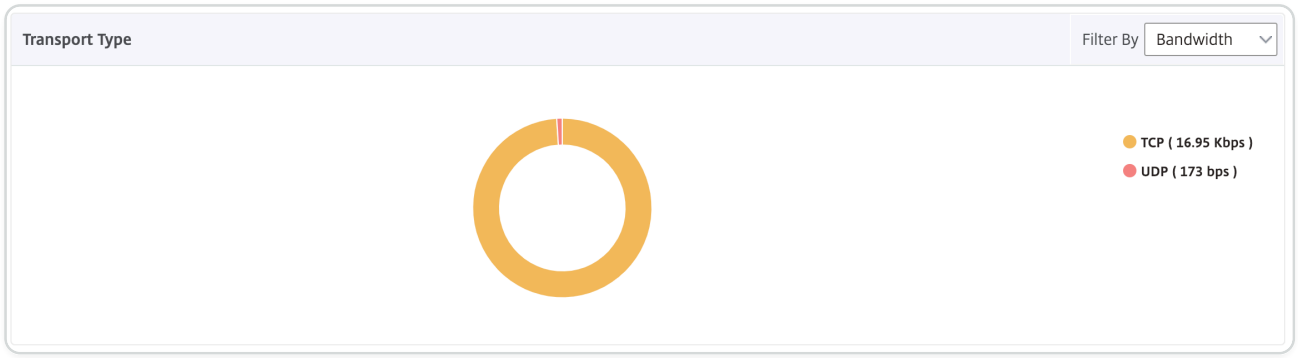
NetScaler Console now supports enlightened data transport (EDT) for displaying analytics for HDX Insight. That is, NetScaler Console now supports both UDP and TCP protocol. EDT support for NetScaler Gateway ensures a high definition in-session user experience of virtual desktops for users running Citrix Workspace.

HDX Insight now displays the number of EDT sessions and non-EDT sessions as part of the active sessions report. The Users table displays a detailed report of all the users in the system. The table shows metrics such as WAN latency, DC latency, retransmits, RTOs and some of these metrics are not available for users who do have EDT sessions as they are calculated from the TCP stack currently. Therefore, they appear as "NA".

© 1997–2026 Citrix Systems, Inc. All rights reserved.



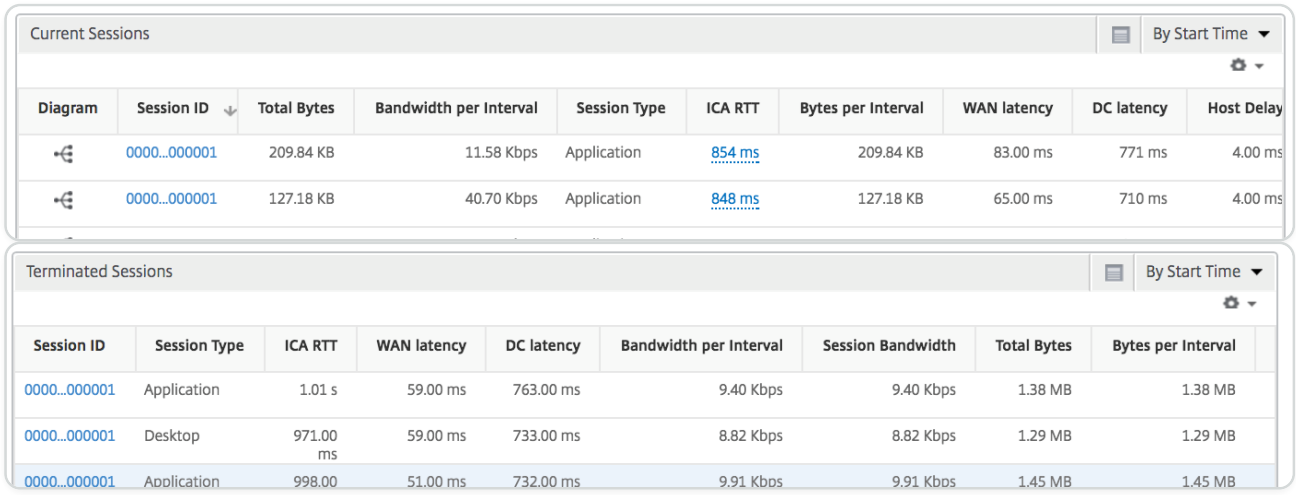
A new donut chart has been introduced to allow you to see bandwidth consumed by the user and also the total number of bytes based on the type of protocol used by the users.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX INSIGHT METRICS AVAILABLE FROM NETSCALER CONSOLE 12.0 AND LATER

L7 CLIENT-SIDE LATENCY	THE AVERAGE L7 LATENCY OBSERVED BETWEEN THE ICA CLIENT AND THE NETSCALER INSTANCE. THIS METRIC IS USEFUL IN NON-CITRIX DEVICES BEING PRESENT IN THE DELIVERY PATH.
L7 Server-side Latency	The average L7 latency observed between the NetScaler device and the Citrix Virtual App. This metric is useful in non-Citrix devices being present in the delivery path.
Maximum Breach Latency	The highest value of the L7 latency when a breach of a defined threshold for a set time interval occurs.
Average Breach Latency	The average value of L7 latency when the system is in a "L7 latency breached" state.
L7 Threshold Breach Count	The number of times a L7 threshold breach has occurred.



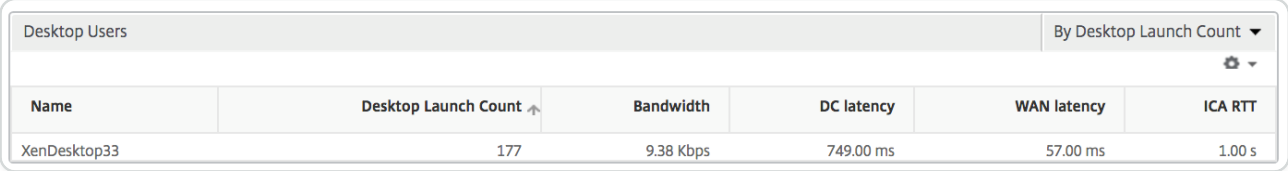
DESKTOP USERS

This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

METRICS	DESCRIPTION
Name	Name of the Citrix Virtual Desktop.
Desktop Launch Count	Number of times the desktop has launched.

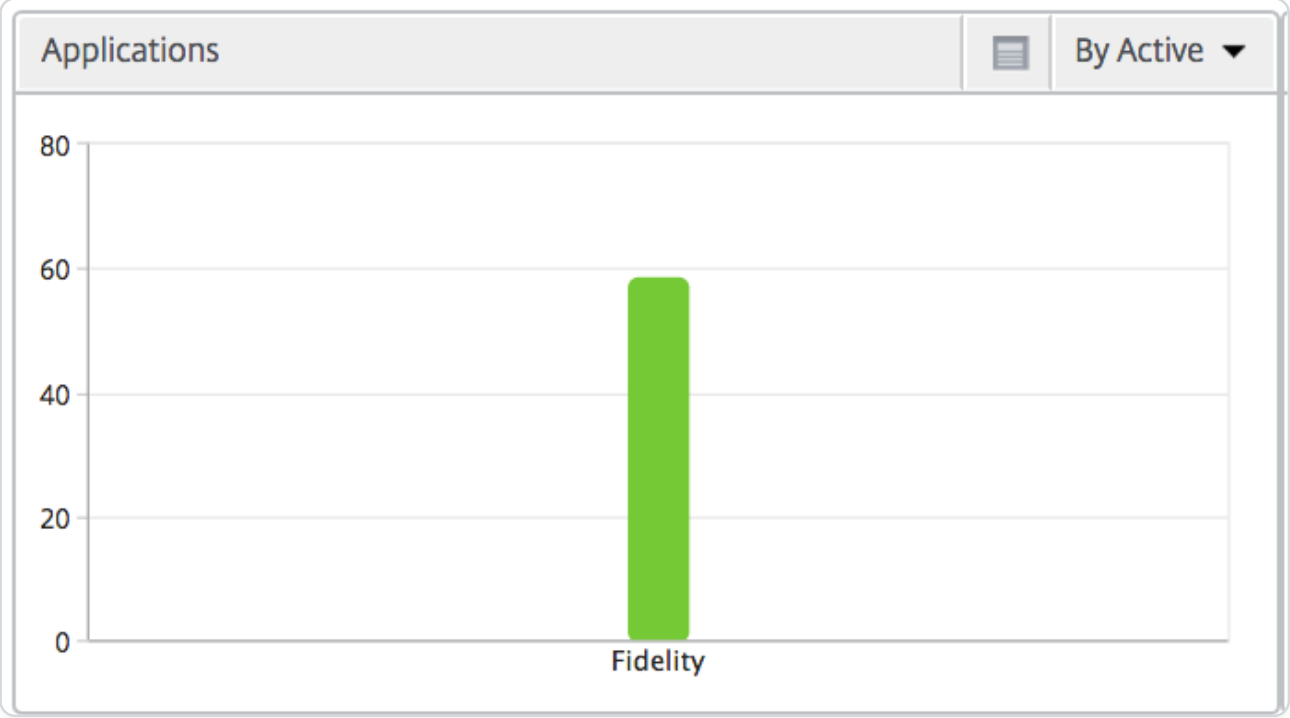
© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Bandwidth	Total bits per second taken for end to end communication during the selected time interval.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back-end servers.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.



APPLICATIONS

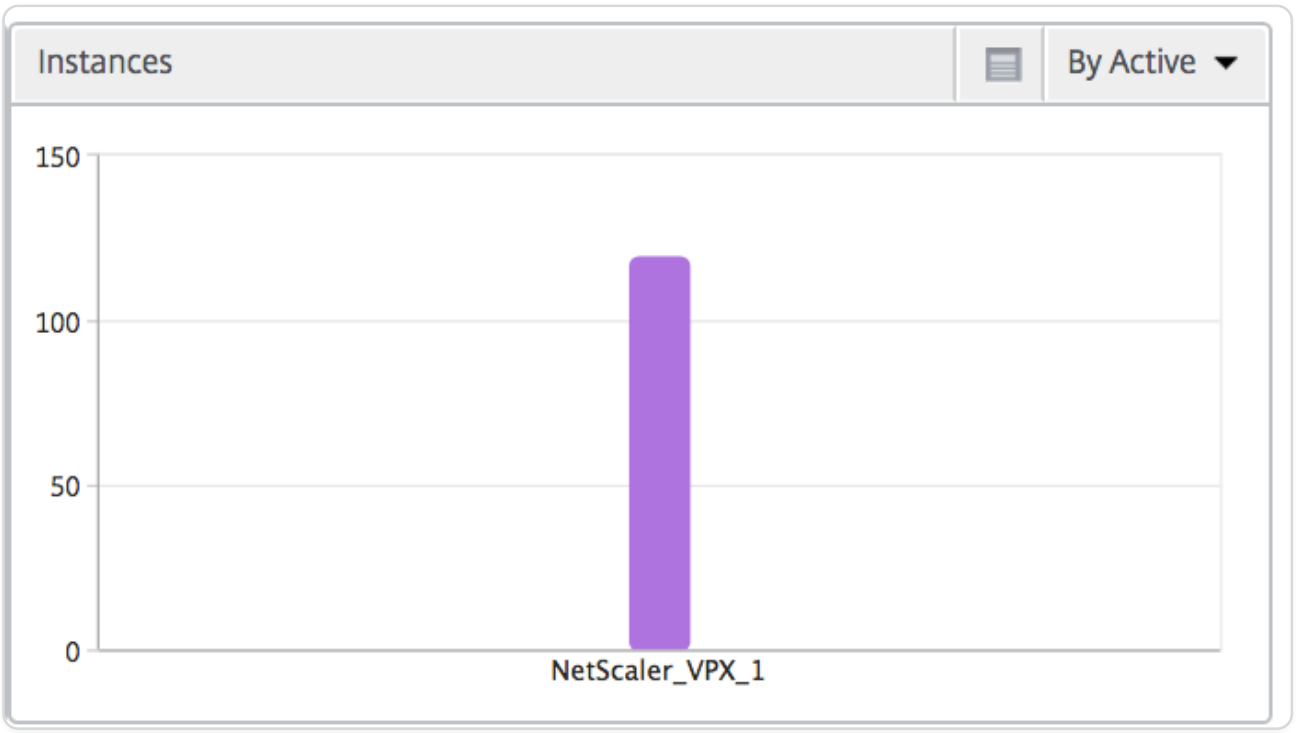
A bar graph representing apps sorted by Active, total session launch count, total app launch count, and launch duration.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

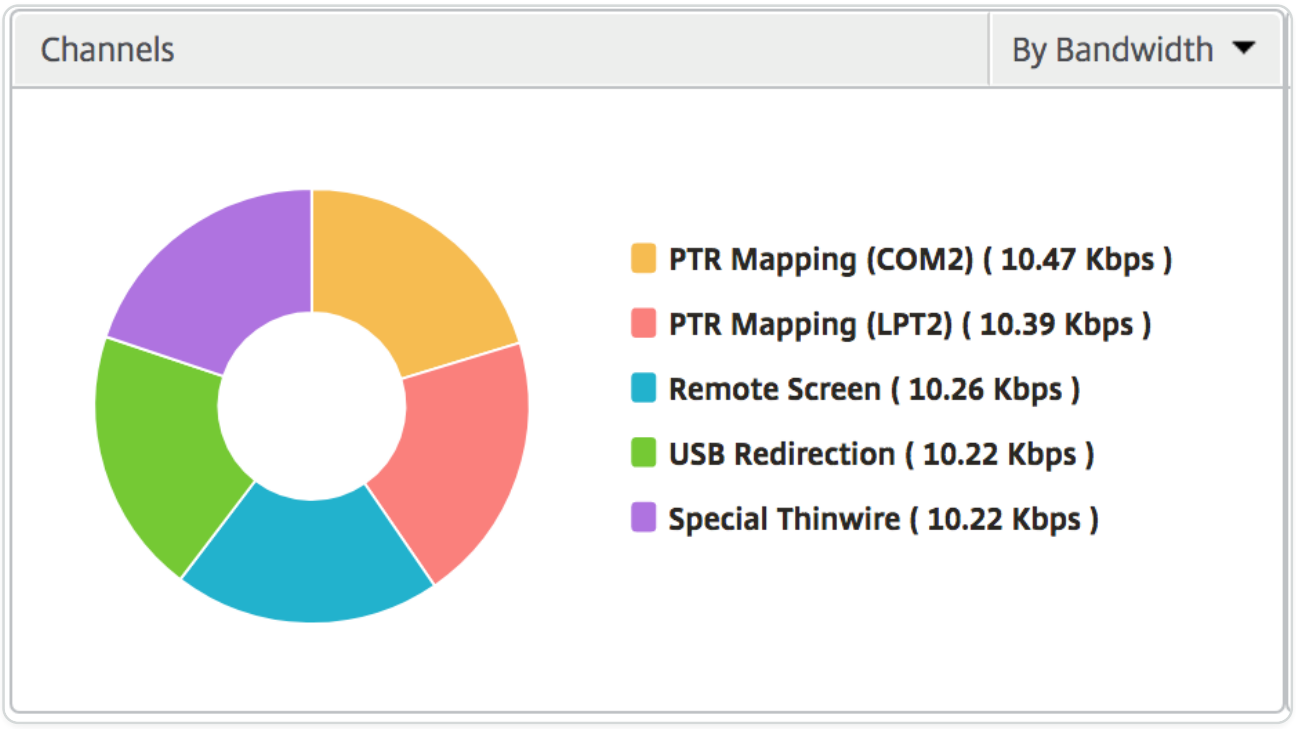
INSTANCES

A bar graph representing NetScaler Instances sorted by Active and total apps



CHANNELS

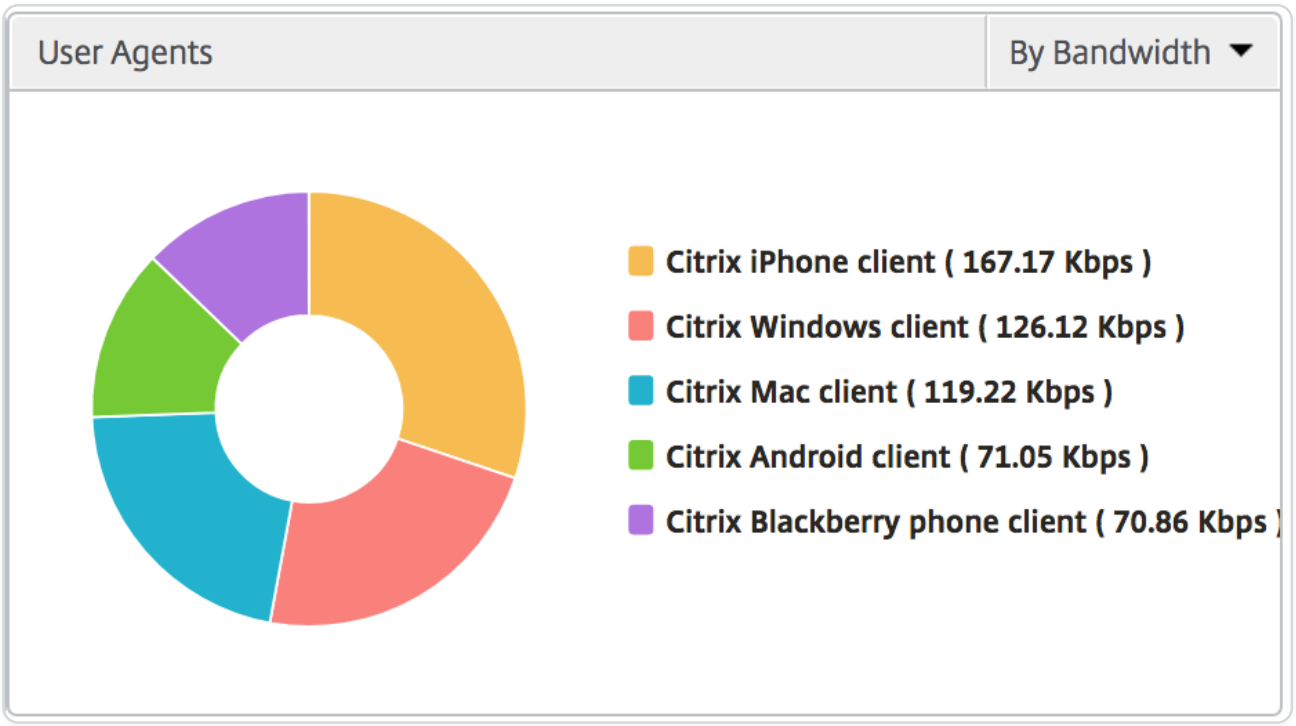
Channels represent the overall bandwidth or the total bits consumed by each ICA virtual channel in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bits.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

USER AGENTS

User Agents represent the overall bandwidth/total bits consumed by each end point in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bits.



Per User Session View

The per user session view provides reporting for a particular selected user's session.

To view the metrics for a selected user's session:

1. Navigate to **Gateway** > **HDX Insight** > **Users**.
2. Select a particular user from the **User Summary Report** section.
3. Select a session from **Current Sessions** or **Terminated Sessions** column.

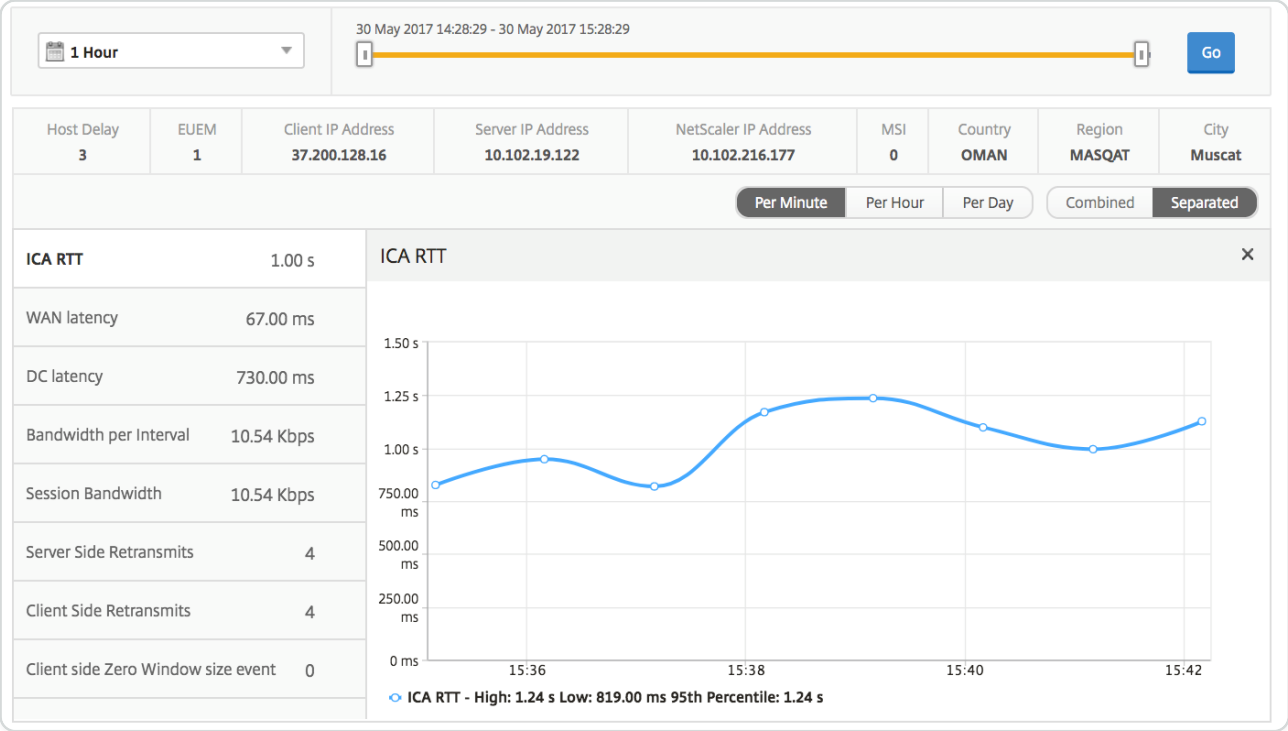
TIMELINE CHART

METRICS	DESCRIPTION
Session Reconnects	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
ACR Counts	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
	application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back-end servers.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back-end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back-end server.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



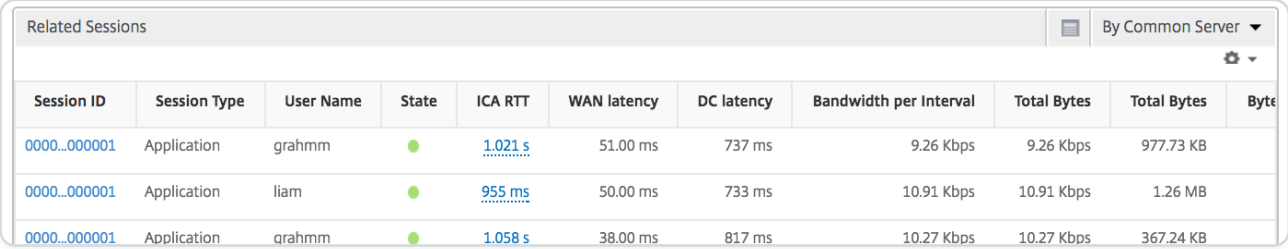
ACTIVE APPLICATION

The **Active Applications** section displays the active applications of the selected user. These applications can also be sorted by number of active sessions and launch durations.



RELATED SESSIONS

The related Sessions section displays the related sessions of the selected user's sessions. The relationship can be selected as common servers or common NetScaler.



Instance View Reports and Metrics

The reports and metrics in the instance view are focused on one or more NetScaler instances.

To navigate to the Instance view:

1. Log on to your NetScaler Console using a supported web browser.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Navigate to **Gateway** > **HDX™ Insight** > **Instances**.

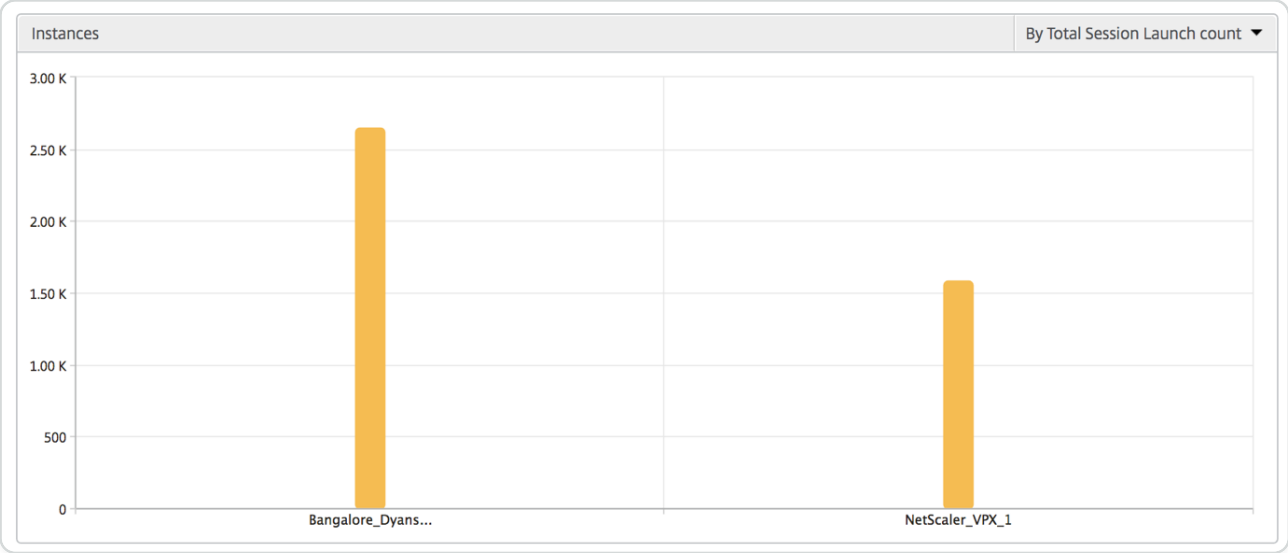
Instance Summary View

This view is called the summary view as it shows the reports for all the NetScaler instances that are added to NetScaler Console.

All these metrics/reports, unless explicitly mentioned have the values corresponding to them for the selected time period.

INSTANCE BAR GRAPH

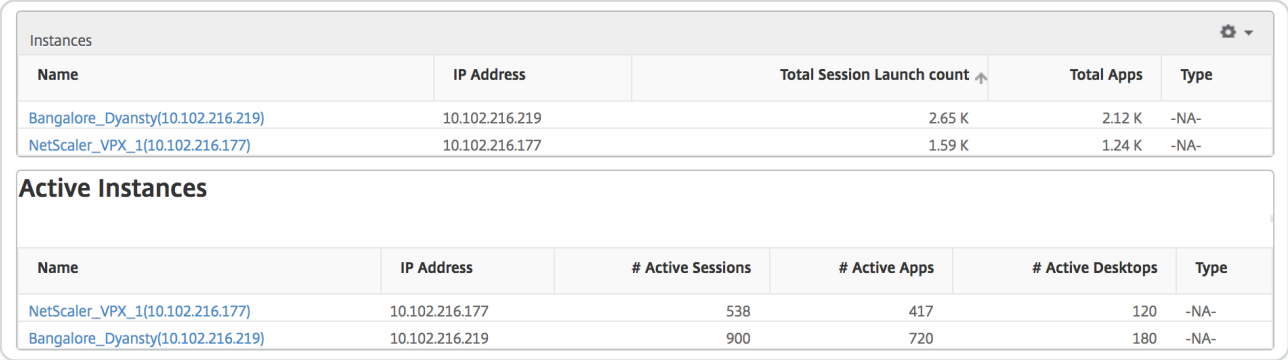
This graph displays the instance vs the Total Session Launch count and Total Apps from the list on the top right on the graph canvas.



INSTANCE/ACTIVE INSTANCES SUMMARY REPORT

METRICS	DESCRIPTION
Name	Host name of the NetScaler instance.
IP Address	NetScaler IP address.
Total Session Launch count	Total number of unique user sessions created during a given time interval.
Total Apps	Total number of unique applications launched during a given time interval.
Type	N/A

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Instances

Name	IP Address	Total Session Launch count	Total Apps	Type
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	2.65 K	2.12 K	-NA-
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	1.59 K	1.24 K	-NA-

Active Instances

Name	IP Address	# Active Sessions	# Active Apps	# Active Desktops	Type
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	538	417	120	-NA-
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	900	720	180	-NA-

THRESHOLD REPORT

Threshold report represents the count of thresholds breached where the *entity* is selected as Instance in the selected period. For more information, see how to create thresholds and alerts.

SKIPPED FLOWS

A skipped flow is a record which skipped parsing ICA® connection. This flow can occur due to multiple reasons like using unsupported Citrix Virtual App orDesktop versions, unsupported version of workspace or workspace type, and so on. This table shows the IP address and the skipped flow count. These workspaces may not be part of allow list workspaces. Hence these sessions are skipped from monitoring.

For more details on issues related to ICA parsing, see Record generation issue for HDX/ICA traffic in NetScaler checklist



Skipped Flows

IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

WORLD VIEW

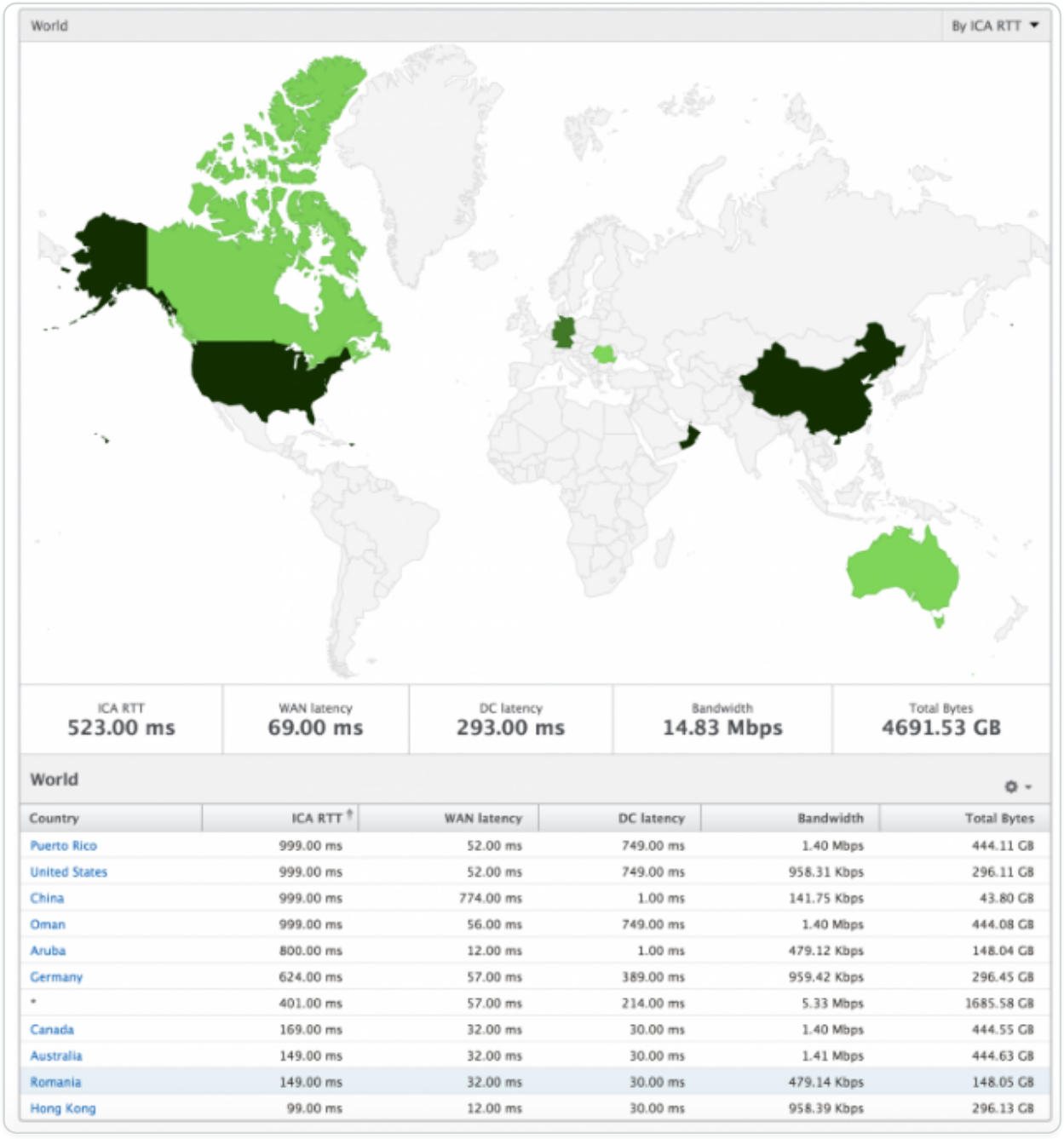
The World Map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill-down to a particular country and further into cities as well by clicking the region. The administrators can further drill down to view information by city and state. From NetScaler Console version 12.0 and later, you can drill down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metric is displayed in the form of a heat map:

- ICA RTT
- WAN Latency
- DC Latency

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Bandwidth
- Total Bytes



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Per Instance View

Per instance view provides detailed end user experience reporting for a particular selected NetScaler instance.

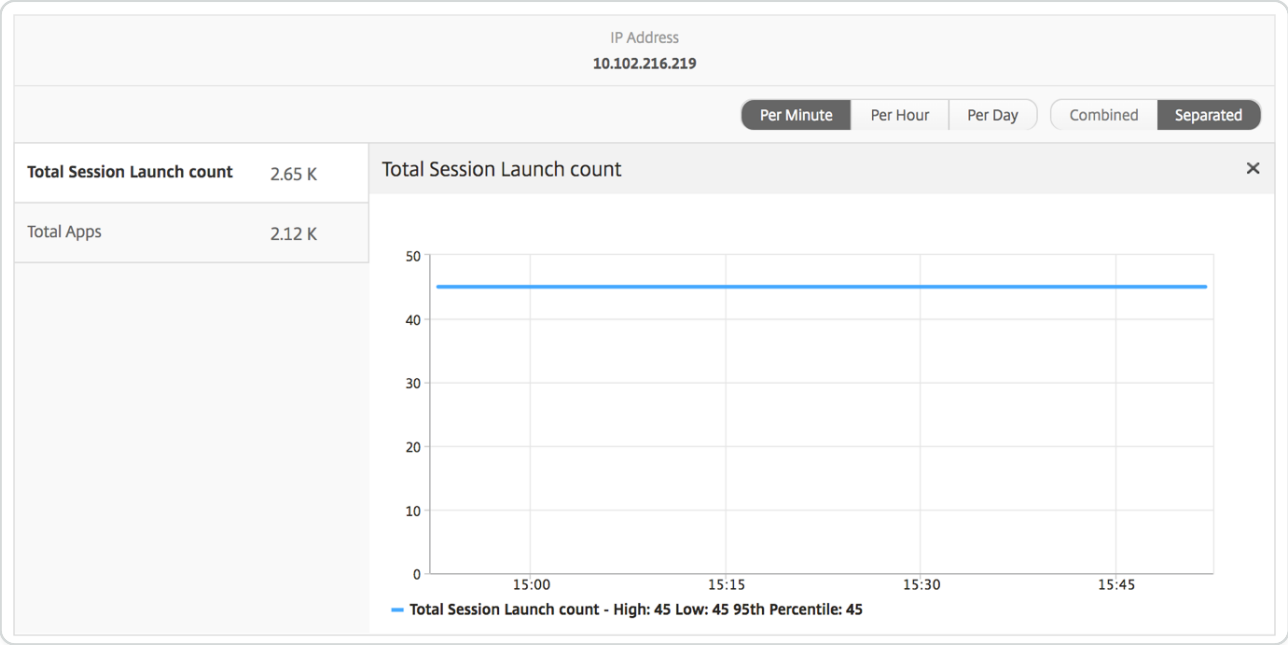
To navigate to the Instance view:

1. Navigate to **Gateway** > **HDX Insight** > **Instances**.
2. Select a particular Instance from the **Instance Summary Report**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

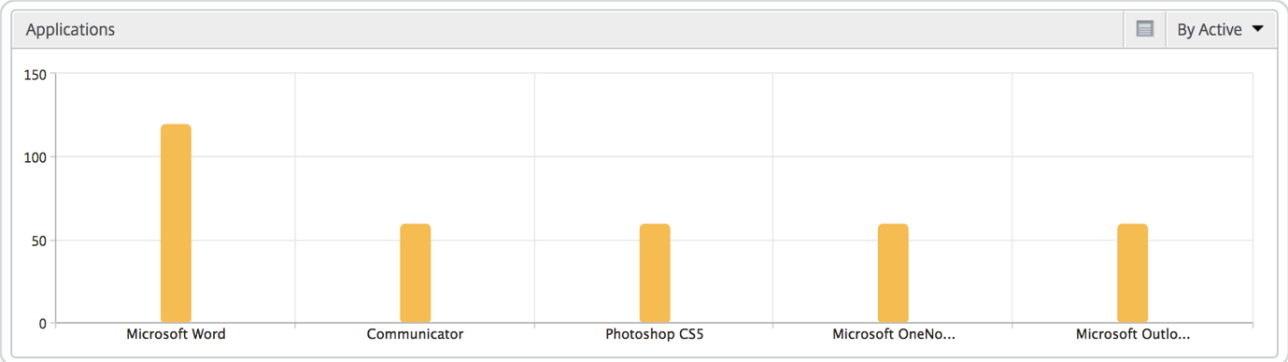
LINE CHART

METRICS	DESCRIPTION
IP Address	This represents the NetScaler IP address of the selected instance.
Total session launch count	Total number of active Citrix Virtual App sessions during the given time interval.
Total Apps	Total number of unique applications launched during a given time interval.



APPLICATIONS BAR GRAPH

Displays the top 5 applications based on Active apps, total session launch count, total app launch count, or launch duration.

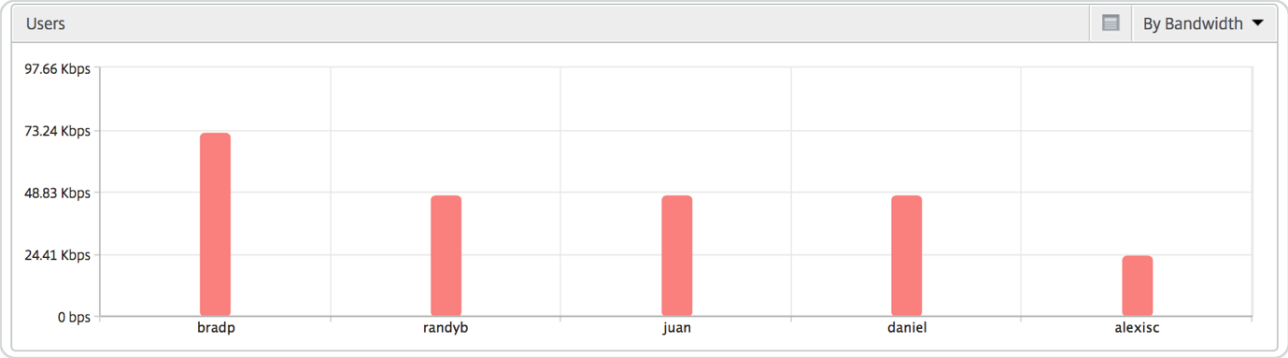


USERS BAR GRAPH

The Users bar graph displays top 5 users based on the following criteria

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Bandwidth
- WAN Latency
- DC Latency
- ICA RTT

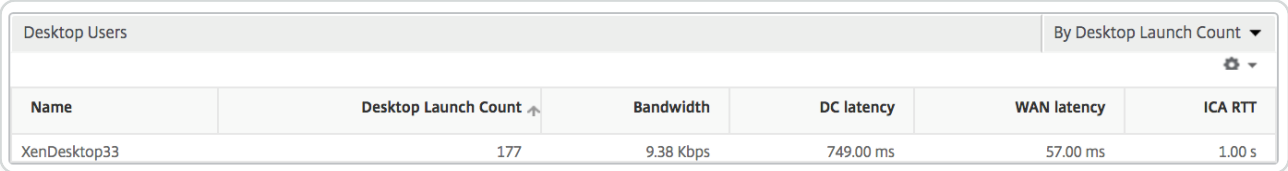


DESKTOP USERS REPORT

This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

METRICS	DESCRIPTION
Name	The Citrix Virtual Desktop name.
Desktop Launch Count	Number of times the desktop has launched.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back-end servers.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



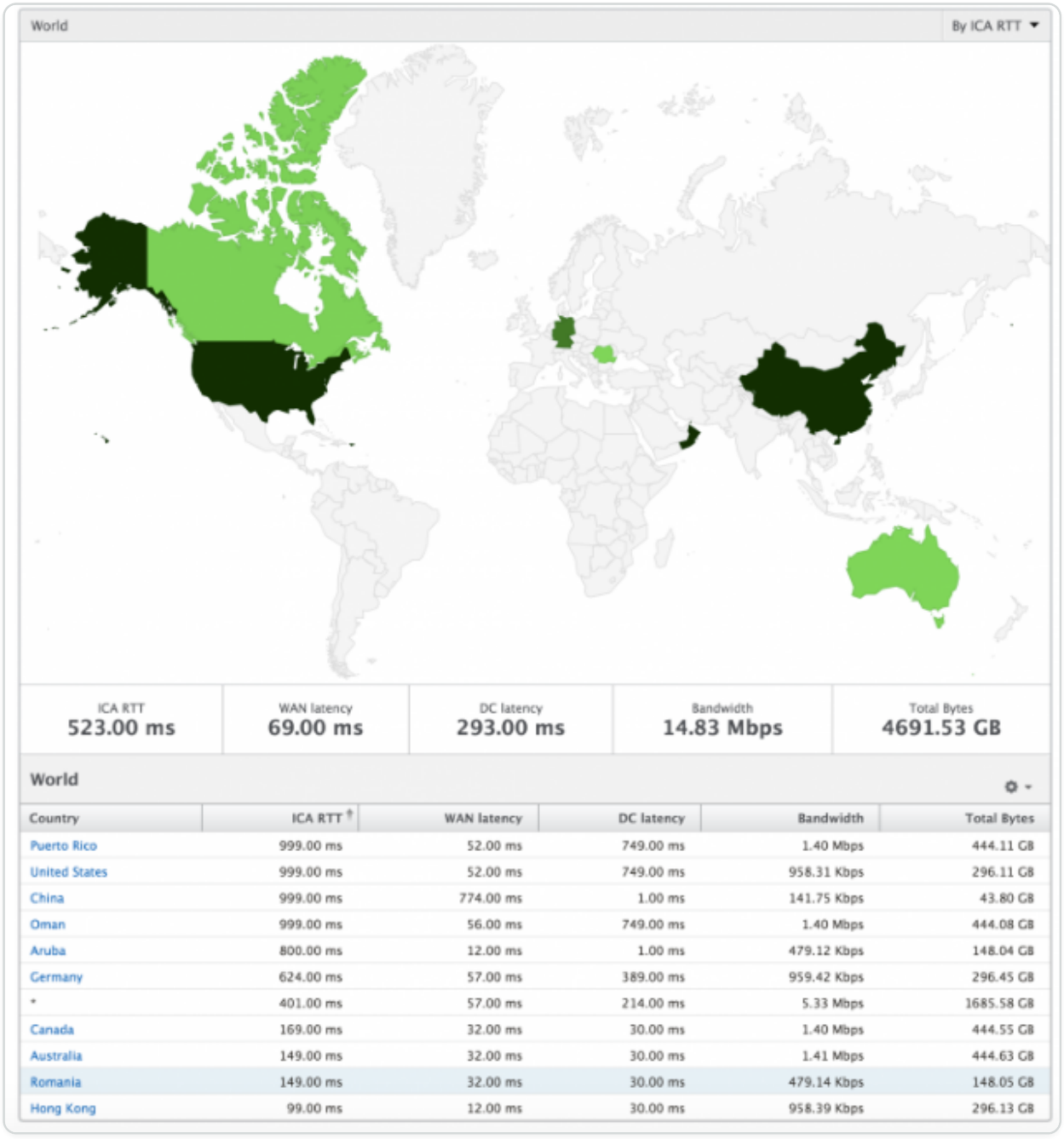
WORLD VIEW

The World Map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill-down to a particular country and further into cities as well by clicking the region. The administrators can further drill down to view information by city and state. From NetScaler Console version 12.0 and later, you can drill down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metric is displayed in the form of a heat map:

- ICA RTT
- WAN Latency
- DC Latency
- Bandwidth
- Total Bytes

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

License View Reports and Metrics

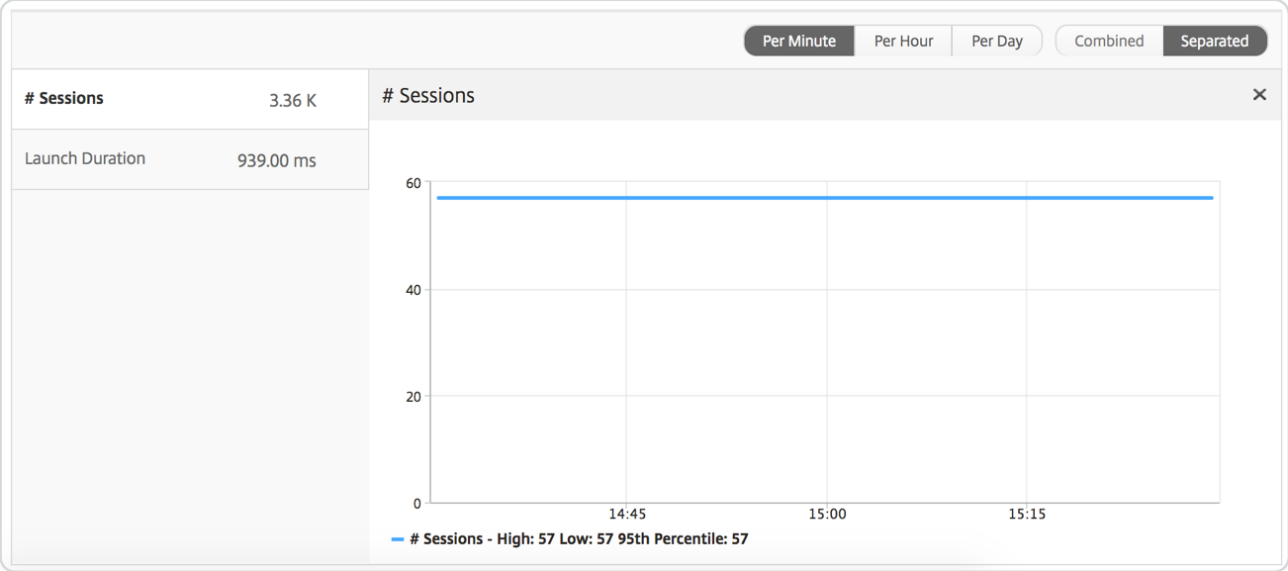
The license view gives details on the NetScaler Gateway license information. Navigate to **Gateway** > **HDX Insight** > **Licenses**.

Line Chart

METRICS	DESCRIPTION
Licenses in use	The NetScaler Gateway CCU licenses being used during the selected timeline. Each count represents the number of user sessions. This

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
	is independent of the application and desktop sessions launched by that user.
Total licenses	Total number of NetScaler Gateway CCU licenses available for the customer to utilize.



Threshold Report

The threshold report represents the count of thresholds breached where the *entity* is selected as License in the selected period.

Troubleshoot HDX™ Insight issues

If the HDX Insight solution is not functioning as expected, the issue might be with one of the following. Refer to the checklists in the respective sections for troubleshooting.

- HDX Insight configuration.
- Connectivity between NetScaler and NetScaler Console.
- Record generation for HDX/ICA traffic in NetScaler.
- Population of records in NetScaler Console.

HDX Insight configuration checklist

- Ensure that the AppFlow feature is enabled in NetScaler. For details, see Enabling AppFlow.
- Check HDX Insight configuration in the NetScaler running configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Run the `show running | grep -i <appflow_policy>` command to check the HDX Insight configuration. Make sure that the bind type is ICA REQUEST. For example;

```
bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
```

For transparent mode, the bind type must be ICA_REQ_DEFAULT. For example;

```
bind appflow global afp 100 END -type ICA_REQ_DEFAULT
```

- For single-hop/Access Gateway or double-hop deployment, make sure that HDX Insight AppFlow policy is bound to the VPN virtual server, where HDX/ICA traffic is flowing.
- For Transparent mode or LAN user mode make sure the ICA® ports 1494 and 2598 are set.
- Check `appflowlog` parameter in NetScaler Gateway or VPN virtual server is enabled for Access Gateway or double-hop deployment. For details, see Enabling AppFlow for Virtual Servers.
- Check “Connection Chaining” is enabled in double-hop NetScaler. For details see, Configuring NetScaler Gateway appliances to export data.
- After HA Failover if the HDX Insight details are Skip parsed, check ICA param “enableSRonHAFailover” is enabled. For details, see Session Reliability on NetScaler High Availability Pair.

Connectivity between NetScaler and NetScaler Console checklist

- Check AppFlow collector status in NetScaler. For details, see How to check the status of connectivity between NetScaler and AppFlow Collector.
- Check HDX Insight AppFlow® policy hits.

  Run the command `show appflow policy <policy_name>` to check the AppFlow policy hits.

  You can also navigate to **System > AppFlow > Policies** in the GUI to check the AppFlow policy hits.
- Validate any firewall blocking AppFlow ports 4739 or 5557.

Record generation for HDX/ICA traffic in NetScaler checklist

Run the command `tail -f /var/log/ns.log | grep -i "default ICA Message"` for log validation. Based on the logs that are generated, you can use this information for troubleshooting.

- Log: **Skipped parsing ICA connection - HDX Insight not supported for this host**

  Cause: Unsupported Citrix Virtual Apps and Desktops versions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Workaround: Upgrade the Citrix Virtual Apps and Desktops servers to a supported version.

- Log: **Client type received 0x53, NOT SUPPORTED**

  Cause: Unsupported version of Citrix Workspace app

  Solution: Upgrade Citrix Workspace app to a supported version.

- Log: **Error from Expand Packet - Skipping all hdx processing for this flow**

  Cause: Issue with uncompressing ICA traffic

  Solution: No reports are available for this ICA session until a new session is established.

- Log: **Invalid transition: NS_ICA_ST_FLOW_INIT/NS_ICA_EVT_INVALID -> NS_ICA_ST_UNINIT"**

  Cause: Issue with parsing the ICA handshake

  Solution: No reports are available for this particular ICA session until a new session is established.

- Log: **Missing EUEM ICA RTT**

  Cause: Unable to parse End-User Experience Monitoring channel data

  Solution: Make sure End-User Experience Monitoring service in started on the Citrix Virtual Apps and Desktops servers. Make sure you are using the supported versions of Citrix Workspace App.

- Log: **Invalid Channel Header**

  Cause: Unable to identify channel header

  Solution: No reports are available for this particular ICA session until a new session is established.

- Log: **Skip code**

  If you see any of the following values for skip code, then the Insight details are skip parsed.

  Skip code 0 indicates that the record is successfully exported from NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SKIP CODE	ERROR MESSAGE	CAUSE OF ERROR
100	NS_ICA_ERR_NULL_FRAG	Error handling ICA fragments, likely due to memory conditions
101	NS_ICA_ERR_INVALID_HS_CMD	Invalid handshake command received
102	NS_ICA_ERR_REDUC_PARAM_CNT	Invalid parameter specified for V3 expander initialization
103	NS_ICA_ERR_REDUC_INIT	Unable to initialize the V3 expander correctly
104	NS_ICA_ERR_REDUC_PARAM_BYTES	Insufficient bytes to assign a coder to a channel
105	NS_ICA_ERR_INVALID_CHANNEL	Invalid ICA channel number
106	NS_ICA_ERR_INVALID_DECODER	Invalid decoder specified for a channel
107	NS_ICA_ERR_INVALID_TW_PARAM	Invalid parameter count specified on Thinwire channel
108	NS_ICA_ERR_INVALID_TW_DECODER	Invalid decoder for Thinwire channel
109	NS_ICA_ERR_REDUC_NO_DECODER	No decoder defined for channel
110	NS_ICA_ERR_REDUC_V3_EXPANDER	Failed to expand channel data
111	NS_ICA_ERR_REDUC_BYTES_V3_OOR	Expander error: Bytes consumed more than bytes available
112	NS_ICA_ERR_REDUC_BYTES_OOR	Error: Uncompressed data overrun

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SKIP CODE	ERROR MESSAGE	CAUSE OF ERROR
113	NS_ICA_ERR_REDUC_INVALID_CMD	Undefined Expander command
114	NS_ICA_ERR_CGP_FILL_HOLE	Error while handling split CGP frames
115	NS_ICA_ERR_MEM_NSB_ALLOC	NSB allocation error – due to low memory conditions
116	NS_ICA_ERR_MEM_REDUC_CTX_ALLOC	Memory allocation error for expander context
117	NS_ICA_ERR_ICA_OLD_SERVER	Old server, capability blocks not supported
118	NS_ICA_ERR_PIR_MANY_FRAG	Packet Init request is fragmented, unable to process
119	NS_ICA_ERR_INIT_ICA_CAPS	ICA capability initialization error
120	NS_ICA_ERR_NO_MSI_SUPPORT	Host does not support MSI feature. Indicates for XenApp version lower than 6.5 or XenDesktop versions lower than 5.0
121	NS_ICA_ERR_CGP_INVALID_CMD	Invalid CGP command encountered
122	NS_ICA_ERR_INSUFFICENT_CHANNEL_BYTES	Insufficient bytes over channel
123	NS_ICA_ERR_CHANNEL_DATA	Incorrect data on EUEM, CONTROL, or SEAMLESS channel
124	NS_ICA_ERR_INVALID_PURE_CMD	Invalid command received while processing pure ICA channel data

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SKIP CODE	ERROR MESSAGE	CAUSE OF ERROR
125	NS_ICA_ERR_INVALID_PURE_LEN0	Invalid length encountered while processing pure ICA channel data
126	NS_ICA_ERR_INVALID_PURE_LEN	Invalid length encountered while processing PURE ICA channel data
127	NS_ICA_ERR_INVALID_CLNT_DATA	Invalid data length received from client
128	NS_ICA_ERR_MSI_GUID_SZ	Error in MSI GUID size
129	NS_ICA_ERR_INVALID_CHANNEL_HEADER	Detected invalid channel header
130	NS_ICA_ERR_CGP_PARSE_RECONNECT_ID	Retrieval of reconnected session failed
131	NS_ICA_ERR_DISABLE_SR_NON_NS_RECONNECT	Error in disabling SR
132	NS_ICA_ERR_REDUC_NOT_V3	Unsupported ICA Reducer version
133	NS_ICA_ERR_HS_COMPRESSION_DISABLED	Compression disabled, not honored by host
134	NS_ICA_ERR_IDENT_PROTO	Unable to identify ICA or CGP protocol, seen with incorrect receivers
135	NS_ICA_ERR_INVALID_SIGNATURE	Incorrect ICA signature or magic string
136	NS_ICA_ERR_PARSE_RAW	Error while parsing the ICA handshake packet
137	NS_ICA_ERR_INCOMPLETE_PKT	Incomplete packet received in handshake

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SKIP CODE	ERROR MESSAGE	CAUSE OF ERROR
138	NS_ICA_ERR_ICAFRAME_TOO_LARGE	ICA frame is too large, exceeds 1,460 bytes
139	NS_ICA_ERR_FORWARD	Error while forwarding the ICA data
140	NS_ICA_ERR_MAX_HOLES	Unable to process CGP command as it is split beyond supported limit
141	NS_ICA_ERR_ASSEMBLE_FRAME	Unable to reassemble ICA frame correctly
142	NS_ICA_ERR_UNSUPPORTED_RECEIVER_VERSION	Skipped ICA parsing for this workspace (client) as it is not in the allow list
143	NS_ICA_ERR_LOOKUP_RECONNECT_ID	Unable to detect parsing state for client reconnect cookie
144	NS_ICA_ERR_SYNCUP_RECONNECT_ID	Invalid reconnect cookie length detected post client reconnect
145	NS_ICA_ERR_INVALID_RECONNECT_ID	Client reconnects cookie missed the needed constraint
146	NS_ICA_ERR_INVALID_CLIENT_VERSION	Invalid workspace version string received from client
147	NS_ICA_ERR_UNKNOWN_CLIENT_PRODUCT_ID	Invalid product ID received from client
148	NS_ICA_ERR_V3_HDR_CORRUPT_LEN	Invalid channel length post expansion
149	NS_ICA_ERR_SPECIAL_THINWIRE	Decompression error

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SKIP CODE	ERROR MESSAGE	CAUSE OF ERROR
150	NS_ICA_ERR_SEAMLESS_INSUFFBYTE	Encountered insufficient bytes for seamless command
151	NS_ICA_ERR_EUEM_INSUFFBYTE	Encountered insufficient bytes for EUEM command
152	NS_ICA_ERR_SEAMLESS_INVALID_EVENT	Invalid event for seamless channel parsing
153	NS_ICA_ERR_CTRL_INVALID_EVENT	Invalid event for CTRL channel parsing
154	NS_ICA_ERR_EUEM_INVALID_EVENT	Invalid event for EUEM channel parsing
155	NS_ICA_ERR_USB_INVALID_EVENT	Invalid event for USB channel parsing
156	NS_ICA_ERR_PURE_INVALID_EVENT	Invalid event for pure channel parsing
157	NS_ICA_ERR_VCP_INVALID_EVENT	Invalid event for virtual channel parsing
158	NS_ICA_ERR_ICAP_INVALID_EVENT	Invalid event for ICA data parsing
159	NS_ICA_ERR_CGPP_INVALID_EVENT	Invalid event for CGP data parsing
160	NS_ICA_ERR_BASICCRYPT_INVALIDSTATE	Invalid state for a crypt command in basic encryption
161	NS_ICA_ERR_BASICCRYPT_INVALIDCRYPTCMD	Invalid crypt command in basic encryption
162	NS_ICA_ERR_ADVCRYPT_INVALIDSTATE	Invalid state for a crypt command in RC5 encryption
163	NS_ICA_ERR_ADVCRYPT_INVALIDCRYPTCMD	Invalid crypt command in RC5 encryption

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SKIP CODE	ERROR MESSAGE	CAUSE OF ERROR
164	NS_ICA_ERR_ADVCRYPT_ENC	Error in RC5 encryption/ decryption
165	NS_ICA_ERR_ADVCRYPT_DEC	Error in RC5 encryption/ decryption
166	NS_ICA_ERR_SERVER_NOT_REDUCER_V3	VDA does not support Reducer Version 3
167	NS_ICA_ERR_CLIENT_NOT_REDUCER_V3	Workspace does not support Reducer Version 3
168	NS_ICA_ERR_ICAP_INSUFFBYTE	Unexpected number of bytes in ICA handshake
169	NS_ICA_ERR_HIGHER_RECONSEQ	Higher CGP resumption sequence number from peer post reconnects
170	NS_ICA_ERR_DESCSRINFO_ABSENT	Unable to restore ICA parsing state post reconnect
171	NS_ICA_ERR_NSAP_PARSING	Error while parsing Insight channel data
172	NS_ICA_ERR_NSAP_APP	Error while parsing app details from Insight channel data
173	NS_ICA_ERR_NSAP_ACR	Error while parsing ACR details from Insight channel data
174	NS_ICA_ERR_NSAP_SESSION_END	Error while parsing session end details from Insight channel data
175	NS_ICA_ERR_NON_NSAP_SN	Skipped ICA parsing on service node due to the absence of Insight channel support

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SKIP CODE	ERROR MESSAGE	CAUSE OF ERROR
176	NS_ICA_ERR_NON_NSAP_CLIENT	NSAP is not supported by client
177	NS_ICA_ERR_NON_NSAP_SERVER	NSAP is not supported by VDA
178	NS_ICA_ERR_NSAP_NEG_FAIL	Error while NSAP data negotiation
179	NS_ICA_ERR_SN_RECONNECT_TKT_FETCH	Error in fetching service reconnects ticket in service node
180	NS_ICA_ERR_SN_HIGHER_RECONSEQ	Error when receiving higher reconnect sequence number in service node
181	NS_ICA_ERR_DISABLE_HDXINSIGHT_NONNSAP	Error while disabling HDX Insight for non-NSAP connections

Sample logs:

```
Jan 9 22:57:02 <local0.notice> 10.106.40.223 01/09/2020:22:57:02 GMT ns-223 0-PPE-2 : default ICA Message 1234 0 : "Session setup data send: Session GUID [57af35043e624abab409f5e6af7fd22c], Client IP/Port [10.105.232.40/52314], Server IP/Port [10.106.40.215/2598], MSI Client Cookie [Non-MSI], Session setup time [01/09/2020:22:56:49 GMT], Client Type [0x0052], Receiver Version [19.12.0.23], User [user1], Client [10.105.232.40], Server [WIN2K12-215], Ctx Flags [0x8820220228], Track Flags [0x1775010c3fc], Skip Code [0]"
```

```
Jan 9 22:55:41 <local0.notice> 10.106.40.223 01/09/2020:22:55:41 GMT ns-223 0-PPE-0 : default ICA Message 156 0 : "Skipping ICA flow: Session GUID [4e3a91175ebcbe686baf175eec7e0200], Client IP/Port [10.105.232.40/60059], Server IP/Port [10.106.40.219/2598], MSI Client Cookie [Non-MSI], Session setup time [01/09/2020:22:55:39 GMT], Client Type [0x0052], Receiver Version [19.12.0.23], User [user1], Client [10.105.232.40], Server [10.106.40.219], Ctx Flags [0x8820220008], Track Flags [0x1600010c040], Skip Code [171]"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Error counters

Various counters are captured ICA parsing. The following table lists the various counters for ICA parsing. Run the command `nsconmsg –g hdx –d statswt0` for viewing the counter details.

HDX COUNTER NAME	PURPOSE	CATEGORY(STATS/ERROR/ DIAGNOSTICS)
hdx_tot_ica_conn	Indicates total number of Pur e ICA connections detected by NS. Incremented whenever an ICA connection based on the ICA signature o n a client PCB is detected.	Stats
hdx_tot_cgp_conn	Indicates total number of CG P connections detected by N S (Session Reliability ON). Incremented whenever a CG P connection based on the CGP signature on a client PCB is detected.	Stats
hdx_dbg_tot_udt_conn	Indicates total number of UDP ICA connections detected by NS	Stats
hdx_dbg_tot_nsap_conn	Indicates total number of NSAP supported connections detected by NS	Stats
hdx_tot_skip_conn	Indicates how many ICA conn ections were skipped by pars er due to invalid ICA or CGP signature.	Stats
hdx_dbg_active_conn	Total Active EDT/CGP/ ICA connections at that instan t.	Stats

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX COUNTER NAME	PURPOSE	CATEGORY(STATS/ERROR/ DIAGNOSTICS)
hdx_dbg_active_nsap_conn	Total Active EDT/CGP/ ICA NSAP connections at that instant.	Stats
hdx_dbg_skip_appflow_disabled	Total number of instances where AppFlow was detached from a session because of disabling AppFlow	Stats/Diagnostics
hdx_dbg_transparent_user	Total number of transparent user access	Stats/Diagnostics
hdx_dbg_ag_user	Total number of Access Gateway user access	Stats/Diagnostics
hdx_dbg_lan_user	Total number of LAN user mode access	Stats/Diagnostics
hdx_basic_enc	Indicates the number of ICA connections using basic encryption	Stats/Diagnostics
hdx_advanced_enc	Indicates the number of ICA connections using advanced RC5 based encryption	Stats/Diagnostics
hdx_dbg_reconnected_session	Total number of reconnect requests from client without any NetScaler error	Stats/Diagnostics
hdx_dbg_host_rejected_ns_reconnect	Total number of hosts rejected reconnects requests by client	Stats/Diagnostics
hdx_euem_available	Indicates the number of connections having the End User Experience Monitoring channel available. End User Experience Monitoring cha	Stats/Diagnostics

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX COUNTER NAME	PURPOSE	CATEGORY(STATS/ERROR/ DIAGNOSTICS)
	nnel is required to collect stati stics such as ICA RTT.	
hdx_err_disabled_sr	Session Reliability is disabled using `nsapimgr` knob. Sess ion does not work for this session.	Error
hdx_err_skip_no_msi	XA/XD server is Missing MSI capability. This indicates an older server version, HDX Ins ight skips this connection.	Error
hdx_err_skip_old_server	Old unsupported server version	Error
hdx_err_clnt_not_whitelist	Client receiver not in allow list, HDX Insight skips this connection	Error
hdx_sm_ica_cam_channel_di sabled	Total number of NS_ICA_CA M_CHANNEL disabled via SmartAccess pol icy	Diagnostics
hdx_sm_ica_usb_channel_di sabled	Total number of NS_ICA_US B_CHANNEL disabled via SmartAccess pol icy	Diagnostics
hdx_sm_ica_clip_channel_di sabled	Total number of NS_ICA_CLI P_CHANNEL disabled via SmartAccess pol icy	Diagnostics
hdx_sm_ica_ccm_channel_di sabled	Total number of NS_ICA_CC M_CHANNEL disabled via S martAccess policy	Diagnostics
hdx_sm_ica_cdm_channel_di sabled	Total number of NS_ICA_CD M_CHANNEL	Diagnostics

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX COUNTER NAME	PURPOSE	CATEGORY(STATS/ERROR/ DIAGNOSTICS)
	disabled via SmartAccess pol icy	
hdx_sm_ica_com1_channel_ disabled	Total number of NS_ICA_CO M1_CHANNEL disabled via SmartAccess pol icy	Diagnostics
hdx_sm_ica_com2_channel_ disabled	Total number of NS_ICA_CO M2_CHANNEL disabled via SmartAccess pol icy	Diagnostics
hdx_sm_ica_cpm_channel_di sabled	Total number of NS_ICA_CP M_CHANNEL disabled via SmartAccess pol icy	Diagnostics
hdx_sm_ica_lpt1_channel_di sabled	Total number of NS_ICA_LPT 1_CHANNEL disabled via SmartAccess pol icy	Diagnostics
hdx_sm_ica_lpt2_channel_di sabled	Total number of NS_ICA_LPT 2_CHANNEL disabled via SmartAccess pol icy	Diagnostics
dx_dbg_sm_ica_msi_disable d	Total number of cases where MSI is disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_file_channel_dis abled	Total number of NS_ICA_FIL E_CHANNEL is disabled via SmartAccess pol icy	Diagnostics
hdx_dbg_usb_accept_device	Total number of USB devices accepted	Diagnostics

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX COUNTER NAME	PURPOSE	CATEGORY(STATS/ERROR/ DIAGNOSTICS)
hdx_dbg_usb_reject_device	Total number of USB devices rejected	Diagnostics
hdx_dbg_usb_reset_endpoint	Total number of USB endpoints reset	Diagnostics
hdx_dbg_usb_reset_device	Total number of USB devices reset	Diagnostics
hdx_dbg_usb_stop_device	Total number of USB devices stopped	Diagnostics
hdx_dbg_usb_stop_device_response	Total number of responses from stopped USB devices	Diagnostics
hdx_dbg_usb_device_gone	Total number of USB devices gone	Diagnostics
hdx_dbg_usb_device_stopped	Total number of USB devices stopped	Diagnostics

nstrace validation

Check for CFLOW protocol to see all AppFlow records going out of NetScaler.

Population of records in NetScaler Console checklist

- Run the command `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"` and check logs to confirm NetScaler Console is receiving AppFlow records.
- Confirm NetScaler instance is added to NetScaler Console.
- Validate NetScaler Gateway/VPN virtual server is licensed in NetScaler Console.
- Make sure multi-hop parameter setting is enabled for double-hop.
- Make sure NetScaler Gateway is cleared for second-hop in double-hop deployment.

Before contacting Citrix technical support

For a speedy resolution, make sure that you have the following information before contacting Citrix technical support:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Details of the deployment and network topology.
- NetScaler and NetScaler Console versions.
- Citrix Virtual Apps and Desktops server versions.
- Client workspace versions.
- Number of Active ICA sessions when the issue occurred.
- Tech support bundle captured by running the `show techsupport` command at the NetScaler command prompt.
- Tech support bundle captured for NetScaler Console.
- Packet traces captured on all NetScaler. To start a packet trace, type, `start nstrace -size 0'` To stop a packet trace, type, `stop nstrace`
- Collect entries in the system's ARP table by running the `show arp` command.

Known Issues

Refer NetScaler release notes for known issues on HDX Insight.

Metrics information for thresholds

You can create thresholds and get it notified whenever the threshold value breaches. In a typical deployment, you can set thresholds to:

- Track various application metrics
- Facilitate planning
- Get notified whenever the applications metric value exceeds the set threshold

To configure threshold:

1. Navigate to **Settings > Analytics Settings > Thresholds**.
2. On the **Thresholds** page, click **Add**.

Web

METRICS	ENTITY	DESCRIPTION
Applications	Hits	Total number of hits received by a virtual server (application)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	ENTITY	DESCRIPTION
	Bandwidth (MB)	Total bandwidth consumed by the virtual server (application)
	Response Time (ms)	The time taken for the virtual server to respond
Clients	Requests	The total request received by a client
	Render Time (ms)	The time taken to render server response by the client
	Client Network Latency	The time taken for requests from the client network
Devices	Hits	Total number of hits received by a device. For example: laptop, mobile phone
	Bandwidth (MB)	Total bandwidth consumed by a device
Domains	Hits	Total number of hits received by a network domain
	Bandwidth (MB)	Total bandwidth consumed by a network domain
	Response Time (ms)	The time taken to respond requests by a network domain
Operating System	Hits	Total number of hits received by an operating system
	Bandwidth (MB)	Total bandwidth consumed by an operating system
	Render Time (ms)	The time taken to render server response by an operating system

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	ENTITY	DESCRIPTION
Request Methods	Hits	Total number of requests received by a Request Method. For example: GET, POST
	Bandwidth (MB)	Total bandwidth consumed by a Request Method
Response Status	Hits	Total number of hits received with response codes
	Bandwidth (MB)	Total bandwidth consumed by response code
Servers	Hits	Total number of requests/hits received by a server
	Bandwidth (MB)	Total bandwidth consumed by a server
	Server Network Latency (ms)	The time taken for requests from the server network
	Server Processing Time (ms)	The time taken by a server to respond to requests
URLs	Hits	Total number of hits received by a URL. For example: www.Citrix.com
	Load Time (ms)	The time taken for a URL to load from the server
	Render Time (ms)	The time taken by the URL to render and display
User Agents	Hits	Total number of requests received by a user agent. For example: Chrome web browser

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	ENTITY	DESCRIPTION
	Bandwidth (MB)	Total bandwidth consumed by the user agent
	Render Time (ms)	The time taken to render the server response by the user agent

Security

METRIC	ENTITY	DESCRIPTION
Applications	Threat Index	A single-digit rating system that indicates the criticality of attacks on the application. The more critical the attacks on an application, the higher the threat index for that application. The values range from 1 through 7.
	Safety Index	A single-digit rating system that indicates how securely you have configured the NetScaler instances to protect applications from external threats and vulnerabilities. The lower the security risks for an application, the higher the safety index. The values range from 1 through 7.

APPANALYTICS

METRIC	ENTITY	DESCRIPTION
Applications	AppScore	App Score defines how well an application is performing and shows whether the application is performing well

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIC	ENTITY	DESCRIPTION
		in terms of responsiveness. The values range from 0 to 80.

HDX™

For information on HDX thresholds, see Create thresholds and configure alerts for HDX Insight

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infrastructure

The NetScaler Console infrastructure features enable you to monitor and manage your NetScaler instances. You can analyze infrastructure health, manage instances and events, handle SSL certificates, run configuration and upgrade jobs, and provision instances across your network.

The following topics help you monitor and manage your infrastructure:

- Infrastructure Analytics
- Instance management
- Events
- SSL Dashboard
- Configuration
- Upgrade jobs
- Network functions
- Network reporting
- Provisioning
- Orchestration

Infrastructure Analytics

A key goal for network administrators is to monitor NetScaler instances. NetScaler instances offer interesting insights into usage and performance of applications and desktops accessed through it. Administrators must monitor the NetScaler instance and analyze the application flows processed by each NetScaler instance. Administrators must also be able to remediate any probable issues in configuration, setup, connectivity, certificates, and other impacts in application usage or performance. For example, a sudden change in application traffic pattern can be due to change in SSL configuration like disabling of an SSL protocol. Administrators must be able to quickly identify the correlation between these data points to ensure the following:

- Application availability is in an optimal state
- There are no resource consumption, hardware, capacity, or configuration change issues
- There are no unused inventories

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- There are no expired certificates

Infrastructure Analytics feature simplifies the process of data analysis by correlating multiple data sources and quantifying to a measurable score that defines the health of an instance. With this feature, administrators get a single touch point to understand the problem, the origin of the problem, and probable remediations that they can perform.

Infrastructure Analytics in NetScaler Console

The Infrastructure Analytics feature collates all the data gathered from the NetScaler instances and quantifies it into an **Instance Score** that defines the health of the instances. The instance score is summarized over tabular view or as circle pack visualization. The Infrastructure Analytics feature helps you to visualize the factors that resulted or might result in an issue on the instances. This visualization also helps you to determine the actions that must be performed to prevent the issue and its recurrence.

Instance score

Instance score indicates the health of an NetScaler instance. A score of 100 means a perfectly healthy instance without any issues. Instance score captures different levels of potential issues on the instance. It is a quantifiable measurement of instance health and multiple "health indicators" contribute to the score.

Health indicators are the building blocks of the instance score, where the score is computed periodically for a predefined "monitoring period," based on all detected indicators in that time window. Currently, Infrastructure analytics calculates the instance score once every hour based on the data collected from the instances. An indicator can be defined as any activity (an event or an issue) that belongs to one of the following categories on the instances.

- System resource indicators
- Critical events indicators
- SSL configuration indicators
- Configuration deviation indicators

Health indicators explained

- System resources indicators

  The following are the critical system resource issues that might occur on NetScaler instances and monitored by NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **High CPU usage**. The CPU usage has crossed the higher threshold value in the NetScaler instance.
- **High memory usage**. The memory usage has crossed the higher threshold value in the NetScaler instance.
- **High disk usage**. The disk usage has crossed the higher threshold value in the NetScaler instance.
- **Disk errors**. There are errors on hard disk 0 or hard disk 1 on the hypervisor where the NetScaler instance is installed.
- **Power failure**. The power supply has failed or disconnected from the NetScaler instance.
- **SSL card failure**. The SSL card installed on the instance has failed.
- **Flash errors**. There are Compact Flash Errors seen on the NetScaler instance.
- **NIC discards**. The packets discarded by the NIC card have crossed the higher threshold value in the NetScaler instance.

For more information on these system resources errors, see Instance dashboard.

- Critical events indicators

  The following critical events are identified by the events under event management feature of NetScaler Console that are configured with critical severity.

  - **HA sync failure**. Configuration sync between the NetScaler instances in high availability has failed on the secondary server.
  - **HA no heartbeats**. The primary server in a pair of NetScaler instances in high availability is not receiving heart beats from the secondary server.
  - **HA bad secondary state**. The secondary server in a pair of NetScaler instances in high availability is in Down, Unknown, or Stay secondary state.
  - **HA version mismatch**. The version of the NetScaler software images installed on a pair of NetScaler instances in high availability does not match.
  - **Cluster sync failure**. Configuration sync between the NetScaler instances in cluster mode has failed.
  - **Cluster version mismatch**. The version of the NetScaler software images installed on the NetScaler instances in cluster mode does not match.
  - **Cluster propagation failure**. Propagation of configurations to all instances in a cluster has failed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

You can have your list of critical SNMP events by changing the severity levels of the events. For more information on how to change the severity levels, see Modify the reported severity of events that occur on NetScaler instances.

For more information on events in NetScaler Console, see Events.

- SSL configuration indicators
  - **Not recommended key strength**. The key strength of the SSL certificates is not as per NetScaler® standards
  - **Not recommended issuer**. The issuer of the SSL certificate is not recommended by Citrix.
  - **SSL certs expired**. The SSL certificate installed in the NetScaler instance has expired.
  - **SSL certs expiry due**. The SSL certificate installed in the NetScaler instance is about to expire in the next one week.
  - **Not recommended algorithms**. The signature algorithms of SSL certificates installed in the NetScaler instance are not as per NetScaler standards.

For more information on SSL certificates, see SSL dashboard.

- Configuration deviation indicators
  - **Config drift template**. There is a drift (unsaved changes) in configuration from the audit templates that you have created with specific configurations you want to audit on certain instances.
  - **Config drift default**. There is a drift (unsaved changes) in configuration from the default configuration files.

For more information on configuration deviations and how to run audit reports to check configuration deviation, see View audit reports..

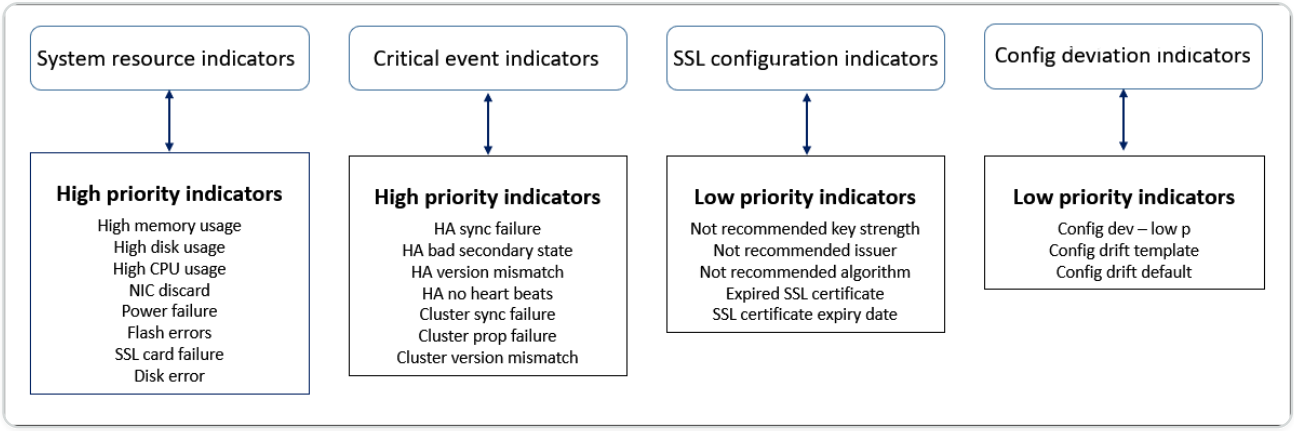
View NetScaler Capacity issues

When a NetScaler instance has consumed most its available capacity, packet-drop might occur while processing the client traffic. By understanding such NetScaler capacity issues, you can proactively allocate additional licenses to steady the NetScaler performance. For more information, see View the capacity issues in a NetScaler instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Value of health indicators

The indicators are classified into high priority indicators and low-priority indicators based on their values as follows:



The health indicators within the same group of indicators have different weights assigned to them. One indicator might contribute more to lowered instance score than another indicator. For example, high memory usage brings down the instance score more than high disk usage, high CPU usage, and NIC discard. If an instance has a greater number of indicators detected on it, the lesser is the instance score.

The value of an indicator is calculated based on the following rules. The indicator is said to be detected in one of the following three ways:

1. **Based on an activity**. For example, a System resource indicator is triggered whenever there is a power failure on the instance, and this indicator reduces the value of the instance score. When the indicator is cleared the penalty is cleared, and the instance score increases.
2. **Based on the threshold value breach**. For example, a System resource indicator is triggered when the NIC card discards packets and the threshold level is breached.
3. **Based on the low and high threshold value breach**. Here, an indicator can be triggered in two ways:
    - When the value of the indicator is between low and high thresholds, in which case a partial penalty is levied on the instance score.
    - When the value crosses the high threshold, in which case a full penalty is levied on the instance score.
    - No penalty is levied on the instance score if the value falls below a low threshold.

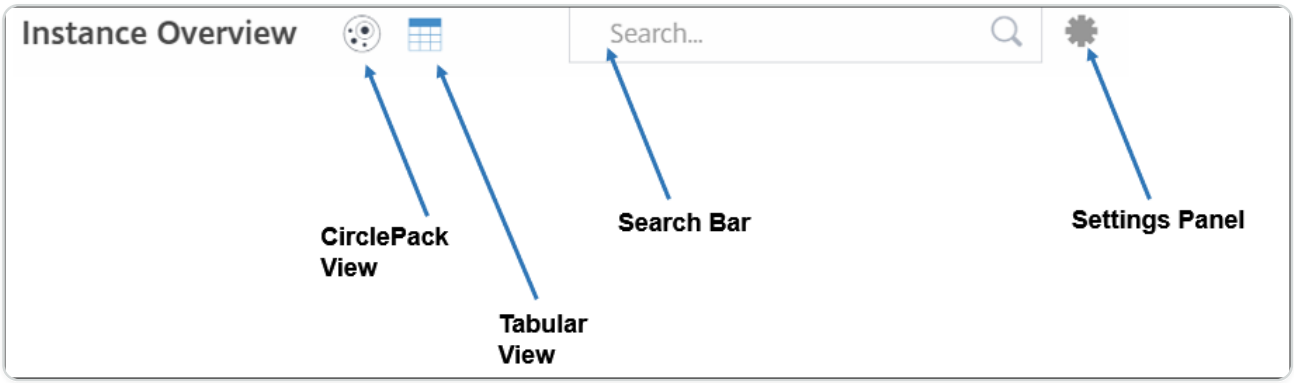
For example, CPU usage is a system resource indicator triggered when the usage value crosses the low threshold and also when the value crosses the high threshold.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infrastructure analytics dashboard

Navigate to **Infrastructure > Infrastructure Analytics**.

The Infrastructure Analytics can be viewed in a **Circle Pack** format or a **Tabular** format. You can toggle between the two formats.

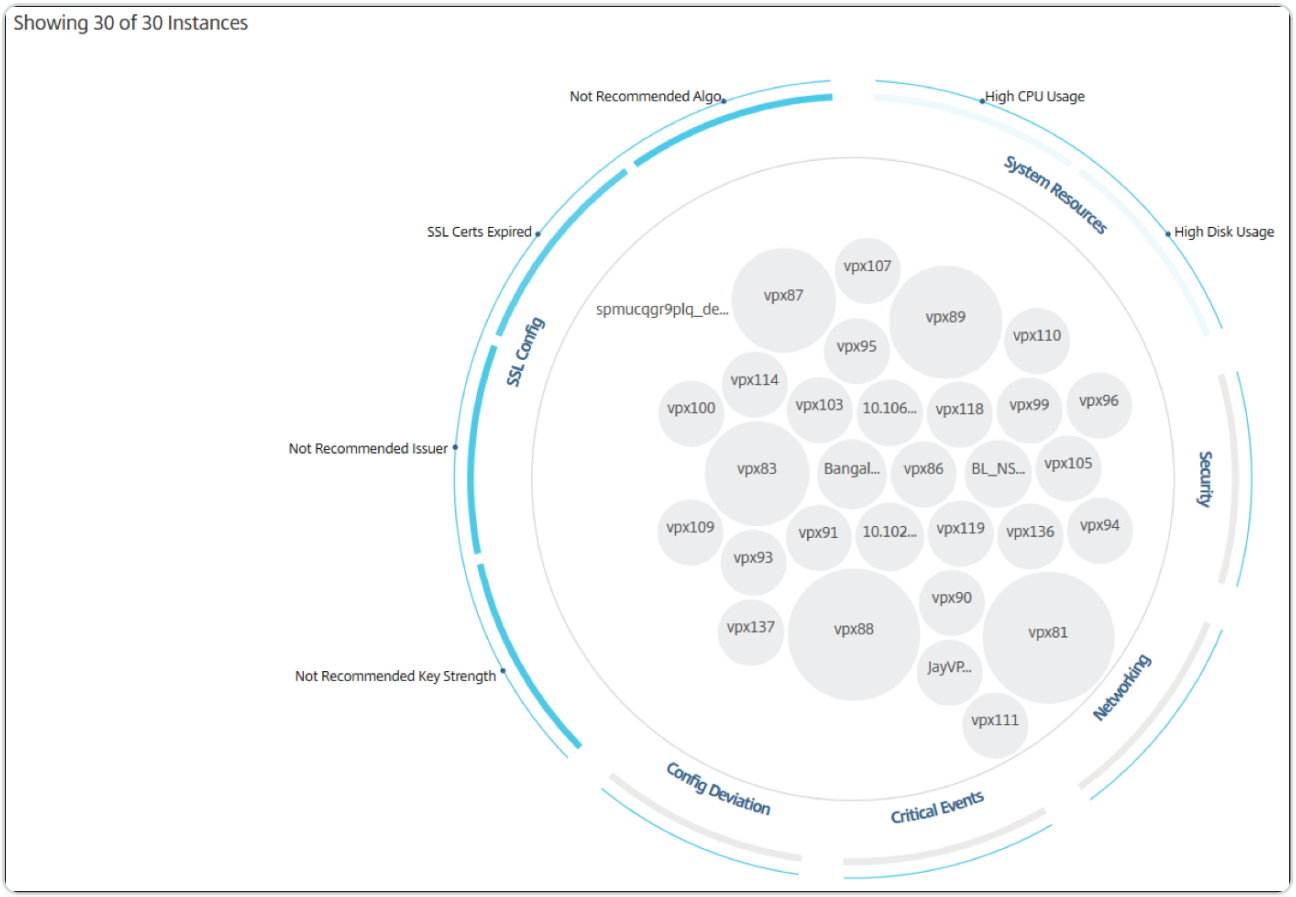


- In the Tabular view, you can search for an instance by typing the host name or the IP address in the Search bar.
- By default, Infrastructure Analytics page displays the Summary Panel on the right side of the page.
- Click the **Settings** icon to display the **Settings** Panel.
- In both the view formats, the Summary Panel displays details of all the instances in your network.

Circle pack view

Circle packing diagrams show instance groups as tightly organized circles. They often show hierarchies where smaller instance groups are either colored similarly to others in the same category, or nested within larger groups. Circle packs represent hierarchical data sets and shows different levels in the hierarchy and how they interact with each other.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Instance circles

Color. Each instance is represented in Circle Pack as a colored circle. The color of the circle indicates the health of that instance.

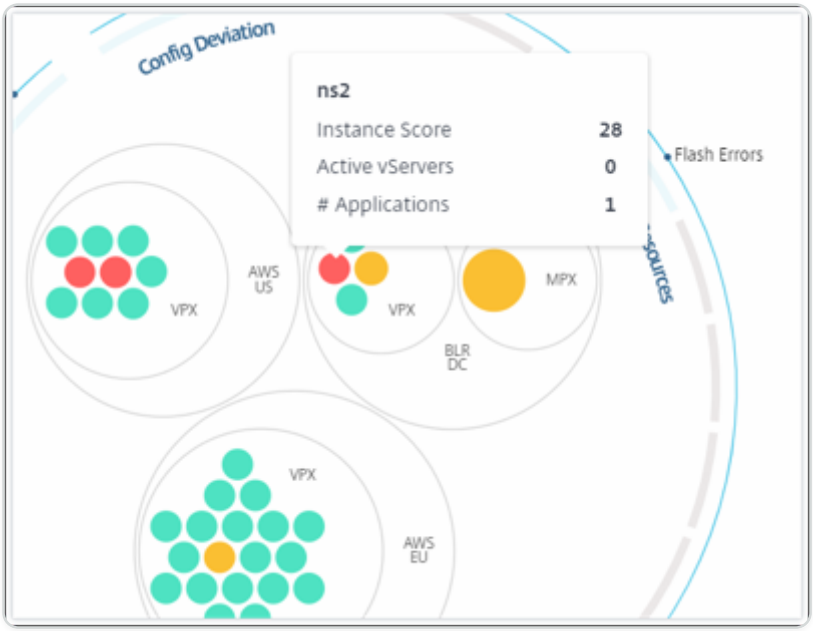
- **Green** - instance score is between 100 and 80. The instance is healthy.
- **Yellow** - instance score is between 80 and 50. Some issues have been noticed and in need of review.
- **Red** - instance score is below 50. The instance is in a critical stage as there are multiple issues noticed on that instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Size. The size of these colored circles indicates the number of virtual servers configured on that instance. A bigger circle indicates that there are a greater number of virtual servers.

You can hover the mouse pointer on each of the instance circles (colored circles) to view a summary. The hover tool tip displays the host name of the instance, the number of active virtual servers and the number of applications configured on that instance.



Grouped instance circles

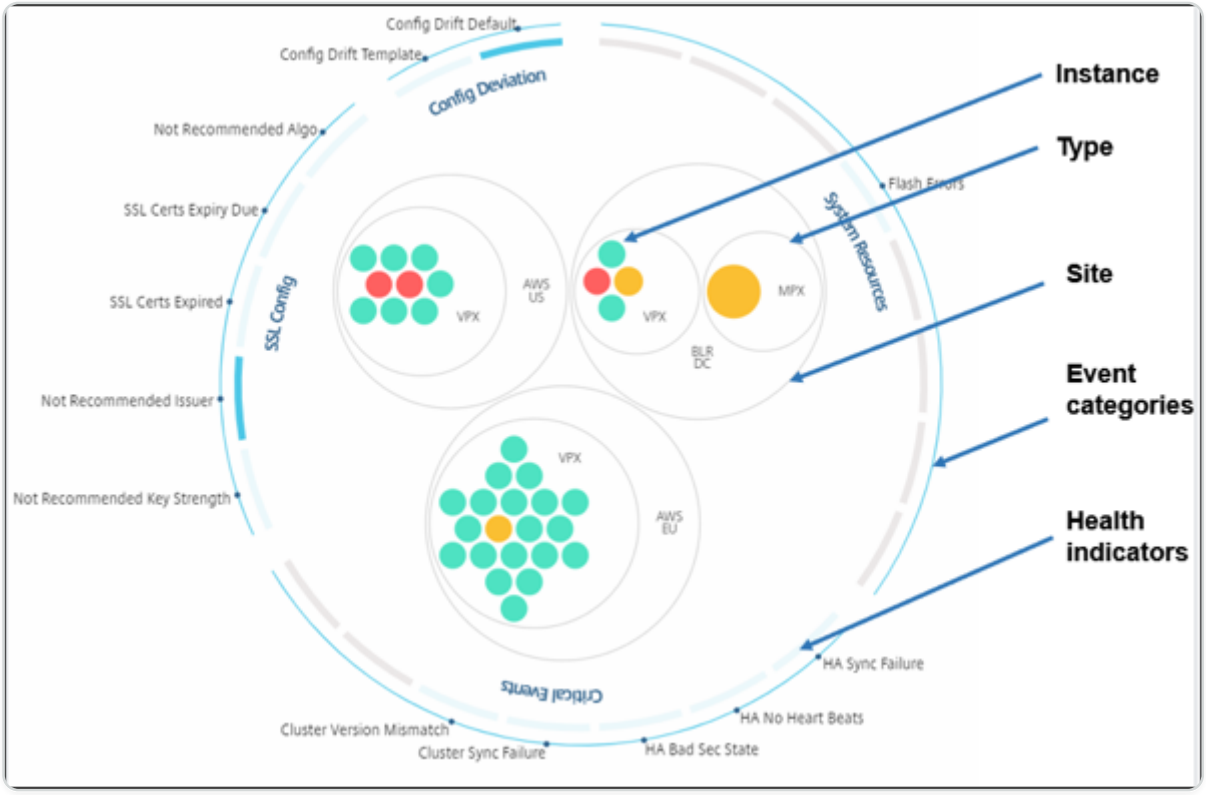
The Circle Pack at the outset, comprises instance circles that are grouped, nested, or packed inside another circle based on the following criteria:

- the site where they are deployed
- the type of instances deployed - VPX, MPX, SDX, and CPX
- the virtual or physical model of the NetScaler instance

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- the NetScaler image version installed on the instances

The following image shows a Circle Pack where the instances are first grouped by the site or data center where they are deployed, and then they are further grouped based on their type, VPX, and MPX.



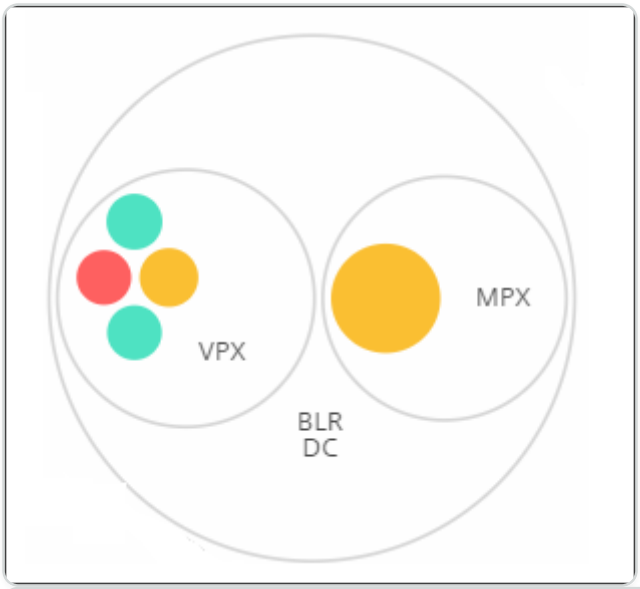
All these nested circles are bounded by two outermost circles. The outer two circles represent the four categories of events monitored by the NetScaler Console (system resources, critical events, SSL configuration, and configuration deviation) and the contributing health indicators.

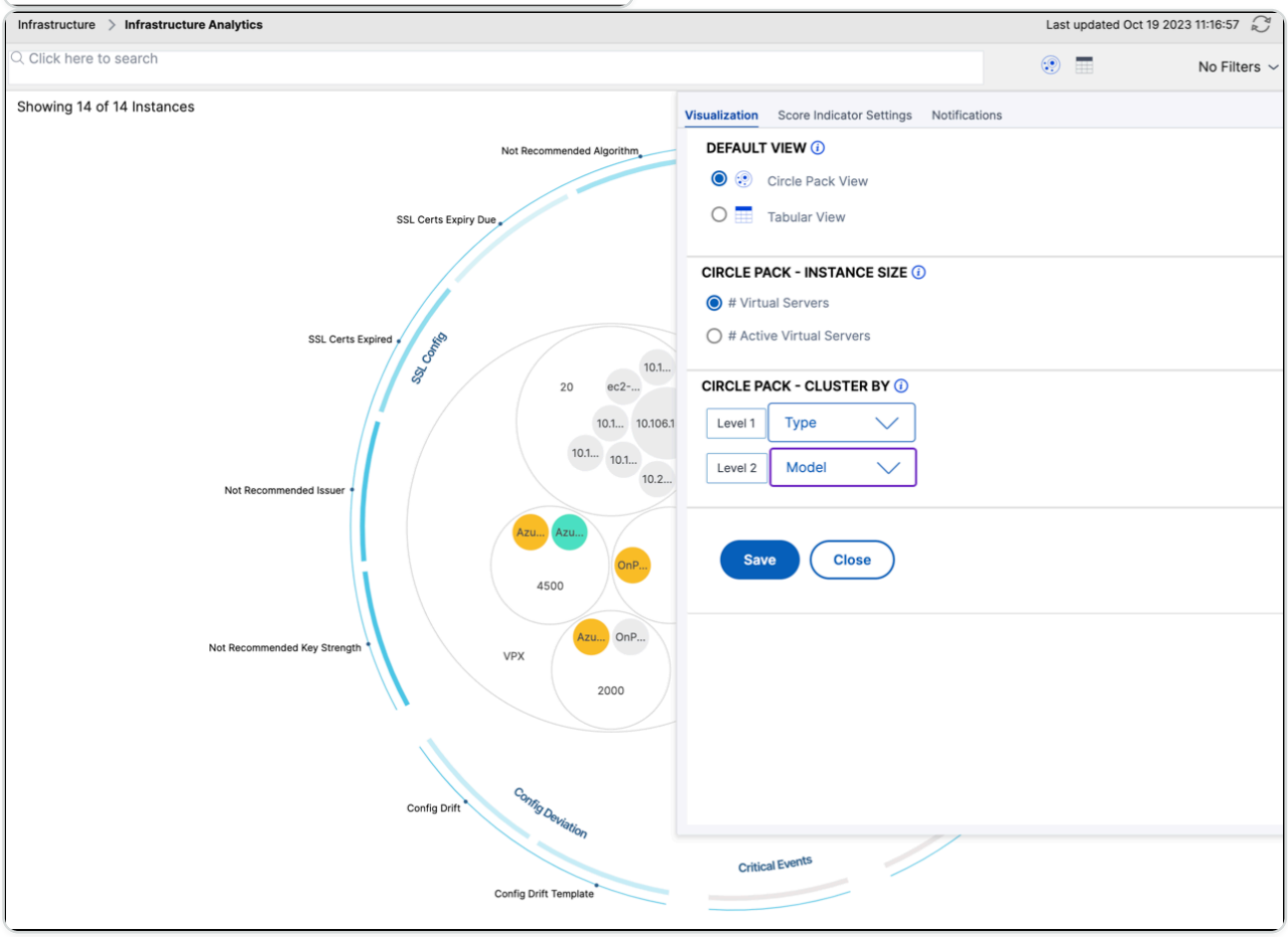
Clustered instance circles

NetScaler Console monitors many instances. To ease the monitoring and maintenance of these instances, Infrastructure Analytics allows you to cluster them at two levels. That is, the instance groupings can be nested within another grouping.

For example, the BLR data center has two types of NetScaler instances - VPX and MPX, deployed in it. You can first group the NetScaler instances by their type and then group all instances by the site where they are grouped. You can now easily identify how many types of instances are deployed in the sites that you are managing.

© 1997–2026 Citrix Systems, Inc. All rights reserved.





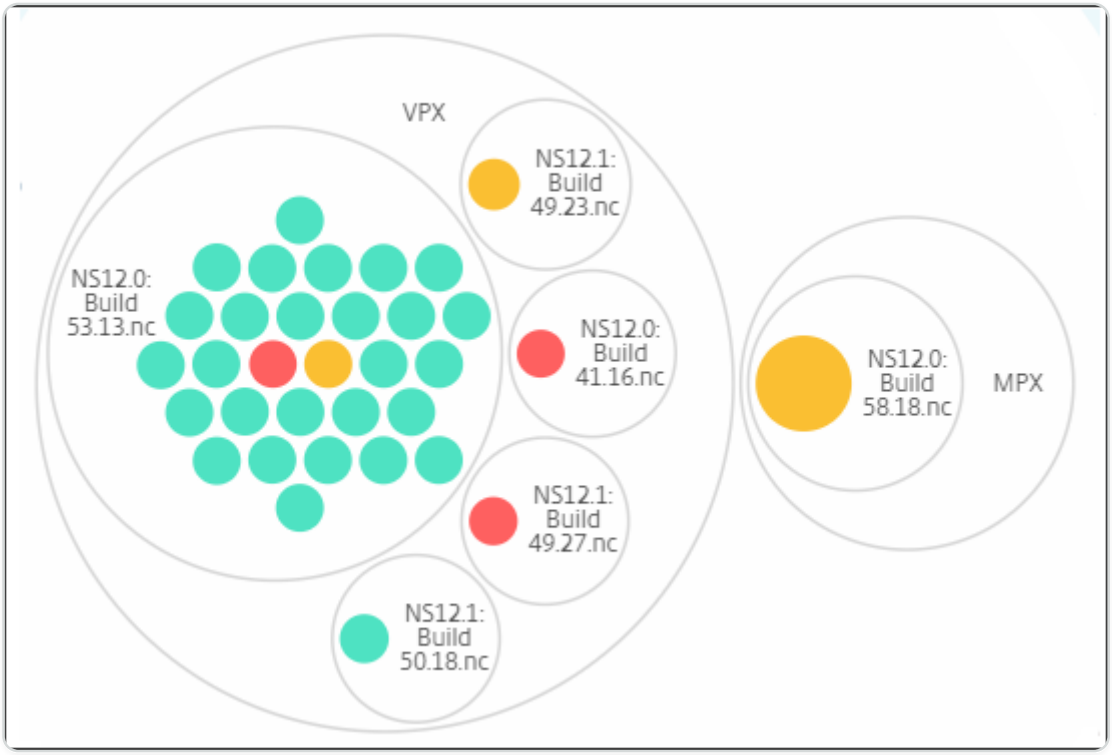
A few more examples of two-level clustering are as follows:

Site and model:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

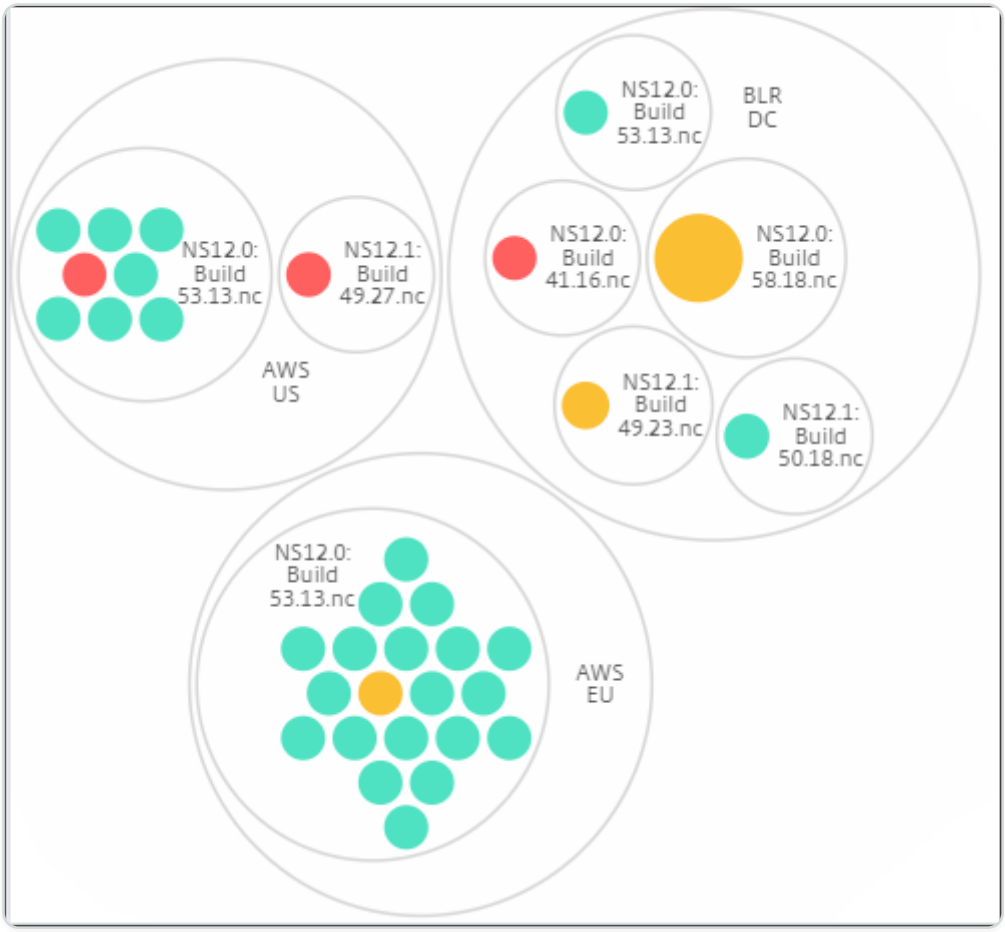


Type and version:



Site and version:

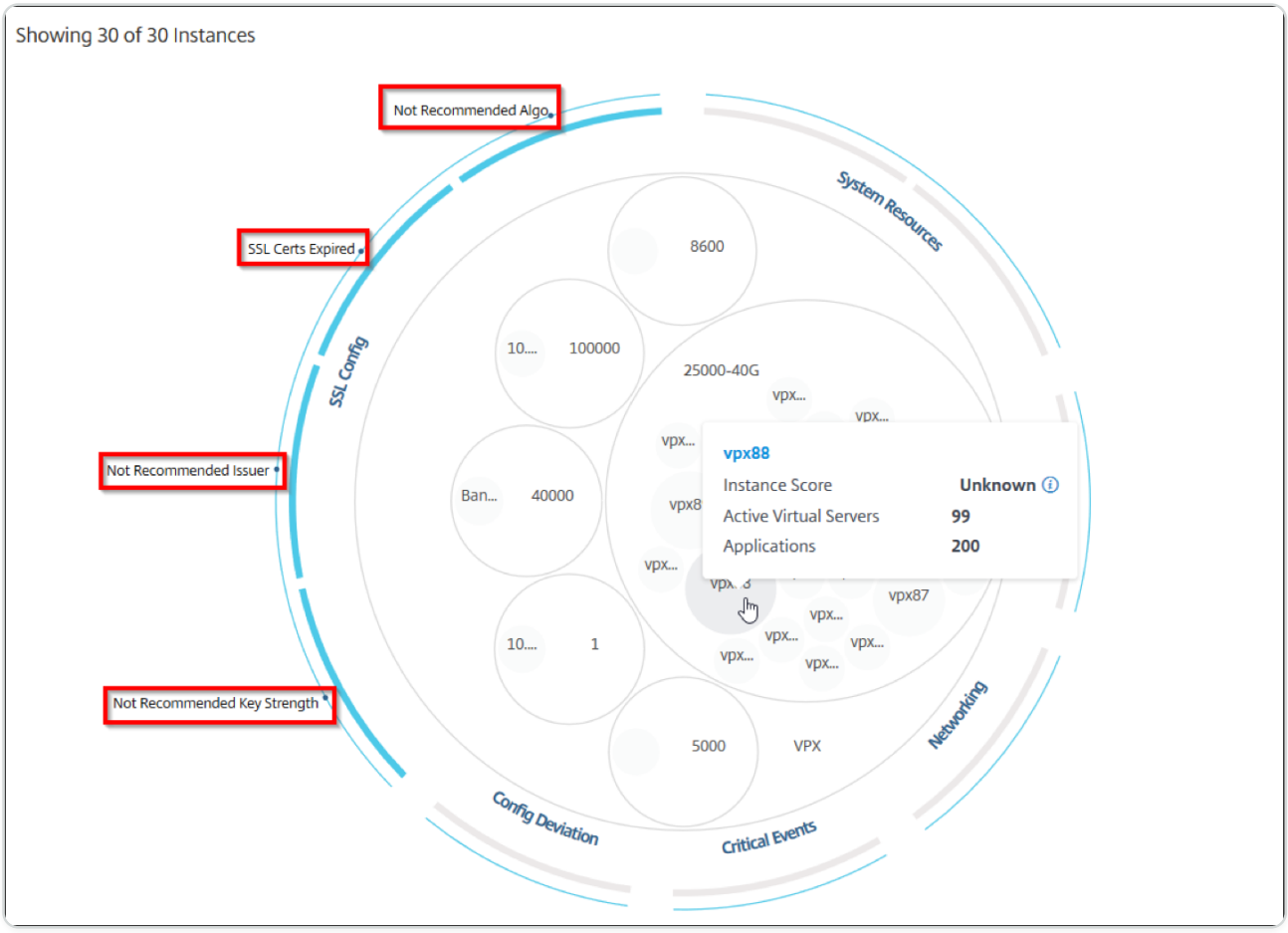
© 1997–2026 Citrix Systems, Inc. All rights reserved.



How to use Circle Pack

Click each of the colored circle to highlight that instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

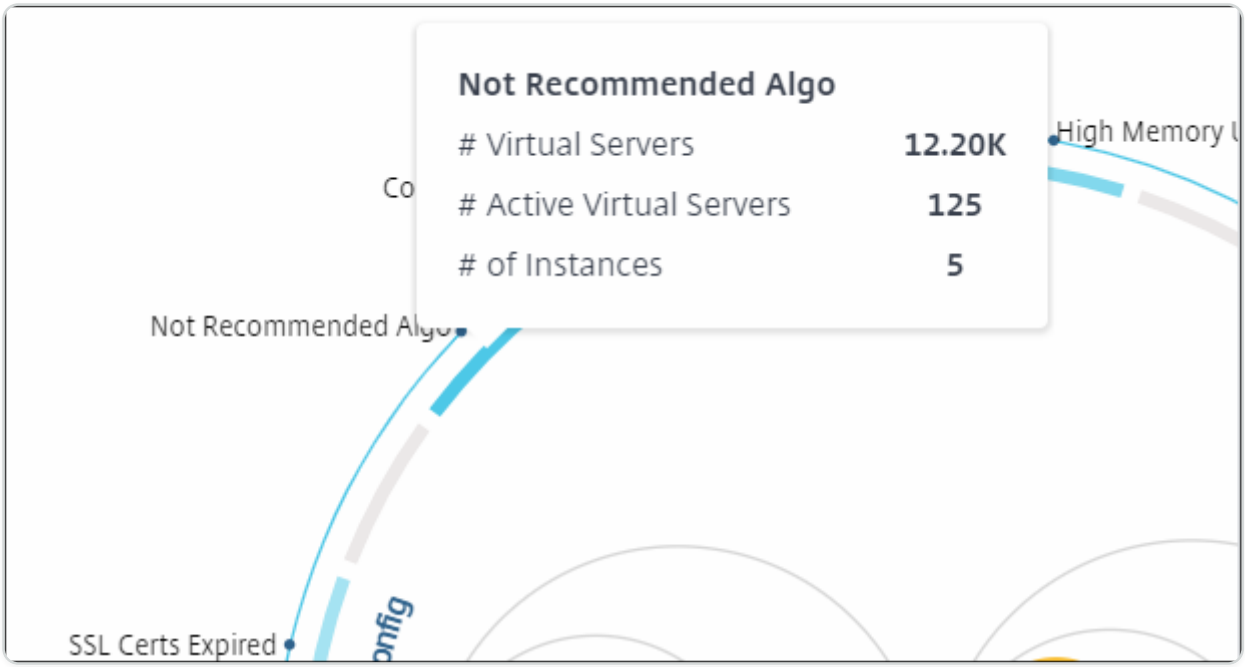


Depending on the events that have occurred in that instance, only those health indicators are highlighted on the outer circles. For example, the following two images of the Circle Pack display different sets of risk indicators, though both instances are in a critical state.



You can also click the health indicators to get more details on the number of instances that have reported that risk indicator. For example, click `Not recommended Algo` to view the summary report of that risk indicator.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



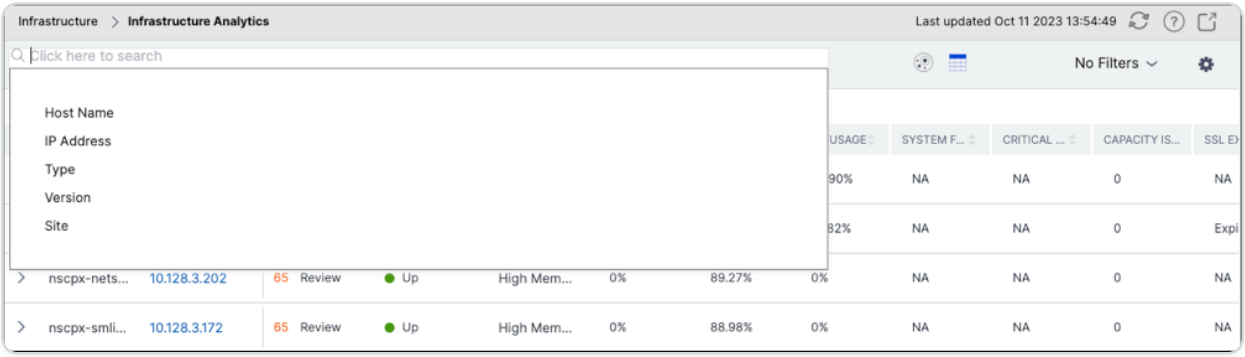
Tabular view

The tabular view displays the instances and the details of those instances in a tabular format. For more information, see Instance details

Search bar

Place the mouse cursor on the search bar and select the following search attributes to filter the results:

- Host name
- IP address
- Type
- Version
- Site



The search results work for both circle view and table view.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How to use the Summary Panel

The **Summary Panel** assists you in efficiently and quickly focuses on the instances that are in need of review or critical state. The panel is divided into three tabs - overview, instance info, and traffic profile. The changes you make in this panel modifies the display in both Circle Pack and Tabular view formats. The following sections describe these tabs in more detail. The examples in the following sections assist you to use the different selection criteria efficiently to analyze the issues reported by the instances.

Overview:

The **Overview** tab allows you to monitor the instances based on the hardware errors, usage, expired certificates and similar indicators that can occur in the instances. The indicators that you can monitor here are as follows:

- CPU usage
- Memory usage
- Disk usage
- System failures
- Critical events
- SSL certificates expiry

For more information on these indicators, see *Health indicators in NetScaler instances*.

The following examples illustrate how you can interact with the **Overview** panel to isolate those instances that are reporting errors.

Example 1: View instances that are in a review state:

Select **Review** check box to view only those instances that are not reporting critical errors, but still needs attention.

The Histograms in the **Overview** panel represent an aggregated number of instances based on high CPU usage, high memory usage, and high disk usage events. The Histograms are graded at 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90%, and 100%. Hover your mouse pointer on one of the bar charts. The legend at the bottom of the chart displays the usage range and the number of instances in that range. You can also click the bar chart to display all the instances in that range.

Example 2: View instances that are consuming between 10% and 20% of the allocated memory:

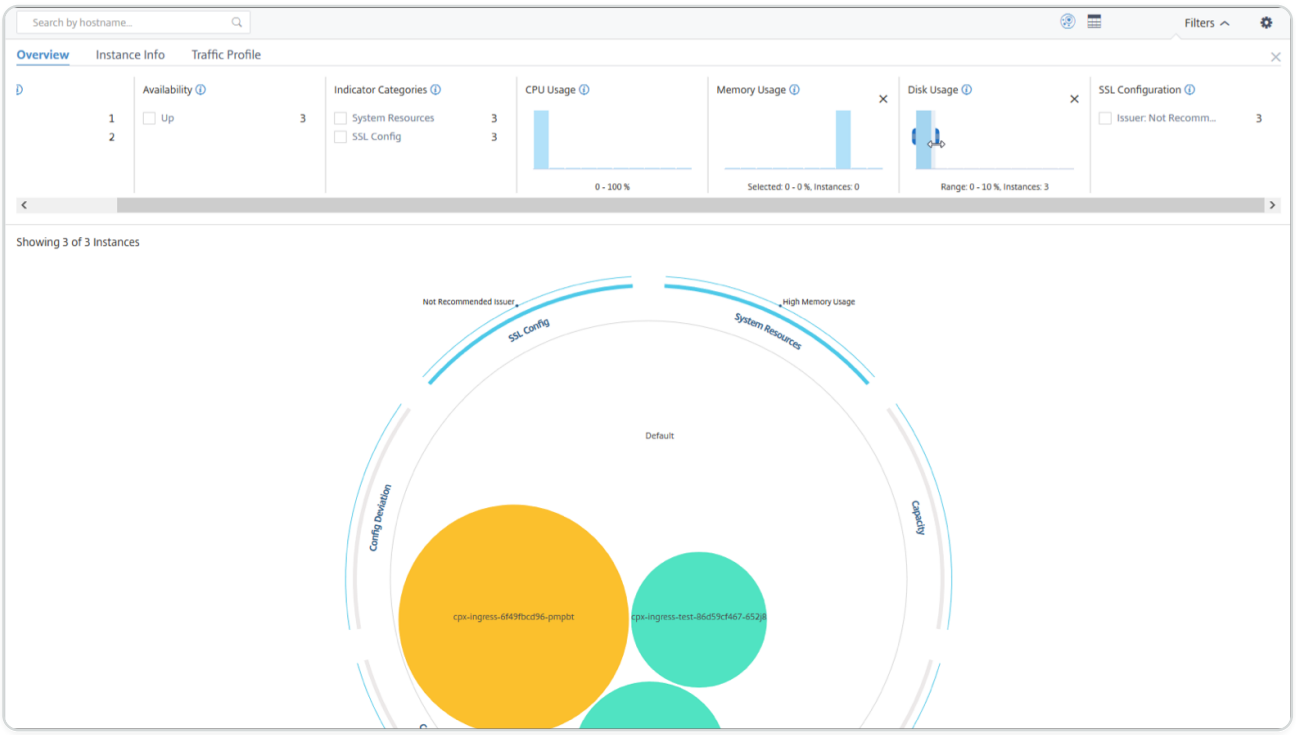
© 1997–2026 Citrix Systems, Inc. All rights reserved.

In the memory usage section, click the bar chart. The legend shows that the selected range is 10–20% and there are 29 instances operating in that range.

You can also select multiple ranges in these histograms.

Example 3: View instances that are consuming disk space in multiple ranges:

To view instances that have consumed memory between 0% and 10% disk space, drag the mouse pointer over the two ranges as shown in the following image.



NOTE:

Click "X" to remove the selection. You can also click **Reset** to remove multiple selections.

The horizontal bar charts in the **Overview** panel indicate the number of instances that report system errors, critical events, and expiry status of the SSL certificates. Select the check box to view those instances.

Example 4: View instances for expired SSL certificates:

In the **SSL certificates expiry** section, select **Expired** check box to view the three instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1 - Click the **Filter** list.

2 - In the **SSL certificates expiry** section, select **Expired** check box to view the instances.

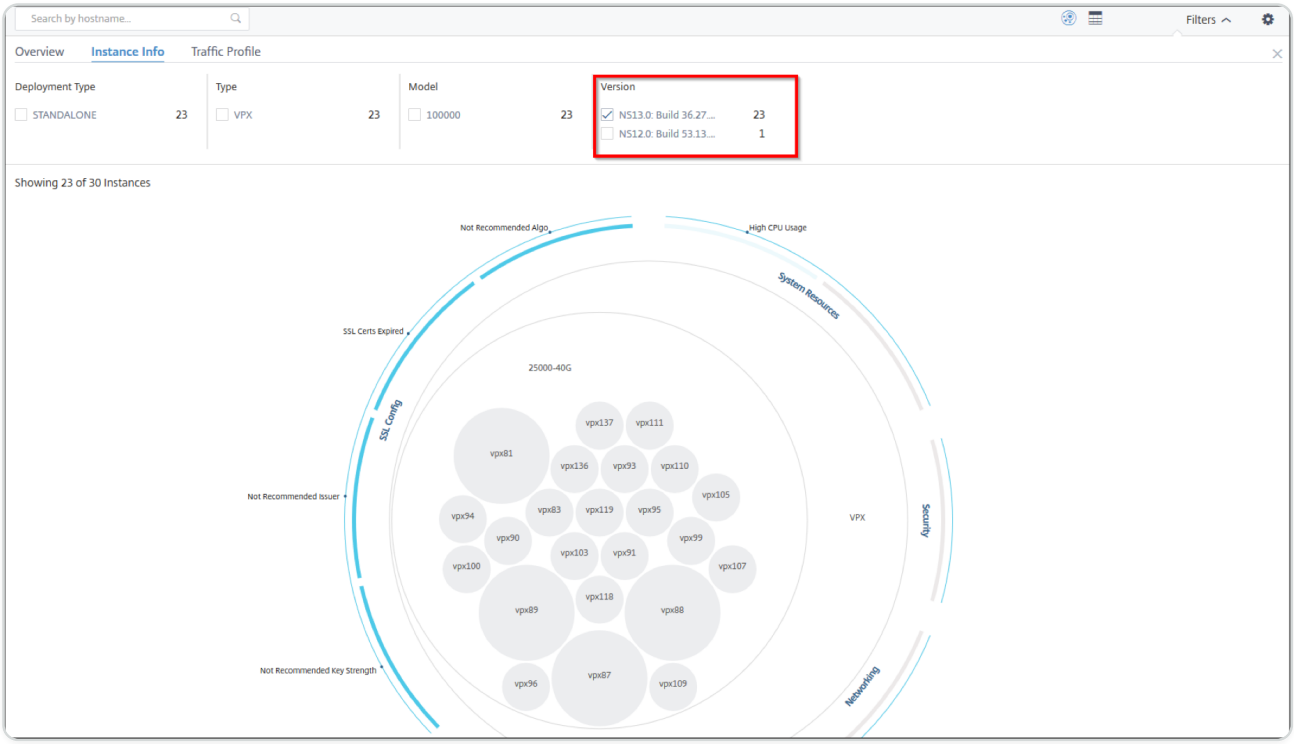
Instance info

The **Instance Info** panel allows you to view instances based on the type of deployment, instance type, model, and software version. You can select multiple check boxes to narrow down your selection.

Example 5: View NetScaler VPX instances with specific build number:

Select the version that you want to view.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

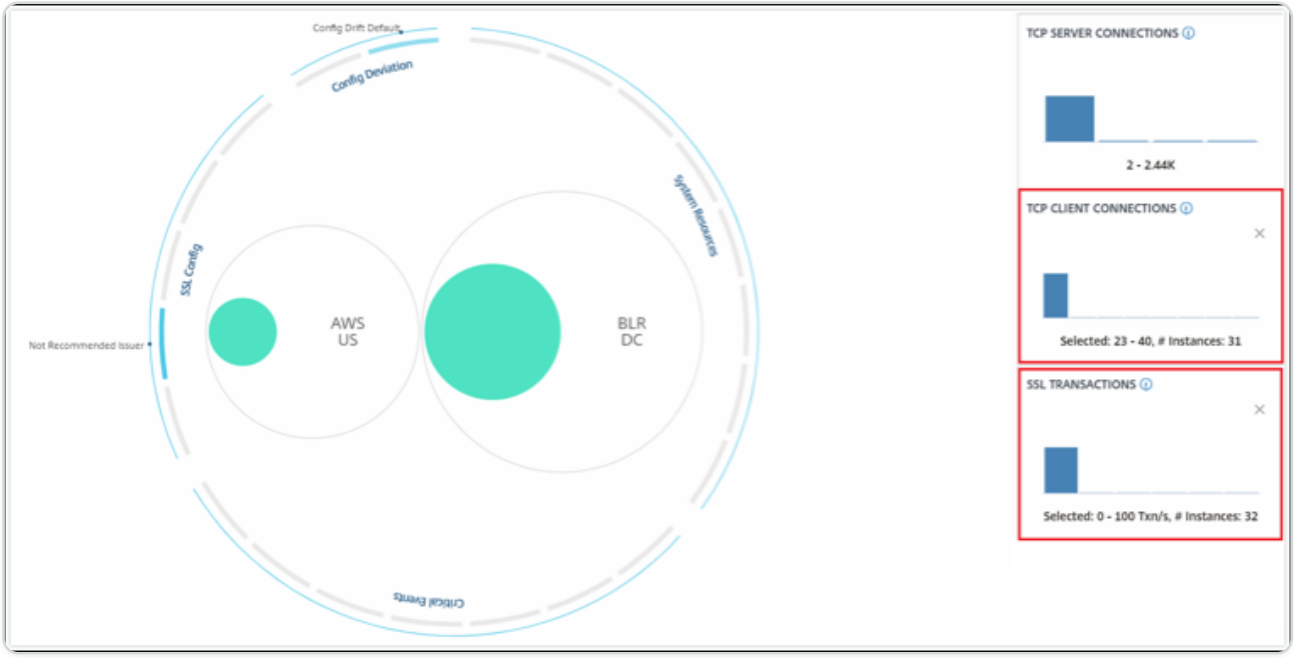


Traffic profile

The Histograms in the **Traffic profile** panel represent an aggregated number of instances based on the licensed throughput on the instances, number of requests, connections, and transactions handled by the instances. Select the bar chart to view instances in that range.

Example 6: View instances supporting TCP connections:

The following image shows the number of instances supporting TCP connections between 23 and 40, and also processing up to 100 SSL transactions per second.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

How to use the settings panel

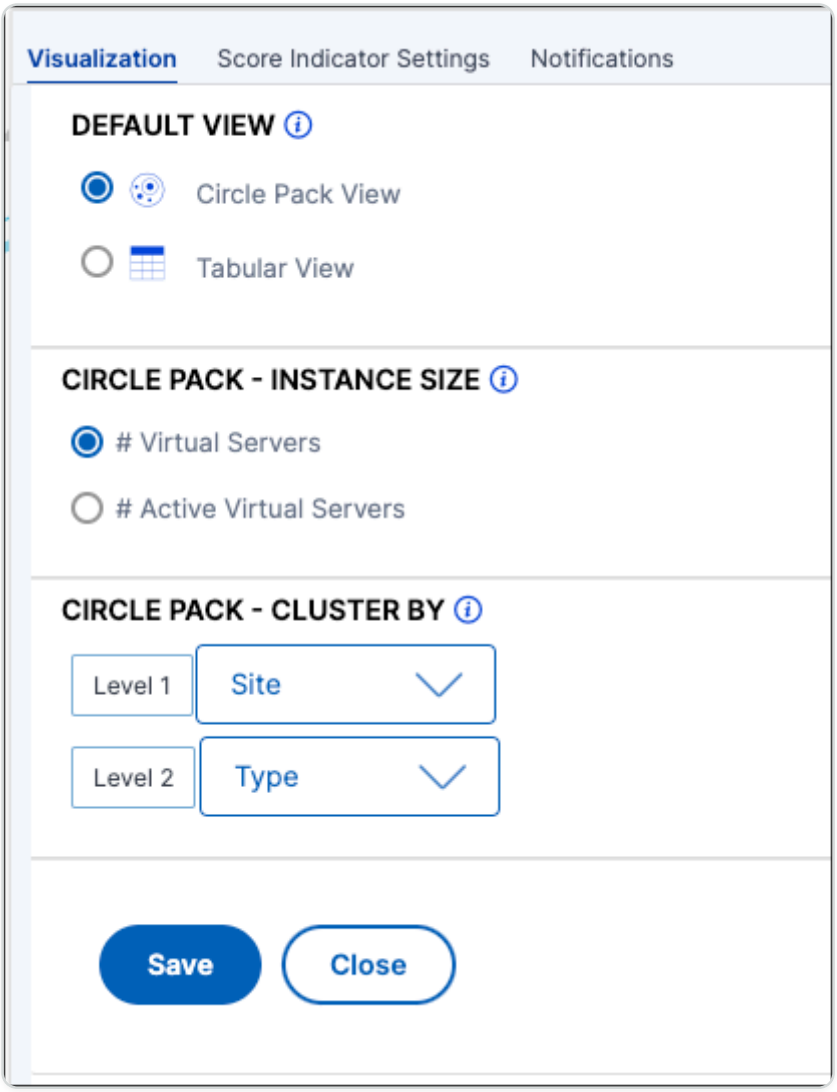
The **Settings** panel allows you to:

- Set the default view of the Infrastructure Analytics.
- Set the low and high threshold values for high CPU usage, high disk usage, and high memory usage.
- Select the instance metrics, configure thresholds, and assign weightage for those metrics to calculate the instance score
- Select the required issues, enable notifications for issues that breach the configured thresholds, and receive notifications only for the selected issues.

View

- **Default View**. Select **Circle Pack** or Tabular format as the default view on the analytics page. The format you select is what you see whenever you access the page in NetScaler Console.
- **Circle Pack - Instance Size**. Allow the size of the instance circle to by either the number of virtual servers or the number of active virtual servers.
- **Circle Pack - Cluster By**. Decide the two-level clustering of the instance circles. For more information on instance clustering, see Clustered instance circles.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Select metrics and customize weightage for instance score calculation

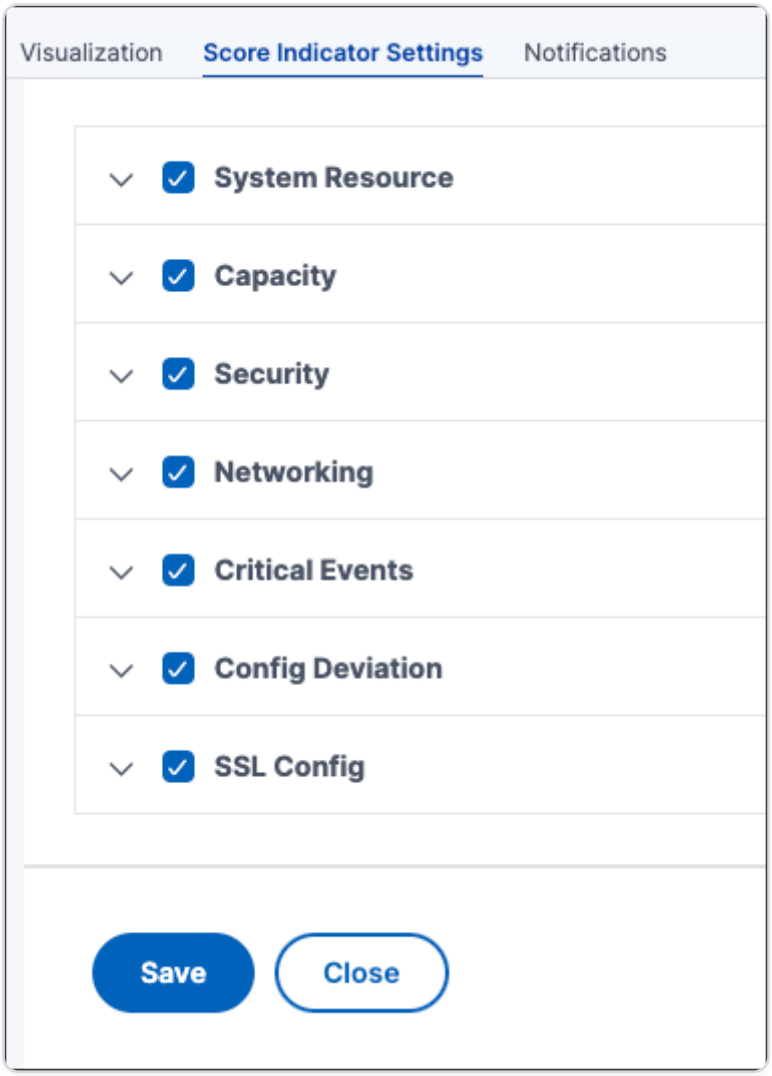
You can select the instance metrics, configure thresholds, and assign weightage for those metrics to calculate the instance score. By default, all metrics are selected, and default weightage is assigned to each metric. You can select metrics depending upon your requirement and assign a suitable weightage to determine the instance score calculation.

Click the **Settings** icon and select the **Score Indicator Settings** tab to:

- Select the required metrics and add thresholds
- Assign the weightage for metrics.

After you configure thresholds and assign weightage, click **Save**. The instance score is updated only based on the selected metrics and their weightage.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Configure notifications

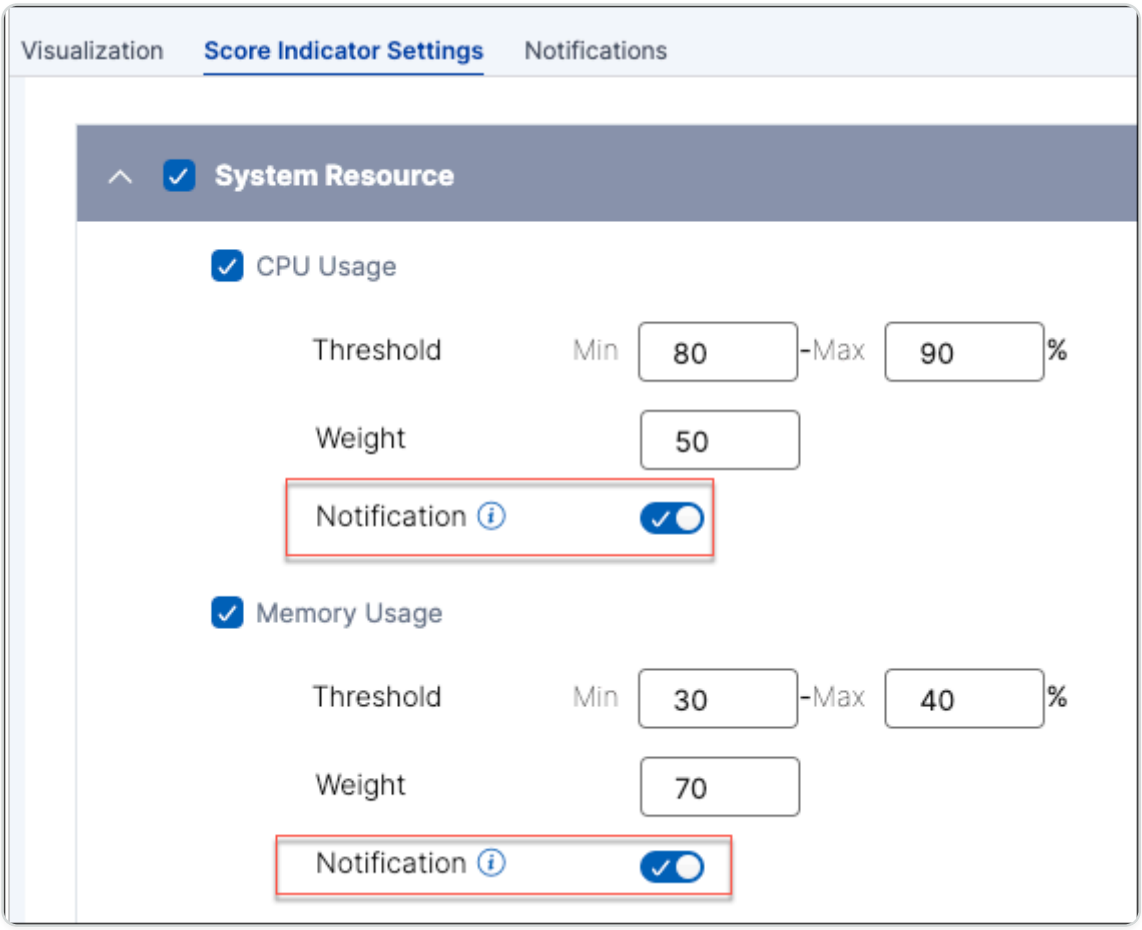
You can select the required issues, enable notifications for issues that breach the configured thresholds, and receive notifications only for the selected issues. This enhancement enables you to receive notifications only for the selected issues that you want to monitor.

NOTE:

By default, issues under all categories are selected. You can enable notification only for the issues that you can configure thresholds.

1. Click the **Settings** icon and select the **Score Indicator Settings** tab.
2. Select the issues that you want to receive notifications.
3. For the issues under **System Resource** and **Capacity** categories, enable the **Notification**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Click **Save**.

NOTE:

You must ensure to configure at least one profile in the **Notifications** tab.

How to visualize data on the dashboard

Using Infrastructure Analytics, network admins can now identify instances needing the most attention within a few seconds. To understand this in more detail, let us consider the case of Chris, a network admin of ExampleCompany.

Chris maintains many NetScaler instances in his organization. A few of the instances process high traffic, and he needs to monitor them closely. He notices that a few high-traffic instances are no longer processing the full traffic passing through them. To analyze this reduction, earlier, he had to read multiple data reports coming in from various sources. Chris had to spend more time trying to correlate the data manually and find out which instances are not in optimal state and need attention. He uses the Infrastructure Analytics feature to see the health of all instances visually.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The following two examples illustrate how Infrastructure Analytics assists Chris in maintenance activity:

Example 1 - To monitor the SSL traffic:

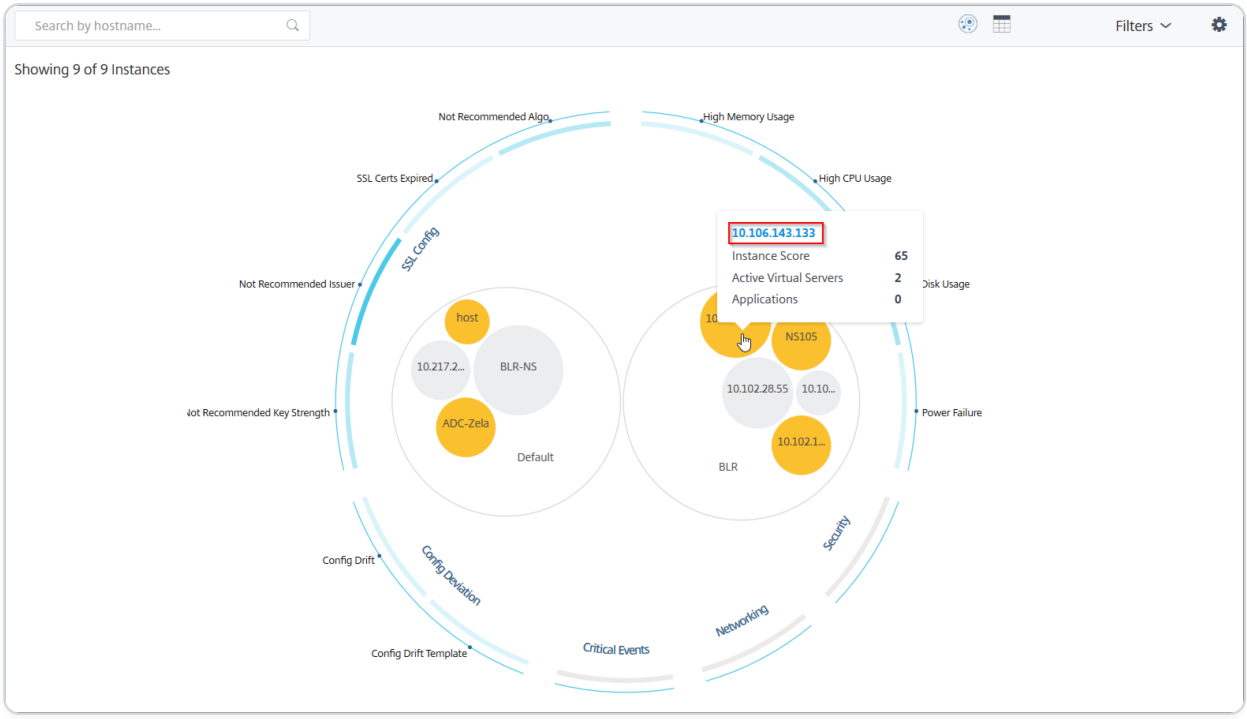
Chris notices on the Circle Pack that one instance has a low instance score and that instance is in "Critical" state. He clicks the instance to see what the issue is. The instance summary displays that there is an SSL card failure on that instance and therefore that instance is unable to process SSL traffic (the SSL traffic has reduced). Chris extracts that information and sends a report to the team to look into the issue immediately.

Example 2 - To monitor configuration changes:

Chris also notices that another instance is in "Review" state and that there has been a config deviation recently. When he clicks the config deviation risk indicator, he notices that RC4 Cipher, SSL v3, TLS 1.0, and TLS 1.1 related configuration changes have been made which might be due to security concerns. He also notices that the SSL transaction traffic profile for this instance has gone down. He exports this report and sends it to the admin to inquire further.

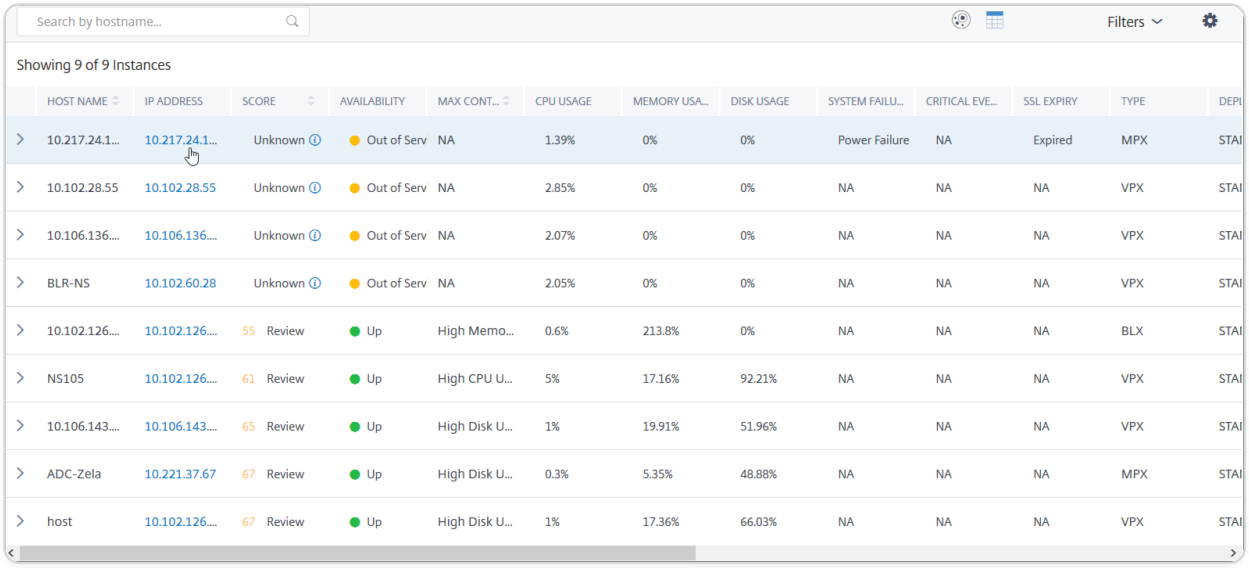
View instance details in Infrastructure Analytics

1. Navigate to **Infrastructure > Infrastructure Analytics**.
2. Click the circle pack view and select the IP address.



You can also click an IP address from the table view.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Host name** – Denotes the host name assigned to the NetScaler instance
- **IP address** – Denotes the IP address of the NetScaler instance
- **Score** – Denotes the NetScaler instance score and the status such as Critical, Good, and Fair
- **Availability** – Denotes the current status of the NetScaler instance such as **Up**, **Down**, or **Out of service**.
- **Max Contribution** – Denotes the issue category that the NetScaler instance has the maximum error counts.
- **CPU usage** – Denotes the current CPU % used by the instance
- **Memory usage** – Denotes the current memory % used by the instance
- **Disk usage** – Denotes the current disk % used by the instance
- **System Failure** – Denotes the total number of errors for the instance system
- **Critical Events** – Denotes the event category that the NetScaler instance has the maximum events
- **SSL expiry** – Denotes the current status of the SSL certificate installed on the NetScaler instance
- **Type** – Denotes the NetScaler instance type such as VPX, SDX, MPX, or CPX
- **Deployment** – Denotes if the NetScaler instance is deployed as a standalone instance or HA pair
- **Model** – Denotes the NetScaler instance model number
- **Version** – Denotes the NetScaler instance version and build number
- **Throughput** – Denotes the current network throughput from the NetScaler instance

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **HTTPS request/sec** – Denotes the current HTTPS requests/sec received by the NetScaler instance
- **TCP connection** – Denotes the current TCP connections established
- **SSL transaction** – Denotes the current SSL transactions processed by the NetScaler instance
- **Site** – Denotes the name of the site that the NetScaler instance is deployed.

NOTE:

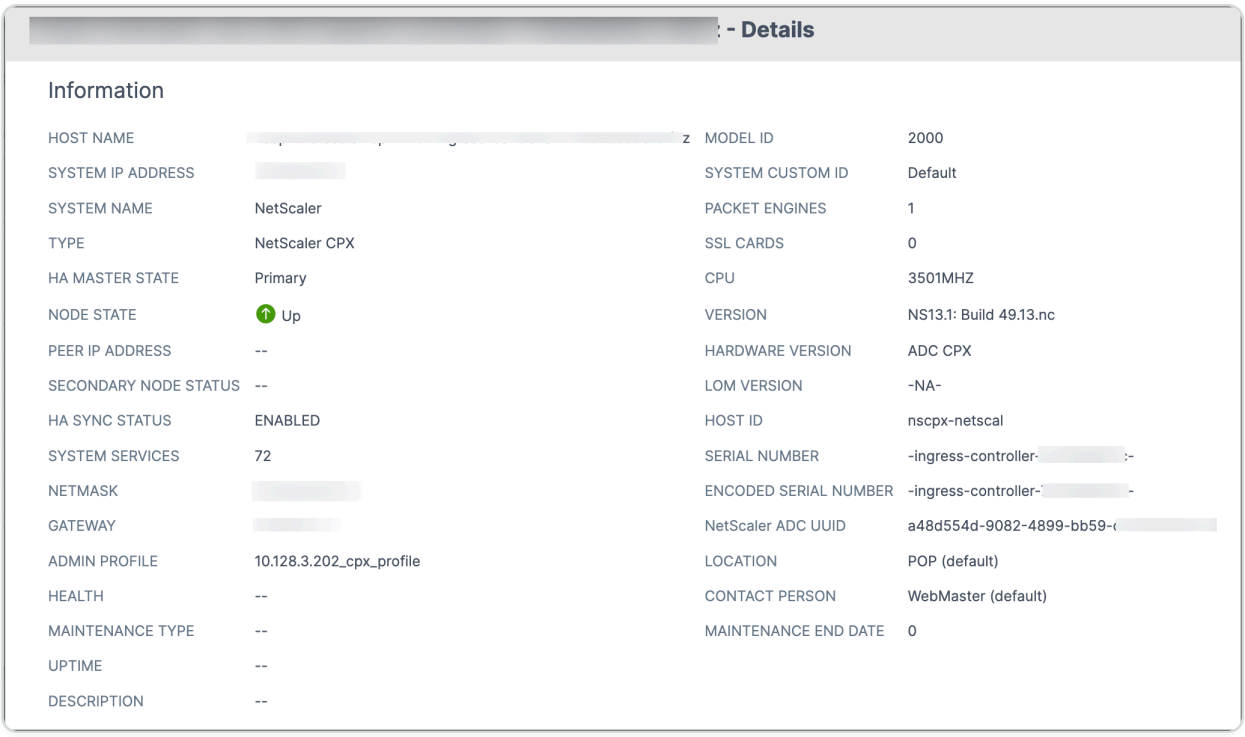
For every 5 minutes, the current values for CPU usage, memory usage, disk usage, throughput, and so on are updated.

Click an IP address and in the page that appears, click **Instance Details** to view the instance details.



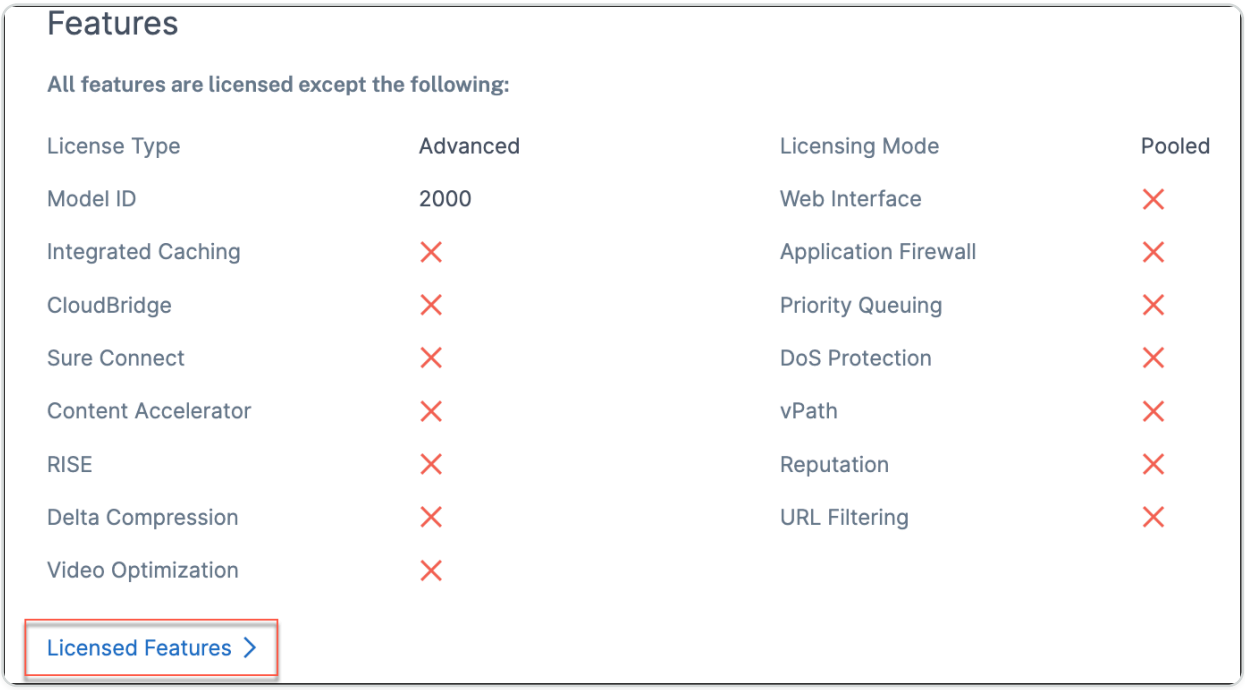
The following details are displayed:

- **Information** - Instance details such as instance type, deployment type, version, model, and so on.

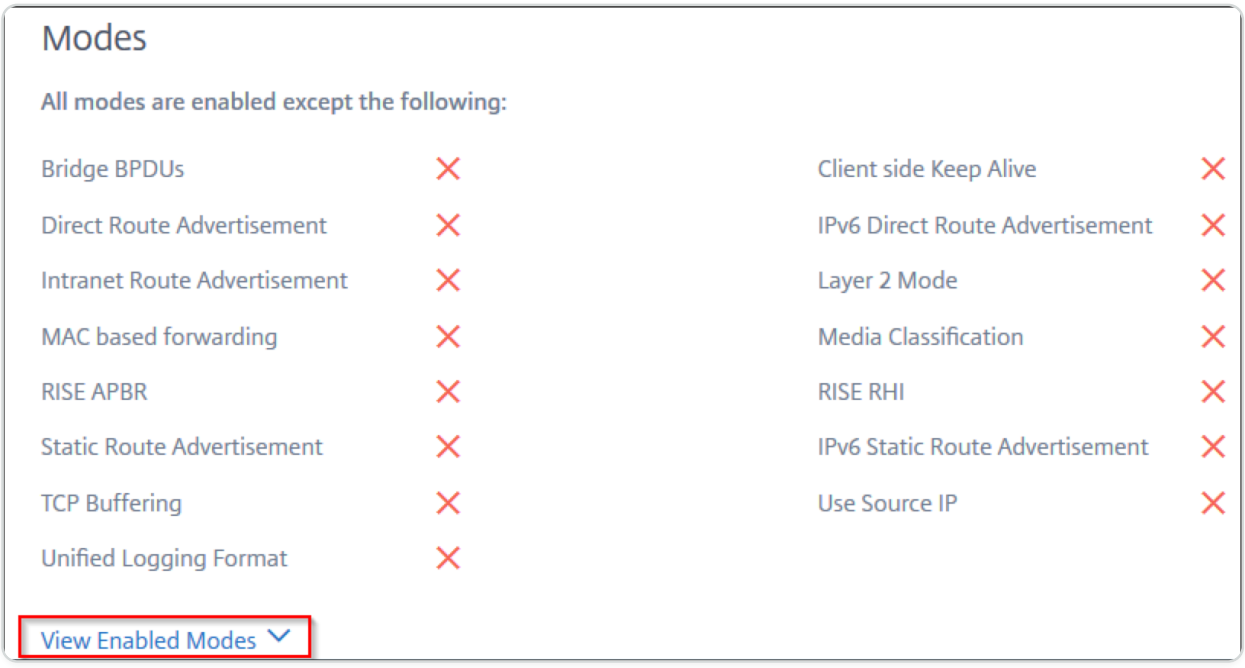


© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Features** – By default, the features that are not licensed are displayed. Click **Licensed Features** to view the features that are licensed.



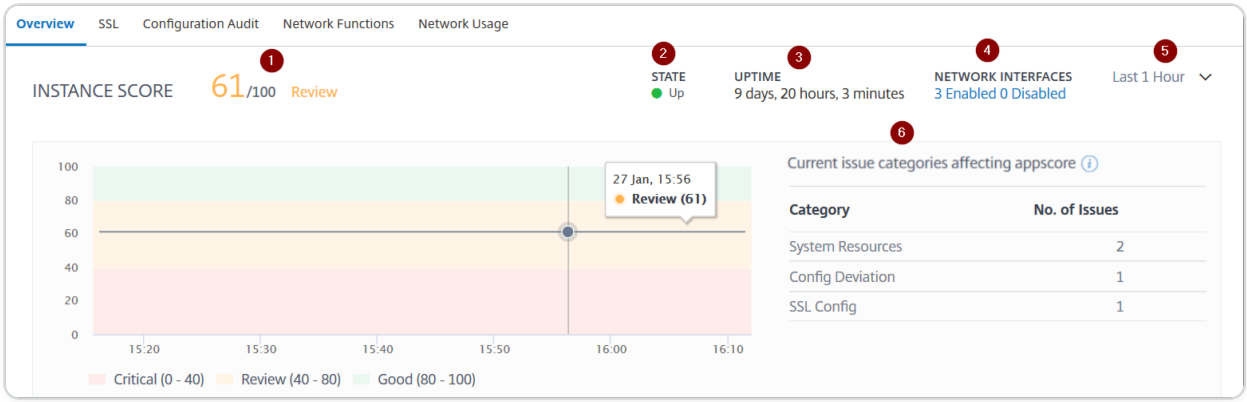
- **Modes** – By default, all modes that are disabled on the instance are displayed. Click **View Enabled Modes** to view the enabled modes on the instance.



The instance dashboard presents an instance overview where you can see the following details:

- **Instance score**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1 – Indicates the current NetScaler instance score for the selected time duration. The final score is calculated as **100 minus total penalties**. The graph displays the score ranges for the selected time duration.

2 – Indicates the current status of the NetScaler instance, such as **Up**, **Down**, and **Out of Service**.

3 – Indicates the duration that the NetScaler instance is up and running.

4 – Indicates the total network interfaces enabled and disabled for the instance. Click **Enabled** or **Disabled** to view the details such as network interface name and the status (enabled or disabled).

5 – Select the time duration from the list to view the instance details.

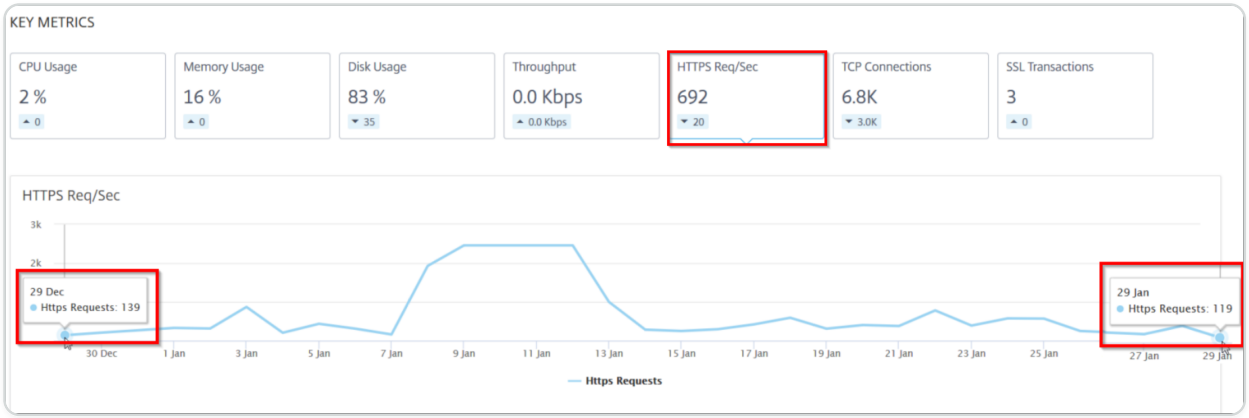
6 – Displays the total issues and issue category of the NetScaler instance.

- **Key Metrics**

  Click each tab to view the details. In each metric, you can view the average value and the difference value for the selected time.

  The following image is an example for HTTPS Req/Sec and the selected time duration is 1 hour. The value **692** is the average HTTPS Req/Sec for the 1-month duration and the value **20** is the difference value. In the graph, the first value is **139** and the last value is **119**. The difference value is **139 – 119 = 20**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can view the following instance metrics in a graph format for the selected time duration:

- **CPU Usage** – The average CPU % from the instance for the selected duration (displays for both packet CPU and for management CPU).
- **Memory Usage** – The average memory usage % from the instance for the selected duration.
- **Disk Usage** – The average disk space % from the instance for the selected duration.
- **Throughput** – The average network throughput processed by the instance for the selected duration.
- **HTTPS request/sec** – The average HTTPs requests received by the instance for the selected duration.
- **TCP connections** – The average TCP connections established by the client and server for the selected duration.
- **SSL transactions** – The average SSL transactions processed by the instance for the selected duration.

- **Issues**

  You can view the following issues that occur in NetScaler instance:

ISSUE CATEGORY	DESCRIPTION	ISSUES
System Resources	Displays all issues related to the NetScaler system resource such as CPU, Memory, disk usage, and so on.	- High CPU Usage
		- High Memory Usage

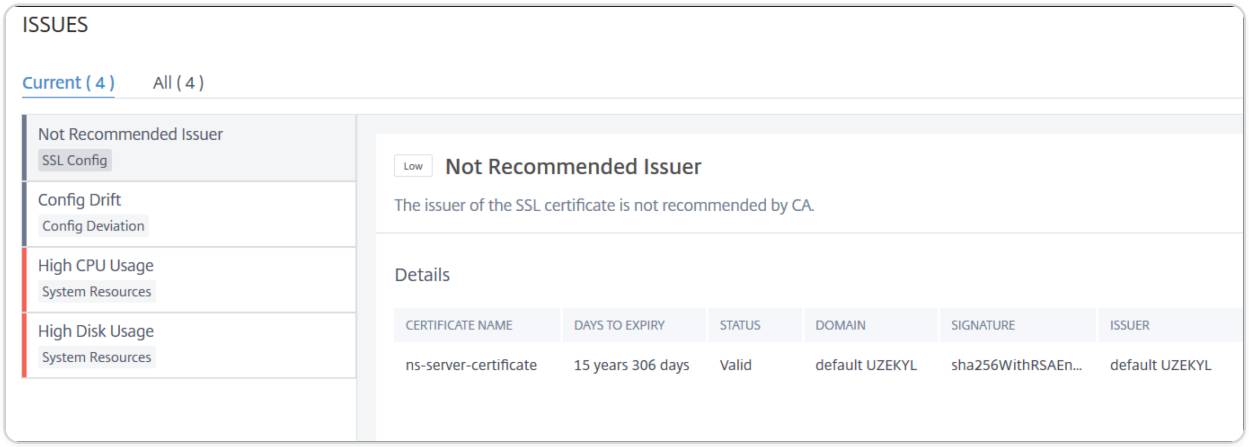
© 1997–2026 Citrix Systems, Inc. All rights reserved.

ISSUE CATEGORY	DESCRIPTION	ISSUES
		- High Disk Usage
		- SSL Card Failures
		- Power Failure
		- Disk Error
		- Flash Error
		- NIC Discards
SSL Config	Displays all issues related to the SSL configuration on the NetScaler instance.	- SSL Certs Expired
		- Not Recommended Issuer
		- Not Recommended Algo
		- Not Recommended Key Strength
Config Deviation	Displays all issues related to the configuration jobs applied in NetScaler instance.	- Config Drift
		- Running vs Template
Critical events	Displays all critical events related to NetScaler instances configured in HA pair and in Cluster.	- Cluster Prop Failure
		- Cluster Sync Failure
		- Cluster versions Mismatch
		- HA Bad Sec State
		- HA No Heat Beats

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ISSUE CATEGORY	DESCRIPTION	ISSUES
		- HA Sync Failure
		- HA Version Mismatch
Capacity issues	Displays NetScaler capacity issues. The NetScaler Console polls these events every five minutes from the NetScaler instance and displays the packet drops or rate-limit counter increments if exists. The issues are categorized on the following capacity parameters.	- Throughput Limit Reached
		- PE CPU Limit Reached
		- PPS Limit Reached
		- SSL Throughput Rate Limit
		- SSL TPS Rate Limit
Networking	Displays the operational issues that occur in the instances.	For more information, see Enhanced Infrastructure Analytics with new indicators.

Click each tab to analyze and troubleshoot the issue. For example, consider that an instance has the following errors for the selected time duration:



© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The **Current** tab displays the issues that are currently affecting the instance score.
- The **All** tab displays all infra issues detected for the selected duration.

View the capacity issues in an NetScaler instance

When a NetScaler instance has consumed most its available capacity, packet-drop may occur while processing the client traffic. This issue causes low performance in a NetScaler instance. By understanding such NetScaler capacity issues, you can proactively allocate additional licenses to steady the NetScaler performance.

In the **Circle Pack View**, you can view the NetScaler instance capacity issues if exists.

To view NetScaler capacity issues,

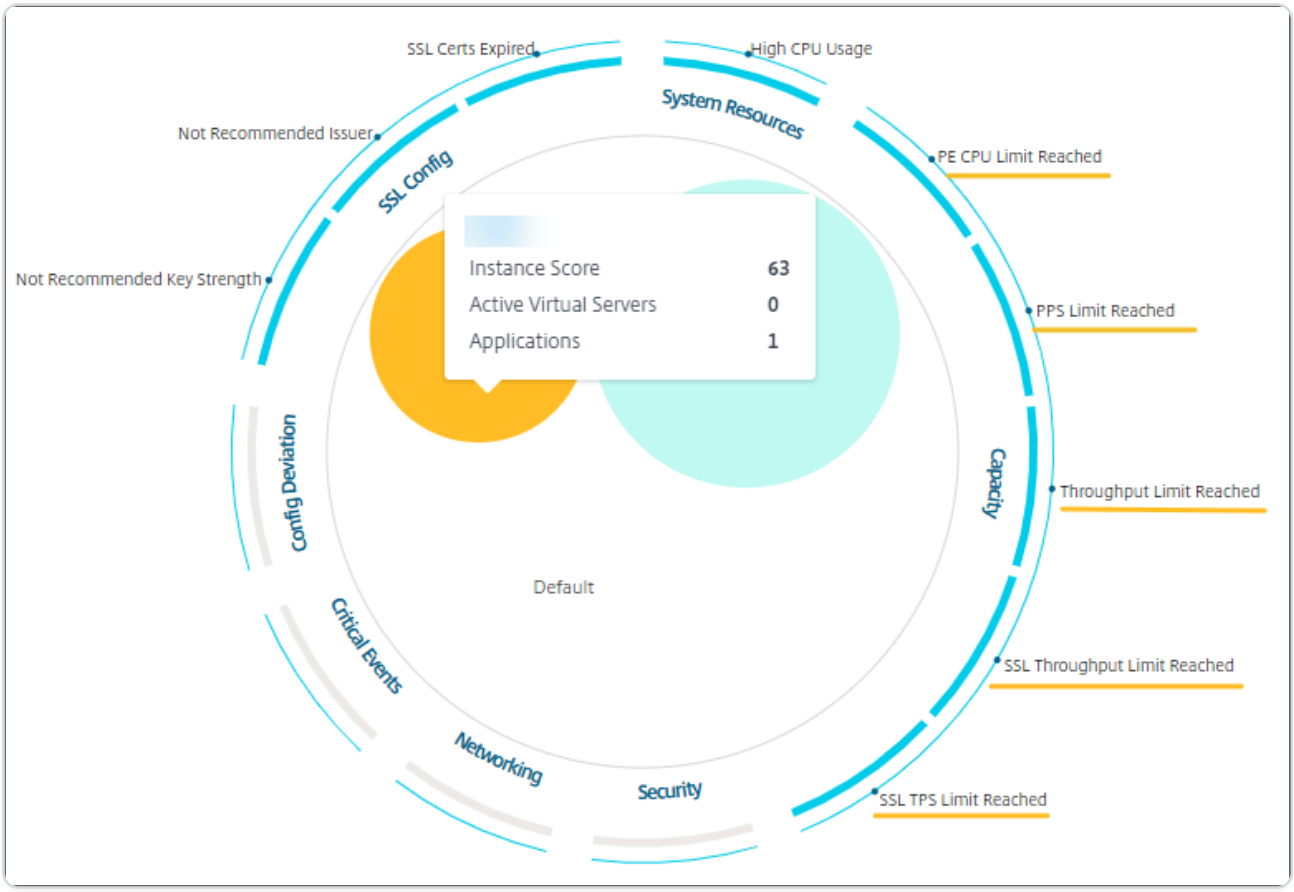
1. Navigate to **Infrastructure > Infrastructure Analytics**.
2. Select the circle pack view.

NOTE:

In **Infrastructure Analytics**, the circle-pack and tabular views display the events and issues that occurred in the last one hour.

The following illustration suggests the capacity issues exist in the selected instance:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The issues are categorized on the following capacity parameters:

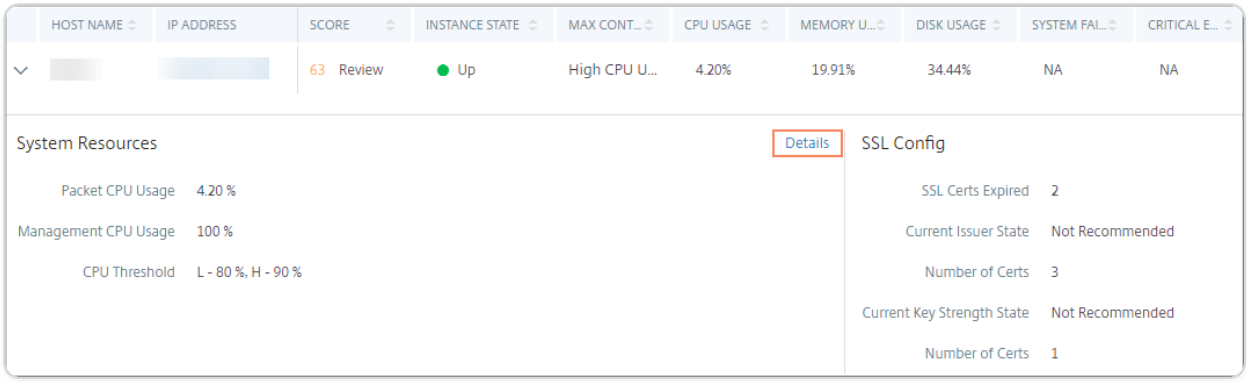
- **Throughput Limit Reached** – The number of packets dropped in the instance after the throughput limit is reached.
- **PE CPU Limit Reached** - The number of packets dropped on all NICs after the PE CPU limit is reached.
- **PPS Limit Reached** – The number of packets dropped in the instance after PPS limit is reached.
- **SSL Throughput Rate Limit** – The number of times the SSL throughput limit reached.
- **SSL TPS Rate Limit** – The number of times the SSL TPS limit reached.

View recommended actions to solve capacity issues

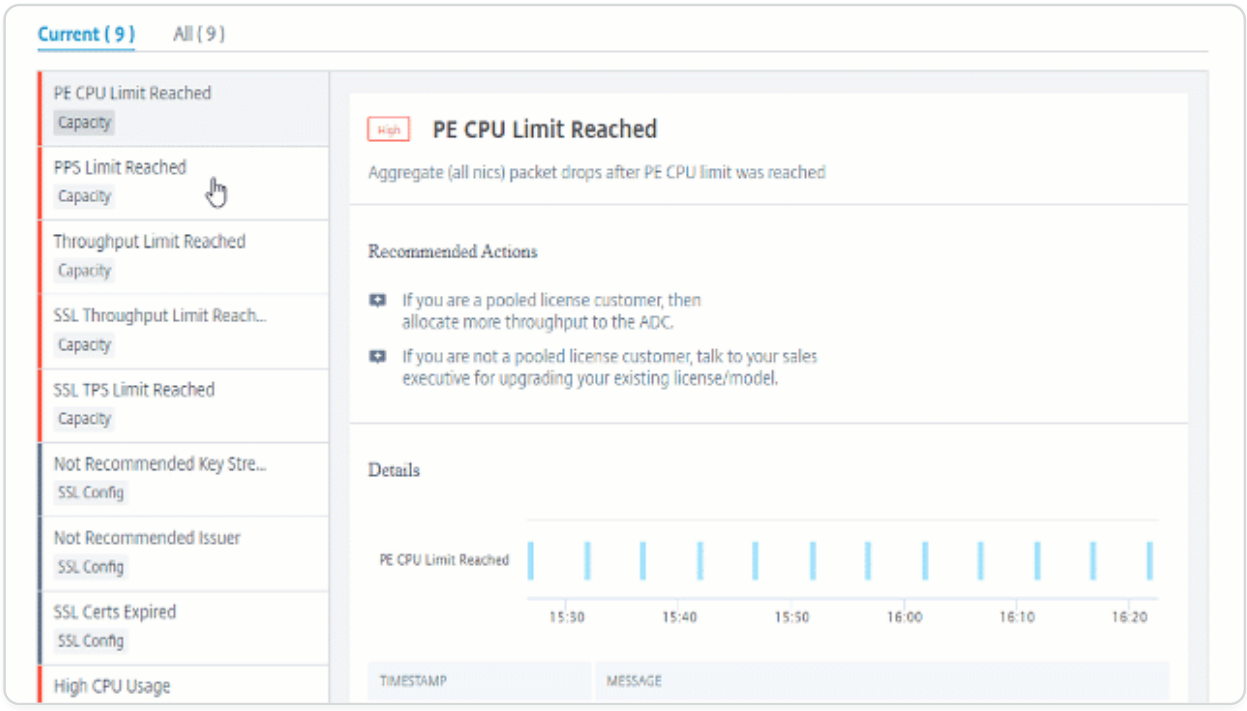
The NetScaler Console recommends actions that can solve capacity issues. To view the recommended actions, perform the following steps:

1. In **Infrastructure > Infrastructure Analytics**, select the tabular view.
2. Select the instance that has capacity issues and click **Details**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. In the instance page, scroll down to the **Issues** section.
4. Select each issue and view the recommended actions to resolve capacity issues.



The NetScaler Console polls these events every five minutes from the NetScaler instance and displays the packet drops or rate-limit counter increments if exists.

The NetScaler Console calculates the instance score on the defined capacity threshold.

- **Low threshold** – 1 packet drop or rate-limit counter increment
- **High threshold** – 10000 packets drop or rate-limit counter increment

Therefore, when a NetScaler instance breaches the capacity threshold, the instance score is impacted.

When packets drop or rate-limit counter increments, an event is generated under the `ADCCapacityBreach` category. To view these events, navigate to **Settings > System Events**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enhanced Infrastructure Analytics with new indicators

Using the NetScaler Console **Infrastructure Analytics**, you can:

- View a new set of operational issues that occur in NetScaler instances.
- View error messages and check recommendations to troubleshoot the issues.

As an administrator, you can quickly identify the root cause analysis of issues.

NOTE:

Rule indicators are not supported for:

- NetScaler instances configured in a cluster mode.
- NetScaler instances configured with admin partitions.

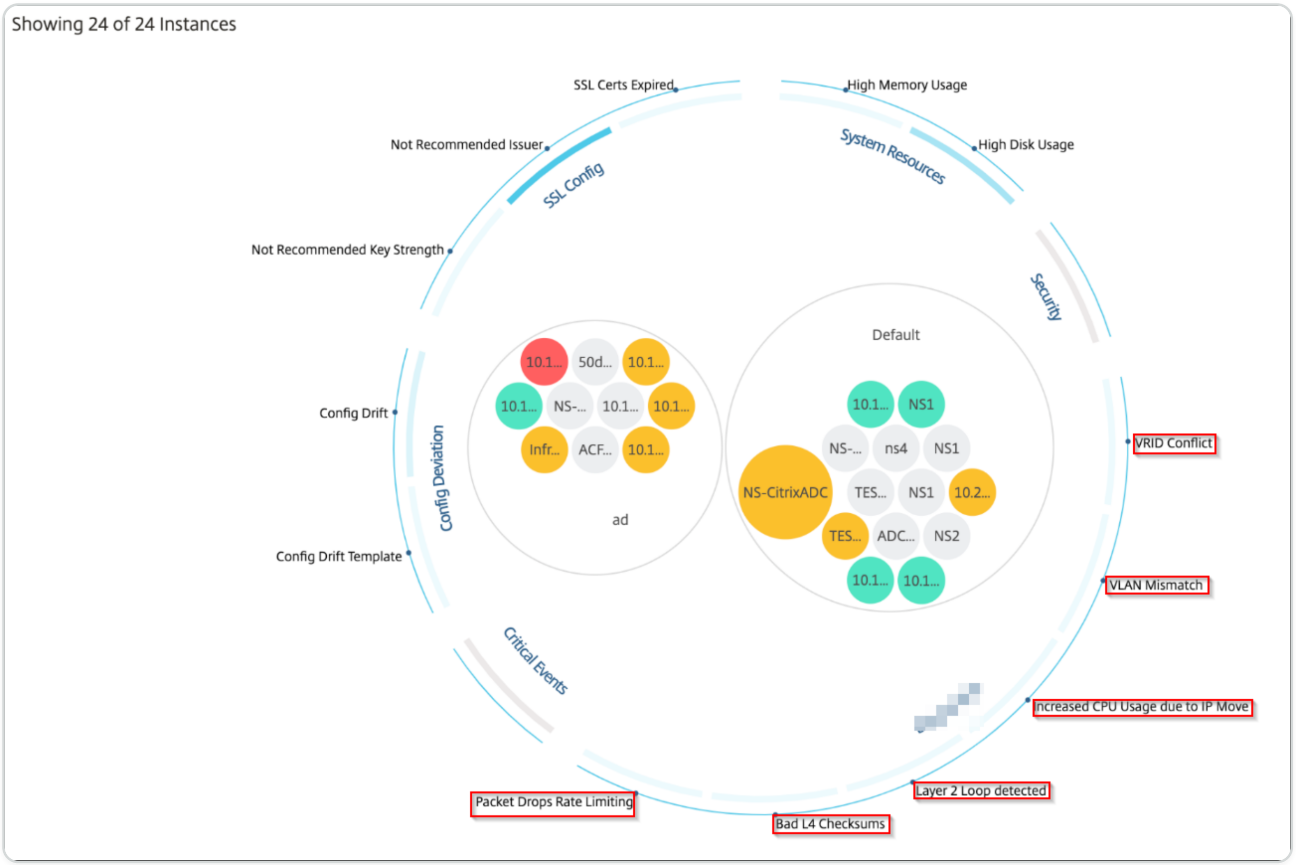
In NetScaler Console, navigate to **Infrastructure > Infrastructure Analytics** to view indicators for:

INDICATOR NAME IN INFRASTRUCTURE ANALYTICS	DESCRIPTION
Port allocation failure	Detects when NetScaler uses SNIP to communicate with a new server connection and total ports available on that SNIP are exhausted. The recommended action is to add another SNIP in the same subnet.
Session Buildup	Detects when NetScaler memory is held up by SSL sessions.
No default route configuration	Detects when the traffic gets dropped because of non-availability of routes.
IP conflict	Detects if a same IP address is configured or applied on two or more instances in a network.
VRID conflict	Detects when intermittent access problems occur for the specified VRID.
VLAN mismatch	Detects if any errors occur during VLAN configuration bound to IP subnets.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INDICATOR NAME IN INFRASTRUCTURE ANALYTICS	DESCRIPTION
TCP small window attack	Detects when there is a possible small window attack in progress. This alert is just for informational, because NetScaler already mitigates this attack.
Rate control threshold	Detects when packets are dropped based on the configured rate control threshold.
Persistence Limit	Detects when maximum hits are imposed on the NetScaler memory.
GSLB site name mismatch	Detects when GSLB configuration synchronization failures occur because of site name mismatch.
Malformed IP header	Detects when sanity checks on IPv4 packets are failed.
Bad L4 checksums	Detects when checksum validation for TCP packets is failed.
Increased CPU usage due to IP move	Detects if a large number of macs need to be updated.
Excessive packet steering	Detects high levels of software packet steering due to the usage of asymmetric rss key type.
Layer 2 loop	Detects the presence of layer 2 loops in the network.
Tagged VLAN mismatch	Detects when tagged VLAN packets are received on an untagged interface.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



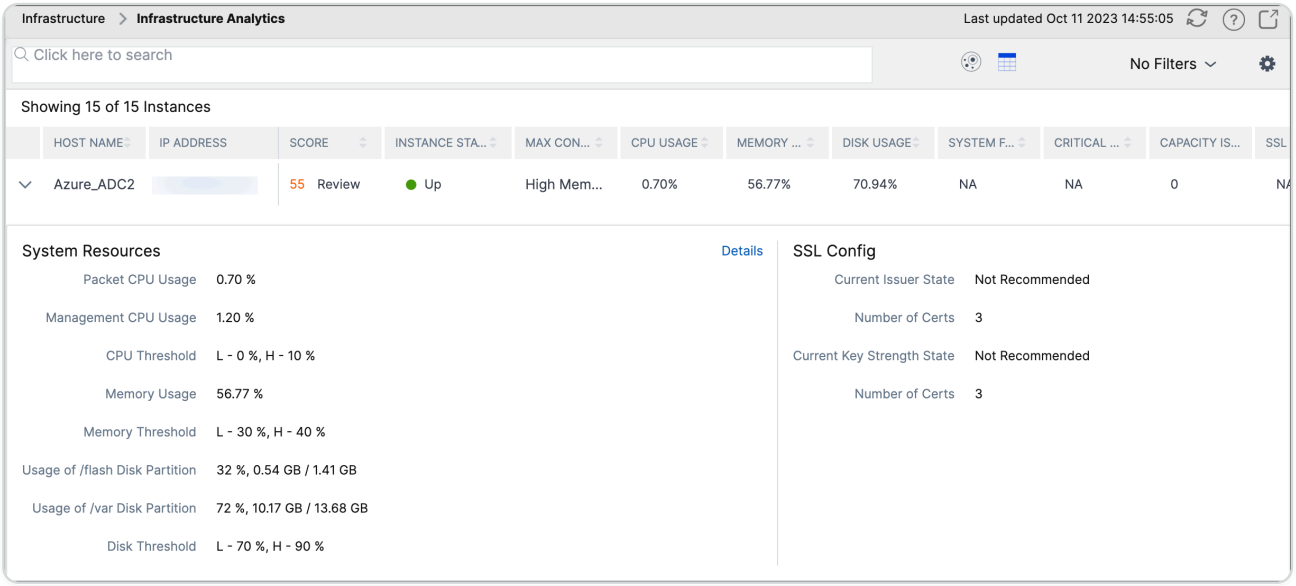
Tabular view

You can also view anomalies using the tabular view option in **Infrastructure Analytics**. Navigate to **Infrastructure > Infrastructure Analytics** and then click



to display all managed instances. Click

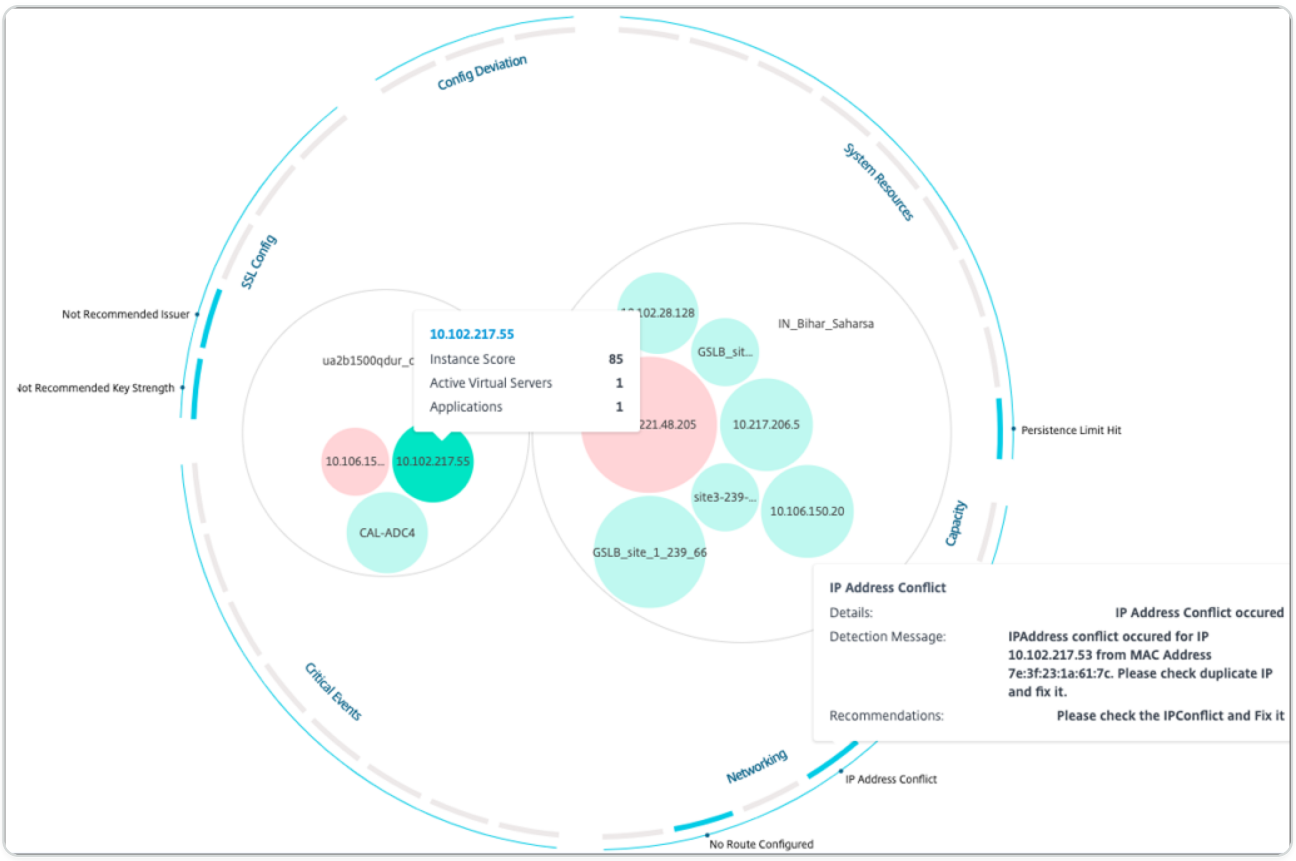
to expand for details.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

View details of an anomaly

For example, if you want to view details for **IP address conflict** in the network, click the anomaly that is displayed for IP address conflict.



- **Details** - Indicates what anomaly is detected
- **Detection Message** - Indicates the MAC address for which the IP address has the conflict
- **Recommendations** - Indicates the troubleshooting procedure to resolve this IP address conflict

Instance management

Instances are Citrix Application Delivery Controller (ADC) appliances that you can manage, monitor, and troubleshoot using NetScaler Console. Add instances to NetScaler Console to monitor them. Instances can be added when you set up NetScaler Console or later as well. After you add instances to NetScaler Console, they are continuously polled to collect information that can later be used to resolve issues or as reporting data.

Instances can be grouped as a static group or as a private IP-block. A static group of instances can be useful when you want to run specific tasks such as configuration jobs, and others. A private IP-block groups your instances based on their geographical locations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Add an instance

You can add instances either while setting up the NetScaler Console server for the first time or later. To add instances, you must specify either the host name or IP address of each NetScaler instance, or a range of IP addresses.

To learn how to add an instance to NetScaler Console, see Add Instances to NetScaler Console.

When you add an instance to the NetScaler Console server, the server implicitly adds itself as a trap destination for the instance and collects an inventory of the instance. To learn more, see How NetScaler Console discovers instances.

After you've added an instance, you can delete it by navigating to **Infrastructure > Instances** and select the instance category. Then, select the instance you want to delete and click **Remove**.

How to use the instance dashboard

The per-instance dashboard in NetScaler Console displays data in a tabular and graphical format for the selected instance. Data collected from your instance during the polling process is displayed on the dashboard.

By default, every minute, managed instances are polled for data collection. Statistical information such as state, the HTTP requests per second, CPU usage, memory usage, and throughput are continuously collected using NITRO calls. As an administrator, you can view all this collected data on a single page, identify issues in the instance, and take immediate action to rectify them.

To view a specific instance's dashboard, navigate to **Infrastructure > Instances > NetScaler**. On the NetScaler page, choose the instance type and then, select the instance you want to view and click **Dashboard**.

- **Overview**. The overview tab displays the CPU and memory usage of the chosen instance. You can also view events generated by the instance and the throughput data. Instance-specific information such as the IP address, its hardware and LOM versions, the profile details, serial number, contact person, and others are also displayed here. By scrolling down further, the licensed features that are available on your chosen instance along with the modes configured on it. For more information, see Instance details.
- **SSL dashboard**. You can use the SSL tab on the per-instance dashboard to view or monitor the details of your chosen instance's SSL certificates, SSL virtual servers, and SSL protocols. You can click the "numbers" in the graphs to display further details.
- **Configuration Audit**. You can use the configuration audit tab to view all the configuration changes that have occurred on your chosen instance. The **NetScaler config saved status** and

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler config drift charts on the dashboard display high-level details about configuration changes in saved against unsaved configurations.

- **Network Functions**. Using the network functions dashboard, you can monitor the state of the entities configured on your selected NetScaler instance. You can view graphs for your virtual servers that display data such as client connections, throughput, and server connections.
- **Network usage**. You can view network performance data for your selected instance on the network usage tab. You can display reports for an hour, a day, a week, or for a month. The timeline slider function can be used to customize the duration of the network reports being generated. By default, only eight reports are displayed, but you can click the "plus" icon at the bottom right-corner of the screen to add another performance report.

How to monitor globally distributed sites

As a network administrator, you might have to monitor and manage network instances deployed across geographical locations. However, it is not easy to gauge the requirements of the network when managing network instances in geographically distributed data centers.

Geomaps in NetScaler Console provides you with a graphical representation of your sites and breaks down your network monitoring experience by geography. With geomaps, you can visualize your network instance distribution by location and monitor network issues.

The following sections explain how you can monitor data centers in NetScaler Console.

Monitoring globally distributed sites in NetScaler Console

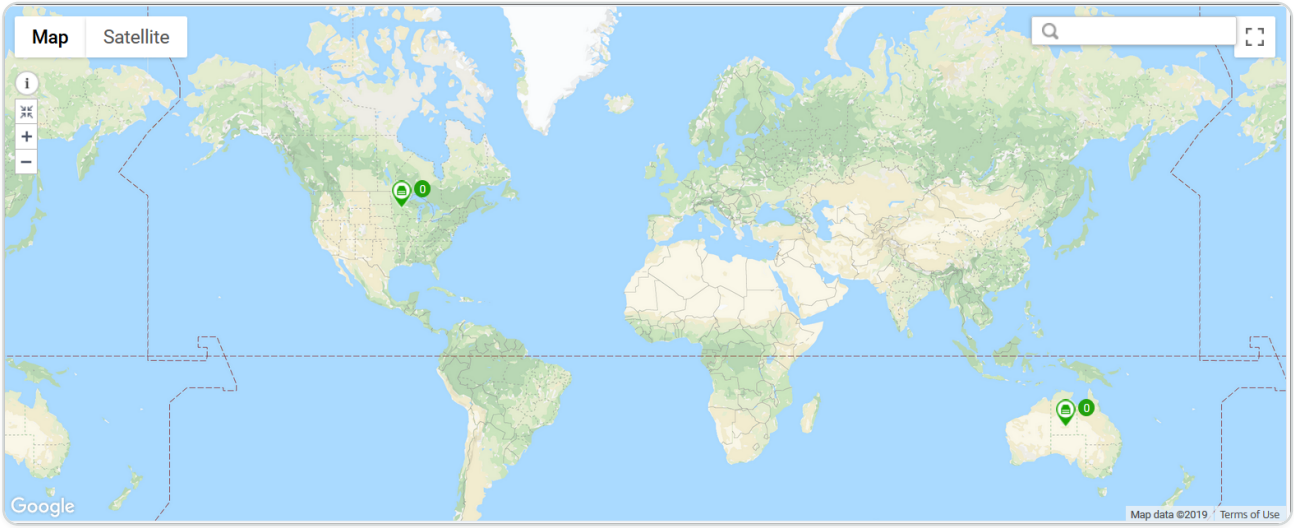
NetScaler Console site is a logical grouping of Citrix Application Delivery Controller (NetScaler) instances in a specific geographical location. For example, while one site is assigned to Amazon Web Services (AWS) and another site might be assigned to Azure. Still another site is hosted on the premises of the tenant. NetScaler Console manages and monitors all NetScaler instances connected to all sites. You can use NetScaler Console to monitor and collect syslog, AppFlow, SNMP, and any such data originating from the managed instances.

Geomaps in NetScaler Console provides you with a graphical representation of your sites. Geomaps also breaks down your network monitoring experience by geography. With geomaps, you can visualize your network instance distribution by location and monitor all network issues. You can click **Infrastructure** on the menu and this displays the **Instances Dashboard** for a visual representation of the sites created on the world map.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

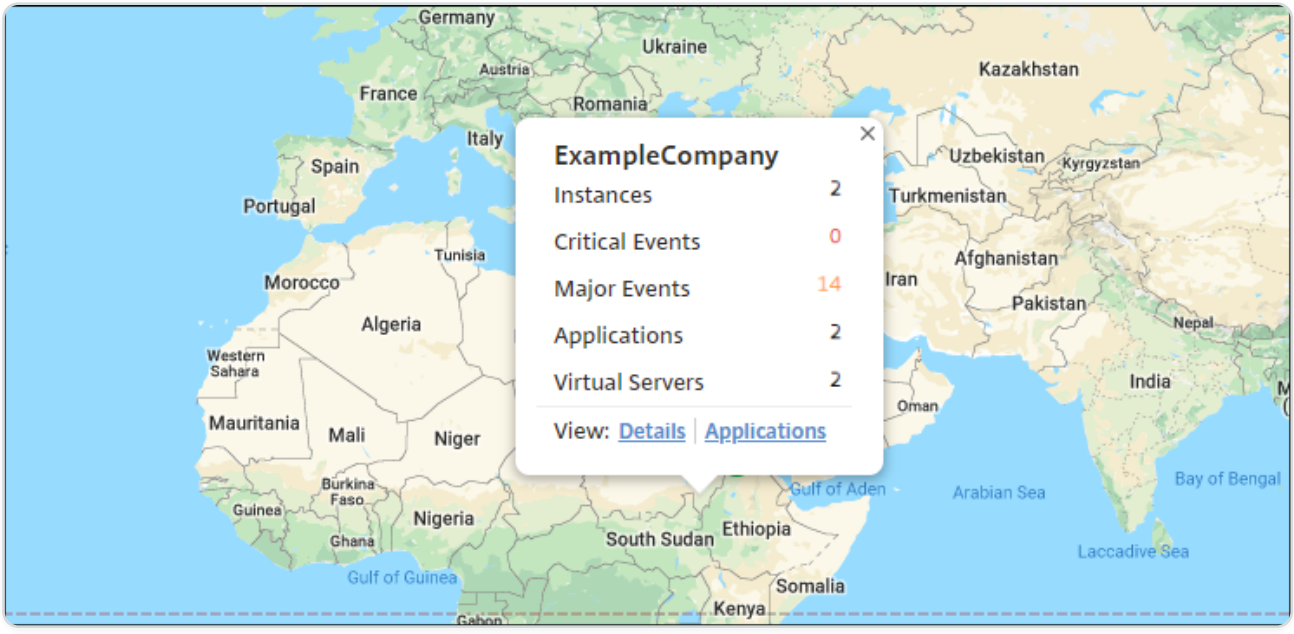
Use case

A leading mobile carrier company, ExampleCompany, was relying on private service providers for hosting their resources and applications. The company already had two sites - one at Minneapolis in the United States and another in Alice Springs in Australia. In this image, you can see that two markers represent the two existing sites.



The markers also display the count of the following components on the site:

- **Instances**: Indicates the number of instances available.
- **Applications**: Indicates the number of applications hosted.
- **Virtual Servers**: Indicates the number of virtual servers available.
- **Critical Events**: Indicates the count of critical events occurred on the instances.
- **Major Events**: Indicates that the count of major events occurred on the instances.

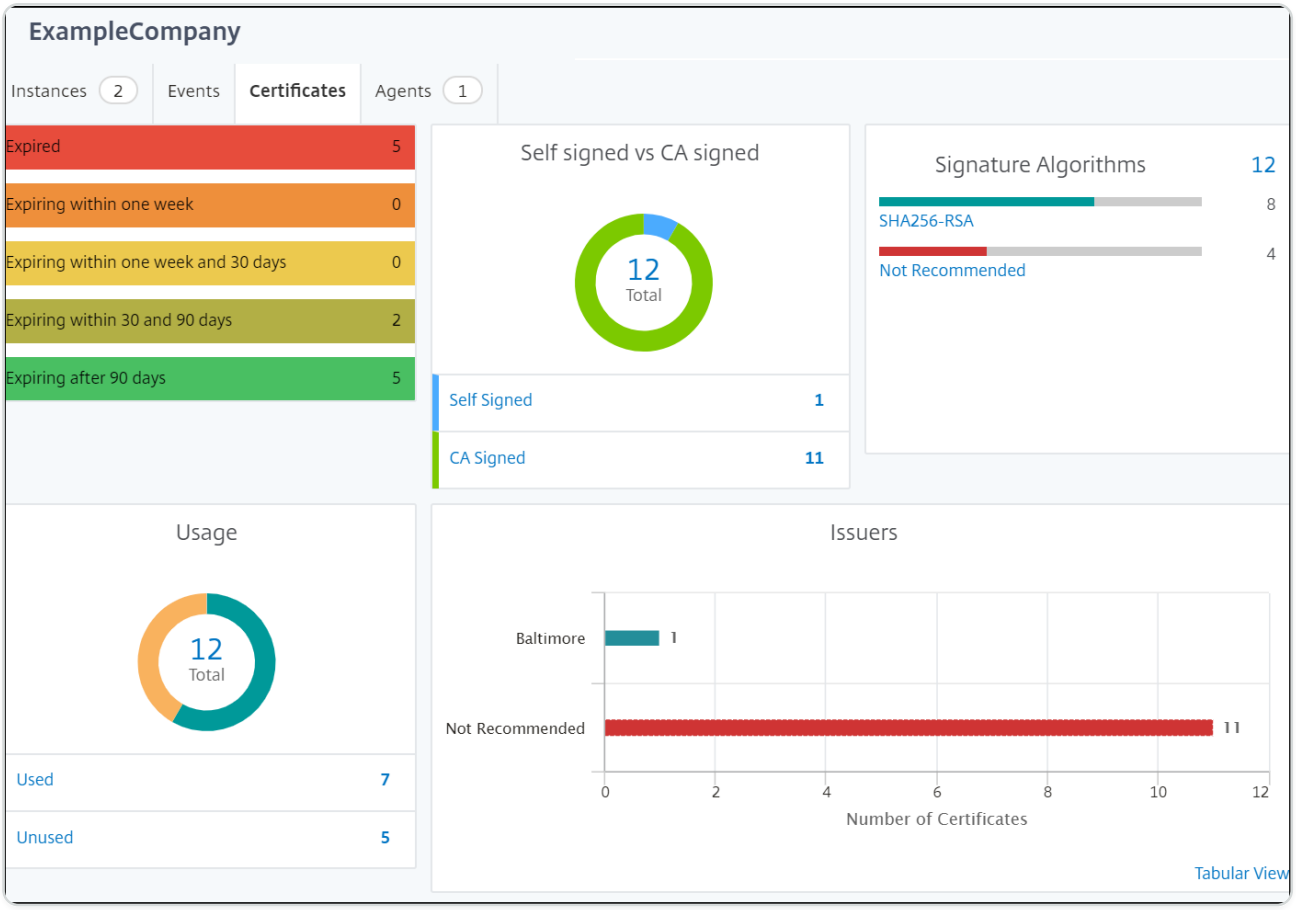


Click **Applications** to see all custom applications created in each site.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Click **Details** to see a list of NetScaler instances added in each site. Click the tabs to view more information:

- **Instances** tab: View the following in this tab:
  - IP address of each network instance
  - Type of the NetScaler instance
  - Number of critical events
  - Significant events and all events raised on a NetScaler instance.
- **Events** tab: View a list of critical and significant events raised on the instances.
- **Certificates** tab: View the following in this tab:
  - List of certificates of all the instances
  - Expiration status
  - Vital information and the top 10 instances by many certificates in use.
- **Agents** tab: View a list of agents to which the instances are bound.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuring Geomaps

ExampleCompany decided to create a third site in Bangalore, India. The company wanted to test the cloud by offloading some of their less-critical, internal IT applications to the Bangalore office. The company decided to use the AWS cloud computing services.

As an administrator, you must first create a site, and next add the NetScaler instances in NetScaler Console. You must also add the instance to the site, add an agent, and bind the agent to the site. NetScaler Console then recognizes the site that the NetScaler instance and the agent belong.

For more information on adding NetScaler instances, see Adding Instances.

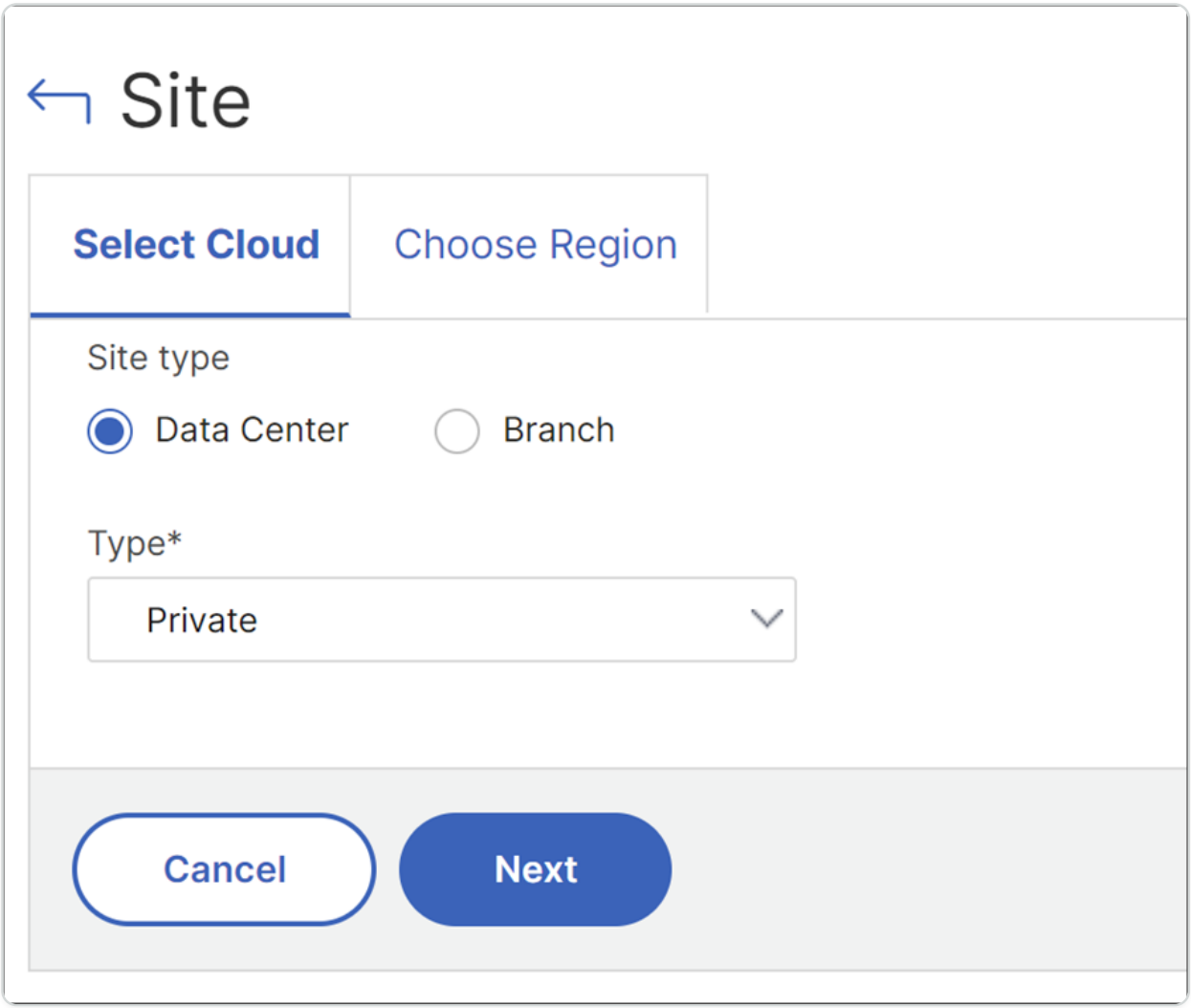
Create a Site

Create sites before you add instances in NetScaler Console. Providing location information allows you to precisely locate the site.

To create a site:

1. Navigate to **Infrastructure > Instances > Site**. Click **Add**.
2. On the **Select Cloud** tab, choose the **Site type**. You can create a site of type **Data Center** or **Branch**.

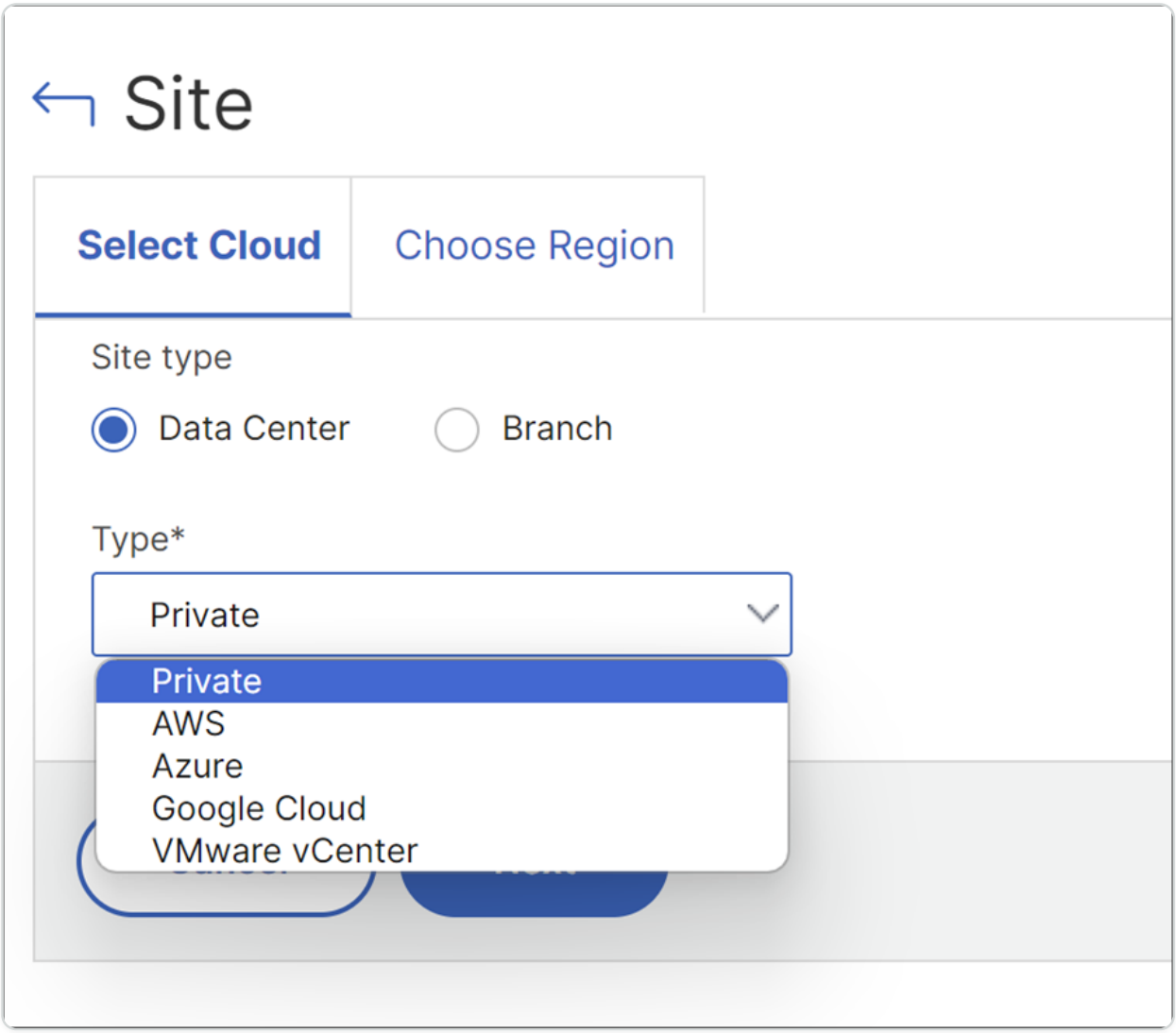
© 1997–2026 Citrix Systems, Inc. All rights reserved.



For Data Center site type, select the **Type** from the list:

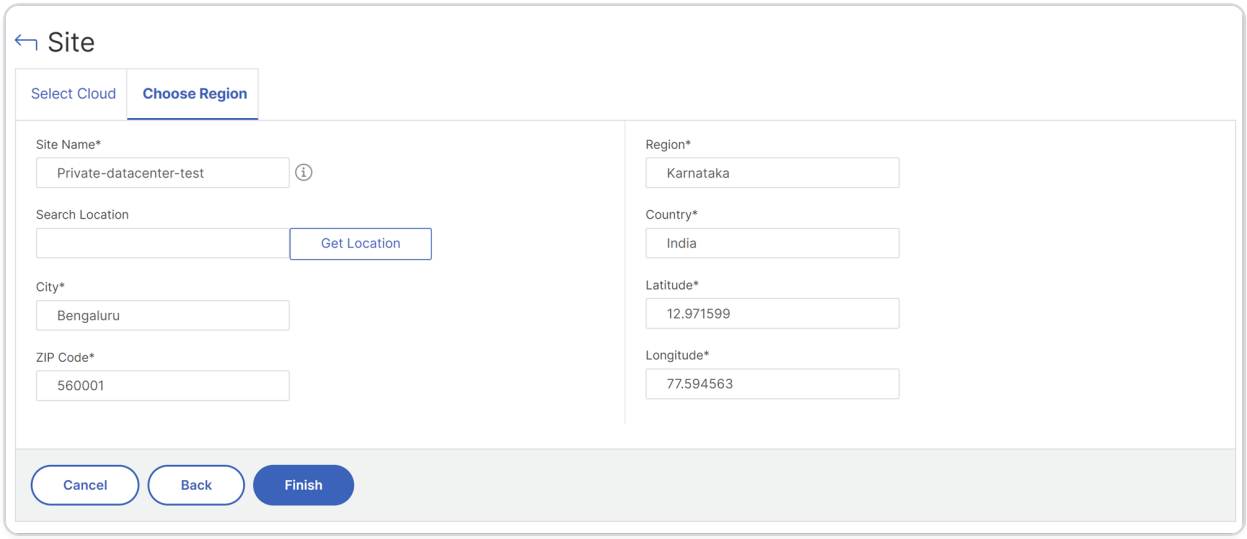
- Private
- AWS
- Azure
- Google Cloud
- VMware vCenter

© 1997–2026 Citrix Systems, Inc. All rights reserved.

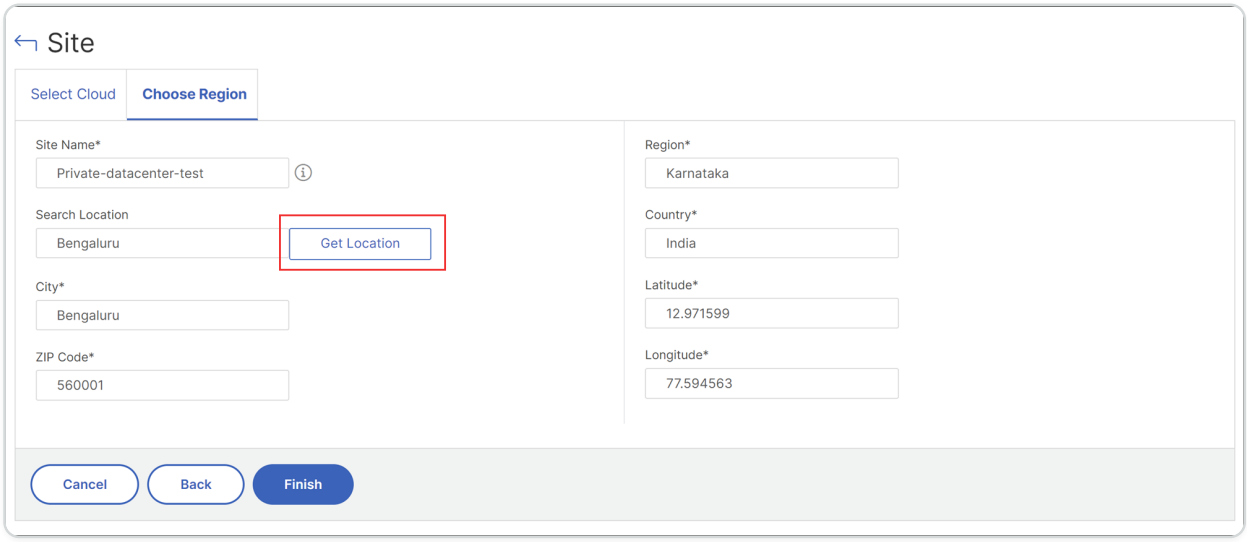


3. Click **Next**.
4. On the **Choose Region** tab, enter the following details:
    - Site Name
    - City
    - Zip Code
    - Region
    - Country
    - Latitude
    - Longitude

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Alternatively, you can enter the location in **Search Location** and click **Get Location** to precisely locate the site. The City, Zip code, Region, Country, Latitude, and Longitude fields are automatically filled in.



5. Click **Finish**.

NOTES:

The outlined steps are applicable for:

- Branch site type.
- Data Center site type with the Private type.
- When the fetch option is not selected for the cloud provider types.

Create a site for cloud provider types

You can create a site with a cloud provider type and choose whether to enable or disable the **Fetch** option. By default, the **Fetch** option is not selected.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The **Fetch** option is available only for AWS, Azure and Google Cloud platforms.

For detailed instructions on creating a site for specific cloud providers, refer to the following sections:

1. Create a site in AWS
2. Create a site in Azure
3. Create a site in Google Cloud
4. Create a site in VMware vCenter

Edit a Site

To modify an existing site:

1. Select the site and click **Edit**.
2. On the **Configure Site** page, you can update the **Site type**. For example, if you have selected **Branch** previously, you can update to **Data Center**.
3. Depending on the site type, you can modify the **Type**. For example, you can change the type from a Private Data Center to a Public Cloud from the list.

Delete a Site

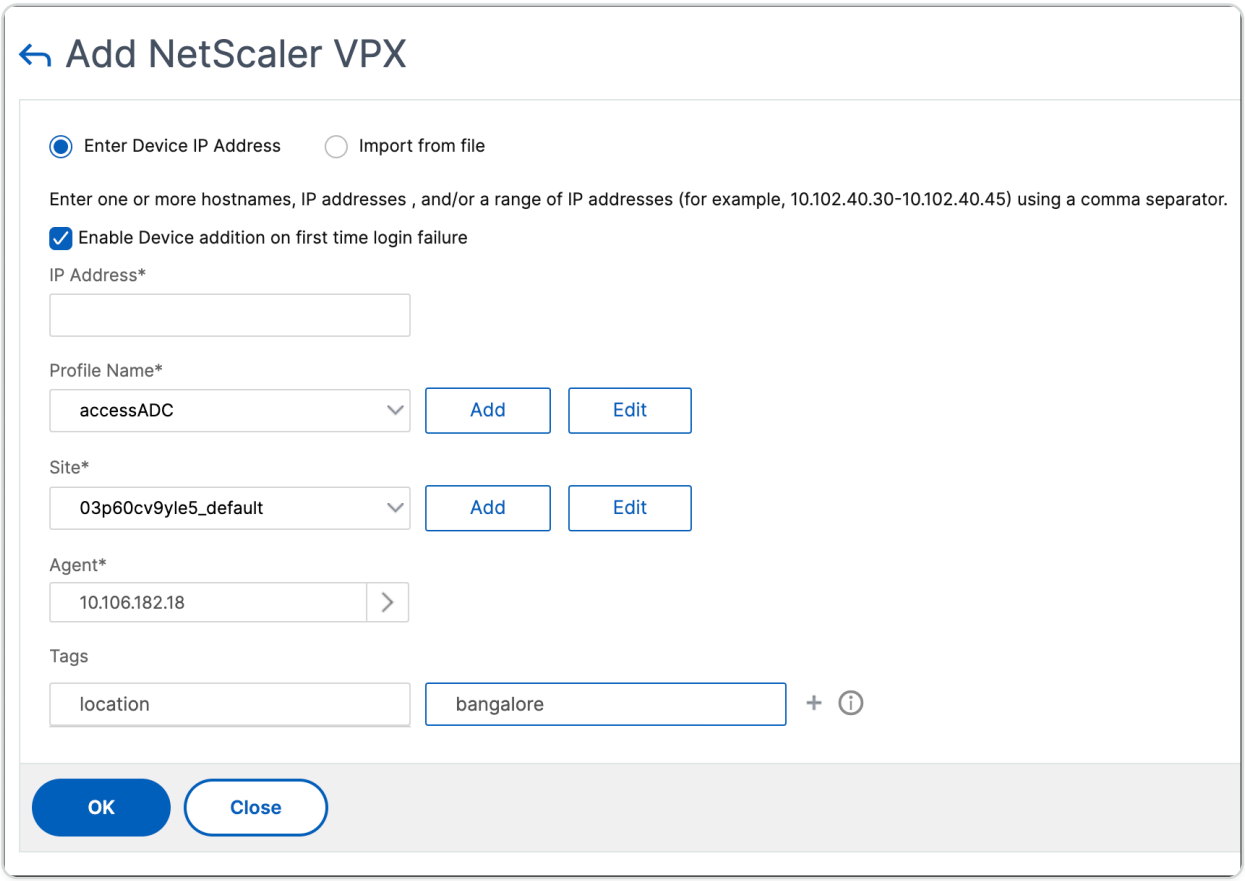
1. To delete a site, select the site and click **Delete**.
2. On the Confirm page, click **Yes**.

To add instances and select sites:

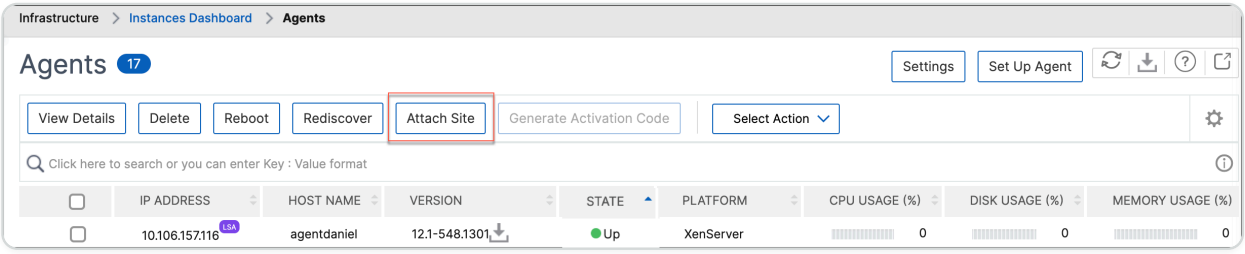
After creating sites, you must add instances in NetScaler Console. You can select the previously created site, or you can also create a site and associate the instance.

1. In NetScaler Console, navigate to **Infrastructure > Instances > NetScaler**.
2. Select the **VPX**, and click **Add**.
3. On the **Add NetScaler VPX** page, type the IP address and select the profile from the list.
4. Select the site from the list. You can click the **Add** button next to **Site** field to create a site or click the **Edit** button to change the details of the default site.
5. Click the right arrow and select the agent from the list that displays.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. After choosing the agent, you must associate the agent with the site. This step allows the agent to be bound to the site. Select the agent and click **Attach Site**.



   a. Select the site from the list and click **Save**.

7. Optionally, you can enter key and value fields for **Tags**.
8. Click **OK**.

You can also attach an agent to a site by navigating to **Infrastructure > Instances > Agents**.

To associate an agent with the site:

1. In NetScaler Console, navigate to **Infrastructure > Instances > Agents**.
2. Select the agent, and click **Attach Site**.
3. You can associate the site and click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console starts monitoring the NetScaler instances added in the Bangalore site along with the instances at the other two sites as well.

To export the report of this dashboard:

To export the report of this page, click the **Export** icon in the top right side of this page. On the **Export** page, you can do one of the following:

1. Select **Export Now** tab. To view and save the report in PDF, JPEG, PNG, or CSV format.
2. Select **Schedule Export** tab. To schedule the report daily, weekly, or monthly and send the report over an email or a slack message.

NOTE:

- If you select **Weekly** recurrence, ensure that you select the weekdays on which you want the report to be scheduled.
- If you select **Monthly** recurrence, ensure that you enter all the days that you want the report to be scheduled separated by commas.

How to create tags and assign to instances

NetScaler Console now allows you to associate your NetScaler instances with tags. A tag is a keyword or a one-word term that you can assign to an instance. The tags add some additional information about the instance. The tags can be thought of as metadata that helps describe an instance. Tags allow you to classify and search for instances based on these specific keywords. You can also assign multiple tags to a single instance.

The following use cases help you to understand how tagging of instances will help you to better monitor them.

- **Use case 1**: You can create a tag to identify all instances that are located in the United Kingdom. Here, you can create a tag with the key as "Country" and the value as "UK." This tag helps you to search and monitor all those instances that are located in the UK.
- **Use case 2**: You want to search for instances that are in the staging environment. Here, you can create a tag with the key as "Purpose" and a value as "Staging_NS." This tag helps you to segregate all instances that are being used in the staging environment from the instances that have client requests running through them.

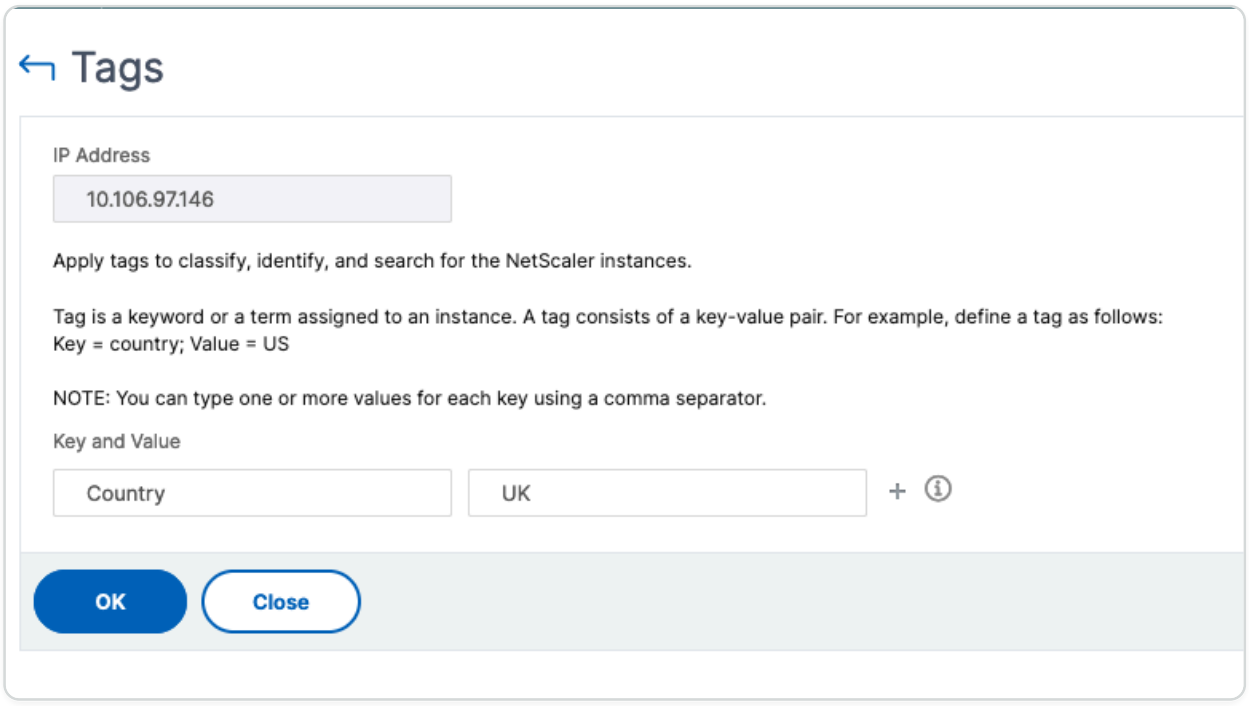
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Use case 3**: Consider a situation where you want to find out the list of NetScaler instances that are located in the Swindon area in the UK and owned by you, David T. You can create tags for all these requirements and assign that to all the instances that satisfy these conditions.

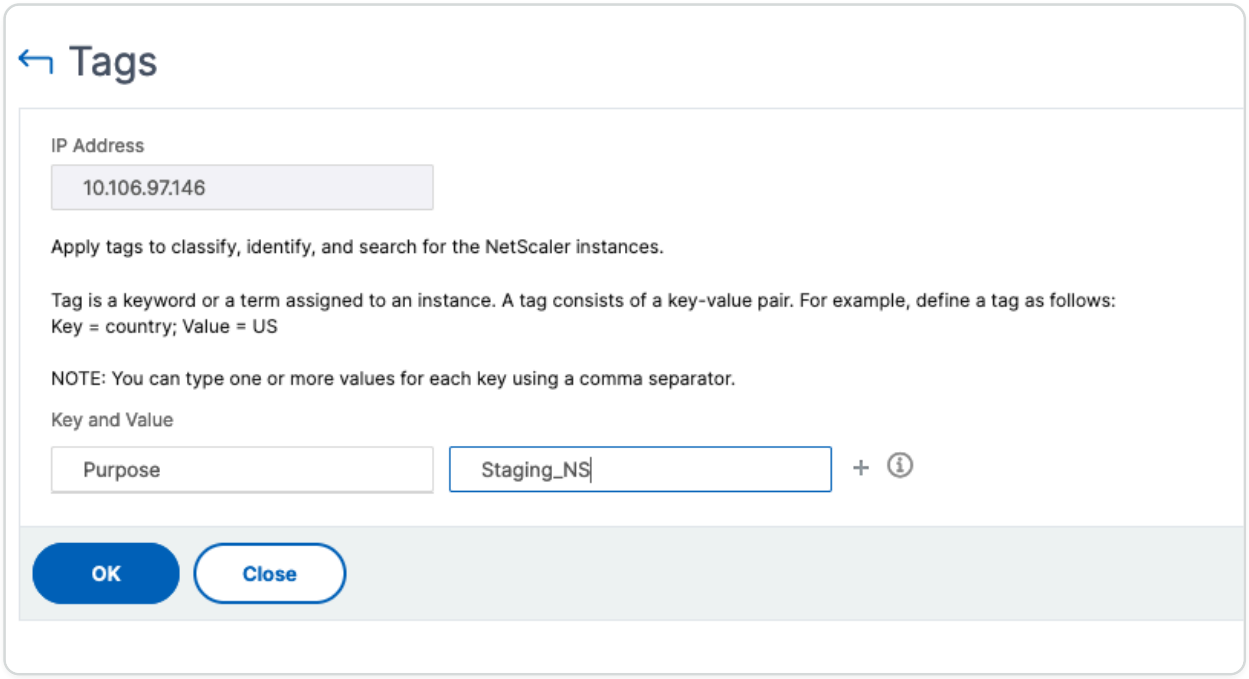
To assign tags to NetScaler VPX instance:

1. In NetScaler Console, navigate to **Infrastructure > Instances > NetScaler**.
2. Select the **VPX** tab.
3. Select the required VPX instance.
4. Click **Tags**. The **Tags** window that appears allows you to create your own "key-value" pairs by assigning values to every keyword that you create.

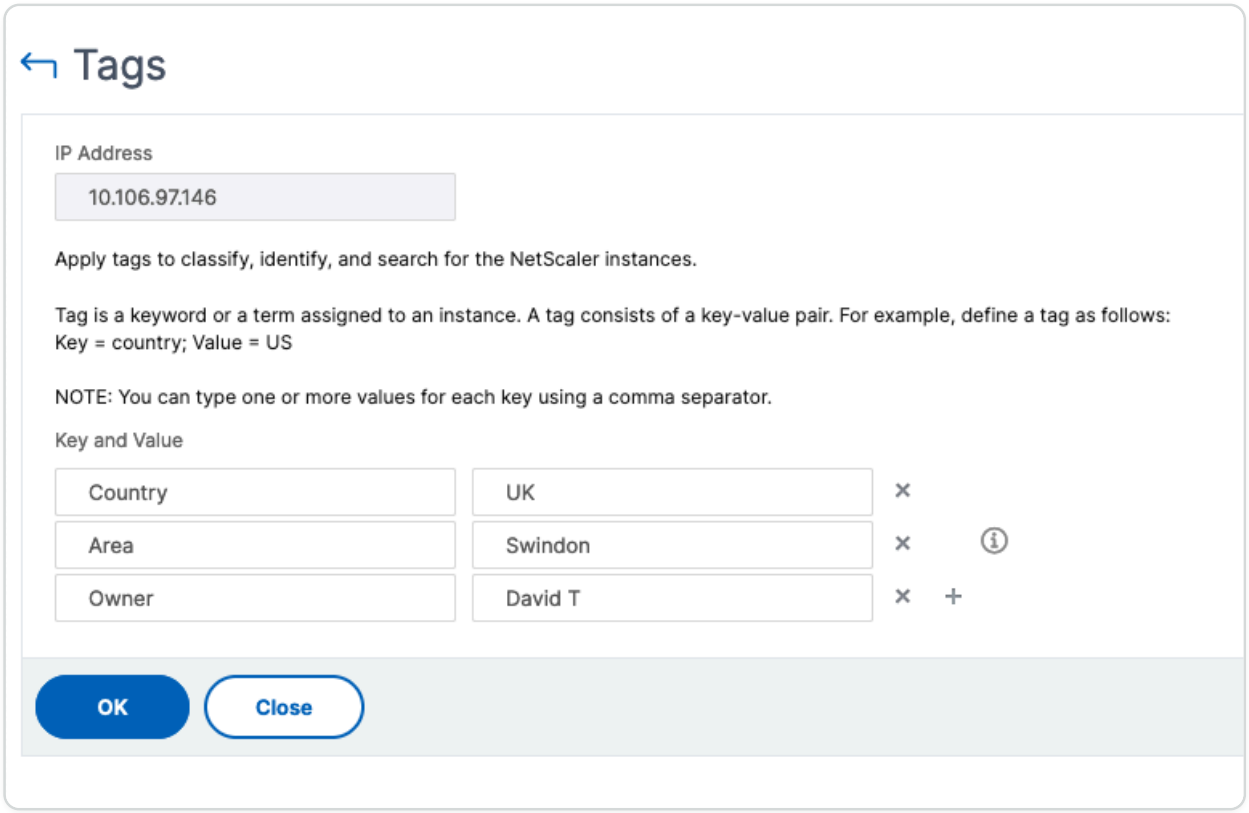
   For example, the following images show a few keywords created and their values. You can add your own keywords and type a value for each keyword.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



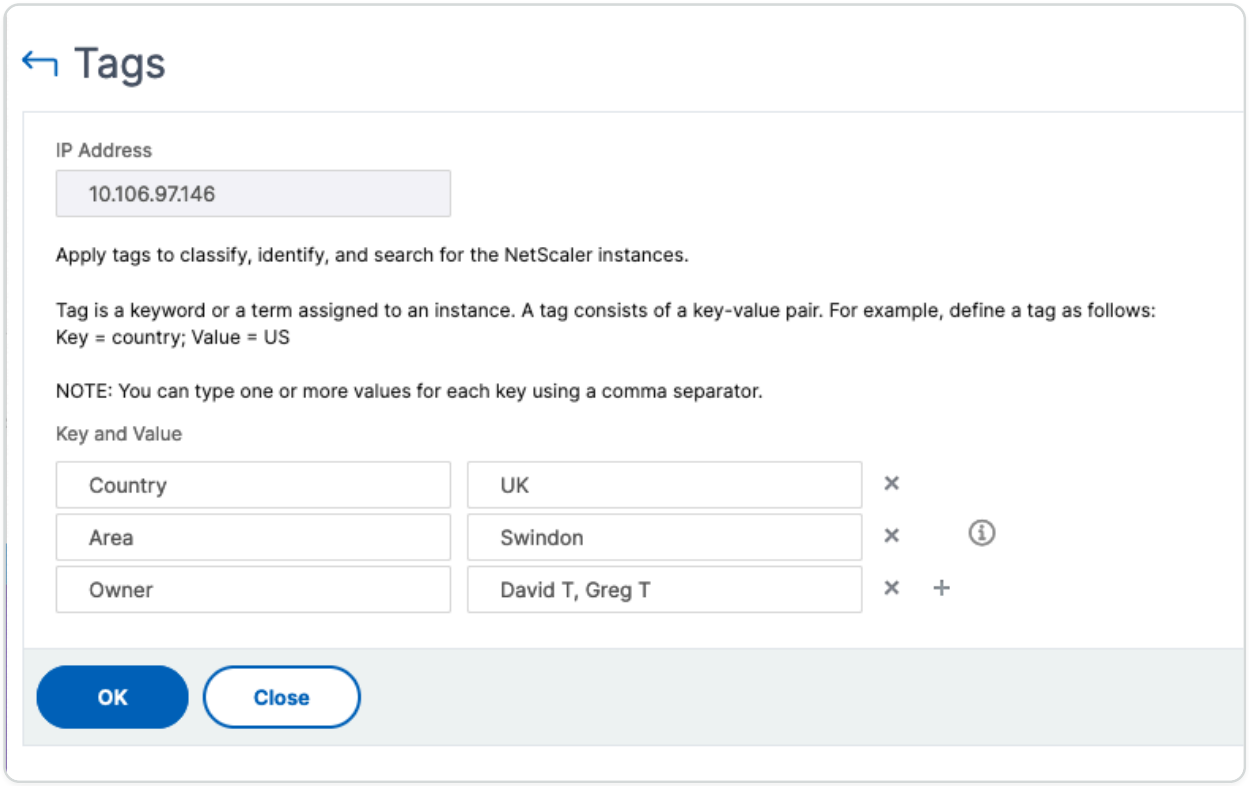
You can also add multiple tags by clicking "+". Adding multiple and meaningful tags allows you to efficiently search for the instances.



You can add multiple values to a keyword by separating them with commas.

For example, you are assigning the admin role to another coworker, Greg T. You can add his name separated by a comma. Adding multiple names helps you to search by either of the names or by both names. NetScaler Console recognizes the comma separated values into two different values.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



To know more about how to search for instances based on tags, see How to search instances using values of tags and properties.

5. Click **OK**.

NOTE

You can later add new tags or delete existing tags. There is no restriction on the number of tags that you create.

How to search instances using values of tags and properties

There might be a situation where NetScaler Console is managing many NetScaler instances. As an admin, you might want the flexibility to search on the instance inventory based on certain parameters. NetScaler Console now offers improved search capability to search a subset of NetScaler instances based on the parameters that you define in the search field. You can search for the instances based on two criteria - tags and properties.

- **Tags**. Tags are terms or keywords that can be assigned by you to a NetScaler instance to add some additional description about the NetScaler instance. You can now associate your NetScaler instances with tags. These tags can be used to better identify and search on the NetScaler instances.
- **Properties**. Each NetScaler instance added in NetScaler Console has a few default parameters or properties associated with that instance. For example, each instance has its own

© 1997–2026 Citrix Systems, Inc. All rights reserved.

host name, IP address, version, host ID, hardware model ID and so on. You can search for instances by specifying values for any of these properties.

For example, consider a situation where you want to find out the list of NetScaler instances that are on version 12.0 and are in the UP state. Here, the version and the state of the instance are defined by the default properties.

Along with the 12.0 version and UP state of the instances, you can also search those instances owned by you. You can create an "Owner" tag and assign a value "David T" to that tag. For more information on how to create and assign tags, see How to create tags and assign to instances.

You can use a combination of tags and properties to create your own search criteria.

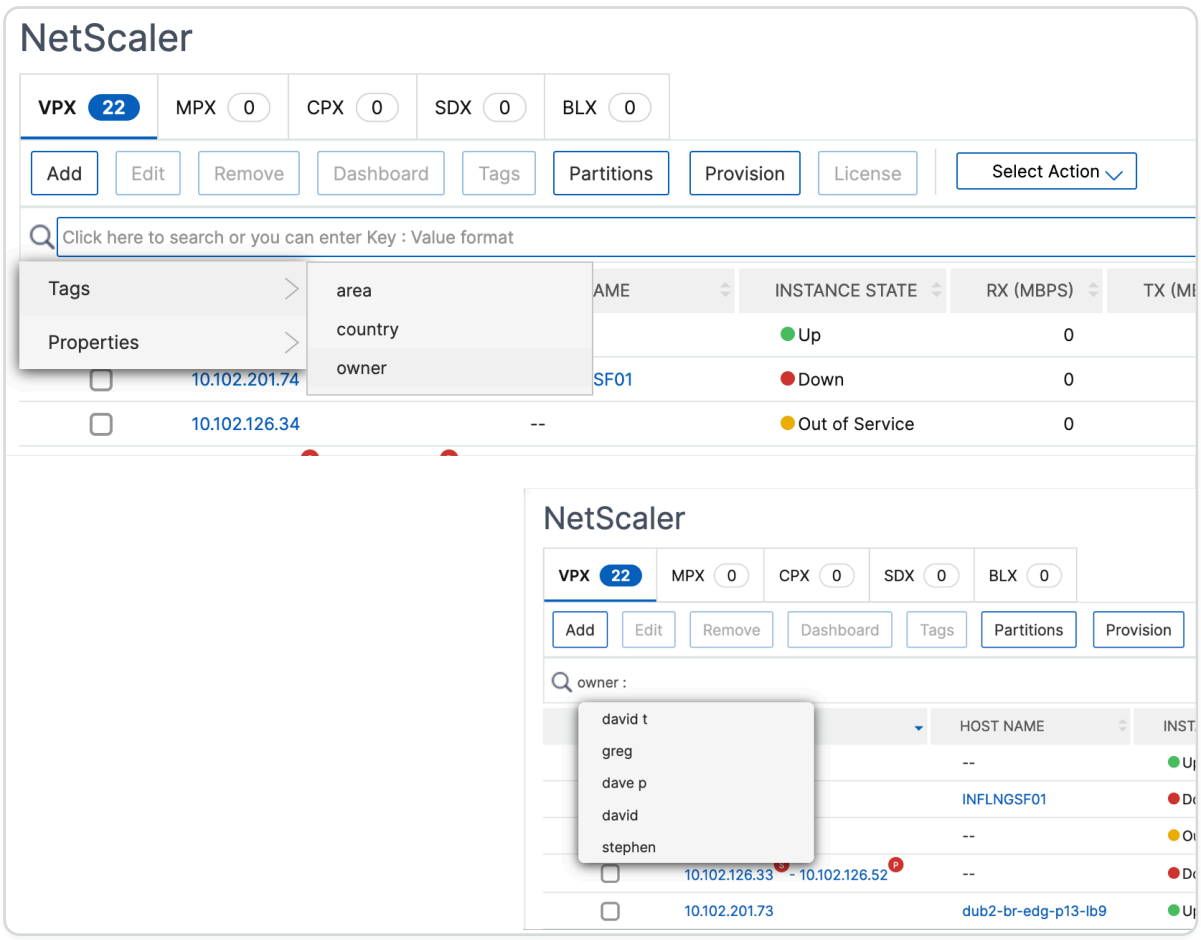
To search for NetScaler VPX instances

1. In NetScaler Console, navigate to **Infrastructure > Instances > NetScaler**.
2. Select the **VPX** tab.
3. Click the search field. You can create a search expression by using Tags or Properties or by combining both.

   The following examples show how you can use the search expression efficiently to search for the instance.

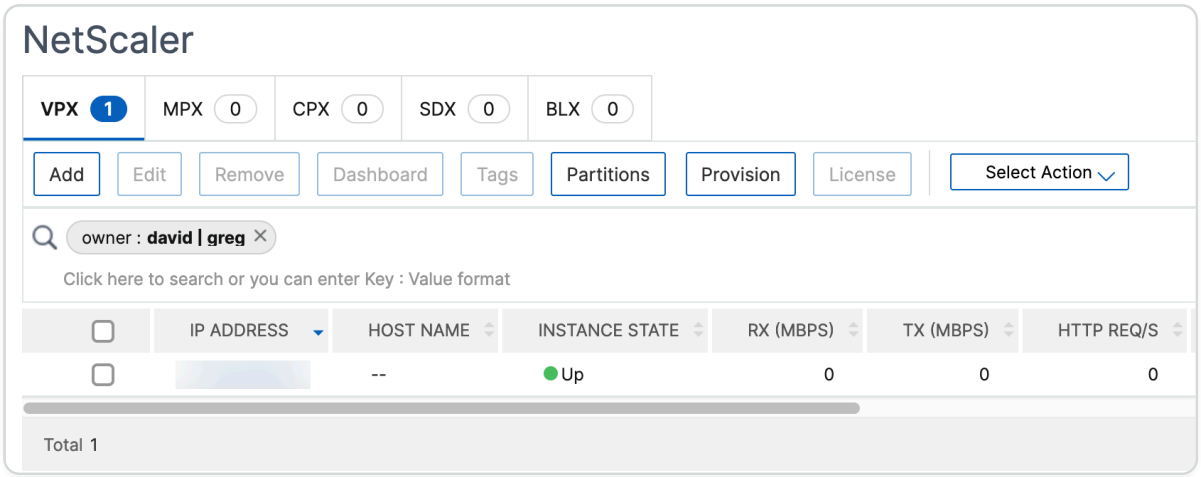
   a. Select **Tags** option and select **Owner**. Select "David T".

© 1997–2026 Citrix Systems, Inc. All rights reserved.



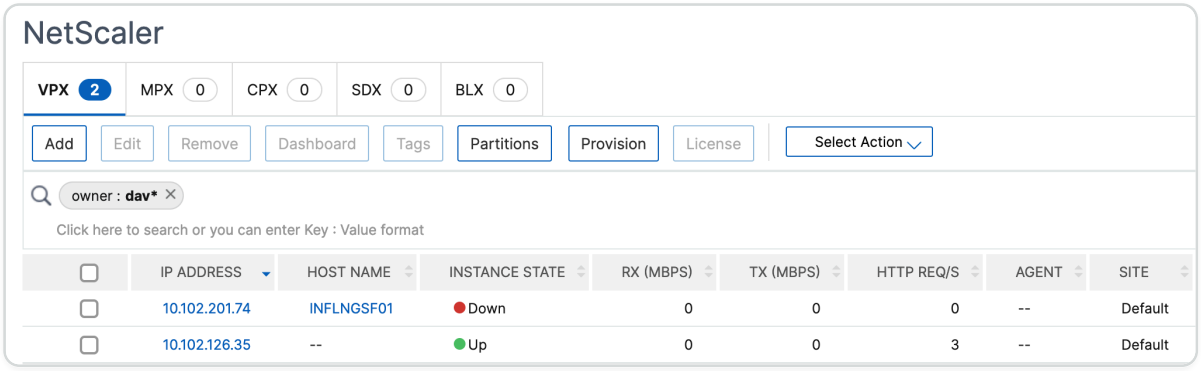
NetScaler Console supports regular expressions and wildcard characters in the search expressions.

a. You can use regular expressions to further expand the search criteria. For example, you want to search instances owned by either David or Stephen. In such a case, you can type the values by separating the values with a "\|" expression.



b. You can also use wildcard characters to replace or represent one or more characters. For example, you can type `Dav*` to search for all instances owned by "David" and "Dave P".

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE:

For more information on regular expressions and wildcard characters and how to use them, click the "information" icon in the search bar.

Centralized GeoIP DB Updates through NetScaler® Console

NetScaler Console allows administrators to upload the GeoIP DB (Geolocation Database) file from MaxMind directly through the NetScaler Console. You can either push the GeoIP DB file immediately to managed NetScaler instances or schedule the update for a later time. These files are essential for accurate IP-to-location mapping, commonly used in GSLB and security policies.

With this enhancement you also get update history tracking, which allows you to view whether an update was successful or failed. Also, you can view, delete, or download previously uploaded or pushed GeoIP DB versions from NetScaler Console. This enhancement also introduces manual update of GeoIP DB file in NetScaler Console, version control, and automated update workflows, allowing seamless GeoIP DB updates without impacting GSLB services.

Previously, NetScaler did not have a centralized mechanism for managing GeoIP DB updates on NetScaler. Administrators had to perform the updates manually on each device, which was time-consuming, error-prone, and disruptive in production environments.

This enhancement provides the following benefits:

- **Automation**: The update process is automated and performed without scheduled downtime and therefore reduces operational overhead.
- **Effective scalability**: Managing updates across multiple NetScaler instances is efficient and easy to scale.
- **Version control**: If an issue arises, you can track the historical versions, upload, and sync an older GeoIP DB file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Limitations

- **Format Conversion Support Limited to MaxMind**: The automatic format conversion is supported only for MaxMind files. For other vendors, files must already be in the supported format.
- **Deletion Limitation**: Deleting a file that is actively in use is not allowed. Ensure no active dependency before removal.

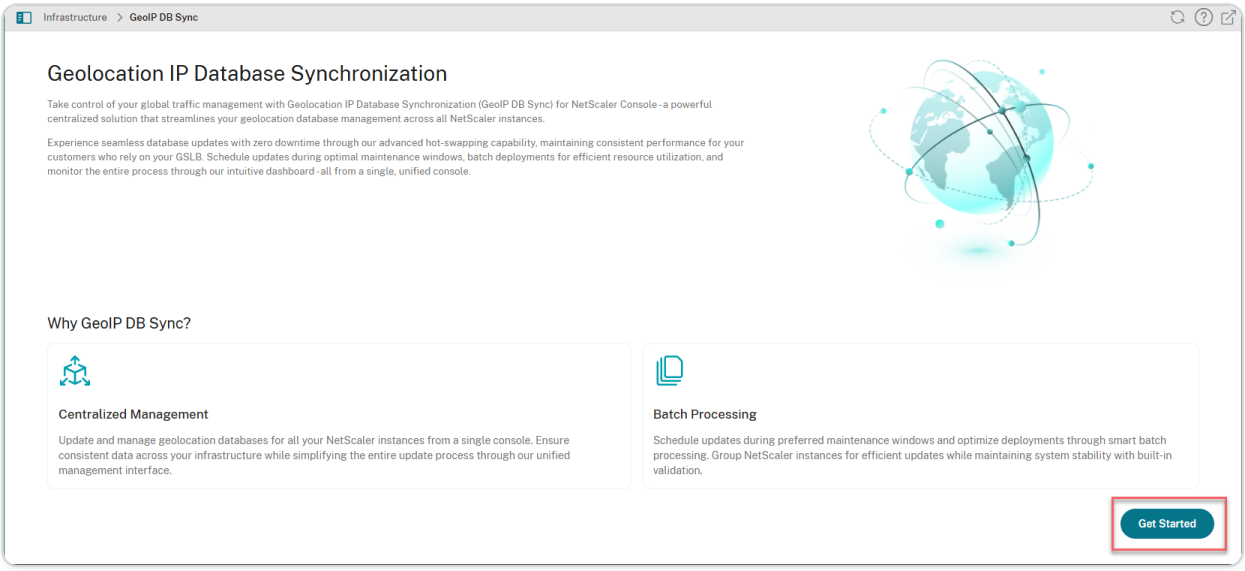
Configuring centralized GeoIP DB Updates through NetScaler Console

Prerequisites

- Ensure that you have a valid MaxMind license required to use GeoIP DB files.
- If you are using file format for other vendor files, ensure that the files are in supported format.

Perform the following steps to upload the GeoIP DB file from MaxMind or any other vendor:

1. Navigate to **Infrastructure > GeoIP DB Sync** and click **Get Started**.



2. Select one of the following options:
    - **Local**: You can upload a file from your local system.
    - **Appliance**: You can choose a file that is already present on a NetScaler Console.

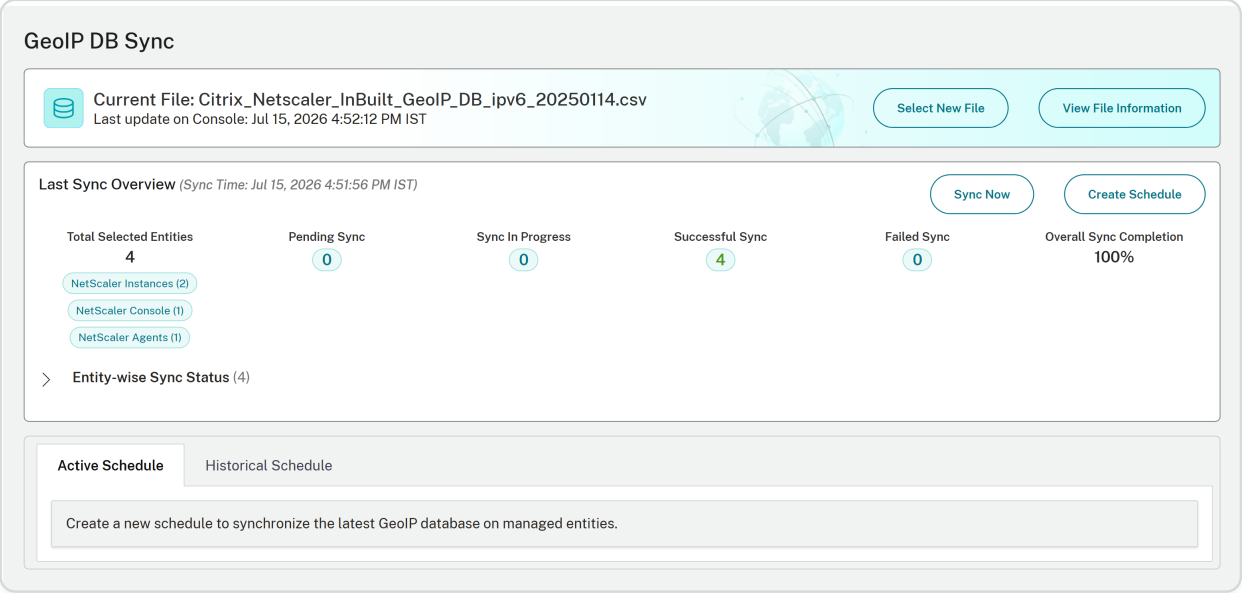
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTES:

- If you are uploading the GeoIP DB file for the first time, you do not see the **Appliance** option. Only if the file is already uploaded, then the **Appliance** option appears during subsequent uploads.
- If you upload a MaxMind file, the NetScaler Console service automatically converts the file to the format that NetScaler recommends during the upload. If you upload a file from other providers, then it must in CSV format and adhere to the following field order recommended by NetScaler: IP range, country code, region, city.

3. After uploading the file, choose one of the following actions:

   - **Sync Now:** Proceed immediately to the sync configuration dialog.
   - **Create Schedule:** Select a future date and time to deploy the file to the target entities.



4. If you click **Sync Now**, choose one of the following deployment modes:

   - **Sync all:** Automatically distributes the GeoIP DB file to all NetScaler instances, agents, and NetScaler Console.
   - **Customize:** Manually select your targets:
     - **Select NetScaler Console:** Displays NetScaler Console to which you are currently logged in.
     - **Select NetScaler Instances:** Filters and identifies specific instances using the group dropdown menu or a Key:Value search.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

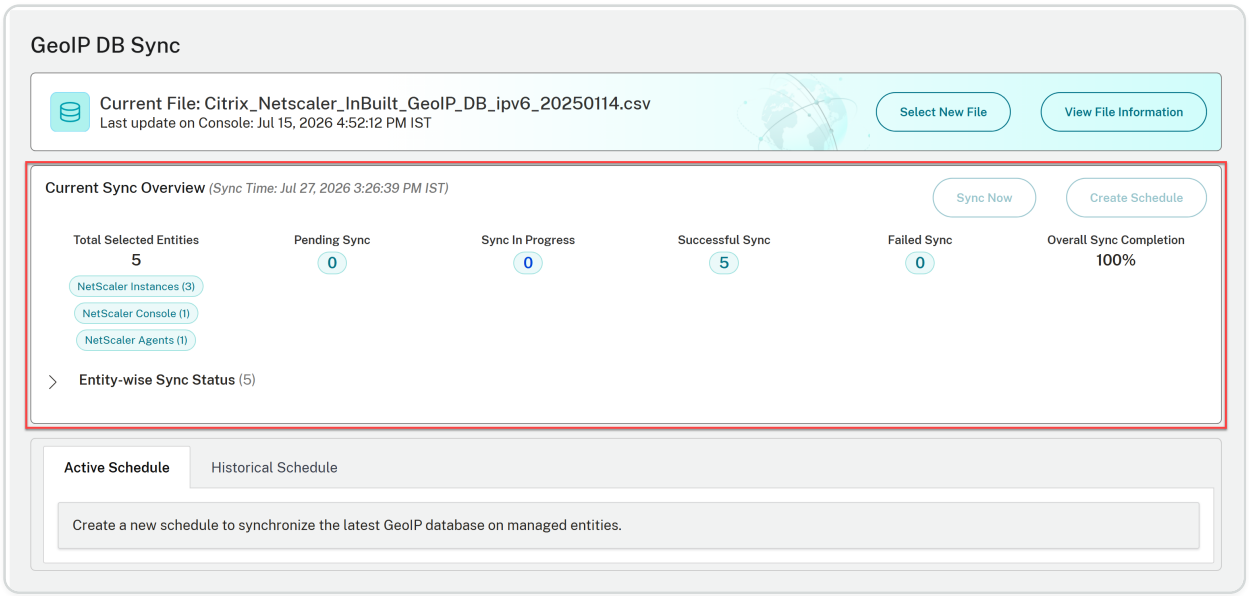
- **Select Agents:** Displays a list of available agents.

Before clicking **Start Sync**, answer the prompt: *"Does the current file contain IPv6?"*. Select **Yes** *only* if your GeoIP file contains IPv6 address blocks. This setting dictates how each target entity parses the data.

5. Monitor the progress and results on the **GeoIP DB Sync** page. The **Last Sync Overview** panel displays the following metrics:

   - **Total Selected Entities:** The combined count of all targeted NetScaler Console instances, and agents.
   - **Pending Sync:** The entities that are queued but not yet started.
   - **Sync In Progress:** The entities that are actively receiving the file.
   - **Successful Sync:** The entities that completed without error.
   - **Failed Sync:** The entities that encountered an error.
   - **Overall Sync Completion:** The percentage of selected entities that completed successfully.

   Expand **Entity-wise Sync Status** to view a per-device table that lists the IP address, host name, type, state, version, and sync status. Use the filter bar to narrow the results by any field, for example, **Sync Status: Completed**.



6. Based on your requirement, perform any of the following actions from the **GeoIP DB Sync** page:

   - **Select New File:** Upload a GeoIP DB file from your local system, or select an already uploaded file from NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **View File Information:** Review the previously uploaded files. If an issue arises, you can track historical versions, upload, and sync an older GeoIP DB file.
- **Active Schedule:** View the upcoming scheduled sync jobs that are yet to run.
- **Historical Schedule:** View the completed GeoIP DB sync operations. Each entry shows the entity scope (for example, **2 NetScaler Instances, 1 Agent, and NetScaler Console**), the execution timestamp, and the GeoIP file used. Click any entry to view the full job detail, including per-entity sync results (status, start time, and end time) for the NetScaler Console instances, and agents individually.

Manage admin partitions of NetScaler instances

You can configure admin partitions on your Citrix Application Delivery Controller (NetScaler) instances so that different groups in your organization are assigned different partitions on the same NetScaler instance. You can assign a network administrator to manage multiple partitions on multiple NetScaler instances.

NetScaler Console provides a seamless way of managing all partitions owned by an administrator from a single console. You can manage these partitions without disrupting other partition configurations.

To allow multiple users to manage different admin partitions, you have to create groups and then, assign users and partitions to those groups. For more information about creating a group or user, see (../../setting-up/configuring-role-based-access-control.md#configure-users-on-NetScaler Console) and (../../setting-up/configuring-role-based-access-control.md#configure-groups-on-NetScaler Console).

A user can view and manage only the partitions in the group to which the user belongs. When you discover a NetScaler instance, the admin partitions configured on that NetScaler instance get added to the system automatically. Each admin partition is considered as an instance in NetScaler Console.

View admin partitions

Consider that you have two NetScaler VPX instances and two admin partitions are configured on each instance. For example, NetScaler instance 10.xx.xx.100 has partition-1 and partition-2 and the 10.xx.xx.101 instance has first-partition and second-partition.

Perform the following steps to view admin partitions:

1. Navigate to **Infrastructure > Instances > NetScaler**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. In the **VPX** tab, click **Partitions**.

For example, if you create a group with the following conditions:

- In **Settings > Users & Roles > Create Group > Authorization Settings > Select Instances**, you select "10.xx.xx.100-partition-1" and "10.xx.xx.101-first-partition" instances.
- You assign "User1" to the group.

User1 can view and manage only those partitions that are added to the group. However, the partitions that are not added to the group are restricted to the user even though they belong to the same instances.

In this example, 10.xx.xx.100-partition-2 and 10.xx.xx.101-second-partition are restricted because the instances are not added to the group where the user is assigned.

If you want a different user to manage the admin partitions 10.xx.xx.100-partition-2 and 10.xx.xx.101-second-partition, create a group with the following conditions:

- In the **Authorization Settings** tab, select the 10.xx.xx.100-partition-2 and 10.xx.xx.101-second-partition instances.
- Assign the required user to the group.

This group enables the assigned user to view and manage the selected admin partitions.

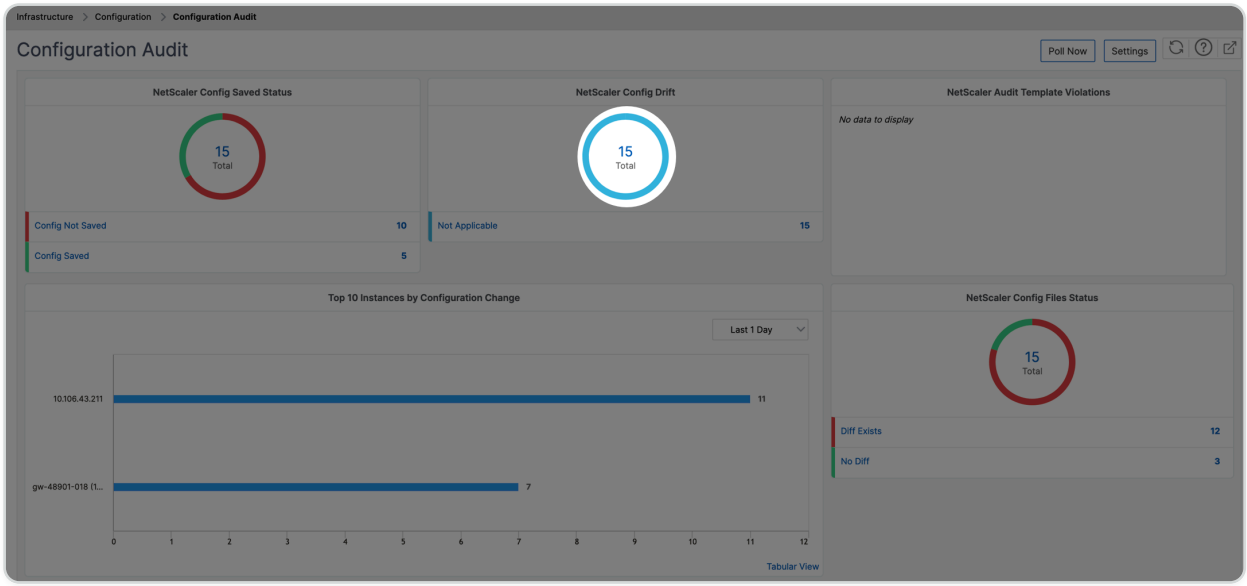
View the revision history difference

Revision history difference for an admin partition allows you to view the difference between the five latest configuration files for a partitioned NetScaler instance. You can compare the configuration files against each other (example Configuration Revision - 1 with Configuration Revision -2) or against the current running/saved configuration with Configuration Revision. Along with the differences in configuration, the correction configurations are also shown. You can export all the corrective commands to your local folder and correct the configurations.

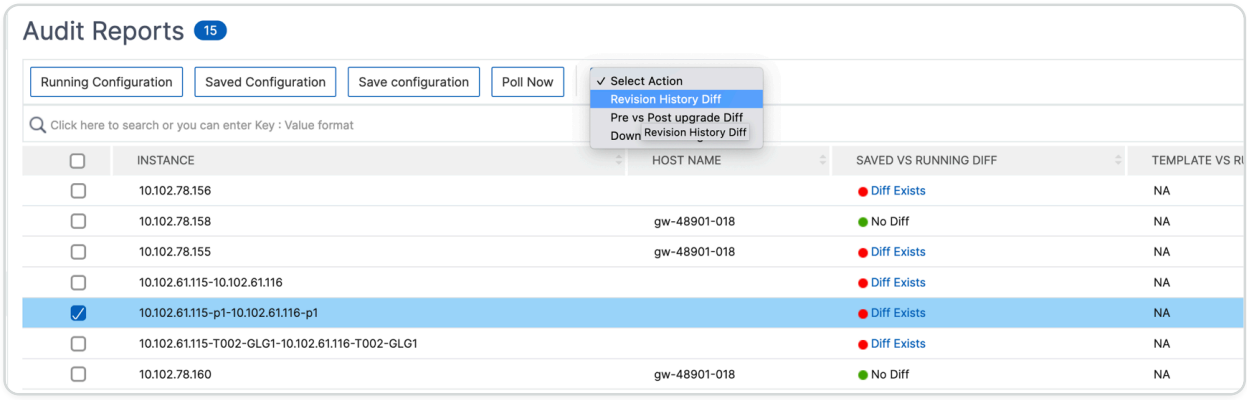
To view the revision history difference:

1. Navigate to **Infrastructure > Configuration > Configuration Audit**. The Configuration Audit dashboard displays various reports. Click the number displayed in the center of the donut chart.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



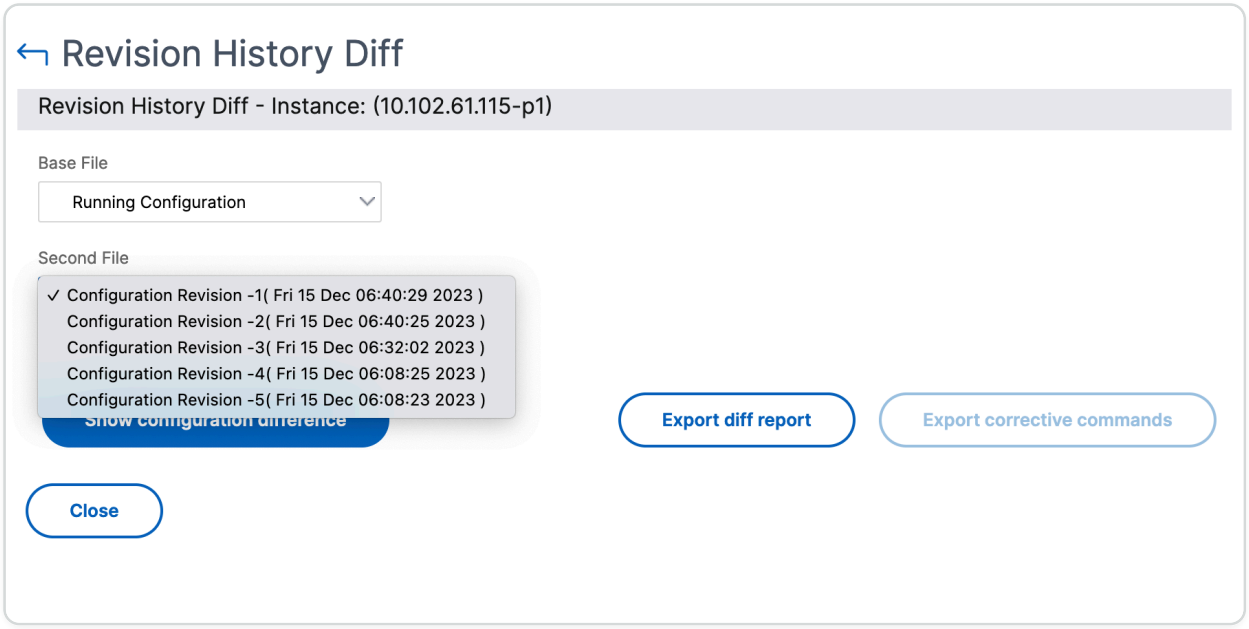
2. Select the partitioned NetScaler instance.
3. From the Action box, click **Revision History Diff.**



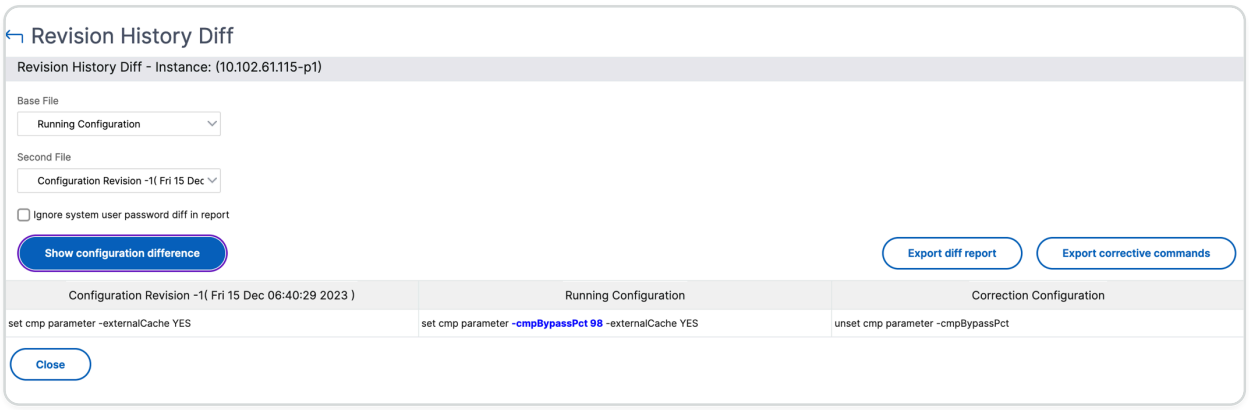
4. On the **Revision History Diff** page, select the files that you want to compare. For example, compare the Saved Configuration with Configuration Revision-2 and then, click **Show configuration difference**.

   You can then view the differences between the five latest configuration files for the selected partitioned NetScaler instance. The following is an example admin partition that has five saved configurations:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

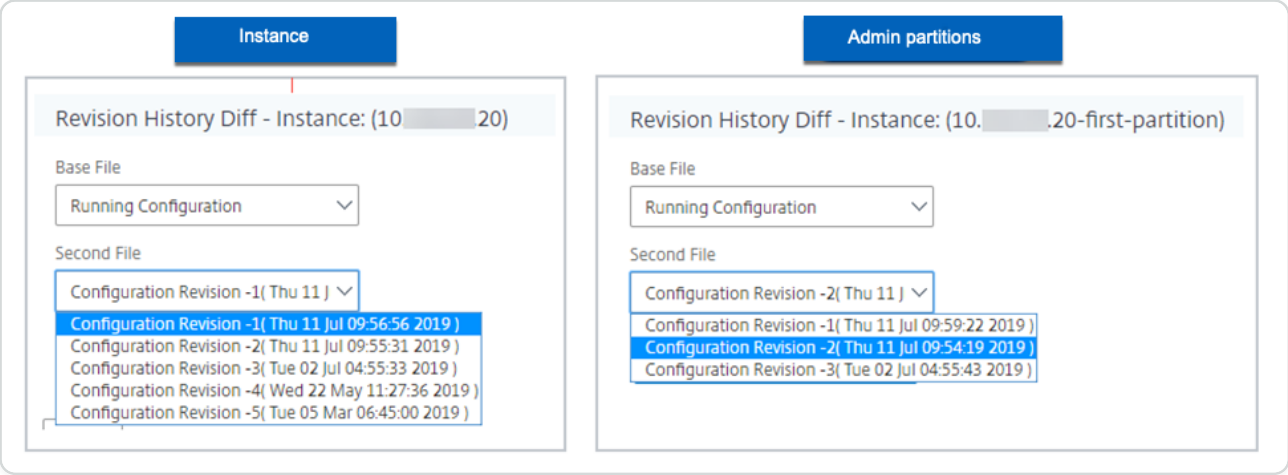


You can also view the corrective configuration commands and export these corrective commands to your local folder. These corrective commands are the commands that need to be run on the base file to get the configuration to the desired state (configuration file that is being used for comparison).



The saved configurations on an admin partition and the instance are different. In the following example, the 10.xx.xx.20 instance has five saved configurations where the admin partition of this instance has three different saved configurations:

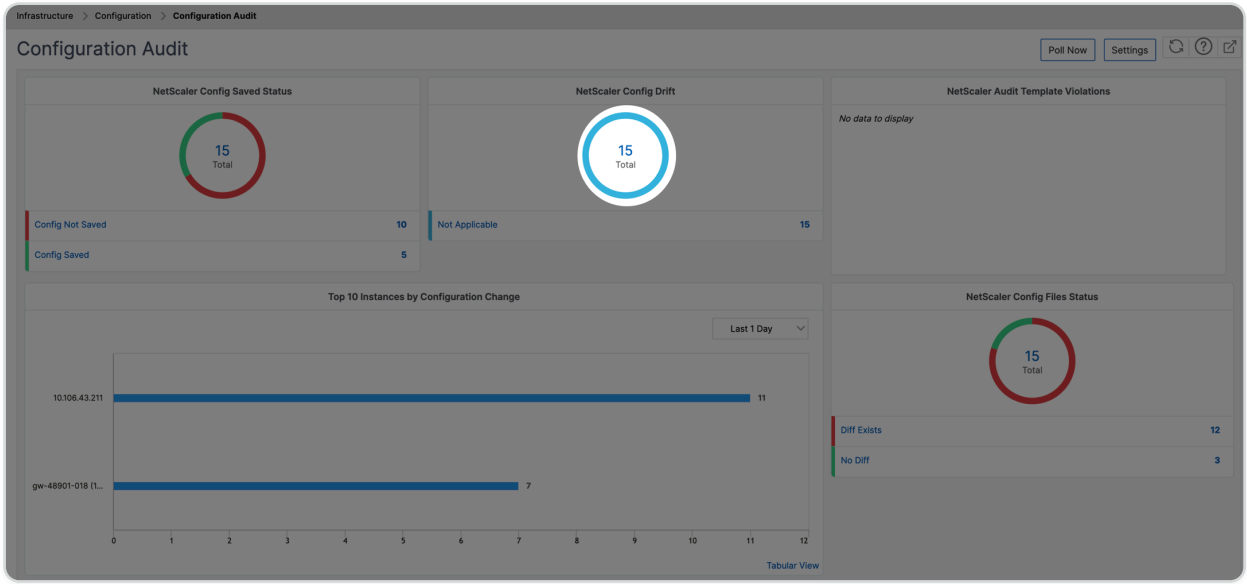
© 1997–2026 Citrix Systems, Inc. All rights reserved.



View the template vs running difference

Audit templates for partition allow you to create a custom configuration template and associate it with a partition instance. Any variation in the running configuration of the instance with the audit template is shown in the "**Template vs Running diff**" column of the **Audit Reports** page. Along with the differences in configuration, the correction configurations are also shown. You can also export all the corrective commands to your local folder and correct the configurations.

1. Navigate to **Infrastructure > Configuration > Configuration Audit**. The Configuration Audit dashboard displays various reports. Click the number displayed in the center of the donut chart.

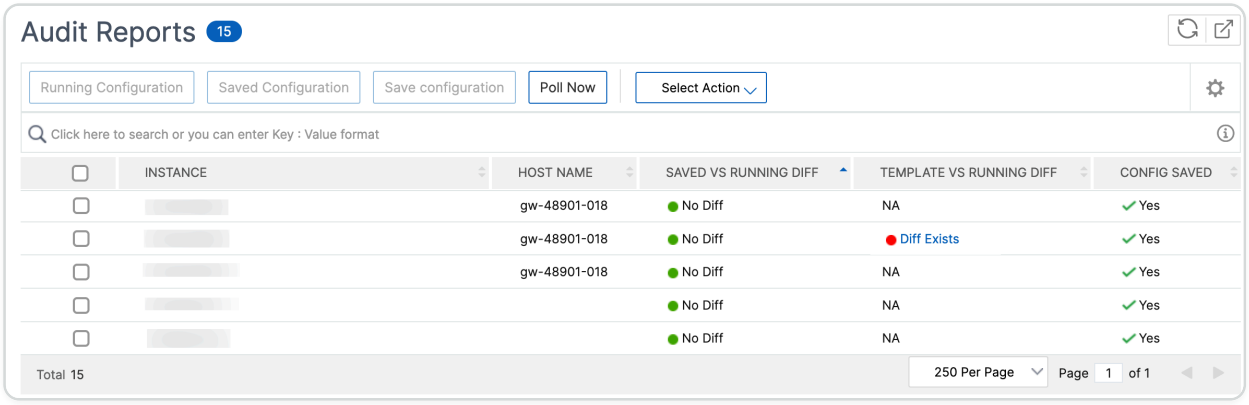


2. In the **Audit Reports** page, click the **Diff Exists** hyperlink under the Template vs Running Diff column.

   If there is any difference between the audit template and the running configuration, the difference is shown as a hyperlink. Click the hyperlink to view the differences if there is any.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Along with the differences in configuration, the correction configurations are also shown. You can also export all the corrective commands to your local folder and correct the configurations.



To export the report of this dashboard:

To export the report of this page, click the **Export** icon on the top right side of this page. On the **Export** page, you can do one of the following:

1. Select **Export Now** tab. To view and save the report in PDF, JPEG, PNG, or CSV format.
2. Select **Schedule Export** tab. To schedule the report daily, weekly, or monthly and send the report over an email or a slack message.

NOTE:

- If you select **Weekly** recurrence, ensure that you select the weekdays on which you want the report to be scheduled.
- If you select **Monthly** recurrence, ensure that you enter all the days that you want the report to be scheduled separated by commas.

Back up and restore NetScaler instances

You can back up the current state of a Citrix Application Delivery Controller (NetScaler) instance and later use the backed-up files to restore the NetScaler instance to the same state. You must always back up an instance before you upgrade it or for precautionary reasons. A backup of a stable system enables you to restore it back to a stable point if it becomes unstable. There are multiple ways to perform backups and restores on a NetScaler instance. You can manually backup and restore NetScaler configurations using the GUI, CLI, or you can use NetScaler Console to perform automatic backups and manual restores. NetScaler Console backs up the current state of

© 1997–2026 Citrix Systems, Inc. All rights reserved.

your managed NetScaler instances by using NITRO calls and the Secure Shell (SSH) and Secure Copy (SCP) protocols.

NetScaler Console creates a complete backup and restores the following NetScaler instance types:

- NetScaler SDX
- NetScaler VPX
- NetScaler MPX
- NetScaler BLX

For more information, see Backup and restore a NetScaler instance.

NOTE:

- From NetScaler Console, you cannot perform the backup and restore operation on a NetScaler cluster.
- You cannot use the backup file taken from one instance to restore a different instance.

The backed-up files are stored as a compressed TAR file in the following directory:

```
/var/mps/tenants/root/tenants/<specify-the-tenant-name>/device_backup/
```

To avoid issues due to non-availability of disk space, you can save a maximum of three backup files in this directory.

To back up and restore NetScaler instances, you must first configure the backup settings on NetScaler Console. After configuring the settings, you can select a single NetScaler instance or multiple instances and create a backup of the configuration files in these instances. If necessary you can also restore the NetScaler instances by using these backed-up files.

Create a backup for a selected NetScaler instance by using NetScaler Console

Perform this task if you want to back up a selected NetScaler instance or multiple instances:

1. In NetScaler Console, navigate to **Infrastructure > Instances**. Under **Instances**, select the type of instances (for example, VPX) to display on the screen.
2. Select the instance that you want to back up.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For MPX, VPX, and BLX instance, select **Backup/Restore** from the **Select Action** list.
- For an SDX instance, click **Backup/Restore**.

3. On the **Backup Files** page, click **Back Up**.
4. Specify whether to encrypt your backup file for more security. You can either enter your password or use the global password that you previously specified on the Instance Backup Settings page.
5. Click **Continue**.

Transfer a backup file to an external system

You can transfer a copy of your backup file to another system as a precautionary measure. When you want to restore the configuration, you have to first upload the backup file to the NetScaler Console server and then perform the restore operation.

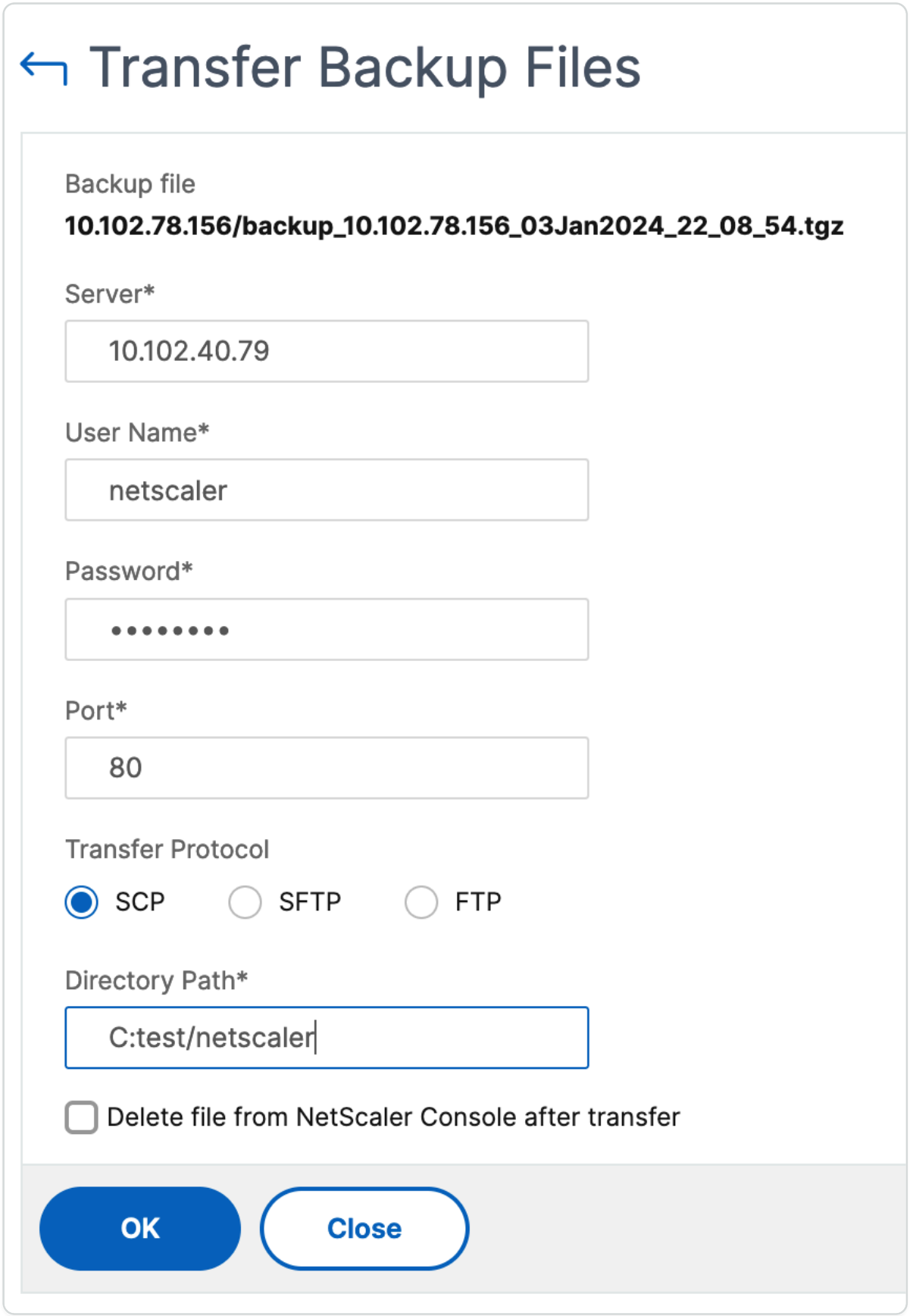
To transfer a NetScaler Console backup file:

1. Navigate to **Infrastructure > Instances > NetScaler** and then select the instance type. For example, VPX.
2. Select the instance and from the **Select Action** list, select **Backup/Restore**.
3. Select the backup file and then click **Transfer**.

   The **Transfer Backup File** page is displayed. Specify the following parameters:

   a. **Server** - IP address of the system where you want to transfer the back-up file.
   b. **User name** and **password** – User credentials of the new system, where the backed-up files are being copied.
   c. **Port** – Port number of the system the files are being transferred to.
   d. **Transfer protocol** – Protocol being used to make the backup file transfer. You can select SCP, SFTP, or FTP protocols to transfer the back-up file.
   e. **Directory path** – The location where the backed-up file is being transferred to on the new system.
   f. Click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The backup files from the NetScaler Console service are sent to the external server through an agent. If there are many agents, a NetScaler backup file is sent through the same agent which was used to add that NetScaler instance. To know more about the instances associated with an agent, navigate to **Infrastructure > NetScaler > Agents**.

Restore a NetScaler instance by using NetScaler Console

NOTE:

If you have NetScaler instances in a HA pair, you need to note the following:

- Restore the same instance from which the backup file was created. For example, let us consider a scenario that a backup was taken from the primary instance of the HA pair. During the restore process, ensure that you are restoring the same instance, even if it is no longer the primary instance.
- When you initiate the restore process on the primary NetScaler instance, you cannot access the primary instance and the secondary instance gets changed to **STAYSECONDARY**. Once the restore process is completed on the primary instance, the secondary NetScaler instance changes from **STAYSECONDARY** to **ENABLED** mode and becomes part of the HA pair again. You can expect a possible downtime on the primary instance until the restore process gets completed.

Perform this task to restore a NetScaler instance by using the backup file that you created earlier:

1. Navigate to **Infrastructure > Instances**, select the instance that you want to restore, and then click **View Backup**.
2. On the **Backup Files** page, select the backup file containing the settings that you want to restore, and then click **Restore**.

NOTE:

To upload an externally transferred backup file, use the **Upload** button.

Restore a NetScaler SDX appliance using NetScaler Console

In NetScaler Console, the backup of a NetScaler SDX appliance includes the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler instances hosted on the appliance
- SVM SSL certificates and keys
- Instance prune settings (in XML format)
- Instance backup settings (in XML format)
- SSL certificate poll settings (in XML format)
- SVM db file
- NetScaler config files of devices present on SDX
- NetScaler build images
- NetScaler XVA images, these images are stored in the following location: `/var/mps/sdx_images/`
- SDX Single Bundle Image (SVM+XS)
- Third Party instance images (if provisioned)

You must restore your NetScaler SDX appliance to the configuration available in the backup file. During appliance restore, the entire current configuration is deleted.

If you are restoring the NetScaler SDX appliance by using a backup of a different NetScaler SDX appliance, make sure that you add the licenses and configure the appliance's Management Service network settings to match those in the backup file before you start the restore process.

Ensure that the NetScaler SDX platform variant that was backed up was taken is the same as the one on which you are trying to restore. You cannot restore from a different platform variant.

NOTE:

Before you restore the SDX RMA appliance, ensure that the backed-up version is either the same or higher than the RMA version.

To restore the SDX appliance from the backed-up file:

1. In the NetScaler Console GUI, navigate to **Infrastructure > Instances > NetScaler**.
2. Click **Backup/Restore**.
3. Select the backup file of the same instance that you want to restore.
4. Click **Repackage Backup**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When the SDX appliance is backed up, the XVA files and images are stored separately to save the network bandwidth and the disk space. Therefore, you must repackage the backed-up file before you restore the SDX appliance.

When you repackage the backup file, it includes all the backed-up files together to restore the SDX appliance. The repackaged backup file ensures the successful restoration of the SDX appliance.

5. Select the backup file that is repackaged and click **Restore**.

Export the report of this dashboard

To export the report of this page, click the **Export** icon on the top right side of this page. On the **Export** page, you can do one of the following:

1. Select **Export Now** tab. To view and save the report in PDF, JPEG, PNG, or CSV format.
2. Select **Schedule Export** tab. To schedule the report daily, weekly, or monthly and send the report over an email or a slack message.

NOTE

- If you select **Weekly** recurrence, ensure that you select the weekdays on which you want the report to be scheduled.
- If you select **Monthly** recurrence, ensure that you enter all the days that you want the report to be scheduled separated by commas.

Force a failover to the secondary NetScaler instance

You might want to force a failover if, for example, you need to replace or upgrade the primary Citrix Application Delivery Controller (NetScaler) instance. You can force failover from either the primary instance or the secondary instance. When you force a failover on the primary instance, the primary becomes the secondary and the secondary becomes the primary. Forced failover is only possible when the primary instance can determine that the secondary instance is UP.

A forced failover is not propagated or synchronized. To view the synchronization status after a forced failover, you can view the status of the instance.

A forced failover fails in any of the following circumstances:

- You force failover on a standalone system.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The secondary instance is disabled or inactive. If the secondary instance is in an inactive state, you must wait for its state to be UP to force a failover.
- The secondary instance is configured to remain secondary.

The NetScaler instance displays a warning message if it detects a potential issue when you run the force failover command. The message includes the information that triggered the warning, and requests confirmation before proceeding.

You can force a failover on a primary instance or on a secondary instance.

To force a failover to the secondary NetScaler instance using NetScaler Console:

1. In NetScaler Console, navigate to **Infrastructure > Instances**. Go to **VPX** tab and select an instance.
2. Select instances in an HA setup from the instances listed under the selected instance type.
3. From the **Action** box, select **Force Failover.**
4. Click **Yes** to confirm the force failover action.

Force a secondary NetScaler instance to stay secondary

In a High Availability (HA) setup, the secondary node can be forced to stay secondary regardless of the state of the primary node.

For example, suppose that the primary node needs to be upgraded and the process takes a few seconds. During the upgrade, the primary node might go down for a few seconds, but you do not want the secondary node to take over, and you want it to remain the secondary node even if it detects a failure in the primary node.

When you force the secondary node to stay secondary, it remains secondary even if the primary node goes down. Also, when you force the status of a node in an HA pair to stay secondary, it does not participate in HA state machine transitions. The status of the node is displayed as STAYSECONDARY.

NOTE

When you force a system to remain secondary, the forcing process is not propagated or synchronized. It affects only the node on which you run the command.

To configure a secondary NetScaler instance to stay secondary by using NetScaler Console:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. In NetScaler Console, navigate to **Infrastructure > Instances**, and then select an instance under an instance type (VPX).
2. Select instances in an HA setup from the instances listed under the selected instance type.
3. From the **Action** box, select **Stay Secondary**.
4. Click **Yes** to confirm the execution of the "Stay Secondary" action.

Create instance groups

To create an instance group, you must first add all your NetScaler instances to NetScaler Console. After you have added the instances successfully, create instance groups based on their instance family. Creating a group of instances helps you to upgrade, backup, or restore on the grouped instances at one time.

The **Instance View** allows you to view all managed instances along with their associated groups, making it easy to identify unmapped instances. You can assign unmapped instances to a group.

To create an instance group using NetScaler Console

1. In NetScaler Console, navigate to **Infrastructure > Instances > Instance Groups**, and then click **Add**.
2. Specify a name to your instance group and select **NetScaler** from the **Instance Family** list.
3. In **Category**, select the **Default** option.
4. Click **Select Instances**. On the **Select Instances** page, select the instances that you want to group and click **Select**.

   The table lists the selected instances and their details. If you want to remove any instance from the group, select the instance from the table and click **Delete**.
5. Click **Create**.

To identify and add unmapped instances to a group

1. Navigate to **Infrastructure > Instances > Instance Groups > Instances View**.
2. Select one or more unmapped instances.
3. Click **Add Instance Group**.
4. Select the required **Instance Group** from the list. The interface also displays:

   - Available instance groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Instances already mapped to each group, helping prevent duplicate or incorrect assignments.

5. Click **Save**. The selected instances are assigned to the chosen group.

Global Server Load Balancing site groups

When you want to ensure continuous availability and disaster recovery for your ADC instances, you can configure a GSLB site group. It balances the load across sites by directing client requests to the closest or best performing site, or to surviving sites if there is an outage.

Sometimes, in a GSLB site group, the configuration objects of the ADC instances try to overwrite each other. It leads to a race condition. To address such issues, you need to control the primary node selection in the GSLB site group. The configuration in the primary node will be applied to the remaining ADC instances. In NetScaler Console, you can create a GSLB site group and do the following:

- Choose a primary node among the selected ADC instances.
- Set the priority order for primary node selection if the selected primary node goes down.

You can view your GSLB site groups in **Infrastructure > Instances > GSLB Site Group**.

Create a GSLB site group

Do the following steps to create a GSLB site group with ADC instances:

1. Go to **Infrastructure > Instances > GSLB Site Group**.
2. Click **Add**.
3. Specify a name for the GSLB site group.
4. Select the instances that you want to add in the GSLB site group. These instances act as sites in the group.
5. Select at least one site and click **Make Active Site**.

   Instance that is set to priority `1` becomes the primary node. You can reorder the priority of the active sites. Select the lower priority instance and click **Move up priority**.
6. Click **Create**.

In **Infrastructure > Network Functions > GSLB**, the GUI displays the entities only from the primary ADC node of the GSLB site group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create SNMP managers and users for NetScaler agent

You can query the SNMP agent for system-specific information from a remote device called an SNMP manager. The agent then searches the management information base (MIB) for requested data and sends the data to the SNMP manager.

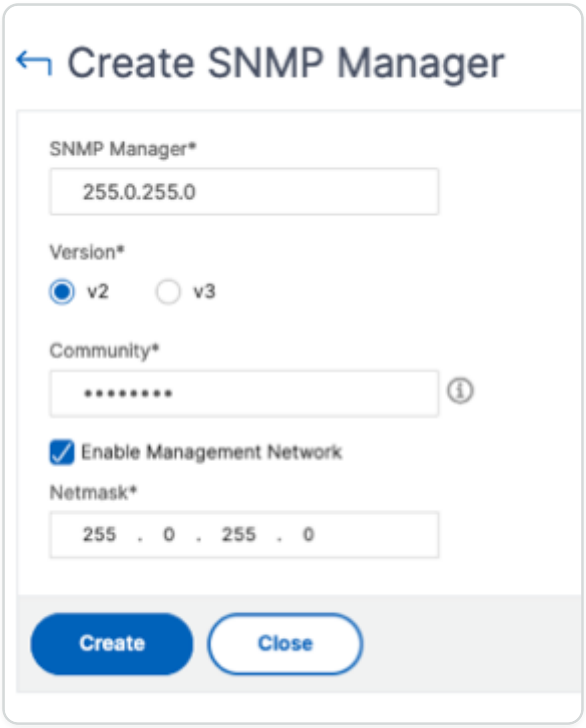
You can add an SNMP manager to query a NetScaler agent. The manager complies with SNMP V2 and V3. If you specify one or more SNMP managers, the NetScaler agent does not accept SNMP queries from any hosts except the specified SNMP managers.

Add an SNMP v2 manager

To add an SNMP v2 manager for the NetScaler agent:

1. Navigate to **Infrastructure > Instances > Agents**, select a NetScaler agent, and click **Select Action > Manage SNMP**.
2. In the **SNMP > SNMP Manager** tab, click **Add**.
3. In the **Create SNMP Manager** page, specify the following details:
    - **SNMP Manager**. Enter the name or IP address of the SNMP Manager.
    - **Version**. Select v2.
    - **Community**. Enter a community name. An SNMP community configuration authenticates SNMP queries from SNMP managers.
    - **Enable Management Network**: Select this checkbox to specify the netmask of the SNMP manager network.
    - **Netmask**: Enter the subnet mask associated with an IP address.
4. Click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

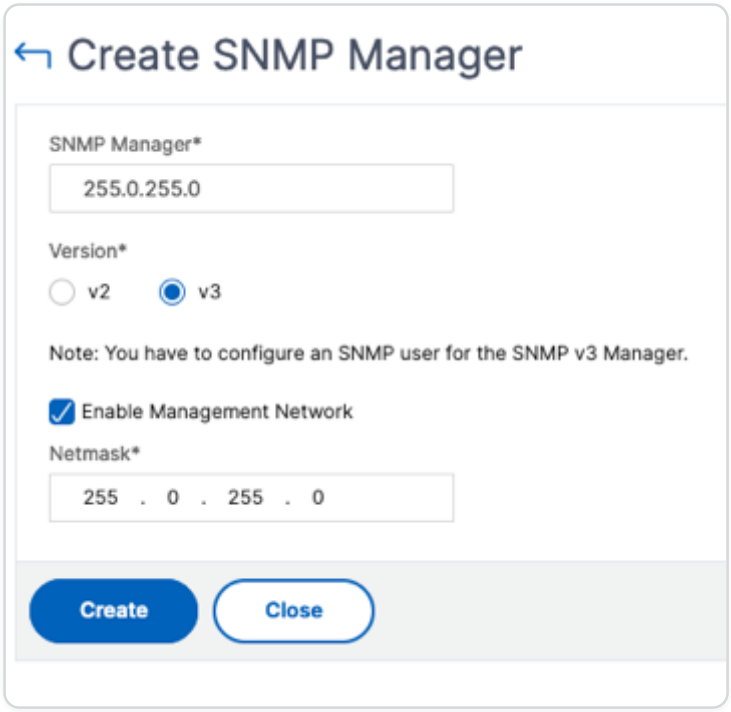


Add an SNMP v3 manager

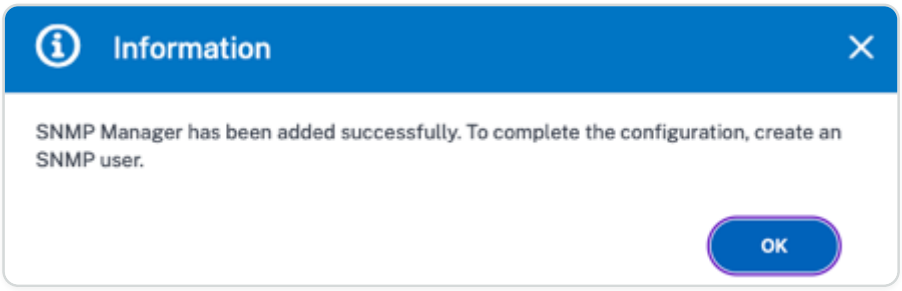
To add an SNMP v3 Manager for the NetScaler agent:

1. Navigate to **Infrastructure > Instances > Agents**, select a NetScaler agent, and click **Select Action> Manage SNMP**.
2. In the **SNMP > SNMP Manager** tab, click **Add**.
3. In the **Create SNMP Manager** page, specify the following details:
   - **SNMP Manager**. Enter the name or IP address of the SNMP Manager.
   - **Version**. Select v3.
   - **Enable Management Network**: Select this checkbox to specify the netmask of the SNMP manager network.
   - **Netmask**: Enter the subnet mask associated with an IP address.
4. Click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



A dialog box appears confirming that an SNMP manager is created and prompting you to configure an SNMP user.



NOTE:

You must configure an SNMP user for an SNMP v3 manager. To configure the SNMP user, go to **SNMP > SNMP User**.

Add an SNMP user

Add an SNMP user to respond to the SNMP v3 queries from an SNMP manager.

To add an SNMP user for the NetScaler agent:

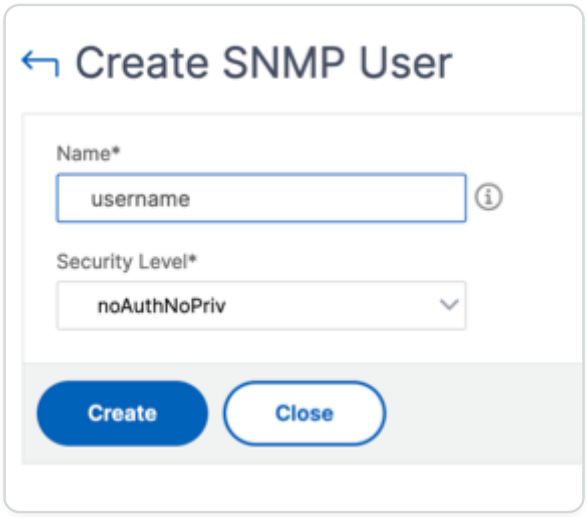
1. Navigate to **Infrastructure > Instances > Agents**, select a NetScaler agent, and click **Select Action > Manage SNMP**.
2. In the **SNMP > SNMP User** tab, click **Add**.
3. In the **Create SNMP User** page, add the following details:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Name**. Enter the user name.
- **Security Level**. Security level required for communication between the NetScaler agent and the SNMP manager.

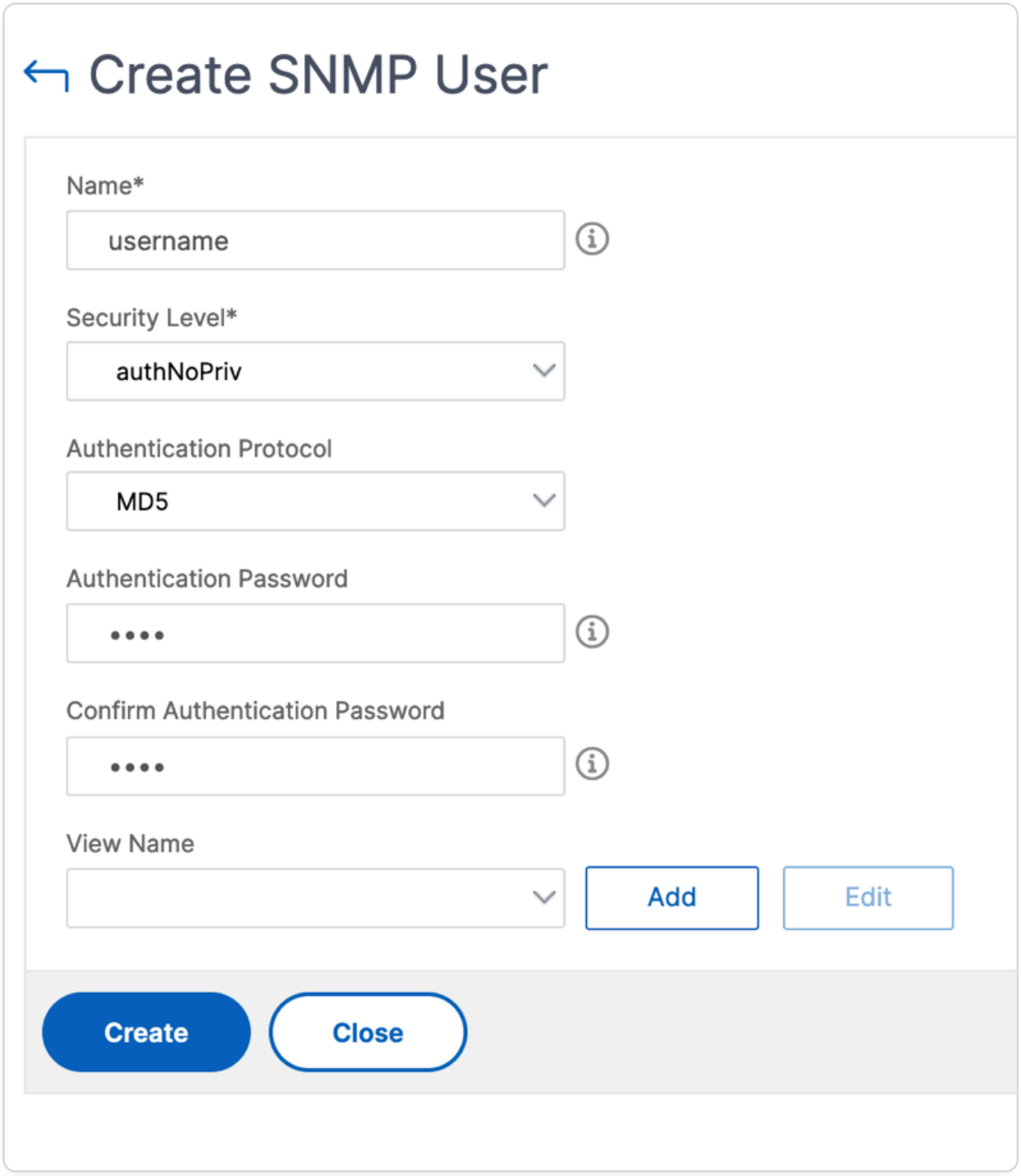
  Select one of the following security levels:

- **noAuthNoPriv**. Require neither authentication nor encryption.



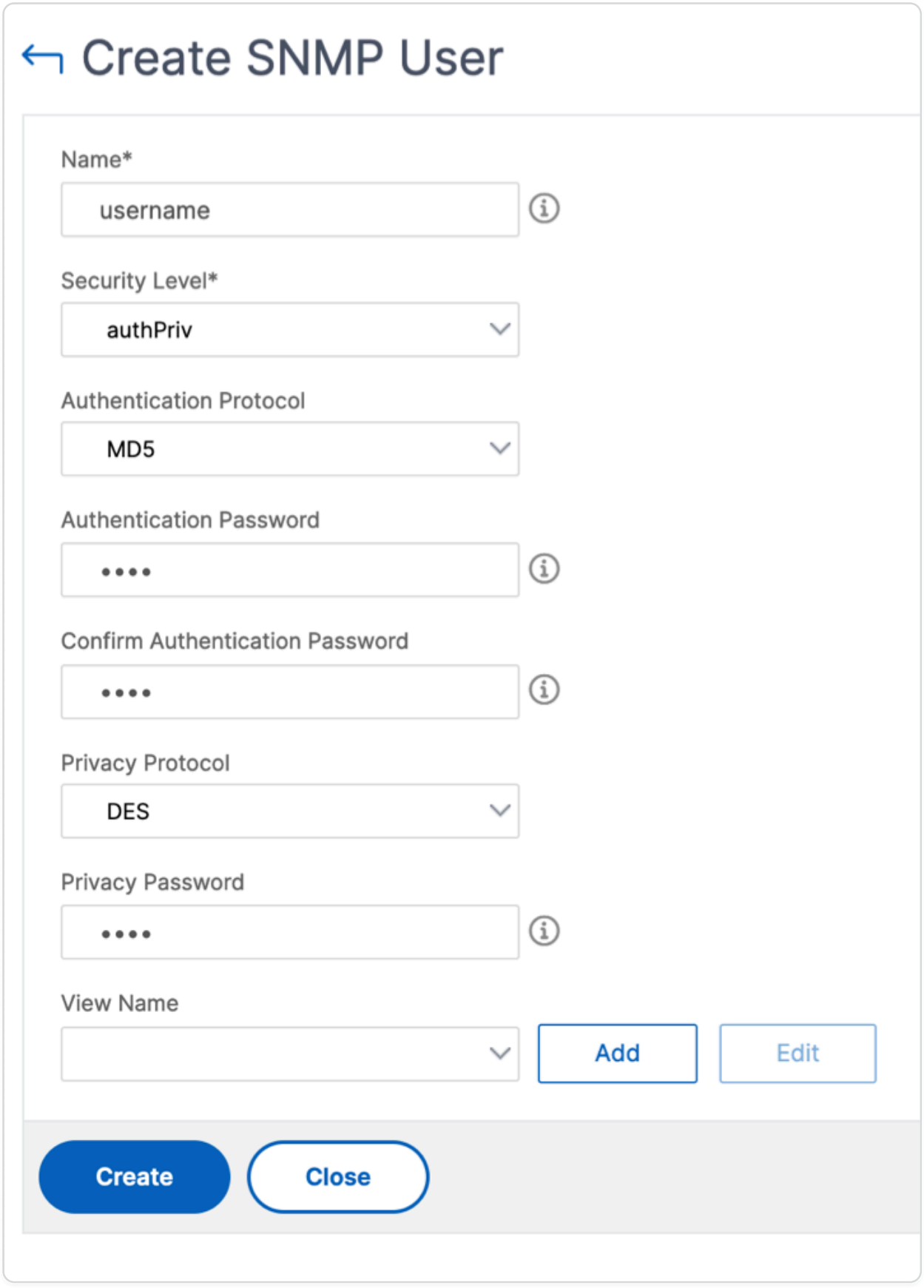
- **authNoPriv**. Require authentication but no encryption.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **authPriv**. Require authentication and encryption.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Based on the security level you've assigned to the user, provide extra authentication protocols, such as authentication protocols, privacy passwords, and assign SNMP views.

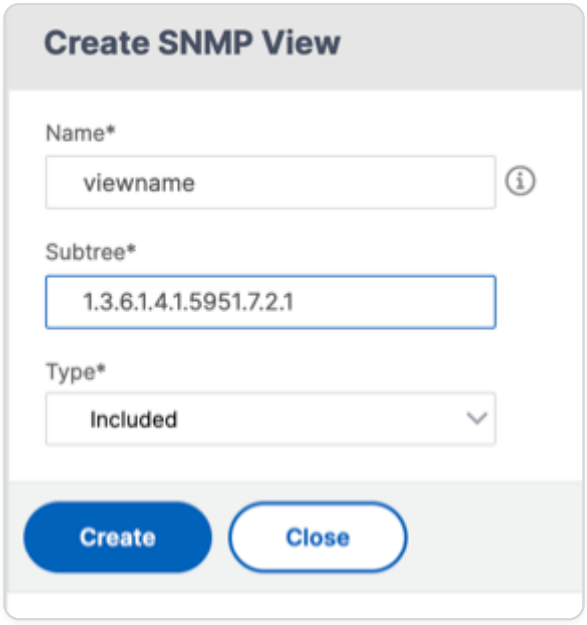
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Managing SNMP views

SNMP views are used to implement access control for an SNMP user. The SNMP views restrict the user access to specific portions of the MIB.

To allow or restrict an SNMP OID for the NetScaler agent:

1. Navigate to **Infrastructure > Instances > Agents**, select a NetScaler agent, and click **Select Action> Manage SNMP**.
2. In the **SNMP > SNMP User** tab, click **Add**.
3. In the **Create SNMP View**, enter the following details:
   - **View Name**: A name for the SNMP view. An instance can have many SNMP views with the same name, differentiated by the subtree parameter settings.
   - **Subtree**: A particular branch (subtree) of the MIB tree that you want to associate with this SNMP view. You must specify the subtree as an SNMP OID.
   - **Type**: This field allows you to include or exclude subtrees from a view.
4. Click **Create**.



Provision NetScaler VPX instances on SDX

You can provision one or more NetScaler VPX instances on the SDX appliance by using NetScaler Console. The number of instances that you can deploy depends on the license you have purchased. If the number of instances added is equal to the number specified in the license, the NetScaler Console does not allow you to provision more NetScaler instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Before you begin, ensure to add an SDX instance in NetScaler Console where you want to provision VPX instances.

To provision a VPX instance, do the following:

1. Navigate to **Infrastructure > Instances > NetScaler**.
2. In the **SDX** tab, select an SDX instance where you want to provision a VPX instance.
3. In **Select Action**, select **Provision VPX**.

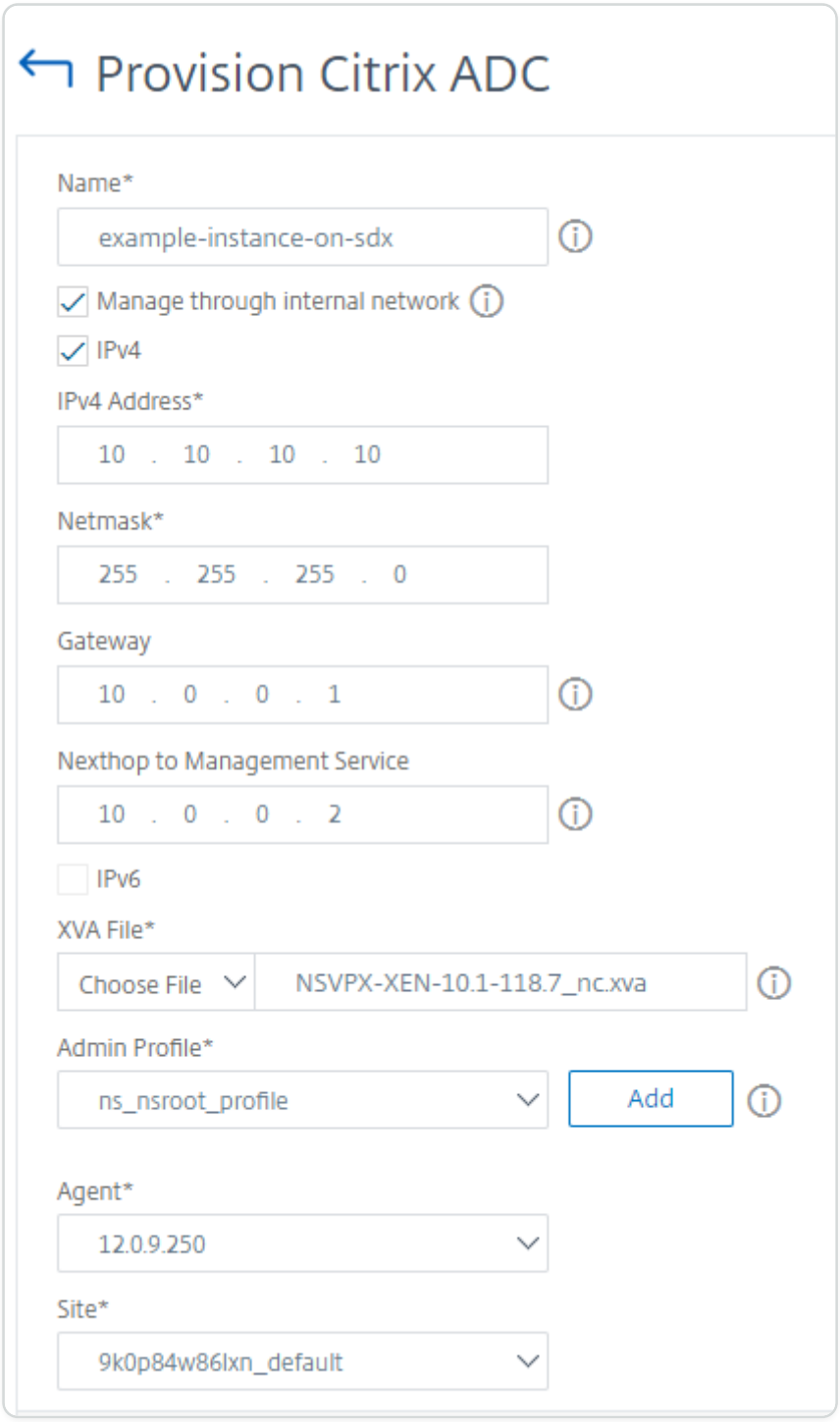
Step 1 - Add a VPX instance

The NetScaler Console uses the following information to configure VPX instances in an SDX appliance:

- **Name** - Specify a name to a NetScaler instance.
- Establish a communication network between SDX and VPX. To do so, select the required options from the list:
  - **Manage through internal network** - This option establishes an internal network for a communication between the NetScaler Console and a VPX instance.
  - **IP address** - You can select an **IPv4** or **IPv6** address or both to manage the NetScaler VPX instance. A VPX instance can have only one management IP (also called NetScaler IP). You cannot remove the NetScaler IP address.

    For the selected option, assign a netmask, default gateway, and next hop to the NetScaler Console for the IP address.
- **XVA File** - Select the XVA file from which you want to provision a VPX instance. Use one of the following options to select the XVA file.
  - **Local** - Select the XVA file from your local machine.
  - **Appliance** - Select the XVA file from an NetScaler Console file browser.
- **Admin Profile** - This profile provides access to provision VPX instances. With this profile, NetScaler Console retrieves the configuration data from an instance. If you have to add a profile, click **Add**.
- **Agent** - Select the agent with which you want to associate the instances
- **Site** - Select the site where you want the instance to be added.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Step 2 - Allocate licenses

In the **License Allocation** section, specify the VPX license. You can use Standard, Advanced, and Premium licenses.

- **Allocation mode** - You can choose **Fixed** or **Burstable** modes for the bandwidth pool.

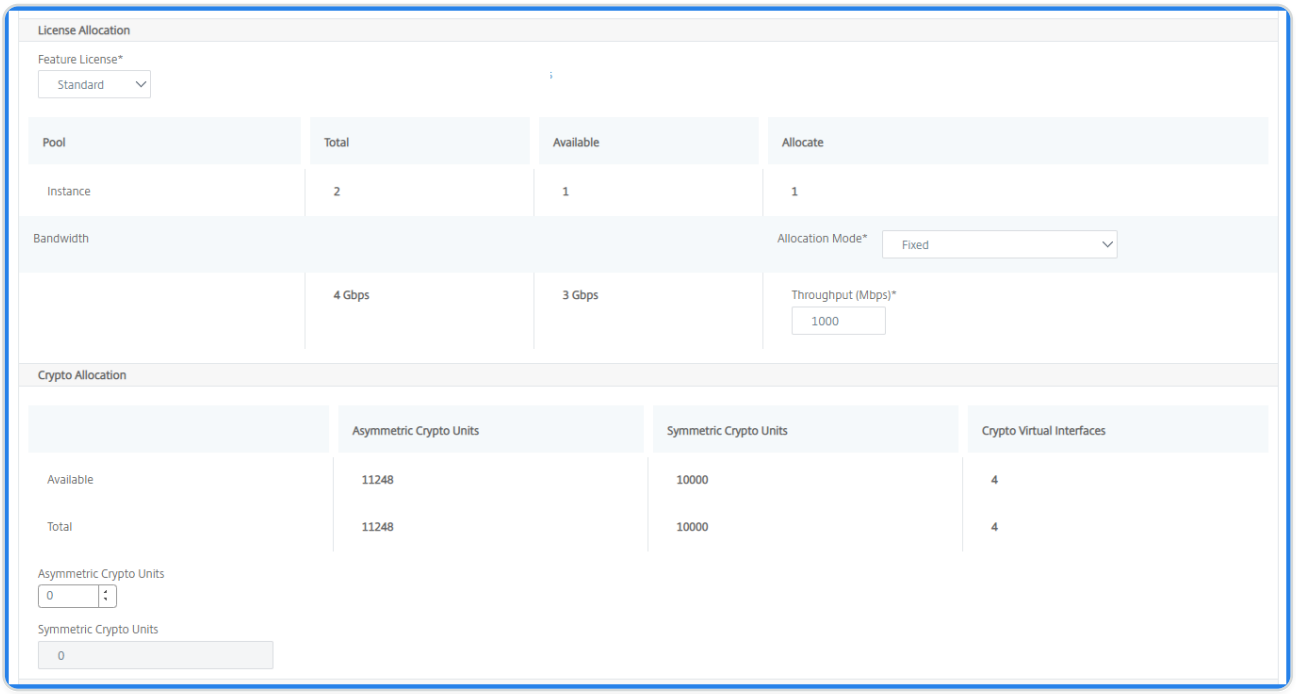
  If you choose **Burstable** mode, you can use extra bandwidth when the fixed bandwidth is reached.

- **Throughput** - Assign the total throughput (in Mbps) to an instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

Buy a separate license (SDX 2-Instance Add-On Pack for Secure Web Gateway) for Citrix Secure Web Gateway™ (SWG) instances on SDX appliances. This instance pack is different from the SDX platform license or SDX instance pack.



From the SDX 12.0 57.19 version, the interface to manage crypto capacity has changed. For more information, see Manage crypto capacity.

Step 3 - Allocate resources

In the **Resource Allocation** section, allocate resources to a VPX instance to maintain traffic.

- **Total Memory (MB)** - Assign total memory to an instance. The minimum value is `2048` MB.
- **Packets per second** - Specify the number of packets to transmit per second.
- **CPU** - Specify number of CPU cores to an instance. You can use shared or dedicated CPU cores.

  When you select a shared core to an instance, the other instances can use the shared core at the time of resource shortage.

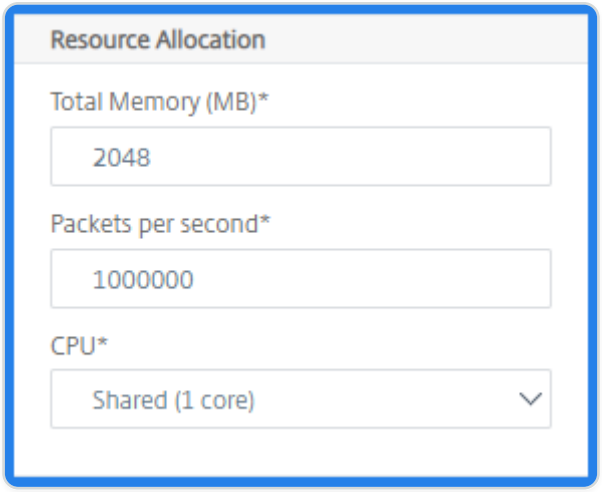
  Restart instances on which CPU cores are reassigned to avoid any performance degradation.

  If you are using the SDX 25000xx platform, you can assign a maximum of 16 cores to an instance. Also, if you are using the SDX 2500xxx platform, you can assign a maximum of 11 cores to an instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

For an instance, the maximum throughput that you configure is 180 Gbps.



See the table in Provision NetScaler instances that lists the supported VPX, single bundle image version, and the number of cores you can assign to an instance.

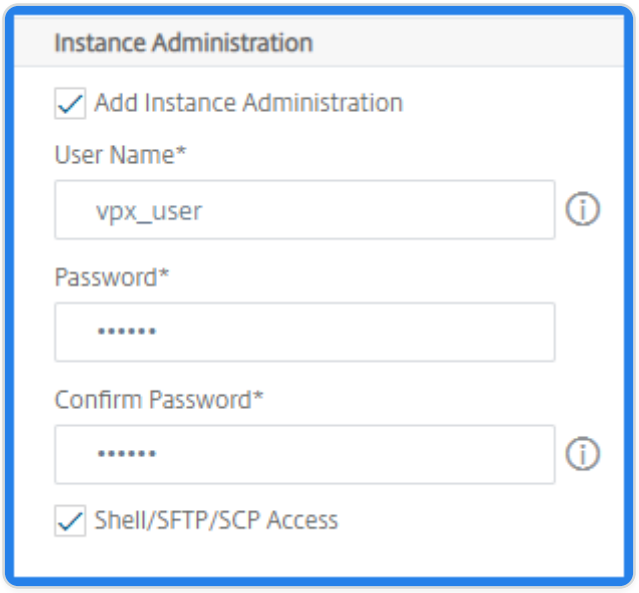
Step 4 - Add instance administration

You can create an admin user for the VPX instance. To do so, select **Add Instance Administration** in the **Instance Administration** section.

Specify the following details:

- **User name**: The user name for the NetScaler instance administrator. This user has superuser access but does not have access to networking commands to configure VLANs and interfaces.
- **Password**: Specify the password for the user name.
- **Shell/Sftp/Scp Access**: The access allowed to the NetScaler instance administrator. This option is selected by default.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Step 5 - Specify network settings

Select the required network settings to an instance:

- **Allow L2 Mode under network settings** - You can allow L2 mode on the NetScaler instance. Select Allow L2 Mode under Networking Settings. Before you log on to the instance and enable L2 mode. For more information, see Allowing L2 Mode on a NetScaler instance.

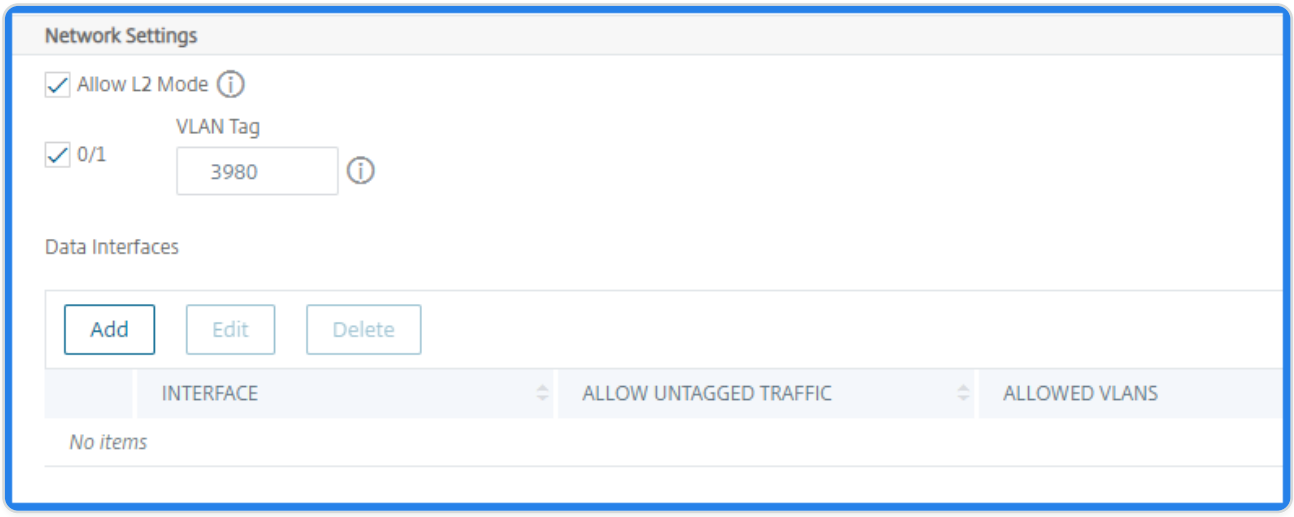
  NOTE

  If you disable L2 mode for an instance, you must log on to the instance and disable L2 mode from that instance. Otherwise, it might cause all the other NetScaler modes to be disabled after you restart the instance.

- **0/1** - In **VLAN tag**, specify a VLAN ID for the management interface.
- **0/2** - In **VLAN tag**, specify a VLAN ID for the management interface.

By default interface **0/1** and **0/2** are selected.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



In **Data Interfaces**, click **Add** to add data interfaces and specify the following:

- **Interfaces** - Select the interface from the list.

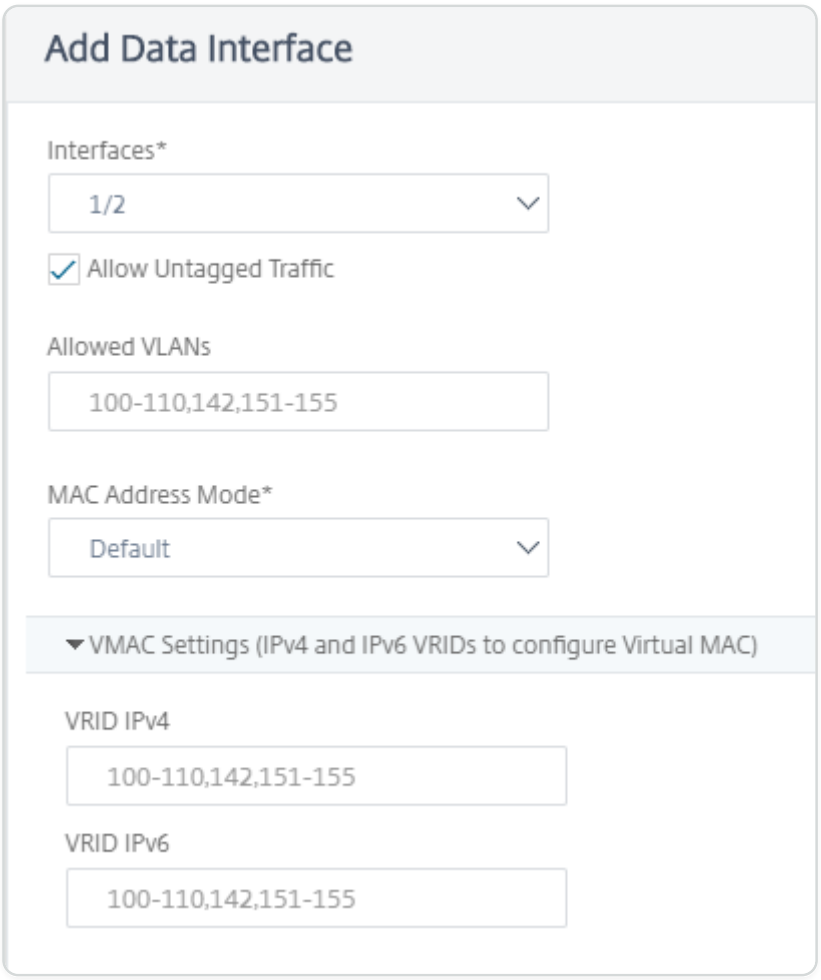
  NOTE

  The interface IDs of interfaces that you add to an instance do not necessarily correspond to the physical interface numbering on the SDX appliance.

  For example, the first interface that you associate with instance-1 is SDX interface 1/4, it appears as interface 1/1 when you view the interface settings in that instance. This interface indicates it is the first interface that you associated with instance-1.
- **Allowed VLANs** - Specify a list of VLAN IDs that can be associated with a NetScaler instance.
- **MAC Address Mode** - Assign a MAC address to an instance. Select from one of the following options:
  - **Default** - Citrix Workspace assigns a MAC address.
  - **Custom** - Choose this mode to specify a MAC address that overrides the generated MAC address.
  - **Generated** - Generate a MAC address by using the base MAC address set earlier. For information about setting a base MAC address, see Assigning a MAC Address to an Interface.
- **VMAC Settings (IPv4 and IPv6 VRIDs to configure Virtual MAC)**
  - **VRID IPV4** - The IPv4 VRID that identifies the VMAC. Possible values: 1–255. For more information, see Configuring VMACs on an Interface.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- VRID IPV6 - The IPv6 VRID that identifies the VMAC. Possible values: 1–255. For more information, see Configuring VMACs on an Interface.



Click **Add**.

Step 6 - Specify Management VLAN settings

The Management Service and the management address (NSIP) of the VPX instance are in the same subnetwork, and communication is over a management interface.

If the Management Service and the instance are in different subnetworks, specify a VLAN ID while you provision a VPX instance. Therefore, the instance is reachable over the network when it active.

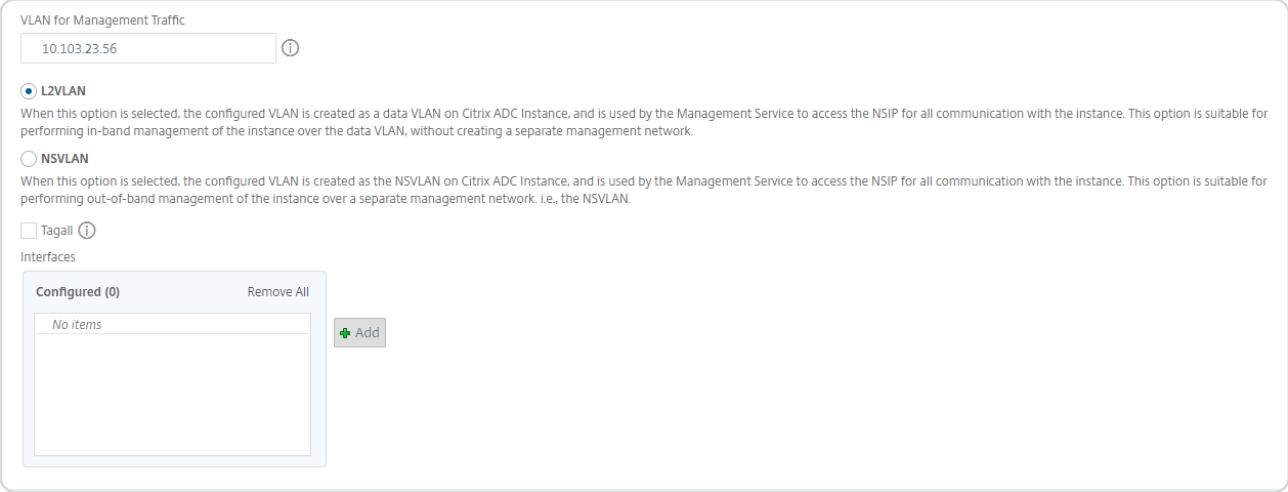
If your deployment requires the NSIP is accessible only through the selected interface while provisioning the VPX instance, select **NSVLAN**. And, the NSIP becomes inaccessible through other interfaces.

- HA heartbeats are sent only on the interfaces that are part of the NSVLAN.
- You can configure an NSVLAN only from the VPX XVA build `9.3-53.4` and later.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT

- You cannot change this setting after you provision the VPX instance.
- The `clear config full` command on the VPX instance deletes the VLAN configuration if **NSVLAN** is not selected.

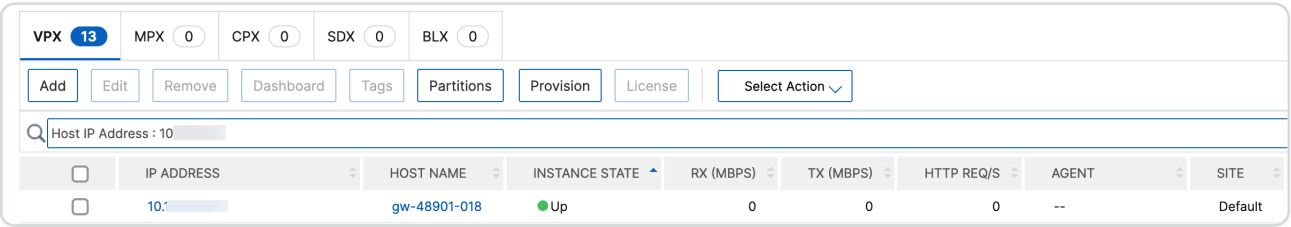


Click **Done** to provision a VPX instance.

View the provisioned VPX instance

To view the newly provisioned instance, do the following:

1. Navigate to **Infrastructure > Instances > NetScaler**.
2. In the **VPX** tab, search an instance by the **Host IP address** property and specify SDX instance IP to it.



Rediscover multiple NetScaler instances

You can rediscover multiple Citrix Application Delivery Controller (NetScaler) instances (VPX, MPX, SDX, BLX, and CPX) in your NetScaler Console setup. After you rediscover the instances, you can view the latest states and configurations of those instances. The NetScaler Console server rediscovers all ADC instances and checks whether the instances are reachable.

To rediscover multiple NetScaler VPX instances:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigate to **Infrastructure > Instances > NetScaler**. Select the instance tab (VPX, MPX, SDX, BLX, and CPX) and select the instances you want to rediscover.
2. In the **Action** box, click **Rediscover**. You can also rediscover multiple VPX instances.
3. When the confirmation message for running the Rediscover utility appears, Click **Yes**.

   The screen reports the progress of rediscovery of each of the instances.

Polling overview

Polling is a process, where NetScaler Console collects certain information from NetScaler instances. You might have configured multiple NetScaler instances for your organization, across the world. To monitor your instances through NetScaler Console, NetScaler Console has to collect certain information such as CPU usage, memory usage, SSL certificates, licensed features, license types from all managed NetScaler instances. The following are the different types of polling that occur between NetScaler Console and the managed instances:

- Instance polling
- Inventory polling
- Performance data collection
- Instance backup polling
- Configuration audit polling
- SSL certificate polling
- Entity polling

NetScaler Console uses protocols such as NITRO call, Secure Shell (SSH), and Secure Copy (SCP) to poll information from NetScaler instances.

How NetScaler Console polls managed instances and entities

NetScaler Console automatically polls at regular intervals by default. NetScaler Console also enables you to configure polling intervals for a few polling types and allows you to poll manually when required.

The following table describes the details of types of polling, polling interval, protocol used, and so on:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POLLING TYPE	POLLING INTERVAL	POLLED INFORMATION	PROTOCOL USED	POLLING INTERVAL CONFIGURATION
Instance polling	Every 5 minutes (by default)	Statistical information such as state, HTTP requests per second, CPU usage, memory usage, and throughput.	NITRO call	No
Inventory polling	Every 60 minutes (by default)	Inventory details such as build version, system information, licensed features, and modes.	NITRO call and SSH	No
Performance data collection	Every 5 minutes (by default)	Network reporting information	NITRO call	No
Instance backup polling	Every 12 hours (by default)	The backup file of the current state of the managed NetScaler instances	NITRO call, SSH, and SCP	Yes. Navigate to **Infrastructure > Instances > NetScaler**. Select the instance and from the **Select Action** list, click **Backup/ Restore**.
Configuration audit polling	Every 10 hours (by default)	Configuration changes that occur on NetScaler	SSH, SCP, and NITRO call	Yes. Navigate to **Infrastructure >**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POLLING TYPE	POLLING INTERVAL	POLLED INFORMATION	PROTOCOL USED	POLLING INTERVAL CONFIGURATION
		instances (for example, running vs. saved configuration)		**Configuration > Configuration Audit**. On the Configuration Audit page, click **Settings** and configure the polling interval for Configuration Audit Polling.
				You can poll configuration audits manually and add all configuration audits of the instances immediately to NetScaler Console. To do so, navigate to **Infrastructure > Configuration > Configuration Audit** and click **Poll Now**. The **Poll Now** page lets you poll all or selected instances in the network.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POLLING TYPE	POLLING INTERVAL	POLLED INFORMATION	PROTOCOL USED	POLLING INTERVAL CONFIGURATION
SSL certificates polling	Every 24 hours (by default)	SSL certificates that are installed on NetScaler instances.	NITRO call and SCP	Yes. Navigate to **Infrastructure > SSL Dashboard**. On the SSL Dashboard page, click **Settings** to configure the polling interval
				You can poll SSL certificates manually and add all certificates of the instances immediately to NetScaler Console. To do so, navigate to **Infrastructure > SSL Dashboard** and click **Poll Now**. The **Poll Now** page lets you poll all or selected instances in the network.
Entity polling				
All instances	Every 720 minutes (by default)	All entities that are configured on the	NITRO call	Yes. It can be set between 30 minutes and

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POLLING TYPE	POLLING INTERVAL	POLLED INFORMATION	PROTOCOL USED	POLLING INTERVAL CONFIGURATION
		instances. An entity is either a policy, virtual server, service, or action attached to a NetScaler instance. To enable entity polling, see Enable or disable NetScaler Console features.		1440 minutes. To configure, navigate to **Infrastructure > Network Functions**. On the Networks Function page, click **Settings** to configure the polling interval.
				You can poll entities manually and add all entities of the instances immediately to NetScaler Console. To do so, navigate to **Infrastructure > Network Functions** and click **Poll Now**. The **Poll Now** page lets you poll all or selected instances in the network

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POLLING TYPE	POLLING INTERVAL	POLLED INFORMATION	PROTOCOL USED	POLLING INTERVAL CONFIGURATION
Selected NetScaler instances	Every 15 minutes (by default)	Poll only those NetScaler instances where changes are made before the default polling cycle is triggered.	NITRO call	Yes. It can be set between 5 minutes and 60 minutes. Navigate to **Infrastructure > Network Functions**, click **Settings**, and specify the time in the **Delay time for Network Functions** text box.

NOTE:

In addition to polling, events generated by managed NetScaler instances are received by NetScaler Console through SNMP traps sent to the instances. For example, an event is generated when there is a system failure or change in configuration.

During instance backup, SSL files, CA certificate files, NetScaler templates, database information, and so on are downloaded to NetScaler Console. During a configuration audit, ns.conf files are downloaded and stored in the file system. All information collected from managed NetScaler instances are stored internally within the database.

Different ways of polling instances

The following are the different ways of polling that NetScaler Console performs on the managed instances:

- Global polling of instances
- Manual polling of instances
- Manual polling of entities

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Global polling of instances

NetScaler Console automatically polls all the managed instances in the network depending on the interval configured by you. Though the default polling interval is 60 minutes, you can set the interval depending on your requirements by navigating to **Infrastructure > Network Functions > Settings**.

Manual polling of instances

When NetScaler Console is managing many entities, the polling cycle takes a longer time to generate the report that might result in a blank screen or the system might still display earlier data.

In NetScaler Console, there is a minimum polling interval period when automatic polling does not happen. If you add a new NetScaler instance, or if an entity is updated, NetScaler Console does not recognize the new instance or the updates made to an entity until the next polling happens. And, there is no way to immediately get a list of virtual IP addresses for further operations. You must wait for the minimum polling interval period to elapse. Though you can do a manual poll to discover newly added instances, this leads to the entire NetScaler network to be polled, which creates a heavy load on the network. Instead of polling the entire network, NetScaler Console now allows you to poll only selected instances and entities at any given time.

NetScaler Console automatically polls managed instances to collect information at set times in a day. Selected polling reduces the refresh time that NetScaler Console requires to display the most recent status of the entities bound to these selected instances.

To poll specific instances in NetScaler Console:

1. In NetScaler Console, navigate to **Infrastructure > Network Functions**.
2. On **Network Functions** page, at the top right-hand corner, click **Poll Now**.
3. The pop-up page **Poll Now** provides you an option to poll all NetScaler instances in the network or poll the selected instances.
    a. **All Instances** tab - click **Start Polling** to poll all the instances.
    b. **Select Instances** tab - select the instances from the list
4. Click **Start Polling**.

    NetScaler Console initiates manual polling and adds all the entities.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Manual polling of entities

NetScaler Console also allows you to poll only a few selected entities that are bound to an instance. For example, you can use this option to know the latest status of a particular entity in an instance. In this case, you need not poll the instance as a whole to know the status for one updated entity. When you select and poll an entity, NetScaler Console polls only that entity and updates the status in the NetScaler Console GUI.

Consider an example of a virtual server being **DOWN**. The status of that virtual server might have changed to **UP**, before the next automatic polling happens. To view the changed status of the virtual server, you might want to poll only that virtual server, so that the correct status is displayed on the GUI immediately.

You can now poll the following entities for any update in their status, services, service groups, load balancing virtual servers, cache reduction virtual servers, content switching virtual servers, authentication virtual servers, VPN virtual servers, GSLB virtual servers, and application servers.

NOTE:

If you poll a virtual server, only that virtual server is polled. The associated entities such as services, service groups, and servers are not polled. If you need to poll all associated entities, you must manually poll the entities or you must poll the instance.

To poll specific entities in NetScaler Console:

As an example, this task assists you to poll load balancing virtual servers. Similarly, you can poll other network function entities too.

1. In NetScaler Console, navigate to **Infrastructure > Network Functions > Load Balancing > Virtual Servers**.
2. Select the virtual server that shows the status as **DOWN**, and then click **Poll Now**. The status of the virtual server now changes to **UP**.

Unmanage an instance

If you want to stop the exchange of information between NetScaler Console and the instances in your network, you can unmanage the instances.

To unmanage an instance:

1. Navigate to **Infrastructure > Instances > NetScaler**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Select the NetScaler instance tab (for example, VPX).
3. In the list of instances, either right-click an instance and then select **Unmanage**, or select instance and from the **Action** list, select **Unmanage**.

   The status of the selected instance changes to **Out of Service**.

   The instance is no longer managed by NetScaler Console, and it no longer exchanges data with NetScaler Console.

Trace the route to an instance

By tracing the route of a packet from the NetScaler Console to an instance, you can find information such as the number of hops necessary to reach the instance. The traceroute traces the path of the packet from source to destination. It displays the list of network hops along with the host name and IP address of each entity in the route.

Traceroute also records the time taken by a packet to travel from one hop to another. If there is any interruption in the transfer of packets, the traceroute shows where the problem exists.

To trace the route of an instance:

1. Navigate to **Infrastructure > Instances > NetScaler**.
2. Select the NetScaler instance tab (for example, VPX).
3. In the list of instances, either right-click an instance and then select **TraceRoute**, or select the instance and, from the **Action** list, click **TraceRoute**.

   The TraceRoute message box shows the route to the instance and the amount of time, in milliseconds, consumed by each hop.

View NetScaler-owned IP addresses

You can view the IP addresses configured on NetScaler instances directly from NetScaler Console GUI. Please note that the configuration changes and other operations can only be performed on NetScaler instances.

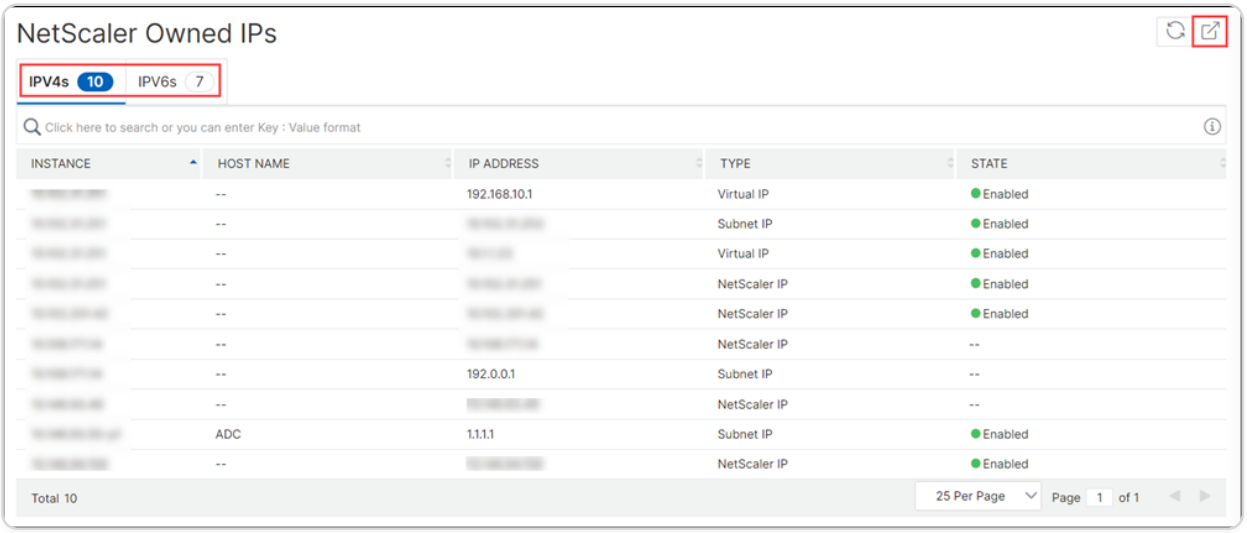
To view the NetScaler-owned IP addresses, navigate to **Infrastructure > Instances > NetScaler Owned IPs**.

This feature displays both IPv4 and IPv6 addresses configured on NetScaler instances. The types of IP addresses include:

- NetScaler IP address

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Subnet IP address
- Virtual IP address
- ADNS service IP address
- GSLB IP address
- Cluster IP address
- Mapped IP address



Export NetScaler-owned IP addresses

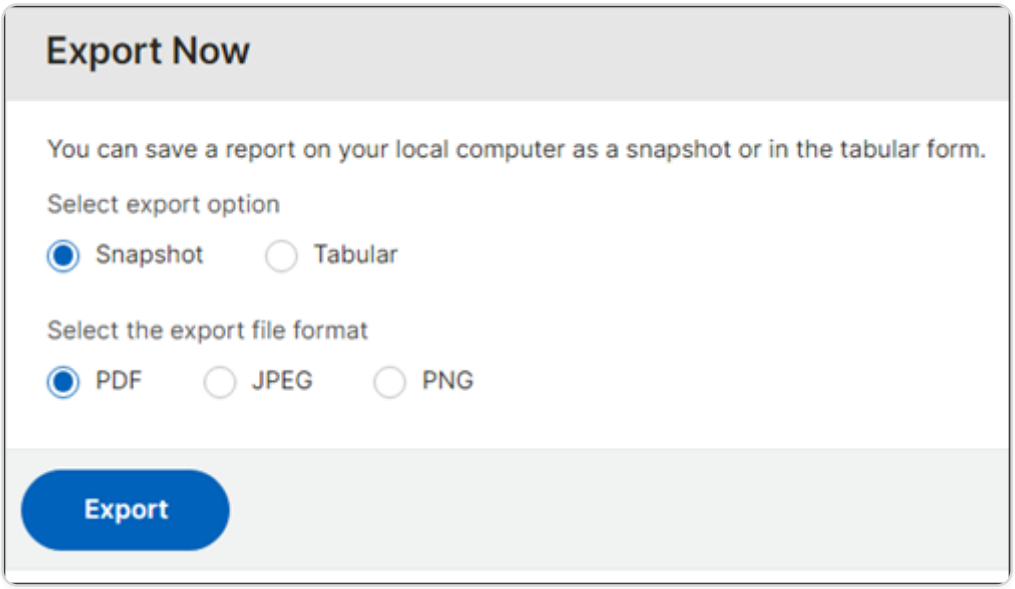
To export NetScaler-owned IP addresses, follow these steps:

1. Navigate to **Infrastructure > Instances > NetScaler Owned IPs**.
2. On the **NetScaler Owned IPs** page, click the export icon at the top-right corner.
3. On the **Export Reports** page, click **Export Now**.
4. On the **Export Now** page, select the export option:

   For **Snapshot** export:

   a. Select the export file format: PDF, JPG, or PNG.

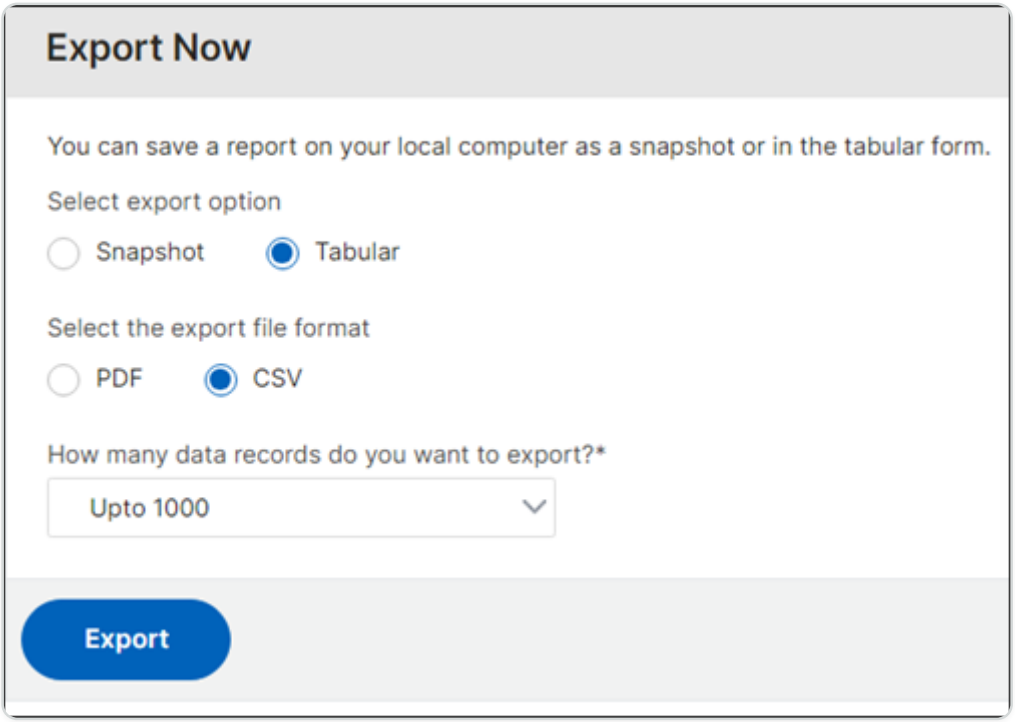
© 1997–2026 Citrix Systems, Inc. All rights reserved.



For **Tabular** export:

a. Select the export file format: PDF or CSV.

b. Select the number of data records to export from the list.



5. Click **Export**.

Schedule the export of NetScaler-owned IP addresses

To schedule the export of NetScaler-owned IP addresses, follow these steps:

1. Navigate to **Infrastructure > Instances > NetScaler Owned IPs**.
2. On the **NetScaler Owned IPs** page, click the export icon at the top-right corner.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. On the **Export Reports** page, click **Schedule Export**.
4. On the **Schedule Export** page, enter the following details:
    a. Enter the subject and description.
    b. Select the export type.

        For **Snapshot** export type:

        - Select the export file format: PDF, JPG, or PNG.

        For **Tabular** export type:

        - Select the export file format: PDF or CSV.
        - Select the number of data records to export from the list.

    c. Select the recurrence: Daily, Weekly or Monthly.
    d. Select the export time.
    e. Select how to send the exported IP addresses: Email, Slack or both.

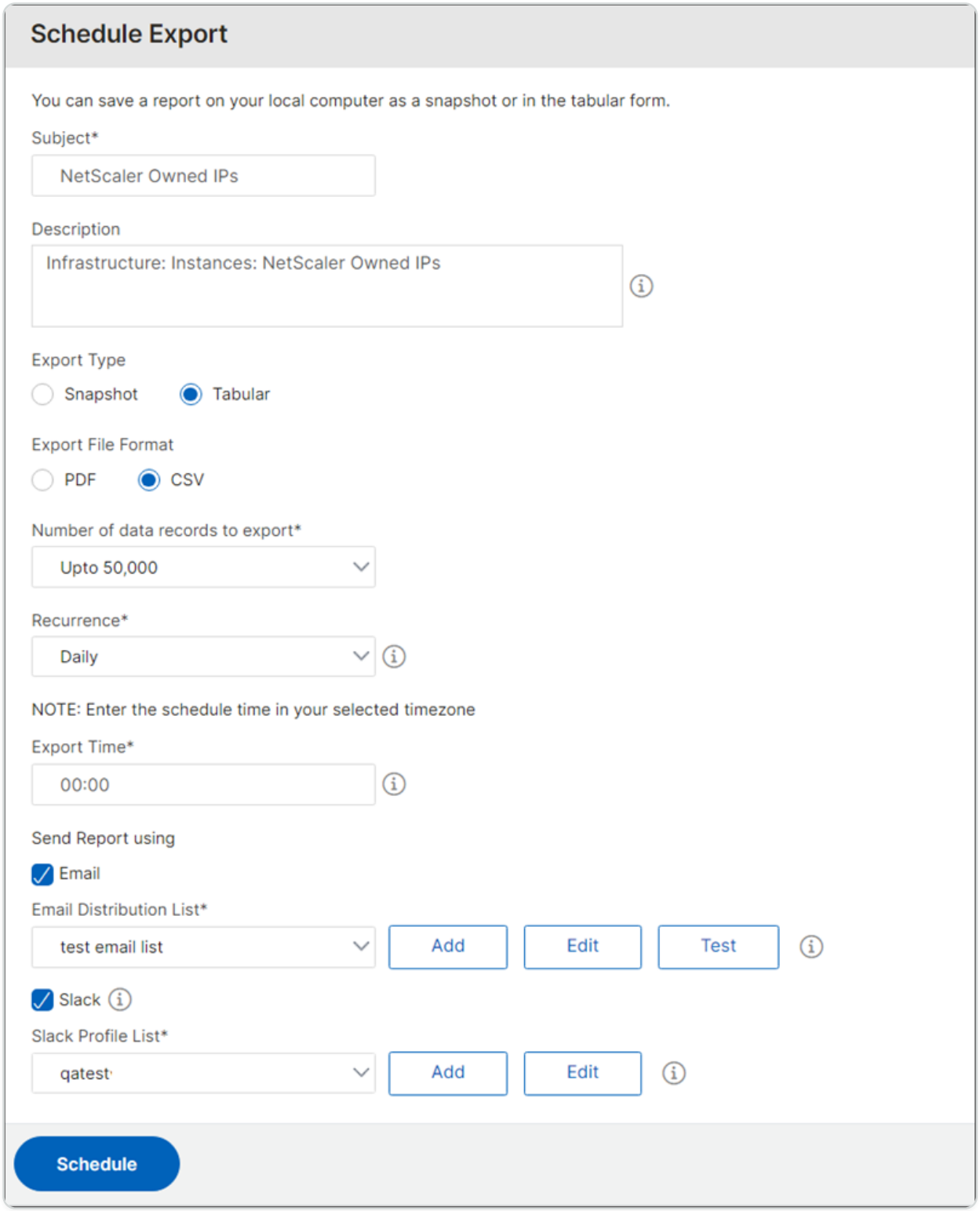
        For Email:

        - Select **Email** and choose the email distribution list to send the list of NetScaler-owned IP addresses.
            - To add an email distribution list, click **Add** and specify the email server details.
            - To edit an email distribution list, click **Edit**.
            - To verify that the email distribution list is working, click **Test**. This will send a test email to the selected email distribution list.

        For Slack:

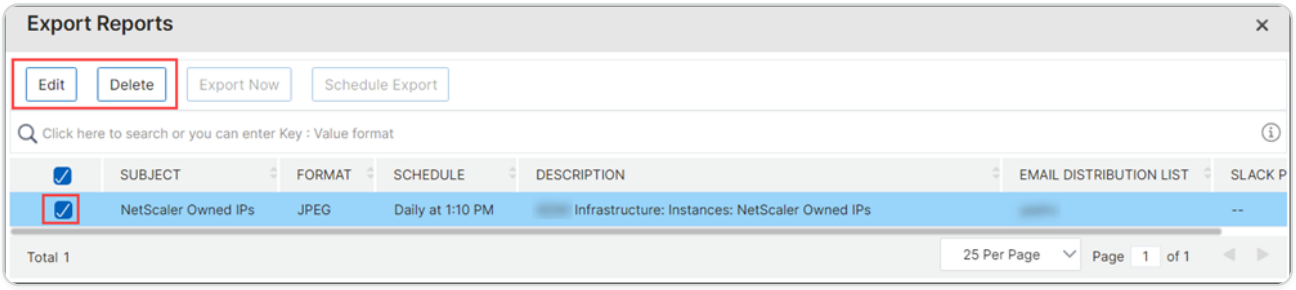
        - Select **Slack** and choose the Slack profile list to send the list of NetScaler-owned IP addresses.
            - To add a Slack profile, click **Add** and specify the **Profile Name**, **Channel Name**, and **Token** of the Slack channel.
            - To edit an existing Slack channel, click **Edit**.
5. Click **Schedule** to schedule the export.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Once scheduled, your export schedule appears on the **Export Reports** page, and you can select the schedule to perform the edit or delete operation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



How to change the NetScaler MPX or VPX root password

Occasionally, you must change the root password of the NetScaler appliance for security reasons or compliance of password rotation policy.

This document describes the steps required to change the root password of the NetScaler MPX and VPX appliances managed through NetScaler Console cloud.

If you change the NetScaler password, you must modify the NetScaler Console admin profile that is associated with the NetScaler. An NetScaler Console admin profile maintains the NetScaler credentials for REST API, SSH, SCP, or SNMP based communication with the NetScaler appliance. Through admin profiles, NetScaler Console manages NetScaler MPX and VPX appliances.

Change password using the Configuration Jobs feature

By using the NetScaler Console Configuration Jobs feature, you can simplify the repetitive password change process and apply the changes to the NetScaler appliances, without accessing the individual instances.

Follow these steps to change the password:

- Step 1. Create a Configuration Template.
- Step 2. Create a Configuration Job.
- Step 3. Create an admin profile and modify it.

Note:

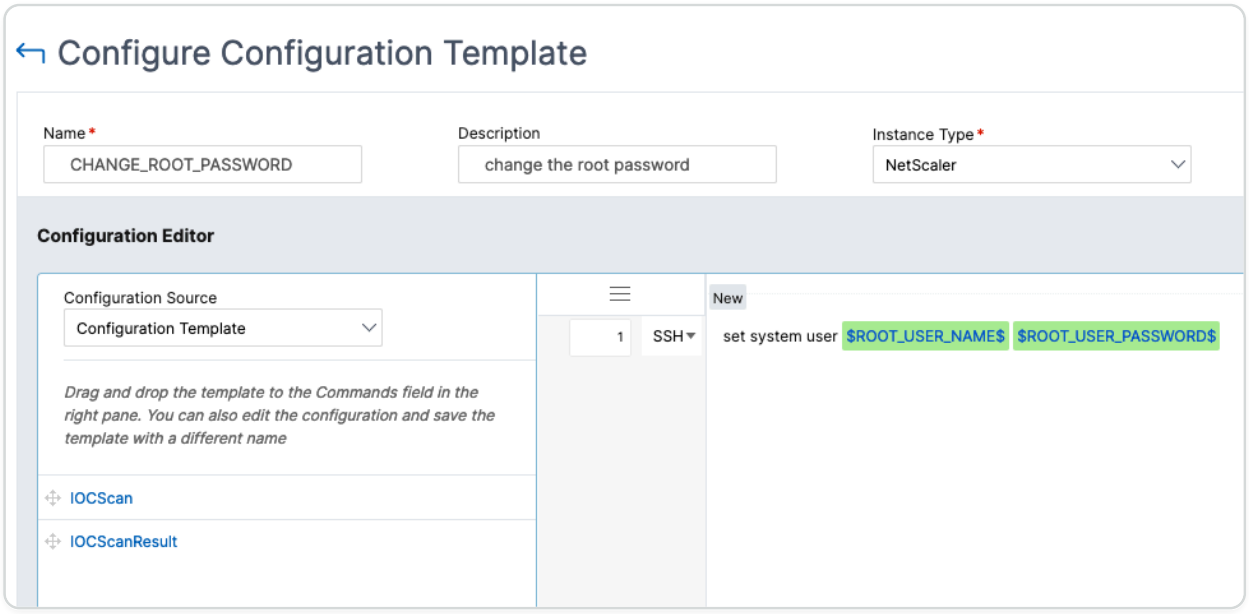
> If the NetScaler appliances are managed by other tools as well, you must change the credentials on those tools as well.

Create a Configuration Template

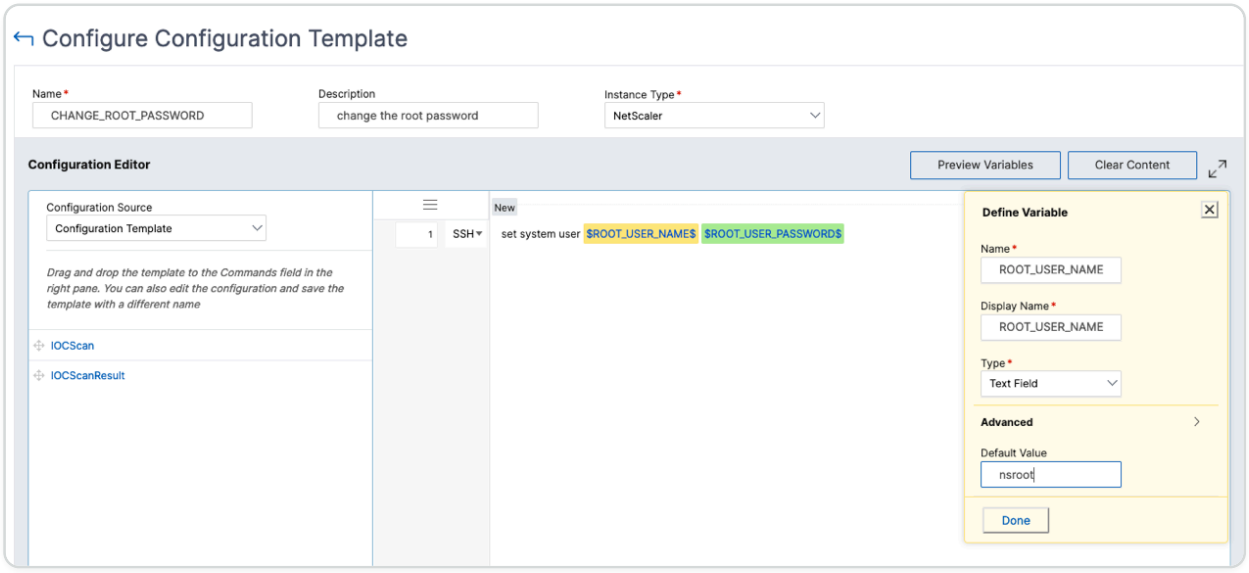
1. From the NetScaler Console GUI, navigate to **Infrastructure > Configuration > Configuration Templates**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Select **Add**. Create a Configuration Template with by typing the SSH command `set system user $ROOT_USER_NAME$ $ROOT_USER_PASSWORD$`.



3. Select the $ROOT_USER_NAME$ variable, and select **Text Field as Type**.
4. Optionally, provide the default value for the root user name. Select **Done** to save the variable settings.



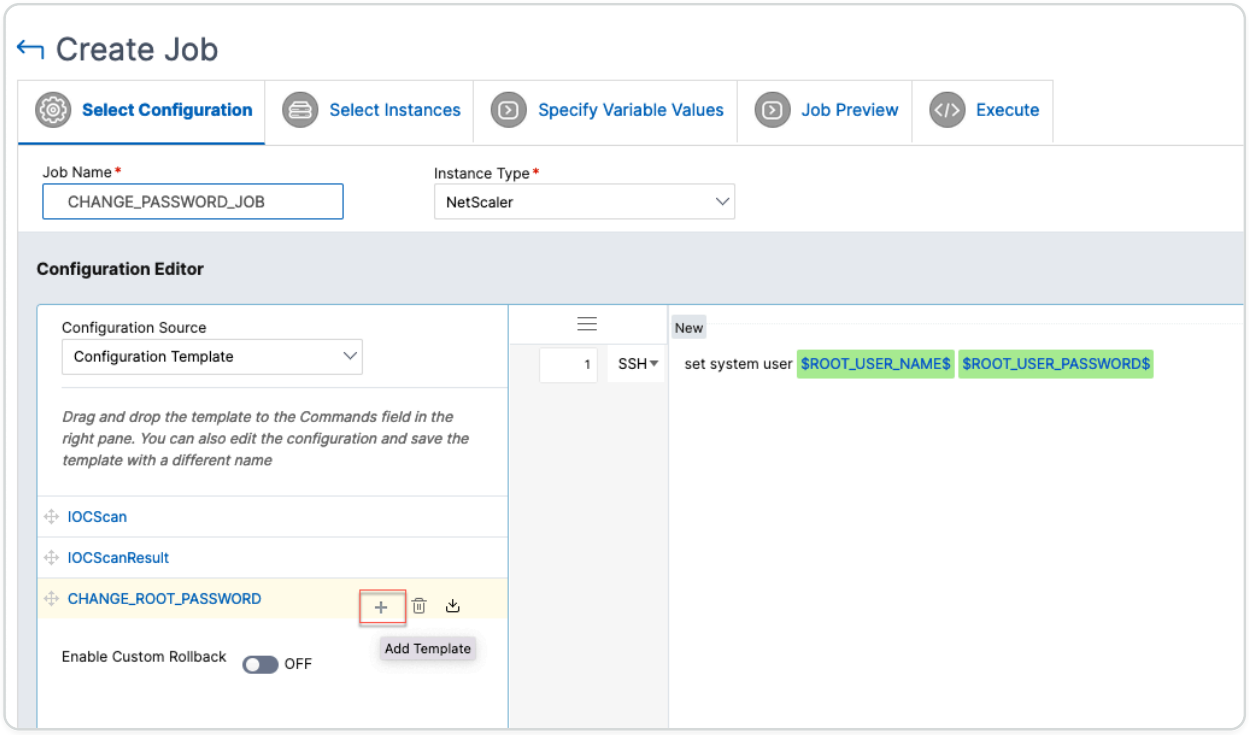
5. Select the $ROOT_USER_PASSWORD$ variable, and select **Password Field as Type**. Select **Done** to save the variable settings.
6. Select **OK** to save the Configuration Template.
7. The new Configuration Template appears under **Configuration Templates**.

Create a Configuration Job

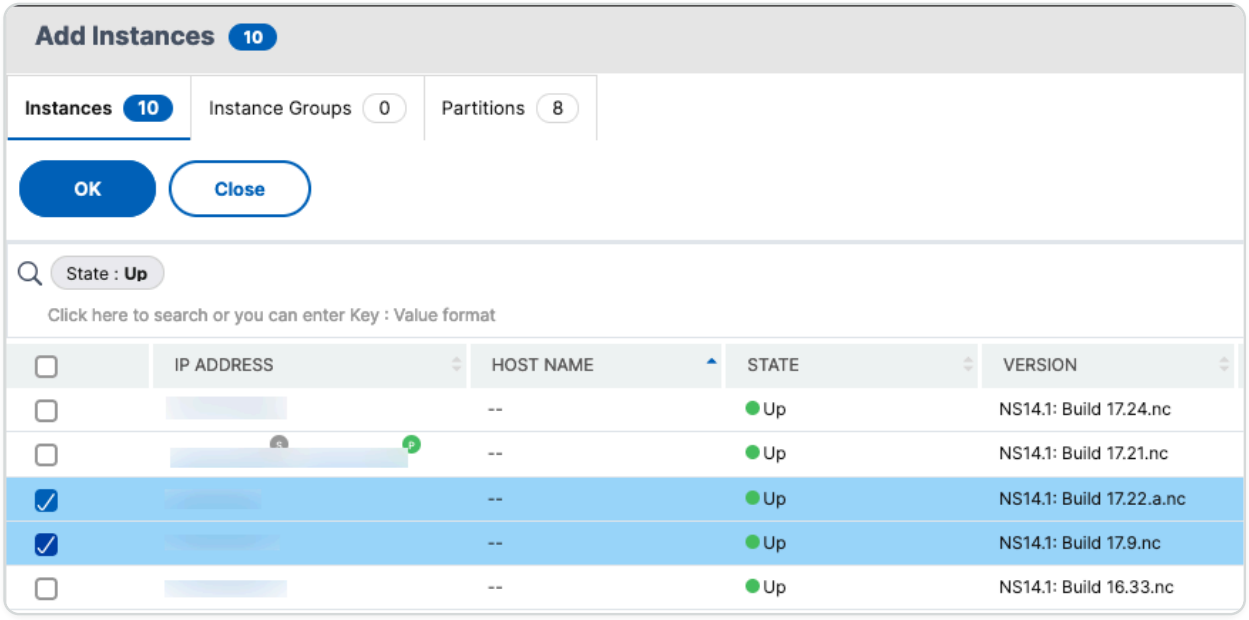
1. From the NetScaler Console GUI, navigate to **Infrastructure > Configuration Jobs**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Select **Create Job** and click the "+" icon of the new configuration template. Select **Next**.

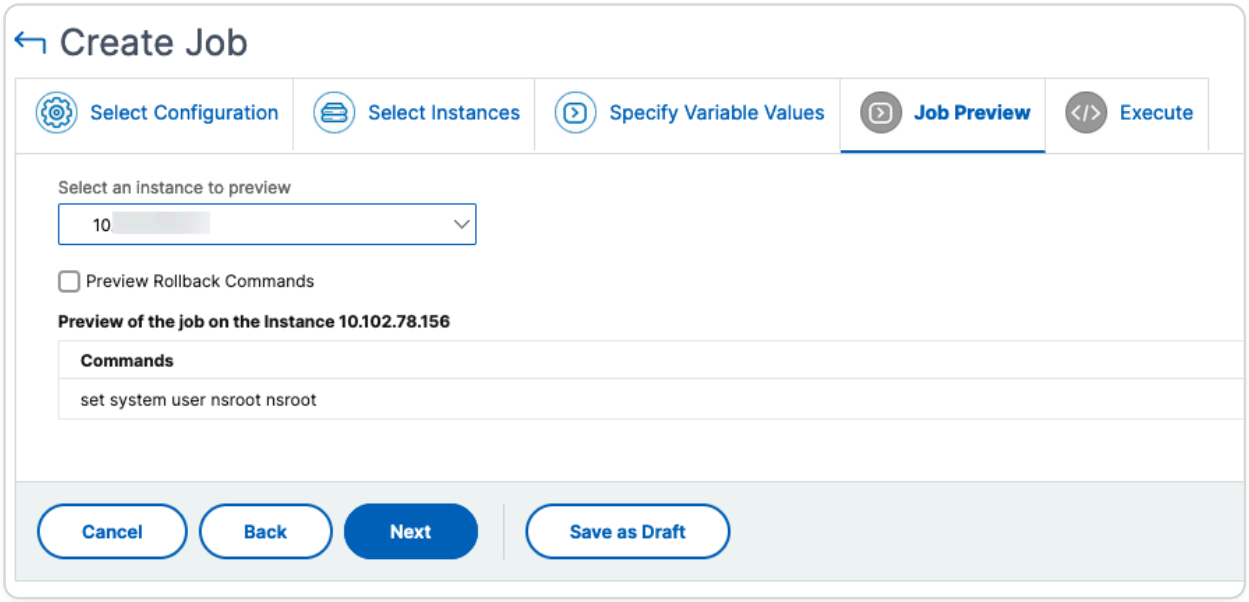


3. Select the NetScaler instance or instances for which the password must be modified.



4. In the **Select Instances** pane, select the instances, and click **Next**.
5. In the **Specify Variable Values** pane provide values for user name and password, and click **Next**.
6. Under **Job Preview**, check the actual CLI commands that the NetScaler Console will run on the NetScaler instances. If the preview looks fine, click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

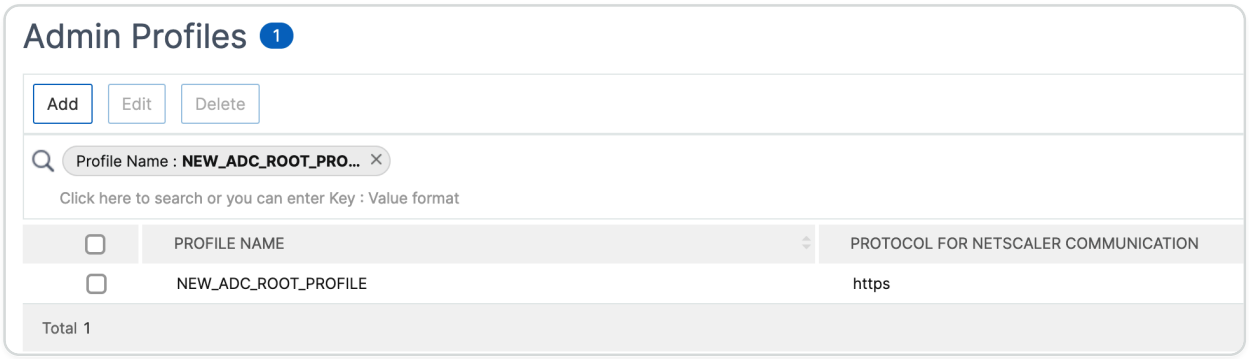


7. In the **Execute** pane, you have the choice to run the Job immediately or schedule it for later. You can also choose to run the Job in parallel on all the selected instances or do it sequentially. Select Finish after you've provided the execution details.
8. Configuration Job shows if the execution succeeded or failed.
9. Select the **Job** and click **Details**. The execution details show the status at individual instance level.

Modify the admin profile

After you've modified the NetScaler passwords, you must add and modify the admin profiles of the instances. Follow these steps:

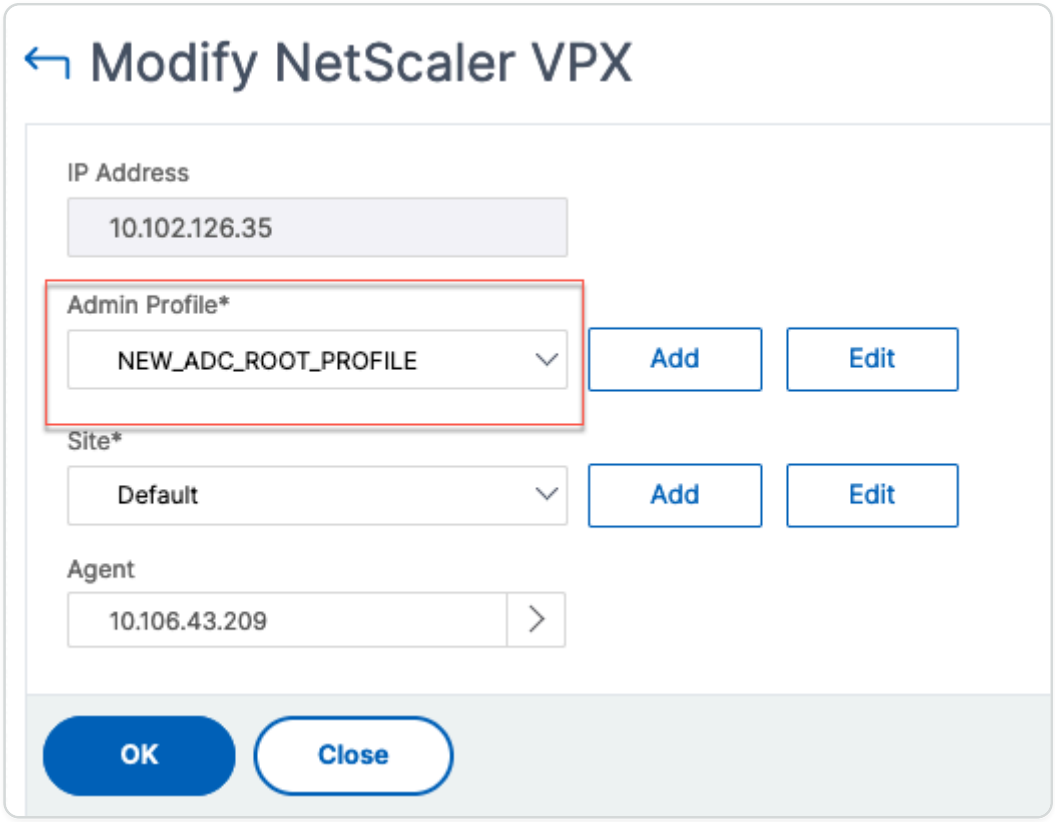
1. Navigate to **Infrastructure > Instances > NetScaler**.
2. Click **Profiles** to see all the admin profiles.
3. Select **Add** to create an admin profile and provide new NetScaler credentials.



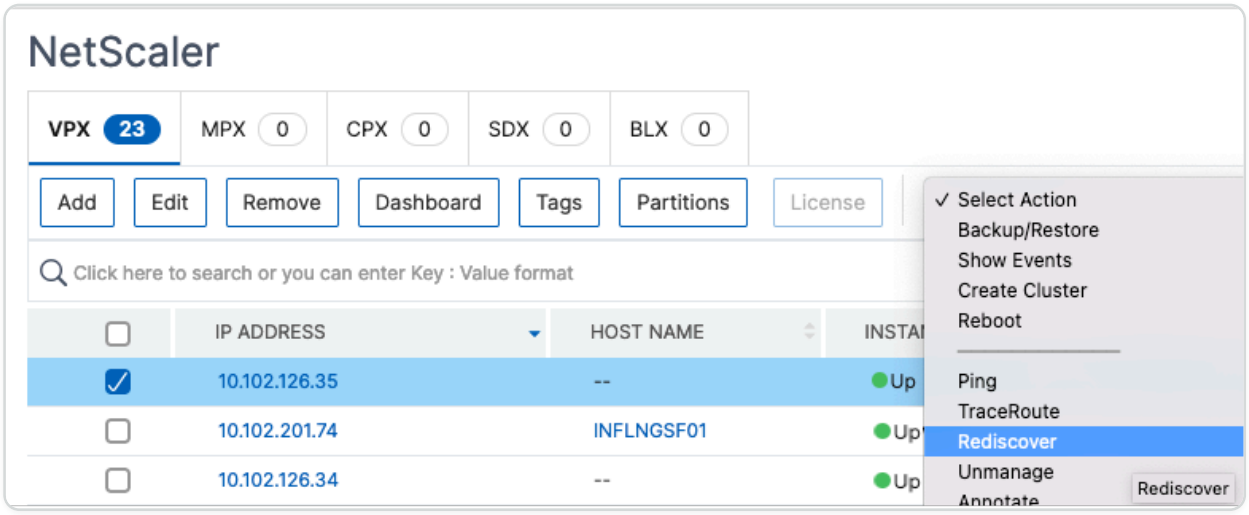
4. The newly created profile appears under **Admin Profiles**.
5. Go to **Network > Instances > NetScaler**. Select the NetScaler instance for which the password has been modified, and the select **Edit**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Select the newly created Profile Name and click **OK**.



7. Select the instance again, right-click, and select **Rediscover**.



You've successfully changed the password.

For information about changing the password of an SDX appliance, see How to change a NetScaler SDX root password.

How to change a NetScaler SDX nsroot password

Occasionally, you must change the nsroot password of the NetScaler appliance for security reasons or compliance of password rotation policy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This document describes the steps required to change the nsroot password of a NetScaler SDX appliance managed through NetScaler Console cloud.

If you change the NetScaler password, you must modify the NetScaler Console admin profile that is associated with the NetScaler. A NetScaler Console admin profile maintains the NetScaler credentials for REST API, SSH, SCP, or SNMP based communication with the NetScaler appliance. Through admin profiles, NetScaler Console manages NetScaler SDX appliances.

Change password

Follow these steps to change the password:

- Step 1. Change the SDX password from the SDX Management Service GUI.
- Step 2. Modify the NetScaler Console admin profile associated with the SDX.

Note:

> If the SDX appliance is managed by other tools as well, you must change the credentials on those tools as well.

Change the SDX password from the SDX Management Service GUI

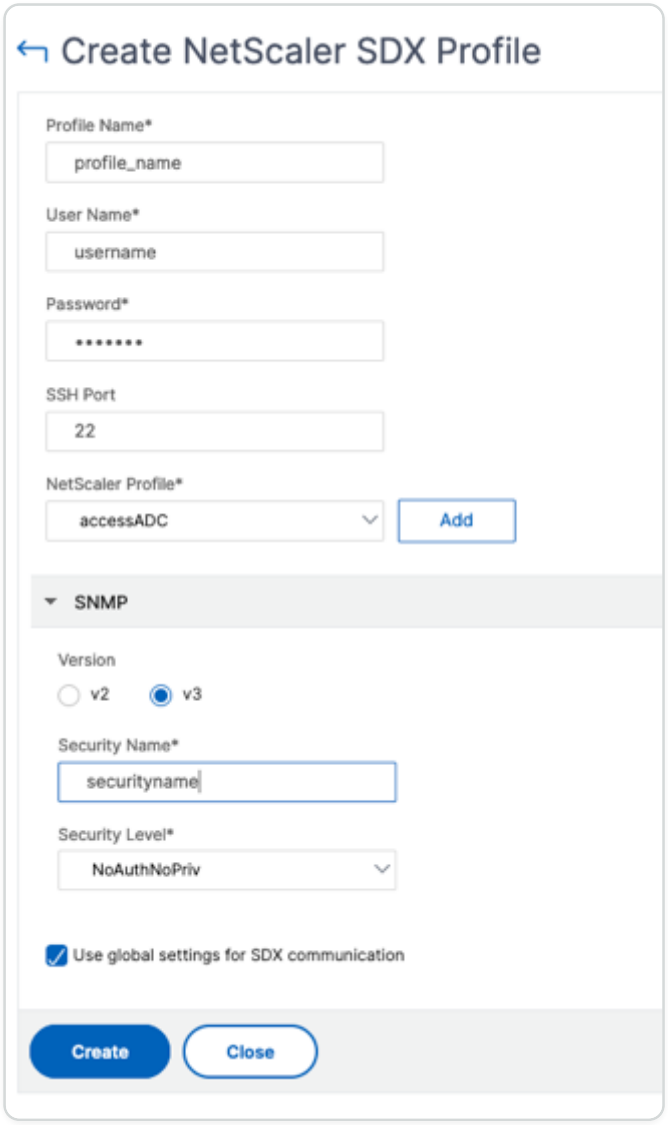
1. From SDX Management Service, navigate to **System > User Administration > Users**.
2. Select the user name for which you want to change the password and click **Edit**.
3. Select **Change Password**.
4. Enter a new password and click **OK**.
5. The SDX password has been changed

Modify the NetScaler Console admin profile

After you've modified the SDX passwords, you must modify the admin profiles of the instances. Follow these steps:

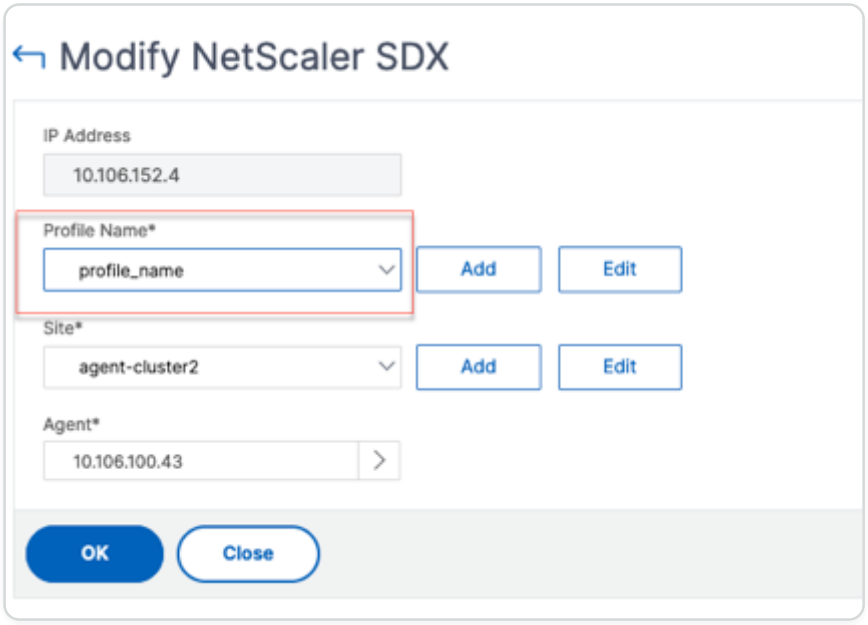
1. Navigate to **Infrastructure > Instances Dashboard > NetScaler > SDX**.
2. Select **Profiles** to see all the admin profiles.
3. Select **Add** to create an admin profile.
4. Provide new NetScaler credentials, and click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

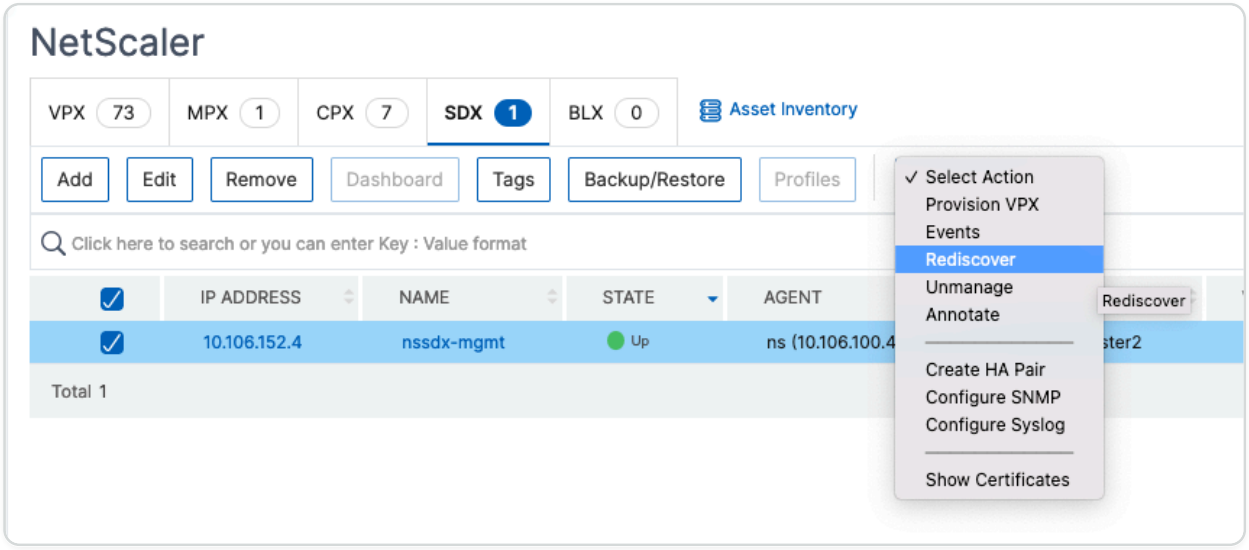


5. The newly created profile appears under **Admin Profiles**.
6. Go to **Network > Instances > NetScaler > SDX**. Select the instance for which the password has been modified, and the select **Edit**.
7. Select the newly created profile name and click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. Select the instance again, right-click, click **Rediscover**.



You've successfully changed the password.

For information about changing the password of an SDX appliance, see How to change a NetScaler MPX or VPX root password.

How to generate a technical support bundle for a NetScaler® instance

For help with analyzing and resolving any issues with a NetScaler instance, you can generate a technical support bundle on the instance and send the bundle to Citrix technical support. The technical support bundle is a zipped tar archive of system configuration data and statistics. The technical support bundle collects the following data from the NetScaler instance on which you generate the bundle:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Configuration files. All files in the /flash/nsconfig directory.
- `newnslog` files. The currently running `newnslog` and some previous files. To minimize the archive file size, the `newnslog` collection is restricted to 500 MB, 6 files, or 7 days, whichever occurs first. If older data is needed, it might require manual collection.
- Log files. Files in /var/log/messages, /var/log/ns.log, and other files under /var/log and /var/nslog.
- Application core files. Files created in the /var/core directory within the last week, if any.
- Output of some CLI show commands.
- Output of some CLI stat commands.
- Output of BSD shell commands.

It is mandatory to specify the time for generating technical support files. You must explicitly choose a time reference when generating a technical support file. You can either select the `custom` option and specify a custom date and time or use the `Now` option. Specifying the time ensures that the exact time context is explicitly defined.

The time parameter specifies the reference time, in Common Log Format, used to locate `newnslog` files. The format is: `DD/MMM/YYYY:HH:MM:SS`.

When time is specified, up to four `newnslog` log files are collected:

- The `newnslog` file corresponding to the specified time range
- The log file created immediately before the first file (if available)
- The log file created immediately after the first file (if available)
- The latest `newnslog` directory

NOTE:

If the scope is set to cluster, the second and third log files are not collected on any node.

You can also securely upload the technical support bundle to the Citrix technical support server. Starting from NetScaler 14.1 release 8.x build, you must generate an authentication token before you upload the technical support bundle. In the previous builds, you can upload the technical support bundle using Citrix username and password.

To generate the authentication token:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Launch a browser and enter the following URL - `<https://cis.citrix.com/auth/api/create_identity_v2/?expiration=3600>`.
2. Log in using multifactor authentication.

   NOTE:

   For information on how to enroll for multifactor authentication, see How to Enroll into multifactor authentication (MFA).

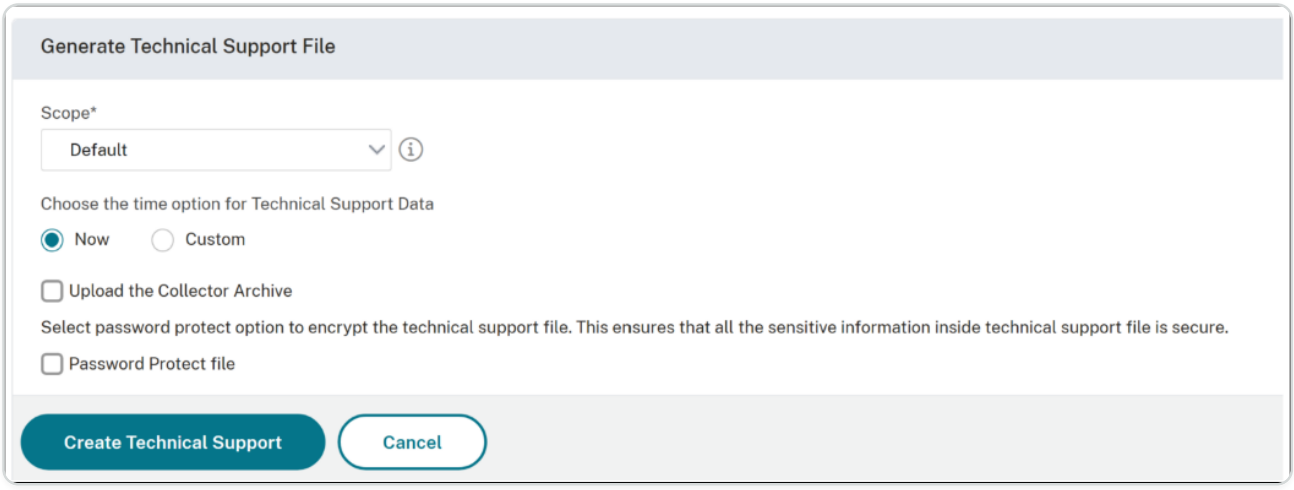
3. Click **Copy** to copy the authentication token displayed on the screen. The token is valid for 3600 seconds (1 hour). The maximum allowed length for the token is 1023 characters.

After copying the authentication token, use the GUI to upload the file.

To upload the technical support bundle using the GUI:

1. Navigate to **Infrastructure > Instances > NetScaler**.
2. Select a NetScaler instance.
3. Select **Generate Technical Support File** from **Select Actions**.
4. Click **Generate Technical Support File**.
5. Use the **Scope** option to specify if you want to gather data on the present node, all cluster nodes, or for the specified partitions.
6. Select one of the following options from **Choose the time option for Technical Support Data**:
   - **Now** - Uses the current system time and preserves the behavior of earlier releases.
   - **Custom** - Uses the specified date and time.
7. Select **Upload the Collector Archive**.
8. In the **My Citrix Account** section, enter the authentication token in the **Citrix Authentication Token** field.
9. Click **Create Technical Support**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Events

When the IP address of a Citrix Application Delivery Controller (NetScaler) instance is added to NetScaler Console, NetScaler Console sends a NITRO call and implicitly adds itself as a trap destination for the instance to receive its traps or events.

Events represent occurrences of events or errors on a managed NetScaler instance. For example, when there is a system failure or change in configuration, an event is generated and recorded on the NetScaler Console server. Events received in NetScaler Console are displayed on the Events Summary page (**Infrastructure > Events**), and all active events are displayed in the Event Messages page (**Infrastructure > Events > Event Messages**).

NetScaler Console also checks on the events generated on instances to form alarms of different severity levels and displays them as messages, some of which might require immediate attention. For example, system failure can be categorized as a "Critical" event severity and can be addressed immediately.

You can configure rules to monitor specific events. Rules make it easier to monitor various events generated across your NetScaler infrastructure.

You can filter a set of events by configuring rules with specific conditions and assigning actions to the rules. When the events generated meet the filter criteria in the rule, the action associated with the rule is run. The conditions for which you can create filters are: severity, NetScaler instances, category, failure objects, configuration commands, and messages.

You can also ensure that multiple notifications are triggered for a specific time interval for an event until the event is cleared. As an extra measure, you might want to customize your email with a specific subject line, user message, and upload an attachment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

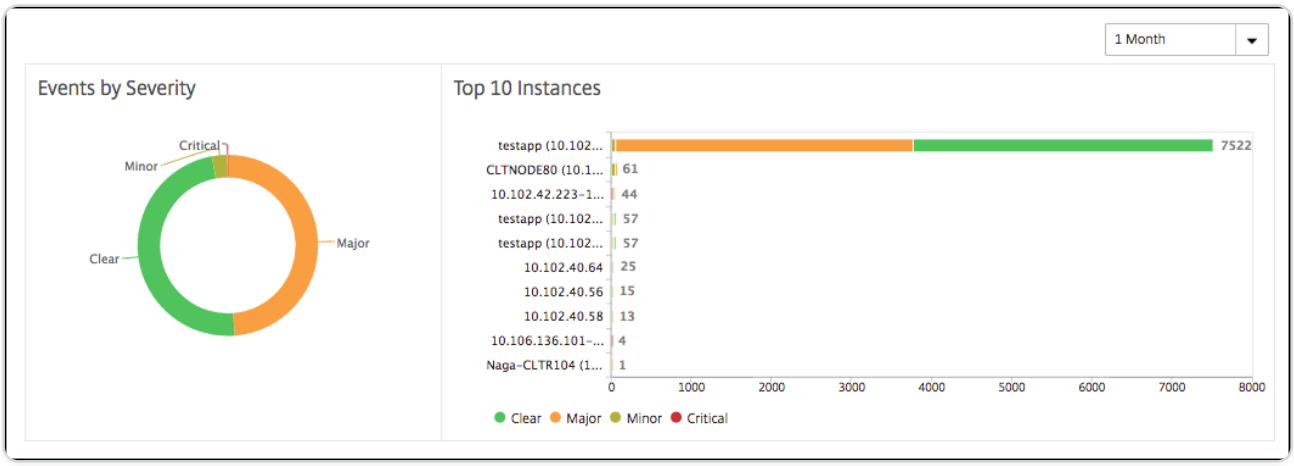
Use events dashboard

As a network administrator, you can view details such as configuration changes, login conditions, hardware failures, threshold violations, and entity state changes on your Citrix Application Delivery Controller (NetScaler) instances, along with events and their severity on specific instances. You can use the events dashboard of NetScaler Console to view reports generated for critical event severity details on all your NetScaler instances.

To view the details on the events dashboard:

Navigate to **Infrastructure > Events > Reports**.

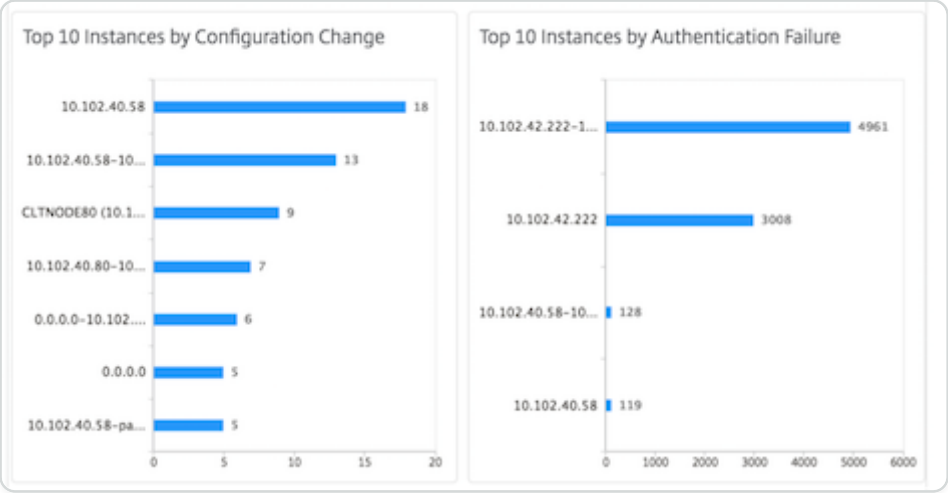
The Top 10 Devices graph on the dashboard displays a report of the top 10 instances by the number of events generated on them. You can click an instance on the graph to view further details of the event's severity.



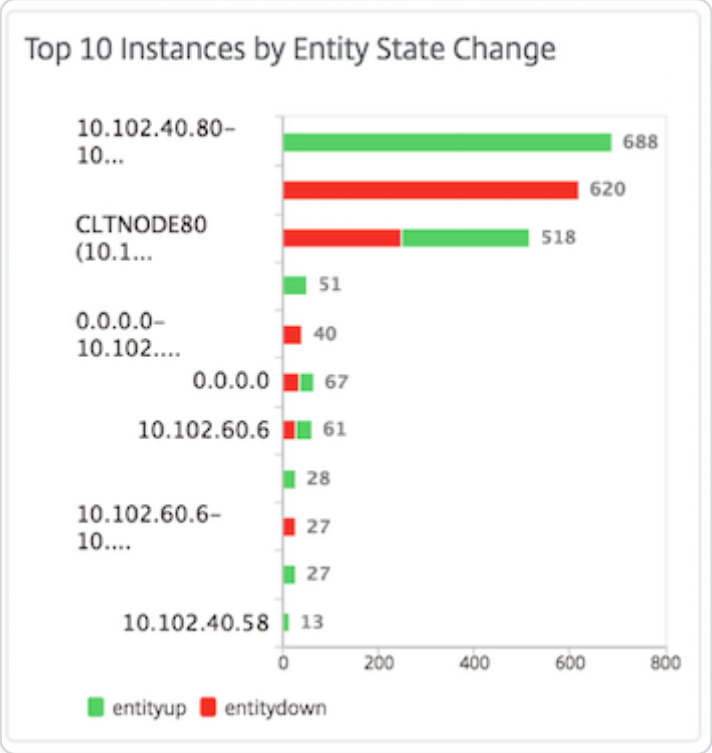
You can view more details by navigating to the NetScaler instance type (**Infrastructure > Events > Reports** > **NetScaler/ NetScaler SDX/ NetScaler**) to view the following:

- Top 10 devices by hardware failure
- Top 10 devices by configuration change
- Top 10 devices by authentication failure

© 1997–2026 Citrix Systems, Inc. All rights reserved.

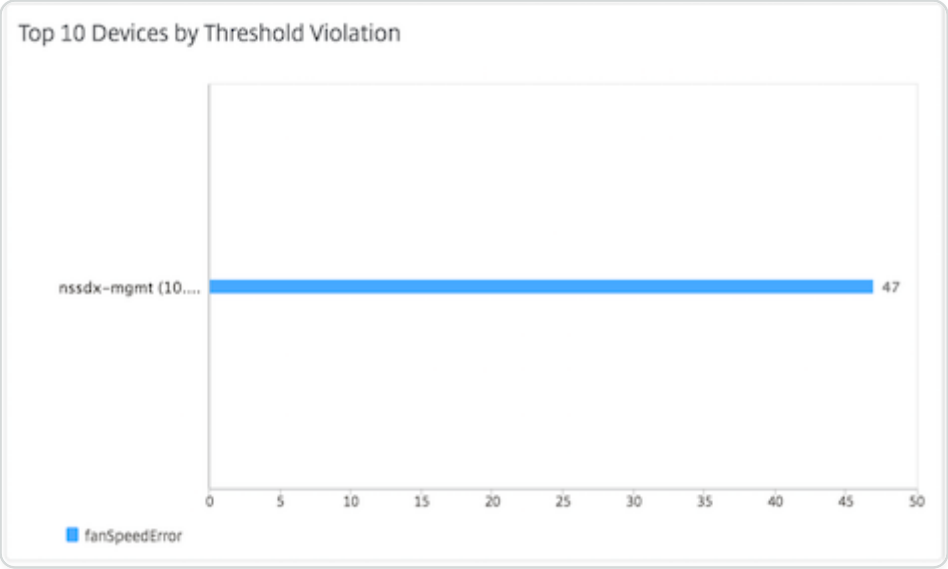


- Top 10 devices by entity state changes



- Top 10 devices by threshold violation

© 1997–2026 Citrix Systems, Inc. All rights reserved.



To export the report of this dashboard:

To export the report of this page, click the **Export** icon on the top right side of this page. On the **Export** page, you can do one of the following:

1. Select **Export Now** tab. To view and save the report in PDF, JPEG, PNG, or CSV format.
2. Select **Schedule Export** tab. To schedule the report daily, weekly, or monthly and send the report over an email or a slack message.

NOTE:

- If you select **Weekly** recurrence, ensure that you select the weekdays on which you want the report to be scheduled.
- If you select **Monthly** recurrence, ensure that you enter all the days that you want the report to be scheduled separated by commas.

Create event rules

You can configure rules to monitor specific events. Rules make it easier to filter the events generated across your infrastructure.

You can filter a set of events by configuring rules with specific conditions and assigning actions to the rules. When the events generated meet the filter criteria in the rule, the action associated with the rule is run.

You can create filters for the following conditions:

- Severity

© 1997–2026 Citrix Systems, Inc. All rights reserved.

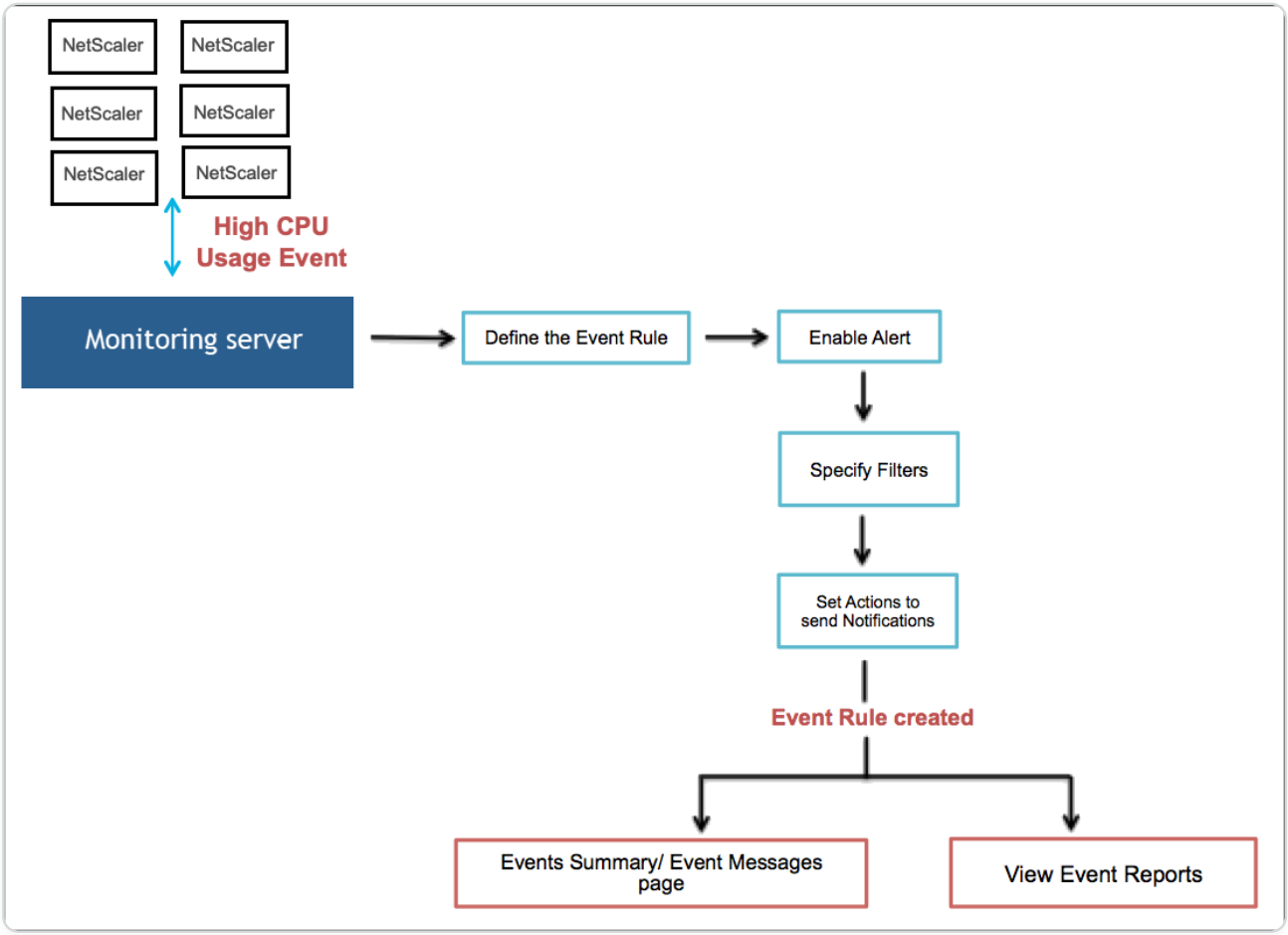
- Citrix Application Delivery Controller (NetScaler) instances
- Category
- Failure objects
- Configuration commands
- Messages

After you create events, you can assign actions to the events. For more information, see Add event rule actions.

For example, as an administrator you might want to monitor "high CPU usage" events on NetScaler instances which might lead to an outage. You can do any of the following actions to receive notifications:

- Create a rule to monitor instances and add an action to the rule to receive notifications when such events occur.
- Schedule a rule to monitor instances at a specific interval. So, you receive notifications when such events occur within that interval.

The following image explains the workflow of how event rules work.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure an event rule

To configure a event rule, navigate to **Infrastructure > Events > Rules**, and click **Add**. In the **Create Rule** page, do the following tasks:

1. Specify name and instance family
2. Configure event age
3. Choose severity of the event that the rule detects
4. Specify category of the event
5. Specify NetScaler® instances to which the rule applies
6. Select failure objects
7. Specify advanced filters
8. Specify actions to be taken when the rule detects an event

Step 1 - Specify name and instance family

1. **Name**. Enter a name for the event rule.
2. **Instance Family**. Select an instance family from the **Instance Family** drop-down list.

   You can filter event rules by **Instance Family** to track the NetScaler instance from which NetScaler Console receives an event.



Step 2 - Configure event age

1. **Event Age**. Specify the time interval (in seconds) after which NetScaler Console refreshes an event rule.

   For example, you want an email to be sent every time your NetScaler instance has a "high CPU usage" event for 60 seconds or longer. You can set the event age to 60 seconds. Now

© 1997–2026 Citrix Systems, Inc. All rights reserved.

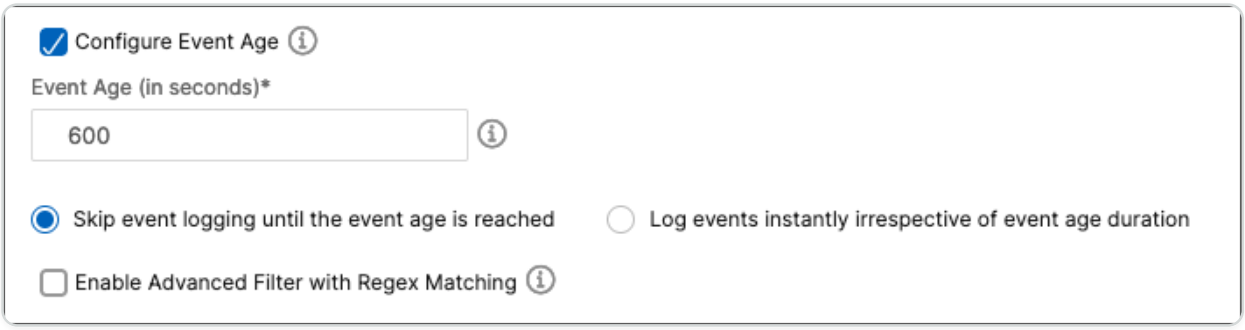
whenever your NetScaler instance has a "high CPU usage" event for 60 seconds or more, you receive an email notification.

NOTE:

Event Age is a mandatory field. The minimum value for the event age is 60 seconds. If you keep the **Event Age** field blank, the event rule is applied immediately after the event occurs.

2. Choose one of the following options to track your events:

   - **Skip event logging until the event age is reached**. Events that occur before the specified event age aren't logged in the NetScaler Console server database. When the event age is reached, events are logged in the database and configured event actions are triggered.
   - **Log events instantly irrespective of event age duration**. All events are logged in the NetScaler Console server database regardless of the specified event age. After the event age is reached, configured event actions are triggered.



3. **Enable Advanced Filter with Regex Matching**. Select this option to include a regular expression other than asterisk (*) pattern matching. This option is applicable for failure objects, configuration commands, and messages.

Step 3 - Choose severity of event

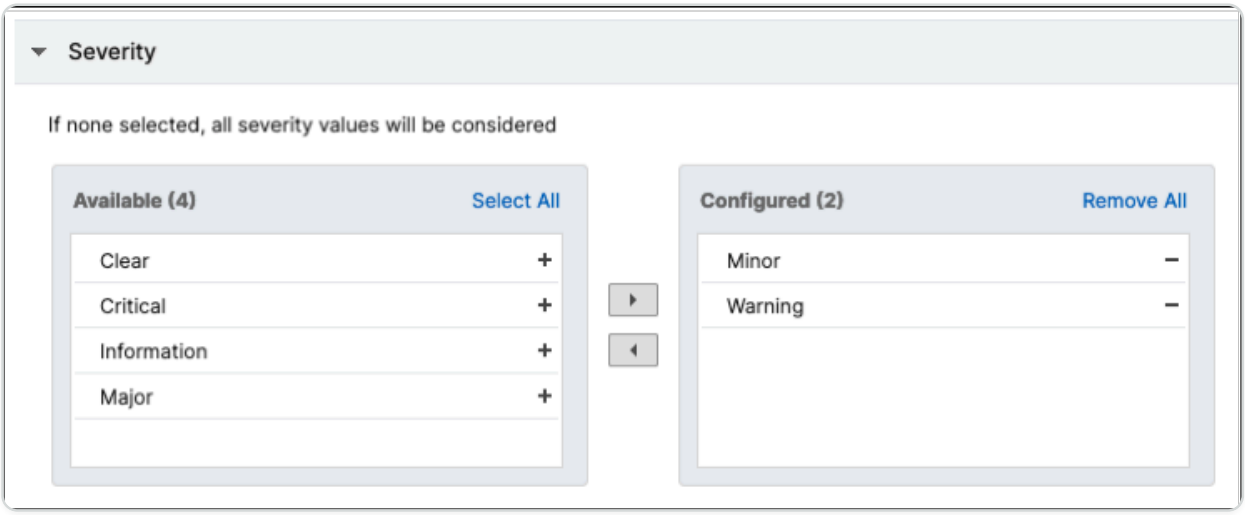
- In **Severity** section, select a severity for your event rule.

  You can define the following levels of severity: Critical, Major, Minor, Warning, Clear, and Information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

You can configure severity for both generic and Advanced-specific events. To modify event severity for NetScaler instances managed on NetScaler Console, navigate to **Infrastructure > Events > Event Settings**. Choose the **Category** for which you want to configure event severity and click **Configure Severity**. Assign a new severity level and click **OK**.



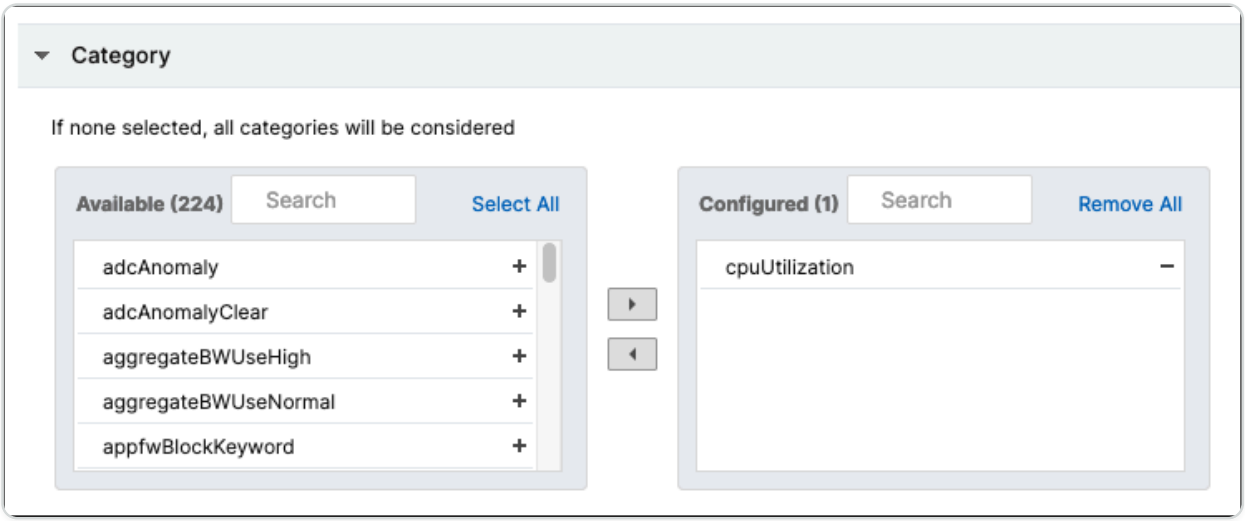
Step 4 - Specify event category

You can specify the category or categories of the events generated by your NetScaler instances. All categories are created on NetScaler instances. These categories are then mapped with the NetScaler Console that can be used to define event rules.

- Select the category that you want to consider and move it from the **Available** table to the **Configured** table.

  In the example, you must choose "cpuUtilization" as the event category from the table displayed.

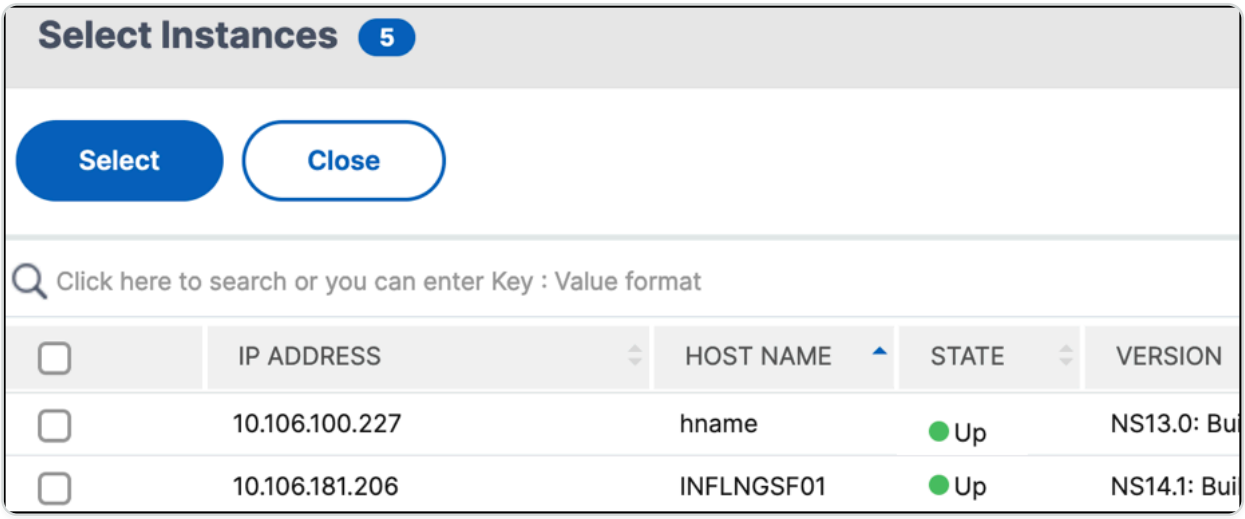
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Step 5 - Specify NetScaler instances

In the **Instances** section, do the following:

1. Click **Select Instances**. In the **Select Instances** page, select the IP addresses of the NetScaler instances for which you want to define the event rule.
2. Click **Select**.



Step 6 - Select failure objects

Failure objects are entity instances or counters for which an event has been generated.

1. Click **Select Failure Objects**.
2. In the **Failure Objects** page, select a failure object from the list. Click **Select**.
3. To add a failure object, enter a regular expression in **Add Failure Objects**. Depending on the specified regular expression, the failure objects are automatically added to the list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

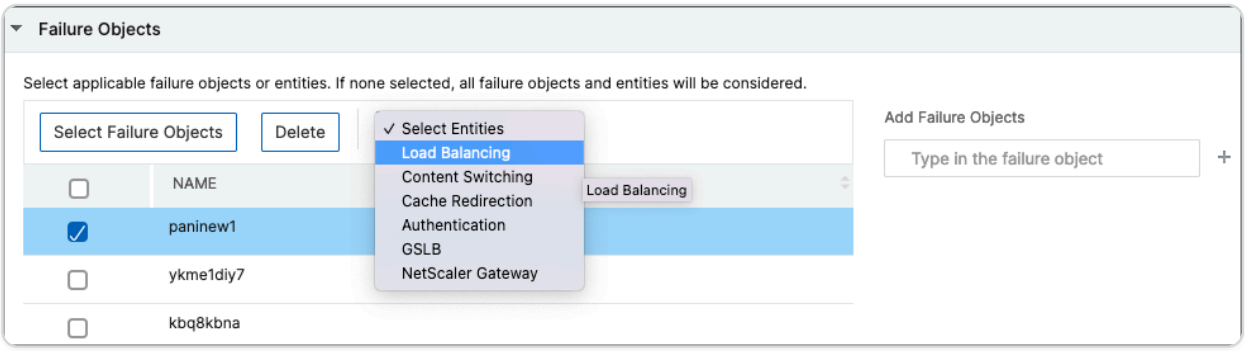
IMPORTANT:

To list failure objects using regular expression, select **Enable Advanced Filter with Regex Matching** in Step 1.

The advanced filter allows you to track issues on the failure objects quickly and identify the cause for an issue. For example, if a user has login issues, then the failure object is the user name or password, such as `nsroot`.

4. To add entities, choose an entity from **Select Entities**.

   This list can have counter names for all threshold-related events, entity names for all entity-related events, certificate names for certificate-related events, and so on.



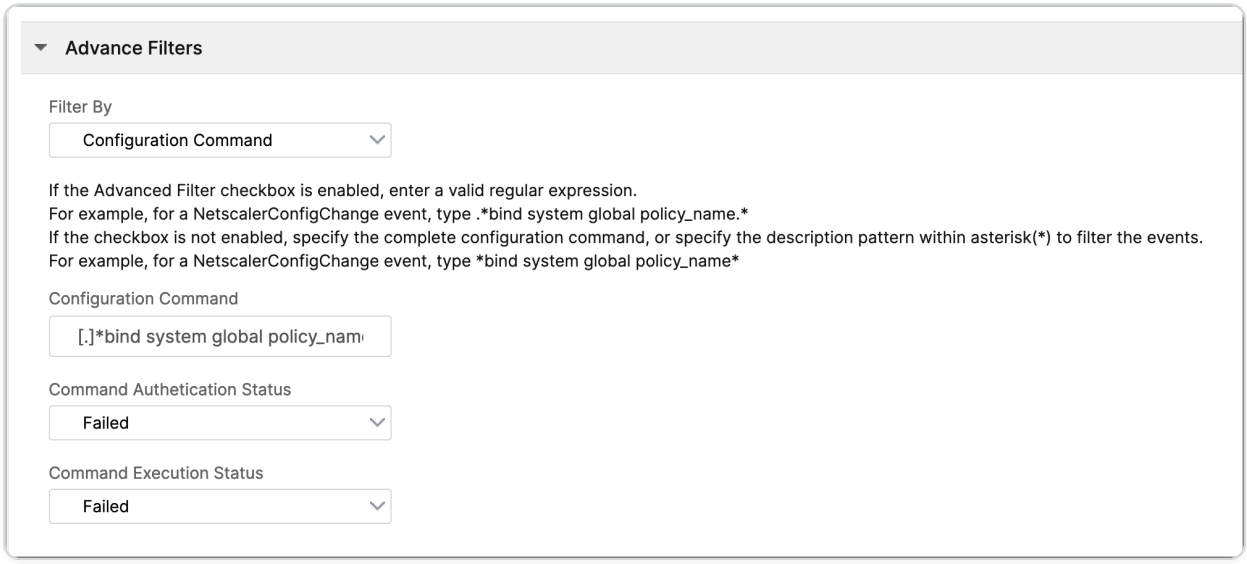
Step 7 - Specify advanced filters

You can further filter an event rule with advanced filters. Select one of the following filters:

- **Configuration Commands** - Specify the complete configuration command, or specify a regular expression to filter events.

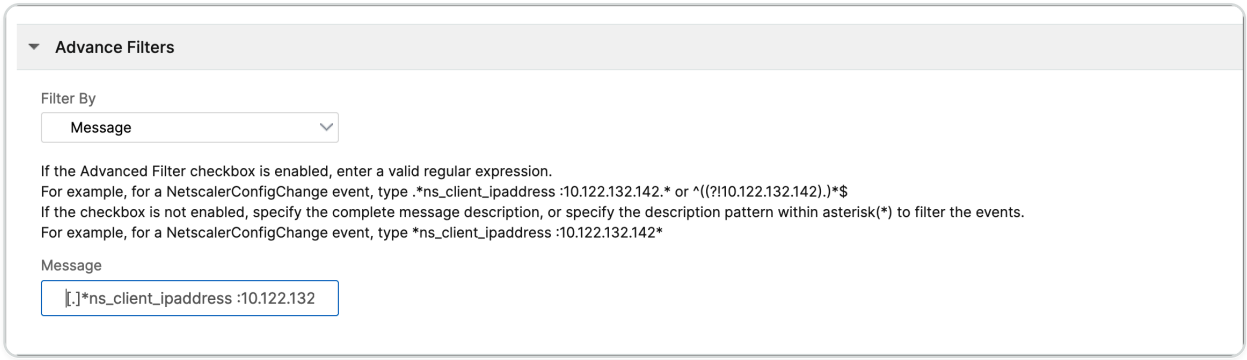
  You can also filter the event rules by the command's authentication status and its execution status. For example, for a `NetscalerConfigChange event`, type `[.]*bind system global policy_name[.]*`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Messages** - Specify the complete message description, or specify a regular expression to filter the events.

  For example, for a `NetscalerConfigChange` event, type `[.]*ns_client_ipaddress :10.122.132.142[.]* or ns_client_ipaddress :\^([.]*10.122.132.142[.]*)`.



IMPORTANT:

To filter configuration commands and messages using regular expression other than asterisk (*) pattern matching, select **Enable Advanced Filter with Regex Matching** in Step 1.

Step 8 - Add event rule actions

You can add event rule actions to assign notification actions for an event. These notifications are sent or done when an event meets the defined filter criteria that you've set in Step 7.

1. Click **Add Action**.
2. In the **Add Event Action** page, you can add the following event actions:

- Send email Action

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Send Trap Action
- Run Command Action
- Execute Job Action
- Suppress Action
- Send Slack Notifications
- Send PagerDuty Notifications
- Send ServiceNow Notifications

Send email Action

When you choose **Send e-mail Action**, an email is triggered when the events meet the defined filter criteria.

1. **Email Distribution List**. Select an email distribution list. To add a distribution list, click Add.
    a. In the **Create Email Distribution List** page, do the following:
        i. **Name**. Add a name for the distribution list.
        ii. **Email Servers**. Select an email server. You can also add a server or edit an existing one.
        iii. **From**. Add the sender's email address.
        iv. **To**. Add the recipients email addresses. You can also specify the email addresses be included in the CC and Bcc list.
        v. Click **Create**.
2. **Subject**. Add a subject line for your emails, like the name of the affected entity, that is, the name of the failure object. This subject line provides information about the virtual server where these events occur.

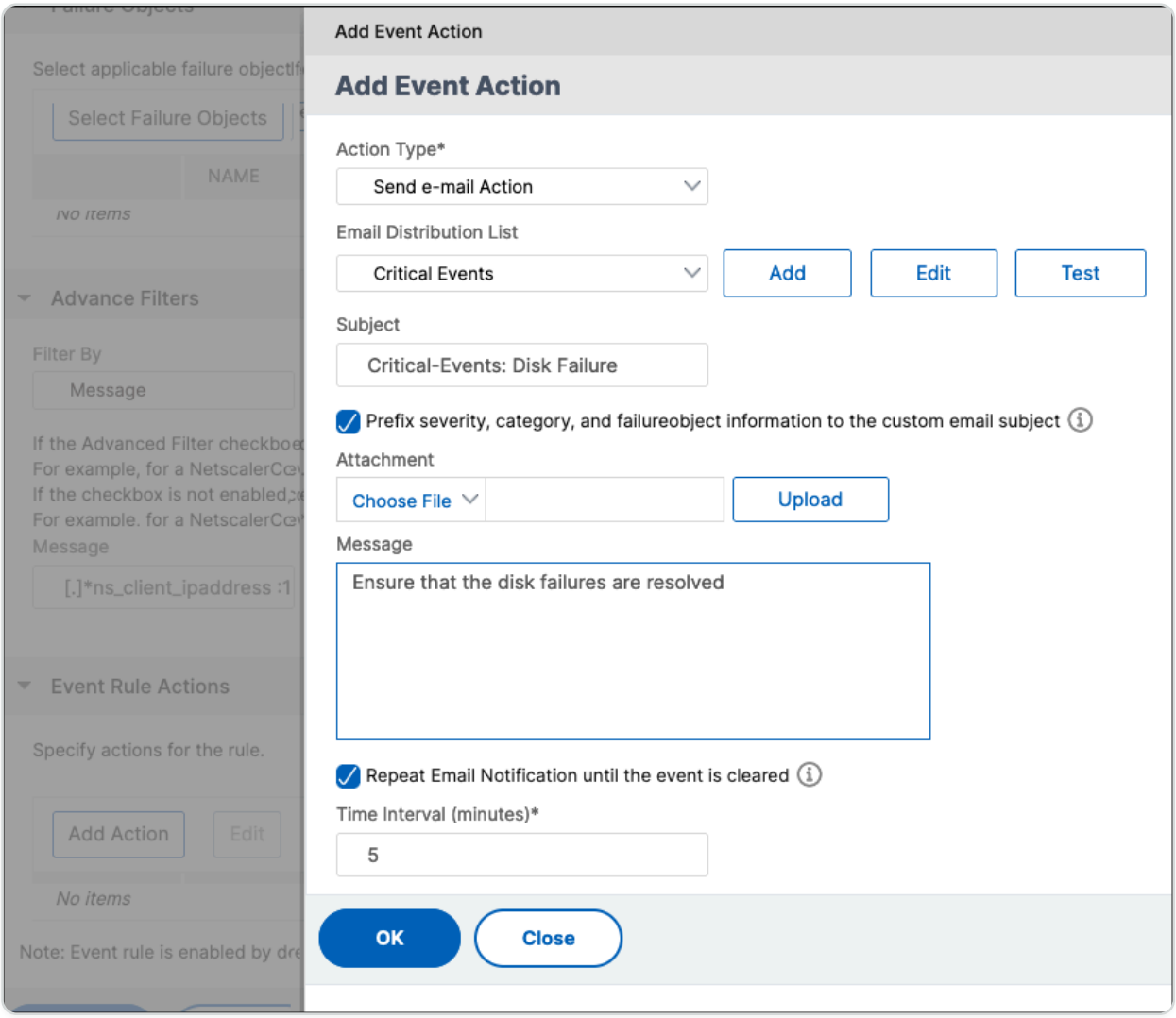
    NOTE:

    If you do not add a subject line, a default subject line is displayed. The default subject line provides information only about the severity of the event, the category of the event, and the failure object. The name of the virtual server where the event occurred is not available.

3. **Attachment**. Upload an attachment to your email. This attachment is sent when an incoming event matches the configured rule.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. **Test**. Click this button to send a test email after configuring an email server, associated distributed lists, and other settings. This option allows you to test the configured settings
5. **Repeat Email Notification until the event is cleared**. Select this option to make sure that email notifications are not missed for critical events. This option sends repeated emails for event rules that meet the criteria you've selected. For example, you've created an event rule for instances that involve disk failures. If you want to be notified until the issue is resolved, opt to receive repeated email notifications about those events.



6. Click **OK**.

NOTE:

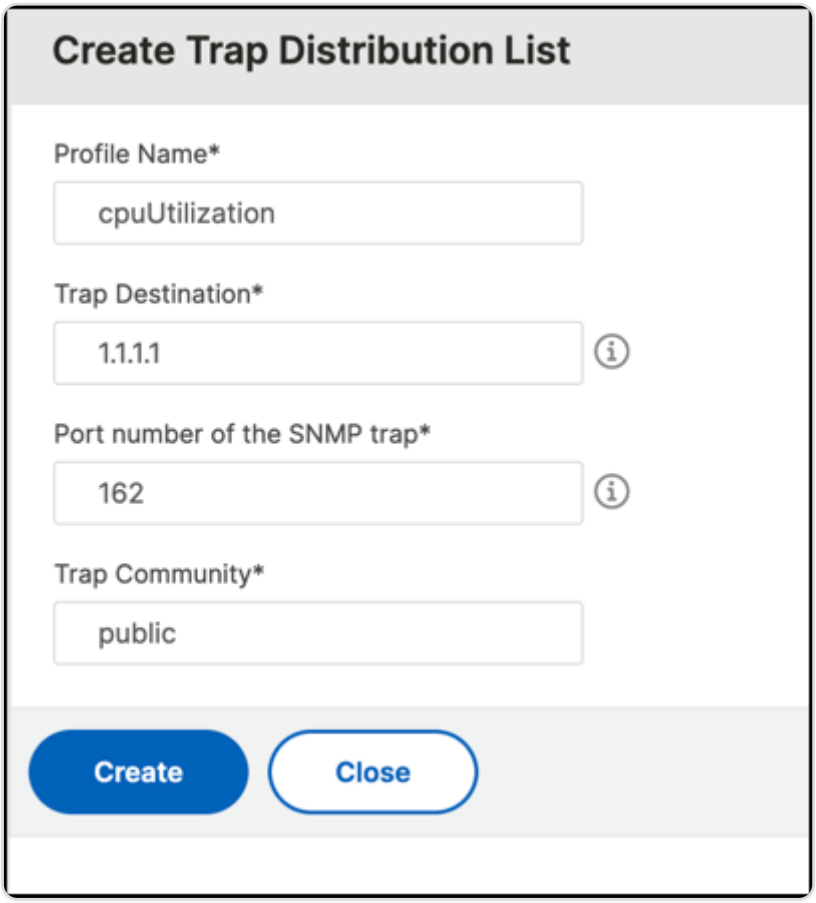
You can also add the email distribution lists by navigating to **Settings** > **Notifications** > **Email**. Click **Add** and create the list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Send Trap Action

When you choose the **Send Trap Action** event action type, SNMP traps are sent or forwarded to an external trap destination. The trap messages are sent to the specific trap listener when events meet the defined filter criteria.

1. **Trap Distribution List**. Select a trap distribution list (or a trap destination and trap profile details). To create a trap distribution list, click **Add**.
2. In the **Create Trap Distribution List** page, do the following:
   a. **Profile Name**. Enter the profile name.
   b. **Trap Destination**. Enter the name or IP address of the instance that should receive the trap messages.
   c. **Port number of the SNMP trap**. Enter the port number.
   d. **Trap Community**. Enter the group to which the instance belongs.



   e. Click **Create**.
3. Click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Run Command Action

When you choose the **Run Command Action** event action, you can create a command or a script that can be run on NetScaler Console for events matching a particular filter criterion.

You can also set the following parameters for the **Run Command Action** script:

Parameter	Description
$source	This parameter corresponds to the source IP address of the received event.
$category	This parameter corresponds to the type of traps defined under the category of the filter
$entity	This parameter corresponds to the entity instances or counters for which an event has been generated. It can include the counter names for all threshold-related events, entity names for all entity-related events, and certificate names for all certificate-related events.
$severity	This parameter corresponds to the severity of the event.
$failureobj	The failure object affects the way that an event is processed and ensures that the failure object displays the exact problem as notified. This can be used to track down problems quickly and to identify the reason for failure, instead of simply reporting raw events.

NOTE:

During command execution, these parameters are replaced with actual values.

For example, consider that you want to set a run command action when a load balancing virtual server status is **Down**. As an administrator, you might want to provide a quick workaround by adding another virtual server. In NetScaler Console, you can:

- Write a script (.sh) file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The following is a sample script (.sh) file:

```
#!/bin/sh

source=$1

failureobj=$2

payload='{"params":{"warning":"YES"},"lbvserver":
{"name":"'$failureobj'","servicetype":"HTTP","ipv46":"x.x.x.x","port":"
80","td":"","m":"IP","state":"ENABLED","rhistate":"PASSIVE","appflowlog
":"ENABLED","

bypassaaaa":"NO","retainconnectionsoncluster":"NO","comment":""}}'

url="http://$source/nitro/v1/config/lbvserver"

curl --insecure -basic -u nsroot:nsroot -H "Content-type: application/
json" -X POST -d $payload $url
```

- Save the .sh file in any persistent location on the agent. For example, `/var`.
- Provide the .sh file location in NetScaler Console to run when the rule criteria are met.

1. In **Command Execution List**, click **Add**.

   The Create Command Distribution List page is displayed.

   a. **Profile Name**. Specify a name of your choice

   b. **Run Command**. Specify the agent location where the script has to run. For example: `sh/var/demo.sh $source $failureobj`.

   c. Select **Append Output** and **Append Errors**

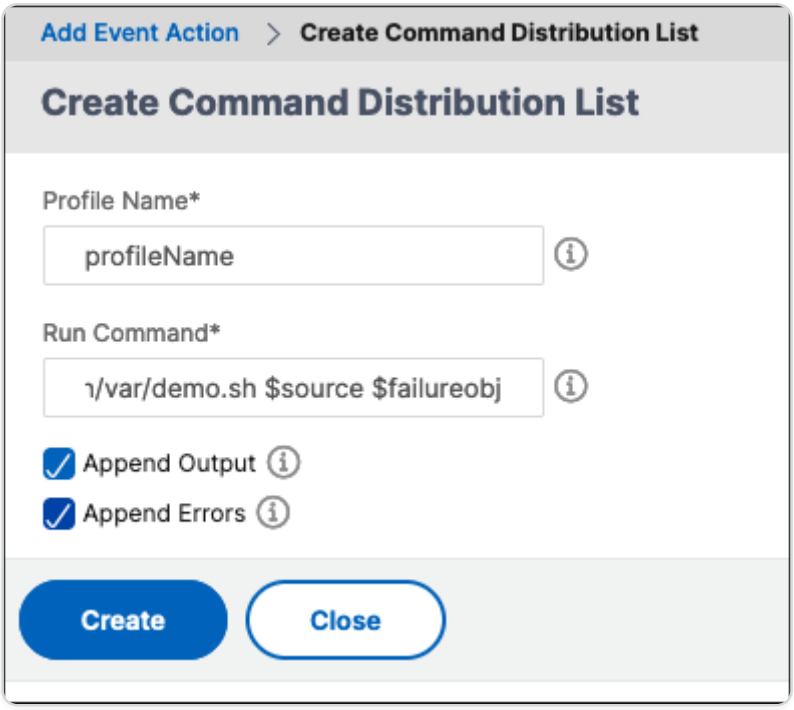
   NOTE:

   You can enable the **Append Output** and **Append Errors** options if you want to store the output and errors generated (if any) when you run a command script in the NetScaler Console server log files. If you do not enable these options, NetScaler Console discards all outputs and errors generated while running the command script.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. Click **Create**.

2. In the **Add Event Action** page, click **OK**.



NOTE:

You can enable the **Append Output** and **Append Errors** options if you want to store the output and errors generated (if any) when you run a command script in the NetScaler Console server log files. If you do not enable these options, NetScaler Console discards all outputs and errors generated while running the command script.

Execute Job Action

When you create a profile with configuration jobs, a job is run as a built-in job or a custom job for NetScaler and NetScaler SDX instances for events and alarms that match the filter criteria you've specified.

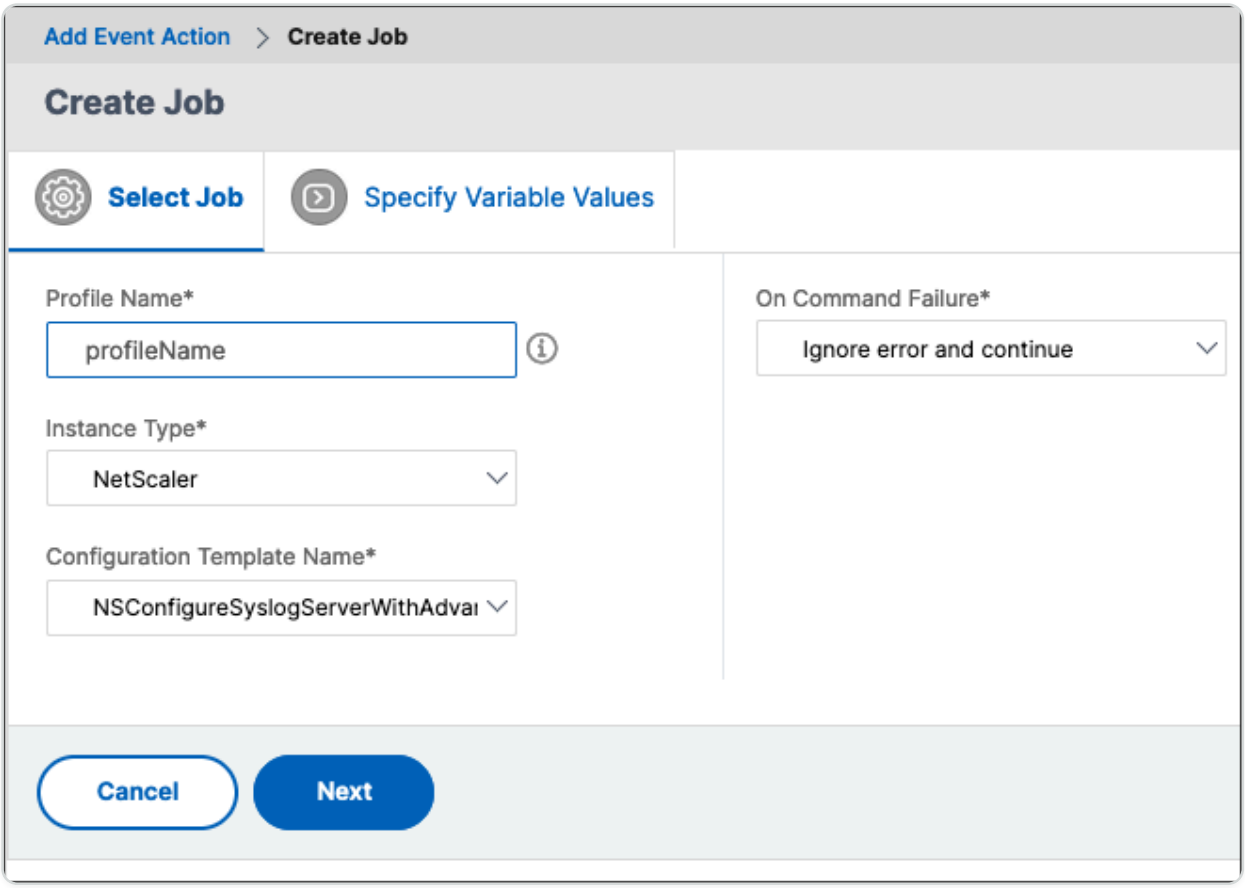
1. In **Job Profile List**, select a job profile. To add a list, click **Add**.
2. In the **Create Job** page, do the following:

   a. **Select Job**. Create a profile with a job that you want to run when the events meet the defined filter criteria. Specify a profile name, the instance type, the configuration template, and the action to be done if the commands on the job fail.

   b. **Specify Variable Values**. Based on the instance type selected and the configuration template chosen, specify your variable values.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

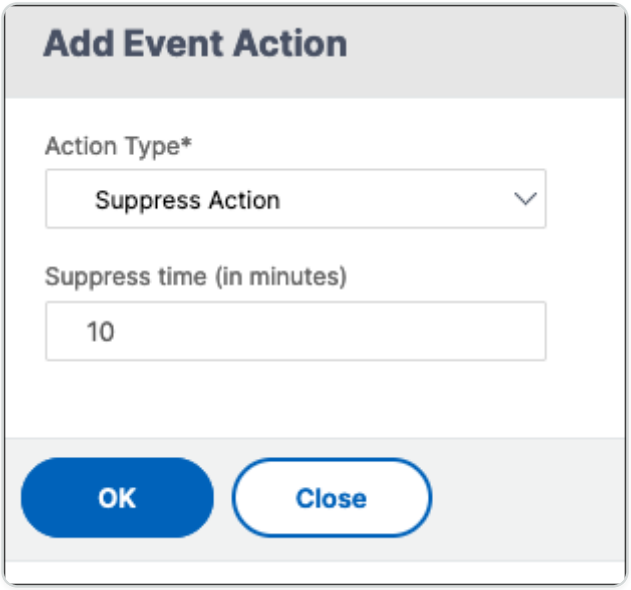
c. Click **Finish** to create the job.



3. Click **OK**.

Suppress Action

- In **Suppress time**, enter a time period, in minutes, for which an event is suppressed or dropped. You can suppress the event for a minimum of 1 minute.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

You can also configure the suppress time as 0 minutes and it means infinite time. If you do not specify any time duration, then NetScaler Console considers the suppress time as zero and it never expires.

Send Slack notifications

When you configure a Slack channel, the event notifications are sent to this channel. You can configure many Slack channels to receive these notifications

1. In **Slack Profile List**, select a Slack profile. To add a Slack profile, click **Add**.
2. In the **Create Slack Profile** page, do the following:
    a. **Profile Name**. Type a name for the profile list to be configured on NetScaler Console
    b. **Channel Name**. Type the name of the Slack channel to which the event notifications are to be sent.
    c. **Webhook URL**. Type the Webhook URL of the channel that you entered. Incoming Webhooks are a simple way to post messages from external sources into Slack. The URL is internally linked to the channel name. All event notifications are sent to this URL and then posted to the chosen Slack channel. An example of a webhook is as follows: `<https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK>`
    d. Click **Create**.
3. Click **OK**.

NOTE:

You can also add the Slack profiles by navigating to **Settings** > **Notifications** > **Slack Profiles**. Click **Add** and create the profile.

Send PagerDuty notifications

You can add a PagerDuty profile as an option in NetScaler Console to monitor the incident notifications based on your PagerDuty configurations. PagerDuty enables you to configure notifications through email, SMS, push notification, and phone call on a registered number.

1. In **PagerDuty Profile list**, select a PagerDuty profile. To add a profile, click **Add**.
2. In the **Create PagerDuty Profile** page:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. **Profile Name**. Enter a profile name of your choice.

b. **Integration Key**. Enter the Integration Key.

   You can get the Integration Key from your PagerDuty portal.

c. Click **Create**.

Before you add a PagerDuty profile in NetScaler Console, make sure you've completed the required configurations in PagerDuty. For more information, see the PagerDuty documentation.

You can select your PagerDuty profile as one of the options to get notifications for the following features:

- **Events** – List of events that are generated for NetScaler instances.
- **Licenses** – List of licenses that are currently active, about to expire, and so on.
- **SSL Certificates** – List of SSL certificates that are added to NetScaler instances.

Use case:

Consider a scenario where you want to:

- Send notifications to your PagerDuty profile.
- Configure a phone call as an option in PagerDuty to receive notifications.
- Get phone call alerts for NetScaler events.

Create the PagerDuty configuration. After the configuration is complete, whenever a new event is generated for the NetScaler instance, you'll receive a phone call. From the phone call, you can decide to:

- Acknowledge the event
- Mark it as resolved
- Escalate to another team member

Send ServiceNow notifications

You can auto-generate ServiceNow incidents for NetScaler Console events by selecting the ServiceNow profile on the NetScaler Console GUI. You must choose the **ServiceNow** profile in NetScaler Console to configure an event rule.

Before you configure an event rule to auto-generate ServiceNow incidents, integrate the NetScaler Console with the ServiceNow instance. For more information, see Configure ITSM adapter for ServiceNow.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. In **ServiceNow Profile**, select the **Citrix_Workspace_SN** profile from the list.
2. Click **OK**.

Schedule an event filter

After creating a filter for your rule, if you do not want the NetScaler Console to send a notification every time the event generated satisfies the filter criteria, you can schedule the filter to trigger only at specific time intervals such as daily, weekly, or monthly.

For example, if you have scheduled a system maintenance activity for different applications on your instances at different times, the instances might generate multiple alarms.

If you have configured a filter for these alarms and enabled email notifications for these filters, the server sends many email notifications when NetScaler Console receives these traps. If you want the server to send these email notifications during a specific time period only, you can do so by scheduling a filter.

To schedule a filter using NetScaler Console:

1. In the NetScaler Console, navigate to **Infrastructure > Events > Rules**.
2. Select the rule you want to schedule a filter for, and click **View Schedule**.
3. On the **Scheduled Rule** page, click **Schedule** and specify the following parameters:
    - **Enable Rule** – Select this check box to enable the scheduled event rule.
    - **Recurrence** - Interval at which to schedule the rule.
    - **Scheduled Time Interval (Hours)** – Hours, at which to schedule the rule (use the 24 hour format).
4. Click **Schedule**.

Modify the reported severity of events that occur on NetScaler instances

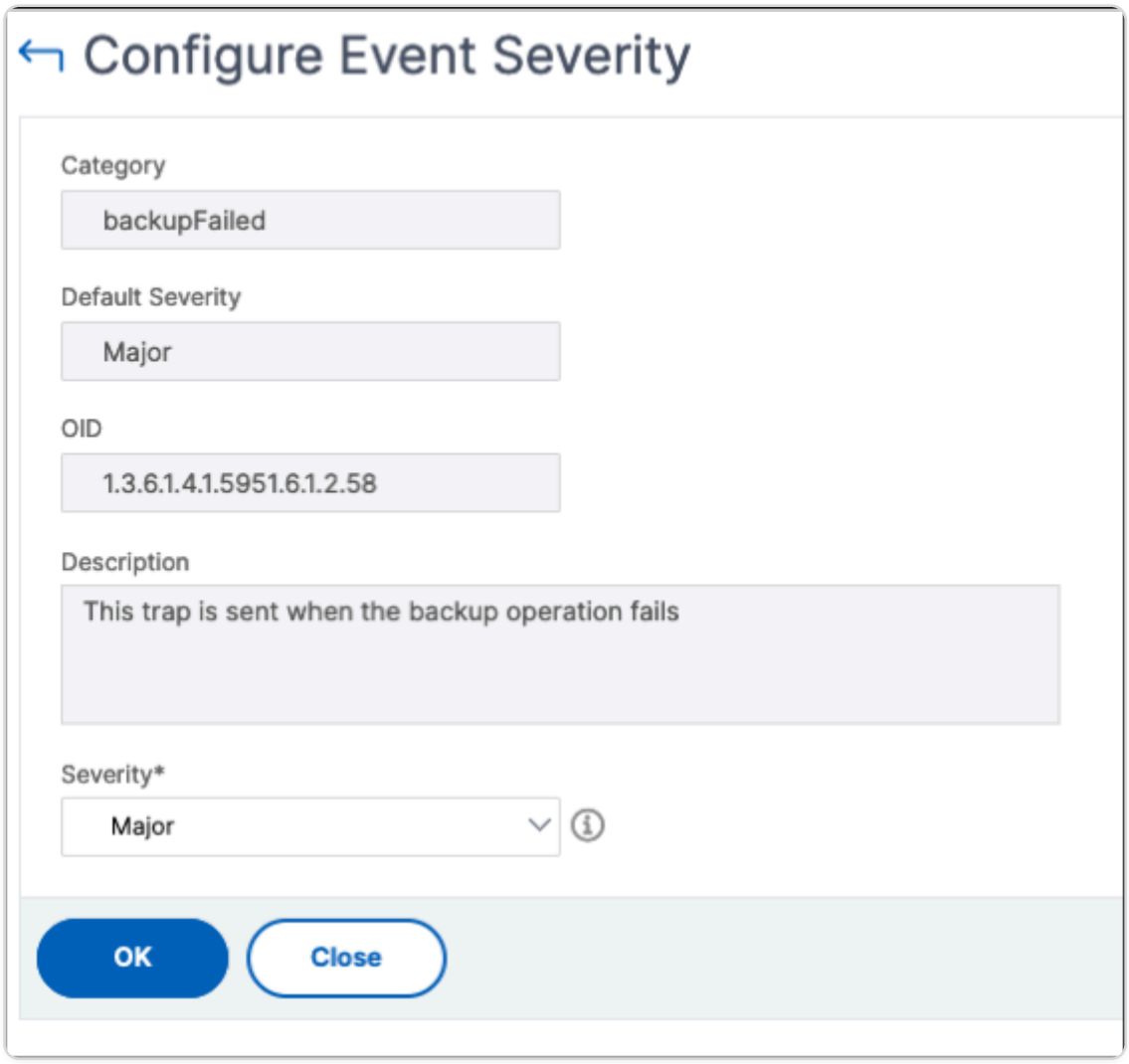
You can manage the reporting of events generated on all your devices, so that you can view event details regarding a particular event on an instance and view reports based on event severity. Also, you can create event rules that use the default severity settings, and you can change the severity settings. You can configure severity for both generic and enterprise-specific events.

You can define the following levels of severity: Critical, Major, Minor, Warning, and Clear.

To modify event severity:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigate to **Infrastructure > Events > Event Settings**.
2. Click the tab for the NetScaler instance type that you want to modify. Then, select the category from the list and click **Configure Severity**.
3. In **Configure Event Severity**, select the severity level from the drop-down list.
4. Click **OK**.



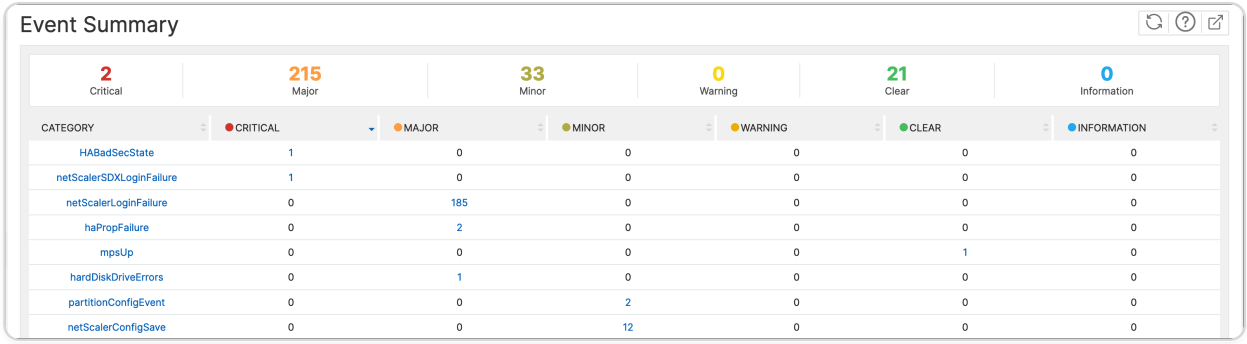
View events summary

You can now view an Events Summary page to monitor the events and traps received on your NetScaler Console. Navigate to **Infrastructure > Events**. The Events Summary page displays the following information in a tabular format:

- **Summary of all the events received by NetScaler Console**. The events are listed by category, and the different severities are displayed in different columns: Critical, Major, Minor, Warning, Clear, and Information. For example, a Critical event would occur when a Citrix Application Delivery Controller (NetScaler) instance goes down and stops sending information

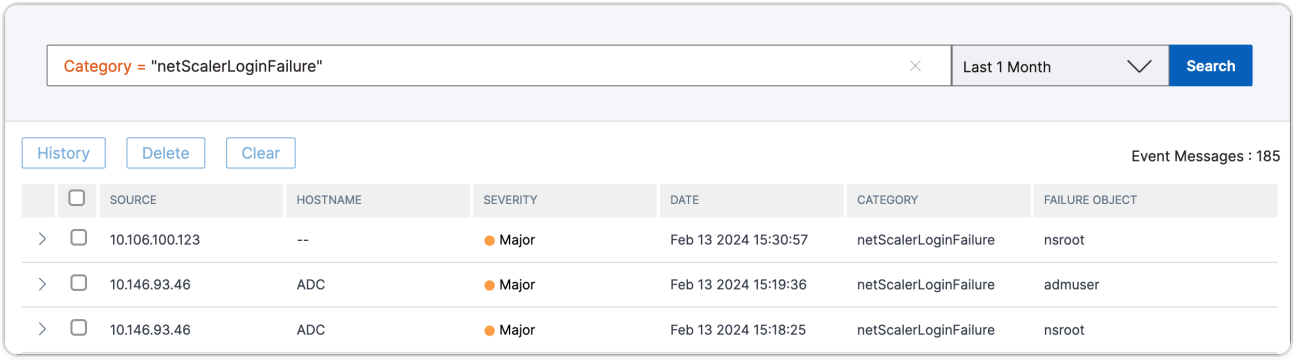
© 1997–2026 Citrix Systems, Inc. All rights reserved.

to the NetScaler Console. During the event, a notification is sent to an administrator, explaining the reason for why the instance is down, the time for which it had been down, and so on. The event is then recorded on the Events Summary page, on which you can view the summary and access the details of the event.



- **Number of traps received for each category**. The number of traps received, categorized by severity. By default, each trap sent from NetScaler instances to NetScaler Console has an assigned severity, but as the network administrator, you can specify its severity in the NetScaler Console GUI.

If you click a category type or a trap, you are taken to the **Events** page, on which filters such as the Category and Severity are preselected. This page displays more information about the event, such as the IP address and host name of a NetScaler instance, date on which the trap was received, category, failure objects, configuration command run, and the message notification.



You can configure the number of days between 1 and 40, for which you want to view the events in NetScaler Console. For example, if you select 30 days, NetScaler Console displays the events for 30 days and after 30 days, the events are cleared. To configure this event setting, navigate to **Settings > Global Settings > Data Rentention Policy**. For more information, see Data retention policy.

To export the report of this dashboard:

To export the report of this page, click the **Export** icon on the top right side of this page. On the **Export** page, you can do one of the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Select **Export Now** tab. To view and save the report in PDF, JPEG, PNG, or CSV format.
2. Select **Schedule Export** tab. To schedule the report daily, weekly, or monthly and send the report over an email or a slack message.

NOTE:

- If you select **Weekly** recurrence, ensure that you select the weekdays on which you want the report to be scheduled.
- If you select **Monthly** recurrence, ensure that you enter all the days that you want the report to be scheduled separated by commas.

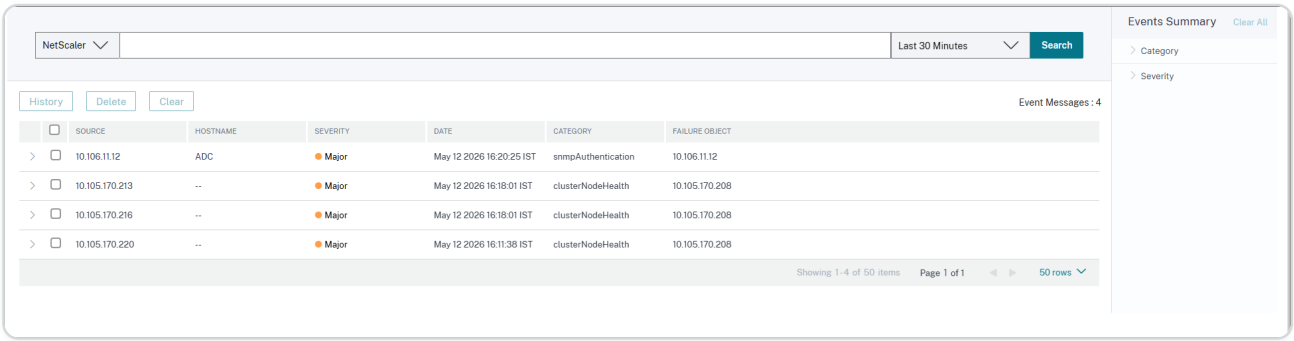
Event messages

All active events received in NetScaler® Console are displayed in the **Infrastructure > Events > Event Messages** page.

On the **Event Messages** page, you can view the list of instances and the details of the events, such as severity, category, date when the event occurred, and the failure object.

You can filter the events based on the time when it occurred, such as, in the last 30 minutes, 1 hour, 1 day. You can also select a custom time based on your preference.

NetScaler Console supports custom SNMP traps, which are tagged as **custom** under **Event Messages**. The **custom** tag helps you distinguish them from the default SNMP alerts.



Display event severities and SNMP trap details

When you create an event and its settings in NetScaler Console, you can view the event immediately on the Event Summary page. Similarly, you can view and monitor the health, up time, models, and the versions of all Citrix Application Delivery Controller (NetScaler) instances added to your NetScaler Console server in minute detail on the Infrastructure Dashboard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

On the Infrastructure dashboard, you can now mask irrelevant values so that you can more easily view and monitor information such as event by severities, health, up time, models, and version of NetScaler instances in minute detail.

For example, events with a **Critical** severity level might occur rarely. However, when these critical events do occur on your network, you might want to further investigate, troubleshoot, and monitor where and when the event occurred. If you select all severity levels except Critical, the graph displays only the occurrences of critical events. Also, by clicking the graph, you are taken to the **Severity based events** page, where you can see all the details regarding when a critical event occurred for the duration that you've selected: the instance source, the date, category, and message notification sent when the critical event occurred.

Similarly, you can view the health of a NetScaler VPX instance on the dashboard. You can mask the time during which the instance was up and running, and display only the times the instance was out of service. By clicking the graph, you are taken to that instance's page, where the *out of service* filter is already applied, and see details such as host name, the number of HTTP requests it received per second, CPU usage, and others. You can also select the instance and see the instance dashboard for more details.

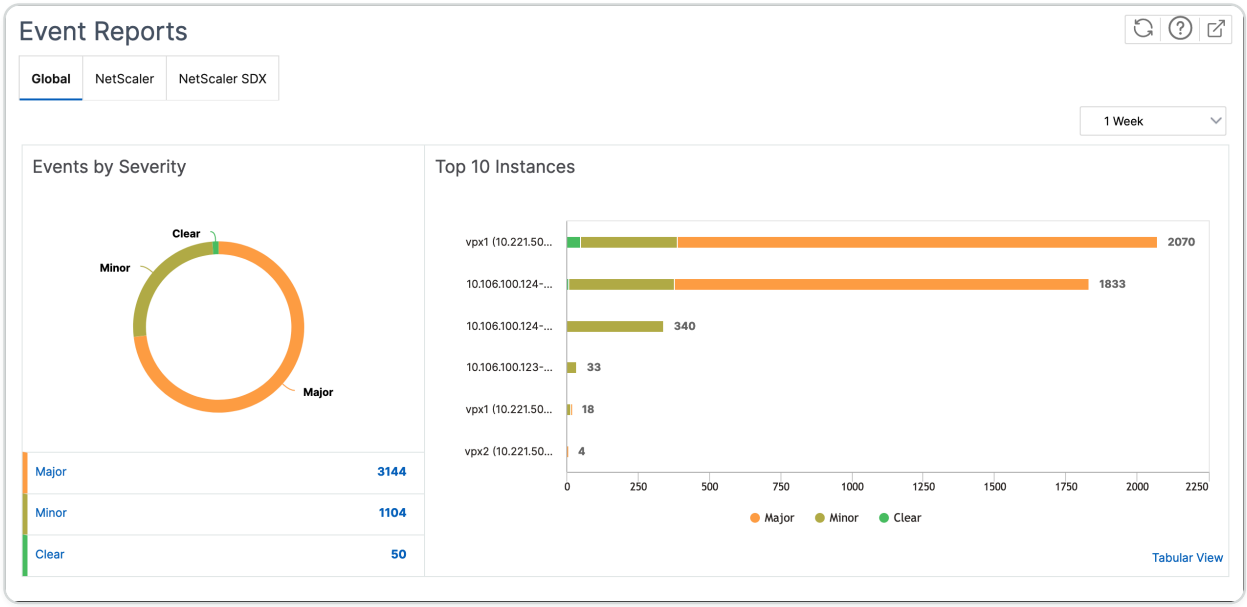
To select specific events by severity in NetScaler Console:

1. Log on to NetScaler Console, using your administrator credentials.
2. Navigate to **Infrastructure > Instances**.

   Or,

   Navigate to **Infrastructure > Events > Reports**.
3. From the drop-down list in the upper-right corner of the page, select the duration for which you want to see events by severity.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

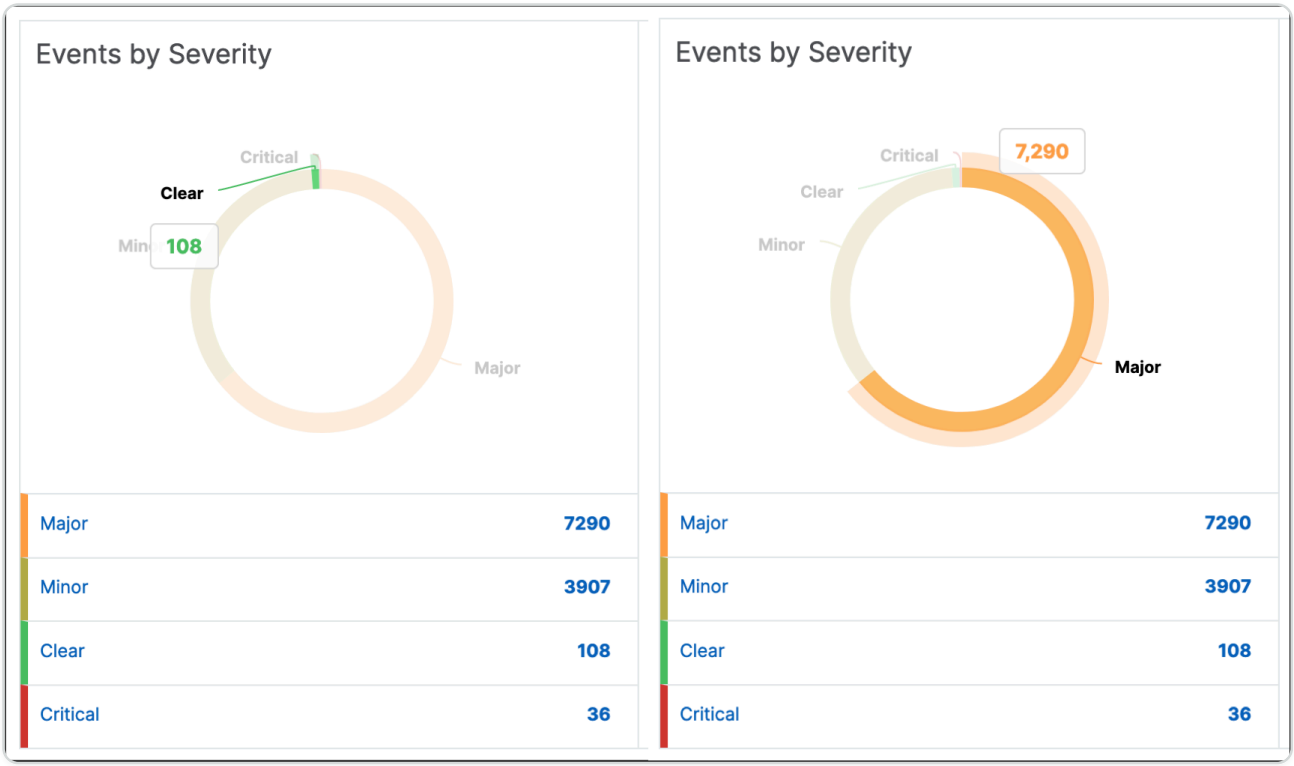


4. The **Events by Severity** donut chart displays a visual representation of all the events by their severity. Different types of events are represented as different colored sections, and the length of each section corresponds to the total number of events of that type of severity.
5. You can click each section on the donut chart to display the corresponding **Severity based events** page, which shows the following details for the selected severity for the selected duration:
    - Instance Source
    - Data of the event
    - Category of events generated by the NetScaler instance
    - Message notification sent

NOTE:

Below the donut chart, you can see a list of severities that are represented in the chart. By default, a donut chart displays all events of all severity types, and therefore all severity types in the list are highlighted. Hover over severity types to view and monitor your chosen severity more easily.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

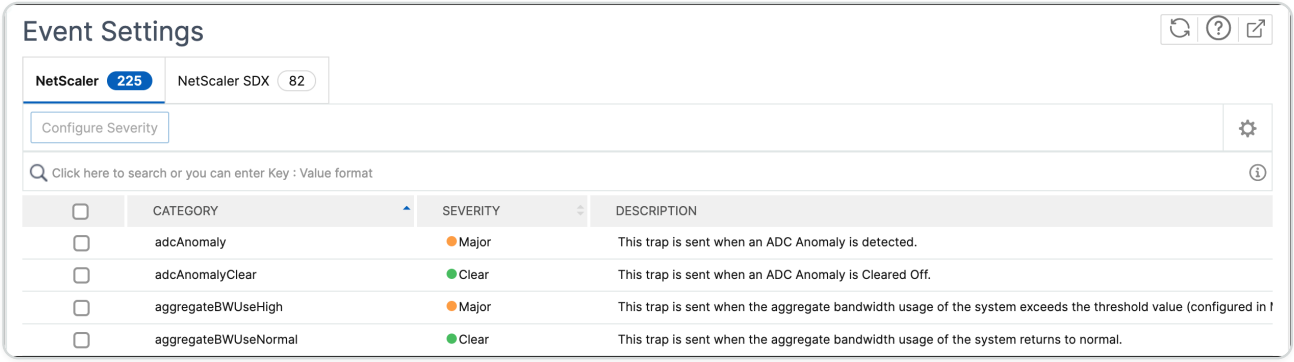


To view NetScaler SNMP trap details on NetScaler Console:

You can now view the details of each SNMP trap received from its managed NetScaler instances on the NetScaler Console on the **Event Settings** page. Navigate to **Infrastructure > Events > Event Settings**. For a specific trap received from your instance, you can view the following details in tabular format:

- **Category** - Specifies the category of the instance to which the event belongs.
- **Severity** - The severity of the event is indicated by colors and its severity type.
- **Description** - Specifies the messages associated with the event.

For example, an event with the trap category **aggregateBWUseNormal**, the description of the trap is displayed as
"This trap is sent when the aggregate bandwidth usage of the system returns to normal."



© 1997–2026 Citrix Systems, Inc. All rights reserved.

View and Export syslog messages

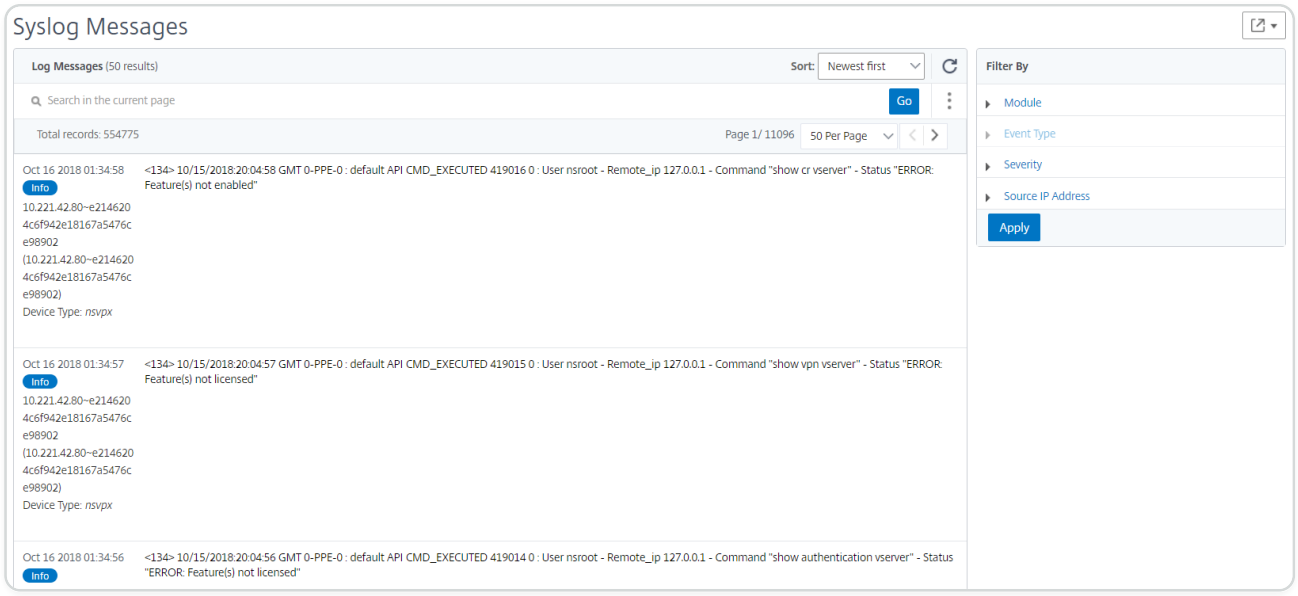
You can view syslog messages without logging into NetScaler Console, by scheduling an export of all syslog messages received on the server. You can export syslog messages that are generated on your Citrix Application Delivery Controller (NetScaler) instances in PDF, CSV, PNG, and JPEG formats. Also, you can schedule the export of these reports to specified email addresses at various intervals.

View syslog messages

You can view all your syslog messages generated on your managed NetScaler instances. To view the messages you must configure the instances to redirect the syslog messages to the NetScaler Console server. The syslog messages are stored in the database centrally and are available on the Syslog Viewer for auditing purposes. You can combine this logging information and derive reports for analytics from the collected data.

You can also configure syslog to log different types of events.

To view the Syslog Viewer, navigate to **Infrastructure > Events > Syslog Messages**. Choose the appropriate filters, to view your System Log messages.

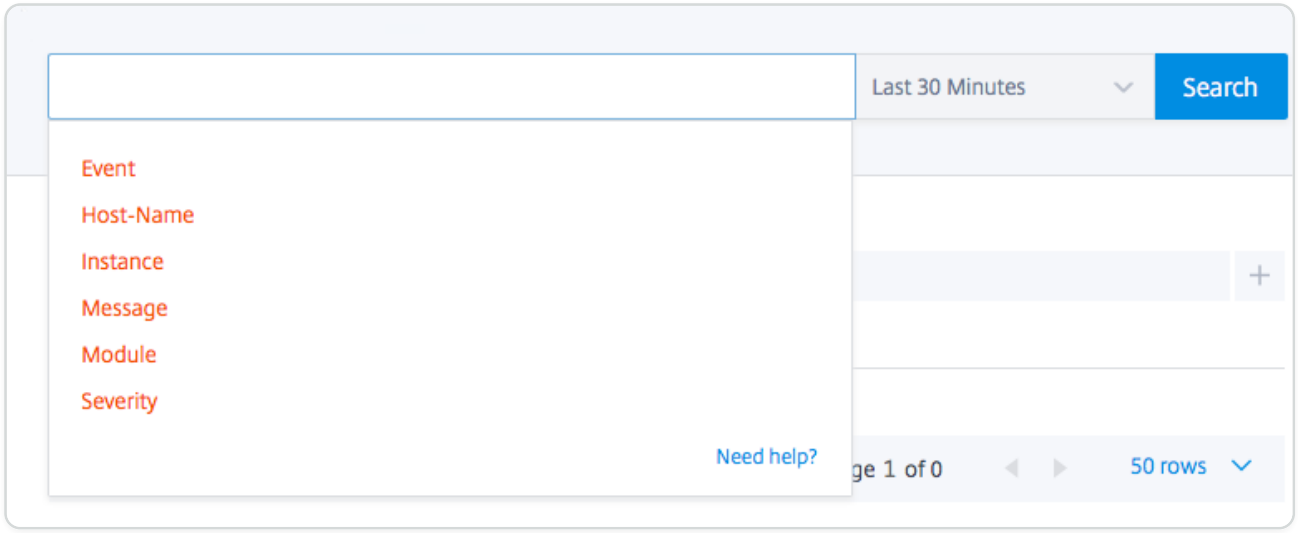


Search syslog messages

You can use filters to search syslog messages and audit log messages to narrow down your results and find exactly what you are looking for and in real time.

To search syslog messages for all NetScaler instances present in the NetScaler Console software, from the NetScaler Console GUI, navigate to **Infrastructure > Events > Syslog Messages**. The new filter categories are instance, module, event, severity, and message.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



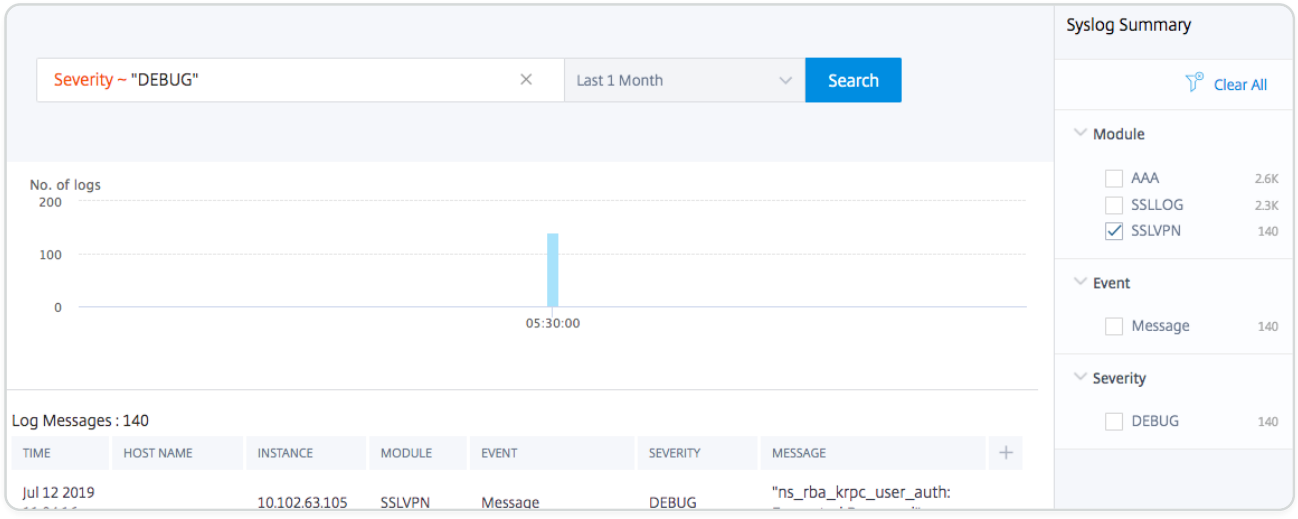
To search all NetScaler Console system audit log messages present in the NetScaler Console software, from the NetScaler Console GUI, navigate to **Settings > Audit Log Messages**. The new filter categories are instance, module, event, severity, and message.

To search audit log messages for all applications present in the NetScaler Console, from the NetScaler Console GUI, navigate to **Infrastructure > Network Functions > Auditing**.

To search the audit log messages for a specific application on the NetScaler Console, from the NetScaler Console GUI, navigate to **Application > Dashboard** and select the virtual server for which you want search the audit log messages. Next, click the **Audit Log** tab.

After you select a filter category, specify if it equals to or contains the search term.

Next, add the search term. For some categories, a prepopulated list of search terms is displayed. By default, the search time is 1 day. You can change the time and date range by clicking the down arrow. You can further narrow down your search by selecting options from the **Syslog Summary** or **Audit Log Summary** pane.

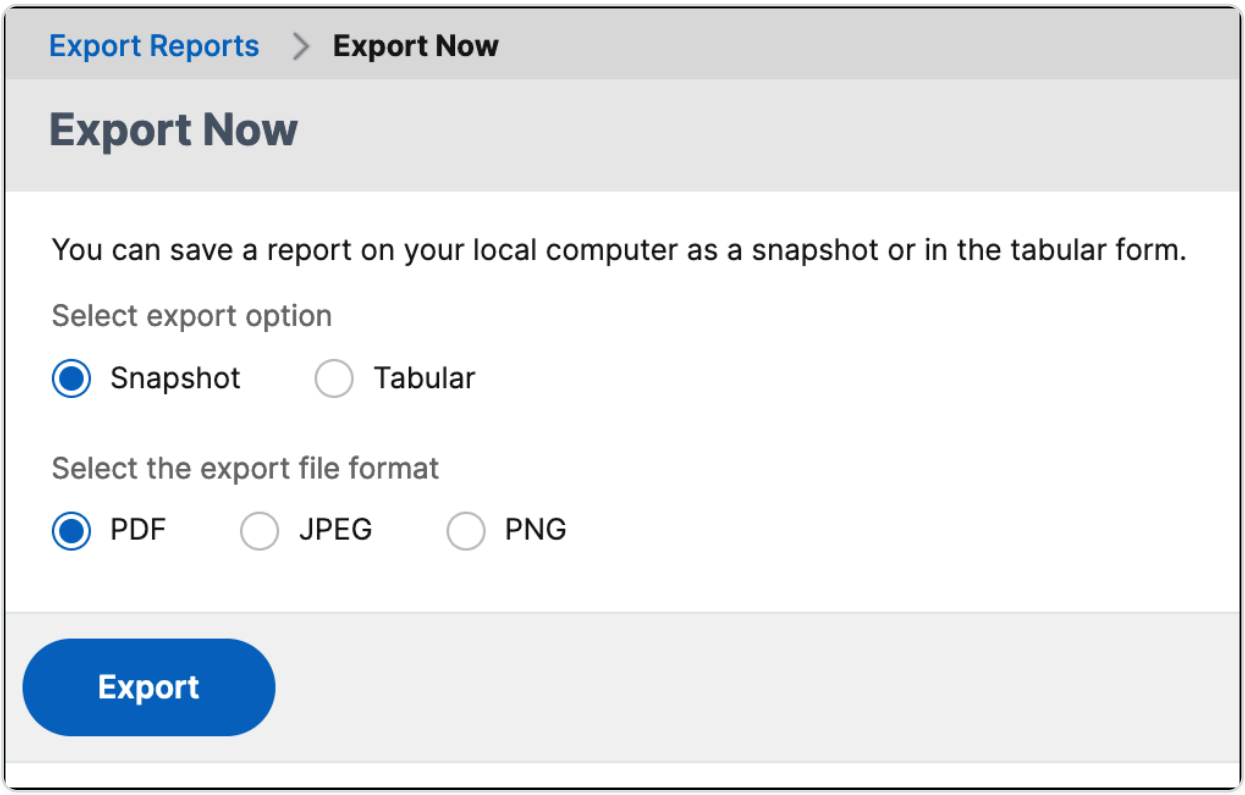


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Export syslog messages

To export a syslog messages report by using NetScaler Console:

1. Navigate to **Infrastructure > Events > Syslog Messages**.
2. In the right pane, click the export button at the top right corner of the Syslog Messages page.
3. Under **Export Now**, select the required format, and then click **Export**.



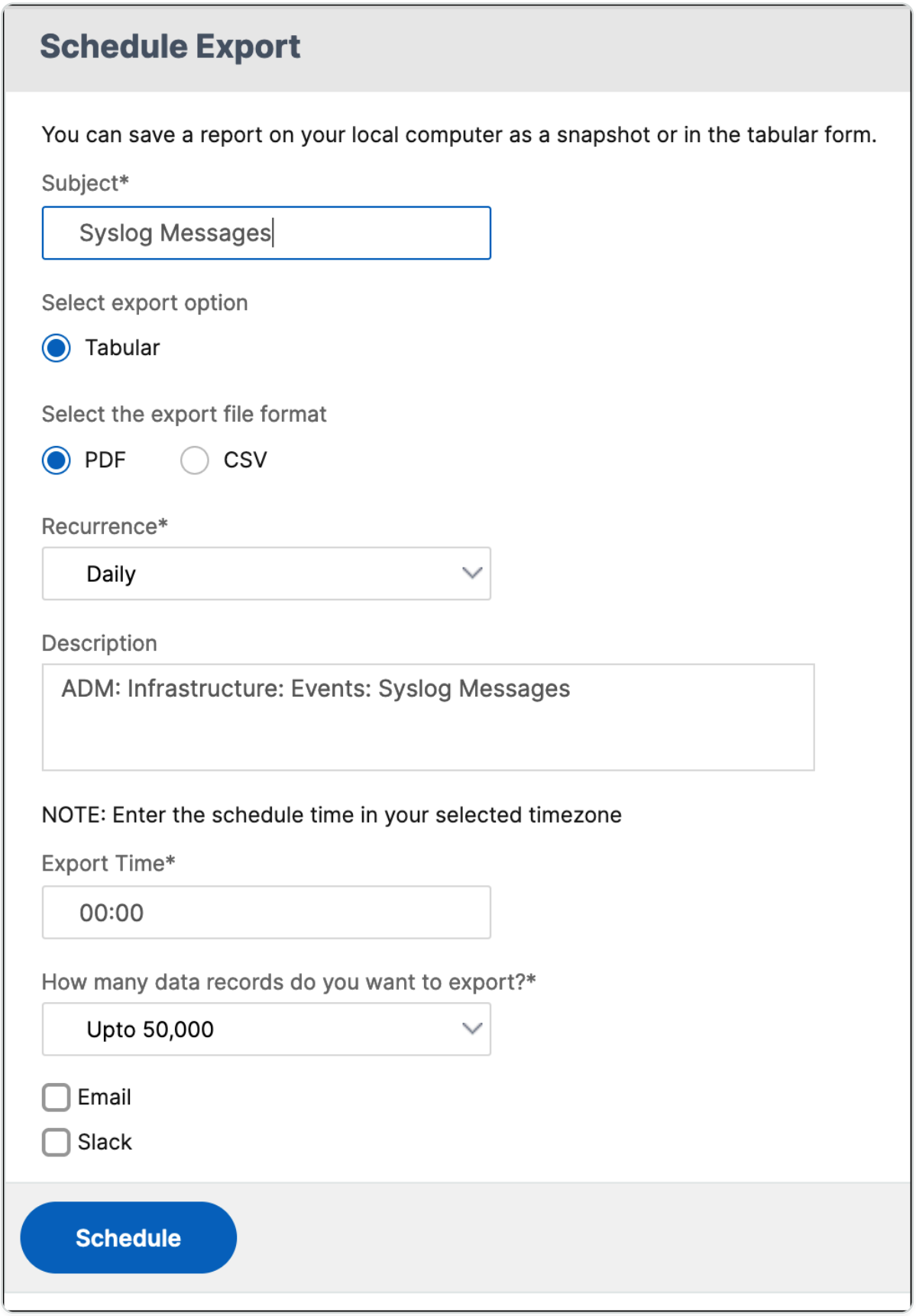
To schedule the export of syslog messages report by using NetScaler Console:

1. Navigate to **Infrastructure > Events > Syslog Messages**.
2. On the **Syslog Messages** page, in the right pane, click **Export**.
3. Under the **Schedule Report** tab, set the following parameters:

   - **Description**: Message describing the reason for exporting the report.
   - **Format**: Format in which to export the report.
   - **Recurrence**: Interval at which to export the report.
   - **Export Time**: Time at which to export the report. Enter the time in a 24 hour format, for your local time zone.
   - **Email Distribution List**: List of recipients to receive the report by email. Choose an email distribution list from the list provided. An email is triggered when the report is generated and

© 1997–2026 Citrix Systems, Inc. All rights reserved.

meets the scheduled time criteria. If you want to create an email distribution list, click **+** and provide mail server and mail profile details.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Suppress syslog messages

When configured as a syslog server, NetScaler Console receives all syslog messages from the configured Citrix Application Delivery Controller (NetScaler) instances. There might be many messages that you might not want to see. For example, you might not be interested in seeing all the informational-level messages. You can now discard some of the syslog messages that you are not interested in. You can suppress some of the syslog messages coming into NetScaler Console by setting up some filters. NetScaler Console drops all messages that match with the criteria. These dropped messages do not appear on the NetScaler Console GUI and these messages are also not stored in the customer's NetScaler Console database.

You can suppress some of the logged syslog messages coming into NetScaler Console by setting up some filters. The two filters that can be used for suppressing syslog messages are severity and facility. You can also suppress messages coming from a particular NetScaler instance or multiple instances. You can also provide a text pattern for NetScaler Console to search and suppress messages. NetScaler Console drops all messages that match with the criteria. These dropped messages do not appear on the NetScaler Console GUI and these messages are also not stored in the customer database. Therefore, a good amount of space is saved on the storage server.

Some use cases for suppressing syslog messages are as follows:

- If you want to ignore all information level messages, suppress level 6 (informational)
- If you only want to record firewall error conditions, suppress all levels other than level 3 (errors)

Suppressing syslog messages by creating filters

1. In NetScaler Console, navigate to **Infrastructure > Events > Syslog Messages**.
2. Click the gear icon to display the **Suppress Filters** page.



3. In the **Suppress Filters** page, click **Add**.
4. In **Create Suppress Filter**, update the following information:

    a. **Name** - type a name for the filter.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

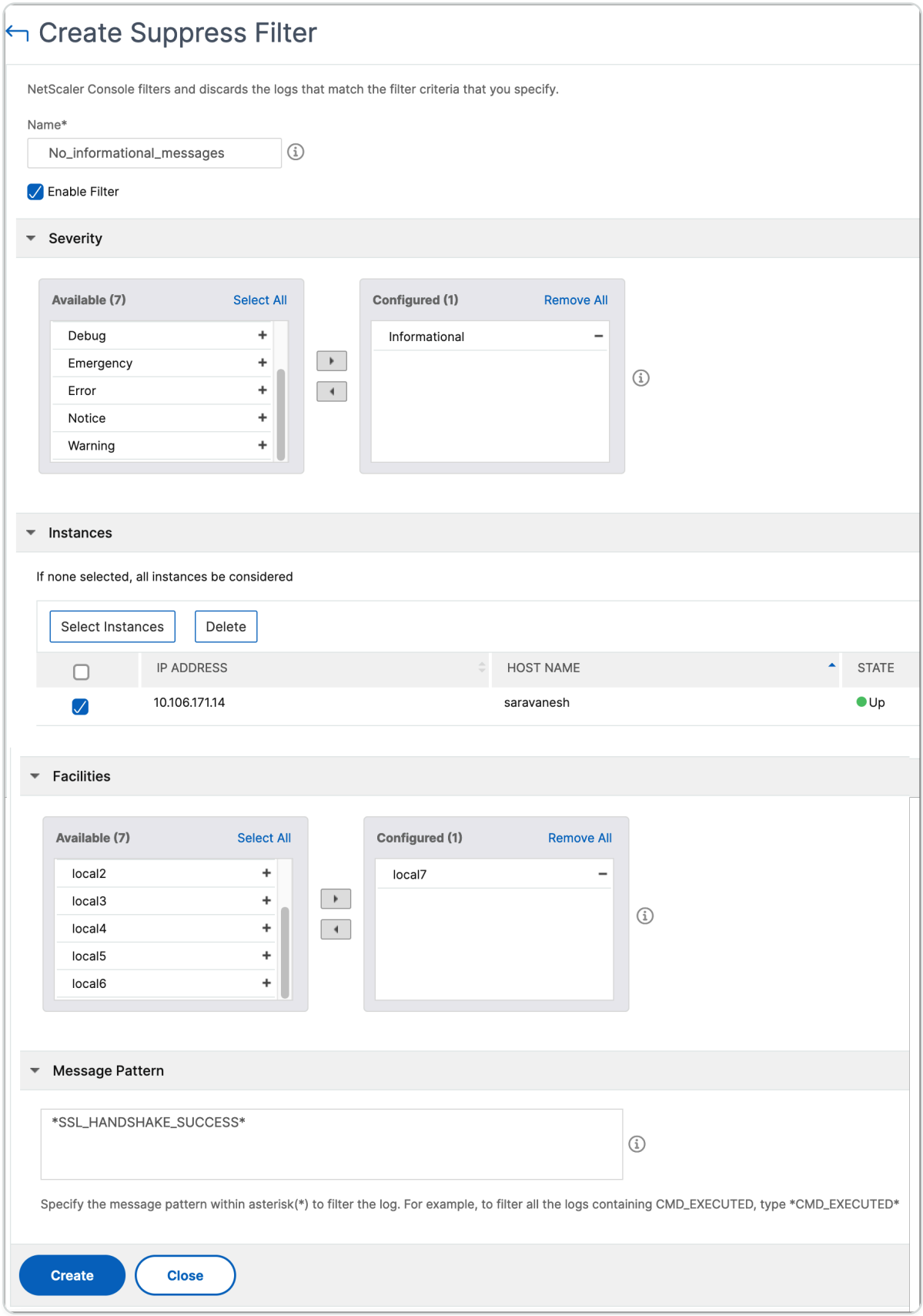
If different users have different access to multiple NetScaler instances, different filters must be created for different instances as users can see only those filters in which they have access to all the instances.

b. **Severity** - Select and add the log levels for which you must suppress the messages.

   For example, if you do not want to view any informational messages coming in, you can select **Informational** to suppress those messages.

c. **Instances** - Select the NetScaler instances on which the syslog messages have been configured.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



d. **Facilities** - Select the facility to suppress messages based on the source that generates them.

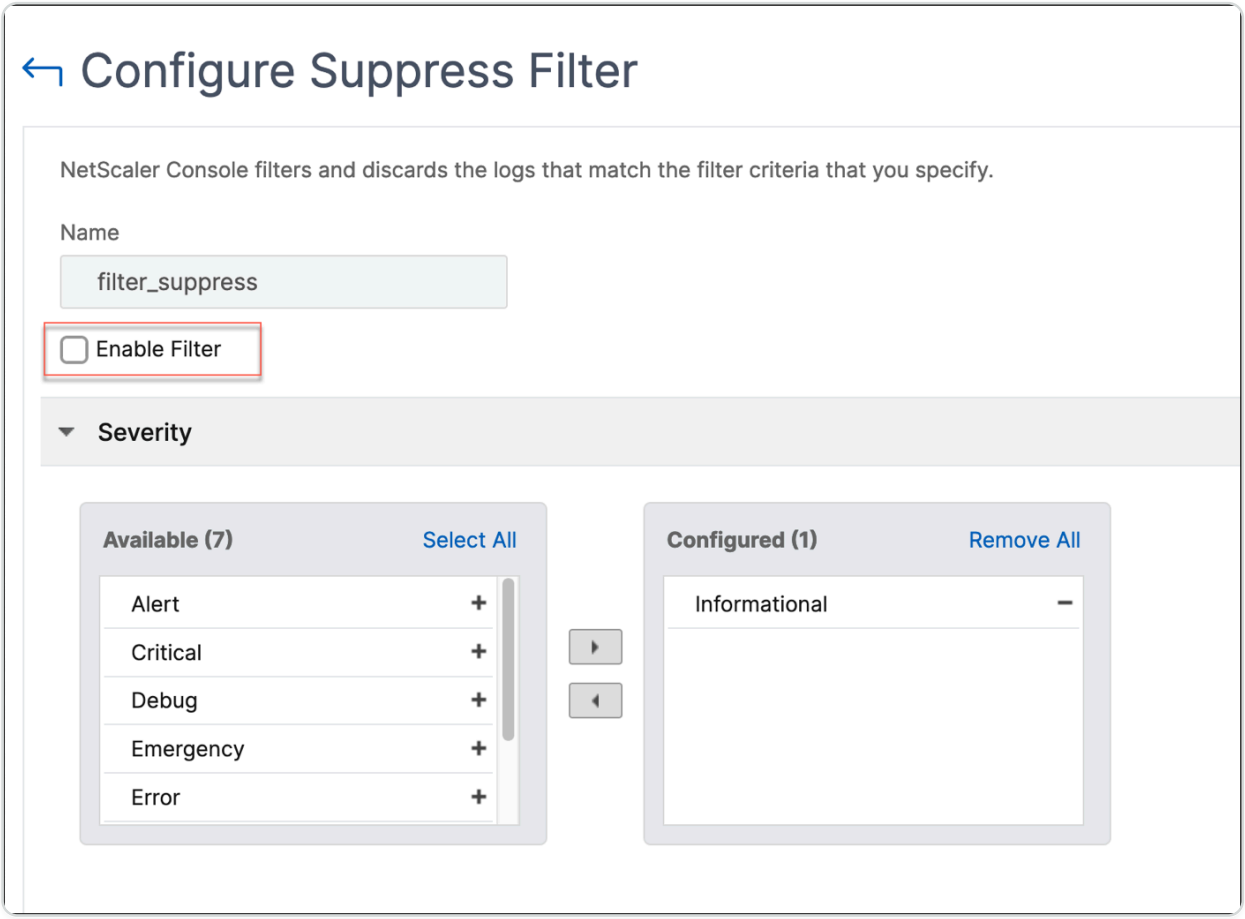
© 1997–2026 Citrix Systems, Inc. All rights reserved.

e. **Message Pattern** - You can also type a text pattern surrounded by asterisks (*) to suppress the messages. The messages are searched for the text pattern string and those messages that contain this pattern are suppressed.

Disabling the filter

To allow the messages to be viewed on NetScaler Console, you must disable the filter.

1. Navigate to **Infrastructure > Events > Syslog Messages**.
2. Click the gear icon to display the **Suppress Filters** page.
3. In the **Suppress Filters** page, select the filter and click **Edit**.
4. On the **Configure Suppress Filter** page, clear the **Enable Filter** check box to disable the filter.



SSL dashboard

NetScaler Console now streamlines every aspect of certificate management for you. Through a single console, you can establish automated policies to ensure the right issuer, key strength, and correct algorithms, while keeping close tabs on certificates that are unused or soon to expire. To

© 1997–2026 Citrix Systems, Inc. All rights reserved.

begin using NetScaler Console's SSL dashboard and its functionalities, you must understand what an SSL certificate is and how you can use NetScaler Console to track your SSL certificates.

A Secure Socket Layer (SSL) certificate, which is a part of any SSL transaction, is a digital data form (X509) that identifies a company (domain) or an individual. The certificate has a public key component that is visible to any client that wants to initiate a secure transaction with the server. The corresponding private key, which resides securely on the NetScaler appliance, is used to complete asymmetric key (or public key) encryption and decryption.

You can obtain an SSL certificate and key in either of the following ways:

- From an authorized certificate authority (CA)
- By generating a new SSL certificate and key on the NetScaler appliance

NetScaler Console provides a centralized view of SSL certificates installed across all managed NetScaler instances. On the SSL Dashboard, you can view graphs that help you track certificate issuers, key strengths, signature algorithms, expired or unused certificates and so on. You can also see the distribution of SSL protocols that are running on your virtual servers and the keys that are enabled on them.

You can also set up notifications to inform you when certificates are about to expire and include information about which NetScaler instances use those certificates.

You can link a NetScaler instance certificate to a CA certificate. However, make sure the certificates you link to the same CA certificate have the same source and the same issuer. After you have linked one or more certificates to a CA certificate, you can unlink them.

NOTE:

You can also use a Venafi Trust Protection Platform server with NetScaler Console to automate the management of the entire lifecycle of SSL certificates. For more information, see Automate SSL certificate management.

Automated certificate renewal by using the ACME protocol

NetScaler Console supports the Automated Certificate Management Environment (ACME), an open protocol designed to automate the renewal of SSL/TLS certificates.

Previously, the network administrators had to undergo the labor-intensive, multi-stage manual process of renewing the certificates. ACME support mitigates these challenges by providing a robust framework for automated certificate renewal to perform the following actions:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Request new certificates from trusted Certificate Authorities (CAs).
- Validate domain ownership using automated methods (Currently, NetScaler Console supports only the DNS-01 challenge).
- Renew certificates automatically before expiry.

ACME support in NetScaler® Console

NetScaler Console uses the `acme.sh` client and supports the following Certificate Authorities:

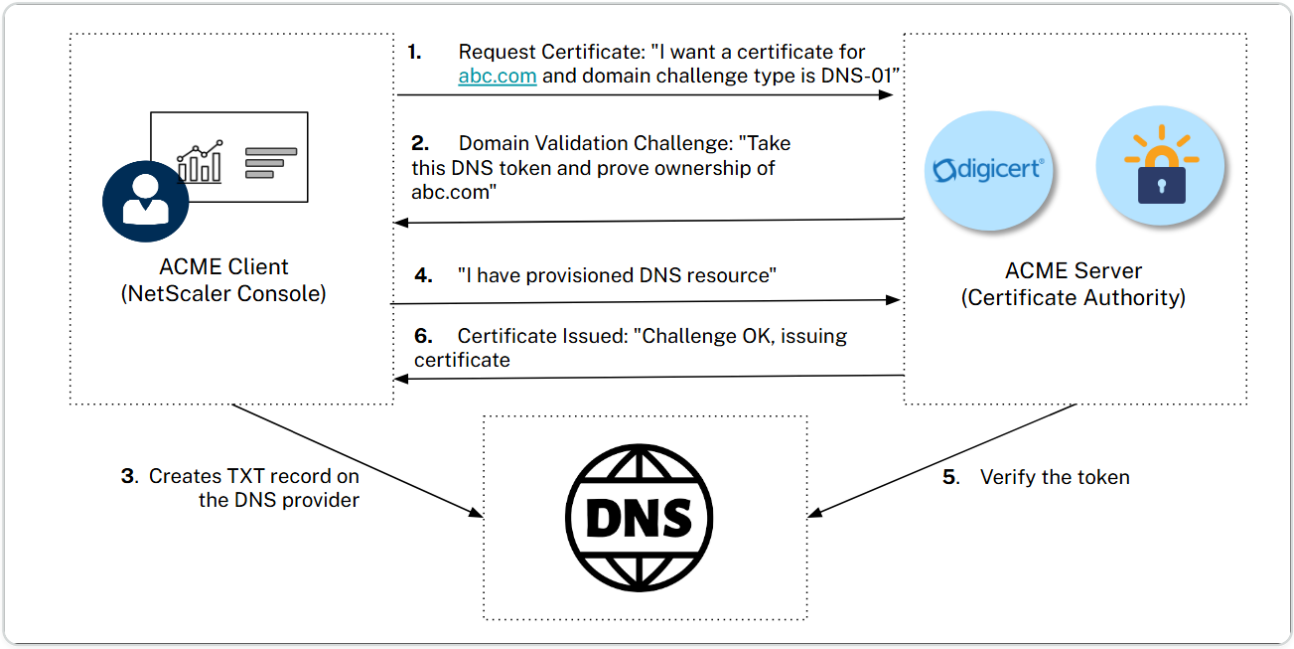
- Let’s Encrypt
- DigiCert Inc
- Sectigo Limited
- Entrust, Inc
- GlobalSign
- GoDaddy.com, Inc
- ZeroSSL
- Google Trust Services
- Google Public CA
- BuyPass Go SSL
- Actalis
- SSL.com
- HashiCorp Vault
- Smallstep
- Pebble
- HARICA
- EJBCA

The following steps explain how automated certificate renewal happens in NetScaler Console:

1. When NetScaler Console initiates a certificate request for a domain using the `acme.sh` client, the client connects to the chosen Certificate Authority (for example, Let's Encrypt or DigiCert).
2. The CA issues a challenge to prove domain ownership, which in this case is a DNS-01 challenge.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. NetScaler Console using pre-configured credentials, automatically updates the DNS TXT record for the domain with the value provided by the CA.
4. The CA validates the TXT record, confirming domain ownership.
5. Upon successful validation, the CA issues the SSL/TLS certificate to NetScaler Console.
6. NetScaler Console stores the certificate in the respective store (Certificate store/Zero-touch store).
7. Based on the renewal window provided by you, NetScaler Console automatically repeats this process for renewal before the certificate's expiration date.



With ACME support in NetScaler Console, you can perform the following actions:

- Automatically renew certificates before they expire
- Switch from one CA to another during renewal
- Generate or upload CSR and request for new certificate

The following are the key benefits:

- Fully Automated Lifecycle with no manual intervention for certificate issuance or renewal.
- Customizable Renewal Schedule that suits organizational needs (for example, set to renew 7 days before expiry).
- Eliminates downtime due to expired certificates.
- Reduced operational overhead by automating expiry tracking and renewals.
- Improved security posture with always-valid, CA best-practice aligned certificates.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration steps for ACME integration

Integrating ACME is a one-time process and includes the following steps:

- Step 1: Configure Certificate Authority (CA).
- Step 2: Select certificates for renewal.
- Step 3: Add a DNS provider and map the respective domains.

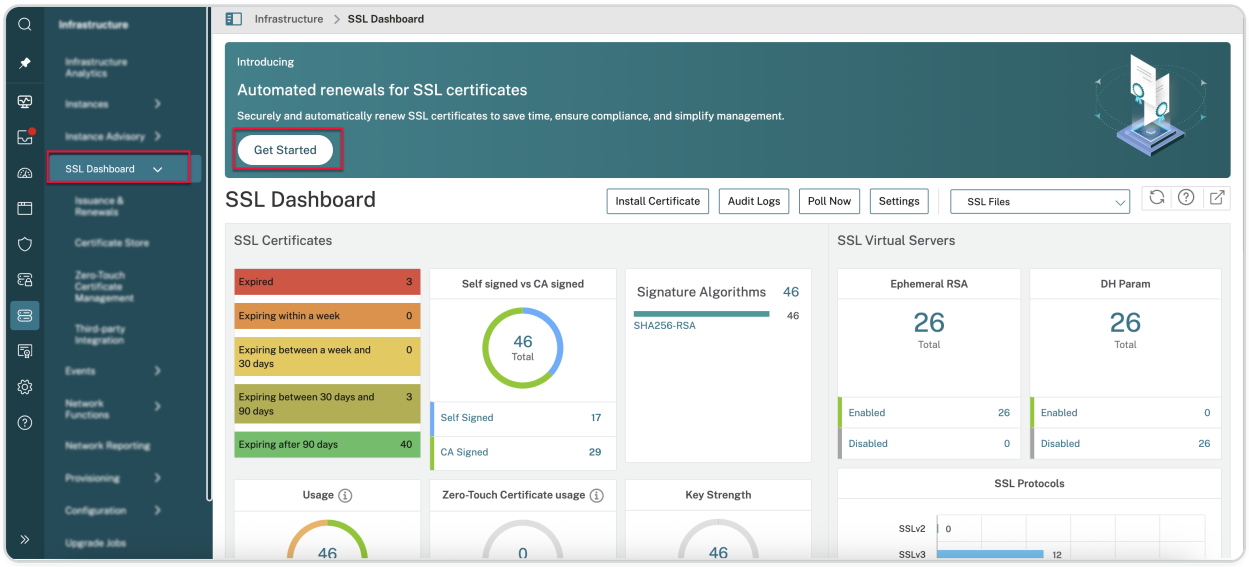
Prerequisites

- Ensure that you must have a valid account for your Certificate Authority (CA) and license for the same.
- Ensure that you have DNS provider access credentials.

Step 1: Configure Certificate Authority (CA)

Perform the following steps to register the Certificate Authority (CA) that is used for renewals:

1. Navigate to **Infrastructure > SSL Dashboard**. If you are configuring ACME for the first time, then you see a banner with "Automated renewals for SSL certificates". Click **Get Started**.



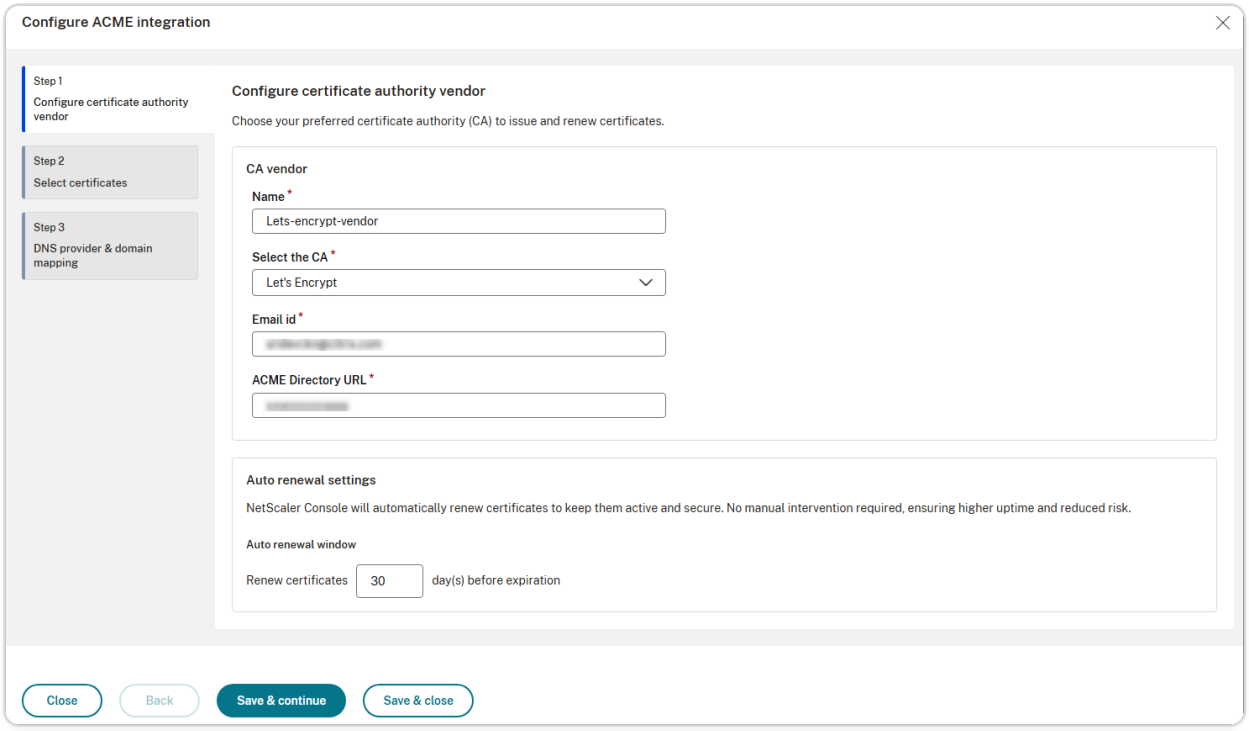
or

Navigate to **Infrastructure > SSL Dashboard > Third-party Integration > CA Vendors** and click **Add**.

2. Enter a name and select the CA vendor.
3. Provide the other details such as email address, ACME Directory URL.
4. Enter the number of days before which the NetScaler Console must automatically renew the certificates.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Click **Save and continue**. NetScaler Console attempts to connect to the CA. If connectivity fails, review the details provided, correct the configuration details, and then retry.

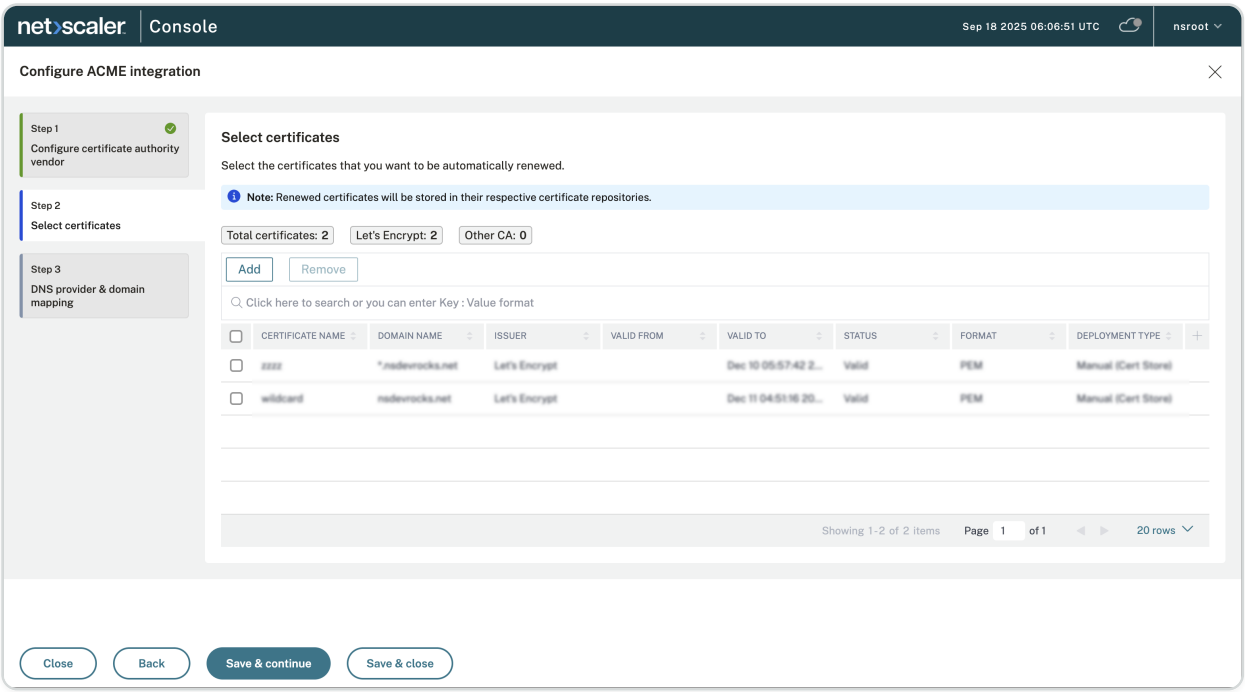


Step 2: Select certificates for renewal

After CA details are added, NetScaler Console automatically scans all certificates (from both the certificate store and the Zero-touch store) and lists the certificates issued by the configured CA separately. Review the certificates listed.

1. Select the certificates that you want to automatically renew. For example, If you configure Let's Encrypt as the CA and have 2 certificates from Let's Encrypt and 2 from another vendor, the dashboard displays: `Let's Encrypt: 2 and Other CA: 2`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

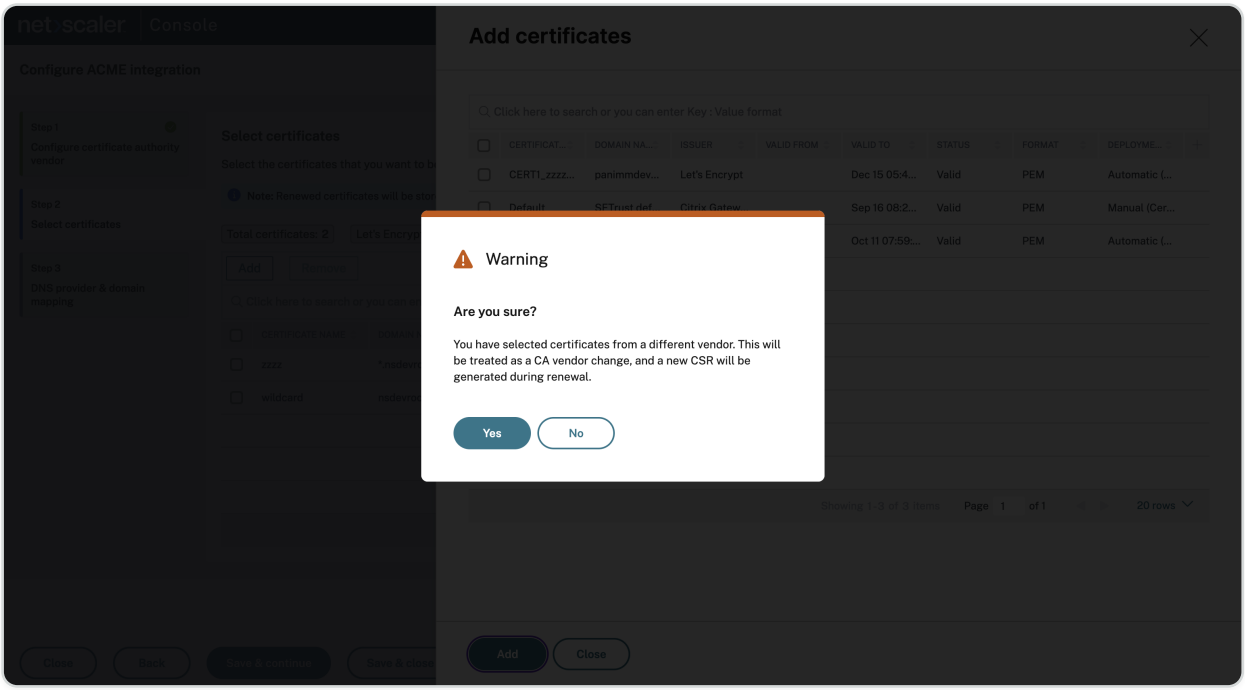


2. You can click **Add** to also add certificates issued by a different CA or **Remove** to remove certificates that you do not want to renew automatically. If you select certificates from a different vendor, you get a prompt to confirm the vendor change. Once you confirm, these certificates get renewed through the newly configured CA when their renewal window is reached.

NOTE:

Ensure that you do not have duplicate certificates in the Certificate store and Zero-touch certificate store. If there are duplicate certificates, then the renewal process happens twice for each store.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Click **Save and continue**.

NOTE:

Certificates remain in their respective stores after renewal. For example, if a certificate is stored in the certificate store, its renewed version is also placed in the certificate store. If the certificate is stored in the Zero-touch store, its renewed version is also placed in the Zero-touch store.

Certificate deployment behavior depends on the store type.

- If the certificates are stored in the certificate store, they must be manually deployed to NetScaler.
- If the certificates are stored in the Zero-touch store, the certificates are automatically deployed to NetScaler without admin intervention. We recommend you to use Zero-touch Certificate Management for seamless, fully automated deployment of renewed certificates. For more information, see Zero-touch certificate management.

Step 3: Add a DNS provider and map the domains

1. Click **Add** on the **DNS provider & domain mapping** page.
2. Select the DNS providers from the **Select DNS provider** drop-down list. The DNS providers supported by the `acme.sh` are listed in the drop-down list. If you do not see your DNS provider in the list that means it is not supported.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Enter provider details such as Access key ID, Secret Access Key and click **Save** to save the configuration.
4. Click **Add Domain** under **Domain Mapping**.
5. Select the domains served by the configured DNS provider.

IMPORTANT:

Ensure that each domain is linked to the correct DNS provider. NetScaler Console uses these mappings to perform the DNS-01 challenge automatically. During issuance or renewal, NetScaler Console creates the required TXT records in the mapped DNS provider. Once validation succeeds, the CA issues or renews the certificate. Certificates are renewed only when all associated domains are mapped correctly to their DNS providers.

For example, if your organization uses Amazon Route53 as the DNS provider. First, add the Amazon Route53 credentials (Access Key ID and Secret Key) under DNS Provider Details. Then, map the domains managed by Amazon Route53 (for example: example.com, app.example.com). When a certificate for these domains is issued or renewed, NetScaler Console automatically creates the required TXT records in Amazon Route53. Once validation is successful, the CA issues or renews the certificates.
The following public DNS providers are supported:

- 1984.hosting
- ACME DNS
- AcmeProxy Server API
- Active24
- Akamai.com Edge DNS
- Aliyun
- All-inkl Kas Server
- Alviy.com
- Amazon Route53
- Anexia.com CloudDNS
- ArtFiles.de
- ArvanCloud.ir

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- autoDNS-InternetX
- Azure DNS
- Azion.om
- Beget.com
- BookMyName.com
- Bunny.net
- CloudFlare
- ClouDNS.net
- ConoHa
- Constellix.com
- Core-Networks
- cPanel Server API
- Curanet.dk
- cyon.ch
- DDNSS.de
- deSEC.io
- DigitalOcean
- DirectAdmin
- DNS.Services
- DNSExit.com
- dns.la
- DNSMadeEasy
- DNSimple
- dnsHome.de
- DNSPod.cn
- DNSPod.com
- Domain-Offensive do.de
- DomeneShop.no
- DreamHost
- DuckDNS.org

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- durabledns.com
- Dyn.com
- DynDnsFree.de
- Dynu.com
- DynV6.com
- easyDNS.net
- edgecenter DNS API
- EUserv.com
- Exoscale
- Fornex.com
- FreeDNS
- FreeMyIP.com
- Gandi LiveDNS
- Gcore.com
- GeoScaling.com
- GoDaddy.com
- Google Cloud DNS
- Google Domains
- Hetzner.com
- Hexonet.com
- hosting.de
- HuaweiCloud.com
- Hurricane Electric
- Hurricane Electric HE.net DDNS
- Infoblox
- Infomaniak.com
- INWX
- IONOS Cloud DNS
- IONOS.de
- InternetBS.net

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ISPConfig 3.1
- jdcloud.com
- Joker.com
- kapper.net
- King.host
- Knot DNS
- Leaseweb.com
- Lexicon DNS client
- lima-city.de
- Linode
- Linode.com-Old
- Loopia
- LuaDNS
- MailinaBox
- MaraDNS
- mijn.host
- Misaka.io
- MyDNS.JP
- Mythic-Beasts.com
- Name.com
- Namecheap
- NameMaster.de
- Namesilo
- Nanelo.com
- NederHost.nl
- Neodigit.net
- Netcup
- Netlify.com
- nic.ru
- Njalla

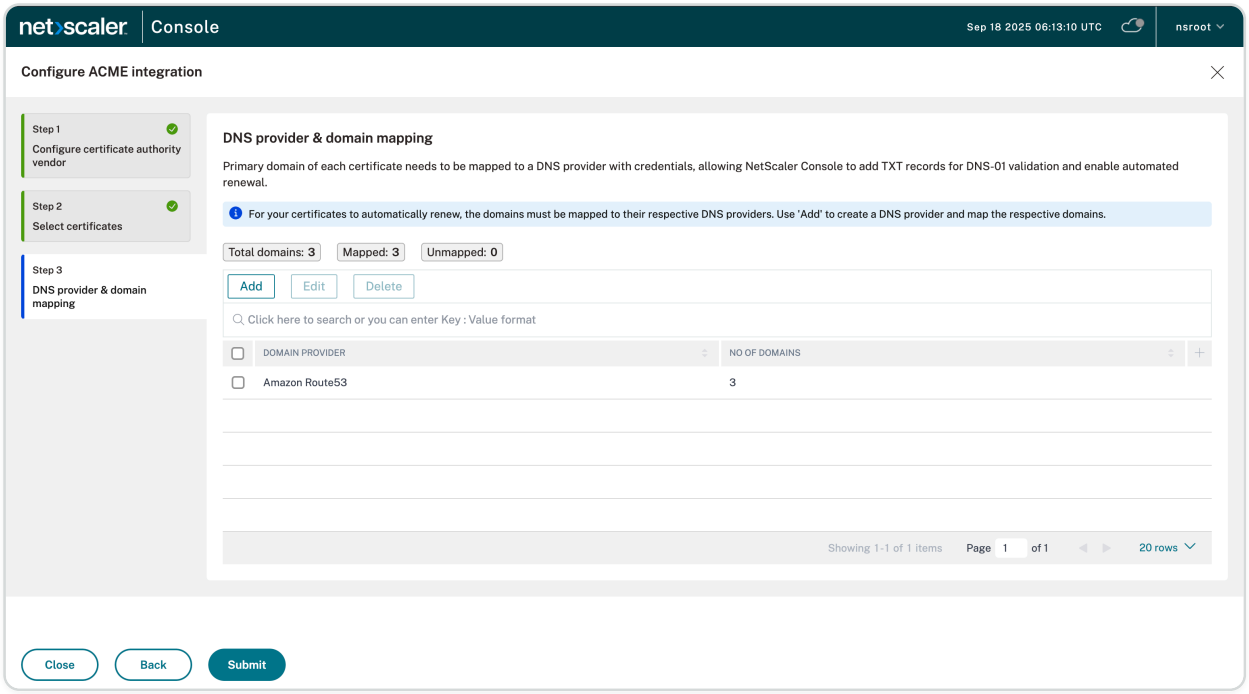
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NLnetLabs NSD
- NS1.com
- Nexcess
- one.com
- Online.net
- omg.lol
- OpenProvider
- OpenStack Designate API
- OPNsense
- Oracle Cloud Infrastructure-OCI
- OVH.com
- Plesk XML
- PointHQ
- Porkbun.com
- PowerDNS
- RackCorp.com
- RackSpace.com
- rage4.com
- RcodeZero
- reg.ru
- ScaleWay.com
- Schlundtech
- Selectel
- SelfHost.de
- ServerCow.de
- Simply.com
- Technitium DNS Server
- tele3.cz
- Tencent.com
- Timeweb.Cloud

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- TransIP.nl
- UltraDNS
- united-domains Reselling
- unoeuro.com
- variomedia.de
- Vercel.com
- veesp.com
- versio.nl AuroraDNS
- VSCALE
- vshosting.cz CloudDNS
- Vultr
- Websupport.sk
- West.cn
- World4You.com
- Yandex 360 for Business DNS API.
- Yandex Cloud DNS
- Zilore
- Zone.eu
- ZoneEdit.com
- Zonomi

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Once all three steps are completed, NetScaler Console configures the ACME CA server. The selected certificates are renewed for the mapped domains. NetScaler Console periodically checks certificate validity and renews them before they expire (based on configured window). With no manual intervention required, certificates always stay valid and up to date.

Issuance and renewals

Navigate to **Infrastructure > SSL Dashboard > Issuance & Renewals** to check all the renewal activities and the new requests raised from the certificate issuance.

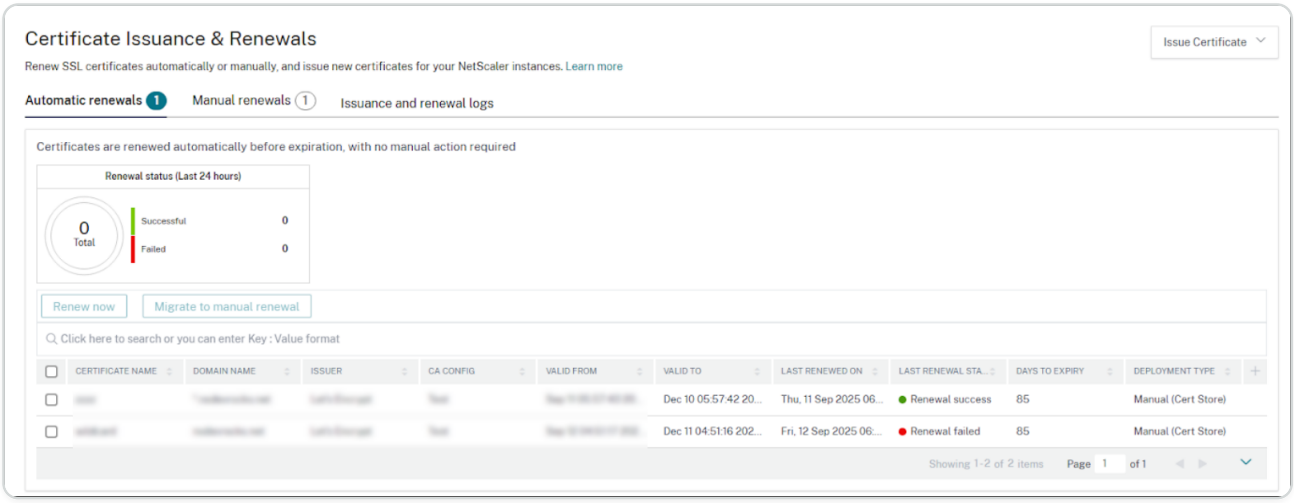
Automatic renewals

The **Automatic renewals** tab lists the certificates that are enrolled for automatic renewal. When the configured renewal window is reached, NetScaler Console renews them automatically.

You can also trigger an on-demand renewal before the scheduled renewal window. For on-demand renewal, select the required certificate, and click **Renew now**.

If you do not want some certificates to be automatically renewed, you can move to manual renewals. To transfer the certificates from automatic renewal to manual renewal, select the required certificates and click **Migrate to manual renewal**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Manual renewals

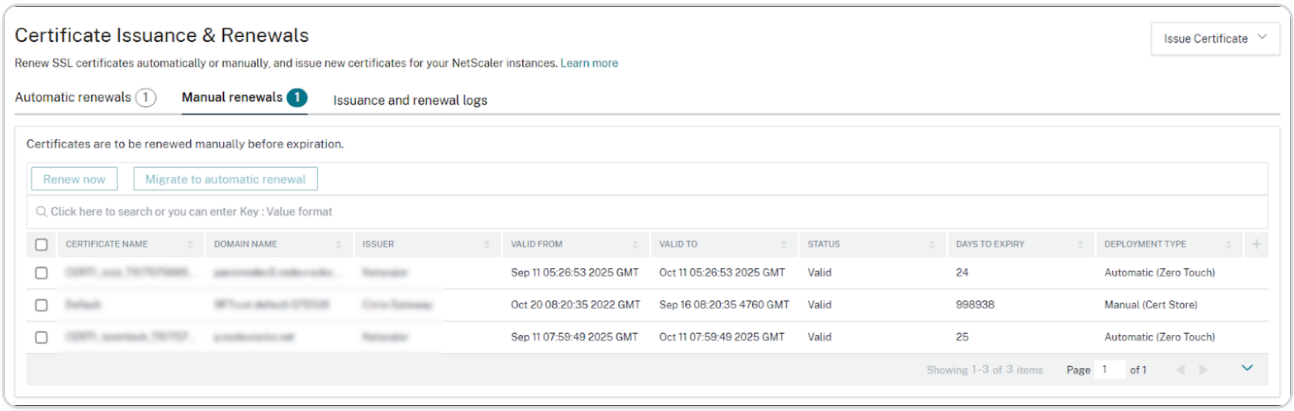
The **Manual renewals** tab lists all the certificates that must be manually renewed. These certificates must be updated manually, either by renewing the certificate offline and uploading the new certificate to the appropriate store, or by using the **Renew now** option.

To renew a certificate, select a certificate and click **Renew now**. If the certificate is issued by a registered CA and its domain's DNS provider is configured, you can renew it on demand by using ACME without moving it to automated renewals.

You can also move a certificate to automatic renewal. To transfer the certificates from manual renewal to automatic renewal, select the required certificates and click **Migrate to automatic renewal**.

NOTE:

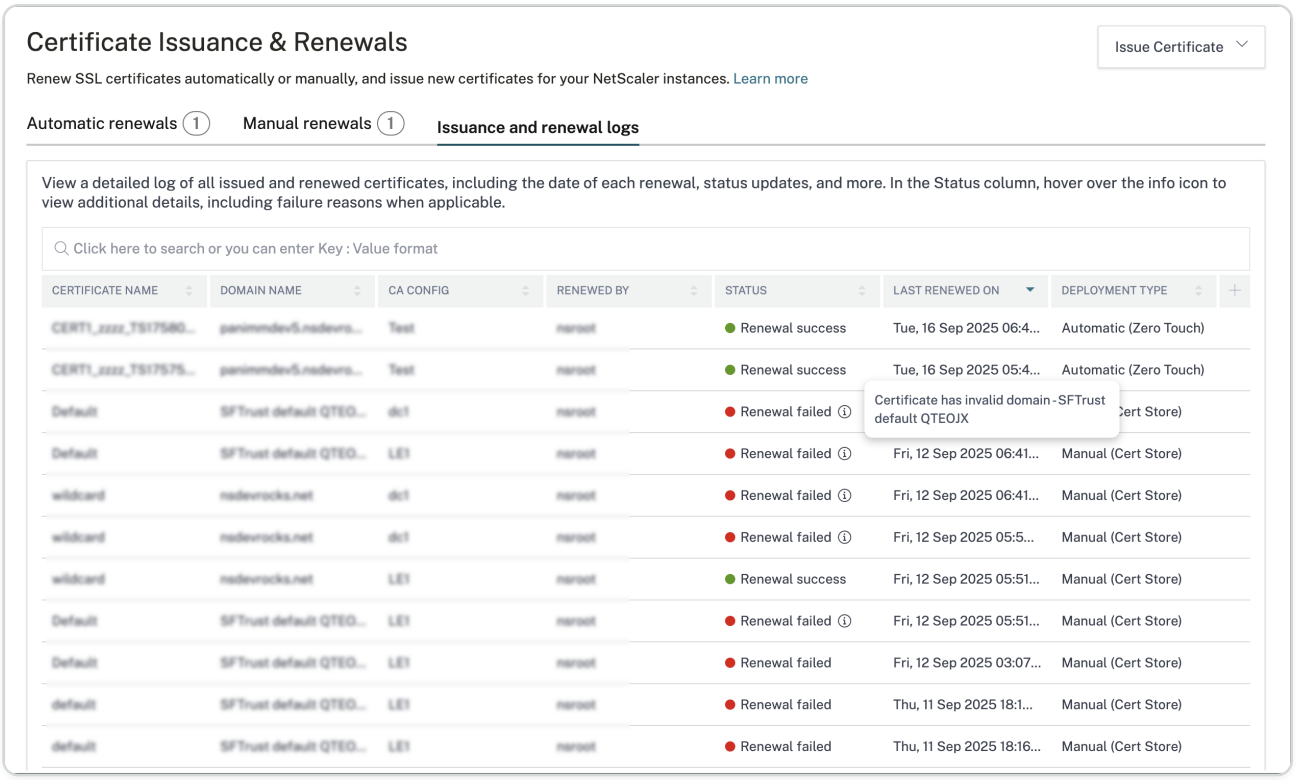
You can renew or migrate only one certificate at a time.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Issuance and renewal logs

The **Issuance and renewal logs** tab provides the list of certificate requests using ACME, including issuances and renewals. For a failed event, you can click the info icon to view detailed error information.



Issue a certificate

ACME integration in NetScaler Console supports requesting new certificates directly by using the ACME protocol. You can either create a CSR within NetScaler Console or upload an existing CSR to request new certificates.

Navigate to **Infrastructure > SSL dashboard > Issuances & Renewal** and click **Issue Certificate** and select one of the following based on your scenario:

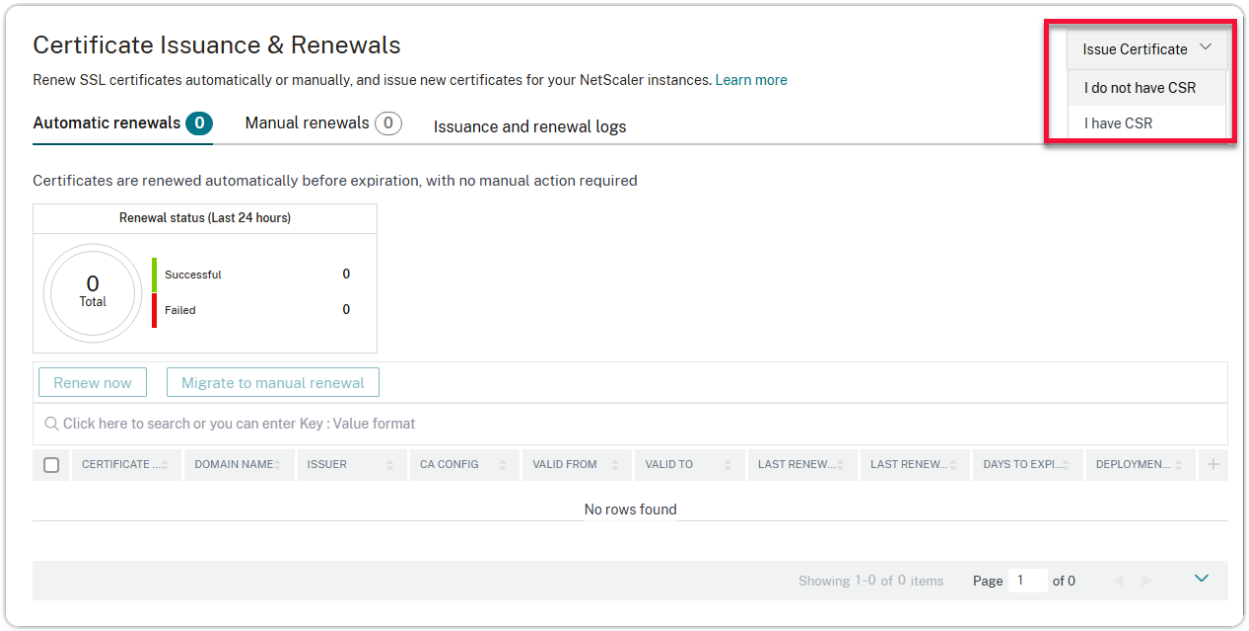
- **I do not have CSR**: If you don't already have a CSR, NetScaler Console allows you to generate one and issue a new certificate.
- **I have CSR**: If you already have a CSR generated offline, you can upload it to issue a certificate.

Issue a certificate without CSR

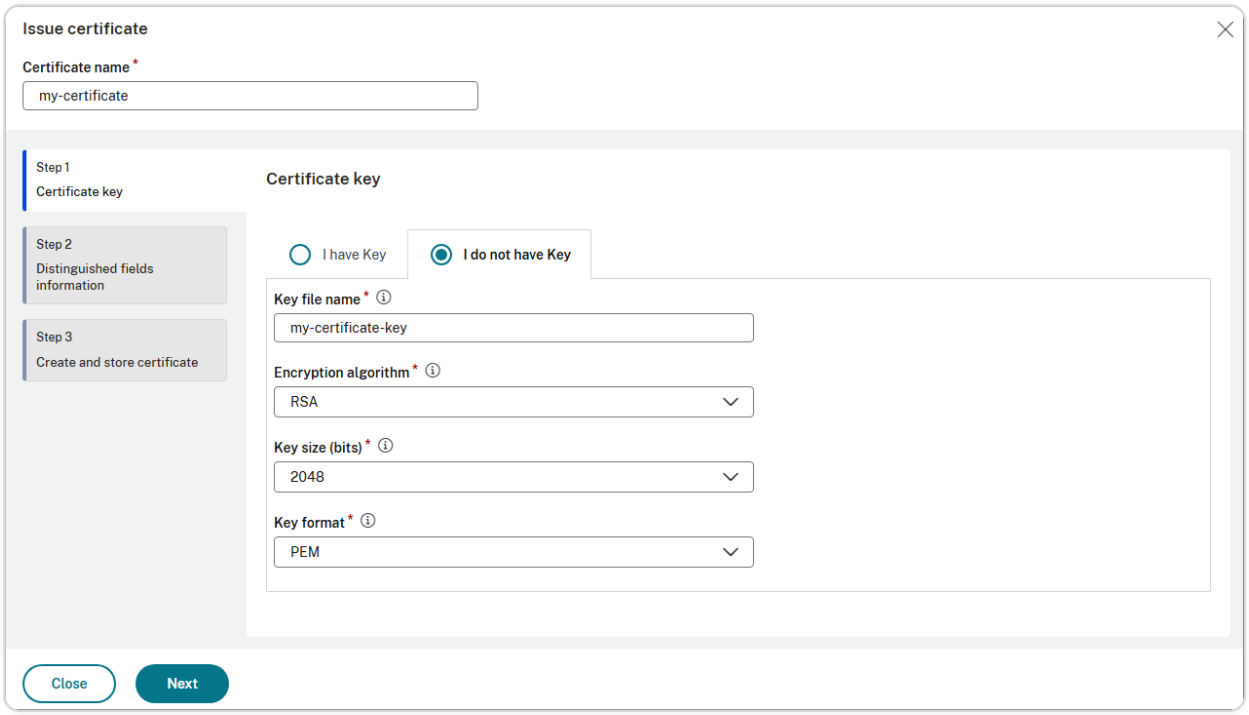
Perform the following steps to generate a CSR and issue a new certificate:

1. Navigate to **Infrastructure > SSL dashboard > Issuances & Renewal** and click **Issue Certificate** and select **I do not have CSR**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

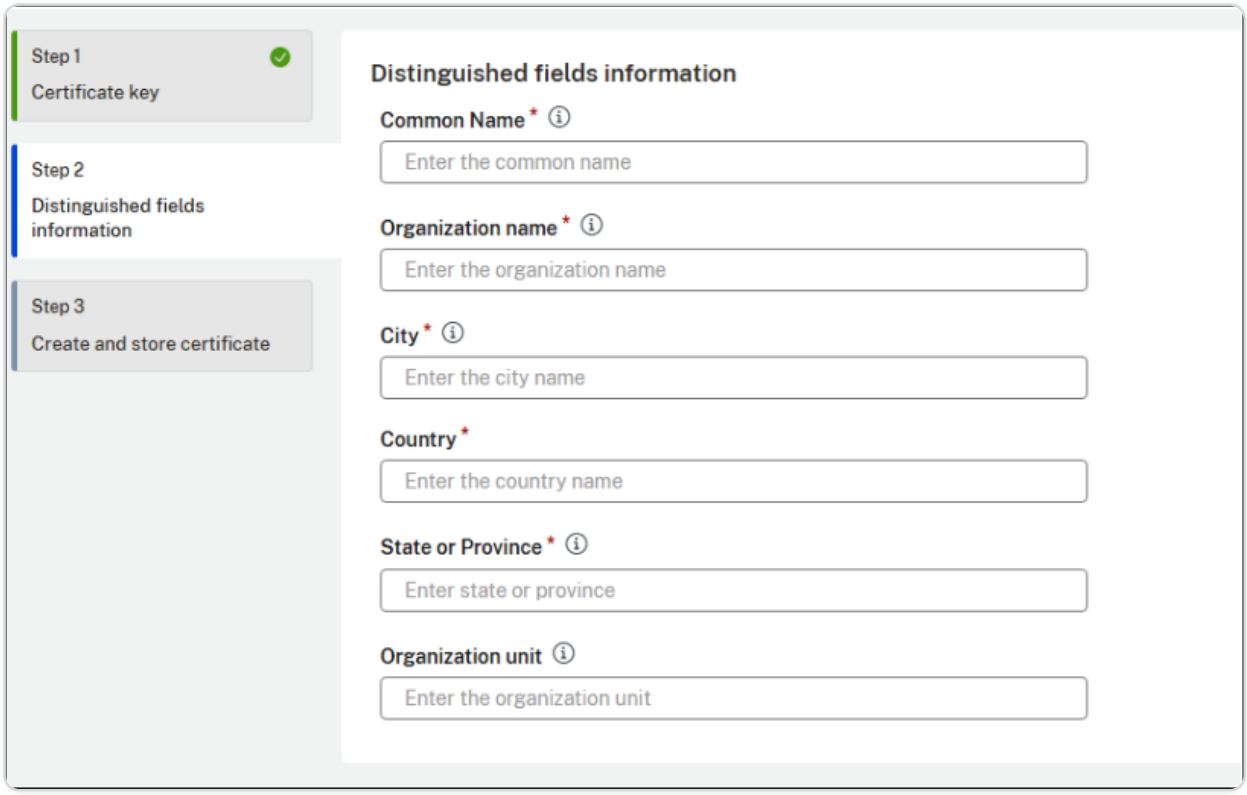


2. On the **Certificate key** page, either upload an existing key by selecting **I have a key** or generate a new one by selecting **I do not have a key**.

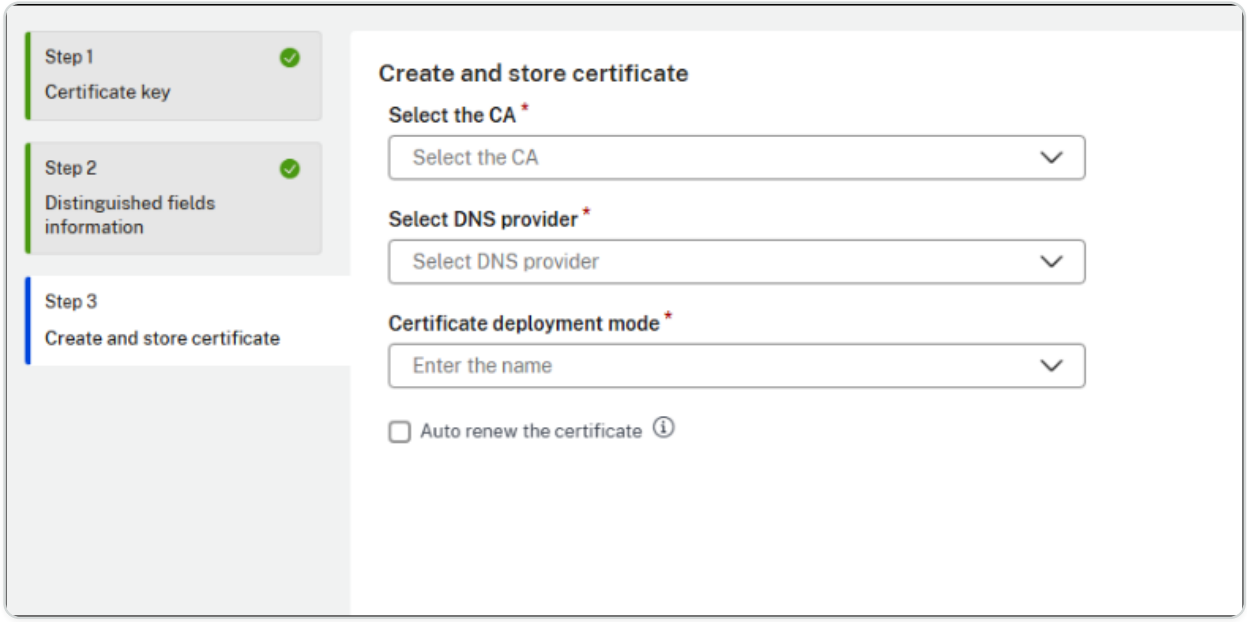


3. Enter the required CSR information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Select the CA, DNS provider, and certificate deployment mode for the ACME request. Choose **Cert Store** for manual deployment, or **Zero Touch Store** for automatic deployment on NetScaler.
5. Select **Auto renew the certificate** if you want the certificate to be automatically renewed in future.



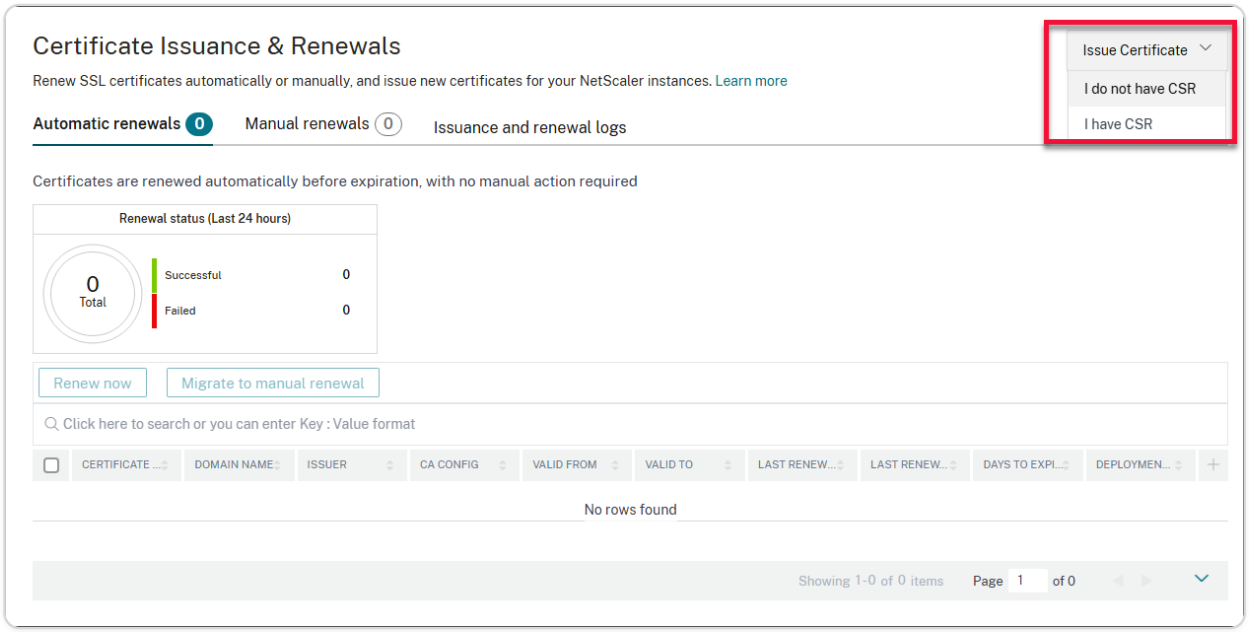
6. Click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

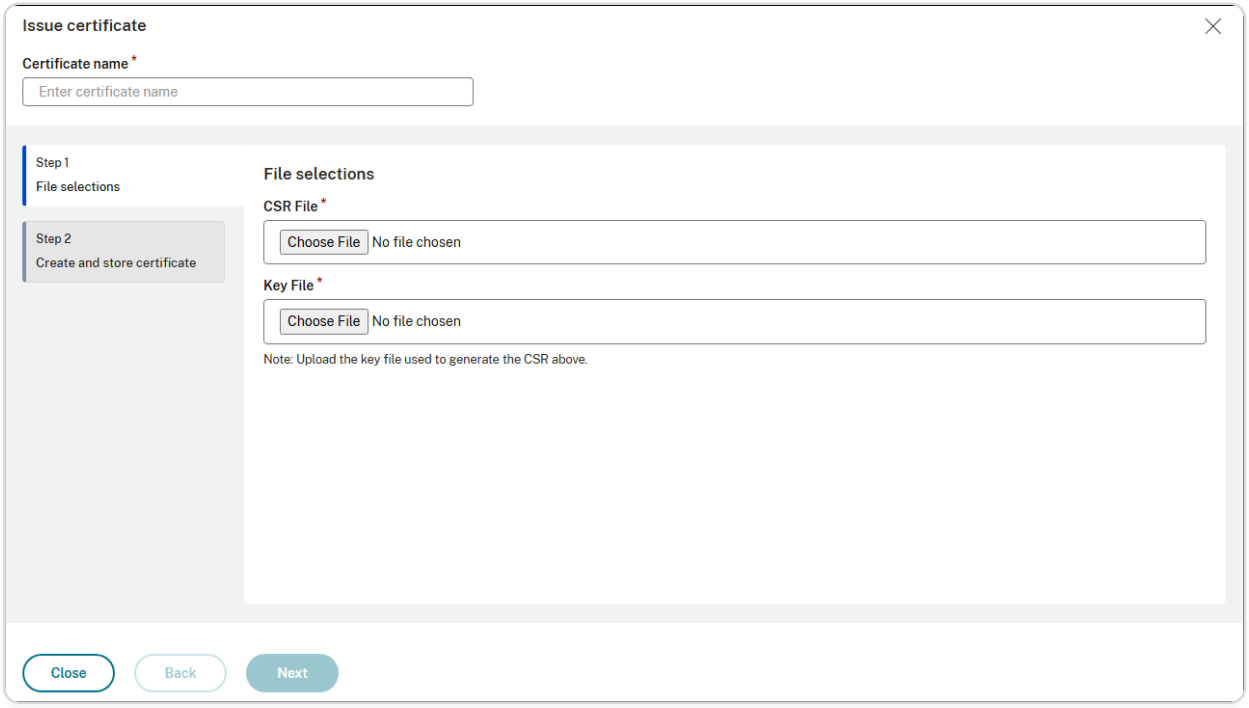
Issue a certificate with CSR

Perform the following steps if you already have a CSR generated offline and you want to upload it to issue a certificate:

1. Navigate to **Infrastructure > SSL dashboard > Issuances & Renewal** and click **Issue Certificate** and select **I have CSR**.



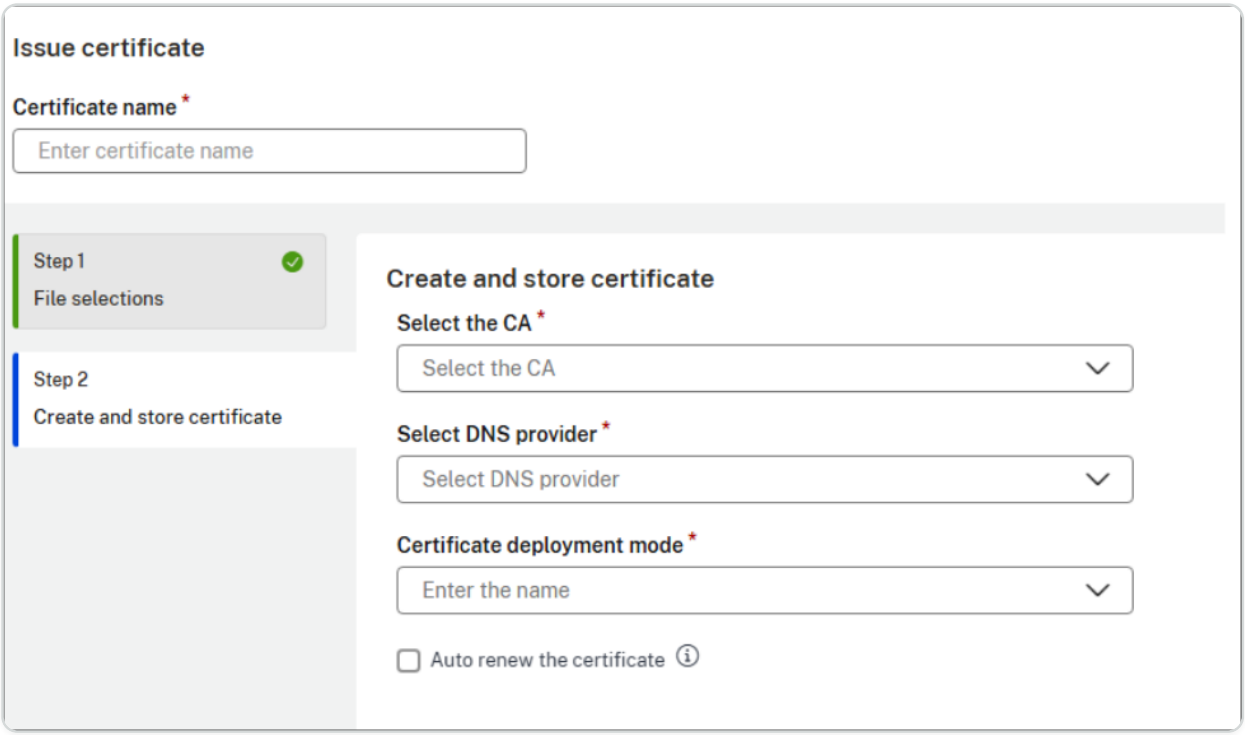
2. Choose the CSR file and associated key file from your local system.



3. Select the CA, DNS provider, and certificate deployment mode for the ACME request. Choose **Cert Store** for manual deployment, or **Zero Touch Store** for automatic deployment on NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Select **Auto renew the certificate** if you want the certificate to be automatically renewed in future.



5. Click **Save**.

Third-party Integration

You can add and manage more than one CA vendor and DNS provider.

You can perform following actions from the **Third Party Integration** page:

- Add or edit a CA vendor
- Change the auto renewal settings
- Add or edit the certificate from an existing configured CA
- Add or edit a DNS provider
- Change domain mappings

Add or edit a CA vendor

You can register more than one CA vendor to manage certificates issued by different vendors. You can also edit the existing CA vendor details.

1. Navigate to **SSL dashboard > Third party integration > ACME > CA Vendors**. Click **Add**.
2. To add a CA vendor, provide a name for the CA vendor and select the CA.
3. To edit an existing CA vendor details, select the CA vendor and click **Edit**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Add or update the required details.
5. Click **Save**.

Change the auto renewal settings

To change the auto renewal settings, perform the following steps:

1. Navigate to **SSL dashboard > Third party integration > ACME > CA Vendors**.
2. Select a CA vendor, and click **Edit**
3. In the **Configure certificate Authority vendor**, change the number of days as per your requirement the **Auto renew settings** section.
4. Click **Save and continue**.
5. Complete the workflow.

Add or edit the certificate from an existing configured CA

To add or edit the certificate from an existing configured CA, perform the following steps

1. Navigate to **SSL dashboard > Third party integration > ACME > CA Vendors**.
2. Select a CA vendor, and click **Edit**.
3. Navigate to **Step 2 Select certificates**, and add or remove the required certificates.
4. Click **Save and continue**.
5. Complete the workflow.

NOTE:

If the certificate has not been unmapped from the original CA, it does not appear in the selection list for the new CA.

Add or edit a DNS provider

To add a new DNS provider or edit existing domain mappings of existing DNS providers, perform the following steps:

1. Navigate to **SSL dashboard > Third party integration > ACME > DNS Providers**.
2. To add a DNS provider, click **Add**. Select the DNS provider, and click **Save**.
3. To edit an existing DNS provider, select a DNS provider and click **Edit**.
4. Add or update the required details.
5. Click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Change domain mappings

To edit the domain mappings of existing DNS providers, perform the following steps:

1. Navigate to **SSL dashboard > Third party integration > ACME > DNS Providers**.
2. Select a DNS provider and click **Edit**.
3. Navigate to **Domain mapping**, and add or remove domains as required.
4. Click **Save**.

IMPORTANT:

If a domain is unmapped, its certificate renewal stops. Always remap domains to a valid DNS provider to ensure that renewals continue.

Limitations

- Certificate renewal happens only for the DNS providers that are supported by `acme.sh`.

Troubleshoot issues related to automatic certificate renewal

A few common error messages that might occur and their associated root cause are listed in this section:

- **Certificate has invalid domain - ADCD** error is reported when the domain name in the certificate is not valid as per ACME requirements.
- **Invalid identifiers requested :: Cannot issue for "testdomain": Domain name needs at least one dot** is reported when the requested domain name is missing a dot (such as "example" instead of "example.com").
- **Could not get nonce from the CA server. Please check the CA server configuration.** is reported when the ACME client fails to obtain a nonce from the CA, often due to network or server issues.
- **Cannot initialize API for the CA server. Please check the CA server configuration.** is reported when the ACME client cannot initialize communication with the CA server, possibly due to misconfiguration.
- **Invalid domain name provided. Please check the domain name and try again.** is reported when the domain name format is invalid or not allowed by the ACME protocol.
- **Domains not changed. Certificate with same configuration already exists.** is reported when a certificate request is made with no changes to the domain list and the certificate already exists.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Error adding TXT record for domain validation. Please check the DNS configuration and try again.** is reported when the ACME client fails to add the required DNS TXT record for domain validation.
- **Signature does not match. Please check the server time as it may not be in sync.** is reported when there is a signature mismatch, often due to time synchronization issues between client and server.
- **Certificate is missing a DNS provider name.** is reported when no DNS provider is specified for DNS-based domain validation.
- **Renewal skipped as no active DNS providers are configured.** is reported when certificate renewal is attempted but no active DNS providers are configured.
- **Error validating contact(s) :: unable to parse email address** is reported when the contact email address provided is invalid or cannot be parsed.
- **Unable to process finalize order request. (For invalid ACME Directory URL)** is reported when the ACME client cannot finalize the order, often due to an invalid or unreachable ACME Directory URL.
- **DNS Provider - TestDNS does not exist or is not active.** is reported when the specified DNS provider is not found or is inactive in the system.
- **Config CA ID is empty/does not exist.** is reported when the CA configuration ID is missing or does not match any existing configuration.

Zero-touch certificate management

In NetScaler Console, you can configure zero-touch certificate management on the managed NetScaler instances running build **14.1-43.x** and later. With zero-touch certificate management, you eliminate manual interventions and build an in-memory zero-touch certificate store to serve the application requests. Navigate to **Infrastructure > SSL Dashboard > Zero-Touch Certificate Management** to upload all the certificates and keys on NetScaler Console, and enable it on the managed NetScaler instances. NetScaler periodically polls the certificate repository and delivers the necessary certificates as required.

With zero-touch certificate management, the following processes are automatically done by NetScaler:

- Adding, binding, and linking the certificates
- Providing the certificates and keys in a specific order or together
- Installing and using the suitable certificates based on the requests

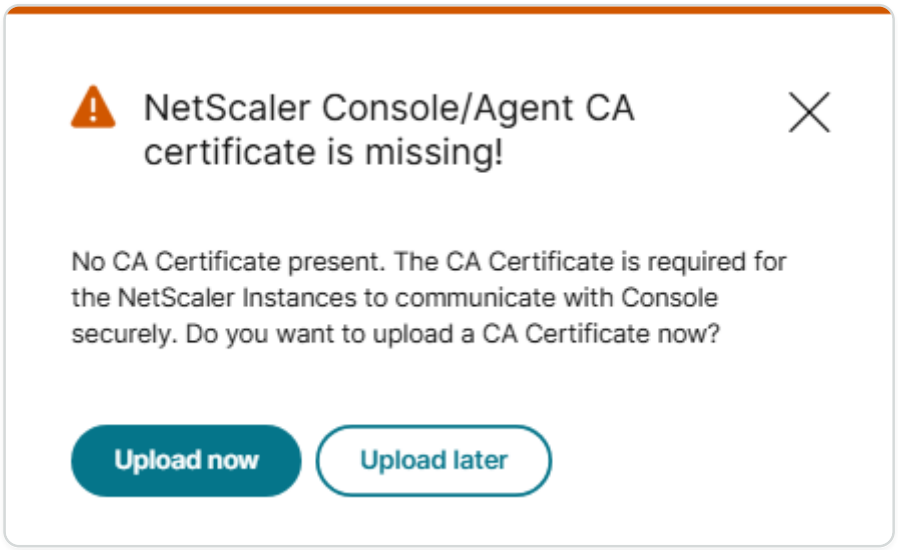
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Deleting the expired certificates during the periodic polling cycle

For more information on how the zero-touch certificate works on NetScaler instances, see NetScaler zero touch certificate management.

As an administrator, you must ensure the following in NetScaler Console:

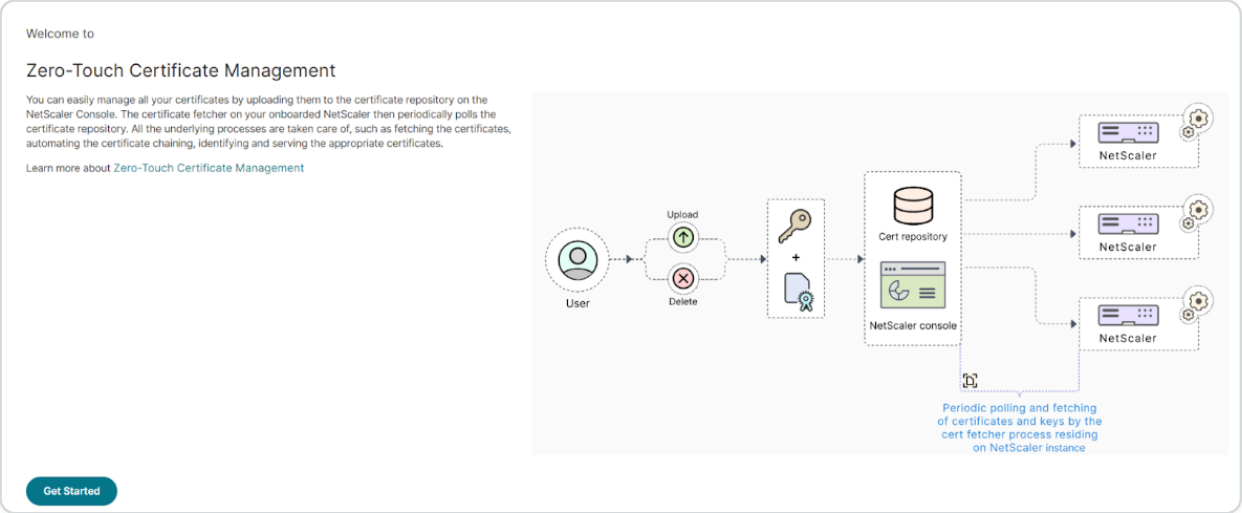
- NetScaler instances are running build 14.1-43.x or later and they are managed in NetScaler Console.
- Upload the certificates (in any format) and keys. Then, enable zero-touch on the managed NetScaler instances.
- Ensure that a valid CA certificate is present on NetScaler Console. If you have an updated Console CA certificate, upload the certificate before you enable zero-touch on the managed NetScaler instances. The following error message is displayed if no CA certificate present on NetScaler Console:



Upload certificates

1. Navigate to **Infrastructure > SSL Dashboard > Zero-Touch Certificate Management**.
2. Click **Get Started**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. NetScaler instances running build 14.1-43.x or later are listed. You can either click **Configure zero-touch** to enable zero-touch or click **Skip** to proceed the next step.
4. Click **Upload** to upload all the certificates (can be in any format, such as .pem, .cer, and .crt).

NOTES:

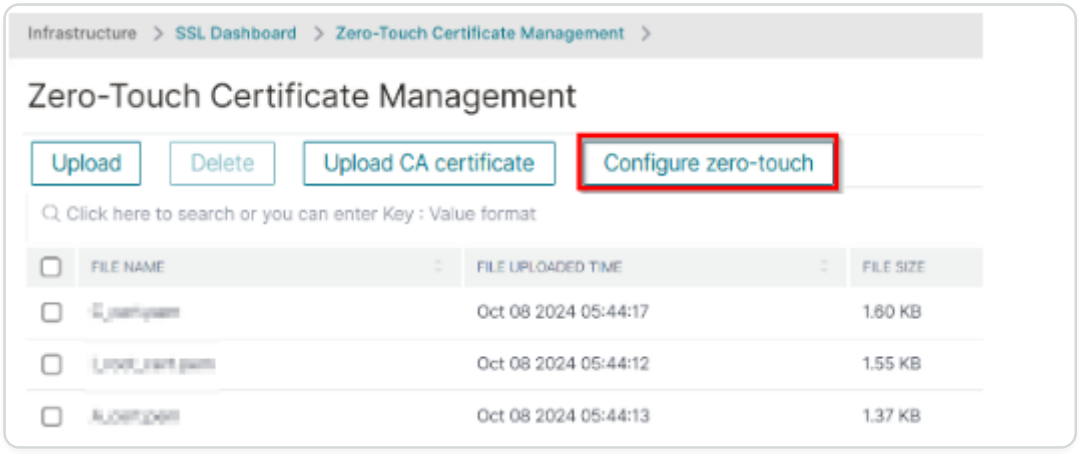
- The certificate or key file must be less than 8192 bytes.
- If you are uploading multiple certificates or key files, the maximum supported size is 50000 bytes.
- If the certificates or key files are password-protected, ensure that you provide the password. If the password is not provided, the certificate or the key file is not uploaded.

Enable zero-touch certificate management

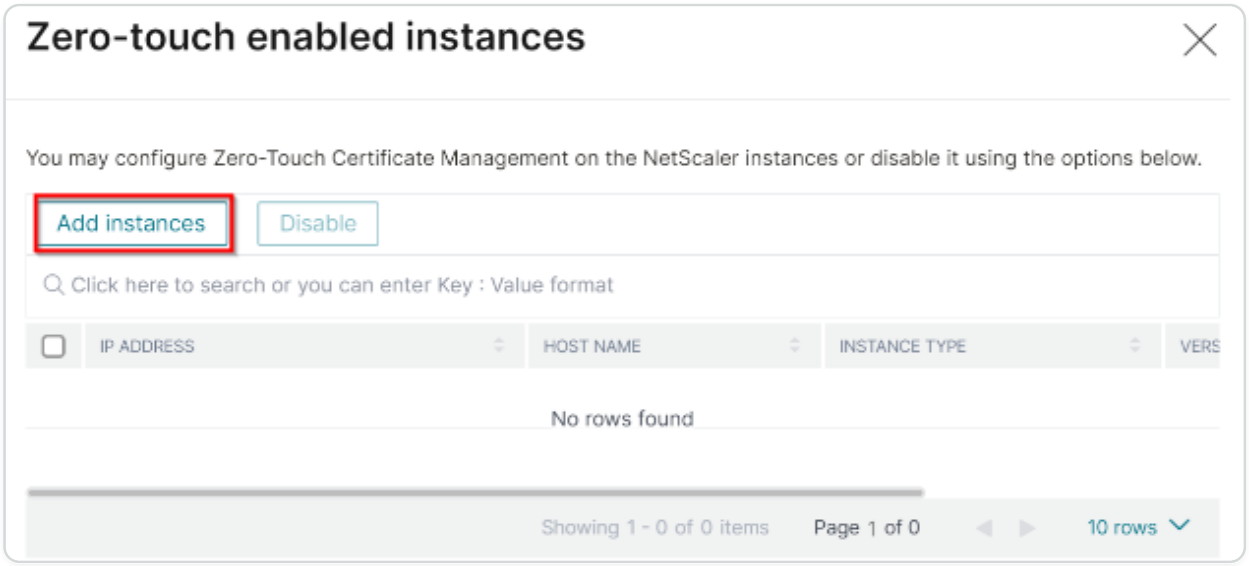
After you upload the certificates, you must enable zero-touch on the managed NetScaler instances.

1. From the **Zero-Touch Certificate Management** page, click **Configure zero-touch**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



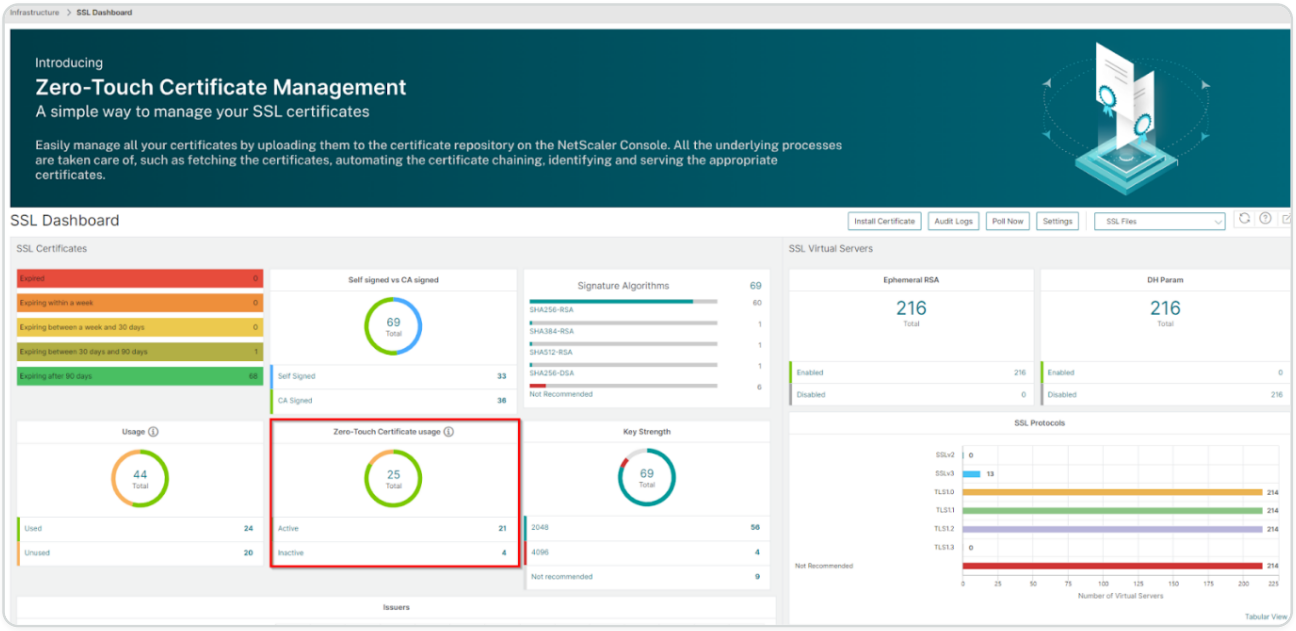
2. Click **Add instances**, select the instances, and then click **Enable**.



NetScaler Console uses the default polling interval to poll all certificates from the NetScaler instances. You can use the **Poll Now** option to poll immediately.

In the **SSL dashboard**, you can also view zero-touch certificate usage that shows details about the active and inactive certificates.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



SSL filter mode support

A NetScaler® instance fetches the metadata of specific SSL certificates and private keys. Implementing this least privilege approach ensures that instances only access the assets they require, preventing a compromise on one instance from exposing your entire certificate infrastructure. This feature is especially useful for environments with multiple administrators managing a group of NetScaler instances for distinct purposes.

Some of the benefits are:

- **Security segmentation** - Restricts metadata access at a per-NetScaler level to minimize the attack surface and adhere to organizational security policies.
- **Streamlined admin experience** - Reduces complexity in multi-tenant or departmental deployments by showing administrators only the assets relevant to their group of NetScaler instances.
- **Optimized resource utilization** - Prevents system memory bloating by fetching the metadata of only the required SSL certificates and private keys.

The filter mode configuration defines how NetScaler instances and SSL files interact through specific synchronization types. You can manage these settings through NetScaler Console to ensure that only the necessary metadata is fetched by each instance.

COMPONENT	SYNC TYPE	DESCRIPTION
NetScaler Instance	Custom Sync	NetScaler instances in this mode fetch only the metadata for certificates and keys

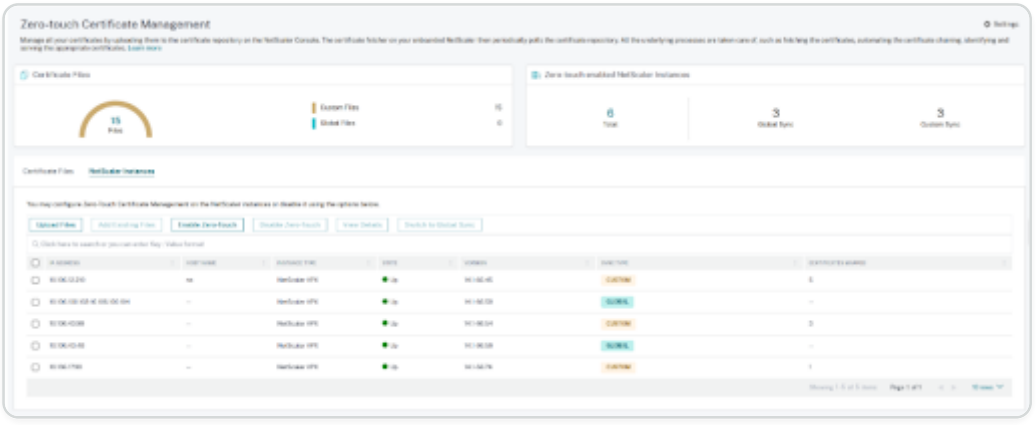
© 1997–2026 Citrix Systems, Inc. All rights reserved.

COMPONENT	SYNC TYPE	DESCRIPTION
		specifically mapped to the instance.
NetScaler Instance	Global Sync	NetScaler instances in this mode fetch the metadata for all uploaded certificates and private keys.
SSL Files	Custom Files	These files are specifically mapped to NetScaler instances in Custom Sync mode.
SSL Files	Global Files	Metadata for these files is fetched by all the NetScaler instances in Global Sync mode.

Configure filter mode settings

To configure filter mode, define synchronization types for your instances and files. This ensures a secure and optimized distribution of sensitive metadata.

You can now upload certificates and private keys directly using the upload button in the Certificate Files and NetScaler Instances sections.

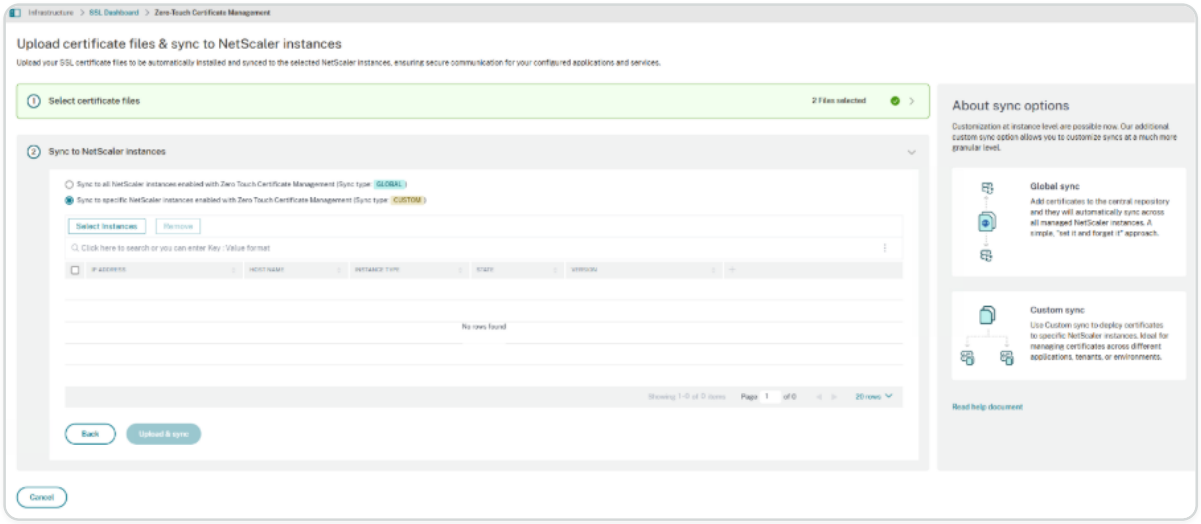


To configure using the GUI:

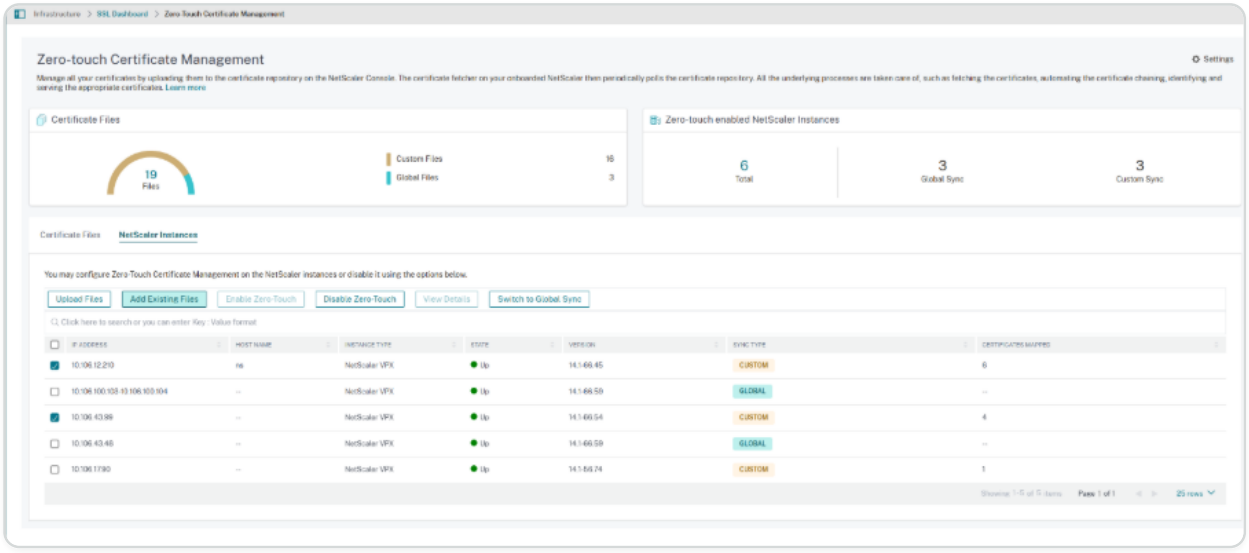
1. **Upload New Files (Day Zero)** - Navigate to Certificate Files and NetScaler Instances > Upload to add new assets. Select from one of the following sync types:
    - **GLOBAL** - Select to use global sync mode and complete the upload.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **CUSTOM** - Select to use custom sync mode, choose the specific instances for mapping, and then upload the files.



2. **Move Existing Files (Day N)** - To shift certificates and keys from global sync to custom sync mode, select the target NetScaler instances and click Add Existing Files.
3. **Select Domains** - Once instances are selected, choose the relevant domains to trigger the shift. NetScaler Console automatically detects and shifts the corresponding certificates and private key files to custom sync mode.
4. **View Assets** - Navigate to the landing page to view all the certificates and private key files mapped to each NetScaler instance in custom sync mode.
5. **Switch Sync Mode** - To return instances to global sync mode, click Switch to Global Sync on the landing page.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use the SSL dashboard

You can use the SSL certificate dashboard in NetScaler Console to view graphs that help you keep track of certificate issuers, key strengths, and signature algorithms. The SSL certificate dashboard also displays graphs that indicate the following:

- Number of days after which certificates expire
- Number of used and unused certificates
- Number of self-signed and CA-signed certificates
- Number of issuers
- Signature algorithms
- SSL protocols
- Top 10 instances by number of certificates in use

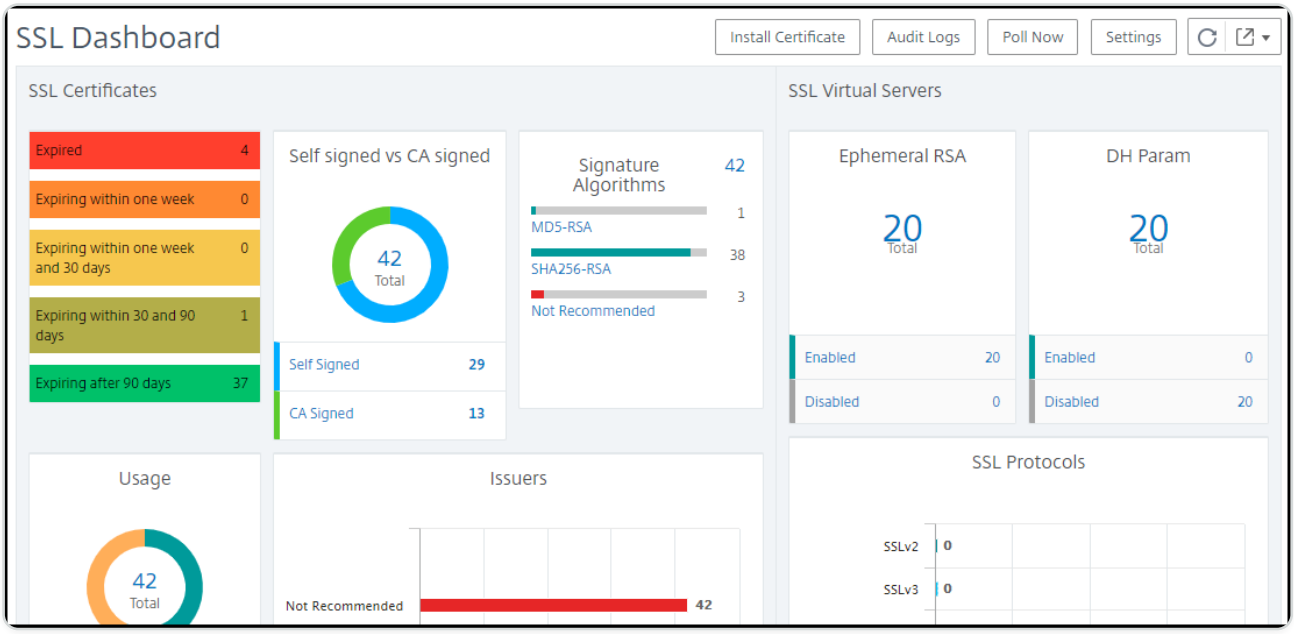
Monitor SSL certificates

Use the SSL dashboard on NetScaler Console to monitor your certificates if your company has an SSL Policy where you have defined certain SSL certificate requirements such as all certificates must have minimum key strengths of 2048 bits and a trusted CA authority must authorize it.

In another example, you may have uploaded a new certificate but forgotten to bind it to a virtual server. The SSL dashboard highlights the SSL certificates being used or not used. In the **Usage** section, you can see the number of certificates that have been installed, and the number of certificates being used. You can further click the graph, to see the certificates name, the instance on which it's being used, its validity, its signature algorithm, and so on.

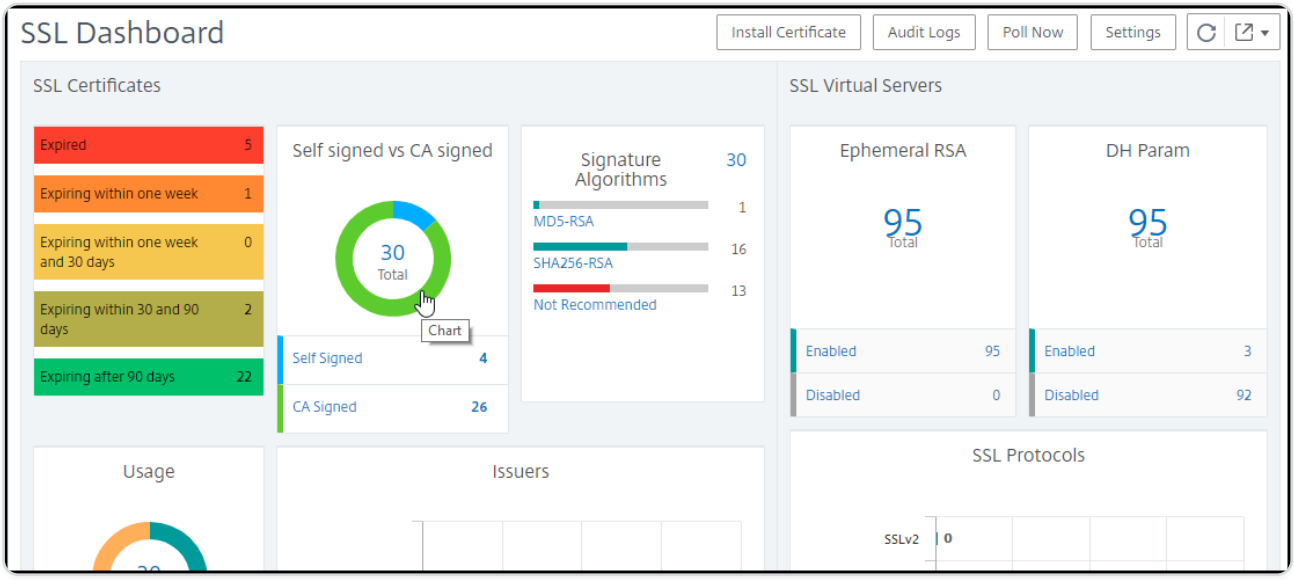
To monitor SSL certificates in NetScaler Console, navigate to **Infrastructure > SSL Dashboard**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



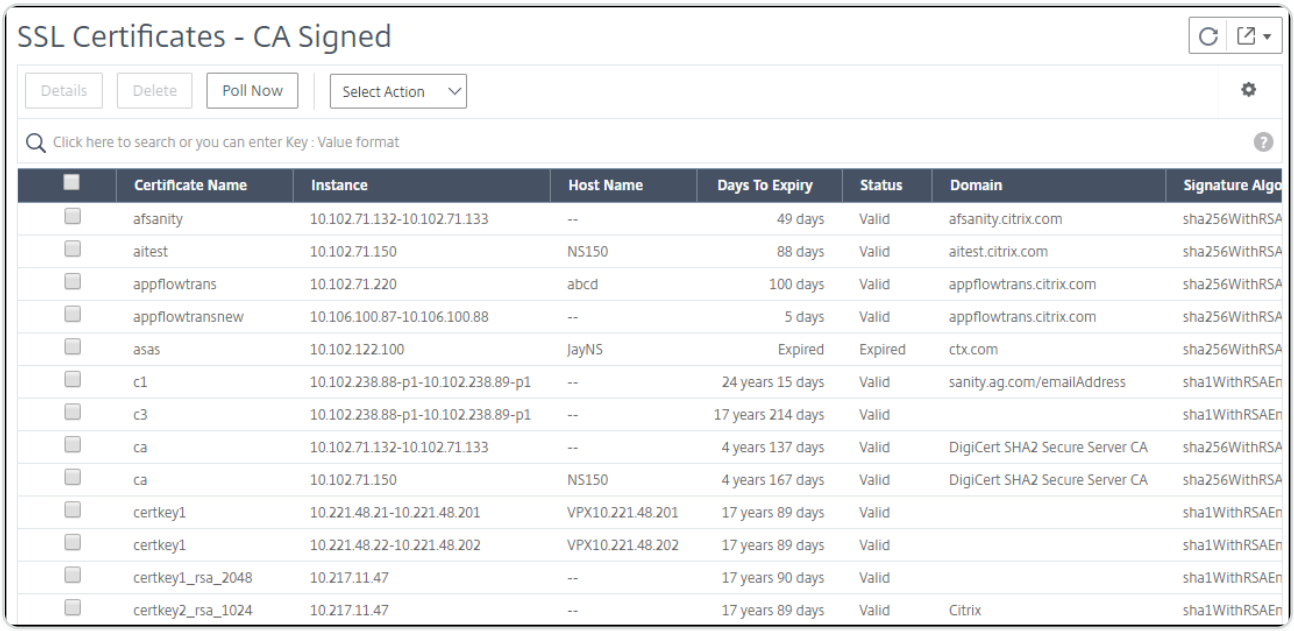
NetScaler Console allows you to poll SSL Certificates and add all the SSL certificates of the instances immediately to NetScaler Console. To do so, navigate to **Infrastructure > SSL Dashboard** and click **Poll Now**. The **Poll Now** page pops up, presenting the option to poll all NetScaler instances in the network or poll selected instances.

You can use the NetScaler Console SSL dashboard to view or monitor the details of SSL certificates, SSL Virtual Servers, and SSL protocols. The numbers are hyperlinks, which you can click to display details related to SSL certificates, SSL Virtual Servers, or SSL protocols.



For example, when a user clicks the number 30 under **Self-signed vs. CA signed** in the above figure, a new window appears, showing details of the 30 SSL certificates on the NetScaler instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

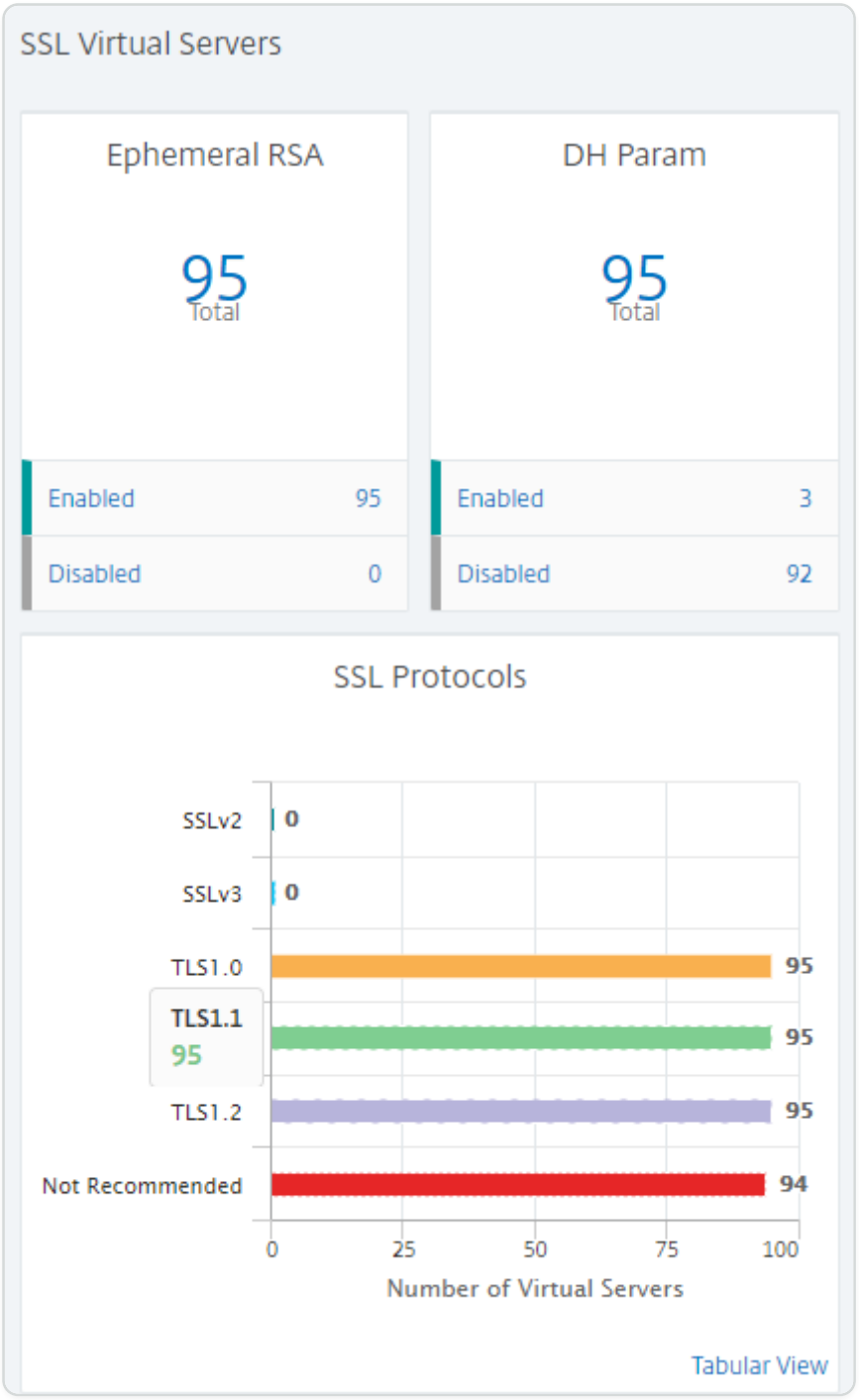


Certificate Name	Instance	Host Name	Days To Expiry	Status	Domain	Signature Algo
afsanity	10.102.71.132-10.102.71.133	--	49 days	Valid	afsanity.citrix.com	sha256WithRSA
aitest	10.102.71.150	NS150	88 days	Valid	aitest.citrix.com	sha256WithRSA
appflowtrans	10.102.71.220	abcd	100 days	Valid	appflowtrans.citrix.com	sha256WithRSA
appflowtransnew	10.106.100.87-10.106.100.88	--	5 days	Valid	appflowtrans.citrix.com	sha256WithRSA
asas	10.102.122.100	JayNS	Expired	Expired	ctx.com	sha256WithRSA
c1	10.102.238.88-p1-10.102.238.89-p1	--	24 years 15 days	Valid	sanity.ag.com/emailAddress	sha1WithRSAEn
c3	10.102.238.88-p1-10.102.238.89-p1	--	17 years 214 days	Valid		sha1WithRSAEn
ca	10.102.71.132-10.102.71.133	--	4 years 137 days	Valid	DigiCert SHA2 Secure Server CA	sha256WithRSA
ca	10.102.71.150	NS150	4 years 167 days	Valid	DigiCert SHA2 Secure Server CA	sha256WithRSA
certkey1	10.221.48.21-10.221.48.201	VPX10.221.48.201	17 years 89 days	Valid		sha1WithRSAEn
certkey1	10.221.48.22-10.221.48.202	VPX10.221.48.202	17 years 89 days	Valid		sha1WithRSAEn
certkey1_rsa_2048	10.217.11.47	--	17 years 90 days	Valid		sha1WithRSAEn
certkey2_rsa_1024	10.217.11.47	--	17 years 89 days	Valid	Citrix	sha1WithRSAEn

The NetScaler Console SSL Dashboard also shows the distribution of SSL protocols that are running on your virtual servers. As an administrator, you can specify the protocols that you want to monitor through the SSL policy, for more information, see Configuring SSL Policies. The protocols supported are SSLv2, SSLv3, TLS1.0, TLS1.1, and TLS1.2. The SSL protocols used on virtual servers appear in a bar chart format. Clicking a specific protocol displays a list of virtual servers using that protocol.

A donut chart appears after Diffie-Hellman (DH) or Ephemeral RSA keys are enabled or disabled on the SSL dashboard. These keys enable secure communication with export clients even if the server certificate does not support export clients, as in the case of a 1024-bit certificate. Clicking the appropriate chart displays a list of the virtual servers on which DH or Ephemeral RSA keys are enabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



View audit logs for SSL certificates

You can now view log details of SSL certificates on NetScaler Console. The log details display operations performed using SSL certificates on NetScaler Console such as: installing SSL certificates, linking and unlinking SSL certificates, updating SSL certificates, and deleting SSL certificates. Audit log information is useful while monitoring SSL certificate changes done on an application with multiple owners.

To view an audit log for a particular operation performed on NetScaler Console using SSL certificates, navigate to **Infrastructure > SSL Dashboard** and select **Audit Logs**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For a particular operation performed using the SSL certificate you can view its status, start time, and end time. Furthermore, you can view the instance on which the operation was performed and the commands run on that instance.

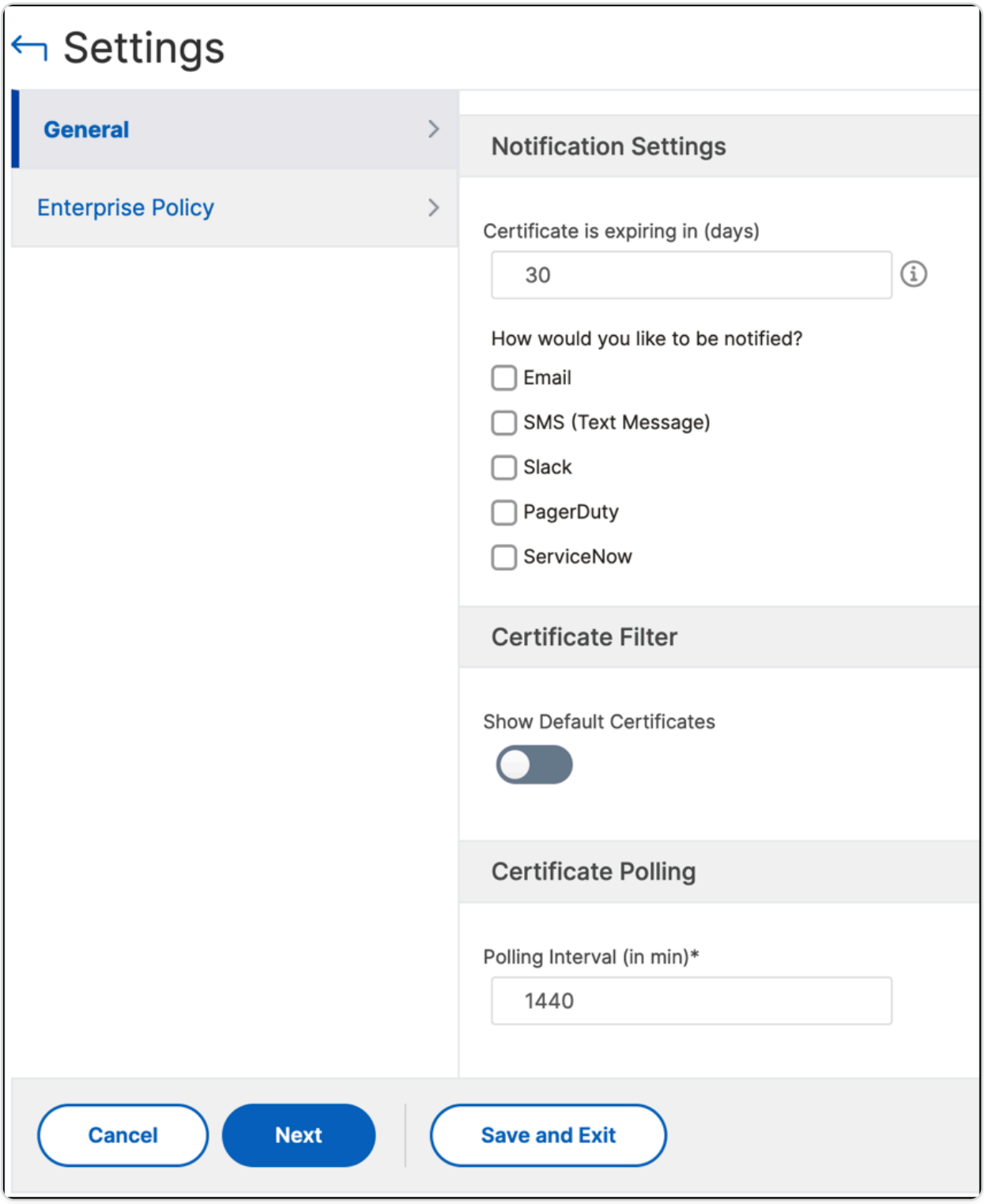
Exclude default NetScaler certificates on the SSL Dashboard

NetScaler Console allows you to show or hide default certificates showing up on the SSL Dashboard charts based on your preferences. By default, all certificates are displayed on the SSL dashboard including default certificates.

To show or hide default certificates on the SSL dashboard:

1. Navigate to **Infrastructure > SSL Dashboard** in the NetScaler Console GUI.
2. On **SSL Dashboard** page, click **Settings**.
3. On the **Settings** page, select **General**.
4. In **Certificate Filter** section, disable the **Show Default Certificates** and select **Save and Exit**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Download SSL certificates

SSL certificates have to be individually managed per instance. NetScaler Console provides visibility into all certificates deployed across multiple instances.

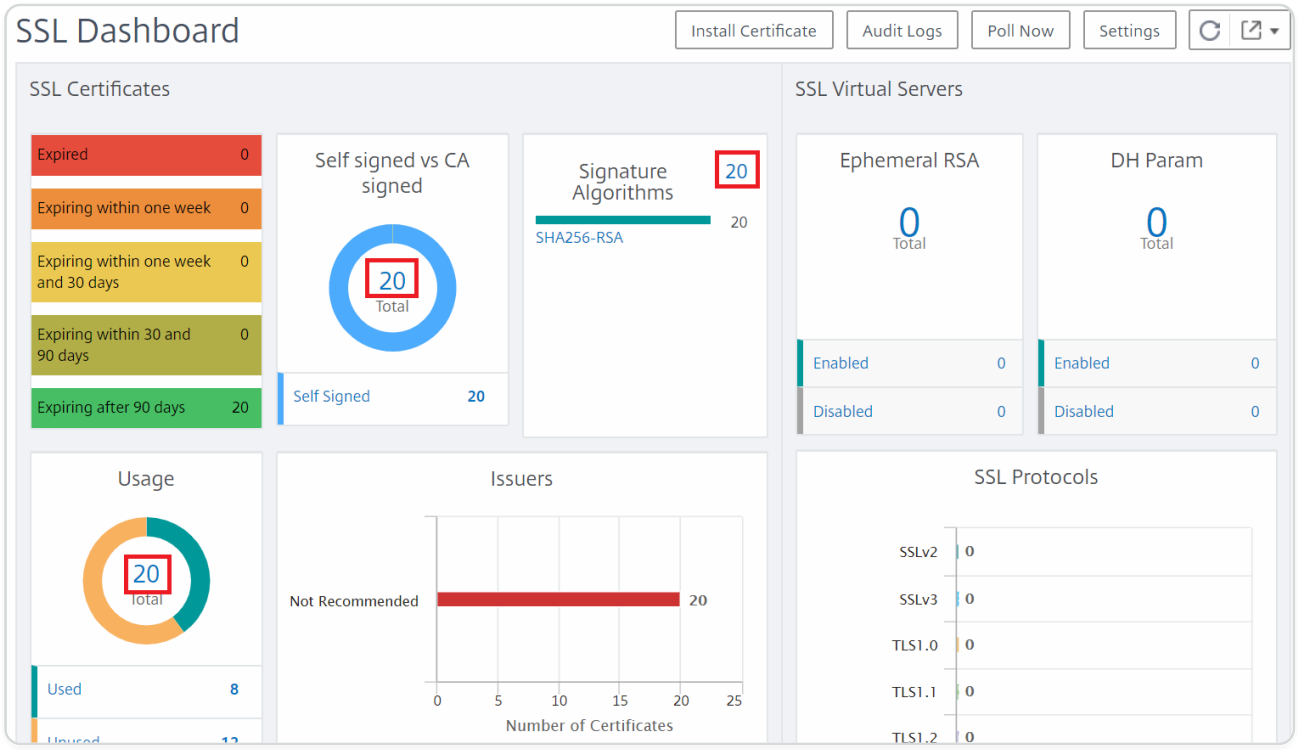
- You can select which certificates are expiring and automate certificate renewals.
- Policies can be set and enforced around the types of certificates and signing authorities that are permitted.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You can also download the SSL certificates for renewal and upload them later.

To download SSL certificates:

1. Navigate to **Infrastructure > SSL Dashboard** in the NetScaler Console GUI.
2. On **SSL Dashboard** page, click the total number of SSL certificates in any of the graphs.



1. On the **SSL Certificates** page, click the certificate that you want to download. For example, you want to download the one that is expiring in the next one week.
2. From the **Select Action** list box, select **Download**. The certificate downloads to your system.

To export the report of this dashboard:

To export the report of this page, click the **Export** icon on the top right side of this page. On the **Export** page, you can do one of the following:

1. Select **Export Now** tab. To view and save the report in PDF, JPEG, PNG, or CSV format.
2. Select **Schedule Export** tab. To schedule the report daily, weekly, or monthly and send the report over an email or a slack message.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

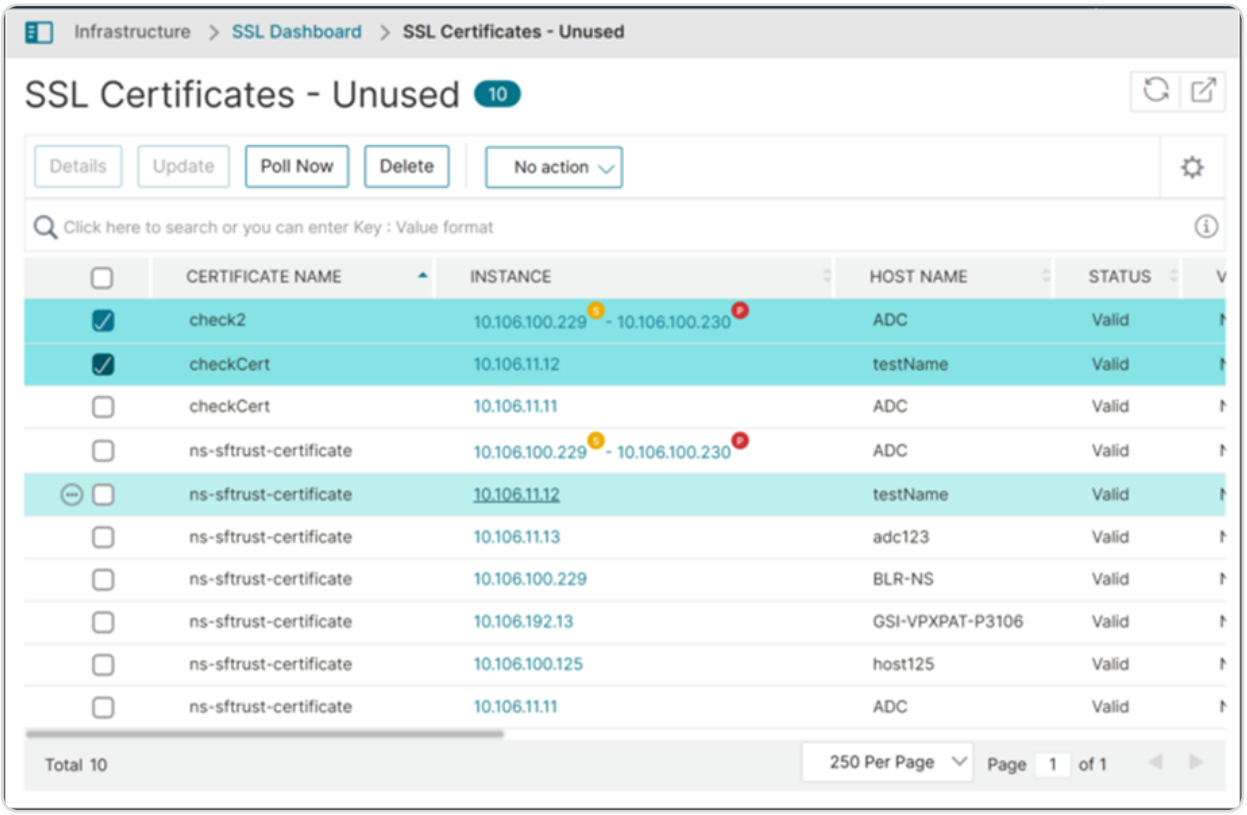
NOTE

- If you select **Weekly** recurrence, ensure that you select the weekdays on which you want the report to be scheduled.
- If you select **Monthly** recurrence, ensure that you enter all the days that you want the report to be scheduled separated by commas.

To delete the SSL certificate on the SSL dashboard

NetScaler 14.1-38.x and later provides an option to delete the associated SSL certificate files from NetScaler while deleting the selected SSL certificate. To delete an SSL certificate:

1. Navigate to **Infrastructure > SSL Dashboard**.
2. In the **SSL Certificates** section where the details of SSL certificates are displayed, click the link on the label **Unused**. A page with a list of unused certificates is displayed.
3. Choose one or more unused certificates to delete.



4. Click **Delete**.
5. A **Confirm** dialogue box appears, providing the following options to delete the certificate files from NetScaler® as well:

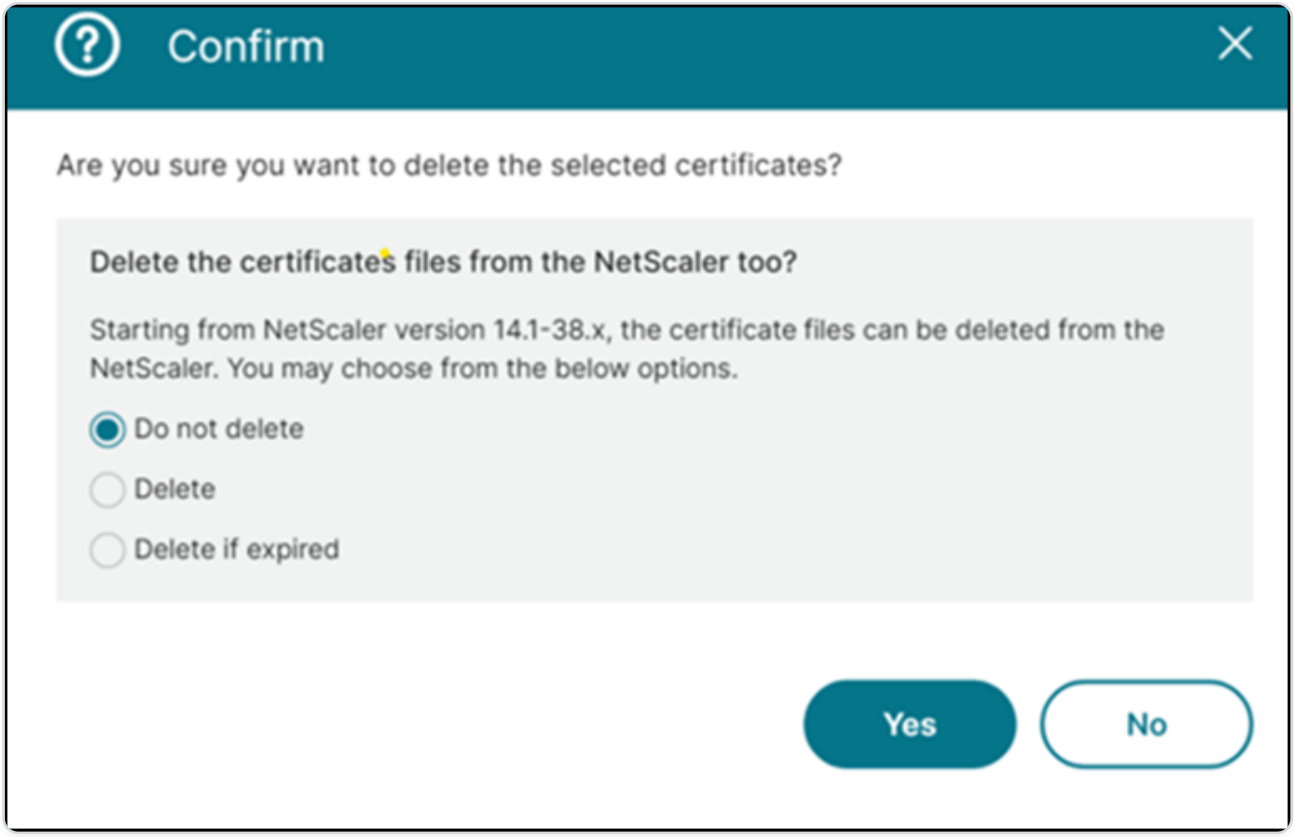
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Do Not Delete**: Skips the deletion of certificate files from NetScaler.
- **Delete**: Deletes the certificate files from NetScaler for both expired and unexpired certificates.
- **Delete if Expired**: Deletes the certificate files from NetScaler for expired certificates only.

NOTE:

- For NetScaler versions earlier than 14.1-38.x, deletion of the certificate file(s) is skipped for all three options.
- Option to delete the certificate file along with configuration is applicable only for NetScaler 14.1-38.x and later.

6. Select the appropriate option based on your needs.
7. Click **Yes** to delete the certificate or click **No** to exit the workflow without making any changes.



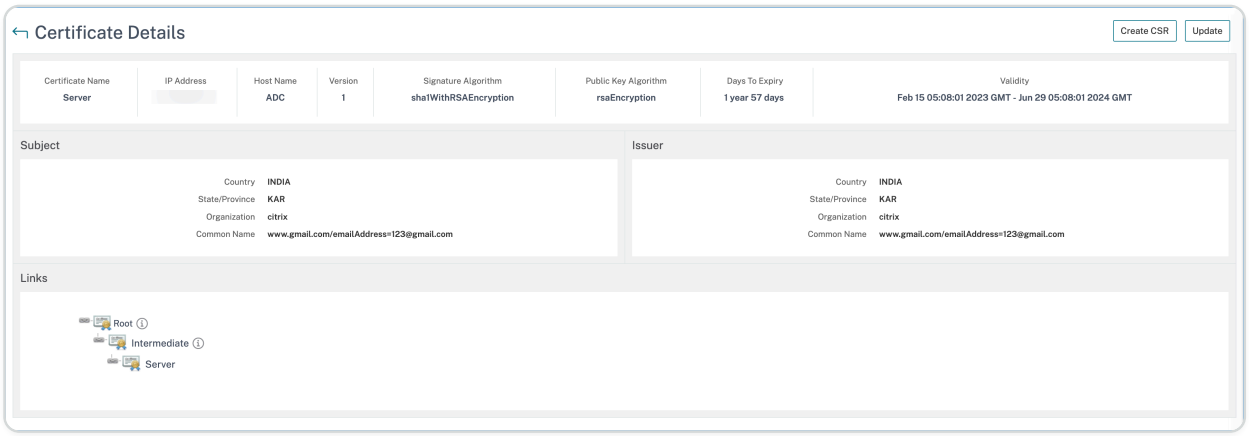
View SSL certificate chain

You can view the complete chain of links for a certificate including the intermediate certificates up to the root CA certificate.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To view a certificate chain:

1. Navigate to **Infrastructure > SSL Dashboard** and click the SSL certificates in any tile.
2. In the **SSL Certificates** page, select a certificate and click **Details**. The certificate chain is displayed under **Links**.



Set up notifications for SSL certificate expiry

As a security administrator, you can configure notifications when the certificates are about to expire and to include information about which NetScaler instances use those certificates. By enabling notifications, you can renew your SSL certificates on time.

For example, you can set an email notification to be sent an email distribution list 30 days before your certificate is due to expire.

To set up notifications from NetScaler Console:

1. In NetScaler Console, navigate to **Infrastructure > SSL Dashboard**.
2. On the **SSL Dashboard** page, click **Settings**.
3. On the **Settings** page, click the **General**.
4. In the **Notification Settings** section, specify when to send the notification in terms of number of days, prior to the expiration date.
5. Choose the type of notification you want to send. Select the notification type and the distribution list from the menu. The notification types are as follows:

    - **Email** – Specify a mail server and profile details. An email is triggered when your certificates are about to expire.
    - **Slack** - Specify a slack profile. A notification is sent when your certificates are about to expire.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **PagerDuty** - Specify a PagerDuty profile. Based on the notification settings configured in your PagerDuty portal, a notification is sent when your certificates are about to expire.
- **ServiceNow** - A notification is sent to the default ServiceNow profile when your certificates are about to expire.

IMPORTANT

Ensure Citrix Cloud ITSM Adapter is configured for ServiceNow and integrated with NetScaler Console. For more information, see Integrate NetScaler Console with ServiceNow instance.

6. Click **Save and Exit**.

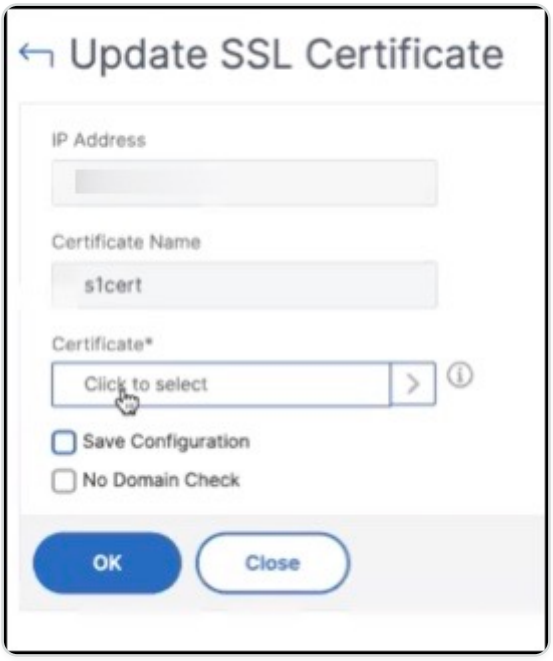
Update an installed certificate

After you receive a renewed certificate from the certificate authority (CA), you don't have to log on to individual NetScaler instances to update the certificates. You can update the existing certificates in NetScaler Console with certificates from the certificate store.

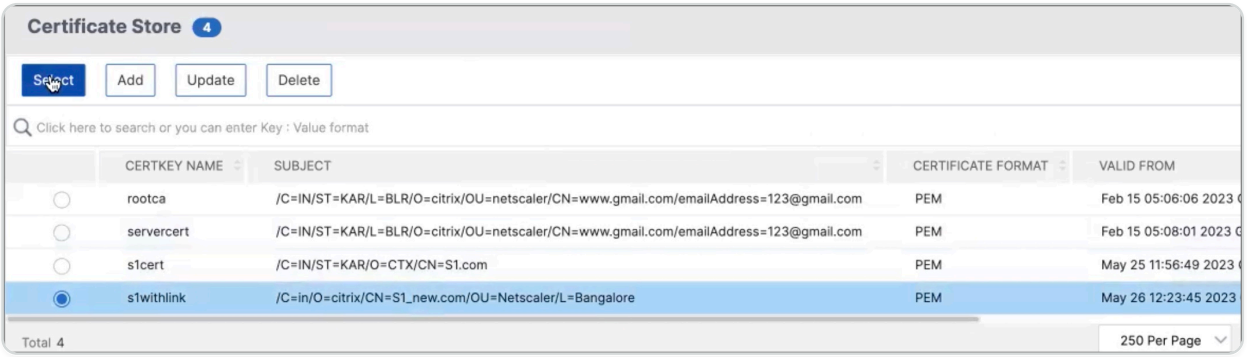
To update an SSL certificate from NetScaler Console:

1. In NetScaler Console, navigate to **Infrastructure > SSL Dashboard**.
2. Click any of the graphs to see the list of SSL certificates.
3. In the **SSL Certificates** page, select a certificate and click **Update**. Alternatively, click the SSL certificate to view its details, and then click **Update** in the upper-right corner of the **SSL Certificate** page.
4. In the **Update SSL Certificate** page, select **Certificate** to display the **Certificate Store** page.

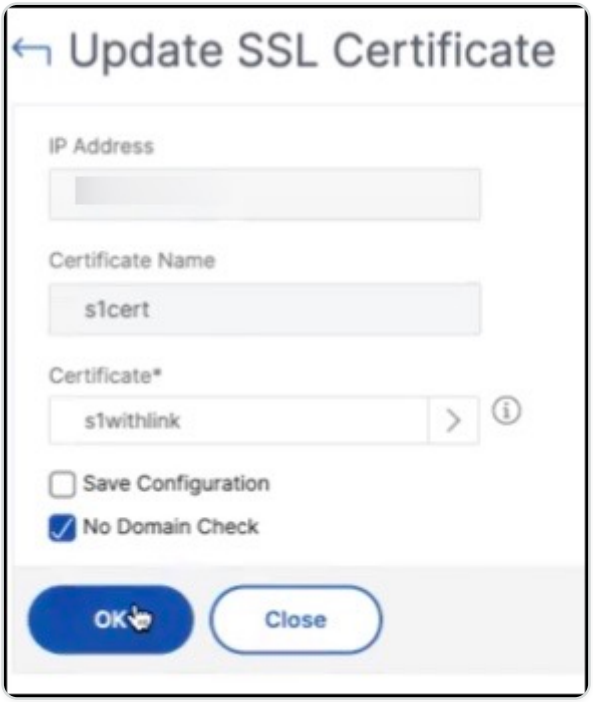
© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. In the **Certificate Store** page, select the certificate file you want to add. Click **Select**.



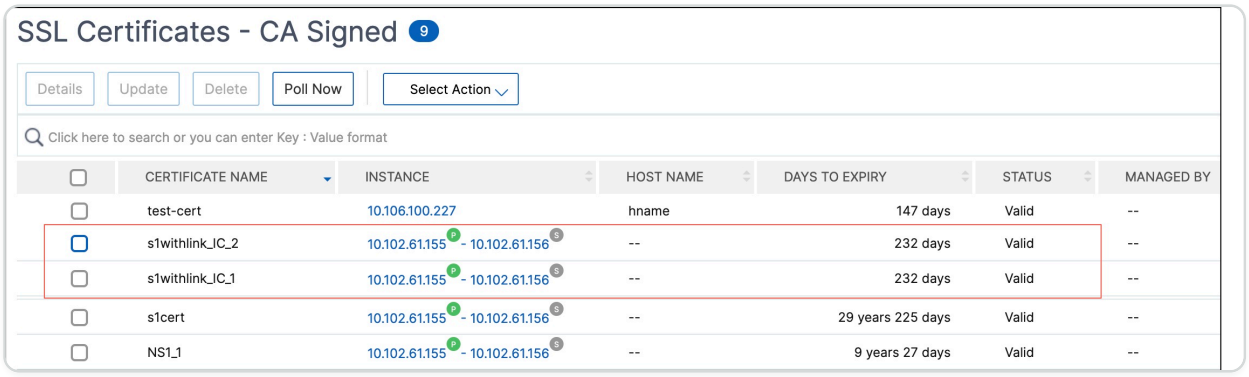
6. If the domain name of the new certificate does not match the old certificate, and you want the server to host the new domain, select **No Domain Check**.



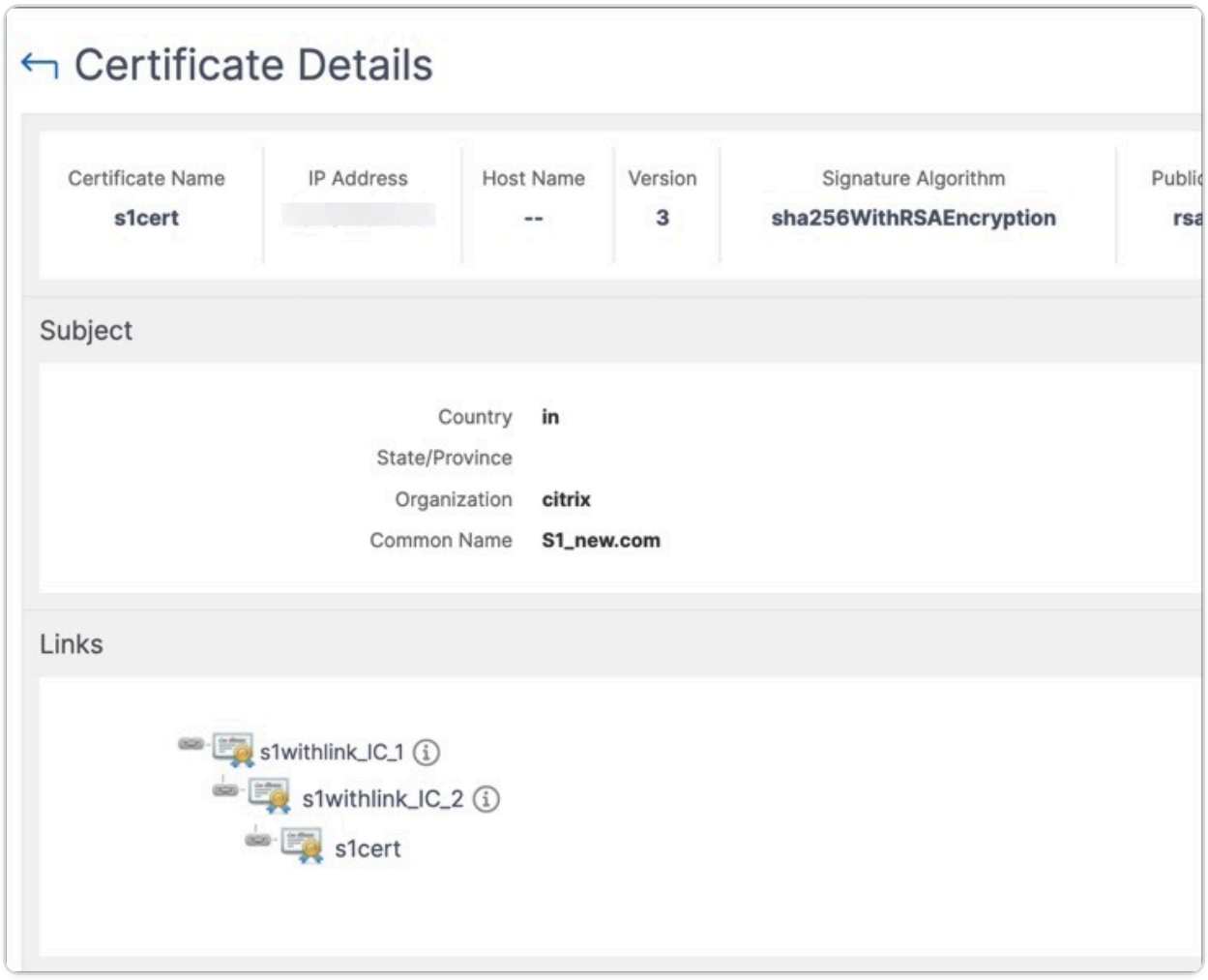
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Click **OK**. All the SSL virtual servers to which this certificate is bound are automatically updated.

When you update an existing SSL certificate with a certificate chain from the certificate store, the existing certificate is updated with the linked certificates.



Select the certificate and click **Details** to view the certificate chain.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Install SSL certificates on a NetScaler instance

Before installing SSL certificates on NetScaler instances, ensure that the certificates are issued by trusted CAs. Also, ensure that the key strength of the certificate keys is 2,048 bits or higher and that the keys are signed with secure signature algorithms.

To install an SSL certificate from another NetScaler Instance:

You can also import a certificate from a chosen NetScaler instance and apply it to other targeted NetScaler instances from the NetScaler Console GUI.

1. Navigate to **Infrastructure > SSL Dashboard**.
2. In the upper-right corner of the SSL dashboard, click **Install**.
3. On the **Install SSL Certificate on NetScaler Instances** page, specify the following parameters:
    a. Certificate Source

        Select the option to **Import from Instance**.

        - Choose the **Instance** that you want to import the certificate from.
        - Choose the **Certificate** from the list of all SSL certificate files on the instance.

    b. Certificate Details

        - **Certificate Name**. Specify a name for the certificate key.
        - **Password**. Password to encrypt the private key. You can use this option to upload encrypted private keys.
4. Click **Select Instances** to select the NetScaler instances on which you want to install your certificates.
5. Click OK.

To install an SSL certificate from NetScaler Console:

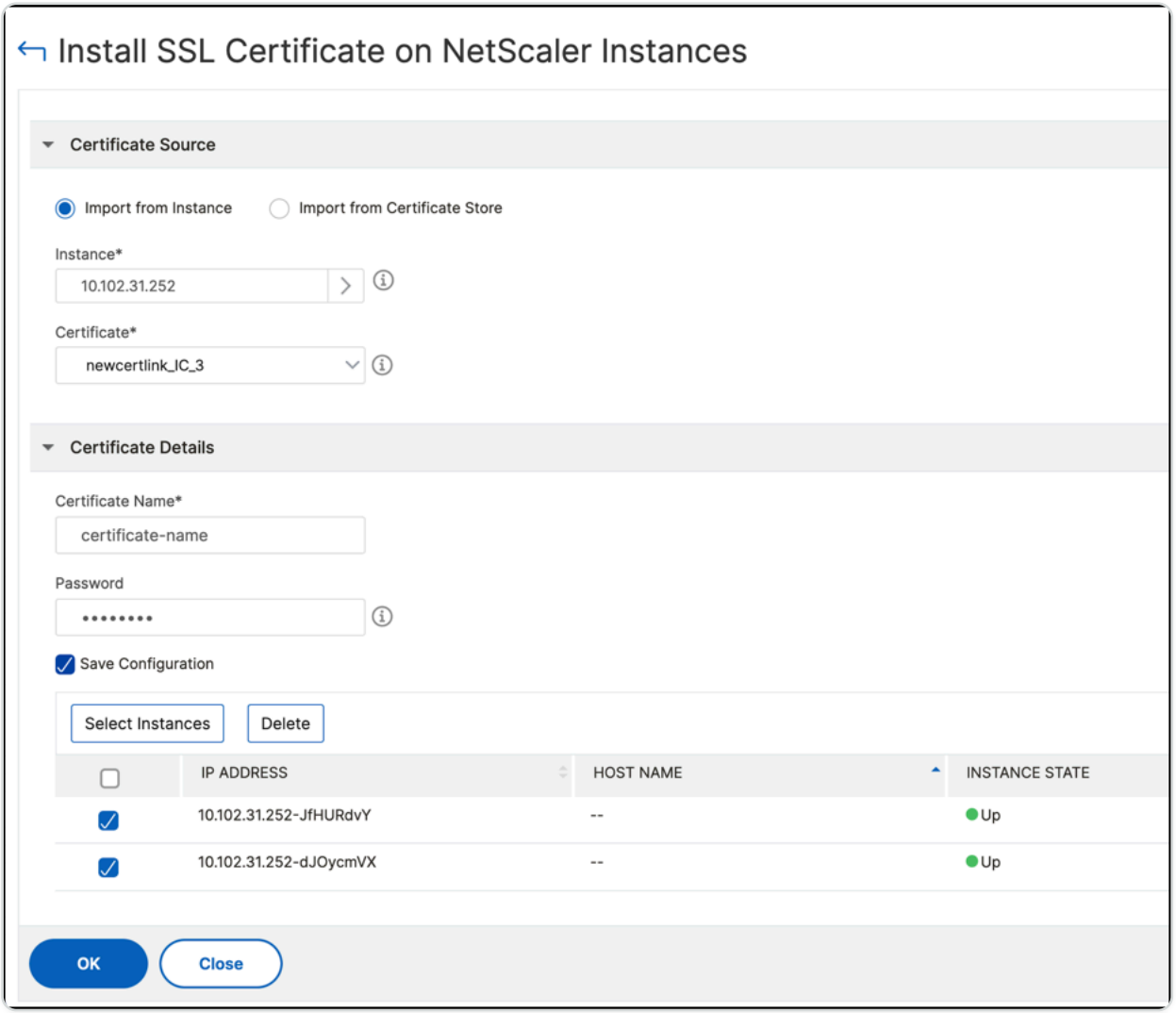
1. Navigate to **Infrastructure > SSL Dashboard**.
2. In the upper-right corner of the dashboard, click **Install Certificate**.
3. On the **Install SSL Certificate on NetScaler Instance** page, specify the following parameters:

    - **Certificate File** - Upload an SSL certificate file by selecting either **Local** (your local machine) or **Appliance** (the certificate file must be present on the NetScaler instance).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Key File** - Upload the key file.
- **Certificate Name** – Specify a name for the certificate key.
- **Password** - Password to encrypt the private key. You can use this option to upload encrypted private keys.
- **Select Instances** - Select the NetScaler instances on which you want to install your certificates.

4. To save the configuration for future use, select the **Save Configuration** check box.
5. Click **OK**.



Create a Certificate Signing Request (CSR)

A Certificate Signing Request (CSR) is a block of encrypted text that is generated on the server on which the certificate will be used. It contains information that is included in the certificate such as the name of your organization, common name (domain name), locality, and country.

To create a CSR using NetScaler Console:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. In NetScaler Console, navigate to **Infrastructure > SSL Dashboard**.
2. Click any of the graphs to see the list of installed SSL certificates, and then select the certificate for which you want to create a CSR and select **Create CSR** from the **Select Action** drop-down list.
3. On the **Create Certificate Signing Request (CSR)** page, specify a name for the CSR.
4. Do one of the following:

   - **Upload a key** - Select the **I have a Key** option. To upload your key file, select either **Local** (your local machine) or **Appliance** (the key file must be present on the NetScaler Console virtual instance).
   - **Create a key** - Select the **I do not have a Key** option, and then specify the following parameters:

OPTIONS	DESCRIPTION
Encryption Algorithm	Type of key. For example, RSA.
Key File Name	Name for your file in which the RSA key is stored.
Key Size	Key size in bits.
Public Exponent Value	Choose either **3** or **F4** from the drop-down list provided. This value is part of the cipher algorithm that is required to create your RSA key.
Key Format	Be default PEM is selected. PEM is the recommended key format for your SSL certificate.
PEM Encoding Algorithm	In the drop-down list, select the algorithm (**DES** or **DES3**) that you want to use to encrypt the generated RSA key. If you select this algorithm, you must provide a PEM Passphrase.
PEM Passphrase	If you've chosen the PEM Encoding Algorithm, enter a passphrase.
Confirm PEM Passphrase	Confirm your PEM passphrase.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

A new key is created. Navigate to **Infrastructure > SSL Dashboard**, select **View Files on NetScaler Console** from the list, and then select the **SSL Keys** tab to view the key.

5. Click **Continue**.
6. On the following page, provide more details.

   Most fields have default values extracted from the subject of the selected certificate. The subject contains details such as the common name, organization name, state, and country.

   In the **Subject Alternative Name** field, you can specify multiple values, such as domain names and IP addresses with a single certificate. The Subject Alternative names help you secure multiple domains with a single certificate.

   Specify the domain names and IP addresses in the following format:

   ```
   DNS:<Domain name>, IP:<IP address>
   ```

   For example, `10.0.0.1` is an IP address and `www.example.com` is a domain name.

   Review the fields and click **Continue**.

NOTE

Most CAs accept certificate submissions by email. The CA returns a valid certificate to the email address from which you submit the CSR.

Link and unlink SSL certificates

You create a certificate bundle by linking multiple certificates together. To link a certificate to another certificate, the issuer of the first certificate must match the domain of the second certificate. For example, if you want to link certificate A to certificate B, the "issuer" of certificate A must match the "domain" of certificate B.

To link one SSL certificate to another certificate using NetScaler Console:

1. In NetScaler Console, navigate to **Infrastructure > SSL Dashboard**.
2. Click any of the graphs to see the list of SSL certificates.
3. Select the certificate that you want to link, and then select **Link** from the **Select Action** drop-down list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. From the list of matched certificates, select the certificate to which you want to link, and then click **OK**.

> **NOTE**
>
> If a matching certificate is not found, the following message is displayed: No certificate found to link.

To unlink an SSL certificate using NetScaler Console:

1. In NetScaler Console, navigate to **Infrastructure > SSL Dashboard**.
2. Click any of the graphs to see the list of SSL certificates.
3. Choose either of the linked certificates that are linked, and then select **Unlink** from the **Select Action** drop-down list.
4. Click **OK**.

> **NOTE**
>
> If the selected certificate is not linked to another certificate, the following message is displayed: Certificate does not have any CA link.

Configure an enterprise policy

You can configure an enterprise policy and add all trusted CAs, secure signature algorithms, and select the recommended key strength for your certificate keys in NetScaler Console. If any of the certificates installed on your NetScaler instance have not been added to the enterprise policy, the SSL certificate dashboard displays the issuer of those certificates as Not Recommended.

Also, if the certificate key strength does not match the recommended key strength in the enterprise policy, the SSL certificate dashboard displays the strengths of those keys as Not Recommended.

To configure an enterprise policy on NetScaler Console:

1. In NetScaler Console, navigate to **Infrastructure > SSL Dashboard**, and then click **Settings**.
2. On the **Settings** page, click the **Enterprise Policy** icon to add all trusted CAs, secure signature algorithms, and select the recommended key strength for your certificates and keys. Supported key strengths are 512, 1024, 2048, 3072, and 4096 bits.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Recommended key strengths** - Denotes the algorithm security and the number of bits in a key.
- **Recommended Signature Algorithms** - Denotes the signed tokens issues for the applications.
- **Recommended Trusted CA** - Denotes the trusted entity that issues the digital certificates. Click the **+** icon to add more entities.
- **Recommended SSL protocols** - Denotes the TLS/SSL versions.

3. Click **Finish** or **Save and Exit** to save your enterprise policy.

> **NOTE**
>
> The SSL dashboard displays only the **Signature Algorithms** that are selected through the **Settings** option and others are displayed as **Not Recommended**.

Poll SSL certificates from NetScaler instances

NetScaler Console automatically polls SSL certificates once every 24 hours by using NITRO calls and the Secure Copy (SCP) protocol. You can also manually poll the SSL certificates to discover newly added SSL certificates on the NetScaler instances. Polling all the NetScaler instances SSL certificates places a heavy load on the network.

Instead of polling all the NetScaler instances SSL certificates, you can manually poll only the SSL certificates of a selected instance or instances.

To poll SSL certificates on NetScaler instances:

1. Navigate to **Infrastructure > SSL Dashboard**.
2. On **SSL Dashboard** page, in the top right-hand corner, click **Poll Now**.
3. The **Poll Now** page pops up, giving you the option to poll all NetScaler instances in the network or poll selected instances.
    a. To poll the SLL certificates of all the NetScaler instances, select the **All Instances** tab and click **Start Polling**.
4. To poll specific instances, select the **Select Instances** tab, select the instances from the list, and click **Poll Now**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use the NetScaler Console certificate store to manage SSL certificates

NetScaler Console certificate store helps you to store and manage your SSL certificates in one location. You can later use the stored certificates to configure NetScaler settings.

The certificate store allows you to add, update, and delete SSL certificates. You can also use the certificate store to import a certificate from a NetScaler instance and apply it to other targeted NetScaler instances.

Add SSL certificates to the certificate store

1. Navigate to **Infrastructure > SSL Dashboard > Certificate Store**. Click **Add**.
2. On the **Add Certificate** page, enter the following details:

    - **Certkey Name** - Enter a name for the certificate. The name must have only ASCII alphanumeric, underscore, and hyphen characters and must be fewer than 30 characters. You cannot change the name after the certificate is created.
    - **Certificate File** - Browse to your local drive and upload the certificate file.
    - **Key File** - Upload the key file from your local computer.
    - **Password** - If you have an encrypted private key in PEM format, type the passphrase that was used to encrypt the private key.
    - **Add Certificate Chain** - Select this option to add the certificate in a certificate chain.
    - **Certificate Chain** - Browse to your local drive and upload the certificate file.
    - Click **Create**.

Update SSL certificates in the certificate store

1. Navigate to **Infrastructure > SSL Dashboard > Certificate Store**. Select the certificate that you want to update and click **Update**.
2. On the **Update Certificate** page, enter the following details:

    - **Certkey Name** - Displays the name of the certificate you selected to update.
    - **Certificate File** - To update the certificate file, upload a certificate file.
    - **Key File** - To update the key file, upload a key file from your local computer.
    - **Password** - If you have an encrypted private key in PEM format, type the passphrase that was used to encrypt the private key.
    - **Add Certificate Chain** - Select this option to add the certificate in a certificate chain.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Certificate Chain** - Browse to your local drive and upload the certificate file.
- Click **OK**.

Delete SSL certificates from the certificate store

1. Navigate to **Infrastructure > SSL Dashboard > Certificate Store**. Click **Delete**.
2. When prompted, click **Yes** to delete the certificate.

Install SSL certificates on NetScaler® instances

1. Navigate to **Infrastructure > SSL Dashboard > Certificate Store**. Select the certificate that you want to install on a NetScaler instance.
2. In the **Install SSL Certificate on NetScaler Instances** page, enter the following details:

   a. **Certificate Source**

   - **Certificate** - Displays the name of the certificate you selected.

   b. **Certificate Details**

   - **Certificate Name** - Displays the name of the certificate.
   - **Save Configuration** - Select this option to save the NetScaler configuration. The NetScaler configuration is saved after the certificate is installed.

3. Click **Select Instances** to select the NetScaler instances on which you want to install your certificates.

Click **OK**.

Import certificates from NetScaler instances

1. Navigate to **Infrastructure > SSL Dashboard > Certificate Store**. Click **Import NetScaler Certificates**.
2. In the **Import NetScaler Certificates** page, you can select one of the following tabs:

   - **Import NetScaler Certificates** - Click **Start Polling** to poll all the SSL certificates on all the NetScaler instances.
   - **Select Instances** - Select a NetScaler instance and click **Import NetScaler Certificates** to poll SSL certificates on only the selected NetScaler instance.

   After polling, the SSL certificates and key files are downloaded and added to the certificate store.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The import operation fails for certificates if identical certificate names exist in the store. However, the import operation continues polling the remaining certificates and adds NetScaler certificates, if available, to the store.

Update server certificates without intermediate uploads

You can renew certificates without the repetitive task of re-uploading intermediate certificates. This enhancement reduces manual workload and minimizes the risk of configuration errors.

Effortless renewals:

NetScaler Console preserves the existing certificate chain during an update by default. This ensures that your chain remains intact and valid, even when you only upload a new server-level certificate.

Key improvements:

- **Reduced complexity**: Eliminates mandatory intermediate uploads during standard server certificate updates.
- **Safety first**: Automatic chain preservation prevents "chain breakage", a common cause of SSL handshake errors.

To update server certificates without intermediate uploads

1. Navigate to **Infrastructure > SSL Dashboard > Certificate Store**.
2. Select the certificate that you want to update and click **Update**.
3. **Overwrite Existing Certificate Chain** - Select this option if your renewal requires changes to the intermediate chain:
    - **With a bundle**: Replaces the existing chain with the newly uploaded bundle.
    - **Without a bundle**: Removes the current certificate chain entirely.
4. **Add Certificate Chain** - Select this option to manually upload and append intermediate certificates if they are not included in your primary server certificate file.

Examples

The final certificate structure depends on your existing certificate's chain status and the options that you select during the update:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SCENARIO A: EXISTING CERTIFICATE HAS NO CHAIN

UPDATE ACTION	RESULT
New uploaded certificate does not include a chain	The server certificate is updated. No intermediate chain is added.
New uploaded certificate includes a chain	The server certificate is updated, and the new intermediate chain is attached.

SCENARIO B: EXISTING CERTIFICATE HAS A CHAIN

UPDATE ACTION	RESULT
New uploaded certificate includes a chain (Overwrite Existing Certificate Chain is enabled)	The server certificate is updated, and the existing intermediate chain is replaced with the new chain.
New uploaded certificate does not include a chain (Overwrite Existing Certificate Chain is enabled)	The server certificate is updated, and the existing intermediate chain is explicitly removed.

Configuration jobs

NetScaler Console configuration management process ensures the proper replication of configuration changes, system upgrades, and other maintenance activities across multiple NetScaler instances in the network.

NetScaler Console allows you to create configuration jobs that help you to perform all these activities with ease on several devices as a single task. Configuration jobs and templates simplify the most repetitive administrative tasks to a single task on NetScaler Console. A configuration job contains a set of configuration commands that you can run on one or multiple managed devices.

Configuration Jobs can either use SSH commands to do configuration commands or use SCP to do file copy from either locally or to another appliance, for example, we can schedule a HA-failover or HA-upgrade.

You can create a configuration job by using one of the following four options in NetScaler Console. Use one of these to create a reusable source of commands and instructions to the system to run a configuration job.

1. Configuration Template

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Instance
3. File
4. Record and Play

Configuration Template

You can create configuration templates while creating a job and saving a set of configuration commands as a template. When you save these templates on the Create Jobs page, they are automatically displayed on the Create Template page. For more information, see How to Use the Master Configuration Template on NetScaler Console.

NOTE

The **Rename** option is disabled for the default configuration templates. However, you can rename custom configuration templates.

You can use one of the following templates:

Configuration Editor: You can use the configuration editor to type in CLI commands, save the configuration as a template, and use it to configure jobs.

Inbuilt Template: You can choose from a list of configuration templates. These templates provide the syntaxes of the CLI commands and allow you to specify values for the variables. The inbuilt templates are listed, with their descriptions in the table below. You can schedule a job by using the built-in template option. A job is a set of configuration commands that you can run on one or more managed instances. For example, you can use the built-in template option to schedule a job to configure syslog servers. You can also choose to run the job immediately or schedule the job to be run at a later stage.

For more information, see How to Use Configuration Templates to Create Audit Templates

Instance

You can perform a single-bundle upgrade of your NetScaler SDX instances running NetScaler release 11.0 and later. To perform a single-bundle upgrade, you use a built-in task in NetScaler Console. You can also upgrade a NetScaler instance by extracting the running configuration or a saved configuration and running the commands on another NetScaler instance of the same type. This upgrade allows you to replicate the configuration of one instance on the other.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

File

You can upload a configuration file from your local machine and create jobs.

Advantages of using a file

- You can use any text file to create a reusable source of configuration commands.
- Any kind of formatting is not required.
- The file can be saved on your local machine.

You can either create and save a new file or import an existing file, and run the commands.

Record and Play

Using Create job you can either enter your own CLI commands, or you can use the record and play button to get commands from a NetScaler session. When you run the job, changes in the ns.conf on the selected instance are recorded and copied to NetScaler Console. See, How to Use Record-and-Play to Create Configuration Jobs.

Export the report of this dashboard

To export the report of this page, click the **Export** icon on the top right side of this page. On the **Export** page, you can do one of the following:

1. Select **Export Now** tab. To view and save the report in PDF, JPEG, PNG, or CSV format.
2. Select **Schedule Export** tab. To schedule the report daily, weekly, or monthly and send the report over an email or a slack message.

NOTE

- If you select **Weekly** recurrence, ensure that you select the weekdays on which you want the report to be scheduled.
- If you select **Monthly** recurrence, ensure that you enter all the days that you want the report to be scheduled separated by commas.

Related Articles

- How to Use SCP (put) Command in Configuration Jobs
- How to Use Variables in Configuration Jobs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- How to Create Configuration Jobs from Corrective Commands

Create a configuration job

A job is a set of configuration commands that you can create and run on one or more multiple managed instances.

You can create jobs to make configuration changes across instances. You can replicate configurations on multiple instances on your network and record and play configuration tasks using the NetScaler Console GUI and convert it into CLI commands.

You can use the Configuration Jobs feature of NetScaler Console to create a configuration job, send email notifications, and check execution logs of the jobs created.

To create a configuration job on NetScaler Console:

1. Navigate to the **Infrastructure > Configuration > Configuration Jobs**.
2. Click **Create Job**.
3. On the **Create Job** page, under the **Select Configuration** tab, specify the Job Name and select the **Instance Type** from the list.
4. In the **Configuration Source** list, select the configuration job template that you want to create. Add the commands for the selected template.
    - You can either enter the commands or import the existing commands from the saved configuration templates.
    - You can also add multiple templates of different types in the Configuration editor while creating a job in the Configuration Jobs.
    - From the **Configuration Source** list, select the different templates and then drag the templates into the configuration editor. The template types can be **Configuration Template**, **In built Template**, **Master Configuration**, **Record and Play**, **Instance** and **File**.

NOTE

If you add the Deploy Master Configuration Job template for the first time, add a template of different type, then the whole job template becomes a Master Configuration type.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can also rearrange and reorder the commands in the configuration editor. You can move the command from one line to another by dragging and dropping the command line. You can also move or rearrange the command line from one line to any target line by simply changing the command line number in the text box. You can also rearrange and reorder the command line while editing the configuration job.

You can define variables that enable you to assign different values for these parameters or run a job across multiple instances. You can review all the variables that you have defined while creating or editing a configuration job in a single consolidated view. Click the **Preview Variables** tab to preview the variables in a single consolidated view that you have defined while creating or editing a configuration job.

You can customize rollback commands for every command on the configuration editor. To specify your customized commands, Enable the custom rollback option.

IMPORTANT

For custom rollback to take effect, complete the **Create Job** wizard. And in the **Execute** tab, select the **Rollback Successful Commands** option from the **On Command Failure** list.

5. In the **Select Instances** tab, select the instances on which you want to run the configuration audit.

   a. In a NetScaler high-availability pair, you can run a configuration job local to a primary or a secondary node. Select on which node you want to run the job.

      - **Execute on primary nodes** - Select this option to run the job only on primary nodes.
      - **Execute on secondary nodes** - Select this option to run the job only on secondary nodes.

      You can also choose both primary and secondary node to run the same configuration job. If you do not select either primary or secondary node, automatically the configuration job runs on the primary node.

   b. Click **Add Instances** and select the instances from the list. Click **OK**.

   c. Click **Next**.

6. In the **Specify Variable Values** tab, you have two options:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Download the input file to enter the values for the variables that you have defined in your commands, and then upload the file to the NetScaler Console server.
b. Enter common values for the variables that you have defined for all instances
c. Click **Next**.

7. Evaluate and verify the commands to be run on each instance on the **Job Preview** tab. This tab also display the rollback commands if specified on the **Select Configuration** tab.
8. In the **Execute** tab, choose to either run your job now, or schedule to run the job later.

   Also, select one of the following actions from the **On Command Failure** list that NetScaler Console must perform if the command fails:

   - **Ignore error and continue**: NetScaler Console ignores the failed command and runs the remaining commands for the selected instance.

     NOTE

     This action does not allow you to abort a configuration job that is in progress.

   - **Stop further execution**: NetScaler Console stops the remaining commands if any command fails during execution.
   - **Rollback successful commands**: NetScaler Console restores the successfully run commands if any command fails during execution.

     If the custom rollback is enabled, the NetScaler Console runs the corresponding rollback commands for the failed commands.

9. Click **Finish**.

To send an email and Slack notification for a job:

An email and Slack notification is now sent every time a job is run or scheduled. The notification includes details such as the success or failure of the job along with the relevant details.

1. Navigate to **Infrastructure > Configuration > Configuration Jobs**.
2. Select the job that you want to enable email and Slack notification and click **Edit**.
3. In the **Execute** tab, go to the **Receive Execution Report Through** pane:

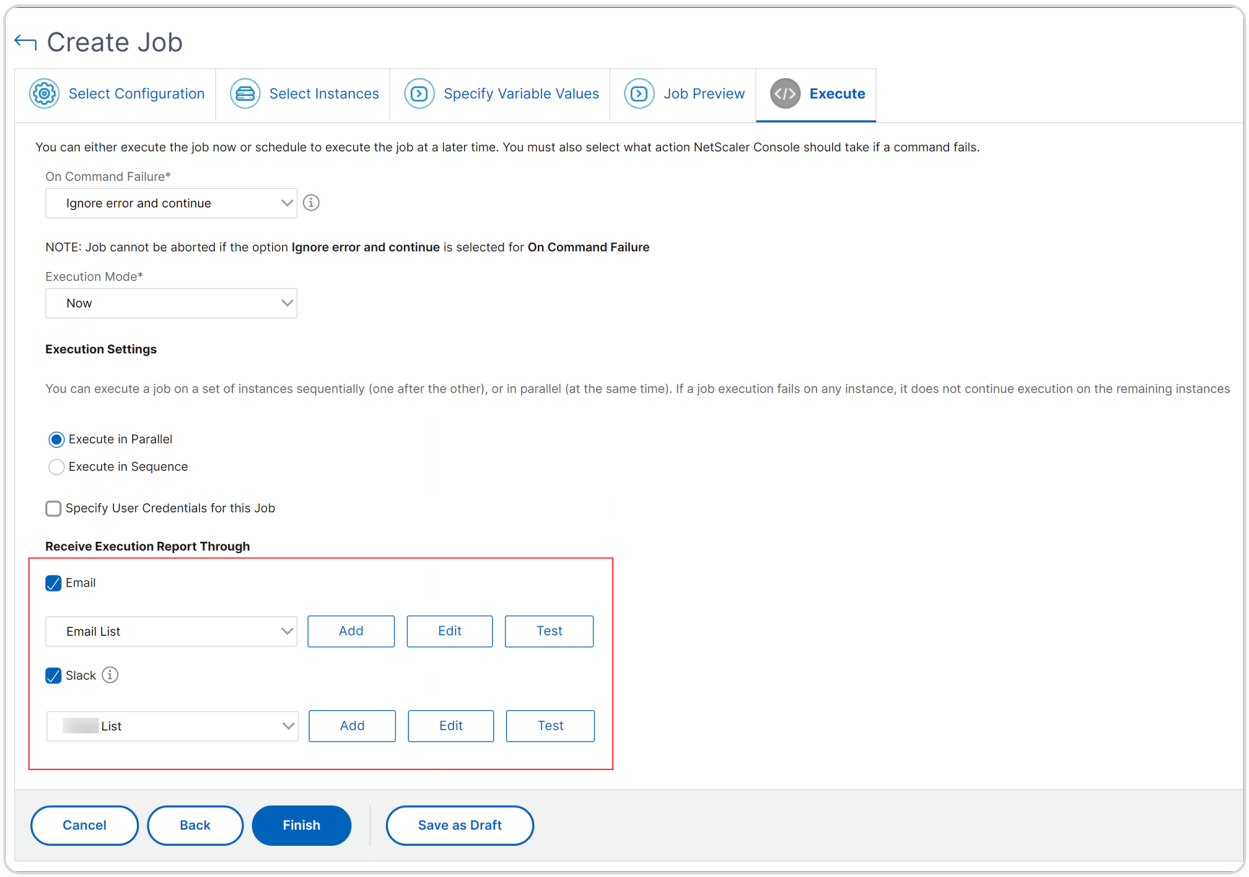
   - Select the **Email** check box and choose the email distribution list to which you want to send the execution report.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you want to add an email distribution list, click **Add** and specify the email server details.

- Select the **Slack** check box and choose the slack channel to which you want to send the execution report.

  If you want to add a Slack profile, click **Add** and specify the **Profile Name**, **Channel Name**, and **Token** of the required Slack channel.



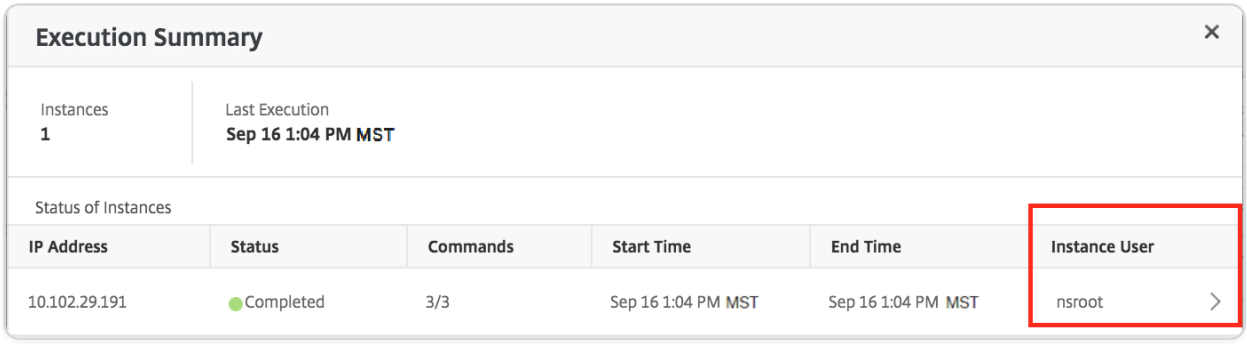
4. Click **Finish**.

To view execution summary details:

1. Navigate to **Infrastructure > Configuration > Configuration Jobs**.
2. Select the job that you want to view the execution summary and click **Details**.
3. Click **Execution Summary** to see:

   - The status of the instance on the job that was run
   - The commands run on the job
   - The start and end time of the job, and
   - The instance user's name

© 1997–2026 Citrix Systems, Inc. All rights reserved.



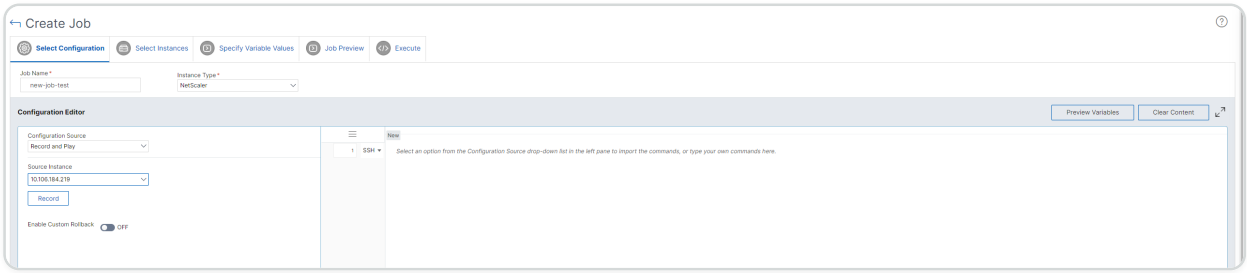
Use record-and-play to create configuration jobs

If you are accustomed to using the NetScaler GUI to configure a NetScaler instance, at times, you might find it difficult to recall the exact CLI commands to create a configuration task and run it on multiple NetScaler instances.

NetScaler Console enables you to record the configuration tasks performed using the GUI of a NetScaler instance and convert it into CLI commands. You can then create a configuration task from these CLI commands and run this task on multiple instances.

To record the GUI configuration and convert it into a configuration task:

1. Navigate to **Infrastructure > Configuration > Configuration Jobs**, and then click **Create Job**.
2. Specify the job name and the type of instance.
3. From the **Configuration Source** list, select **Record and Play**, and then select the source instance from which you want to record the configuration. Click **Record**.

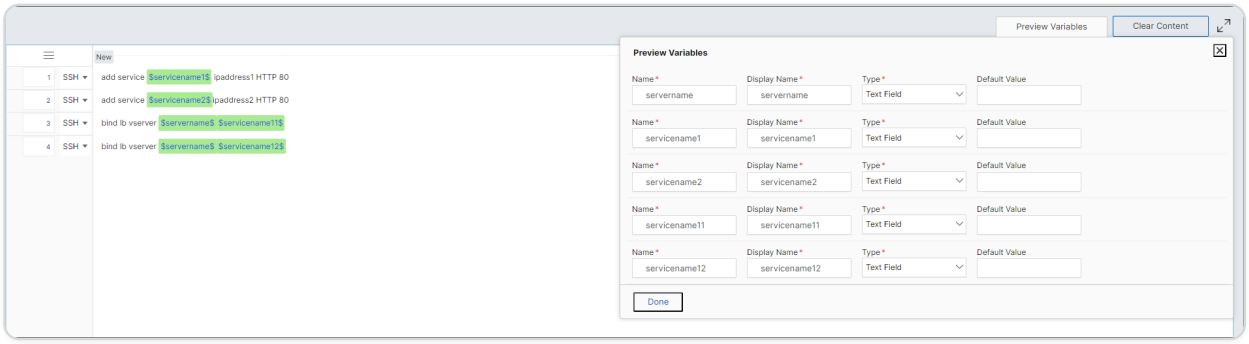


4. The **NetScaler GUI** opens. Configure the features and settings that you want the configuration task to contain. Then, close the NetScaler GUI window and click **Stop** in the **Configuration Editor**. The commands appear as a link in the left pane. Drag the commands to the right pane, and then click **Next**.

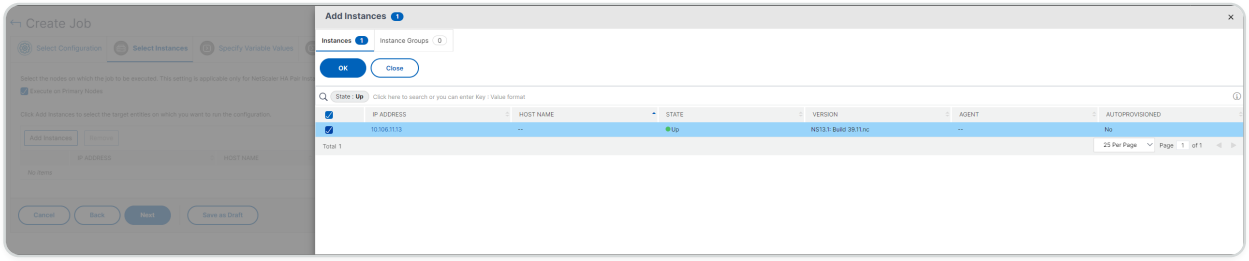
   You can then rearrange and reorder the commands in the configuration editor as appropriate. You can move the command from one line to another by dragging and dropping the command line. You can also move or rearrange the command line from one line to any target line by simply changing the command line number in the text box.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. You can review all the variables that you have defined while creating or editing a configuration job in a single consolidated view.
6. Do one of the following to view all the variables in a single consolidated view:
   - While creating a configuration job, navigate to **Infrastructure > Configuration Jobs**, select **Create Job**. On the **Create Job** page, you can review all the variables that you have added while creating the configuration job.
   - While editing a configuration job, navigate to **Infrastructure > Configuration > Configuration Jobs**, select the Job Name and click **Edit**. On the **Configure Job** page, you can review all the variables that were added while creating the configuration job.
7. You can then click the **Preview Variables** tab to preview the variables in a single consolidated view that you have defined while creating or editing a configuration job.
8. A new pop-up window appears and displays all the parameters of variables such as Name, Display Name, Type, and default value in a tabular format. You can also edit and modify these parameters. Click the **Done** button after you have edited or modified any of the parameters.



9. Click **Add Instances** and select the instances on which you want to run the configuration job. Click **OK**, and then click **Next**.



10. If you have specified variables in the commands, on the **Specify Variable Values** tab, select one of the following options to specify variables for your instances:
    - **Upload input file for variables values**: Click **Download Input Key** File to download an input file. In the input file, enter values for the variables that you have defined in your commands, and then upload the file to the NetScaler Console server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Common variable values for all instances**: Enter values for the variables. The variables vary depending on the selected template.

The input files containing the variables values are persisted (with the same file name) in the configuration jobs. You can view and edit these input files that you have used and uploaded earlier while creating or editing the configuration jobs.

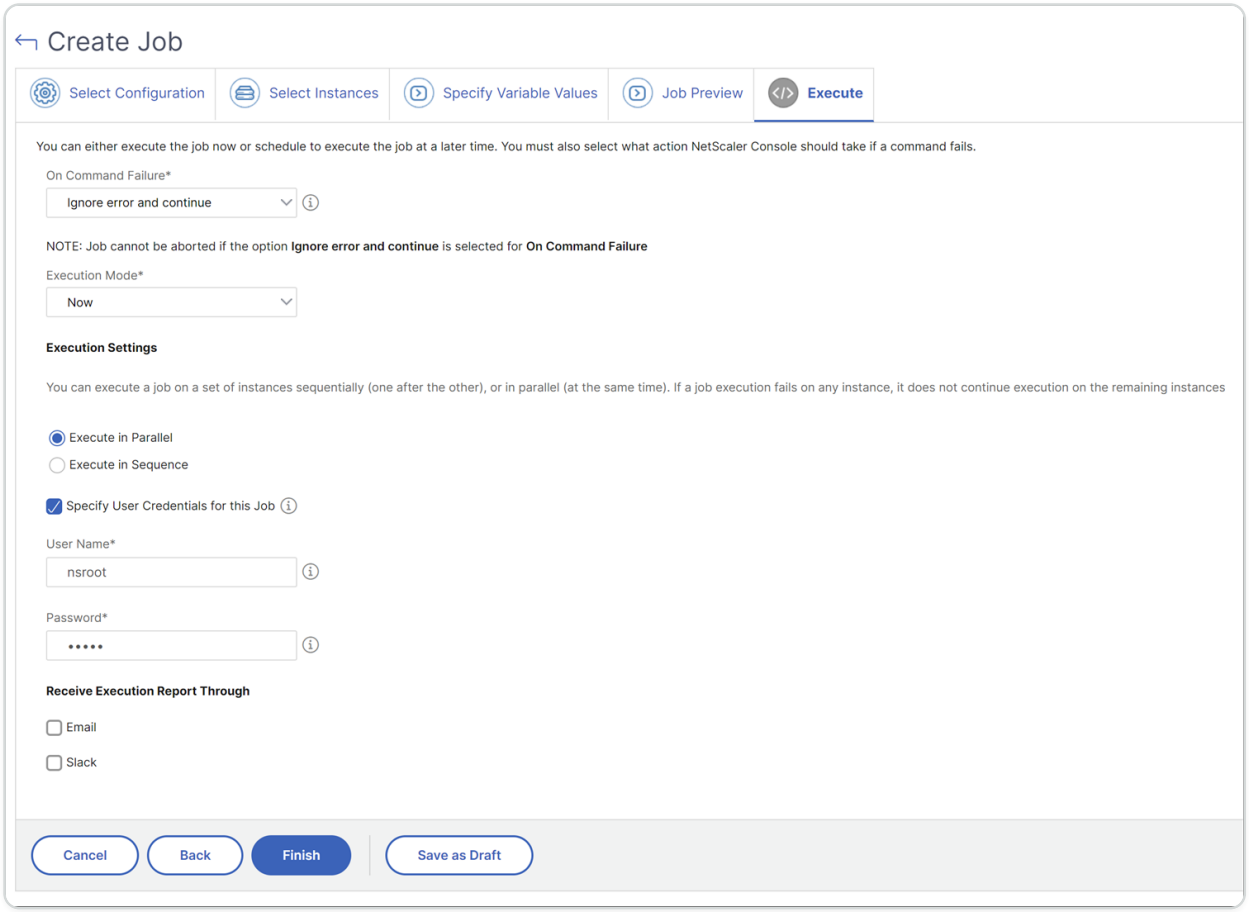
To view the run configuration jobs while creating a configuration job, navigate to **Network** > **Configuration Jobs**, and click **Create Job**. In the **Create Job** page. On the **Specify Variable Values** tab, select the **Common Variable Values for all Instances** option to view the uploaded files. To edit the input files, download the input file and then edit and upload the files (keeping the same file name).

To view the already run configuration jobs while editing a configuration job, navigate to **Network** > **Configuration Jobs**, select the Job Name and click **Edit**. In the **Configure Job** page, on the **Specify Variable Values** tab, select the **Common Variable Values for all Instances** option to view the uploaded files. To edit the input files, download the input file and then edit and upload the files (keeping the same file name).10. On the **Job Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group.

11. On the **Job Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group.
12. On the **Execute** tab, you can choose to run your job now or schedule it to be run later. You can also choose what action NetScaler Console must take if the command fails.

    You can also choose to allow authorized users to run jobs on your managed instances, and you can choose whether to send an email notification regarding the success or failure of the job, along with other details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



13. On the **Jobs** page, you can then view the progress of your configuration task execution on all the instances.

Use configuration jobs to replicate configuration from one instance to multiple instances

You might have configured both load balancing and AppFlow on a NetScaler instance for your deployment. However, now you want to replicate only the AppFlow configuration to other NetScaler instances.

You can use the Configuration Jobs feature of NetScaler Console to extract the AppFlow configuration from a NetScaler instance and replicate it on multiple instances.

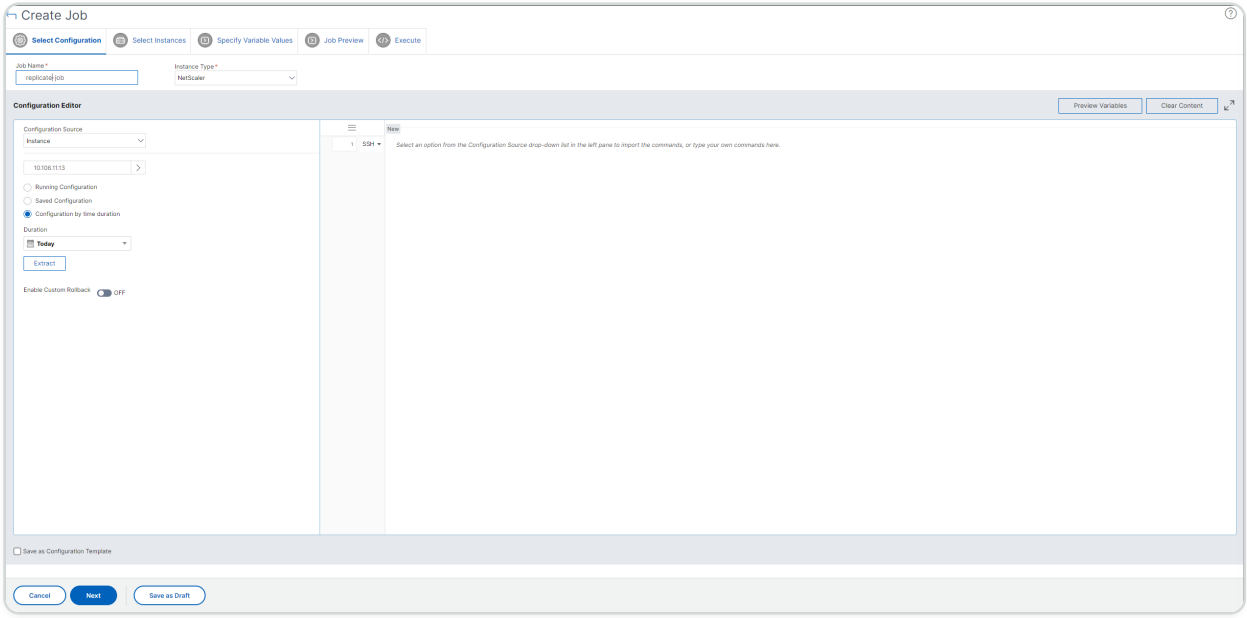
To retrieve and replicate configuration from one instance to other NetScaler Instances:

1. Navigate to **Infrastructure > Configuration > Configuration Jobs**, and then click **Create Job**.
2. Specify the job name and the type of instance.
3. Select **Instance** as the **Configuration Source** and select the source instance whose configuration you want to replicate. Select the type of configuration that you want to extract. If

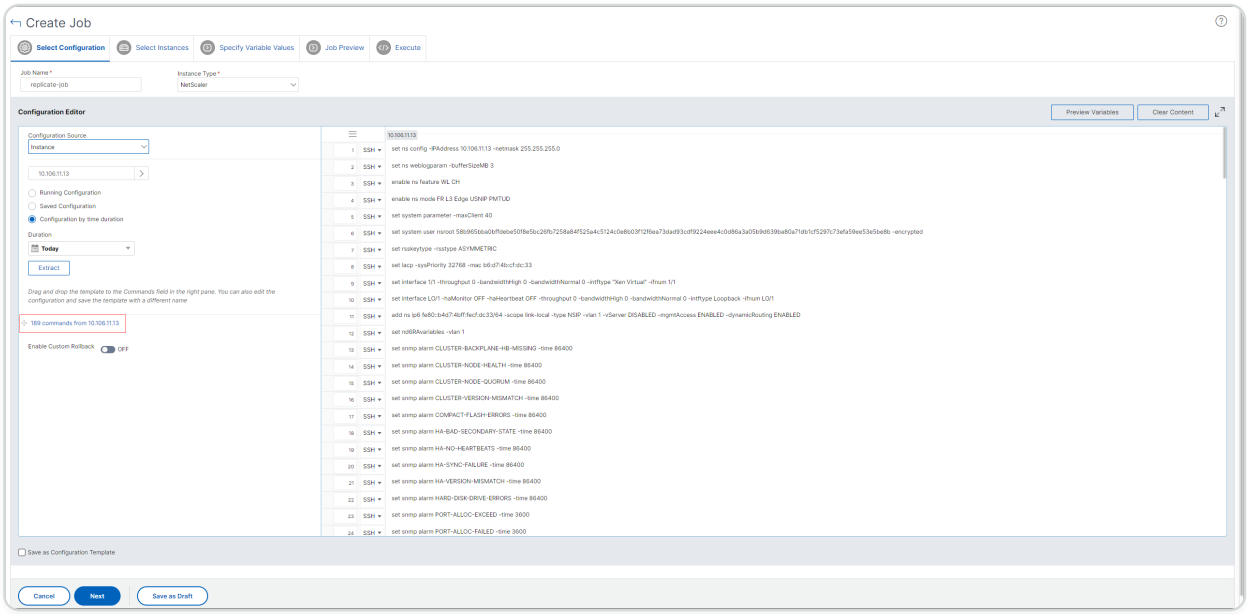
© 1997–2026 Citrix Systems, Inc. All rights reserved.

you select the "Configuration by time duration," set the time period when you had run this configuration, and then click **Extract**.

The number of commands run on that instance in the time duration you selected is displayed on the screen as highlighted in the image below.



4. Drag the commands to the **Commands** field in the right pane.



Retain only the commands related to FEO and manually delete the commands related to load balancing, or commands related to any other configuration, and then click **Next**.

5. Click **Add Instances** and add the instances on which you want to apply the FEO configuration. Click **OK**, and then. click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you have specified variables in the commands, on the Specify Variable Values tab, click **Download Input Key File**. In the downloaded file, specify values for the variables, and then upload the file to NetScaler Console.

On the **Job Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group.

On the **Execute** tab, click **Finish** to run the job on the selected NetScaler instances.

Use variables in configuration jobs

A configuration job is a set of configuration commands that you can run on one or more managed instances. When you run the same configuration on multiple instances, you might want to use different values for the parameters used in your configuration. You can define variables that enable you to assign different values for these parameters or run a job across multiple instances.

For example, consider a basic load balancing configuration where you add a load balancing virtual server, add two services, and bind the services to the virtual server. Now, you might want to have the same configuration on two instances but with different values for the virtual server and services names and IP addresses. You can use the configuration jobs feature to achieve this by using variables to define the names and IP addresses of the virtual server and services.

In this example, the following commands and variables are used:

```
add lb vserver **servername** HTTP **ipaddress portnumber**


add service **servicename1** **ipaddress1** HTTP 80


add service **servicename2** **ipaddress2** HTTP 80


bind lb vserver **servername** **servicename1**


bind lb vserver **servername** **servicename2**
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

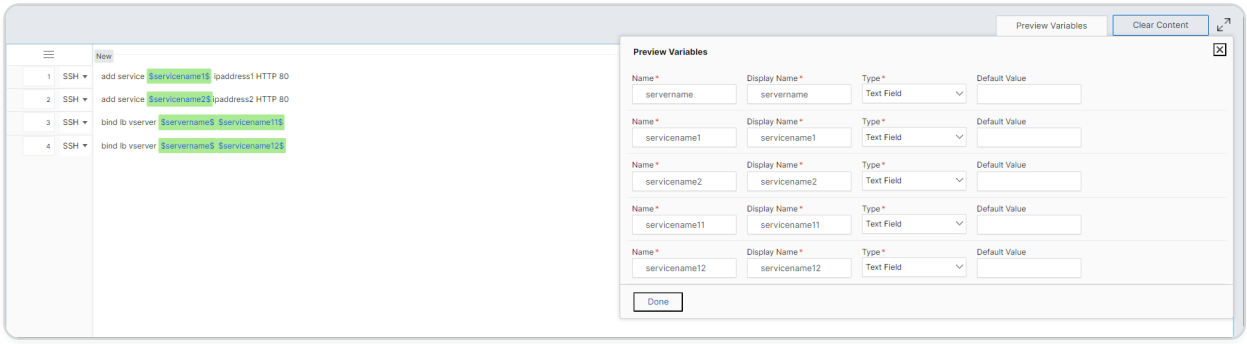
To create a configuration job by defining variables in NetScaler Console:

1. Navigate to **Infrastructure > Configuration > Configuration Jobs**.
2. Click **Create Job**.
3. On the **Create Job** page, select the custom job parameters such as the name of the job, the instance type, and the configuration type.
4. In the Configuration Editor, type in the commands to add a load balancing virtual server, two services, and bind the services to the virtual server. Double-click to select the values that you want to convert to a variable, and then click **Convert to Variable**. For example, select the IP address of the load balancing server `ipaddress`, and click **Convert to Variable**.
5. Once you see dollar signs enclose the variable's value, click the variable to further specify the details of the variable such as name, display name, and type. You can also click the **Advanced** option if you want to further specify a default value for your variable. Click **Save** and then, click **Next**.
6. You can review all the variables that you have defined while creating or editing a configuration job in a single consolidated view.
7. Do one of the following to view all the variables in a single consolidated view:

    - While creating a configuration job, navigate to **Infrastructure > Configuration > Configuration Jobs**, select **Create Job**. On the **Create Job** page, you can review all the variables that you have added while creating the configuration job.
    - While editing a configuration job, navigate to **Network** > **Configuration Jobs**, select the Job Name and click **Edit**. On the **Configure Job** page, you can review all the variables that were added while creating the configuration job.

8. You can then click the **Preview Variables** tab to preview the variables in a single consolidated view that you have defined while creating or editing a configuration job.
9. A new pop-up window appears and displays all the parameters of variables such as Name, Display Name, Type, and default value in a tabular format. You can also edit and modify these parameters. Click the **Done** button after you have edited or modified any of the parameters.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



10. You can then rearrange and reorder the commands in the configuration editor as appropriate. You can move the command from one line to another by dragging and dropping the command line. You can also move or rearrange the command line from one line to any target line by simply changing the command line number in the text box.
11. Select the instances you want to run the configuration job on.
12. In the **Specify Variable Values** tab, select the **Upload input file for variable values** option and then click **Download Input Key File**. In our example, you will need to specify the server name on each instance, the IP addresses of the server and services, port numbers, and the service names. Save the file and upload it. If your values aren't defined accurately, the system might throw an error.
13. The input key file is downloaded to your local system and you can edit it by specifying the variable values for each NetScaler instance you've selected previously and click **Upload** to upload the input key file to NetScaler Console. Click **Next**. The input key file downloads to your local system and you can edit it by specifying the variable values for each NetScaler instance that you have selected previously.

NOTE

In the input key file, the variables are defined at three levels:

- Global level
- Instance-group level
- Instance level

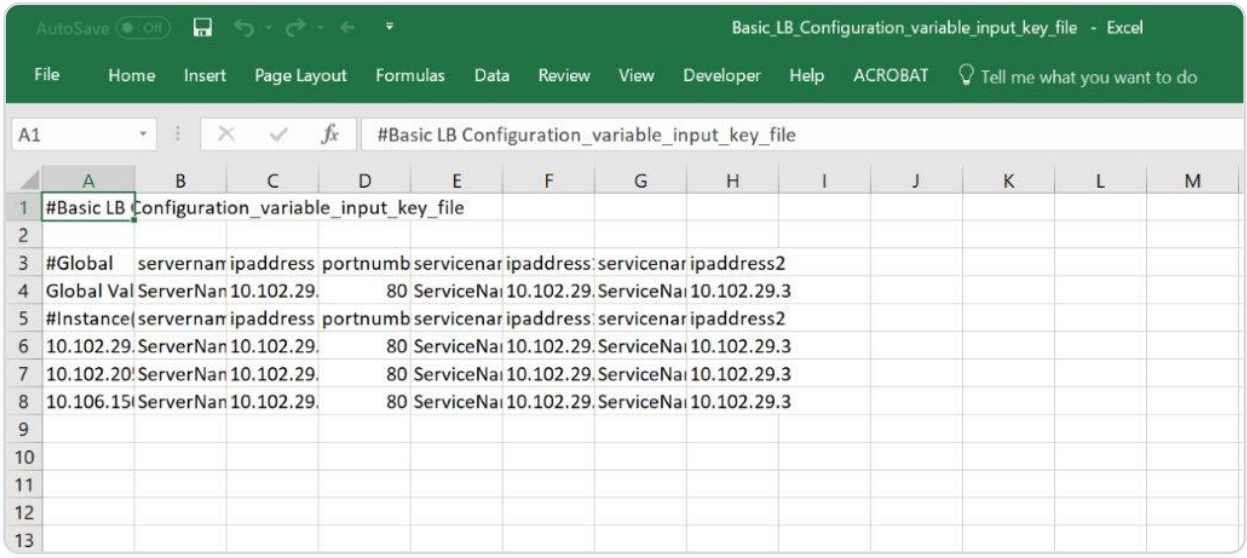
Global variables are variable values that are applied across all instances. Instance group level variable values are applied to all instances that are defined in a group. Instance level variable values are only applied to a specific instance.

NetScaler Console gives first priority to instance level values. If there are no values provided to the variables for individual instances, NetScaler Console uses the value provided at the group

© 1997–2026 Citrix Systems, Inc. All rights reserved.

level. If there are no values provided at group level, NetScaler Console uses the variable value provided at the global level. If you provide an input for a variable across all three levels, NetScaler Console uses the instance level value as the default value.

14. lick **Upload** to upload the input key file to NetScaler Console. Click **Next**.



	A	B	C	D	E	F	G	H
1	#Basic LB Configuration_variable_input_key_file							
2								
3	#Global	servernan	ipaddress	portnumb	servicenar	ipaddress	servicenar	ipaddress2
4	Global Val	ServerNan	10.102.29.	80	ServiceNa	10.102.29.	ServiceNa	10.102.29.3
5	#Instance(	servernan	ipaddress	portnumb	servicenar	ipaddress	servicenar	ipaddress2
6	10.102.29.	ServerNan	10.102.29.	80	ServiceNa	10.102.29.	ServiceNa	10.102.29.3
7	10.102.20	ServerNan	10.102.29.	80	ServiceNa	10.102.29.	ServiceNa	10.102.29.3
8	10.106.15	ServerNan	10.102.29.	80	ServiceNa	10.102.29.	ServiceNa	10.102.29.3
9								
10								
11								
12								
13								

IMPORTANT

When you upload a CSV file from a Mac, Mac stores the CSV file with semicolons instead of commas. This causes the configuration to fail when you upload the input file and run the job. If you are using a Mac, use a text editor to make the necessary changes and then upload the file.

15. You can also give common variable values across all instances and click **Upload** to upload the input key file to NetScaler Console.

    The key input files containing the variables values are persisted (with the same file name) in the configuration jobs. You can view and edit these input files that you have used and uploaded earlier while creating or editing the configuration jobs.

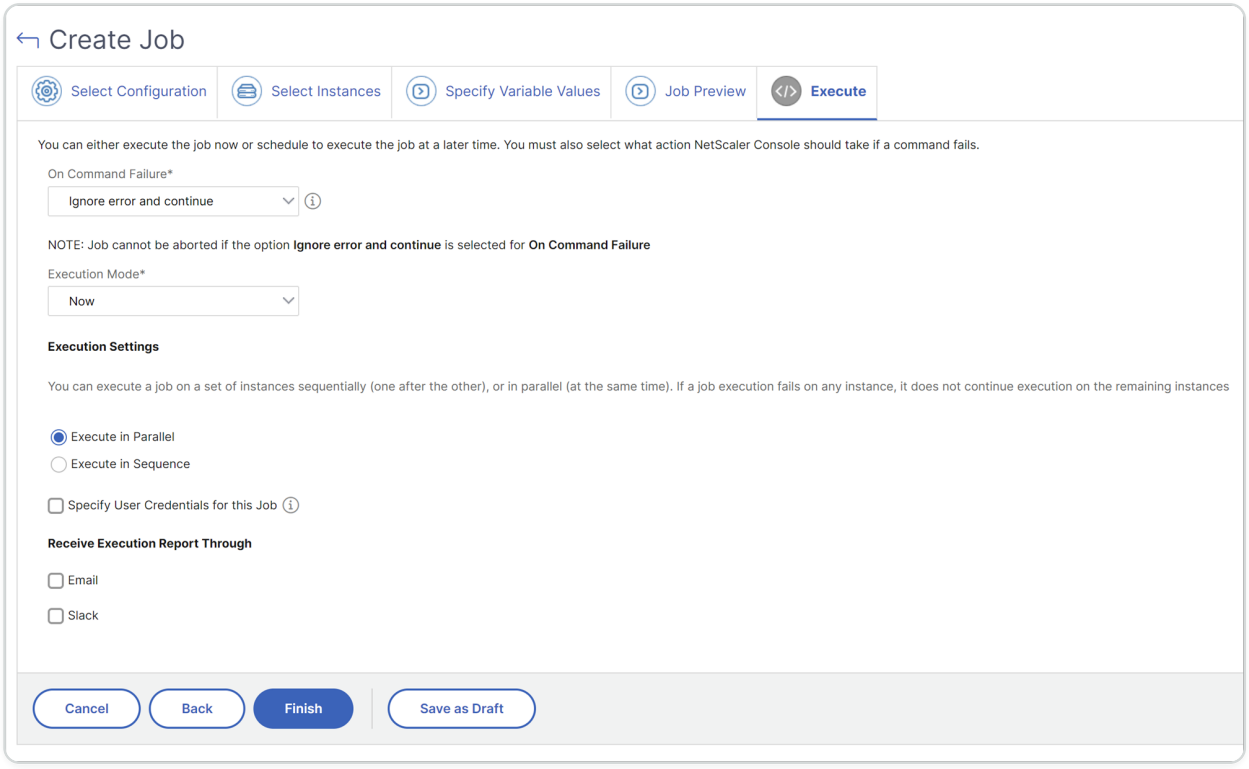
    To view the run configuration jobs while creating a configuration job, navigate to **Network** > **Configuration Jobs**, and click **Create Job**. In the **Create Job** page. On the **Specify Variable Values** tab, select the **Common Variable Values for all Instances** option to view the uploaded files. To edit the input files, download the input file and then edit and upload the files (keeping the same file name).

    To view the already run configuration jobs while editing a configuration job, navigate to **Network** > **Configuration Jobs**, select the Job Name and click **Edit**. In the **Configure Job**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

page, on the **Specify Variable Values** tab, select the **Common Variable Values for all Instances** option to view the uploaded files. To edit the input files, download the input file and then edit and upload the files (keeping the same file name).

16. On the **Job Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group.
17. In the **Execute** tab, you can choose to run your job now or schedule it to be run later. You can also choose what action NetScaler Console must take if the command fails and if you'd like to send an email notification regarding the success or failure of the job along with other details.



After configuring your jobs and running it, you can see the job details by navigating to **Infrastructure > Configuration > Configuration Jobs** and select the job you configured. Click **Details** and then, click **Variable Details** to see the list of variables added to your job.

NOTE

The values that you have provided for the variables in **step 5** are retained by NetScaler Console when you save the job and exit, or when you schedule a job to be run at a later point of time.

Create configuration jobs from corrective commands

You can use the audit template feature in NetScaler Console to monitor configuration changes across managed NetScaler instances and troubleshoot configuration errors.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The typical work flow for auditing configuration changes using audit templates consists of the following steps.

1. Create an audit template with a set of valid/expected NetScaler commands for auditing instance configurations.
2. Select the NetScaler instances against which you want to run the audit template to check for any differences between the running configuration and the expected configurations.
3. Understand the differential/corrective commands and utilize the "Create Job" functionality to get the instance's configurations to the desired state

Consider a scenario where multiple administrators are managing five NetScaler instances. All these administrators make updates to the existing instance configuration as and when there are any changes needed. The super administrator wants to ensure that a certain set of important configuration remains untouched irrespective of the changes being made by other administrators. For this use case, the super administrator creates a template of the configuration that is expected to be present on the NetScaler instances and runs it against the instances. NetScaler Console compares the audit template configuration with the running configuration and reports any mismatch on the **Configuration Audit** dashboard.

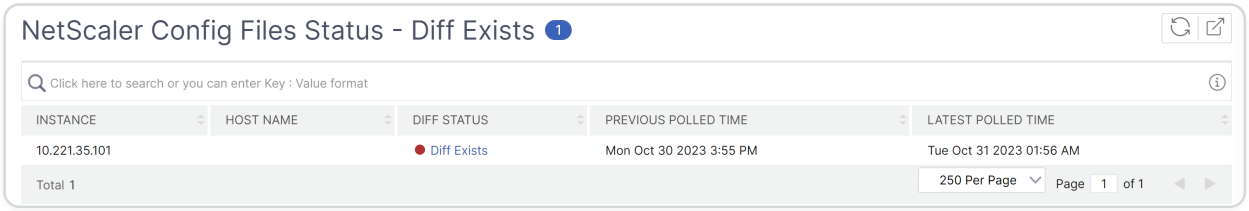
If you notice that there is a change in the configuration of some instances, you can use the NetScaler Console corrective commands feature to create a configuration job with the modified and corrected configuration commands for specific NetScaler instances.

If any difference exists between the audit template configuration and the running configuration, a **Diff Exists** status message appears on the **Audit Report** page. Clicking the **Diff Exits** link takes you to the **Configuration Diff** page, where you can view the corrective command. You can also use these corrective commands to create a configuration job and run that on the specific NetScaler instances to get them back to the desired configuration.

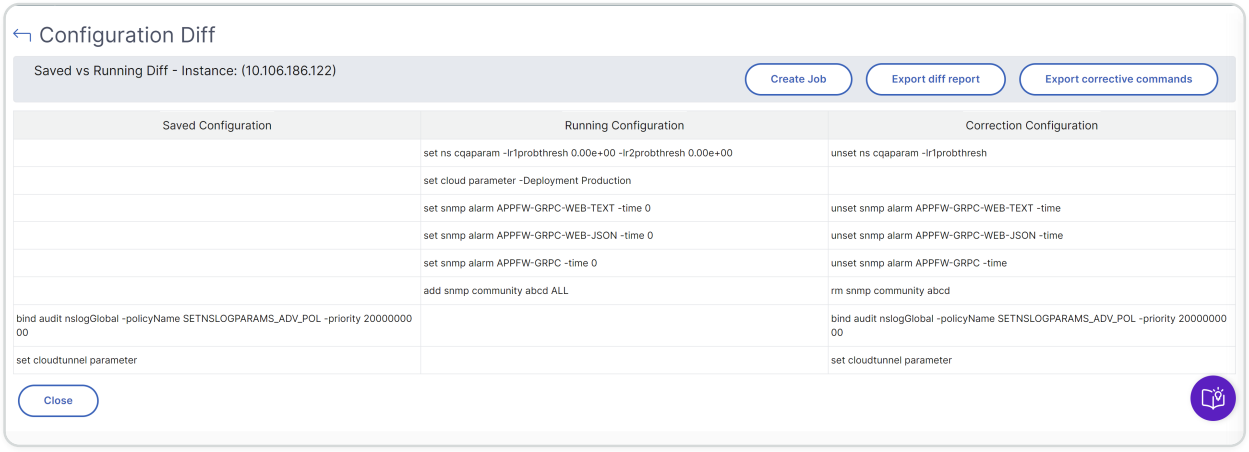
To create a configuration job from corrective commands on NetScaler Console:

1. Navigate to **Infrastructure > Configuration > Configuration Audit**.
2. On the **Configuration Audit** page, click inside any of the two donut charts to access the **Audit Reports** page.
3. Click the **Diff Exists** link (under the **Saved vs Running Diff** column in the table) for the instance for which you want to correct the configuration commands. The **Configuration Diff** page appears, listing the differences between the Saved Configuration, Running Configuration, and Correction Configuration for that instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Click **Create Job** to go to the **Create Job** page, on which the corrective commands pre-populated. For instructions on how to create a configuration job, see How to Create a Configuration Job on NetScaler Console.



Replicate running and saved configuration from one NetScaler instance to another

You can now replicate a NetScaler instance's configuration on other instances. When you configure a job in NetScaler Console, select an instance as the Configuration Source and choose the selected instance's running or saved configuration.

For example, when you select **Running Configuration** and click **Extract**, NetScaler Console sends a request to the selected NetScaler instance to locate the running configuration, and displays it as a template. You can drag the template into the **Commands** field in the right-hand pane. You can modify commands, parameters, and the instances.

To replicate running and saved configuration commands of one instance to another instance on NetScaler Console:

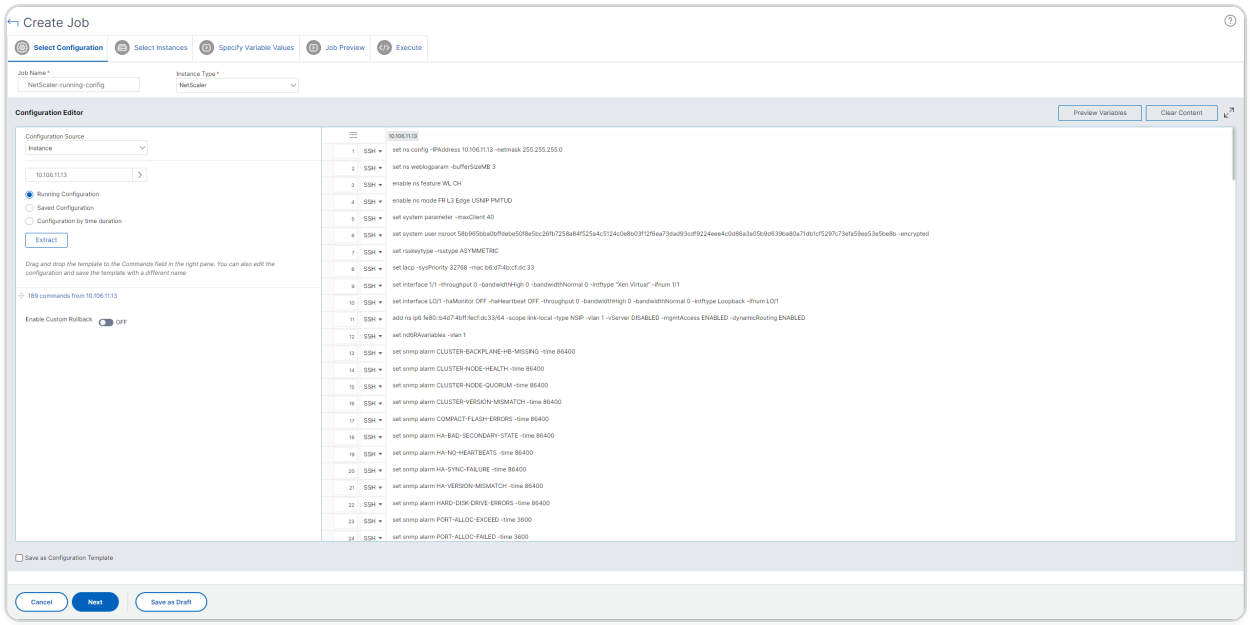
1. Navigate to **Infrastructure > Configuration > Configuration Jobs**, and click **Create Job**.
2. Specify the job name and the type of instance. For example, specify *NetScaler Running Config1* as your job's name and the instance type as *NetScaler*.
3. Select **Instance** as the **Configuration Source**, select the source instance whose configuration you want to replicate on other instances.
4. You see the following three options:

    - Running Configuration

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Saved Configuration
- Configuration by time duration

5. Choose **Running Configuration**, and click **Extract**. The number of running configuration commands run on that instance is displayed.



6. Drag the commands in the **Commands** field in the right pane.
7. You can edit the commands in the Commands field. For example, if the commands extracted are to set up a NetScaler instance. This might include adding partitions, setting up load balancing, binding the load balancing server to services, and so on. You may want to edit your commands, to set up your new NetScaler instances without partitions. So, to remove partitions, manually delete commands related to the creation of partitions and click **Next**.
8. Click **Add Instances** and add the instances on which you want to apply the running configuration commands. Click **OK** and then, click **Next**.
9. If you have specified variables in the commands, on the **Specify Variable Values** tab, click **Download Input Key File**. In the downloaded file, specify values for the variables, and then upload the file to NetScaler Console.
10. On the **Job Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group.
11. In the **Execute** tab, you can choose to run your job now or schedule it to be run later. You can also choose what action NetScaler Console must take if the command fails and if you'd like to send an Email notification regarding the success or failure of the job along with other details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Reuse run configuration jobs

Configuration jobs allow you to create a set of configuration commands that you can run on one or more managed instances. You can also run the same set of saved configuration jobs after modifying the commands, the parameters, the configuration source, and instances in the job. This feature is useful when the same set of commands has to be run on a different instance, or when the job encounters an error and stops further execution.

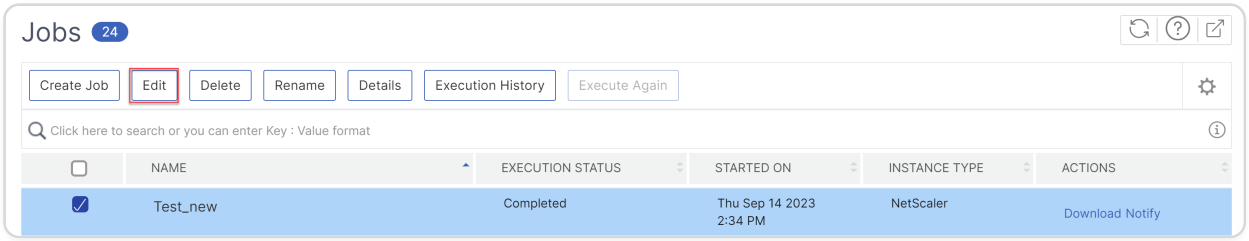
NetScaler Console provides a function to run the completed jobs again. With this function, jobs that are run completely can be run again without changing the job name.

NOTE

You can re-execute only those jobs that are run when the mode of execution is "Now".

To edit completed jobs:

1. From the NetScaler Console home page, navigate to **Infrastructure > Configuration > Configuration Jobs**.
2. In **Jobs** page, select a job that shows the Execution Summary as Completed, and click **Edit**. You can also edit a scheduled configuration job.



3. In **Configure Job** page, you can see that the Job Name and the Instance type are non-editable. You can modify other fields like configuration source, add instances, edit variable values, and set execution settings.
4. Click **Finish** to run the configuration job again.

NOTE

You can also select the job and click **Execute** again to run the job without modifying any source, instance, and commands. This option is useful when you have to run the same set of commands on the same instances. Sometimes, the job might encounter a transient error from the server side, and you might have to run the job again.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use SCP (put) command in configuration jobs

You can use the **Configuration Jobs** feature of NetScaler Console to create configuration jobs, send email notifications, and check execution logs of the jobs created. A job is a set of configuration commands that you can create and run on a single managed instance or on multiple managed instances. For example, you can use configuration jobs for device upgrades.

Configuration jobs in NetScaler Console use Secure Shell (SSH) commands to configure instances, and you can configure a configuration job to use secure copy (SCP) to securely transfer files. SCP is based on the SSH protocol. One of the SCP commands that you can include in a configuration job is the "put" command. You can use the "put" command in configuration jobs to upload or transfer one or more files stored in a local directory on your system to NetScaler Console and then to a directory on the NetScaler instance or instances.

NOTE

The file is uploaded to NetScaler Console and it is later copied (put) to the selected NetScaler instances. The uploaded file is stored in NetScaler Console and is deleted only when the job is deleted. This is necessary for jobs scheduled to run later.

The command has the following syntax:

```
put \<local\_filename\> \<remote\_path/remote\_filename\>
```

Where,

\<local_filename\> is the name of the local file to be uploaded.

\<remote_path/ remote_filename\> is the path to a remote directory, and the name to assign to the file when it is copied to that directory.

While creating the configuration job, you can convert the local and remote file name parameters into variables. This lets you assign different files to these parameters for the same set of NetScaler instances every time you run the job. Also, when you use a file at multiple places in a job and if you want to rename the file, you can redefine the variable instead of changing the file name at all places.

To use the put command to upload files in a configuration job:

1. In NetScaler Console, navigate to **Infrastructure > Configuration > Configuration Jobs**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

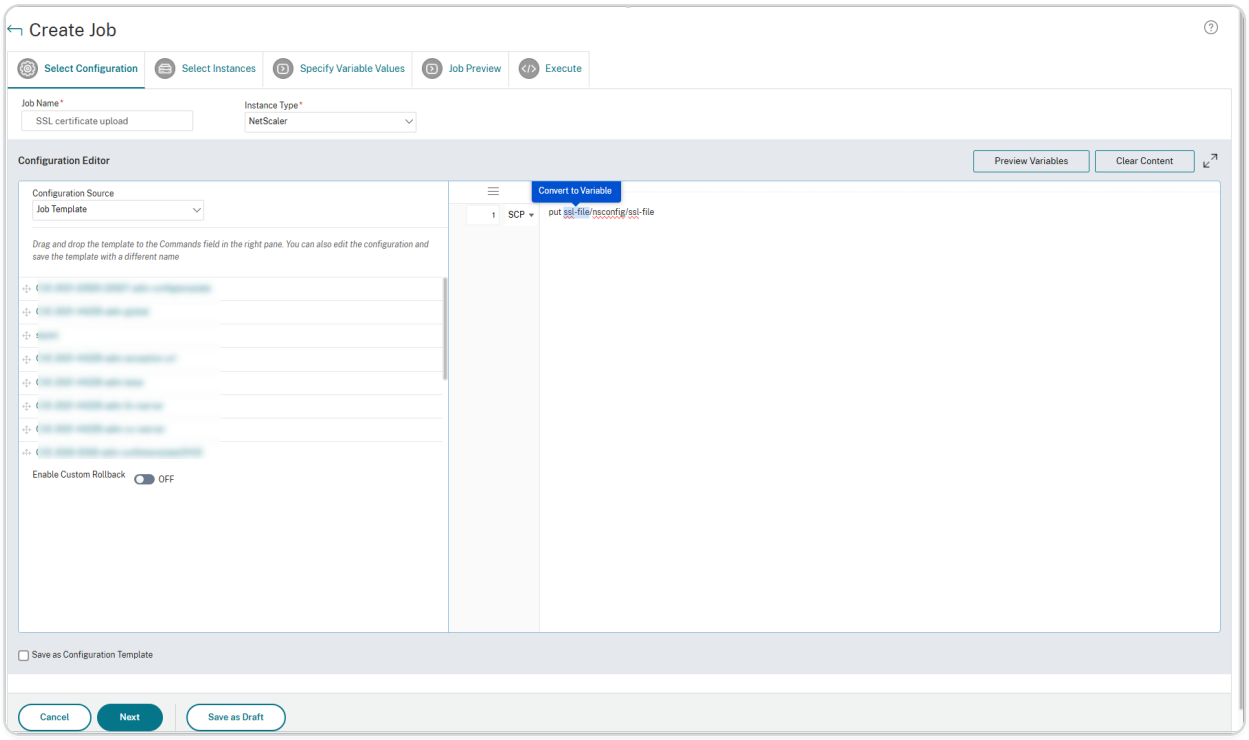
2. On the **Jobs** page, click **Create Job**.
3. On the **Create Job** page, enter the name of the job in the Job name field, and in the **Configuration Editor** pane, enter the "put" command.

   For example, if you want to create a configuration job that copies an SSL certificate file saved on your local system to multiple NetScaler instances, you can add a "put" command that uses a variable instead of the name of a particular file, and define the variable type as "file".

   ```
   put ssl-file /nsconfig/ssl-file
   ```

   In this example,

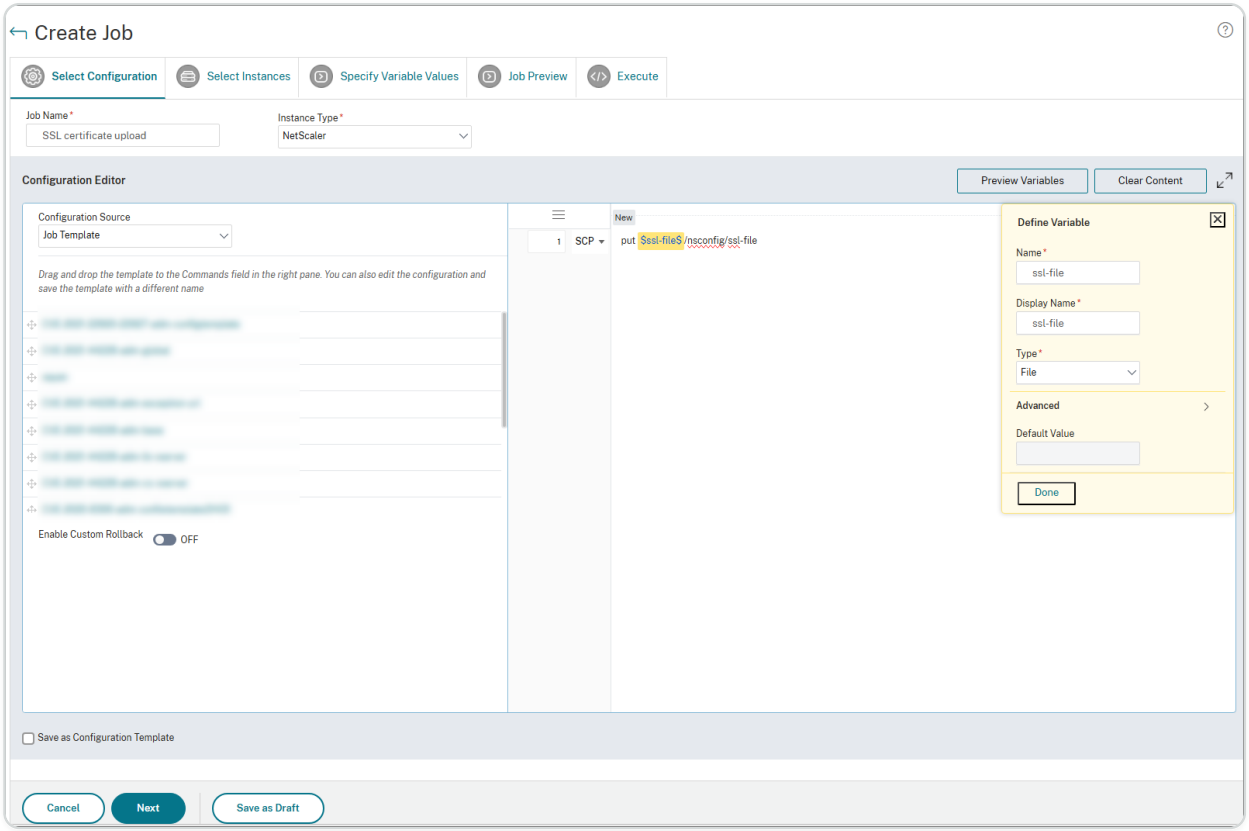
   - `ssl-file` - it is the name of the file that must be uploaded in the NetScaler instance.
   - `/nsconfig/ssl-file` - it is the destination folder on the instance where the `ssl-file` will be put after the execution of the task.
4. In the command that you entered, select the file name that you want to convert to a variable, and then click **Convert to Variable**, as shown in the following figure.



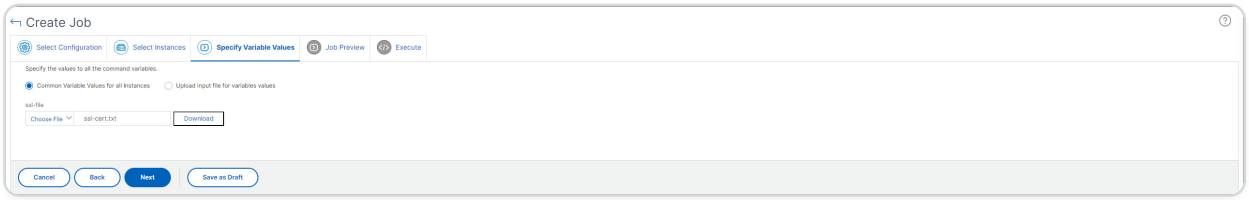
5. Verify that the file name has been enclosed by dollar signs (indicating that it is now a variable), and then click the variable.
6. Specify the details of the variable, such as name, display name, and type.
7. From the **Type** drop-down list, select **File**. Click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Declaring the variable as a "File" type allows you to upload files to NetScaler Console.



8. Click **Next** and select the NetScaler instances to which to copy the files.
9. On the **Specify Variable Values** tab, select **Common Variables Values for all Instances** section, select the file from the local storage on your system, click **Upload** to upload the file to NetScaler Console, and click **Next**.



10. On the **Job Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group.
11. On the **Execute** tab, you can run the job now or schedule it to be run later. You can also choose what action NetScaler Console must take if the command fails. You can also create an Email notification to receive notification about the success or failure of the job, and other details. Click **Finish**.
12. You can see the job details by navigating to **Infrastructure > Configuration > Configuration Jobs**, and selecting the job that you configured. Click **Details**, and then click **Variable Details** to list the variables added to your job.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use configuration templates

A configuration template is a reusable set of configuration commands that you can save in NetScaler Console and apply while creating configuration jobs or configuration audits. Templates help you standardize configurations, reduce repetitive effort, and deploy consistent settings across multiple managed NetScaler instances.

You can create a configuration template while creating a job by saving a set of configuration commands as a template. You can also use built-in templates, master configuration templates, and audit templates, and share them between the Configuration Jobs and Configuration Audit modules.

The following topics describe how to work with configuration templates in NetScaler Console:

- Use the master configuration template
- Schedule jobs created by using built in templates
- Schedule a job for configuring export of metrics from NetScaler to Prometheus
- Use configuration templates to create audit templates
- Reschedule jobs configured by using built in templates
- Reuse configuration audit templates in configuration jobs
- Import and export configuration templates

Use the master configuration template

Using a master configuration template is a flexible option for creating and deploying a master configuration on multiple NetScaler instances.

As an administrator, you might want to make configuration changes and save licenses, certificates, and other files on a NetScaler instance. You can save the new configuration as a master configuration template (.conf file).

To save your master configuration template from a NetScaler instance, you can do one of the following:

- At the command prompt, enter **save ns config**. The configuration is saved in the instance's FLASH memory in the /nsconfig/ns.conf file.
- From the NetScaler instance's GUI, navigate to **Diagnostics** > **View Configuration**. Choose the kind of configuration you'd like to save. For example, if you want to save the saved configuration of your NetScaler instance, select **Saved configuration**. Click the **Save text to a file** link to save the 'ns.conf' file to your local machine.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When you deploy the master configuration template by using the 'DeployMasterConfiguration' configuration template while creating a job, you can customize it further for each specific NetScaler instance by adding more commands, modifying existing commands, and providing different variable values in the input file.

For example, as an administrator you may want to upload certificate keys to your NetScaler instances in addition ns.conf file and deploy the master configuration on them as well.

IMPORTANT

You cannot run a configuration job using the DeployMasterConfiguration template on NetScaler CPX instances, NetScaler instances configured in a cluster, or on partitioned NetScaler instances.

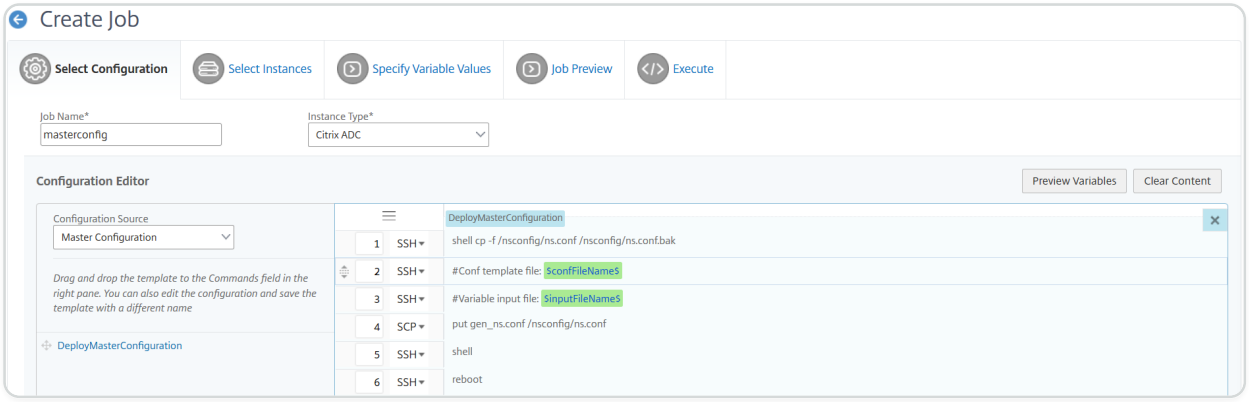
To create a configuration job using the Master Config configuration template on NetScaler Console:

1. In NetScaler Console, navigate to **Infrastructure > Configuration > Configuration Jobs**, and then click **Create Job**.
2. On the **Create Job** page, on the **Select Configuration** tab, specify the **Job Name** and select the **Instance Type** from the drop-down list.
3. Select **Master Configuration** from the **Configuration Source** drop-down list. Drag the DeployMasterConfiguration template's commands to the right pane. You can add, modify, or delete commands in the right pane as well. Click **Next**.

   NOTE

   You can add **put** commands to add input files to your template. In our example, we must upload certificate and key files in addition to the configuration template file and variable input files.

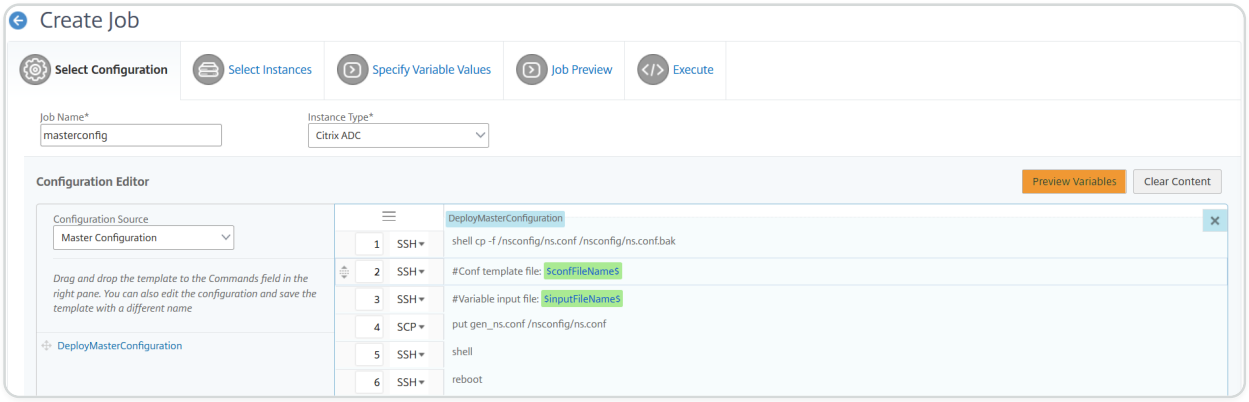
© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. You can review all the variables that you have defined while creating or editing a configuration job in a single consolidated view.
5. Do one of the following to view all the variables in a single consolidated view:

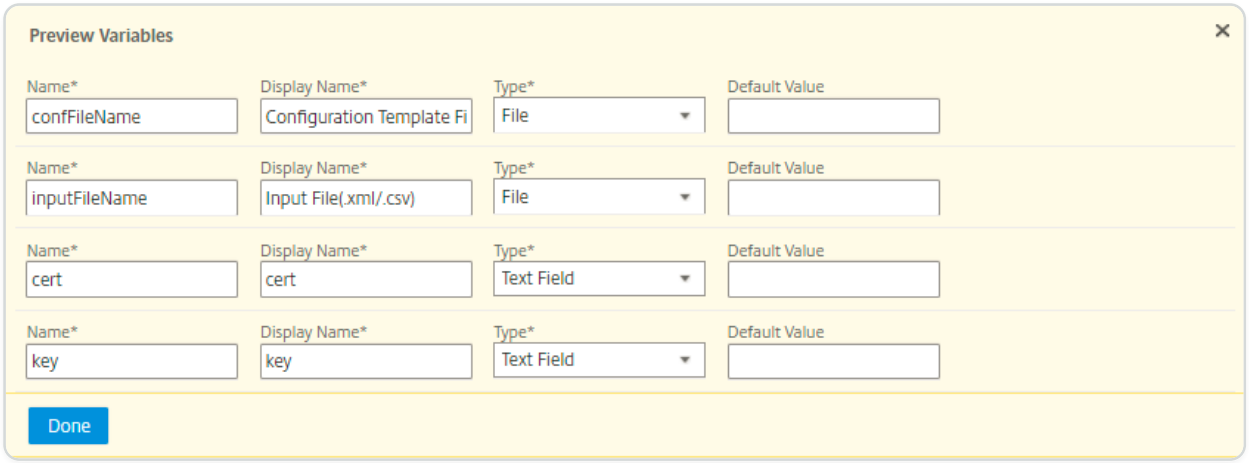
   - While creating a configuration job, navigate to **Infrastructure > Configuration Jobs**, select **Create Job**. On the **Create Job** page, you can review all the variables that you have added while creating the configuration job.
   - While editing a configuration job, navigate to **Infrastructure > Configuration > Configuration Jobs**, select the Job Name and click **Edit**. On the **Configure Job** page, you can review all the variables that were added while creating the configuration job.

6. You can then click the **Preview Variables** tab to preview the variables in a single consolidated view that you have defined while creating or editing a configuration job.



7. A new pop-up window appears and displays all the parameters of variables such as Name, Display Name, Type, and default value in a tabular format. You can also edit and modify these parameters. Click the **Done** button after you have edited or modified any of the parameters.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. Select the instances on which you want to run the configuration job, and then click **Next**.
9. On the **Specify Variable Values** tab, upload the following:

    - **Configuration Template File (.conf)** - Upload the .conf file that you extracted from a NetScaler instance.
    - **Upload the Input File (.xml/csv)** - Upload the input file with values for the variables you have defined in your commands.

    A sample xml file is provided here for your usage. Ensure that the xml files contain the details corresponding to the NetScaler instances that you are using.

```
<?xml version="1.0" encoding="UTF-8" ?>

<properties>

<!--

Provide inputs for all the parameters defined in the master config
file.

-  global. This tag contains all the common parameters and value.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- devicegroup. This tag contains all the instance group specific parameters and values.

If the same parameters are defined in global and instance tags, the instance specific parameters value will take precedence over the instance group. The instance group specific parameters value will take precedence over global parameters in the execution.

- name. This attribute represents the name of the instance group.

- device. This tag contains all the instance specific parameters and value.

If the same parameters are defined in global and instance tags, the instance specific parameters value will take precedence in the execution.

- name. This attribute represents the IP Address of the instance. Host name is not supported for the attibute.

HA pair should be represented as <primaryip>-<secondaryip>. Example 10.102.2.1-10.102.2.2

In the template file, the parameter name must be specified within the dollar sign,Example: $NSIP$, CC_Trap_Dest and parameters names are case sensitive.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-->


<global>


</global>
<devicegroup name="BLR_DEVS">
</devicegroup>
<device name="10.106.101.209">
<param name="IP" value="10.106.101.209"/>
</device>


<!-- HA PAIR-->
<!--<device name="10.102.43.154-10.102.43.155">
<param name="NSIP" value="10.102.43.154"/>
<param name="HostName" value="NS43HA"/>
<param name="LBSERVER" value="haserver43http"/>
<param name="SNMPTrapDest" value="10.102.43.130"/>
</device>-->
</properties>
```

A sample csv file is provided here for your usage.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
#job-s_variable_input_key_file ,,,,

,,,,

#Global,NSIP,HostName,LBSERVER,SNMPTrapDest

Global Values,,,,

#InstanceGroup,NSIP,HostName,LBSERVER,SNMPTrapDest

example_doc,,,,

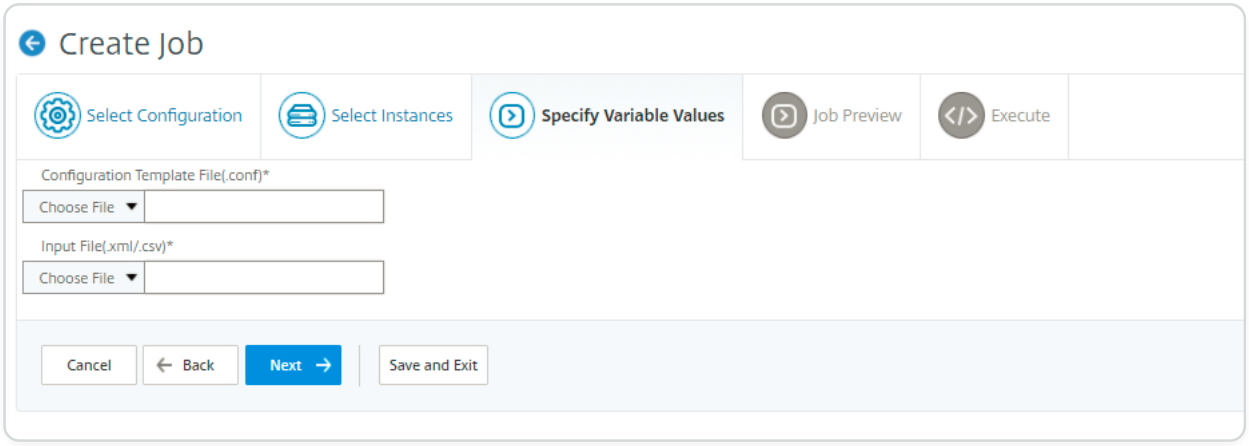
#Instance(s),NSIP,HostName,LBSERVER,SNMPTrapDest

10.xx.xx.xx,,,,
```

The same file is displayed in Microsoft excel:

#job-s_variable_input_key_file				
#Global	NSIP	HostName	*LBSERVER*	SNMPTrapDest
Global Values				
#InstanceGroup	NSIP	HostName	LBSERVER	SNMPTrapDest
example_doc				
#Instance(s)	NSIP	HostName	LBSERVER	SNMPTrapDest

10. Click **Next**.



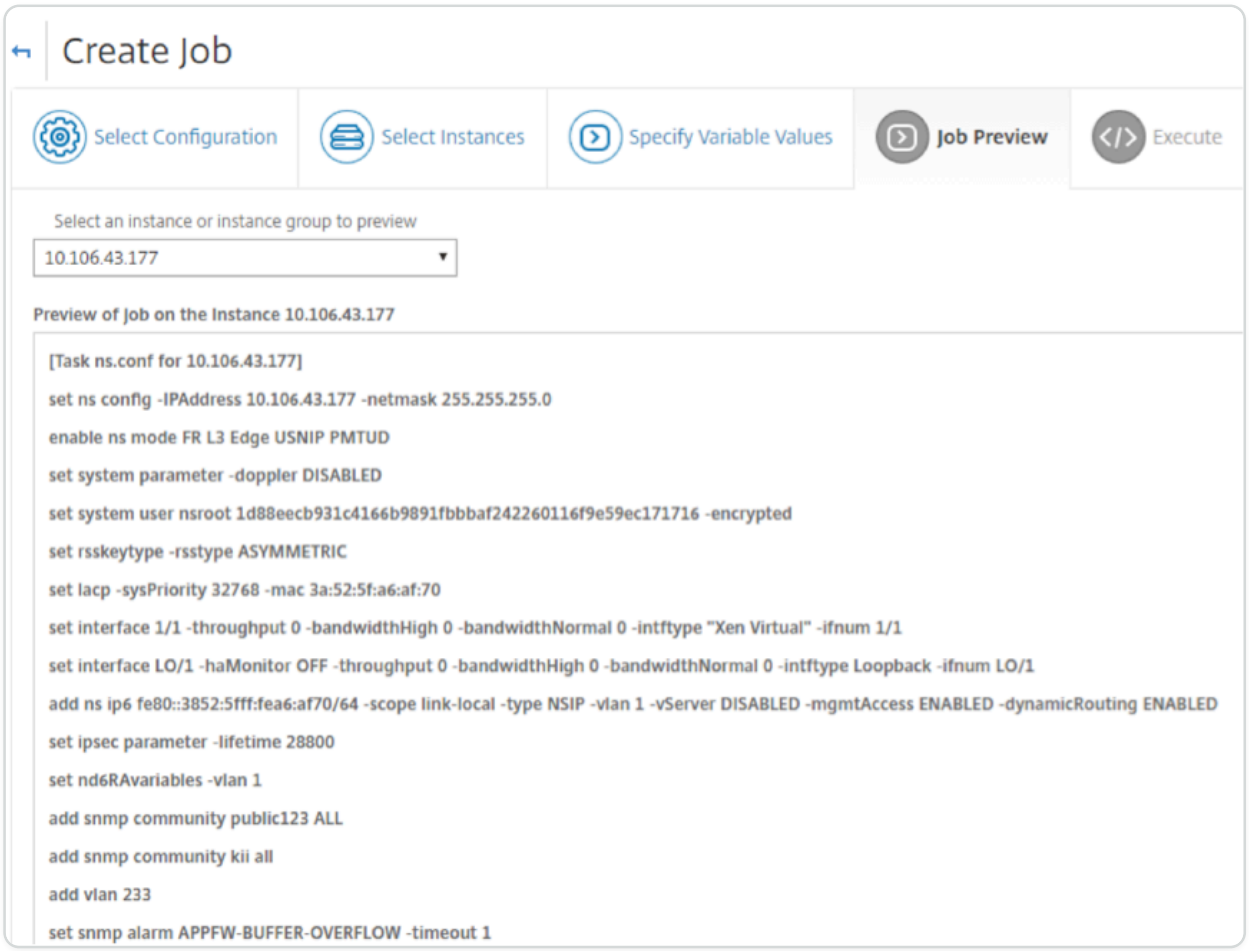
The input files containing the variables values are persisted (with the same file name) in the configuration jobs. You can view and edit these input files that you have used and uploaded earlier while creating or editing the configuration jobs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To view the run configuration jobs while creating a configuration job, navigate to **Network** > **Configuration Jobs**, and click **Create Job**. In the **Create Job** page. On the **Specify Variable Values** tab, select the **Common Variable Values for all Instances** option to view the uploaded files. To edit the input files, download the input file and then edit and upload the files (keeping the same file name).

To view the already run configuration jobs while editing a configuration job, navigate to **Network** > **Configuration Jobs**, select the Job Name and click **Edit**. In the **Configure Job** page, on the **Specify Variable Values** tab, select the **Common Variable Values for all Instances** option to view the uploaded files. To edit the input files, download the input file and then edit and upload the files (keeping the same file name).

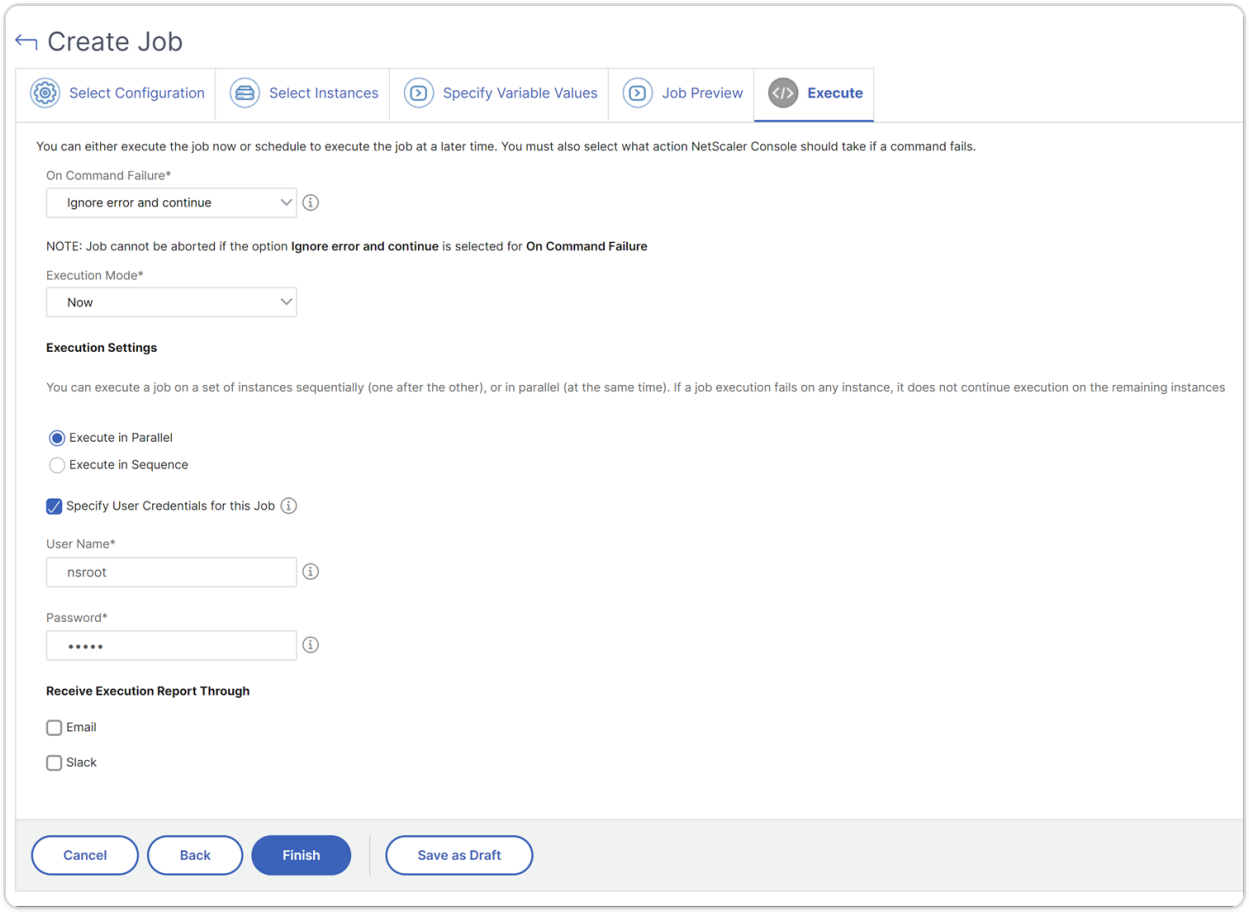
11. On the **Job Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group, and then click **Next**.



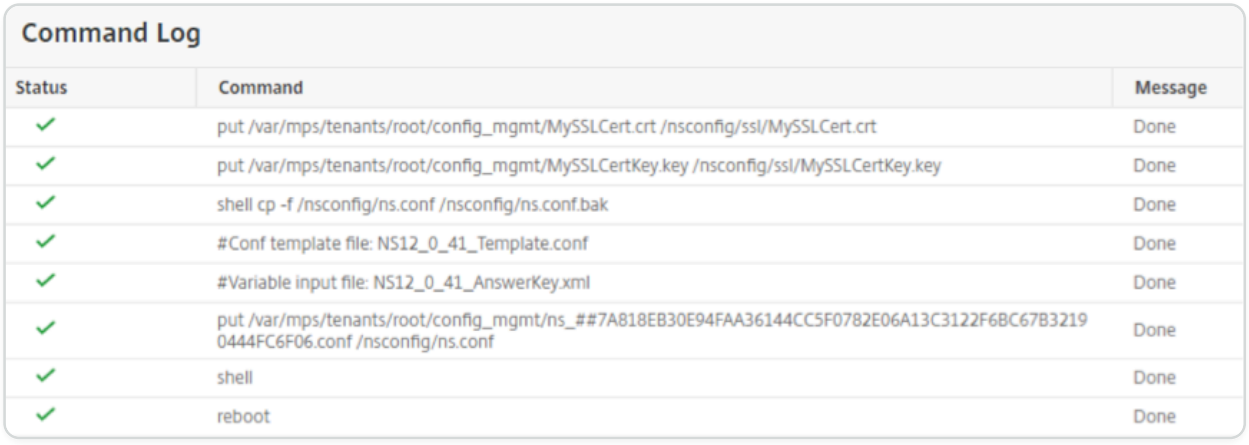
12. On the **Execute** tab, you can choose to run your job now or schedule it to be run later. You can also choose what action NetScaler Console must take if the command fails.

    You can also choose to allow authorized users to run jobs on your managed instances, and you can choose whether to send an email notification regarding the success or failure of the job, along with other details.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



After running your job, you can see the job details by navigating to **Infrastructure > Configuration > Configuration Jobs** and select the job you just configured. Click **Details** and then, click **Execution Summary** to see the details of your job. Click the instance to see the **Command Logs** to see the commands run on the job.



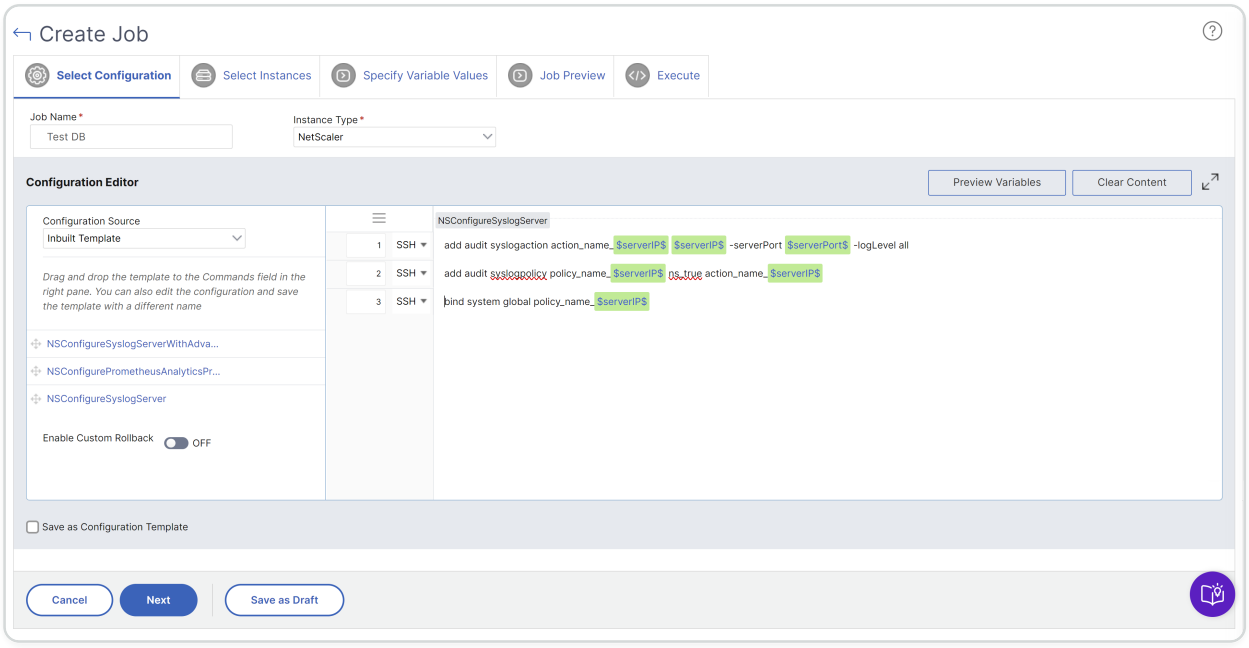
Schedule jobs created by using built in templates

You can schedule a job by using the built-in template option. A job is a set of configuration commands that you can run on one or more managed instances. For example, you can use the built-in template option to schedule a job to configure syslog servers. You can also, choose to run the job immediately or schedule the job to be run at a later stage.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To schedule a job by using built-in templates in NetScaler Console:

1. In NetScaler Console, navigate to **Infrastructure > Configuration > Configuration Jobs**, and then click **Create Job**.
2. On the **Create Job** page, on the **Select Configuration** tab, specify the **Job Name** and select the **Instance Type** from the drop-down list.
3. Select **Inbuilt Template** from the **Configuration Source** drop-down list. Drag the *NSConfigureSyslogServer* command to the right pane, and then click **Next**.



4. On the **Select Instances** tab, click **Add Instances**, select the instances on which you want to run the job, and then click **OK**.
5. Click **Next**. On the **Specify Variable Values** tab, select one of the following options to specify variables for your instances:

   - **Variable values from an input file** - Download an input file to enter values for the variables that you have defined in your commands, and then upload the file to the NetScaler Console server.
   - **Common variable values for all instances** – Specify the syslog server IP address and port.

6. On the **Job Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group.
7. Click **Next**.
8. On the **Execute** tab, set the following conditions:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **On Command Failure** - If a command fails, you can either choose to ignore the errors and continue to run the job or stop further execution of the job. Choose the action that you want to run from the drop-down list.
- **Execution Mode** - You can either run the job now or schedule to run the job later. If you want to schedule the job later, you must specify the execution frequency settings for that job. Choose the schedule you want the job to follow from the drop-down list.

9. You can also run a job on a set of instances sequentially or in parallel by selecting the required method under **Execution Settings**. If a job execution fails on any instance, it does not continue on the remaining instances.

   You can also choose to allow authorized users to run jobs on your managed instances, and you can choose whether to send an email notification regarding the success or failure of the job, along with other details.
10. Click **Finish**.

Schedule a job for configuring export of metrics from NetScaler to Prometheus

Using the `NSConfigurePrometheusAnalyticsProfile` template, you can either use the default schema or custom schema with modified parameters, and run the job to all managed instances.

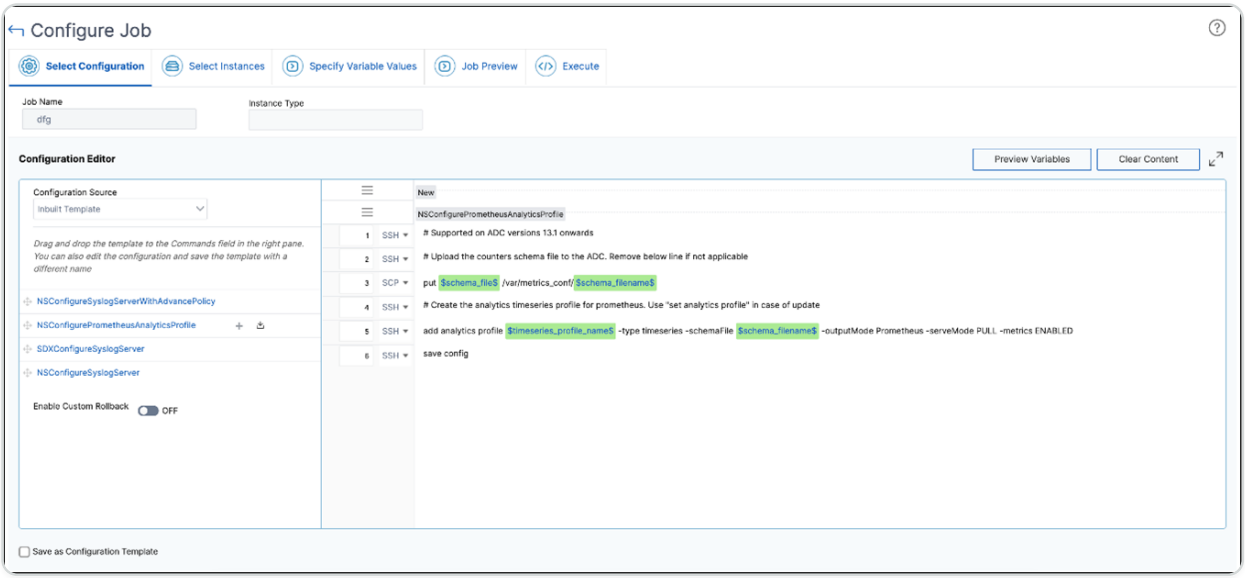
Prerequisite

Ensure that the managed NetScalers are in **13.1 build 39-27 or later**.

To schedule a job:

1. In NetScaler Console, navigate to **Infrastructure > Configuration > Configuration Jobs**, and then click **Create Job**.
2. On the **Create Job** page, specify a name for the job, and select **NetScaler®** from the **Instance Type** list.
3. Select **Inbuilt Template** from the **Configuration Source** list. Drag the *NSConfigurePrometheusAnalyticsProfile* command to the right pane, and then click **Next**. You can also click **+** to add the template.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. If you want to proceed with the default schema:

   a. Remove step 3 (`put $Schema_file /var/metrics.conf/$schema_filename$`). Place the mouse pointer at step 3 and:

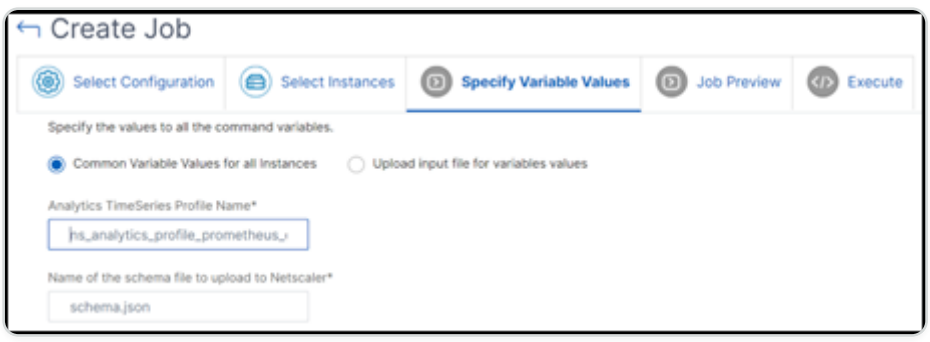
      - In Windows, use Control + A and Delete.
      - In Mac, use Command + A and Delete.

   b. After deleting, click **Next**.

   c. On the **Select Instances** tab, click **Add Instances**, select the instances on which you want to run the job, and then click **Next**.

   d. On the **Specify Variable Values** tab, select **Common Variable values for all instances**.

      - **Analytics TimeSeries Profile Name** - Specify the analytics profile name. For more information, see `https://docs.netscaler.com/en-us/citrix-adc/current-release/ns-ag-appflow-intro-wrapper-con/ns-ag-appflow-config-tsk.html#configure-the-metrics-collector`.
      - **Name of the schema file to upload to Netscaler** - Retain this file name as `schema.json` that is the default file.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

e. Proceed further from Step 6.

5. If you want to proceed with custom schema counter:

   a. Select **Inbuilt Template** from the **Configuration Source** list. Drag the `NSConfigurePrometheusAnalyticsProfile` command to the right pane and click **Next**. You can also click + to add the template.

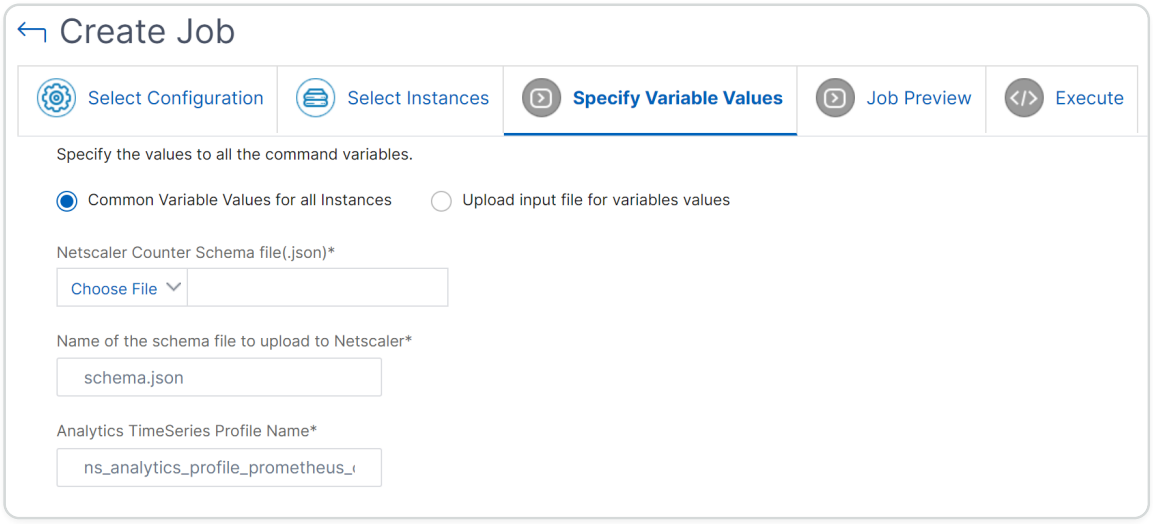
   b. On the **Select Instances** tab, click **Add Instances**, select the instances on which you want to run the job, and then click **Next**.

   c. On the **Specify Variable Values** tab, select **Common Variable values for all instances**.

   - **Netscaler Counter Schema file(.json)** - Select the schema file that you have modified with the parameters. In NetScaler, a reference file `reference_schema.json` with all supported counters is available under the path `/var/metrics_conf/`.



You can use an FTP client to copy the file in your local, edit the required parameters, save, and then upload it.



- **Name of the schema file to upload to Netscaler** - Specify the schema file name that you want to upload to NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Analytics TimeSeries Profile Name** - Specify the analytics profile name. For more information, see `https://docs.netscaler.com/en-us/citrix-adc/current-release/ns-ag-appflow-intro-wrapper-con/ns-ag-appflow-config-tsk.html#configure-the-metrics-collector`.

6. On the **Job Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group.
7. Click **Next**.
8. On the **Execute** tab, set the following conditions:

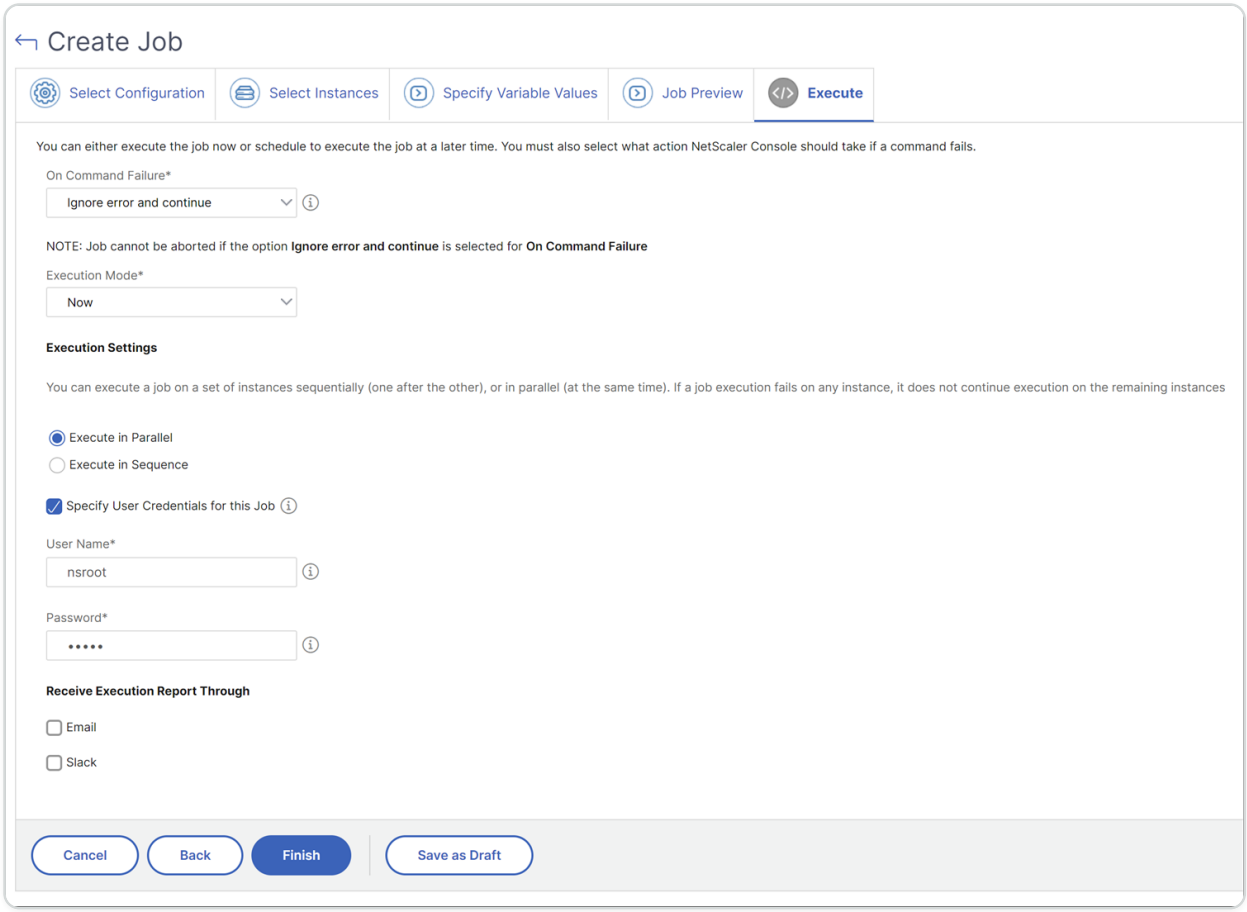
   - **On Command Failure** - If a command fails, you can either choose to ignore the errors and continue to run the job or stop further execution of the job. Choose the action that you want to run from the drop-down list.
   - **Execution Mode** - You can either run the job now or schedule to run the job later. If you want to schedule the job later, you must specify the execution frequency settings for that job. Choose the schedule you want the job to follow from the drop-down list.

9. You can also run a job on a set of instances sequentially or in parallel by selecting the required method under **Execution Settings**. If a job execution fails on any instance, it does not continue on the remaining instances.

   You can also choose to allow authorized users to run jobs on your managed instances, and you can choose whether to send notifications regarding the success or failure of the job, along with other details.

10. Click **Finish**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Use configuration templates to create audit templates

You can now use configuration commands that were previously saved as configuration templates to create Audit Templates that can be applied to specific NetScaler instances. While creating an audit template, you can drag previously saved configuration templates into the **Commands** field, and edit the template to suit your requirements. You can then apply the audit template to specific NetScaler instances. NetScaler Console compares these instances with the audit template and reports any mismatch. This process helps you identify errors and rectify them in a timely manner.

You can create configuration templates while creating a job and saving a set of configuration commands as a template. When you save these templates on the **Create Jobs** page, they are automatically displayed on the **Create Template** page.

For example, consider a basic load balancing configuration for which you add a load balancing virtual server, add two services, and bind the services to the virtual server.

This example uses the following commands:

```
add lb vserver **servername** HTTP **ipaddress portnumber**
```

```
add service **servicename1 ipaddress1** HTTP 80
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

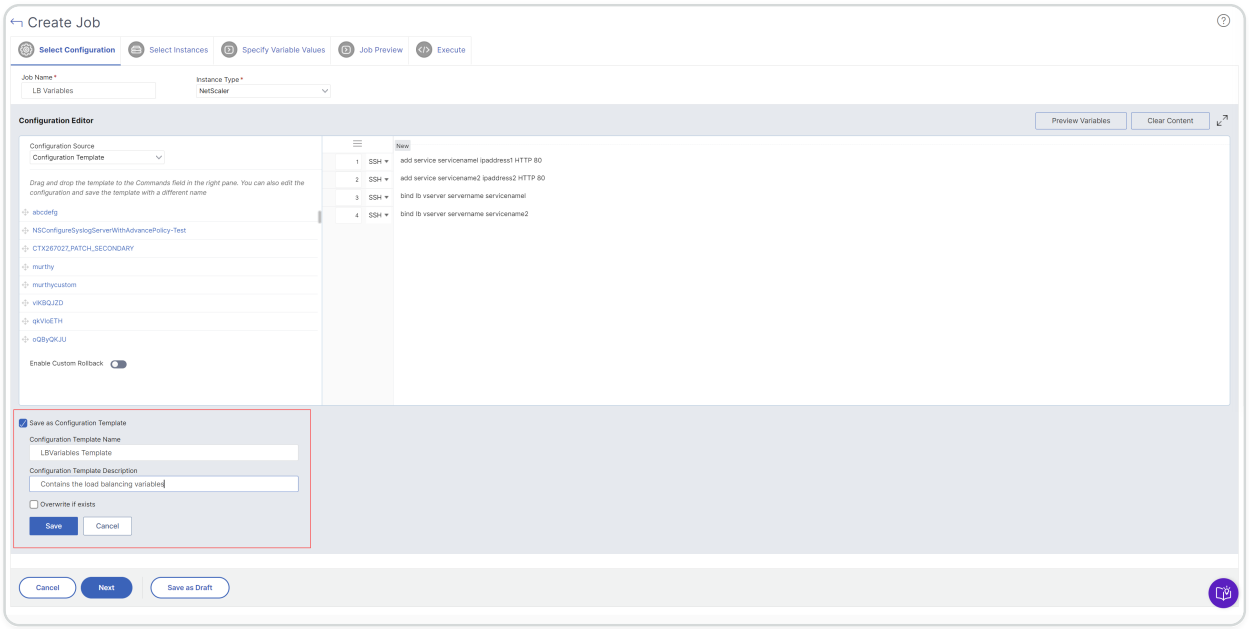
```
add service **servicename2 ipaddress2** HTTP 80
```

```
bind lb vserver **servername servicename1**
```

```
bind lb vserver **servername servicename2**
```

To save a configuration template in NetScaler Console:

1. Navigate to **Infrastructure > Configuration > Configuration Jobs**, and click **Create Job**.
2. On the **Create Job** page, specify the job name and the instance type.
3. Choose **Configuration Template** as the Configuration Source and, in the **Commands** field, enter commands such as those in the preceding example.
4. Select the **Save as Configuration Template** check box and specify a name for your template. You can choose to overwrite other templates that exist with the same name.
5. Click **Save**.

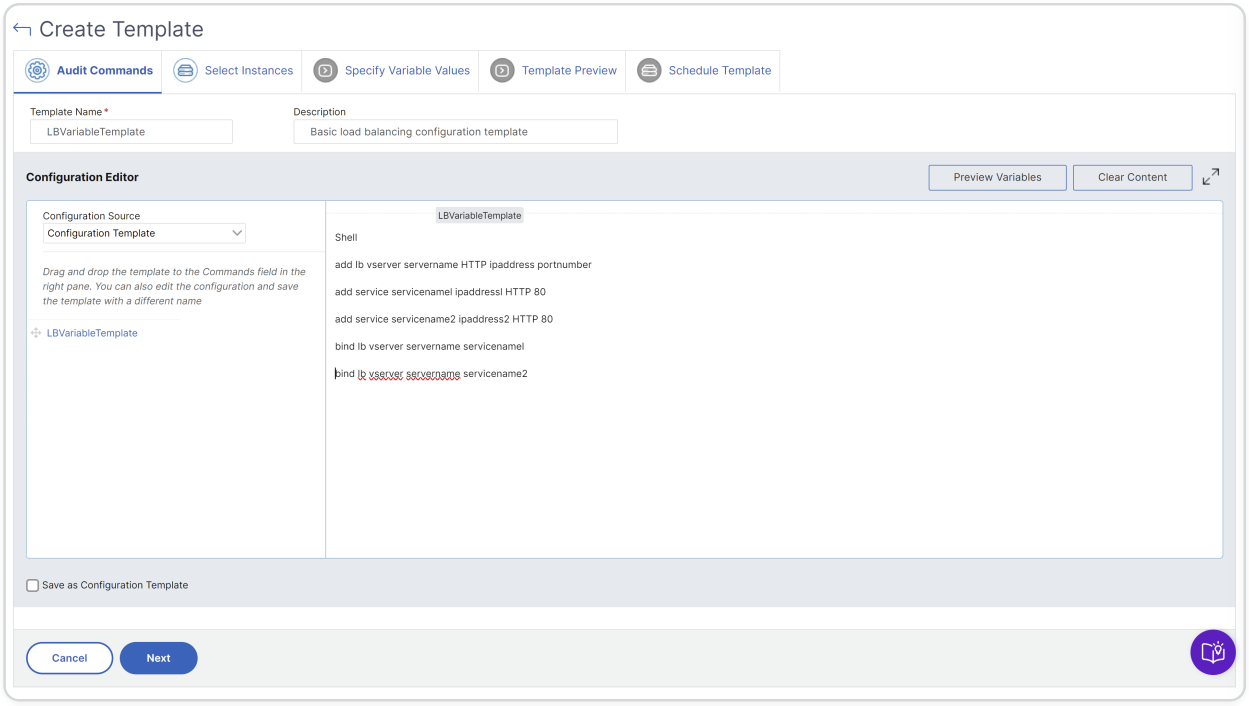


To use a configuration template to create an audit template in NetScaler Console:

1. Navigate to **Infrastructure > Configuration > Configuration Audit > Audit Templates**., and click **Add**.
2. On the **Create Template** page, specify a name for the template name, and enter a description.
3. From the **Configuration Source** list, select **Configuration Template**, and then drag the template into the Commands field in the right pane. You can also edit the configuration and save the template with a different name. Click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. On the **Select Instances** tab, click **Add Instances** and add the instances on which you want to run the configuration. Click **OK**.
5. Click **Finish**.



The audit template appears in the Audit Templates list and is run every 12 hours against the configurations of the specified instances.

Reschedule jobs configured by using built in templates

You can reschedule a job that you scheduled by using built-in templates in NetScaler Console. For example, you can change the action that NetScaler Console must take if a command fails. If you had previously opted to ignore an error and continue, you can change it to roll back all successful commands if a command fails.

To reschedule a job that was configured by using built-in templates in NetScaler Console:

1. In NetScaler Console, navigate to **Infrastructure > Configuration > Configuration Jobs**.
2. Select the job you want to edit, add or remove instances, specify variable values, and then change execution actions and settings.
3. Click **Finish** to reschedule the job.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

You can also select the job and click **Execute** again to run the job without modifying any source, instance, and commands. This is useful when you have to run the same set of commands on the same instances. Sometimes, the job might encounter a transient error from the server side, and you might have to run the job again.

Reuse configuration audit templates in configuration jobs

As an admin, you can now save configuration commands as a set of reusable configuration templates when you create a job and also when you run a configuration audit. The configuration template created and saved in **Configuration Jobs** module is available in Configuration Audit to create an audit template that can be applied to specific NetScaler instances. Similarly, the audit template created in **Configuration Audit** module is available in Configuration Jobs so that you can run the template as a configuration job. Any change made in the template is now visible in both Configuration Jobs and **Configuration Audi**t modules.

Earlier the configuration job and configuration audit templates had to be created separately for the same configuration and saved as different files. This caused a duplication of effort in creating and maintaining the templates.

NetScaler Console allows you to save this template in the system so that the audit template is available in **Configuration Jobs** also. Now the audit templates can be used to create configuration jobs. This way the templates can be used interchangeably between the configuration jobs and configuration audits.

For example, consider a basic load balancing configuration for which you add a load balancing virtual server, add two services, and bind the services to the virtual server.

This example uses the following commands:

```
add lb vserver servername HTTP ipaddress portnumber


add service servicename1 ipaddress1 HTTP 80


add service servicename2 ipaddress2 HTTP 80
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bind lb vserver servername servicename1


bind lb vserver servername servicename2
```

Creating a Template in Configuration Audits and Reusing it in Configuration Jobs

Perform the following task to create a template on the configuration audit module and reuse the same in the configuration jobs module.

To create an audit template:

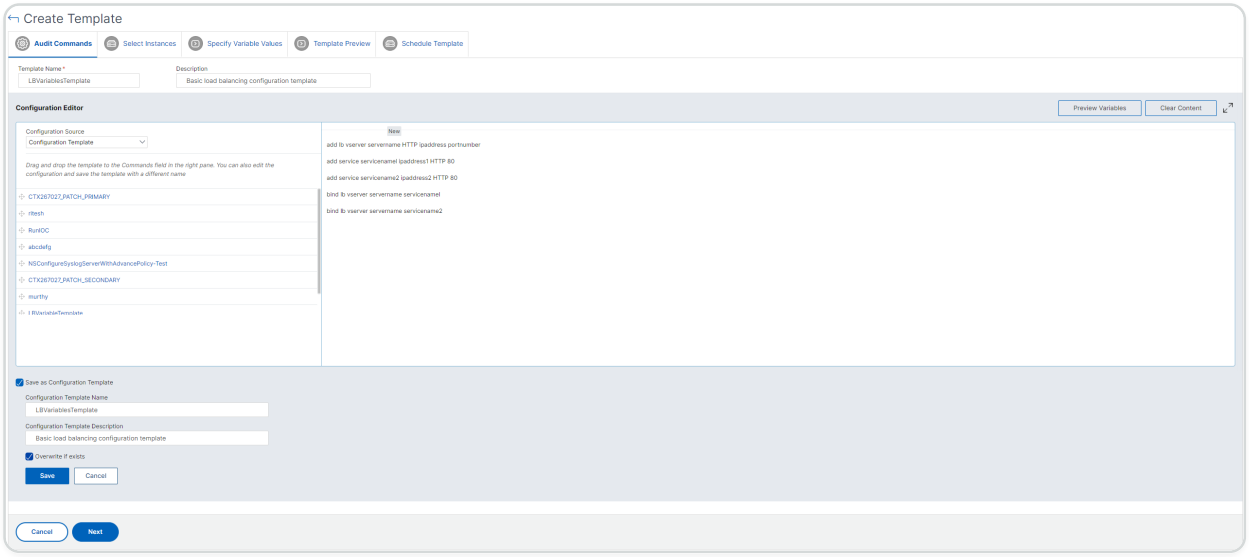
1. In NetScaler Console, navigate to **Infrastructure > Configuration > Configuration Audit** > **Audit Template**, and click **Add**.
2. On the **Create Template** page, specify the template name. You can also add more information about the template in the **Description** field.
3. In the **Commands** pane, enter commands such as those in the preceding example.
4. Select the **Save as Configuration Template** check box and specify a name for your template, for example, you can name this template as "LBVariablesTemplate." You can choose to overwrite other templates that exist with the same name.

   NOTE

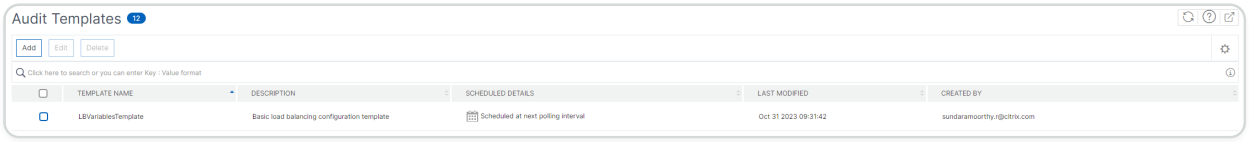
   The audit template name can be the same as the configuration template name.

5. Click **Save** and click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. Click **Next**.
7. In **Select Instances** tab, select the NetScaler instances on which you want to run these configuration commands and click **Finish**. The new template is now visible in the list of audit templates.



8. When you want to run these configuration commands, navigate to **Infrastructure > Configuration > Configuration Jobs**, and click **Create Job**. The audit template that you created earlier is listed as a configuration template.

To reuse the audit template in configuration jobs:

1. Enter a name for the job and select the instance type, and drag the template to the commands pane.

   While creating the configuration job, you can convert the local and remote file name parameters into variables. This lets you assign different files to these parameters for the same set of NetScaler instances every time you run the job.
2. In the command that you entered, select the file name that you want to convert to a variable, and then click **Convert to Variable.**
3. In **Select Instances** tab, select the instances on which you want to run these commands.
4. If you have specified any variables in the commands, in **Specify Variable Values** tab, select one of the following options to specify variables for your instances:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Variable values from an input file - Download an input file to enter values for the variables that you have defined in your commands, and then upload the file to the NetScaler Console server.
- Common variable values for all instances – Specify the syslog server IP address and port.

5. In the **Job Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group and click **Next**.
6. In the **Execute** tab, click **Finish** to run the configuration job.

   Now if you want to add another service to this load balancing server and bind the service to the server, you can edit the commands in the command page and save them.
7. Navigate to **Audit Templates** and click **Add**.
8. Drag the "LBVariablesTemplate" template to the commands pane. You can see that the template has been updated with the new commands.

   The audit template appears in the Audit Templates list and is run every 12 hours against the configurations of the specified instances. You can now create templates and reuse them between configuration jobs and configuration audit modules.

Import and export configuration templates

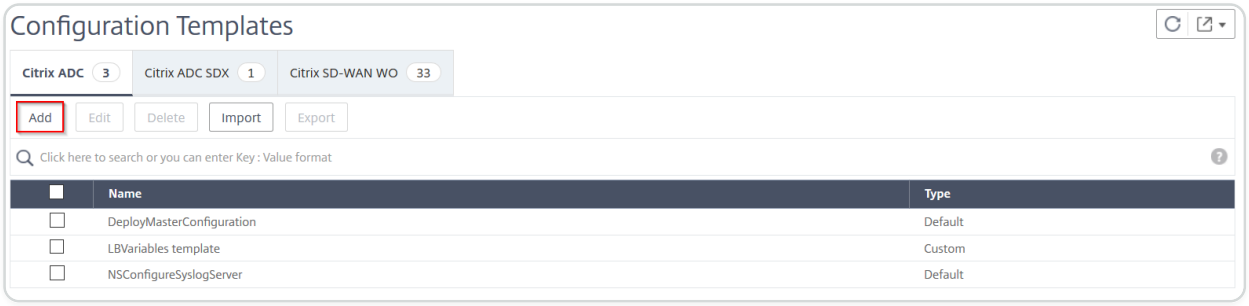
You can export the configuration templates from any NetScaler Console appliance and import the file to the same or other NetScaler Console appliance at any time in the future. The configuration templates data (such as configuration commands, variable definitions, and parameters) are not lost.

You can export the configuration templates to a **.json** file format and save it in the local folder. You can import configuration template .**json** files into NetScaler Console appliances which you might have exported from the same or other NetScaler Console appliance or created manually.

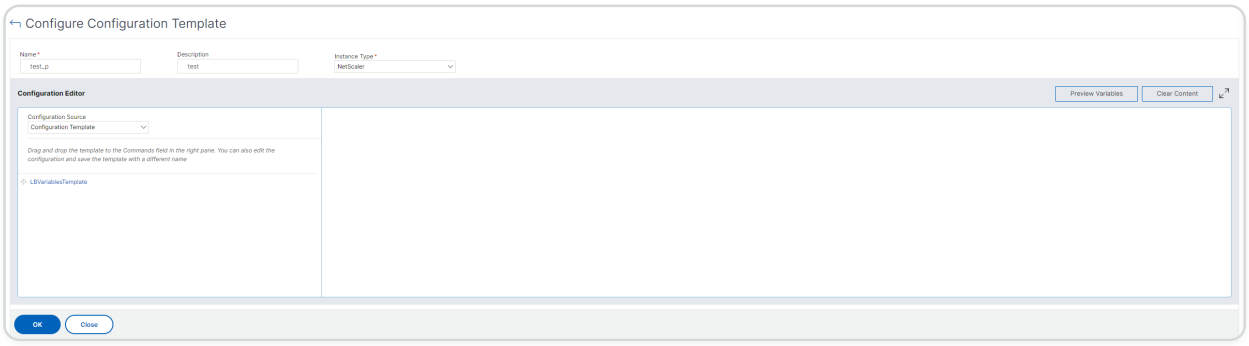
To export the configuration templates:

1. Navigate to **Infrastructure > Configuration > Configuration Templates**.
2. Click **Add** to create the configuration template.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



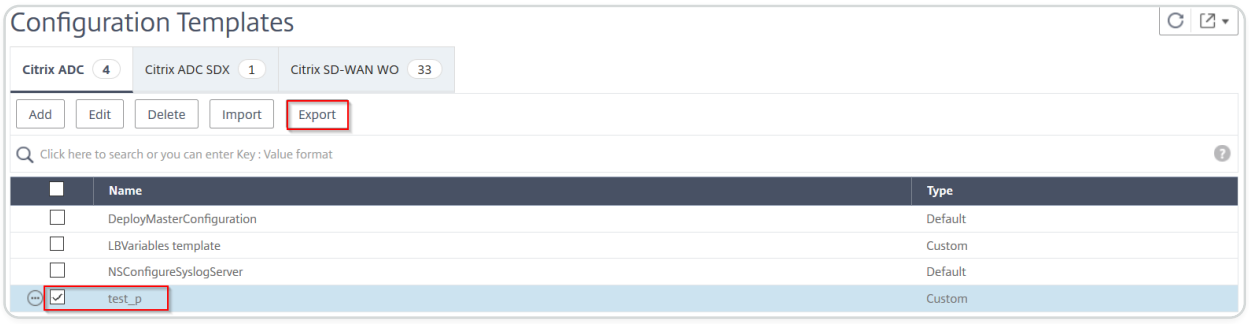
3. On the **Create Configuration Template** page, specify the configuration template name, and choose the instance type. Under **Configuration Editor**, select configuration source as Configuration Template from the drop-down menu. You can drag the existing configuration templates to the configuration editor. Click **OK**.



4. Navigate to **Infrastructure > Configuration > Configuration Templates** to view the templates created in the list of Configuration Templates.



5. Select the newly created configuration template and click the **Export** button.



The corresponding configuration template gets downloaded on your local system in **.json** format.

To import the configuration templates:

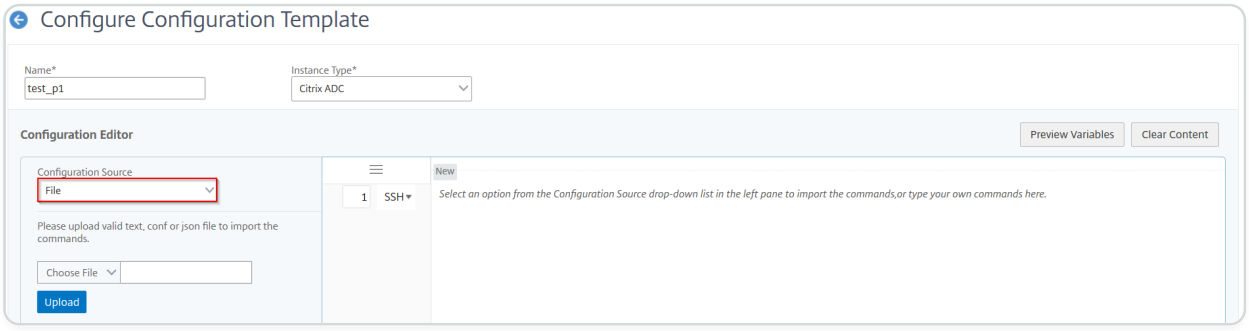
1. Navigate to **Infrastructure > Configuration > Configuration Templates** and click the **Import** button. Select the path where you have the .**json** files of the configuration template and upload

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the .**json** files. It is highly recommended to upload the .**json** files that you have exported already.



2. You can also import the configuration template using **File** option on **Configuration Editor**. Select **File** from the drop-down menu in **Configuration Editor** and **Choose File** (.**json** files) from your local system and upload the configuration template .**json** files.



NOTE

You can import the configuration templates only if the file is saved in the .**json** format. If you import the configuration templates other than **.json** files, from your local system, it shows an error and fails the import of the files.

Configuration audit

This document includes:

- Creating audit templates
- Viewing audit reports
- Audit configuration changes across instances
- Get configuration advice on network configuration
- How to poll configuration audit of NetScaler Console instances
- Generate configuration audit diff for ConfigChange SNMP traps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create audit templates

You want to make sure that certain configurations are running on specific instances for optimal performance of your network. You also want to monitor configuration changes across managed NetScaler instances, troubleshoot configuration errors, and recover unsaved configurations after a sudden system shutdown. You can create audit templates with specific configurations you want to audit on certain instances. NetScaler Console compares these instances with the audit template and reports if there is a mismatch in the configuration. Whenever there is a configuration mismatch, NetScaler Console generates a configuration diff report, which enables you to troubleshoot, and rectify unwanted configuration changes.

You can automate the running of the audit template by

- Scheduling the time at which the template must run
- Setting the frequency at which NetScaler Console must run the template. You can run the template daily, on a specific day in a week, or on a specific date in a month.

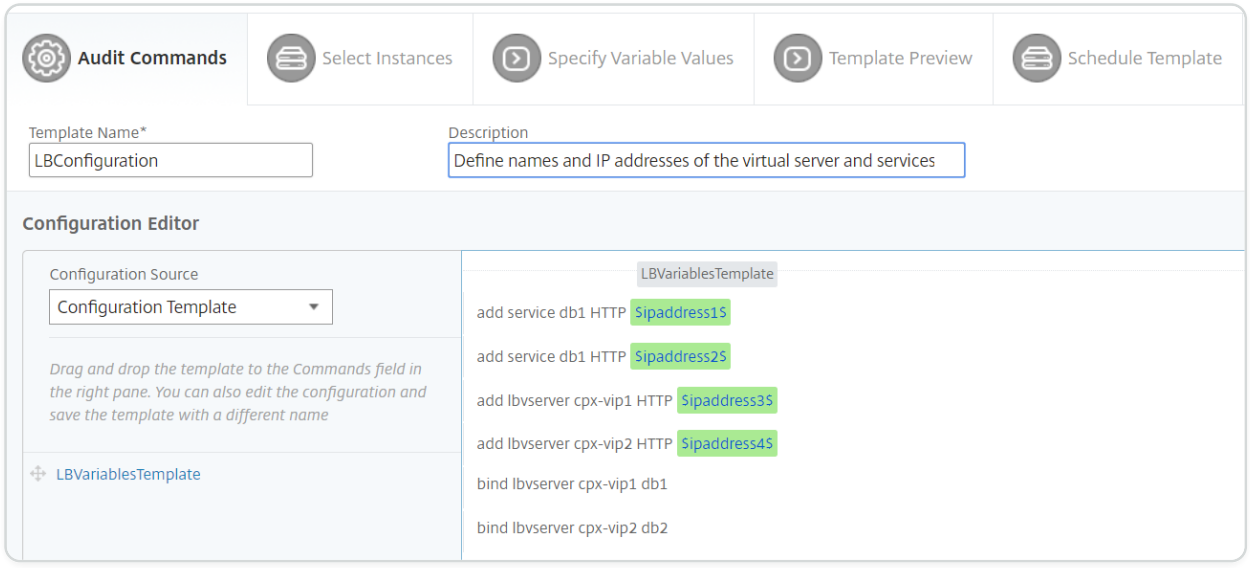
Also, you have an option to send the diff report generated by NetScaler Console to specified email addresses that you can configure. By this option, your user can receive the report as a mail attachment and there is no need for the user to log on to NetScaler Console to export the reports manually.

Note The **Rename** option is disabled for the default configuration templates. However, you can rename custom configuration templates.

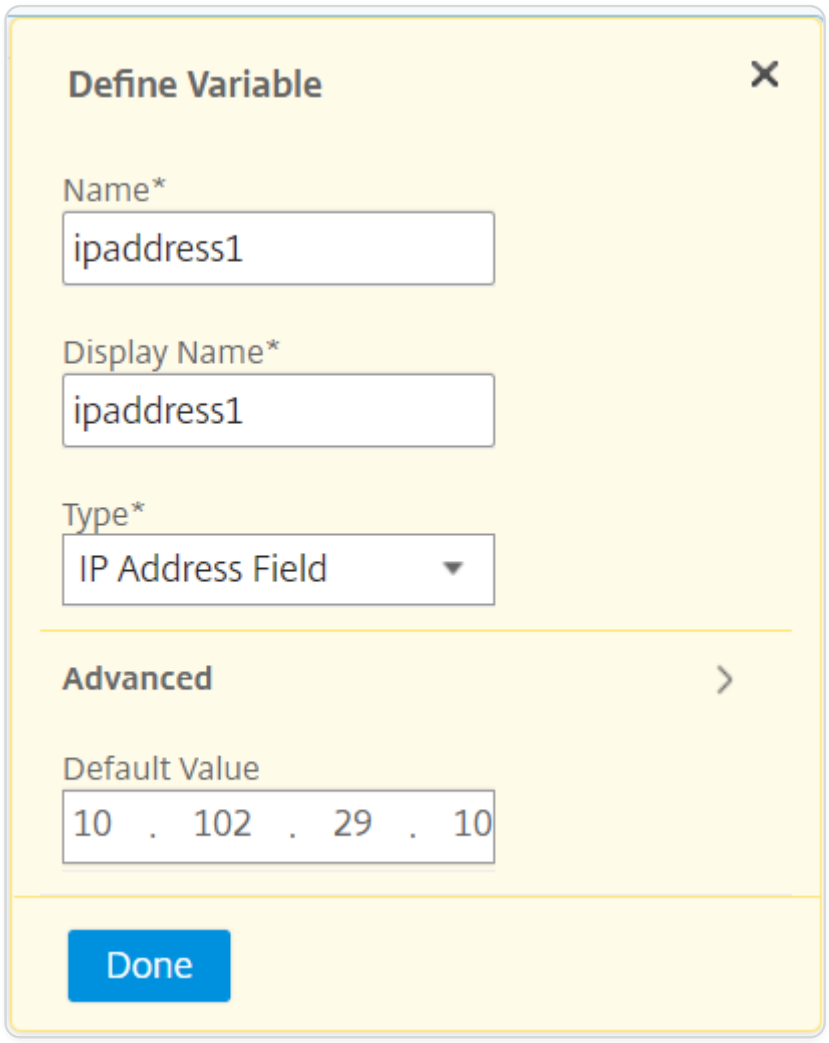
To create audit templates:

1. Navigate to **Infrastructure > Configuration > Configuration Audit > Audit Templates**, and click **Add**.
2. On the **Create Template** page, and in the **Audit Commands** tab, specify the template name and its description.
3. In the **Configuration Editor** page, type in your commands and save the commands as a configuration template. You can also drag an existing template from the left pane to the editor.
4. Select the values that you want to convert to a variable, and then click **Convert to Variable**. For example, select the IP address of the load balancing server "ipaddress1," and click **Convert to Variable**. The variable is now enclosed with "$" as shown in the image below.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

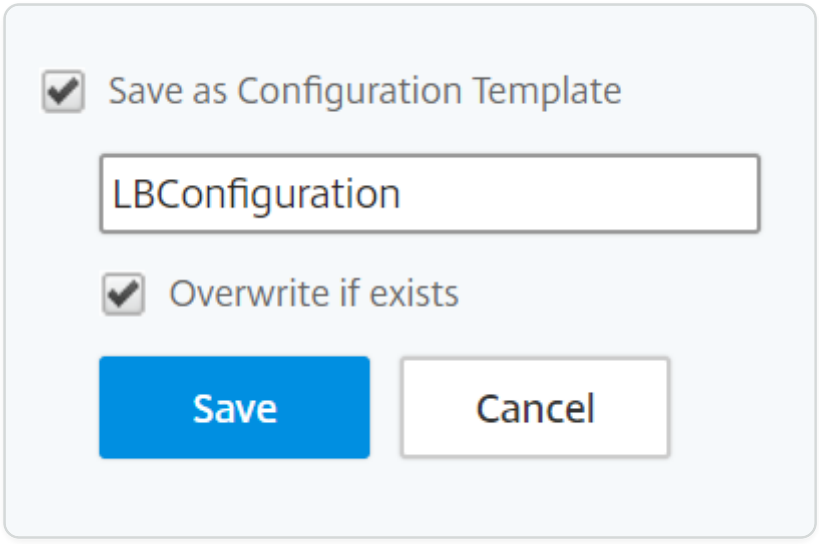


In the **Define Variable** window, set the properties for this variable - name, display name, and the type of the variable. Click the **Advanced** option if you want to further specify a default value for your variable.

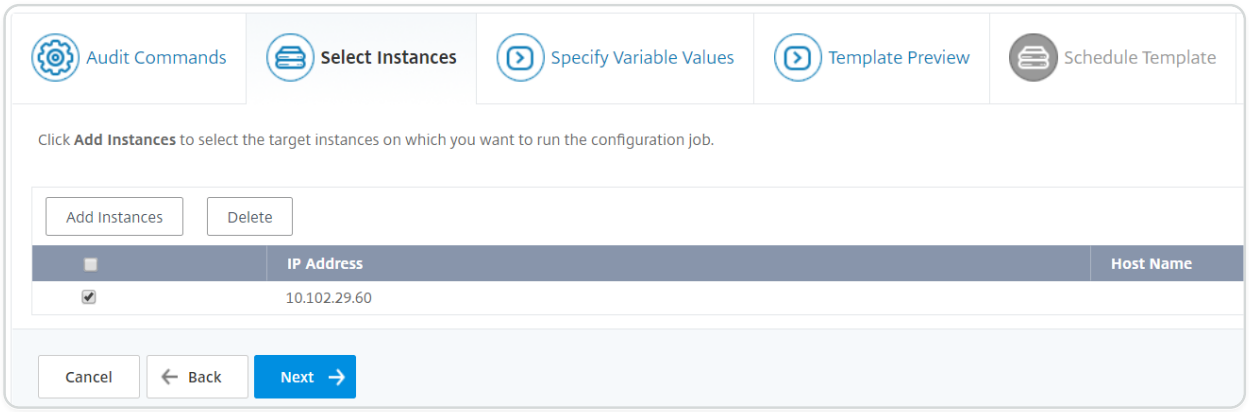


You can also save the commands as a configuration template.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

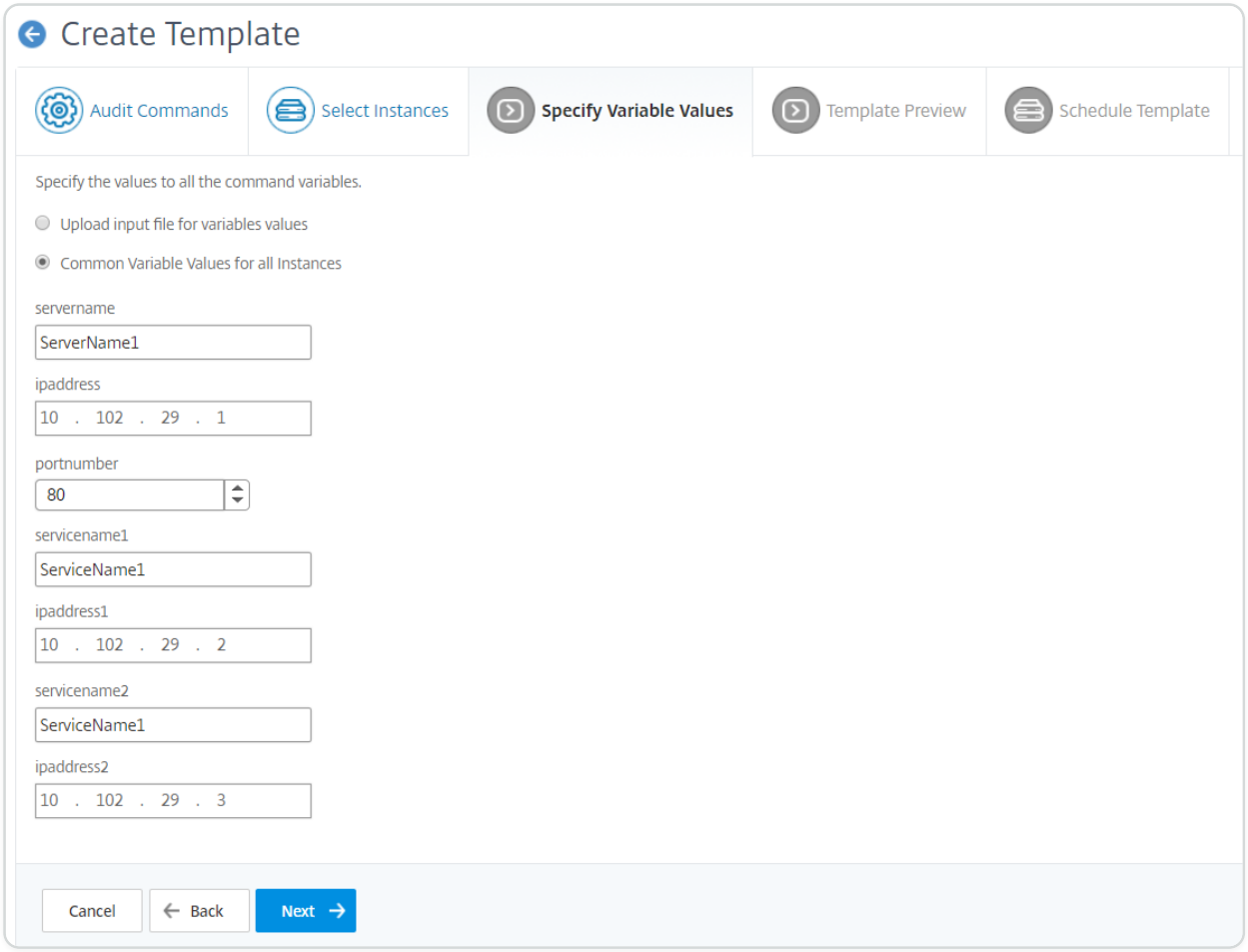


5. Click **Save** and then, click **Next**.
6. In the **Select Instances** tab, select the instances you want to run the configuration audit on and click **Next**.

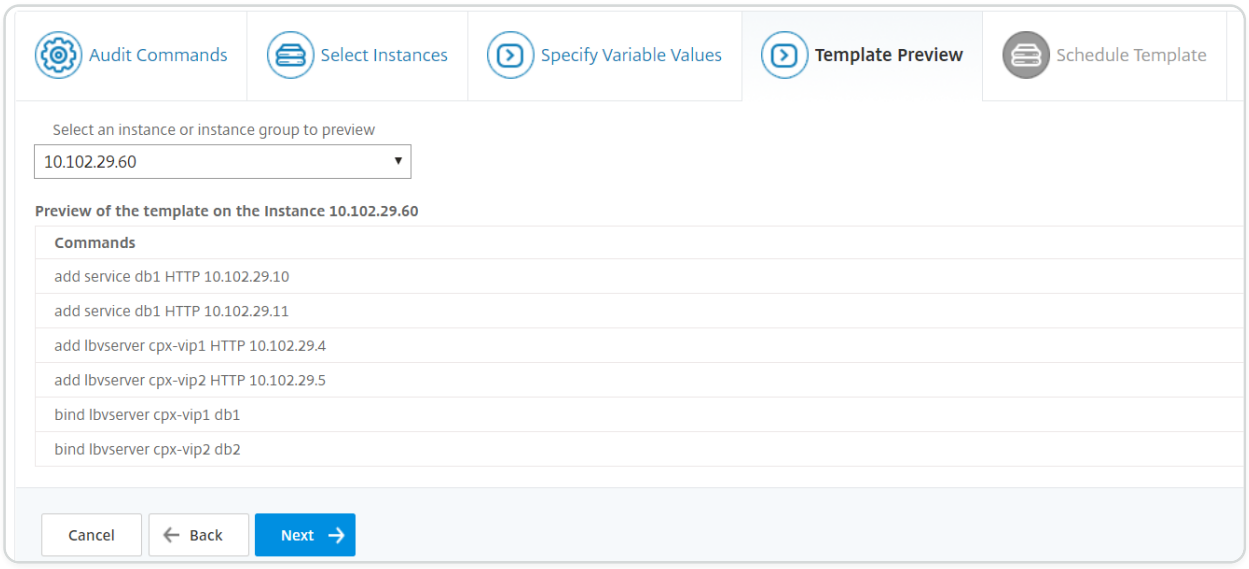


7. In the **Specify Variable Values** tab, you have two options:
   a. Download the input file to enter the values for the variables that you have defined in your commands, and then upload the file to the NetScaler Console server
   b. Enter common values for the variables that you have defined for all instances
8. Click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



9. In the **Template Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group. Click **Next**.



10. In the **Schedule Template** tab, you have the following options to schedule the running of the template and configuring the mail address to send the diff report.

    - **Use global polling interval**. Select this option to run the template on the instances at a time configured globally on NetScaler Console.

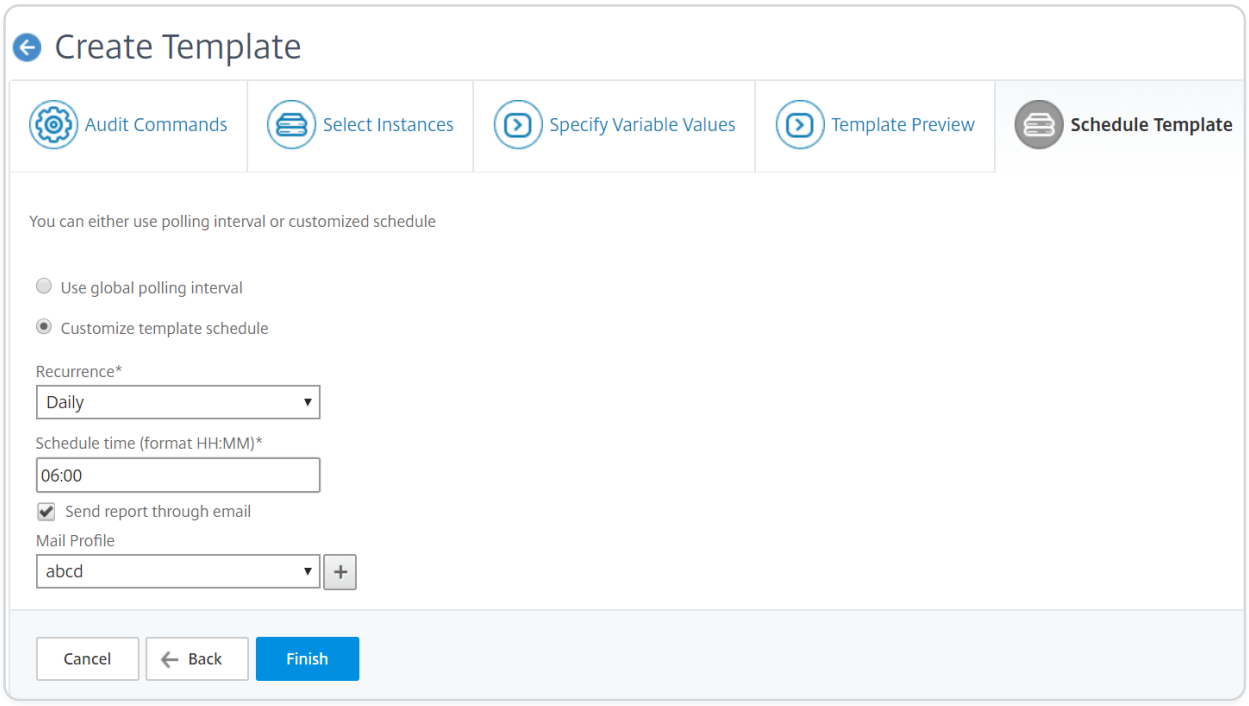
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

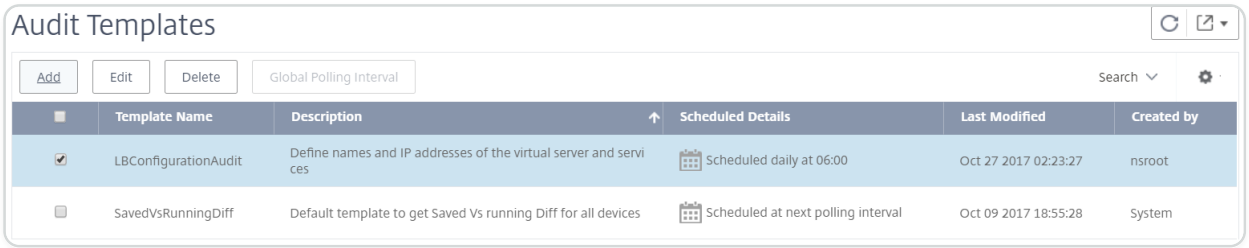
To configure global polling interval in NetScaler Console, navigate to **Infrastructure > Configuration > Configuration Audit > Audit Templates**. and click **Global Polling Interval**. In the **Poll Interval** field, enter the minutes at which NetScaler Console must globally poll the instances.

- **Customize template schedule**. Use this option to configure the time and the frequency at which the templates need to be run
- **Send report through email**. use this option to configure the mail profile to which the diff report must be sent as a mail attachment.

11. Click **Finish**.



The audit template appears in the **Audit Templates** list and is run at the scheduled time against the configurations in the specified instances.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

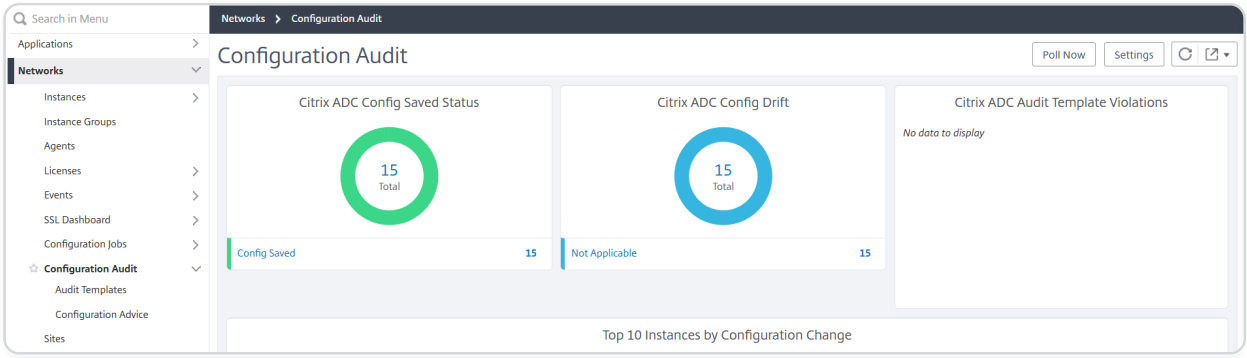
Poll configuration audit of NetScaler instances

NetScaler Console automatically polls the configuration audits every 10 hours to look for configuration changes that occur on NetScaler instances. You can also manually poll the configuration audits to discover recent changes, but polling all the NetScaler instances configuration places a heavy load on the network.

Instead of polling the entire NetScaler instances configuration audit, you can manually poll only the configuration audits of a selected instance or instances.

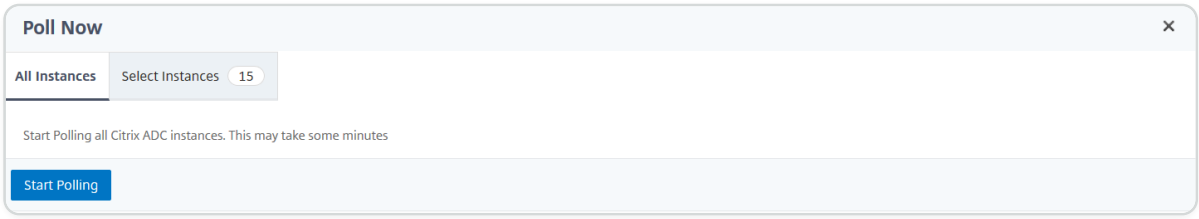
To poll configuration audits of NetScaler instances:

1. In NetScaler Console, navigate to **Infrastructure > Configuration > Configuration Audit**.
2. On **Configuration Audit** page, in the top right-hand corner, click **Poll Now**.

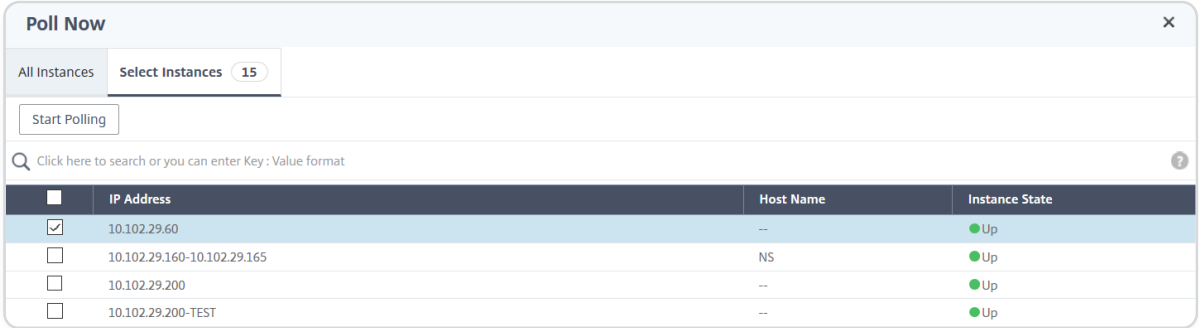


3. The **Poll Now** page pops up, giving you the option to poll all NetScaler instances in the network or poll selected instances.

   a. To poll all NetScaler instances, select the **All Instances** tab and click **Start Polling**.



   b. To poll specific instances, select the **Select Instances** tab, select the instances from the list, and click **Start Polling**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

View audit reports

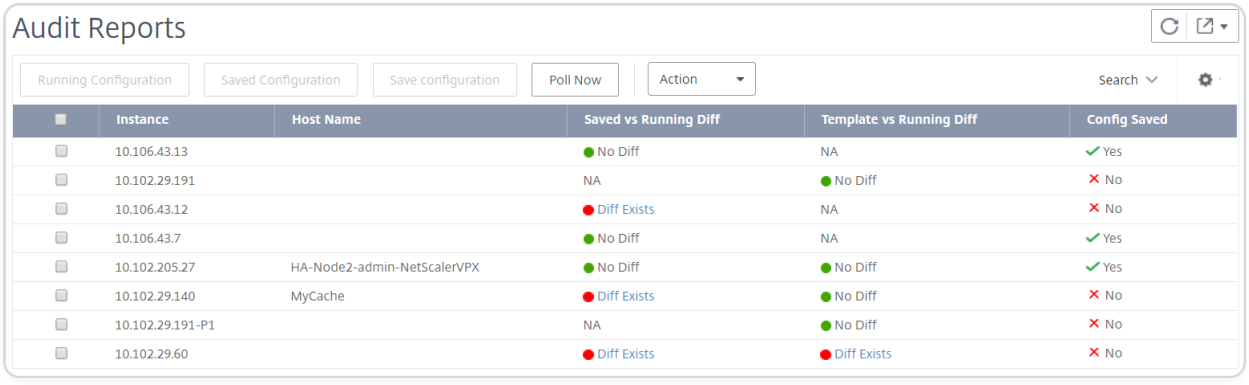
NetScaler Console allows you to view and download the configuration audit diff report in configuration audit section. The configuration audit section enables you to export the summary report across all instances and per instance, and also allows you to export granular diff report for each instance-template pair.

The audit templates that appear in the Audit Templates list are run at the scheduled time against the configurations in the specified instances. The **NetScaler Config Drift** chart on the **Configuration Audit** dashboard displays high-level details about configuration changes in saved against unsaved configurations. When you click **NetScaler Config Drift** chart, the ensuing **Audit Reports** page displays a list of instances that shows both "Diff Exists" and No Diff." You can download the diff reports displayed by NetScaler Console.

NetScaler Console also provides an option to schedule automatic export of diff report as a mail attachment. For more information on how to schedule export of reports, see Creating Audit Templates.

Export configuration audit reports

1. In NetScaler Console, navigate to **Infrastructure > Configuration > Configuration Audit**.
2. On the **Configuration Audit** page, click inside the **NetScaler Config Drift** chart.
3. The **Audit Reports** page lists instances that have a difference. The page also displays a list of instances that does not have any difference in their running configurations.

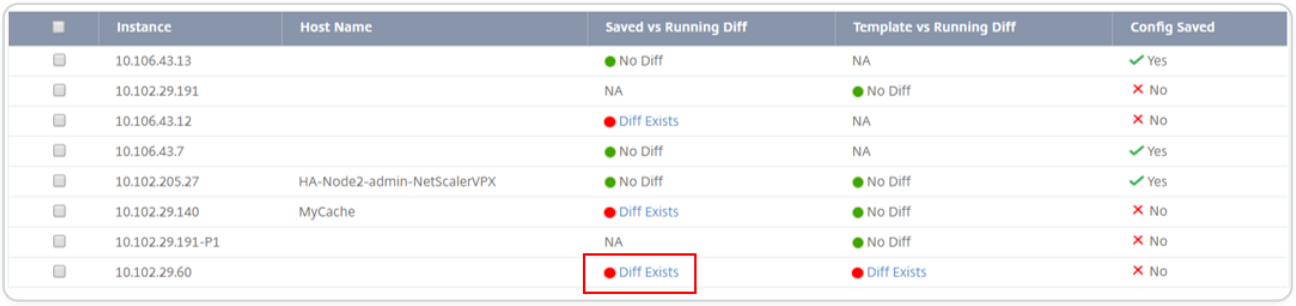


In the image you can see that for some instances a diff is present only in **Saved Vs Running Diff** and for some instances, a diff is present only in **Template vs Running Diff**. For some instances, differences exist in both **Saved Vs Running Diff** and **Template vs Running Diff**.

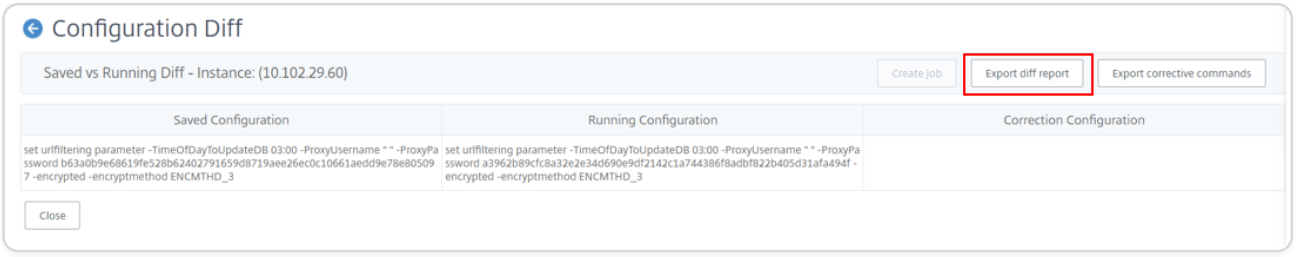
Saved Vs Running Diff:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can view a report of the diff between the configuration saved on the instance and the configuration currently running on that instance. For example, click **Diff Exists** for an instance under **Saved Vs Running Diff.**



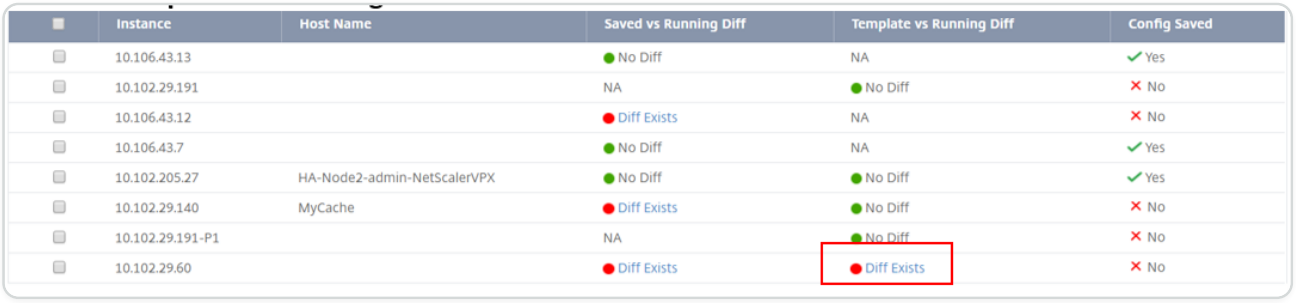
Here, you can see a report for saved configuration against running configuration diff for that instance.



Click **Export diff report** to download a .csv file of the diff report. You can also click **Export corrective** commands to export the commands to a .txt file. You can then run the commands on the associated NetScaler instance from configuration jobs to correct the configuration in that instance.

Template vs Running Diff:

The **Template vs Running Diff** includes all templates other than **Saved Vs Running Diff** which is the default template. You can view the difference that exists between the template and running configuration. For example, click **Diff Exists** for one of the instances under **Template vs Running Diff.**

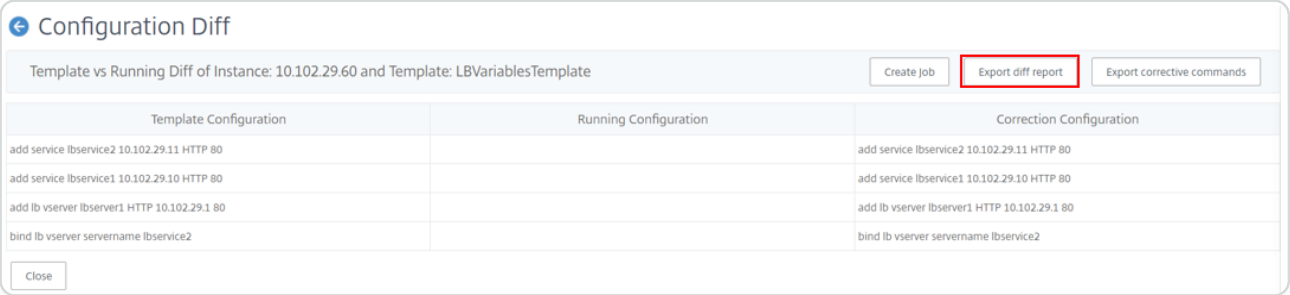


Now you can see that two templates show diff and the NetScaler instance has a different configuration from what the template is looking for.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Click **Diff Exists** again. The following image shows the configuration that the template is looking for and the running configuration that is blank, because no such commands has been configured or has been removed. You can also see the correction configurations or the commands to run to correct the configuration.

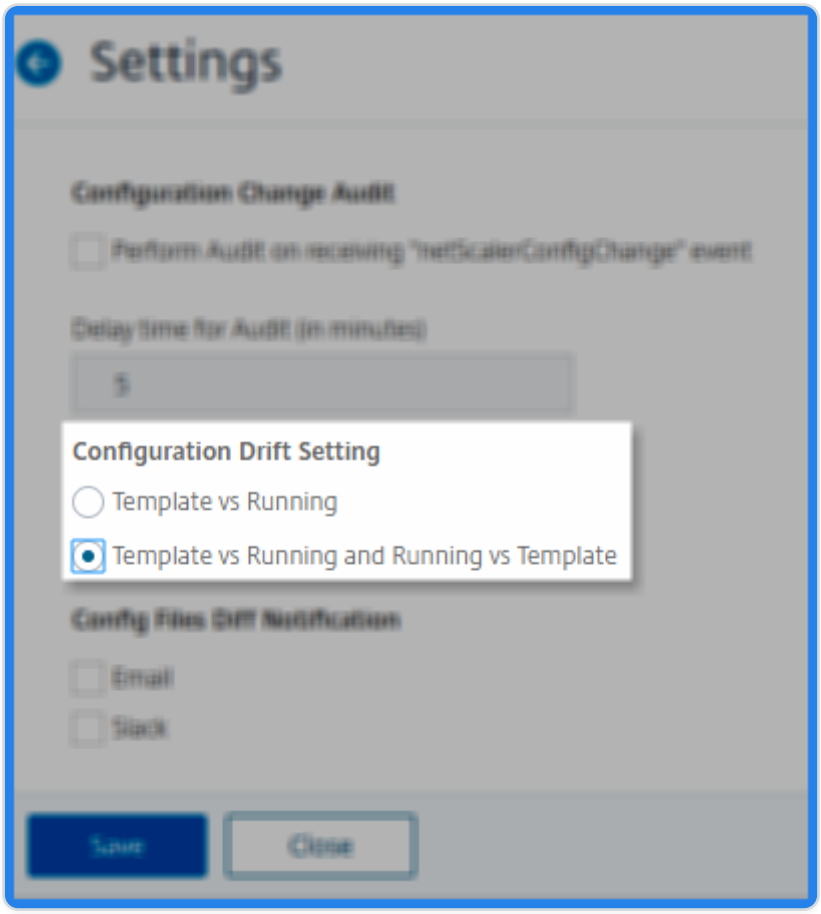


You can also use Template vs Running and Running vs template drift setting, to compare the configuration from both ways:

- Compares the audit template configuration with the running configuration on the instance.
- Compares the running configuration on the instance with the audit template.

By default, the Template vs. running drift setting is selected. To modify the drift setting, from the NetScaler Console GUI, select **Settings** in the **Configuration Audit** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Click **Export diff report** to download a .csv file of the diff report. You can also click **Export corrective commands** to export the commands to a .txt file. You can then run the commands in CLI to correct the configuration in that instance.

The following image shows an example .csv diff file that is downloaded to your system:

#Template vs Running Diff of Instance: 10.102.29.60 and Template: LBVariablesTemplate		
Template Configuration	Running Configuration	Correction Configuration
add service lbservice2 10.102.29.11 HTTP 80		add service lbservice2 10.102.29.11 HTTP 80
add service lbservice1 10.102.29.10 HTTP 80		add service lbservice1 10.102.29.10 HTTP 80
add lb vserver lbserver1 HTTP 10.102.29.1 80		add lb vserver lbserver1 HTTP 10.102.29.1 80
bind lb vserver servername lbservice2		bind lb vserver servername lbservice2

View the file status audit reports

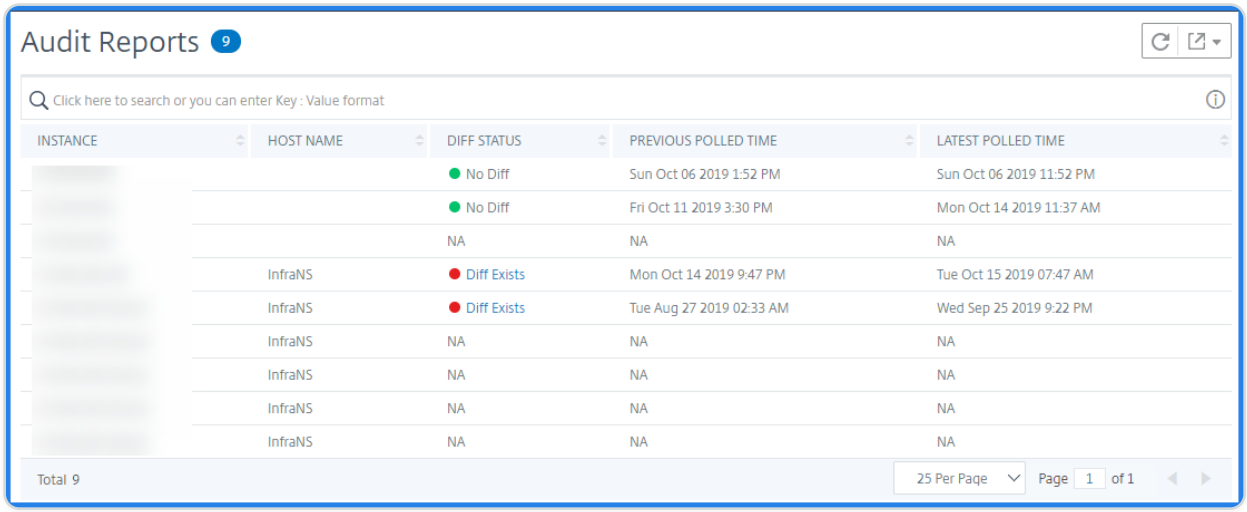
Using the **NetScaler File Status** chart, you can monitor whether any files are added, modified, or removed in the `nsconfig` folder. For example: if the license file is updated on a NetScaler instance, you can check when this file was last updated and take actions appropriately.

To export the file status audit reports for the NetScaler instances:

1. In NetScaler Console, navigate to **Infrastructure > Configuration > Configuration Audit**.
2. On the **Configuration Audit** page, click inside the **NetScaler File Status** chart.

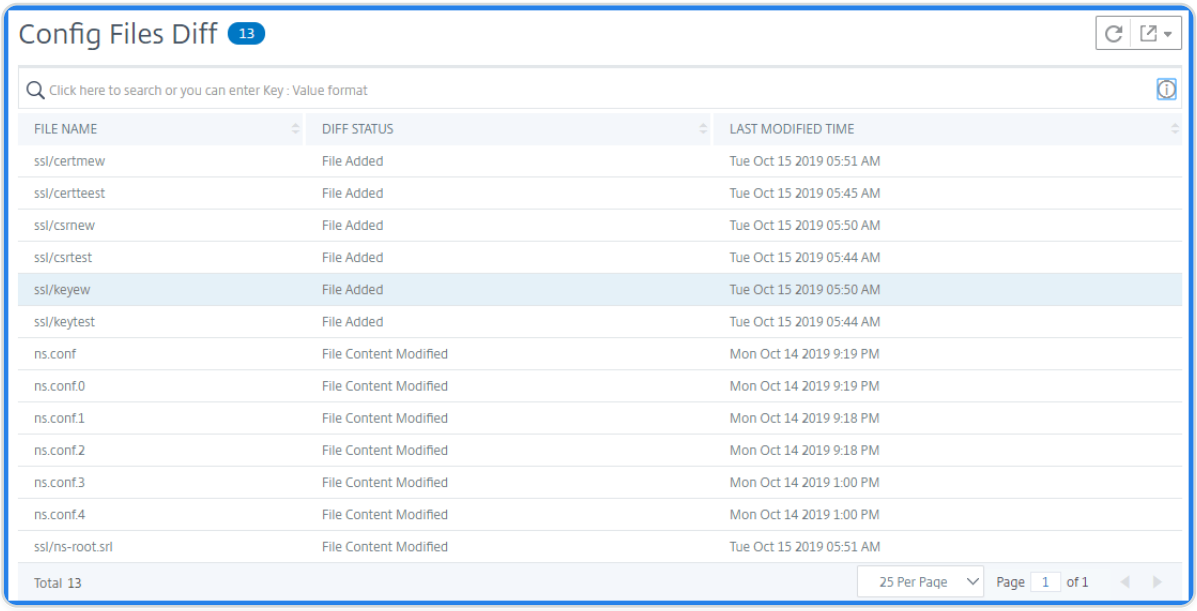
   The **Audit Reports** page lists instances with the Diff status.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **Diff Status** is calculated for the interval between the **Previous Polled Time** to the **Latest Polled Time**. The **Diff Status** can be one of the following:

- **Diff exists** - This status indicates the files have changed in the `nsconfig` folder of an instance since the **Previous Polled Time**. To view what has changed on the file, click **Diff Exists**.



- **No Diff** - This status indicates the files in the `nsconfig` folder hasn't changed since the previous polled time.
- **NA** - This status indicates monitoring the file status is not applicable. This status appears when the NetScaler Console doesn't poll the instance. For example, when an instance is added newly or instance state is inactive the polling of the instance doesn't occur.

Export the report of this dashboard

To export the report of this page, click the **Export** icon on the top right side of this page. On the **Export** page, you can do one of the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Select **Export Now** tab. To view and save the report in PDF, JPEG, PNG, or CSV format.
2. Select **Schedule Export** tab. To schedule the report daily, weekly, or monthly and send the report over email or slack message.

NOTE

- If you select **Weekly** recurrence, ensure that you select the weekdays on which you want the report to be scheduled.
- If you select **Monthly** recurrence, ensure that you enter all the days that you want the report to be scheduled separated by commas.

Exclude files from Config Audit

You can exclude specific files from Config Audit so that they are not monitored for change. Use exclusions for system-generated or frequently updated files (for example, files that change daily) to reduce noise and avoid false positives in audit results.

Examples for file name (or relative path) to exclude from Config Audit file diff:

- Valid file name (or relative path)
  - `ns.conf`, `ssl/ns.cert`
- Invalid file name (or relative path)
  - `/ns.txt`, `\nsconfig\ns.conf` (Excluded file name must be a relative path)
  - `ñs.conf` (Excluded file name must contain only ASCII characters)
  - `C:/nsconfig/ns.conf` (Excluded file name must not use drive-letter paths)
  - `ssl/../../ns.conf` (Excluded file name must not contain parent-directory traversal `..`)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTES:

- All files under `/nsconfig/license/` are excluded from Config Audit by default. NetScaler Console writes LAS files to this directory every 8 hours during token refresh cycles. Since these files are entirely NetScaler Console-managed and not part of the customer's NetScaler configuration, they trigger false-positive **Diff Exists** alerts. The `license/` directory is now seeded as a default exclusion to prevent this false-positive. You can remove this exclusion if needed.
- File diff comparison is applicable only to files under the `/nsconfig` directory.
- When excluding files from Config Audit, users must specify relative paths under `/nsconfig`. For example, if there is an `ssl` folder under `/nsconfig`, exclusions can be provided as: `ssl/abc.pem`
- File differences outside `/nsconfig` are not considered as part of the Config Audit diff.

To exclude files from Config Audit, perform the following steps:

1. Navigate to **Infrastructure > Configuration > Configuration Audit**.
2. Select **Settings**.
3. Under **NetScaler Config File Settings**, add the file paths you want to exclude from auditing.
4. Click **Save**.

Generate configuration audit diff for ConfigChange SNMP Traps

Whenever there is a configuration change in a NetScaler instance in the network, the configuration file is updated. The instance sends a ConfigChange SNMP trap to NetScaler Console. You can enable NetScaler Console to perform a configuration audit on that instance when the instance sends a ConfigChange SNMP trap.

If any difference exists between the audit template configuration and the running configuration, a Diff Exists status message appears on the Audit Report page. Clicking the Diff Exits link takes you to the Configuration Diff page, where you can view the corrective command. You can use these corrective commands to create a configuration job and run that on the specific NetScaler instances. When you run the configuration job, the instances are brought back to the desired configuration. For more information on how to create configuration job from corrective commands, see How to Create Configuration Jobs from Corrective Commands on NetScaler Console.

To run configuration audit templates on receiving ConfigChange SNMP trap:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console allows you to enable the option to run the configuration audit template in NetScaler Console.

1. In NetScaler Console, navigate to **Infrastructure > Configuration > Configuration Audit**.
2. Click **Settings** on the **Configuration Audit** page.
3. Click the edit icon in the **Configuration Change Audit Settings** section.
4. Select the **Do Configuration Audit when netScalerConfigChange event is received** check box.

   NOTE

   This is a global setting for all instances. NetScaler Console performs a configuration audit for every instance that it receives the netScalerConfigChange SNMP traps in the future.

5. In the **Time delay to run the Audit Template (in minutes)** field, type the minutes. NetScaler Console runs the configuration audit template on the NetScaler instance after this time delay when it receives the ConfigChange SNMP trap by that instance.

Audit configuration changes across instances

You want to make sure that certain configurations are running on specific instances for optimal performance of your network. You also want to monitor configuration changes across managed NetScaler instances, troubleshoot configuration errors, and recover unsaved configurations after a sudden system shutdown. You can create audit templates with specific configurations you want to run on certain instances. The NetScaler Console compares these instances with the audit template and reports if there is a mismatch in configuration. This comparison enables you to troubleshoot and rectify the errors.

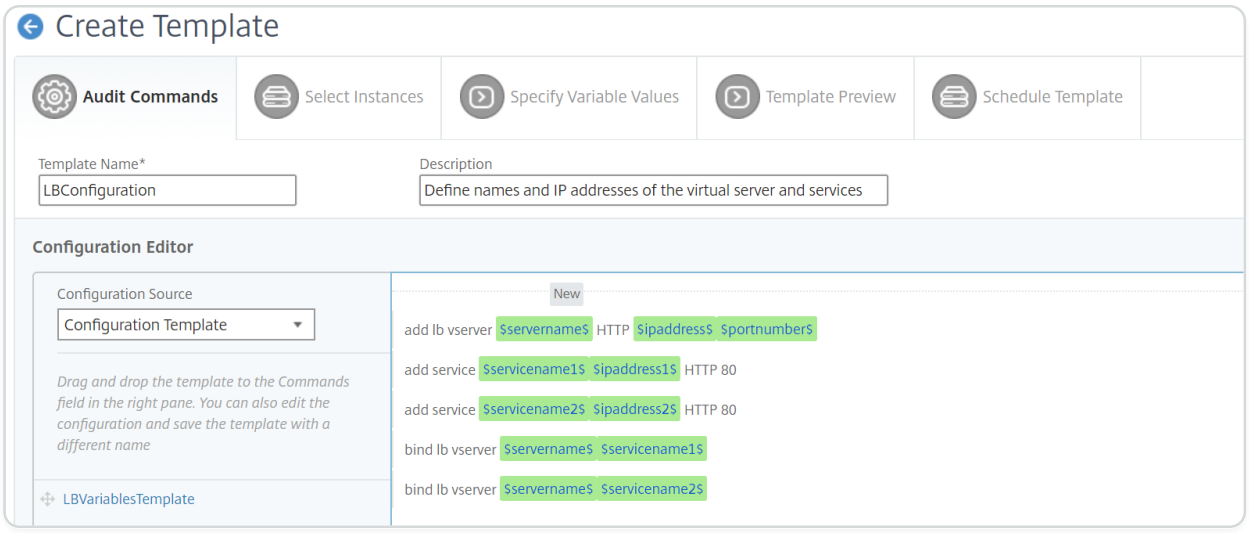
You can automate the running of the audit template by scheduling the time at which the template must be run. You can also set the frequency at which NetScaler Console must run the template. You can run the template daily, on a specific day in a week, or on a specific date in a month. You can also send the diff report generated by NetScaler Console to specified email addresses that you can configure. By this option, your user receives the report as a mail attachment and there is no need for the user to log on to NetScaler Console to check the reports manually.

To create audit templates:

1. Navigate to **Infrastructure > Configuration > Configuration Audit > Audit Templates**, and click **Add**.

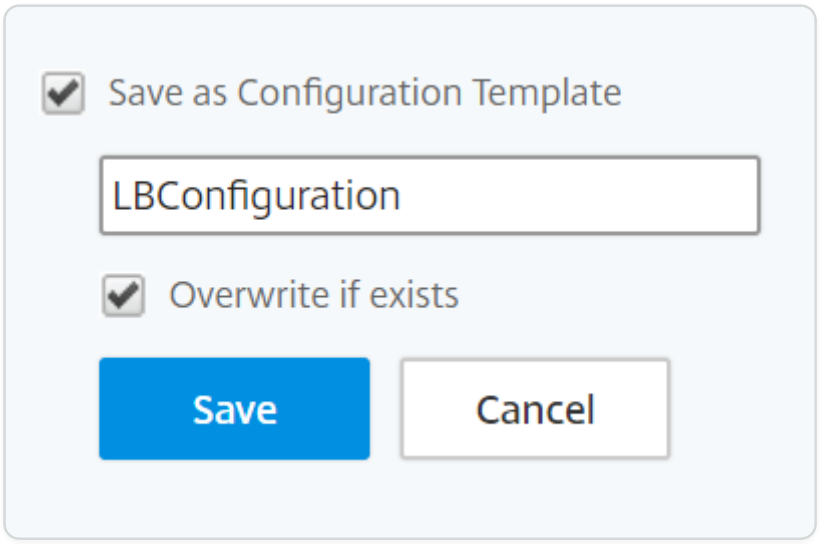
© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. On the **Create Template** page, and in the **Audit Commands** tab, specify the template name and its description.
3. In the **Configuration Editor**, type in your commands and save the commands as a configuration template. You can also drag an existing template from the left pane on the editor.
4. Select the values that you want to convert to a variable, and then click **Convert to Variable**. For example, select the IP address of the load balancing server `ipaddress` and click **Convert to Variable** as shown in the following image.



Click the **Advanced** option if you want to further specify a default value for your variable.

You can also save the commands as a configuration template.



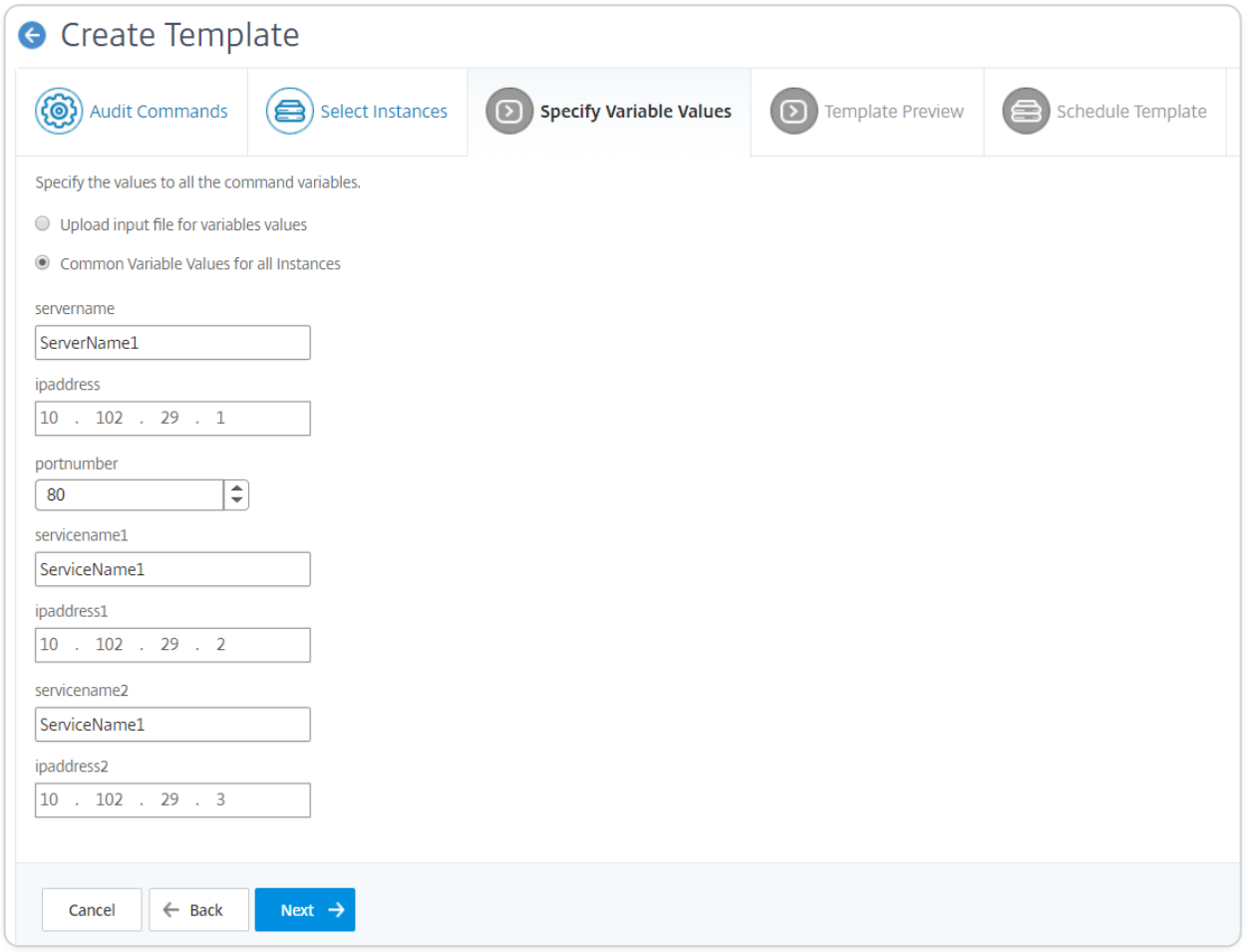
5. Click **Save** and then, click **Next**.
6. In the **Select Instances** tab, select the instances you want to run the configuration audit on.
7. In the **Specify Variable Values** tab, you have two options:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Download the input file to enter the values for the variables that you have defined in your commands, and then upload the file to the NetScaler Console server

b. Enter common values for the variables that you have defined for all instances

8. Click **Next**.



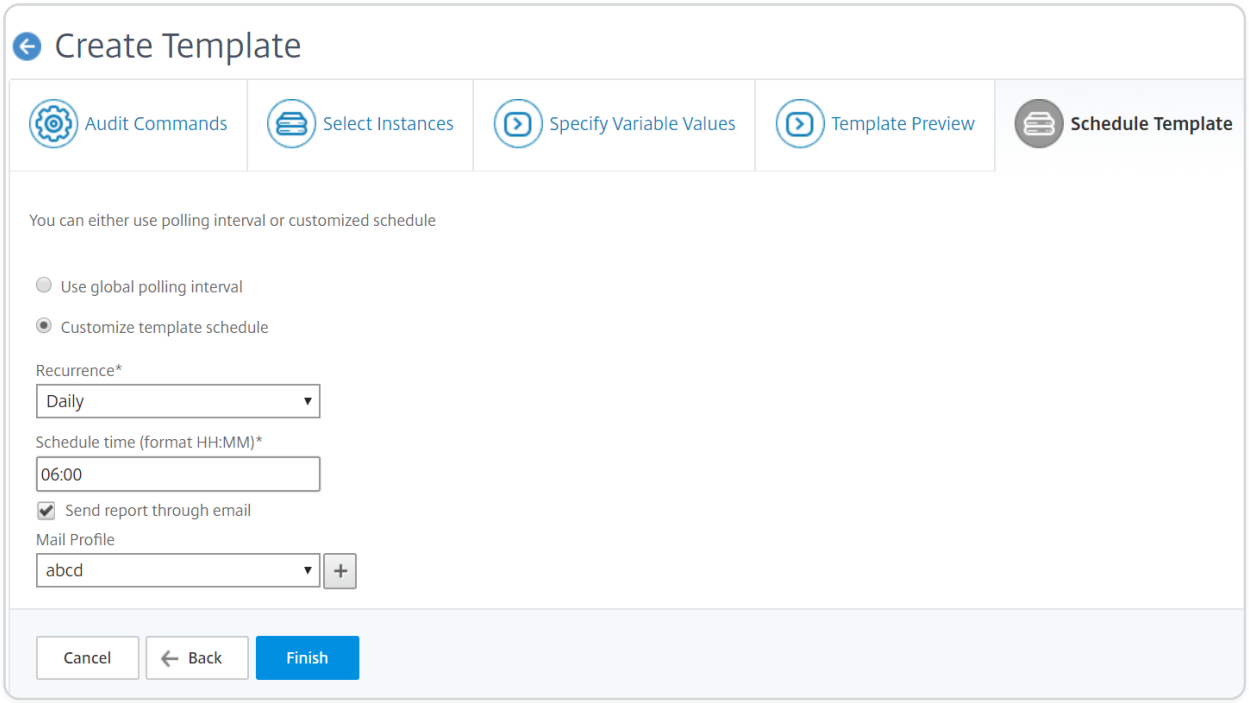
9. In the **Template Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group. Click **Next**.

10. In the **Schedule Template** tab, you have three options to automate the running of the template and the mail address to send the diff report.

    - **Use global polling interval**. Select this option to run the template on the instances at a time configured globally on NetScaler Console
    - **Customize template schedule**. Use this option to configure the time and the frequency at which the templates must be run
    - **Send report through email**. Use this option to configure the mail profile to which the diff report must be sent as a mail attachment.

11. Click **Finish**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



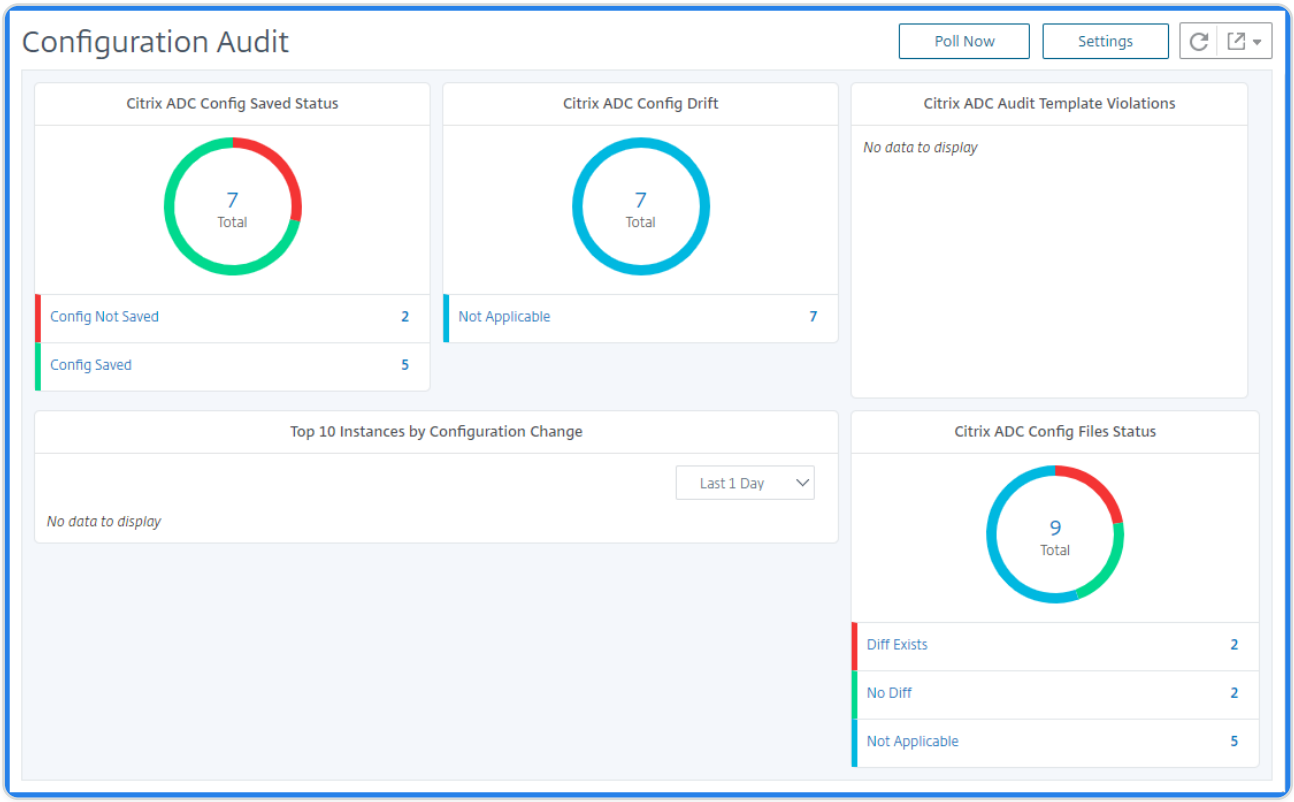
The audit template appears in the Audit Templates list and is run at the scheduled time against the configurations in the specified instances.

Viewing Details of Configuration Changes

You can also use the Configuration Audit dashboard to view high-level details about configuration changes such as:

- The top 10 instances by configuration change
- The number of saved and unsaved configurations
- The file added, removed, or modified in the `nsconfig` folder

© 1997–2026 Citrix Systems, Inc. All rights reserved.

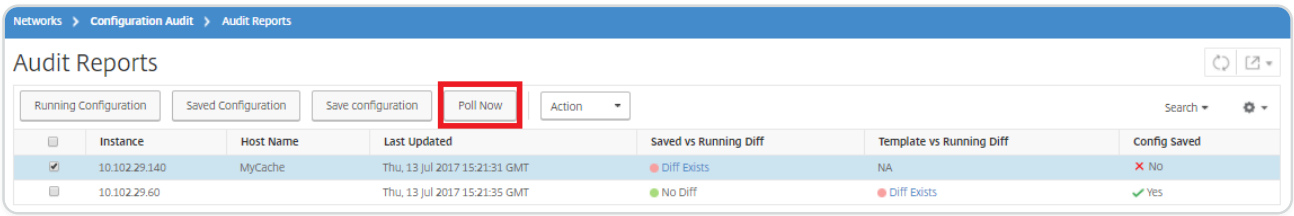


NetScaler Console also allows you to poll configuration audits manually and adds all the configuration audits of the instances immediately to the NetScaler Console. To do so, navigate to **Infrastructure > Configuration > Configuration Audit**, click **Poll Now,** the pop-up page **Poll Now** provides you an option to poll all NetScaler instances in the network, or poll the selected instances.

You can also force an audit on an instance. To do so, click the any of the following charts:

- **NetScaler Config Saved Status**
- **NetScaler Config Drift**

On the **Audit Reports** page, select the instance and, in the **Action** list, select **Poll Now**.



The **NetScaler Config File Status** chart provides you the status of the NetScaler files present in the `nsconfig` folder. The NetScaler Console records and compares changes in files within the `nsconfig` folder and displays the differences. See, View the file status audit reports.

Set configuration audit notifications

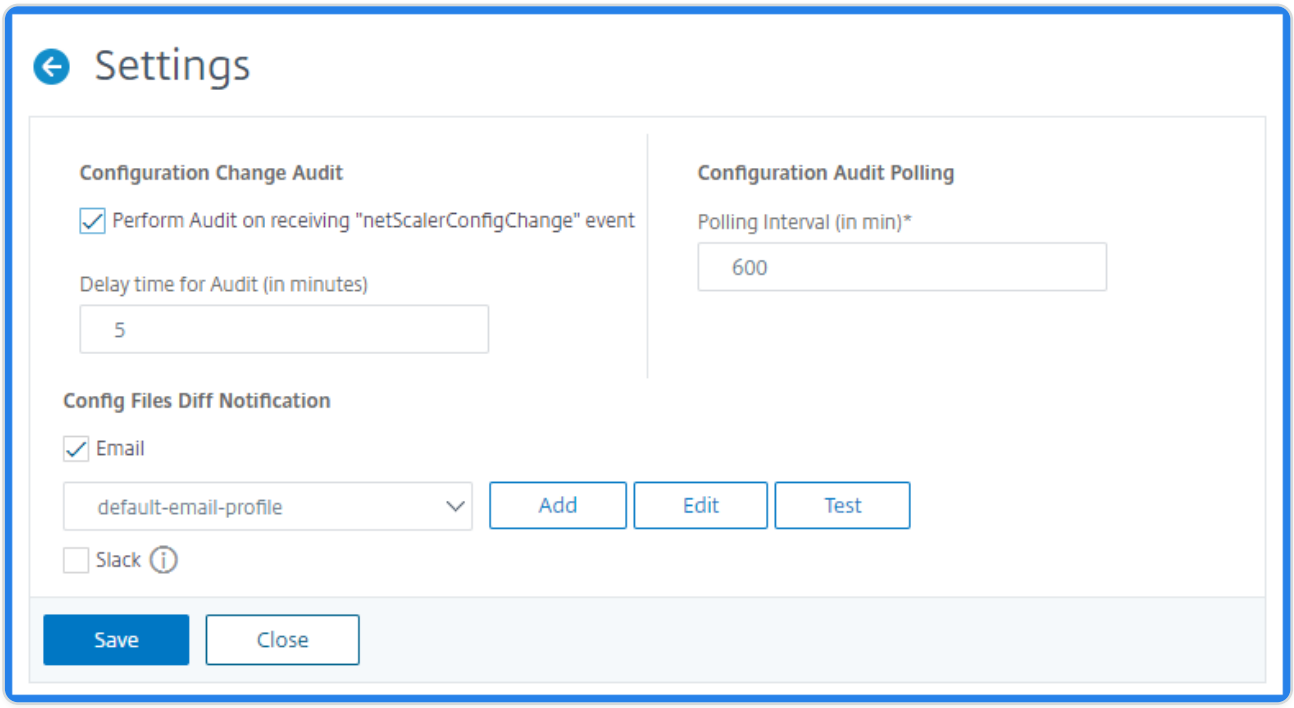
1. Navigate to **Infrastructure > Configuration > Configuration Audit**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. On the **Configuration Audit** page, click **Settings**.
3. On the **Settings** page:
   a. Select the **Perform Audit on receiving "netScalerConfigChange event** check box, to enable the notification settings.
   b. Set the Delay time for Audit.
4. In **Configuration Audit Polling**, set the **Polling Interval**.

   The NetScaler Console polls the configuration audit events for the specified polling interval.
5. In **Config Files Diff Notification**, select the platform on which you want to receive the notifications:

   - **Email** - Select the email distribution list. Click Add to add a email distribution list to receive notification.
   - **Slack** - Select the Slack channel from the list. Click Add to add a channel to receive notification.



Get configuration advice on network configuration

You set up your NetScaler instances with optimal configurations so that you can achieve optimal performance on your applications. However, it is possible that some configurations might not be standard configurations, which affect the performance of your applications.

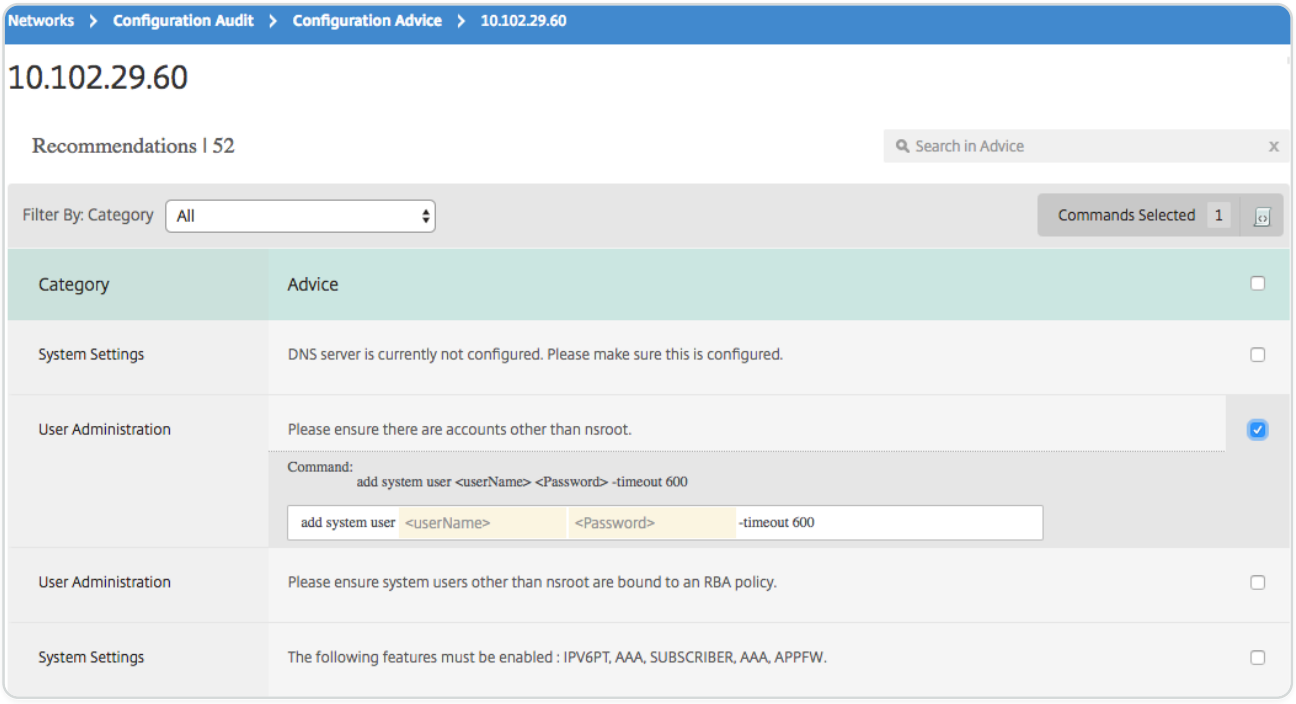
© 1997–2026 Citrix Systems, Inc. All rights reserved.

To help you optimize your application performance, NetScaler Console analyzes the NetScaler instance configuration and provides you with recommendations. You can apply the recommended configurations from NetScaler Console.

To analyze the NetScaler instance:

1. Navigate to **Infrastructure > Configuration > Configuration Audit > Configuration Advice**.
2. Do one of the following:
    - Click **Upload Configuration File** and upload the configuration file of your network instance.
    - Click **Select Device** and select the NetScaler instance that you want to analyze.

NetScaler Console analyzes the configuration on your instance and provides a list of configuration recommendations as shown in the in the following image. Click the check box next to a configuration advice to view the corrective commands.

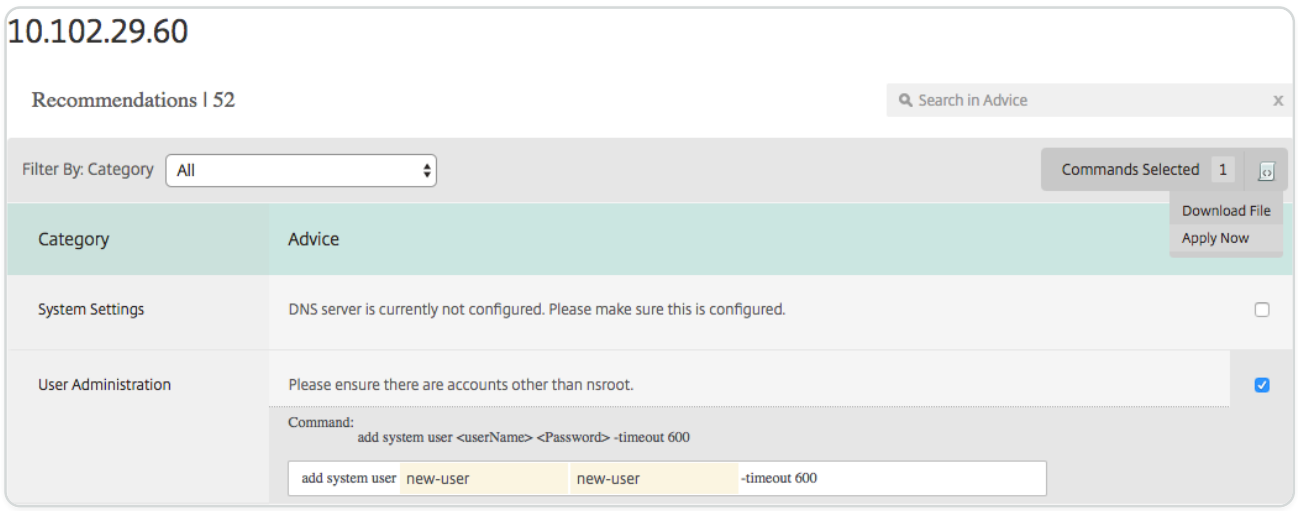


If you want to update your configuration, specify the values for the variables in the corrective commands and click **Apply Now** as shown in the following image.

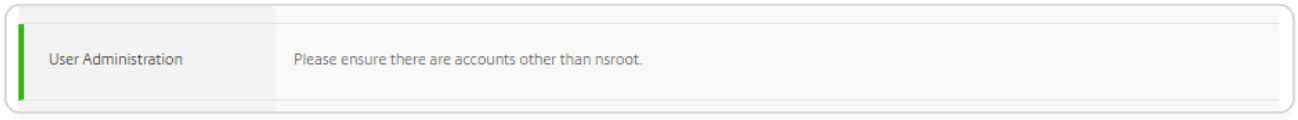
NOTE

The commands listed here are only recommendations. A user with read and write access might be able to edit any command using this feature. Ensure that you grant a limited privileged access to users whom you think must not edit the commands.

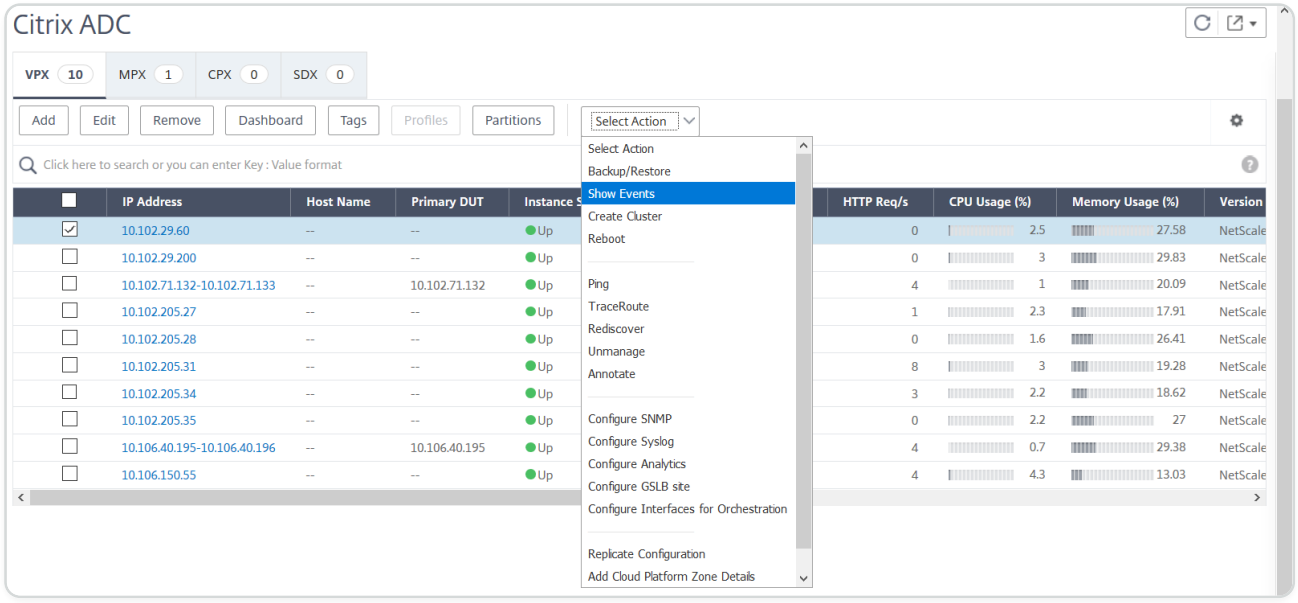
© 1997–2026 Citrix Systems, Inc. All rights reserved.



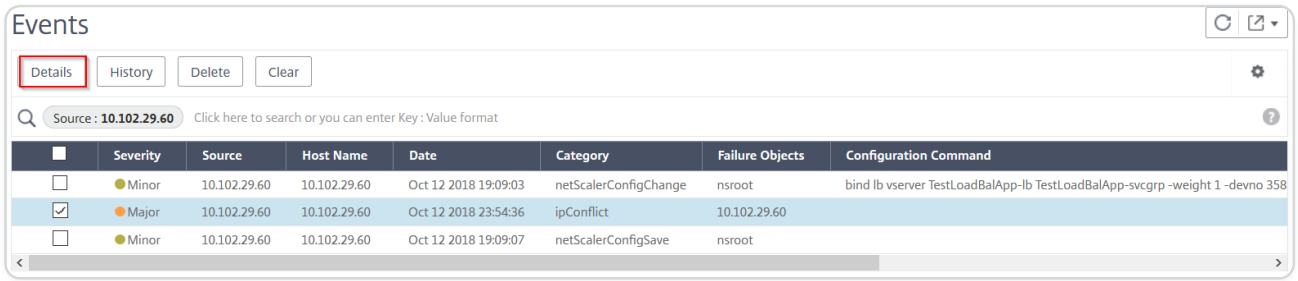
When the command is successfully run on the network instance, the check box next to the advice disappears.



If you want to view the details of the commands run on your network instance, navigate to **Infrastructure > Instances > \<Instance_Type>**, select the IP address of the instance, and then click **Show Events** from the **Select Actions** drop-down list.



On the **Events** page, you can view the details of the configuration change.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Upgrade jobs

IMPORTANT:

File based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler® versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Supported from early September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Note: LAS support for Console on-prem is from release 14.1-51.x onwards. However, file-based licensing is deprecated as of April 15 2026 from Console on-prem releases 14.1-51.x onwards and 13.1-60.x onwards. If you upgrade to Console on-prem release 14.1-51.x or release 13.1-60.x or later, you can continue using file-based licensing until 15th April 2026. However you must upgrade to Console on-prem release 14.1-51.x or later, and switch to LAS before 15th April 2026 because Console on-prem 13.1 does not support LAS.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don’t apply where prohibited by law or regulation.
You can create the following maintenance tasks using NetScaler Console. You can then schedule the maintenance tasks at a specific date and time.

- Upgrade NetScaler instances

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Upgrade NetScaler SDX instances
- Upgrade NetScaler BLX instances
- Upgrade NetScaler instances in the Autoscale Group
- Configure HA pair of NetScaler instances
- Convert HA pair of instances to Cluster

NOTE:

While you can select any number of NetScaler instances for upgrade, NetScaler Console service supports a maximum of 100 concurrent upgrade threads. This means that only 100 instances can be upgraded simultaneously. This limit is dynamic and might vary based on concurrent upgrade activity from other tenants.

Pre-upgrade validation

NetScaler Console performs the following checks:

- **Disk Space Availability on `/var`**: Verifies that sufficient free space is available on the `/var` partition to safely perform image extraction, and installation operations.
- **Disk Space Availability on /flash**: Checks that the `/flash` partition has the minimum required free disk space to support essential system operations during installation.
- **NSPEPI Configuration Check**: Validates the NetScaler configuration file for unsupported or invalid policies to prevent configuration errors after installation or upgrade.
- **High Availability (HA) Configuration Check**: Verifies HA state and role consistency to ensure a healthy and supported HA setup.
- **SSH Connectivity Check**: Confirms SSH accessibility, trust validation, and connectivity to target devices required for remote installation and management operations.
- **Matching ns.conf for Downgrade**: Ensures an appropriate and compatible `ns.conf file` is available for downgrade scenarios to prevent configuration incompatibility.

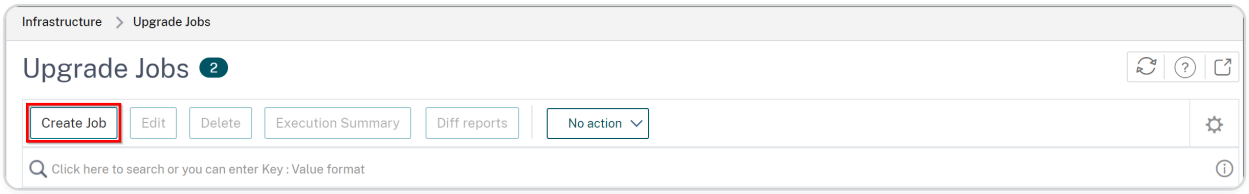
All pre-check results are categorized uniformly as follows:

- **Critical (Blocking)**: The upgrade is blocked. All reported issues must be resolved before proceeding.
- **Warning**: The upgrade can proceed with administrator approval.
- **Advisory**: The upgrade can proceed with administrator approval.

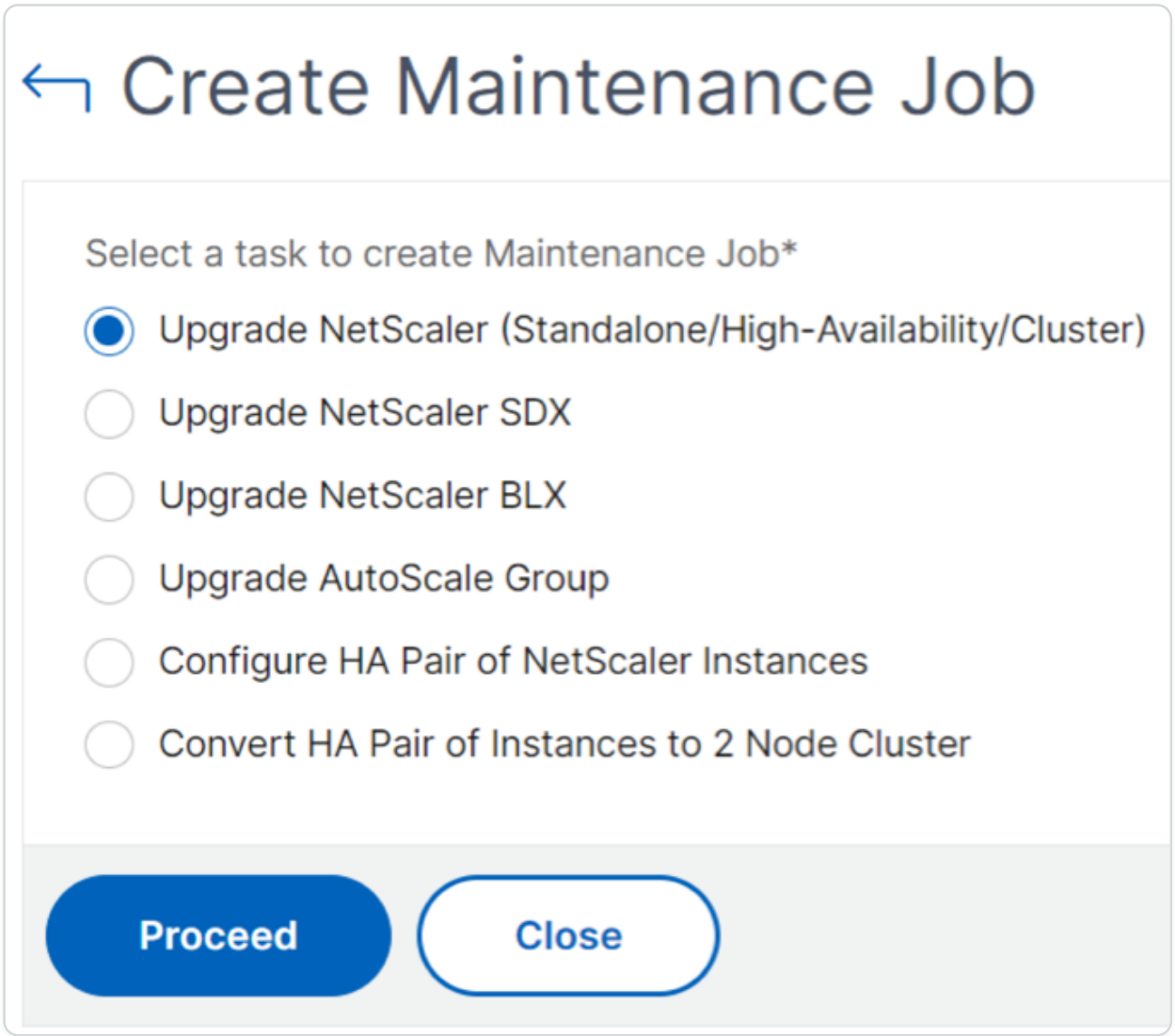
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schedule upgrading of NetScaler instances

1. In NetScaler Console, navigate to **Infrastructure > Upgrade Jobs**. Click **Create Job**.



2. In **Create Maintenance Jobs**, select **Upgrade NetScaler (Standalone/High-Availability/ Cluster)** and click **Proceed**.



3. In **Select Instance**, type a name of your choice for **Job Name**.
4. Click **Add Instances** to add NetScaler instances that you want to upgrade.

   - To upgrade an HA pair, specify the IP address of a primary or secondary node. However, using the primary instance to upgrade the HA pair is recommended.
   - To upgrade a cluster, specify the cluster IP address.

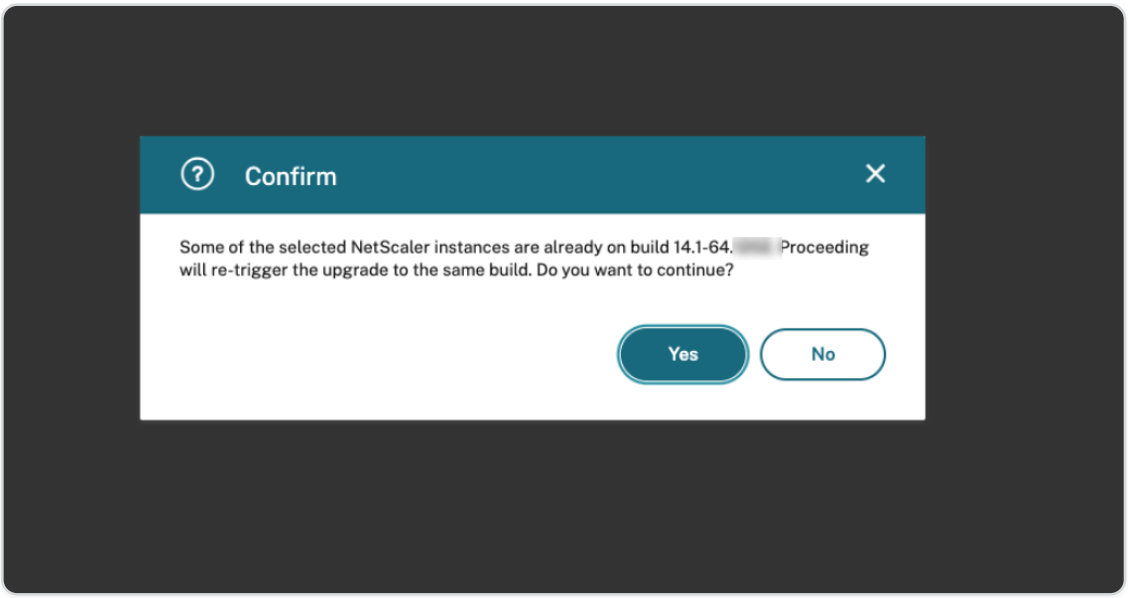
© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Click **Next** to select the image. Select one of the following options from the **Software Image** list:

   - **Local** - Select the instance upgrade file from your local machine.
   - **Appliance** - Select the instance upgrade file from an NetScaler Console file browser. The NetScaler Console GUI displays the instance files that are already uploaded at server side.
     - **Skip image uploading to NetScaler if the selected image is already available** - Select this option if the image is already present in the NetScaler instance.
     - **Clean software image from NetScaler on successful upgrade** - Select this option to clear the uploaded image in the NetScaler instance after the instance upgrade.

NOTE:

- If the selected instances are already on the target build, a warning is displayed. This warning helps prevent the selection of incorrect instances during upgrade jobs. If you intend to re-upgrade the instances, ignore the warning and continue with the upgrade.



- If the selected instance already has an existing upgrade job scheduled, NetScaler Console displays a warning message. This warning message helps prevent unintentionally scheduling duplicate upgrade jobs on the same NetScaler instance.

6. Click **Next** to start the pre-upgrade validation on the selected instances.

   The **Pre-upgrade validation** tab displays the failed instances. Remove the failed instances and click **Next**. For more information, see Pre-upgrade validation.

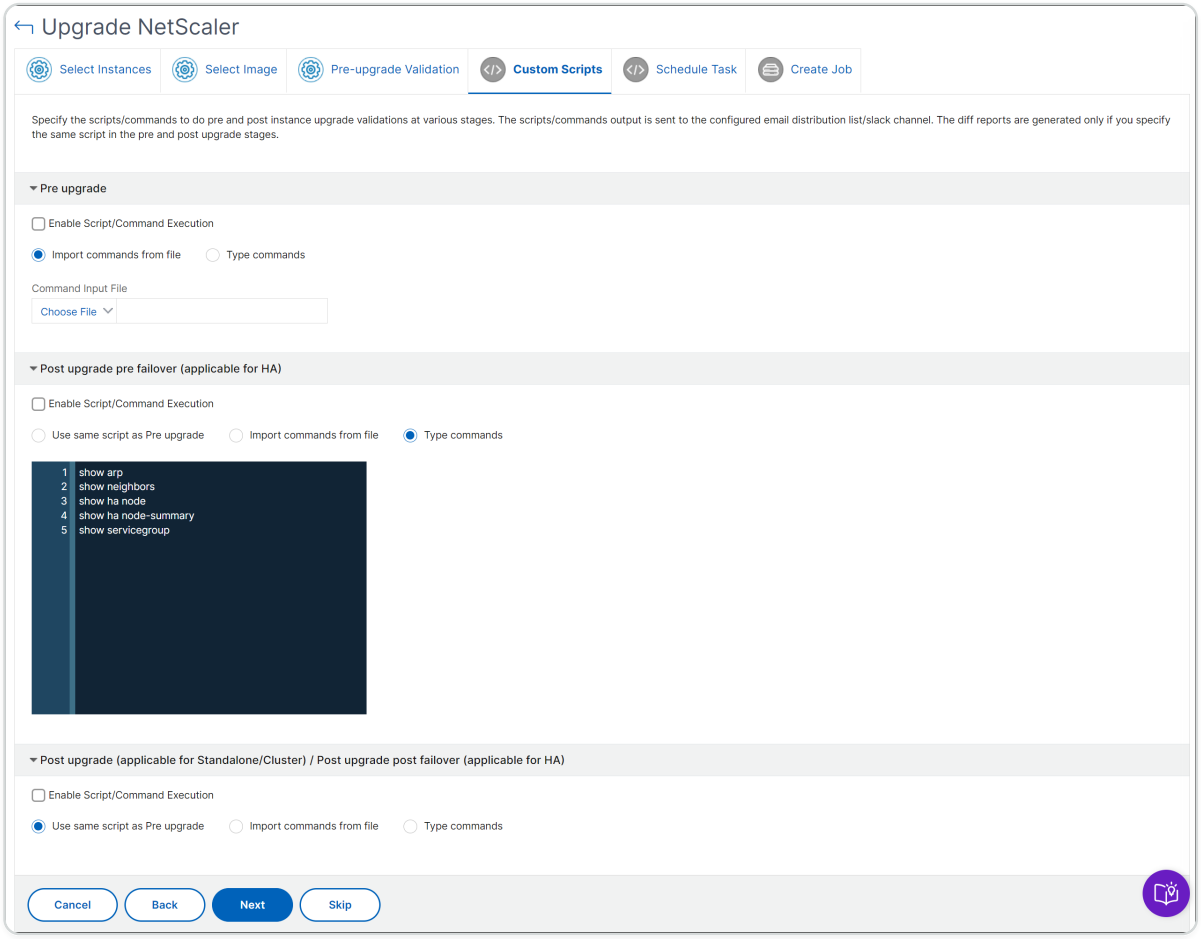
© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT

If you specify cluster IP address, the NetScaler Console does pre-upgrade validation only on the specified instance not on the other cluster nodes.

7. Optional, in **Custom scripts**, specify the scripts to run before and after an instance upgrade. Use one of the following ways to run the commands:

   - **Import commands from file** - Select the command input file from your local computer.
   - **Type commands** - Enter commands directly on the GUI.



You can use custom scripts to check the changes before and after an instance upgrade. For example:

- The instance version before and after the upgrade.
- The status of interfaces, high-availability nodes, virtual servers, and services before and after upgrade.
- The statistics of virtual servers and services.
- The dynamic routes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Click **Next**. In **Schedule Task**, select one of the following options:

    - **Upgrade now** - The upgrade job runs immediately.
    - **Schedule later** - Select this option to run this upgrade job later. Specify the **Execution Date** and **Start Time** when you want to upgrade the instances.

      If you want to upgrade a NetScaler HA pair in two stages, select **Perform two stage upgrade for nodes in HA**.

      Specify the **Execution Date** and **Start Time** when you want to upgrade another instance in the HA pair.

9. Click **Next**. In **Create Job**, specify the following details:

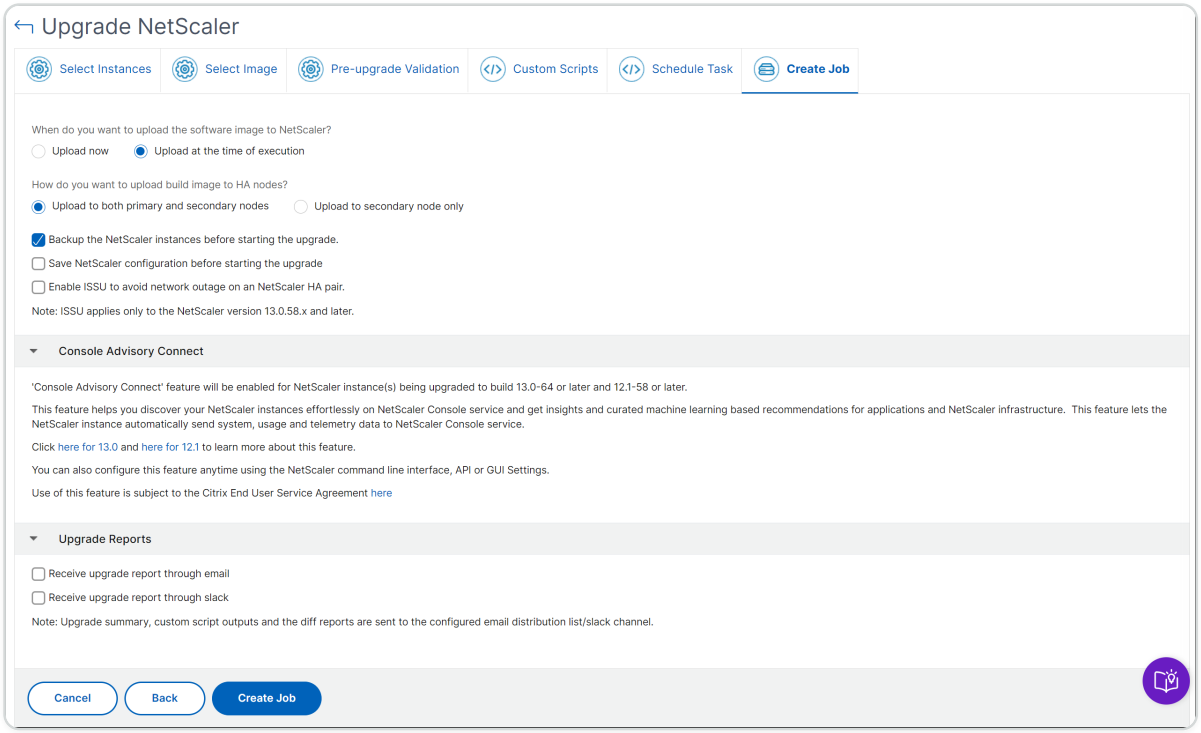
    a. Specify when you want to upload the image to an instance:

        - **Upload now** - Select this option to upload the image immediately. However, the upgrade job runs at the scheduled time.
        - **Upload at the time of execution** - Select this option to upload the image at the time of upgrade job execution.
        - **Backup the NetScaler instances before starting the upgrade.** - Creates a backup of the selected NetScaler instances.
        - **Save NetScaler Configuration before starting the upgrade** - Saves the configuration jobs that are configured on the instance before the upgrade.
        - **Enable ISSU to avoid network outage on NetScaler HA pair** - Enabling In-Service Software Upgrade (ISSU) allows you to upgrade a NetScaler high-availability (HA) pair without causing network downtime. ISSU ensures that the existing connections are honoured during the upgrade by migrating the active sessions seamlessly between the nodes. After enabling ISSU in the upgrade workflow, the system can also trigger ISSU migration completion after the delay time defined by the customer. NetScaler Console triggering a complete ISSU migration completion ensures that the upgrade completes even if connections persist. Specify the ISSU migration timeout in minutes to set the wait time before NetScaler Console completes the migration.

    - **Console Advisory Connect** - If you are upgrading to build **13.0-64 or later** and **12.1-58 or later**, Console Advisory Connect is enabled automatically. For more information, see Low-touch onboarding of NetScaler instances using NetScaler Console service connect.
    - **Receive Execution Report through email** - Sends the execution report in email. To add an email distribution list, see Create an email distribution list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Receive Execution Report through slack** - Sends the execution report in slack. To add a Slack profile, see Create a Slack profile.



10. Click **Create Job**.

Schedule upgrading of NetScaler SDX instances

1. In NetScaler Console, navigate to **Infrastructure > Upgrade Jobs**. Click **Create Job**.
2. Select **Upgrade NetScaler SDX** and click **Proceed**.
3. On the **Upgrade NetScaler SDX** page, in the **Instance Selection** tab:
   a. Add a **Task Name**.
   b. From the **Software Image** list, select either **Local** (your local machine) or **Appliance** (the build file must be present on the NetScaler Console virtual appliance).

      The upload process begins.
   c. Add the NetScaler SDX instances on which you want to run the upgrade process.
   d. Click **Next**.
4. On the **Schedule Task** tab, select **Now** from the **Execution Mode** list to upgrade a NetScaler SDX instance now, and click **Finish**.
5. To upgrade a NetScaler SDX instance later, select **Later** from the **Execution Mode** list. You can then choose the Execution Date and the Start Time for upgrading the NetScaler instance, and click **Finish**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. You can also enable email and slack notifications to receive the execution report of the upgrading NetScaler SDX instance. Click the **Receive Execution Report Through Email** check box and **Receive Execution Report through slack** check box to enable the notifications.

   For more information to configure email distribution list and slack channel, see **step 8** in Schedule upgrading of NetScaler instances

Schedule upgrading of NetScaler BLX instances

1. In NetScaler Console, navigate to **Infrastructure > Upgrade Jobs**. Click **Create Job**.
2. In **Create Maintenance Jobs**, select **Upgrade NetScaler BLX** and click **Proceed**.
3. In **Select Instance**, type a name of your choice for **Job Name**.
4. Click **Add Instances** to add the BLX instances that you want to upgrade.
   - To upgrade an HA pair, specify the IP address of a primary or secondary node. However, using the primary instance to upgrade the HA pair is recommended.
   - To upgrade a cluster, specify the cluster IP address.
5. Click **Next** to select the image. Select one of the following options from the **Software Image** list:
   - **Local** - Select the instance upgrade file from your local machine.
   - **Appliance** - Select the instance upgrade file from an NetScaler Console file browser. The NetScaler Console GUI displays the instance files that are present at `/var/mps/mps_images`.
     - **Skip image uploading to NetScaler if the selected image is already available** - Select this option if the image is already present in the NetScaler instance.
     - **Clean software image from NetScaler on successful upgrade** - Select this option to clear the uploaded image in the NetScaler instance after the instance upgrade.
6. Click **Next** to start the pre-upgrade validation on the selected instances.

   The **Pre-upgrade validation** tab displays the failed instances. Remove the failed instances and click **Next**.

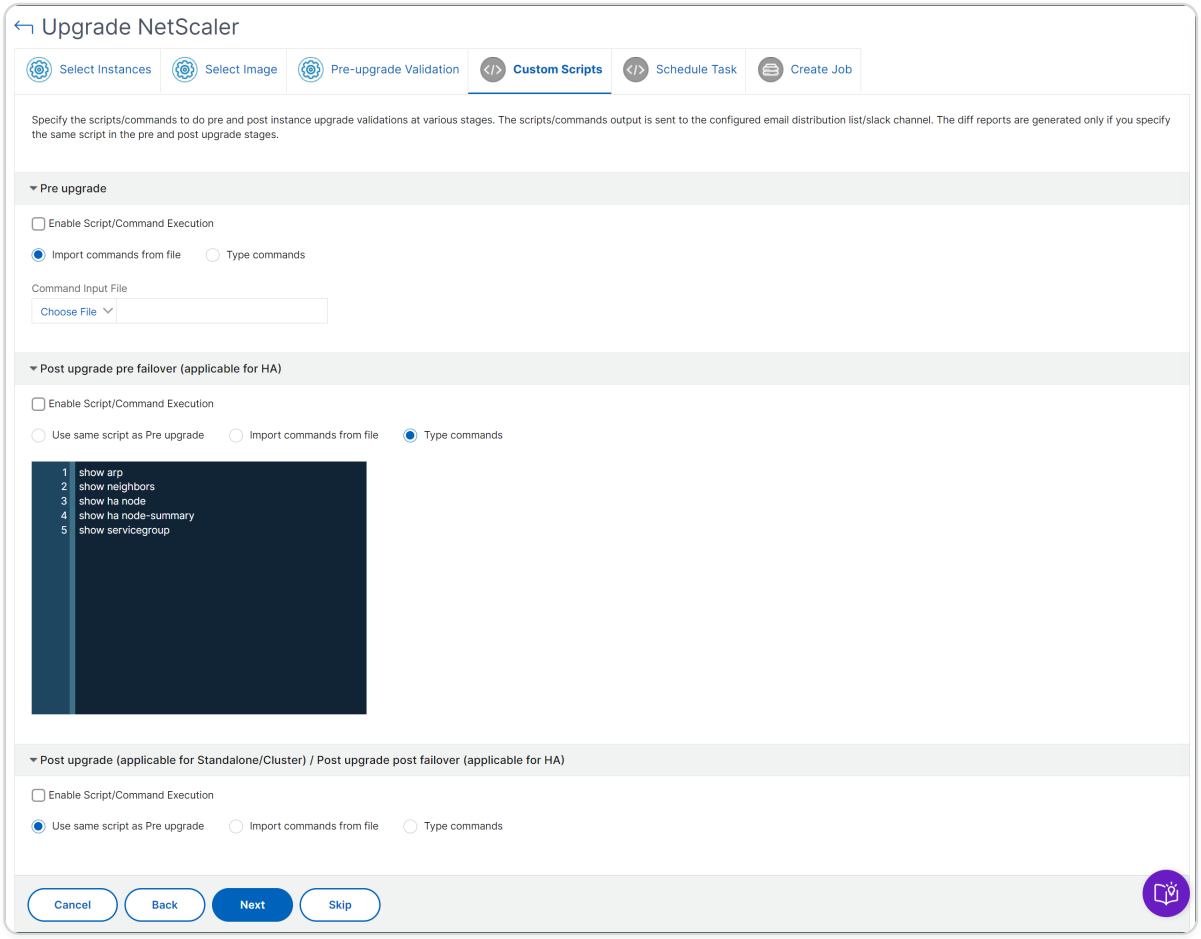
© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT

If you specify cluster IP address, the NetScaler Console does pre-upgrade validation only on the specified instance not on the other cluster nodes.

7. Optional, in **Custom scripts**, specify the scripts to run before and after an instance upgrade. Use one of the following ways to run the commands:

   - **Import commands from file** - Select the command input file from your local computer.
   - **Type commands** - Enter commands directly on the GUI.



You can use custom scripts to check the changes before and after an instance upgrade. For example:

- The instance version before and after the upgrade.
- The status of interfaces, high-availability nodes, virtual servers, and services before and after upgrade.
- The statistics of virtual servers and services.
- The dynamic routes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Click **Next**. In **Schedule Task**, select one of the following options:

    - **Upgrade now** - The upgrade job runs immediately.
    - **Schedule later** - Select this option to run this upgrade job later. Specify the **Execution Date** and **Start Time** when you want to upgrade the instances.

      If you want to upgrade an HA pair in two stages, select **Perform two stage upgrade for nodes in HA**.

      Specify the **Execution Date** and **Start Time** when you want to upgrade another instance in the HA pair.

9. Click **Next**. In **Create Job**, specify the following details:

    a. Specify when you want to upload the image to an instance:

        - **Upload now** - Select this option to upload the image immediately. However, the upgrade job runs at the scheduled time.
        - **Upload at the time of execution** - Select this option to upload the image at the time of upgrade job execution.
        - **Backup the NetScaler instances before starting the upgrade** - Creates a backup of the selected NetScaler instances.
        - **Saves NetScaler Configuration before starting the upgrade** - Saves the configuration jobs that are configured on the instance before the upgrade.
        - **Enable ISSU to avoid network outage on NetScaler HA pair** - Enabling In-Service Software Upgrade (ISSU) allows you to upgrade a NetScaler high-availability (HA) pair without causing network downtime. ISSU ensures that the existing connections are honoured during the upgrade by migrating the active sessions seamlessly between the nodes. After enabling ISSU in the upgrade workflow, the system can also trigger ISSU migration completion after the delay time defined by the customer. NetScaler Console triggering a complete ISSU migration completion ensures that the upgrade completes even if connections persist. Specify the ISSU migration timeout in minutes to set the wait time before NetScaler Console completes the migration.

    - **Console Advisory Connect** - If you are upgrading to build **13.0-64 or later** and **12.1-58 or later**, Console Advisory Connect is enabled automatically. For more information, see Low-touch onboarding of NetScaler instances using Console Advisory Connect.
    - **Receive Execution Report through email** - Sends the execution report in email. To add an email distribution list, see Create an email distribution list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Receive Execution Report through slack** - Sends the execution report in slack. To add a Slack profile, see Create a Slack profile.

10. Click **Create Job**.

Schedule upgrading Autoscale™ group

Perform the following steps to upgrade all the instances in the cloud services that are part of the Autoscale group:

1. In NetScaler Console, navigate to **Infrastructure > Upgrade Jobs**. Click **Create Job**.
2. Select **Upgrade Autoscale Group** and click **Proceed**.
3. In the **Upgrade Settings** tab:
   a. Select the **Autoscale Group** that you want to upgrade.
   b. In **Image**, select the NetScaler version. This image is the existing version of NetScaler instances in the Autoscale group.
   c. In **NetScaler Image**, browse the NetScaler version file to which you want to upgrade.

      If you check **Graceful Upgrade**, the upgrade task waits until the specified drain connection period to expire.
   d. Click **Next**.
4. In the **Schedule Task** tab:
   a. Select one of the following from the Execution Mode list:
      - **Now:** To start the NetScaler instances upgrade immediately.
      - **Later:** To start the NetScaler instances upgrade at later time.
   b. If you select the **Later** option, select the Execution Date and Start Time when you want to start the upgrade task.

   You can also enable email and slack notifications to receive the execution report of the upgrading Autoscale group. Click the **Receive Execution Report Through Email** check box and **Receive Execution Report through slack** check box to enable the notifications.
5. Click **Finish**.

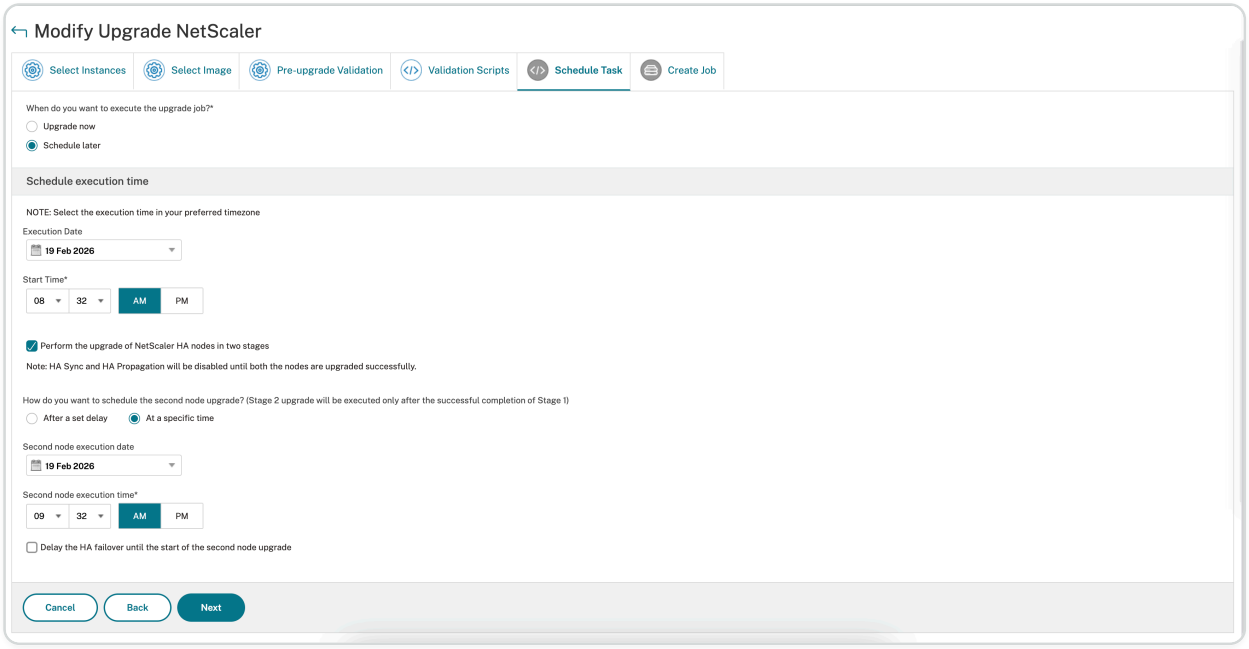
Schedule configuring HA pair of NetScaler instances

1. In NetScaler Console, navigate to **Infrastructure > Upgrade Jobs**. Click **Create Job**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Select **Configure HA Pair of NetScaler Instances** and click **Proceed**.
3. On the **NetScaler HA Pair** page, in the **Instance Selection** tab:
    a. Add a **Task Name**.
    b. Enter the Primary IP Address.
    c. Enter the Secondary IP Address.
    d. Click **Next**.
    e. Click to enable **Turn on INC(Independent Network Configuration) mode** if you have the HA pair instances in two subnets.
4. On the **Schedule Task** tab, select one of the following options:
    - **Upgrade now**: Select this option to upgrade a NetScaler instance immediately. Click **Finish**.
    - **Schedule later**: Select this option to upgrade a NetScaler HA pair later.
5. If you select **Schedule later** option, choose the **Execution Date** and the **Start Time** for upgrading the NetScaler instance.
    a. Select **Perform the upgrade of NetScaler HA nodes in two stages**. When you select this option HA Sync and HA Propagation are disabled until both nodes are upgraded successfully.
    b. Select one of the following options to schedule the secondary node upgrade. With this option, stage 2 upgrade is run only after the successful completion of stage 1.
        - **After a set delay**: Specify a delay (in hours) after the first node upgrade completes before the second node upgrade begins.
        - **At a specific time**: Choose a date and time for secondary node upgrade.
6. Select **Delay the HA failover until the start of the secondary node upgrade**. Click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. You can also enable email and slack notifications to receive the execution report of creating the NetScaler HA pair. Click the **Receive Execution Report Through Email** check box and **Receive Execution Report through slack** check box to enable the notifications.

   For more information to configure email distribution list and slack channel, see **step 8** in Schedule upgrading of NetScaler instances.

Schedule converting HA pair of instances to cluster

1. In NetScaler Console, navigate to **Infrastructure > Upgrade Jobs**. Click **Create Job**.
2. Select **Convert HA Pair of Instances to 2 Node Cluster** and click **Proceed**.
3. On the **Migrate NetScaler HA to Cluster** page, in the **Instance Selection** tab, add a **Task Name**. Specify the Primary IP address, Secondary IP address, Primary Node ID, Secondary Node ID, Cluster IP Address, Cluster ID, and Backplane, and then click **Next**.
4. On the **Schedule Task** tab, select **Now** from the **Execution Mode** list to upgrade a NetScaler instance now, and click **Finish**.
5. To upgrade later, select **Later** from the **Execution Mode** list. You can then choose the **Execution Date** and the **Start Time** for upgrading the NetScaler HA pair instance, and click **Finish**.
6. You can also enable email and slack notifications to receive the execution report of upgrading a NetScaler SDX instance. Click the **Receive Execution Report Through Email** check box and **Receive Execution Report through slack** check box to enable the notifications.

   For more information to configure email distribution list and slack channel, see **step 8** in Schedule upgrading of NetScaler instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use jobs to upgrade NetScaler instances

In NetScaler Console, you can upgrade one or more NetScaler instances. You must know the licensing framework and types of licenses before you upgrade an instance.

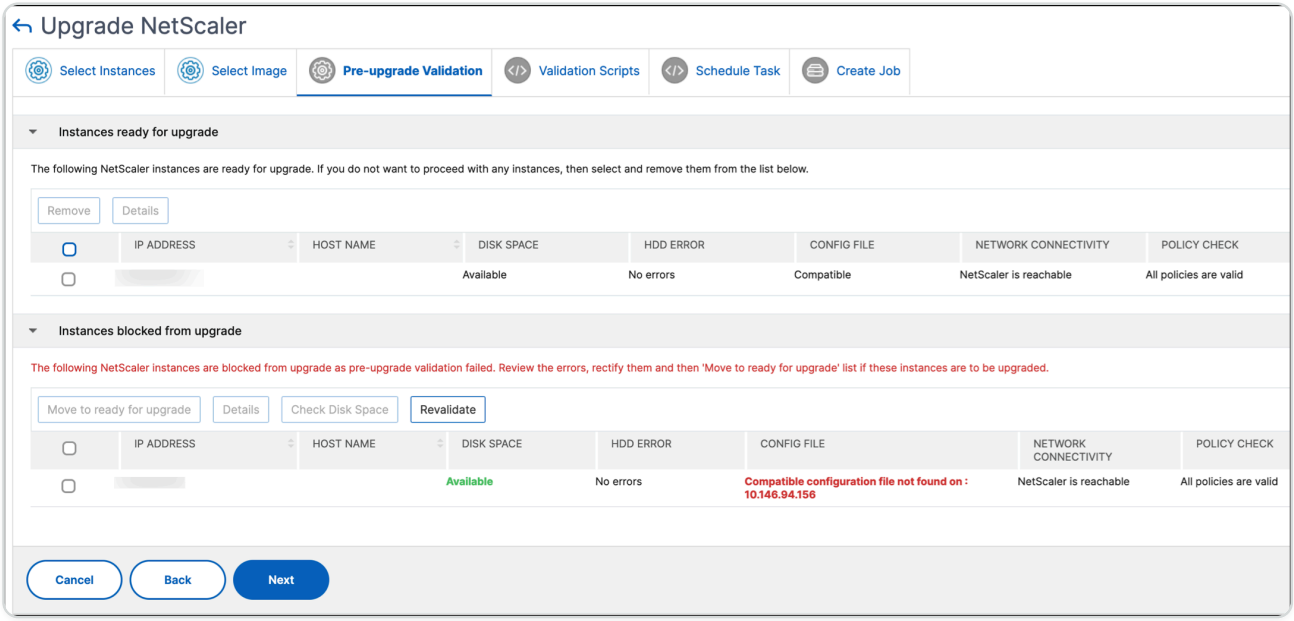
NOTE: If you want to upgrade an instance that has classic policies, we recommend that you convert the classic policies to advanced policies before upgrading the instance, using the NSPEPI tool. This is applicable for the features that are supported by the NSPEPI tool. For more information, see Upgrade considerations for configurations with classic policies.

Prerequisites

NetScaler Console performs the following pre-validation checks on the instance that you want to upgrade:

1. **Check for disk space** - Clean up disk space to have a sufficient disk capacity for an instance upgrade. Resolve disk issues if any.
2. **Check for disk hardware issues** - Resolve the hardware issues if any.
3. **Check for customizations** - Back up your customizations and delete them from the instances. You can reapply the backed-up customization after the instance upgrade.
4. **Policy issues** - NetScaler does not support classic policies from `13.1` version. Before upgrading an instance to this version, migrate classic policies to advanced policies.

   For more information, see Classic and advanced policies.
5. **Check for STAYPRIMARY and STAYSECONDARY nodes** - For a NetScaler HA, the upgrade is blocked for the nodes in STAYPRIMARY and STAYSECONDARY states. These nodes are identified in the pre-validation check and listed under **Instances blocked from upgrade**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Upgrade considerations for customized NetScaler configurations

It is important that both the upgrade changes and your customizations are applied to an upgraded NetScaler appliance. So, if you have customized configuration files in the /etc directory, see Upgrade considerations for customized configuration files before you continue with the NetScaler appliance upgrade. Following are the broad steps that you must perform:

1. Pre upgrade steps in NetScaler
    - Backup customized file before the upgrade
    - Delete the symlink of the customized file before the upgrade
2. Upgrade NetScaler using ADM. To upgrade, follow the instructions available at the beginning of the page.
3. Post upgrade steps in NetScaler
    - Restore customizations after the upgrade

Both the pre-upgrade and post upgrade steps are to be performed on each NetScaler instance. However, in step 2, to upgrade NetScaler using ADM, all the vulnerable NetScaler instances can be selected and upgraded together.

NetScaler high-availability pair

When you upgrade a NetScaler high-availability pair, note the following:

- The secondary node is upgraded first.
- Synchronization and propagation of the nodes are disabled until both the nodes are upgraded successfully.
- After the successful high-availability pair upgrade, an error message appears in the execution history. This message appears if your nodes in the high-availability pair are on different builds or versions. It indicates that synchronization between primary and secondary nodes is disabled.

You can upgrade a NetScaler high-availability pair in two stages:

1. Create an upgrade job and run on one of the nodes immediately or schedule later.
2. Schedule the upgrade job to run on the remaining node later. Ensure to schedule this job after the initial node's upgrade.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler clusters

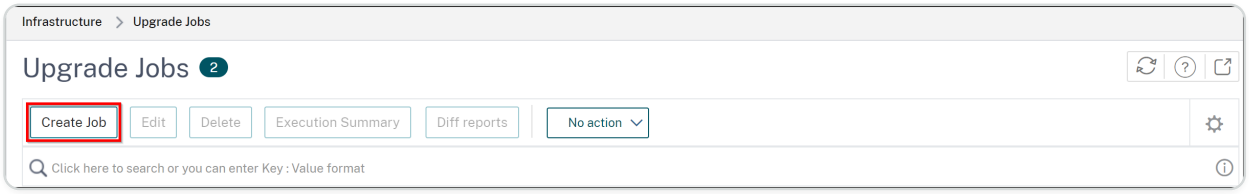
When you upgrade an NetScaler cluster, in the pre-upgrade validation stage, the NetScaler Console only validates the specified instance. So, check and resolve the following issues on the cluster nodes:

- Customization
- Disk usage
- hardware issues

Create a NetScaler upgrade job

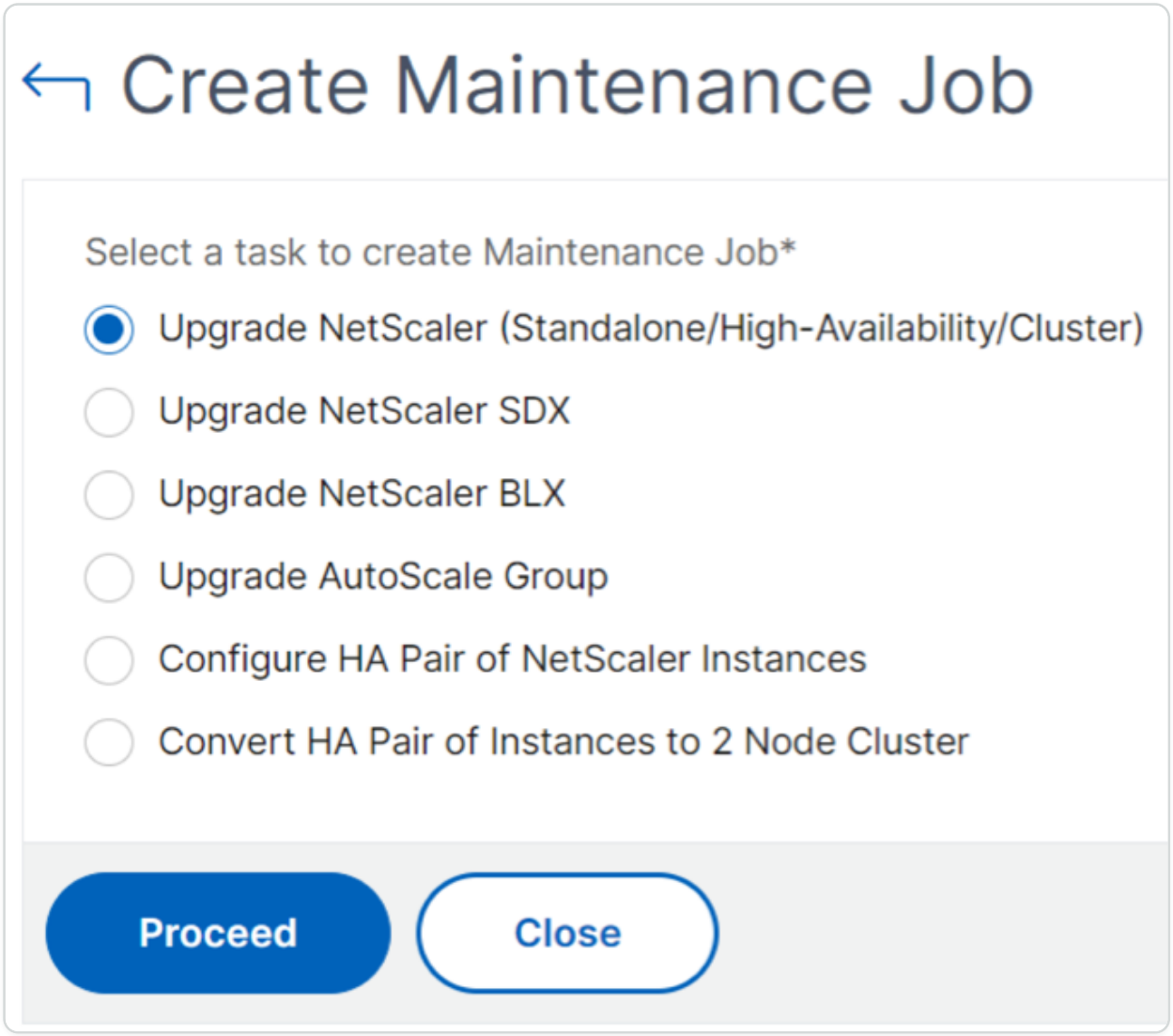
To create a NetScaler upgrade job, do the following:

1. Navigate to **Infrastructure > Upgrade Jobs**.



2. In **Create Maintenance Jobs**, select **Upgrade NetScaler (Standalone/High-Availability/ Cluster)** and click **Proceed**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE:

To upgrade Autoscale groups, see Upgrade an Autoscale group.

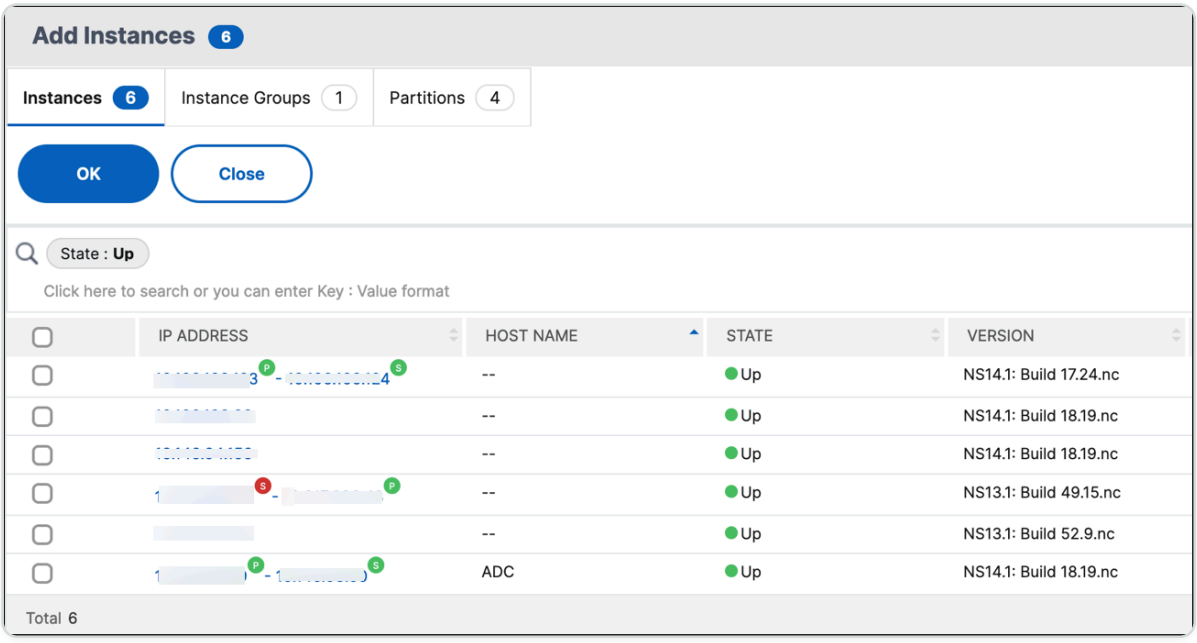
3. In the **Select Instances** tab,

   a. Specify a name of your choice for **Job Name**.

   b. Click **Add Instances** to add NetScaler instances that you want to upgrade.

      - To upgrade a NetScaler high-availability pair, select the IP addresses of the high-availability pair (denoted by the superscript of 'S' and 'P').
      - To upgrade a cluster, select the cluster IP address (denoted by the superscript of 'C').

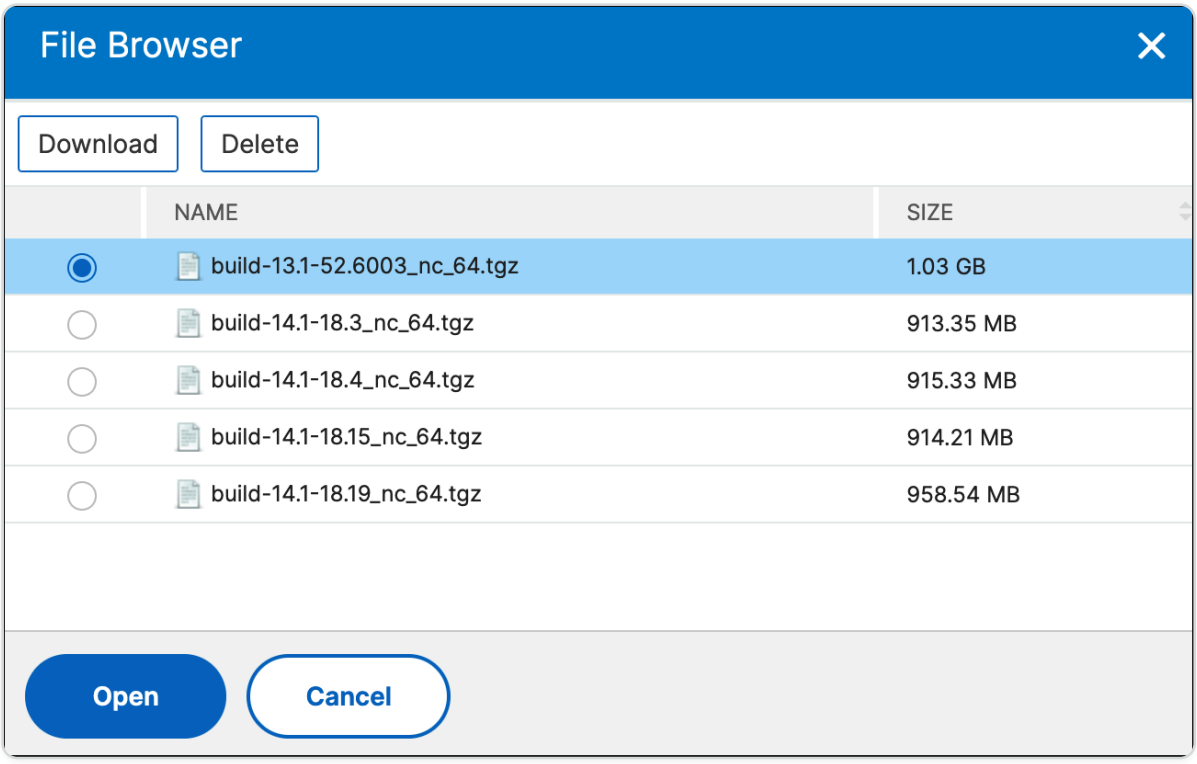
© 1997–2026 Citrix Systems, Inc. All rights reserved.



c. Click **OK**.

4. In the **Select Image** tab, select a NetScaler image from the image library or local or appliance.

   - **Select from Image Library**: Select a NetScaler image from the list. This option lists all NetScaler images that are available in the NetScaler downloads website.



   The NetScaler software images display the preferred builds with the star icon. And, most downloaded builds with the bookmark icon.

   - **Select from local or appliance**: You can upload the image from your local computer or the NetScaler appliance. When you select NetScaler appliance, the NetScaler Console GUI

© 1997–2026 Citrix Systems, Inc. All rights reserved.

displays the instance files that are present in `/var/mps/ns_images`. Select the image from the NetScaler Console GUI.

- **Skip image uploading to NetScaler if the selected image is already available** - This option checks whether the selected image is available in NetScaler. Upgrade job skips uploading a new image and uses the image available in NetScaler.
- **Clean software image from NetScaler on successful upgrade** - This option clears the uploaded image in the NetScaler instance after the instance upgrade.

Click **Next** to start the pre-upgrade validation on the selected instances.

NOTE:

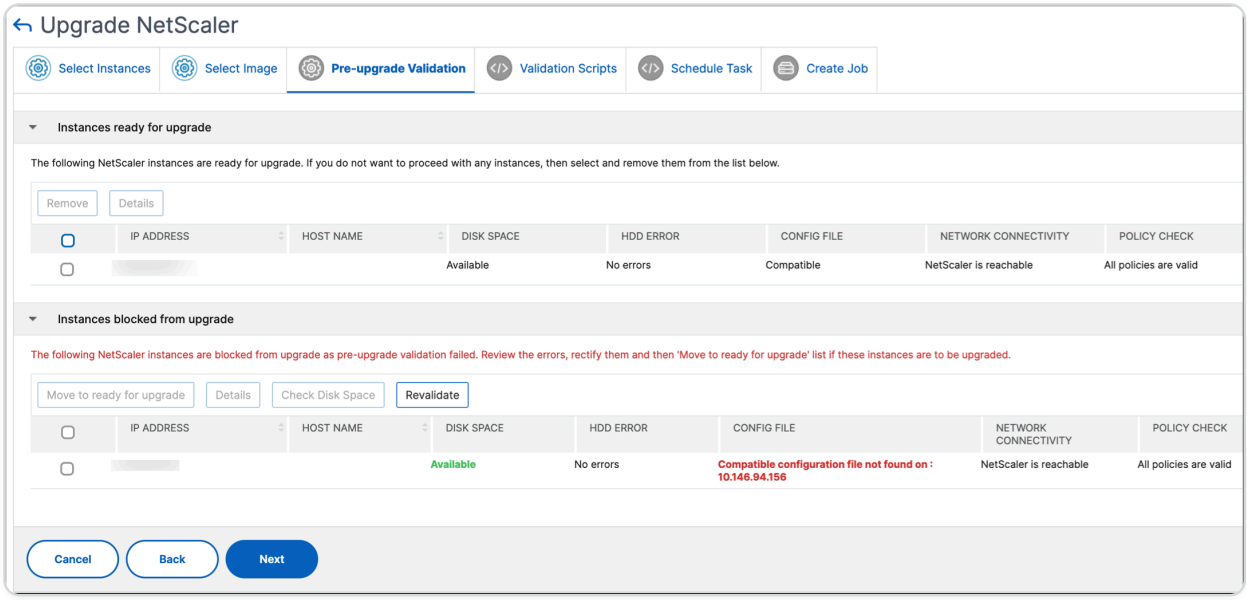
- The downloaded NetScaler images are stored in the agent and are present in `/var/mps/adcimages`. These cached images can be used for multiple NetScaler upgrades, thus eliminating the need to download an image each time for an upgrade.
- NetScaler Console clears the cached NetScaler images every three days based on the last modified time of the images. Only the latest two image files are cached in the agent at a time.

5. The **Pre-upgrade validation** tab displays the following sections:

   - **Instances ready for upgrade**. You can continue with the upgrade of these instances.
   - **Instances blocked from upgrade**. These NetScaler instances are blocked from upgrade because of pre-upgrade validation errors.

     You can review, rectify the errors, and then click **Move to ready for upgrade** to upgrade them. If you face insufficient disk space on an instance, you can check and clean up the disk space. See, Clean up NetScaler disk space.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

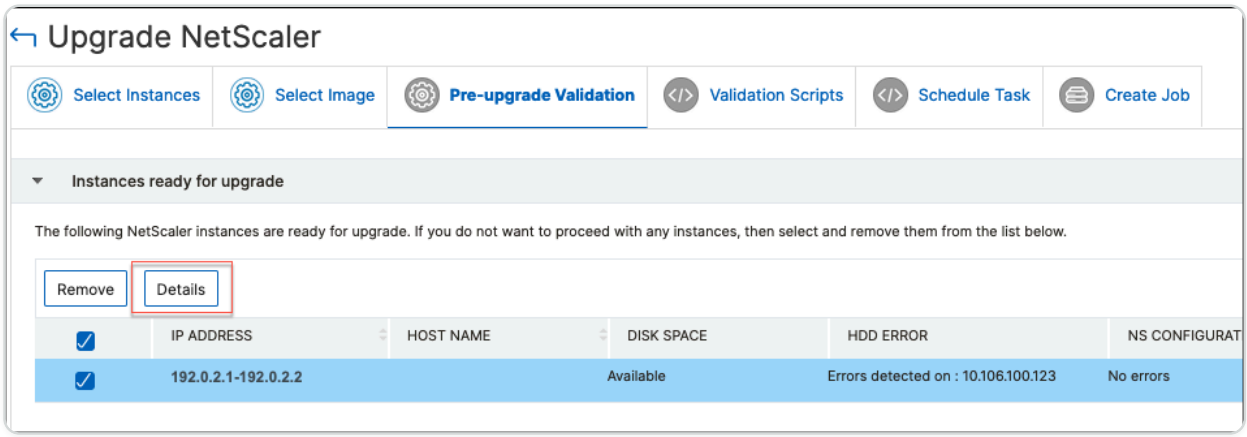


- **Policy Check**: If NetScaler Console finds unsupported classic policies, you can remove such policies to create an upgrade job.

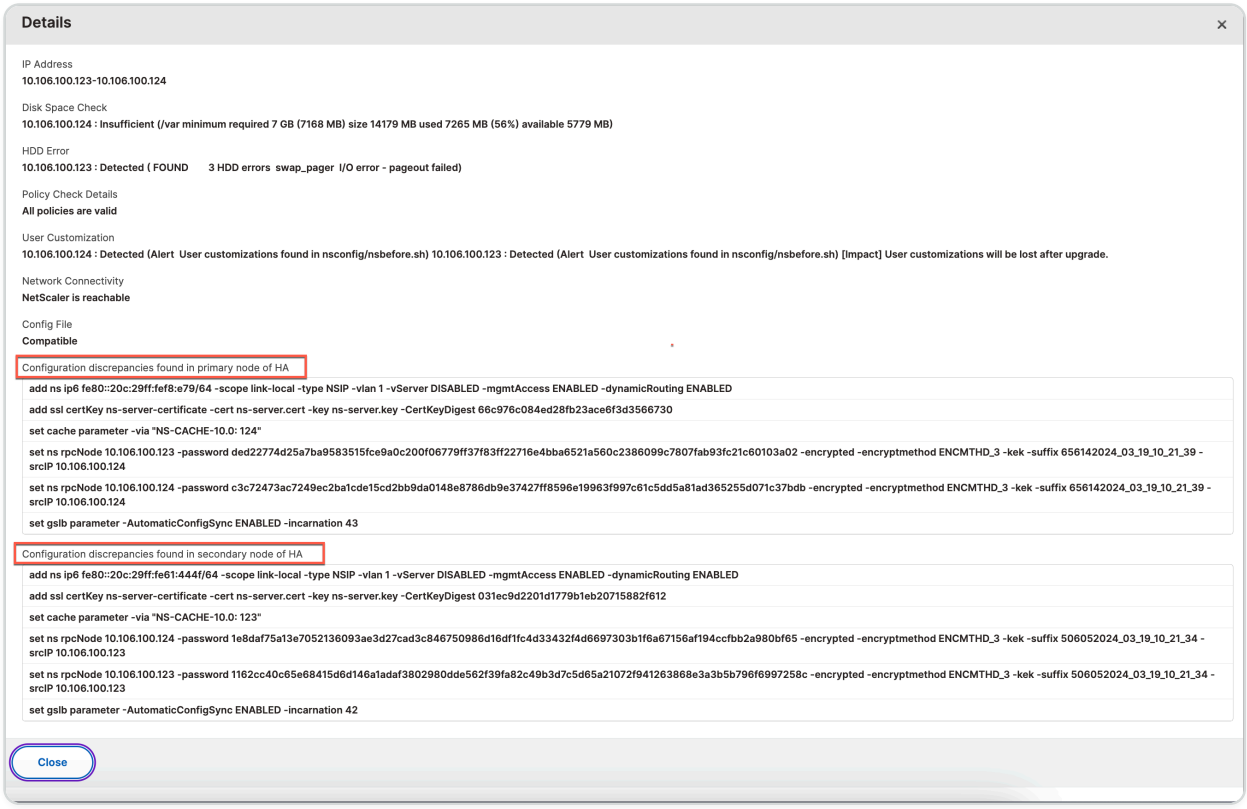
IMPORTANT:

If you specify a cluster IP address, NetScaler Console does pre-upgrade validation only on the specified instance and not on the other cluster nodes.

To view discrepancies between primary and secondary nodes during an upgrade, select the high-availability node, and click **Details**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Configuration discrepancies found in primary node of HA** - Displays all the configurations found in the secondary node of the NetScaler® high-availability pair but missing in the primary node.
- **Configuration discrepancies found in secondary node of HA** - Displays all the configurations found in the primary node of the NetScaler high-availability pair but missing in the secondary node.

NOTE:

You can ignore the following discrepancies that may appear in the configuration discrepancies sections:

- Device-specific configurations like IP addresses.
- Encrypted passwords or certificates, which may differ between nodes, even if the password is the same.

You can review the discrepancies and choose to ignore them if they are not relevant.

6. In **Validation Scripts**, specify the scripts to run before and after an instance upgrade. You can do either of the following:

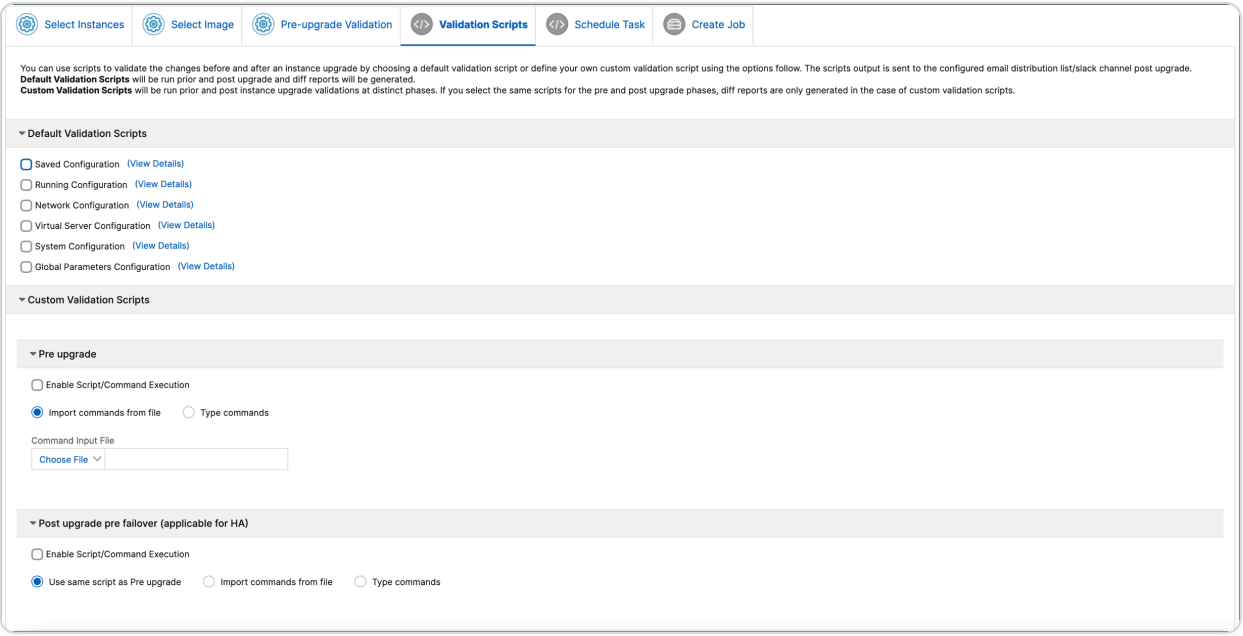
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Default Validation Scripts** - Choose this option to run the predefined validation scripts. These scripts are run both before and after the upgrade job, generating a diff report for the validation script.

  NOTE:

  You cannot change or edit these predefined set of commands.

- **Custom Validation Scripts** - Choose this option to run your own validation script. You can specify if you want the scripts to be run before or after the upgrade. A diff report is generated only if the same scripts are selected before and after the upgrade.



To know the set of commands in each configuration, click **View Details**. For more information, see Use custom scripts.

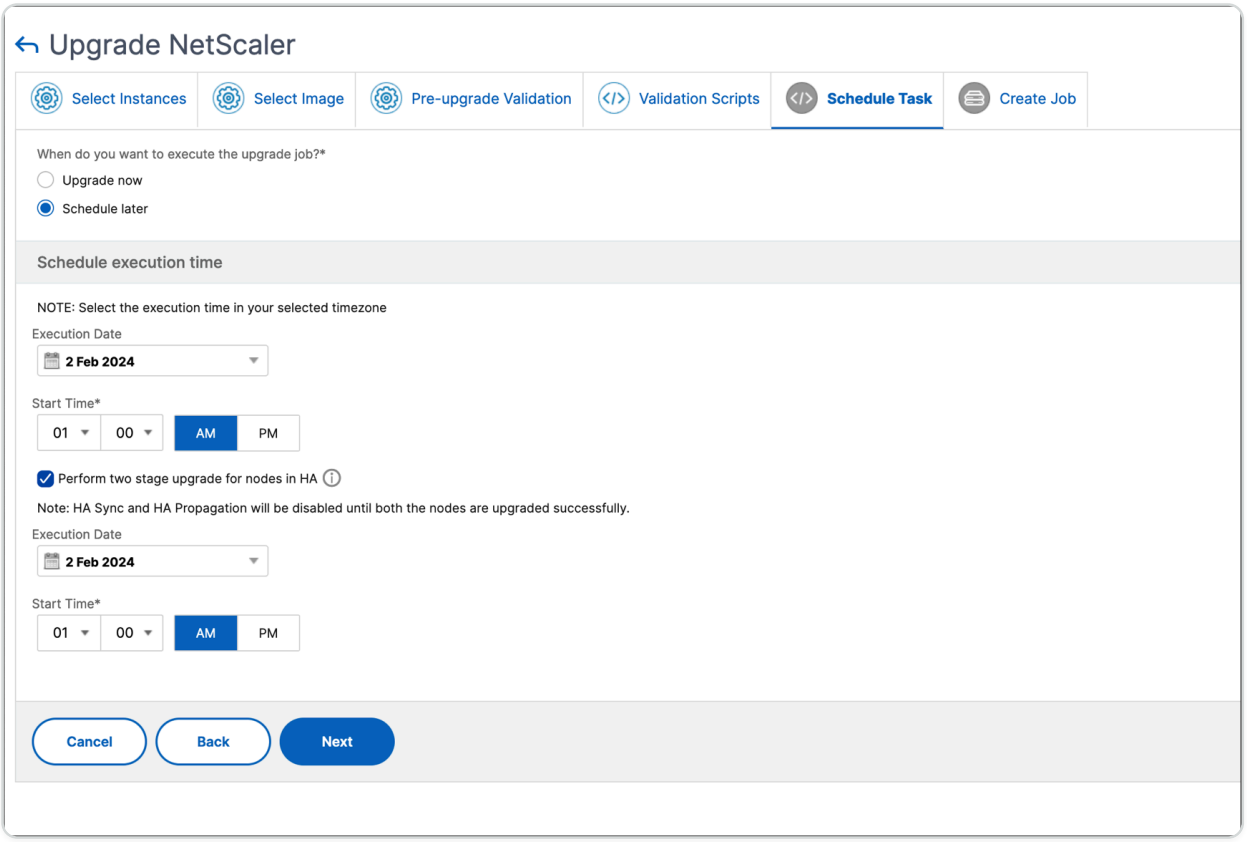
7. In **Schedule Task**, select one of the following options:

   - **Upgrade now**: The upgrade job runs immediately.
   - **Schedule Later**: Select this option to run this upgrade job later. Specify the **Execution Date** and **Start Time** when you want to upgrade the instances.

   If you want to upgrade a NetScaler high-availability pair in two stages, select **Perform two stage upgrade for nodes in high-availability**.

   Specify the **Execution Date** and **Start Time** when you want to upgrade another instance in the high-availability pair.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For more information, see NetScaler high-availability pair.

8. In **Create Job**, specify the following details:

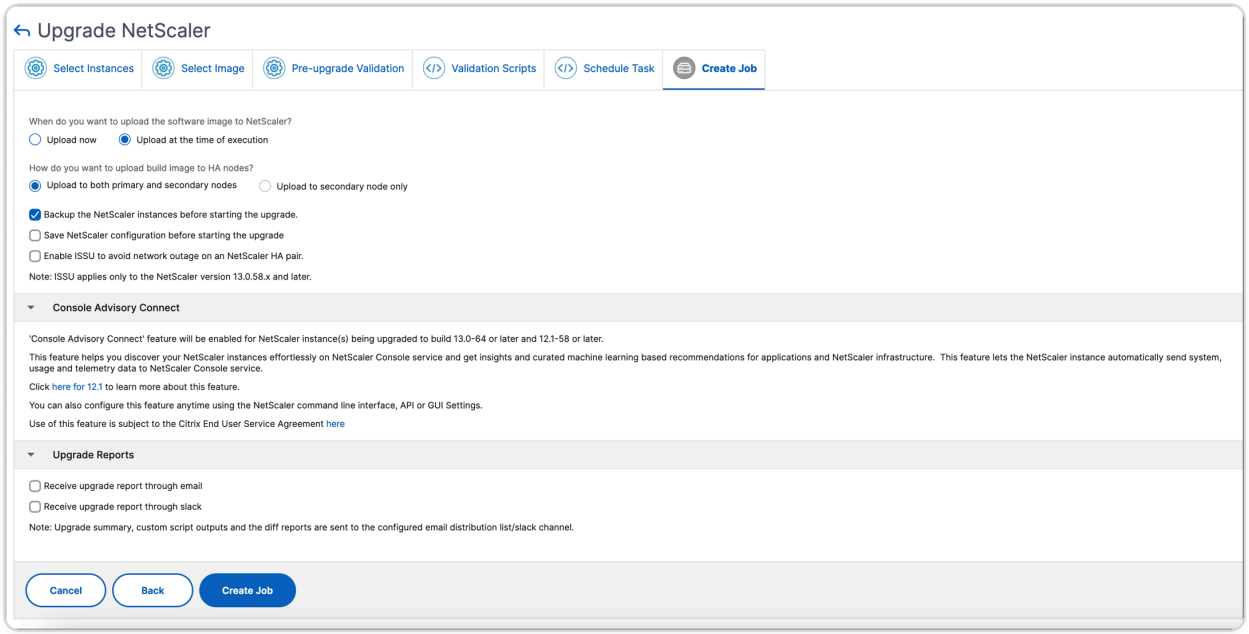
   If you schedule the upgrade job, you can specify when you want to upload the image to an instance:

   - **Upload now**: Select this option to upload the image immediately. However the upgrade job runs at the scheduled time.
   - **Upload at the time of execution**: Select this option to upload the image at the time of upgrade job execution.

   For high-availability pairs, you can specify the nodes on which you want to upload the image:

   - **Upload to both primary and secondary nodes**: Upload the build image file to both the primary and secondary nodes.
   - **Upload to secondary node only**: Upload the build image file to only the secondary node. After the secondary node is upgraded, a failover occurs and the build image file is uploaded to the new secondary node which was previously, the primary node.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For more information on the available scheduling scenarios for high-availability pair, see Scheduling upgrade jobs for NetScaler high-availability pair.

For more information on other upgrade options, see NetScaler upgrade options.

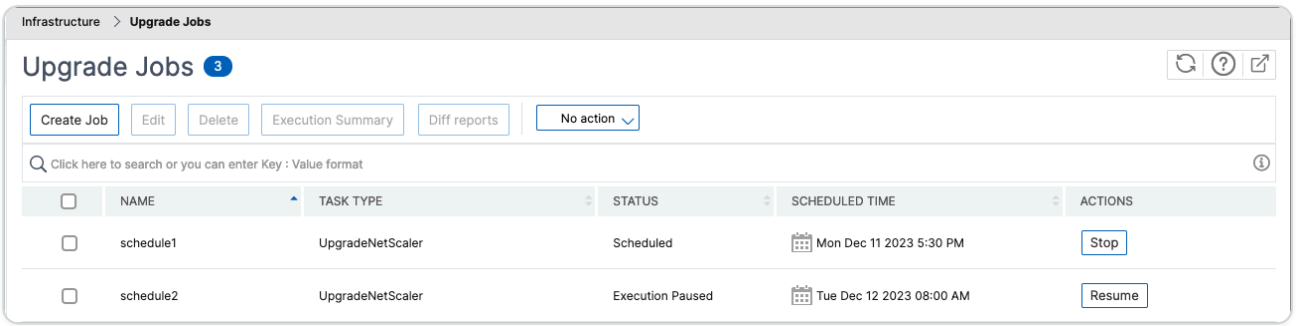
9. Click **Create Job**.

The upgrade job appears in the **Infrastructure > Upgrade Jobs**. When you edit an existing job, you can switch to any tabs if the required fields are already filled. For example, if you are in the **Select Configuration** tab, you can switch to the **Job Preview** tab.

Pause or resume a scheduled upgrade job

You can also pause your scheduled upgrade job.

To use this feature, navigate to **Infrastructure > Upgrade Jobs**, select an existing scheduled upgrade job, and click **Stop** to pause the job. To resume the scheduled upgrade job, click **Resume**.



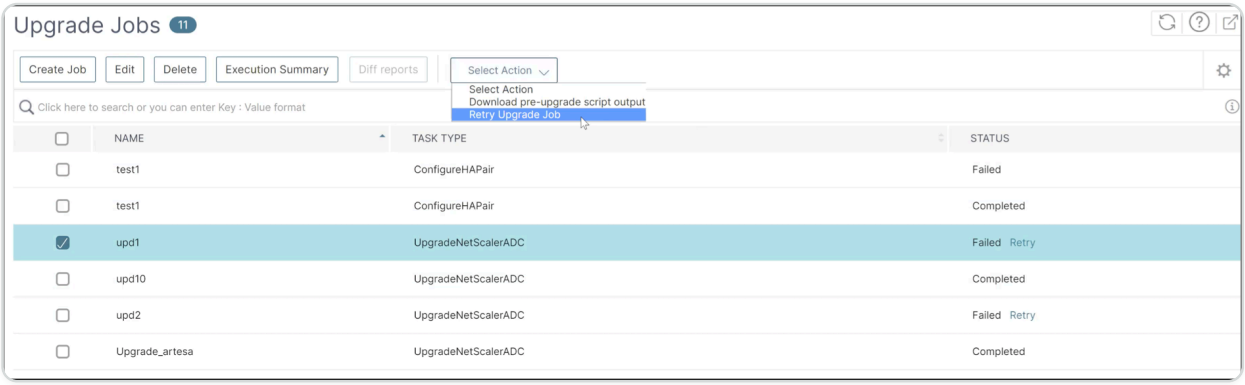
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If the scheduled time for the upgrade job has passed after you decided to resume it, you need to create the upgrade job again.

Retry failed upgrade jobs

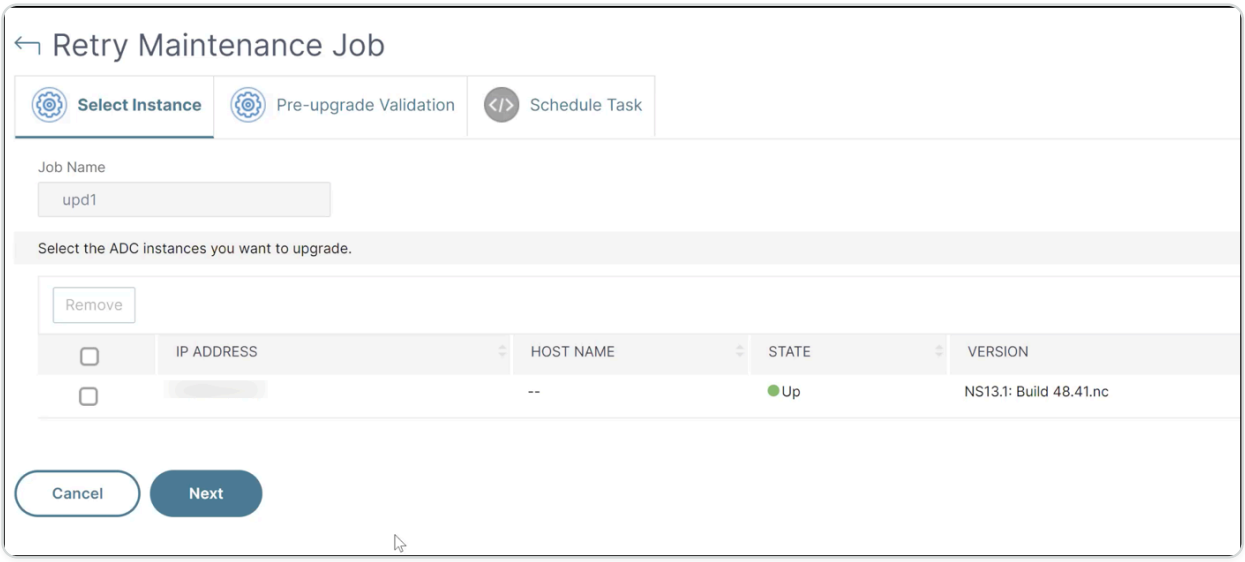
1. In **Infrastructure > Upgrade Jobs**, select the failed upgrade job and click **Retry**. Alternatively, you can also go to **Select Action > Retry Upgrade Job** to retry a failed job.



2. In **Select Instance**, specify the following details:

   - **Job Name** - Enter a name for the upgrade.
   - Select the NetScaler instances that you want to upgrade from the list. To delete any instances, click **Remove**.

   Click **Next** to begin the validation process.



3. The **Pre-upgrade validation** tab displays the following sections:

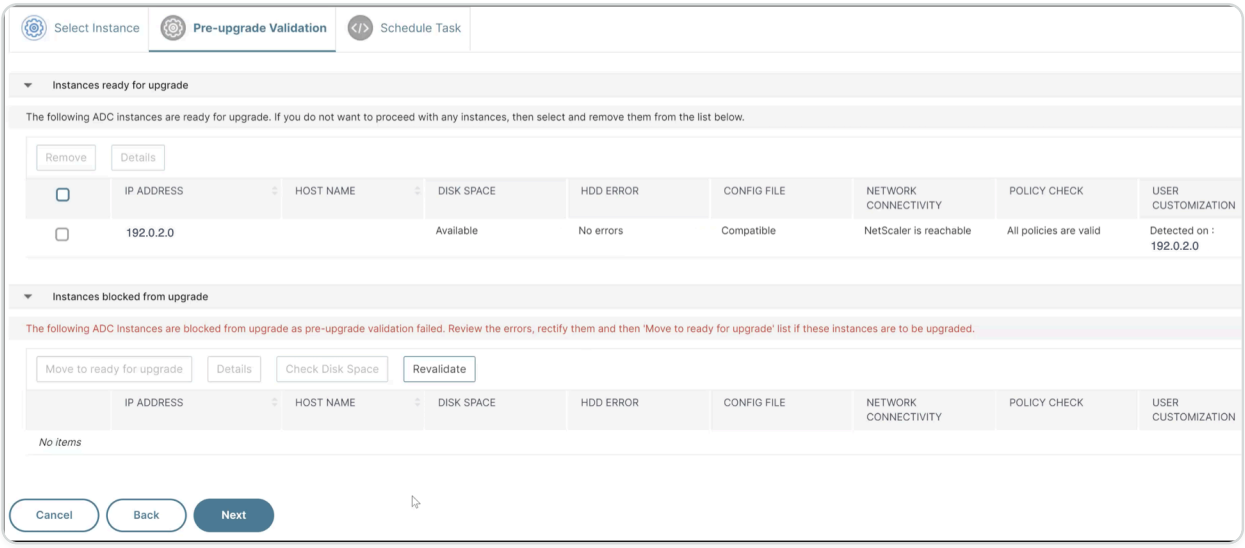
   - **Instances ready for upgrade**. You can continue with the upgrade of these instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Instances blocked from upgrade**. These NetScaler instances are blocked from upgrade because of pre-upgrade validation errors.

  You can review, rectify the errors, and then click **Move to ready for upgrade** to upgrade them. If you face insufficient disk space on an instance, you can check and clean up the disk space. See, Clean up NetScaler disk space.

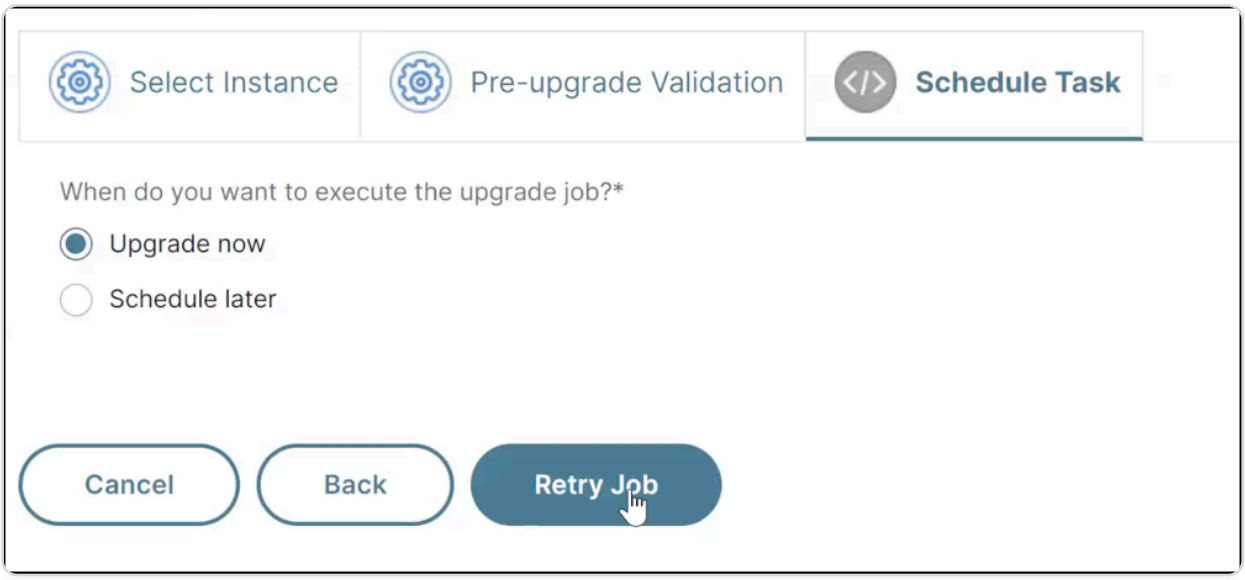
- **Policy Check**: If NetScaler Console finds unsupported classic policies, you can remove such policies to create an upgrade job.



Click **Next**.

4. In **Schedule Task**, select one of the following options:

   - **Upgrade now**: The upgrade job runs immediately.
   - **Schedule Later**: Select this option to run this upgrade job later. Specify the **Execution Date** and **Start Time** when you want to upgrade the instances.



Click **Retry**.

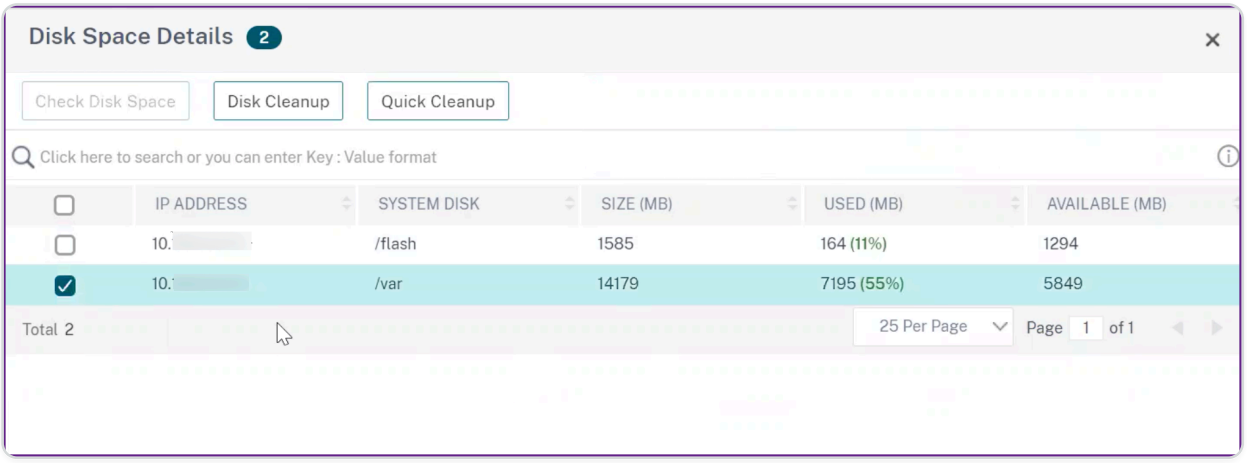
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Clean up the NetScaler disk space

If you face the insufficient disk space issue while upgrading a NetScaler instance, clean up the disk space from the NetScaler Console GUI itself.

1. In the **Pre-upgrade validation** tab, the **Instances blocked from upgrade** section displays the instances that failed the upgrade because of Insufficient disk space. Select the instance that has the disk space issue.
2. Click **Check Disk Space**.

   A **Disk Space Details** pane appears. This pane displays the instances, used memory, and available memory.

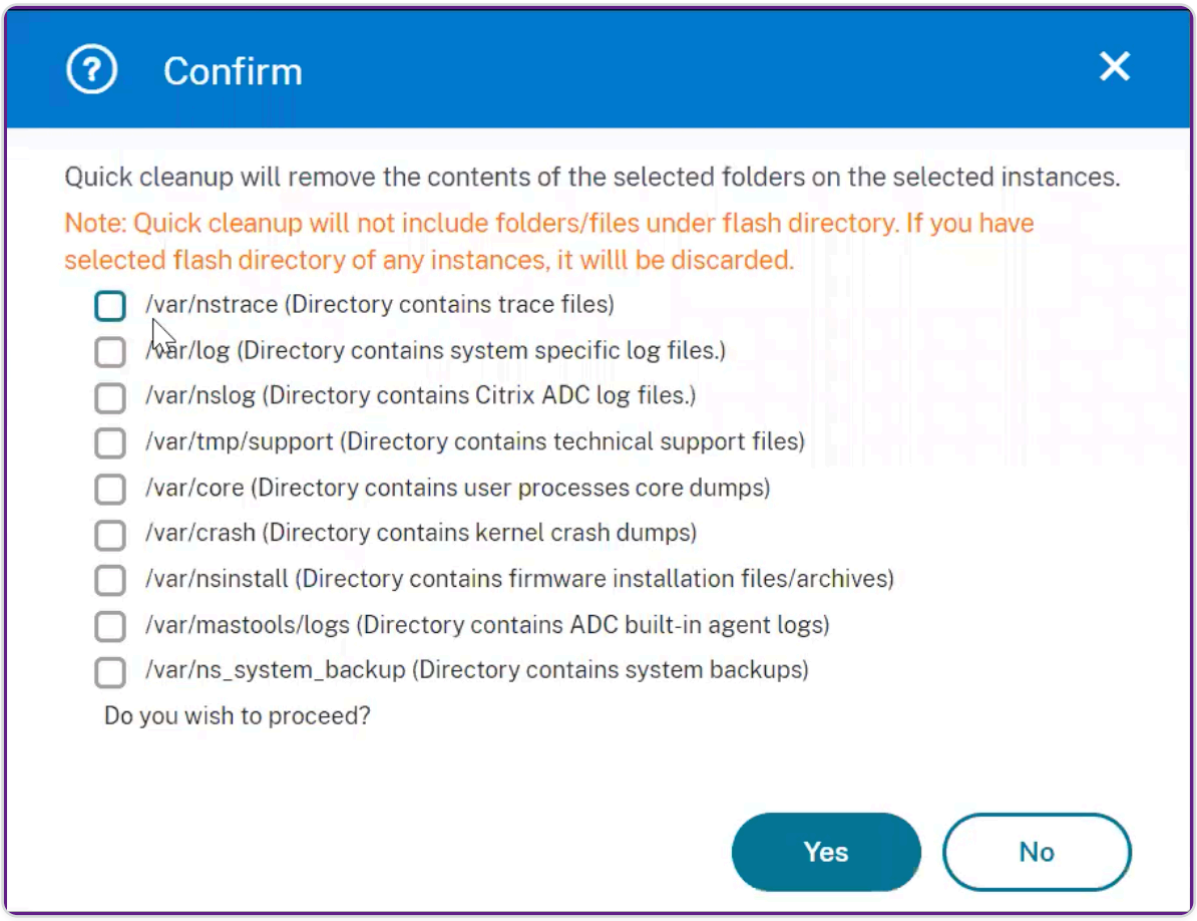


3. In the **Disk Space Details** pane, select the instance that requires cleanup and do one of the following:

   a. **Disk Cleanup** - Navigate to the required folders or directories and delete them to free up disk space.

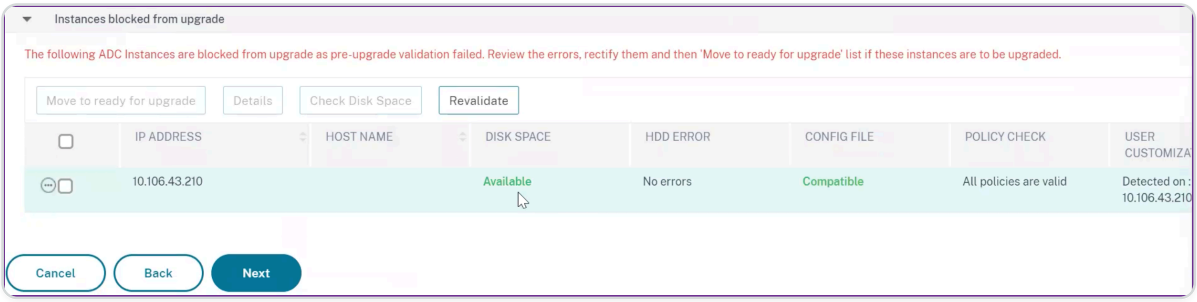
   b. **Quick Cleanup** - Quickly clear up disk space by deleting multiple folders. In the **Confirm** pane that appears, select the folders you want to delete, and click **Yes**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



c. After clearing up the disk space, you can check if sufficient disk space is now available to upgrade the instance. In the **Instances blocked from upgrade** section, click **Revalidate**.

   In the following example, disk space is available. You can now click **Move to ready for upgrade** to upgrade the instance or click **Next** to continue to the next step.



Use custom scripts

You can specify custom scripts while you create a NetScaler upgrade job. The custom scripts are used to check the changes before and after a NetScaler instance upgrade. For example:

- The instance version before and after the upgrade.
- The status of interfaces, high-availability nodes, virtual servers, and services before and after upgrade.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The statistics of virtual servers and services.
- The dynamic routes.

Specify the custom scripts to run in the following stages:

- **Pre upgrade**: The specified script runs before upgrading an instance.
- **Post upgrade pre failover (applicable for HA)**: This stage only applies to the high-availability deployment. The specified script runs after upgrading the nodes, but before their failover.
- **Post upgrade (applicable for standalone) / Post upgrade post failover (applicable for HA)**: The specified script runs after upgrading an instance in the standalone deployment. In the high-availability deployment, the script runs after upgrading the nodes and their failover.

NOTE:

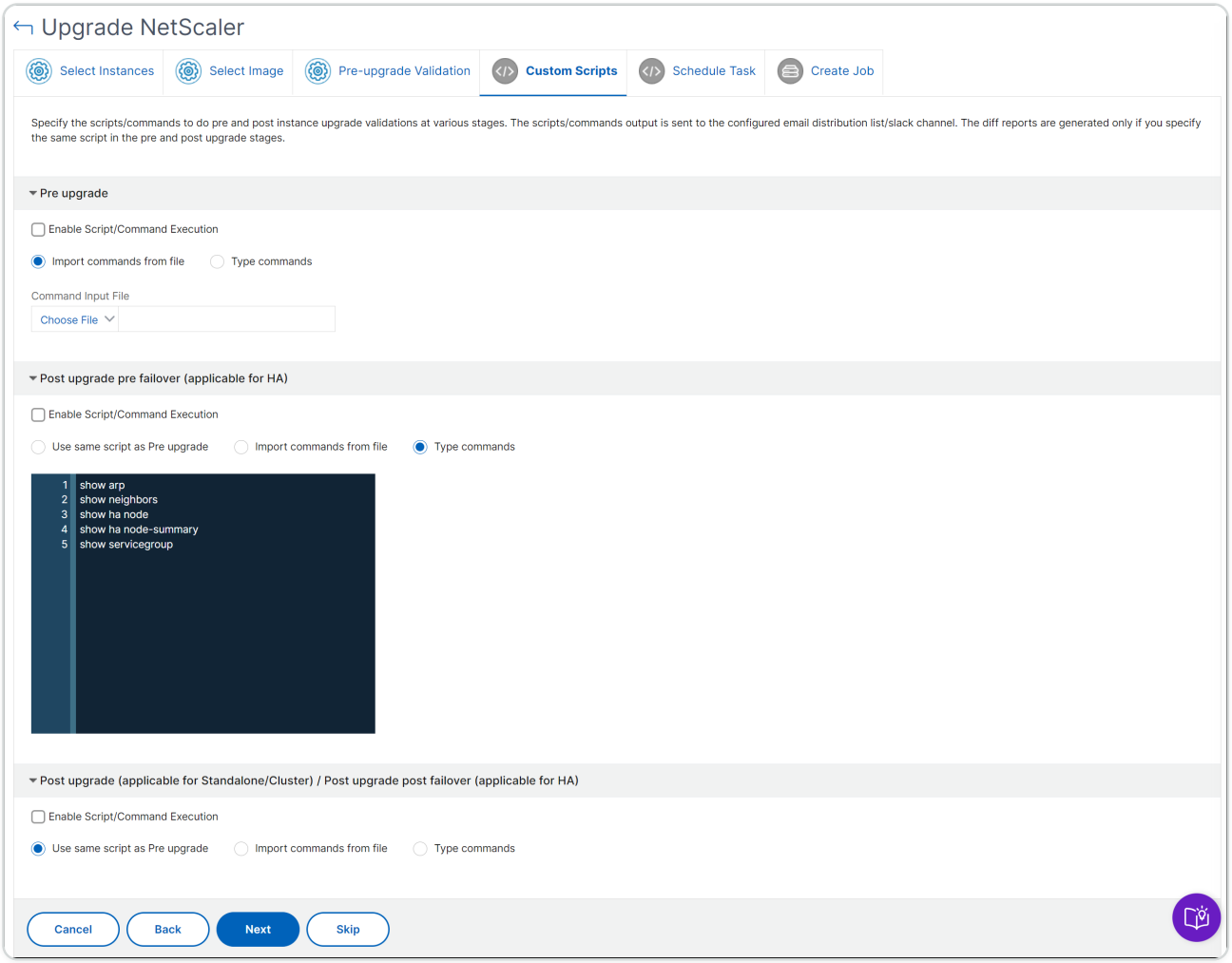
- Ensure to enable script or command execution at the required stages. Otherwise, the specified scripts do not run.
- The diff report is generated only if you specify the same script in the pre-upgrade and post-upgrade stages. So, ensure to select **Use same script as Pre-upgrade** in the post-upgrade stages. See, Download a consolidated diff report of a NetScaler upgrade job.

You can import a script file or type commands directly in the NetScaler Console GUI.

- **Import commands from file**: Select the command input file from your local computer.
- **Type commands**: Enter the commands directly on the GUI.

In the post upgrade stage, you can use the same script specified in the pre-upgrade stage.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



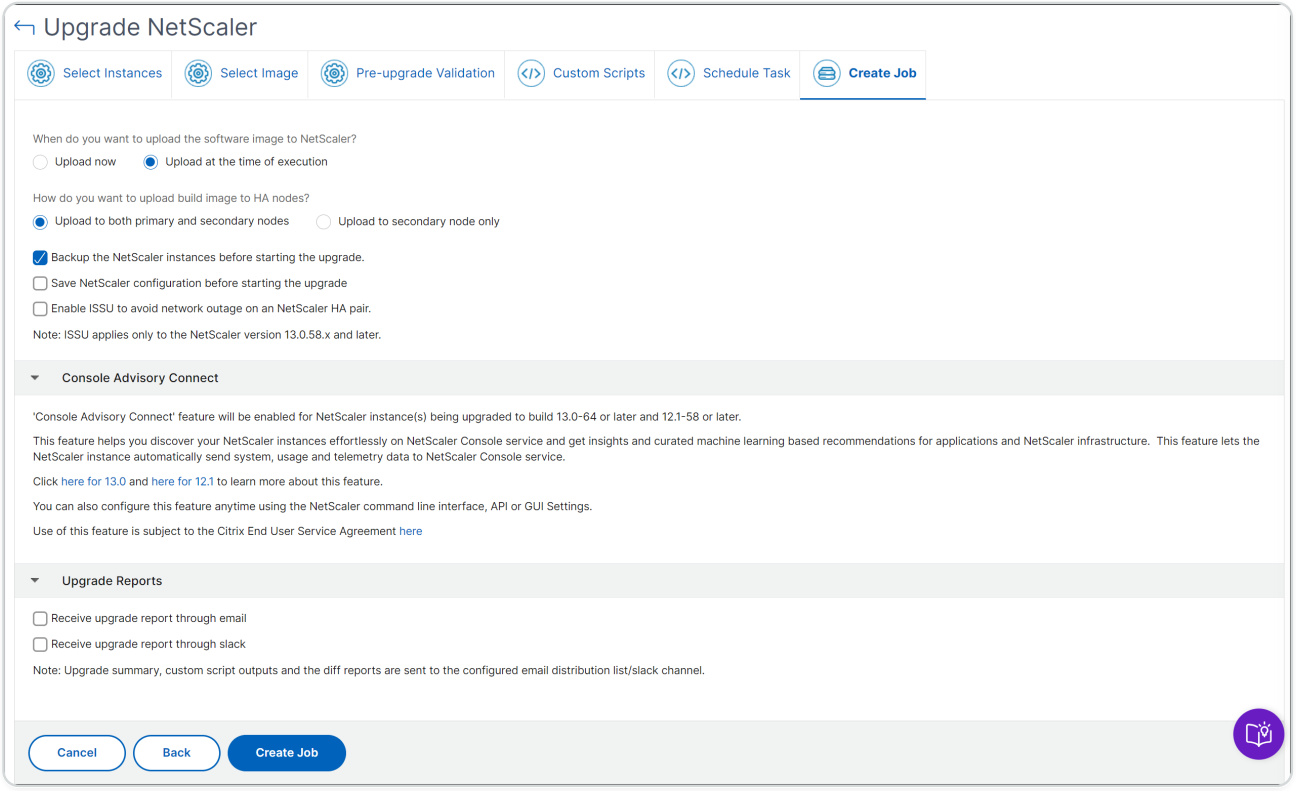
NetScaler upgrade options

While you create a NetScaler upgrade job, you can select the following options in the **Create Job** tab:

- **Backup the NetScaler instances before starting the upgrade.**: Creates a backup of the selected NetScaler instances.
- **Maintain the primary and secondary status of high-availability nodes after upgrade**: Select this option if you want the upgrade job to start a failover after each node's upgrade. In this way, the upgrade job maintains the primary and secondary status of the nodes.
- **Save NetScaler configuration before starting the upgrade** - Saves the running NetScaler configuration before upgrading the NetScaler instances.
- **Enable ISSU to avoid network outage on NetScaler HA pair** - ISSU ensures the zero downtime upgrade on a NetScaler high-availability pair. This option provides a migration functionality that honors the existing connections during upgrade. So, you can upgrade an NetScaler high-availability pair without downtime. Specify the ISSU migration timeout in minutes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Receive Execution Report through email** - Sends the execution report in email. To add an email distribution list, see Create an email distribution list.
- **Receive Execution Report through slack** - Sends the execution report in slack. To add a Slack profile, see Create a Slack profile.



Scheduling upgrade jobs for a NetScaler high-availability pair

The following table lists the different scheduling scenarios in the **Schedule Task** page and the corresponding upgrade options available in the **Create Job** page:

WHEN DO YOU WANT TO EXECUTE THE UPGRADE JOB?	WHEN DO YOU WANT TO UPLOAD THE SOFTWARE IMAGE TO NETSCALER?	HOW DO YOU WANT TO UPLOAD BUILD IMAGE TO HA NODES?
Upgrade now	Not applicable	**Upload to both primary and secondary nodes** (default option)
	Upload to secondary node only	
Schedule later	**Upload at time of execution** (default option)	**Upload to both primary and secondary nodes** (default option)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WHEN DO YOU WANT TO EXECUTE THE UPGRADE JOB?	WHEN DO YOU WANT TO UPLOAD THE SOFTWARE IMAGE TO NETSCALER?	HOW DO YOU WANT TO UPLOAD BUILD IMAGE TO HA NODES?
	Upload to secondary node only	
	Upload now	Not applicable
Schedule later (when **Perform two stage upgrade for nodes in HA** is selected)	**Upload at time of execution** (default option)	**Upload to secondary node only** (default and only option)
	Upload now	Not applicable

Download a consolidated diff report of a NetScaler upgrade job

In NetScaler Console, you can download a diff report of a NetScaler upgrade job. To do so, the upgrade job must have custom scripts. A diff report contains the differences between the outputs of the pre-upgrade and post-upgrade script. With this report, you can determine what changes occurred on the NetScaler instance post upgrade.

NOTE:

The diff report is generated only if you specify the same script in the pre-upgrade and post-upgrade stages.

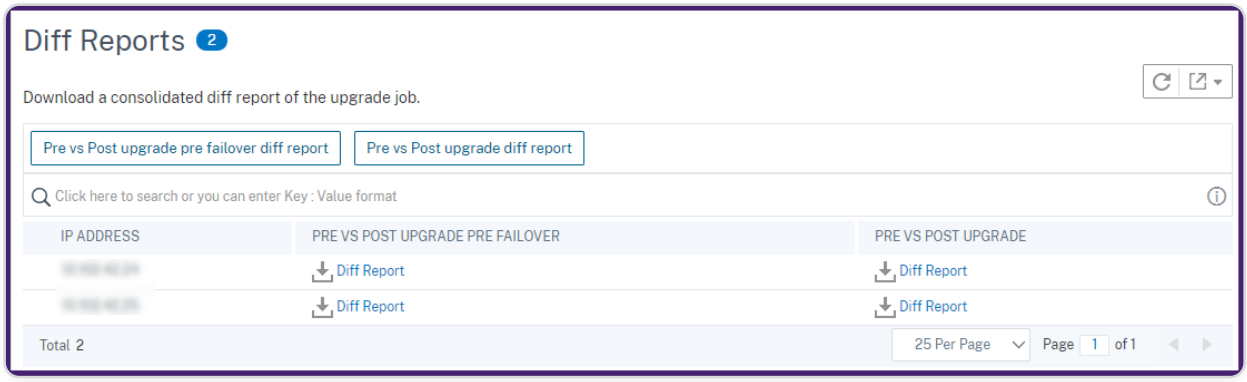
To download a diff report of an upgrade job, do the following:

1. Navigate to **Infrastructure > Configuration Jobs > Maintenance Jobs**.
2. Select the upgrade job for which you want to download a diff report.
3. Click **Diff Reports**.
4. In **Diff Reports**, download a consolidated diff report of the selected upgrade job.

   In this page, you can download any of the following diff reports type:

   - **Pre vs Post upgrade pre failover diff report**
   - **Pre vs Post upgrade diff report**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Network functions

Using the Network Functions feature, you can monitor the state of the entities configured on your managed Citrix Application Delivery Controller (NetScaler) instances. You can view statistics such as transaction details, connection details, and throughput of a load balancing virtual server. You can also enable or disable the entities when you plan a maintenance.

The Network Functions dashboard provides you with the following graphs:

- Top 5 virtual servers with highest client connections
- Top 5 virtual servers with highest server connections
- Top 5 virtual servers with maximum throughput (MB/sec)
- Bottom 5 virtual servers with lowest throughput (MB/sec)
- Top 5 instances with most virtual servers
- State of the virtual servers
- Health of the load balancing virtual servers
- Protocols
- Load Balancing Method
- Load Balancing Persistence

Generate reports for load balancing entities

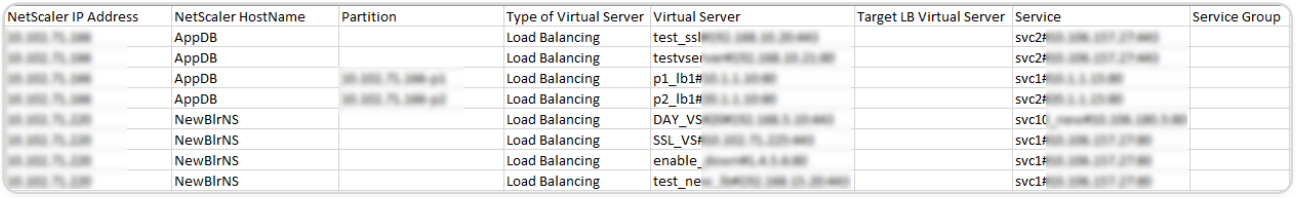
NetScaler Console allows you to view the reports of Citrix Application Delivery Controller (NetScaler) instance entities at all levels. There are two types of reports that you can download in **NetScaler Console > Network Functions** - consolidated reports and individual reports.

Consolidated reports: You can download and view a consolidated or a summarized report for all entities that are managed on NetScaler instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This report allows you to have a high-level view of the mapping between the NetScaler instances, partitions, and the corresponding load balancing entities (virtual servers, service groups, and services) that are present in the network.

The following image shows an example of a summarized report.



NetScaler IP Address	NetScaler HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
[redacted]	AppDB		Load Balancing	test_ssl[redacted]		svc2[redacted]	
[redacted]	AppDB		Load Balancing	testvser[redacted]		svc2[redacted]	
[redacted]	AppDB	[redacted]	Load Balancing	p1_lb1#[redacted]		svc1#[redacted]	
[redacted]	AppDB	[redacted]	Load Balancing	p2_lb1#[redacted]		svc2#[redacted]	
[redacted]	NewBlrNS		Load Balancing	DAY_VS[redacted]		svc1[redacted]	
[redacted]	NewBlrNS		Load Balancing	SSL_VS#[redacted]		svc1#[redacted]	
[redacted]	NewBlrNS		Load Balancing	enable_[redacted]		svc1#[redacted]	
[redacted]	NewBlrNS		Load Balancing	test_ne[redacted]		svc1#[redacted]	

The consolidated report is in a CSV format. The entries in each column are described as follows:

- **NetScaler IP Address**: IP address of the NetScaler instance is displayed in the report
- **NetScaler HostName**: Host name is displayed in the report.
- **Partition**: IP address of the administrative partition is displayed
- **Virtual Server**: \<name_of_the_virtual_server\>#virtual_IP_address:port_number
- **Services**: \<name_of_the_service\>#service-IP_address:port_number
- **Service Groups**: \<name_of_service_group\>#server_member1_IP_address:port,server_member2_IP_address:port,

NOTE

- If there is no host name available, the corresponding IP address is displayed.
- Blank columns indicate that the respective entities are not configured for that NetScaler instance.

Individual reports: You can also download and view independent reports of all instances and entities. For example, you can download a report for only load balancing virtual servers or load balancing services or load balancing service groups.

NetScaler Console allows you to download the report instantly. You can also schedule the report to be generated at a fixed time once a day, once a week, or once a month.

Generate a combined load balancing report

1. In NetScaler Console, navigate to **Infrastructure > Network Functions**.
2. Click **Generate Report**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. On the **Generate Report** page that opens, you have two options to view the report:

   a. On the **Export Now** tab, select **Load Balancing** and click **OK**.

      The consolidated report downloads to your system.

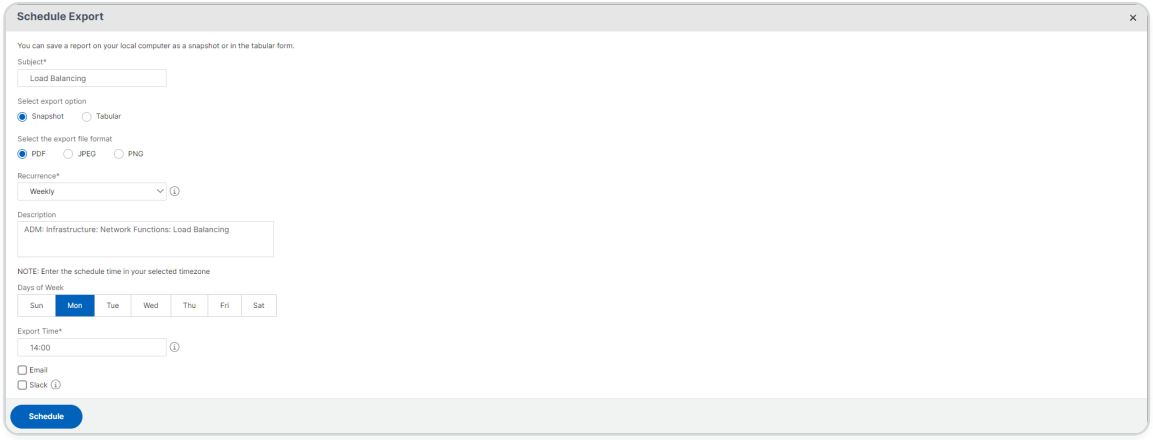
   b. Select **Schedule Report** to create a schedule for generating and exporting reports at regular intervals. Specify the report generation recurrence settings and create an email profile to which the report is exported.

      i. Select **Enable Schedule**.

      ii. **Recurrence** - select **Daily**, **Weekly**, or **Monthly** from the list.

      NOTE

      If you select **Weekly** recurrence, ensure that you select the weekdays on which you want the report to be scheduled.

      NOTE

      If you select **Monthly** recurrence, ensure that you enter days of month, with the values between 1 and 31.

      iii. **Export time** - Enter the time in the Hour: Minute in 24-hour format.

      iv. **Email** - check the check-box and then select a profile from the list, or click **Add** to create an email profile.

      v. **Slack** - Select the Slack check box and then select a profile from the list box, or click **Add** to create a slack profile.

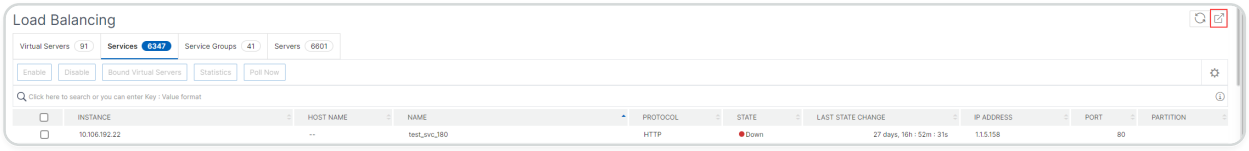
      vi. Click **Schedule** to complete the process.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Generate an individual load balancing entity report

You can generate and export an individual report for a particular type of entity associated with the instances. For example, consider a scenario where you want to see a list of all load balancing services in the network.

1. In NetScaler Console, navigate to **Infrastructure > Network Functions > Load Balancing > Services**.
2. On **Services** page, click the **Export** button at the top right-hand corner.



Select **Export Now** tab if you want to generate and view the report at this instant.

NOTE

You can only download the reports or export the reports as mail attachments. You cannot view the reports on the NetScaler Console GUI.

Export or schedule export of network functions reports

You can generate a comprehensive report for selected network functions such as Load Balancing, Content Switching, Cache Redirection, Global Server Load Balancing (GSLB), Authentication, and NetScaler Gateway in NetScaler Console. This report allows you to have a high-level view of the mapping between the instances, partitions, and the corresponding bound entities (virtual servers, service groups, and services) that are present in the network. You can export these reports in .csv file format.

The report displays the following virtual server data:

- NetScaler IP address
- Host name
- Partition data
- Virtual Server name
- Type of virtual server
- Virtual server
- Target LB virtual server

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

For Content Switching and Cache Redirection virtual servers, the Target LB virtual server column lists all the LB servers, that is, both default servers and policy-based servers.

- Service name
- Service group name

You can schedule to export these reports to specified email addresses at different intervals. For information on how to set up email notifications, see Create event rules.

NOTE

- For GSLB virtual servers, the network functions report displays only GSLB virtual servers and associated services.
- For Content Switching and Cache Redirection virtual servers, the report displays only the bindings to the associated LB servers.
- SSL virtual servers are not listed in this report because a separate list of SSL virtual servers is not maintained on NetScaler Console.
- When a new report is generated, the older reports are automatically purged from your account.

To export and schedule network functions reports:

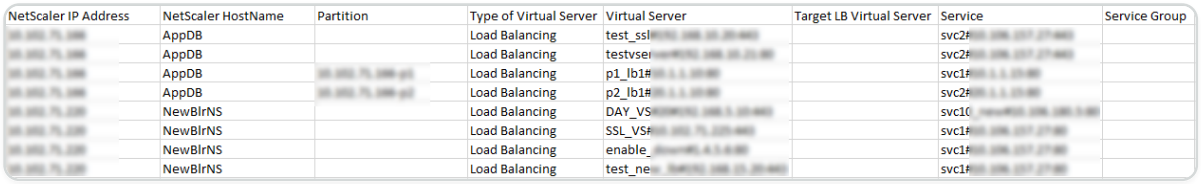
1. Navigate to **Infrastructure > Network Functions**.
2. On the **Network Functions** page, in the right pane, click **Generate Report** at the top right corner of the page.
3. On the **Generate Report** page, you have the following 2 options:

   a. Select **Export Now** tab and click **OK**.

      The report downloads to your system.

      The following image shows an example of a network functions report.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NetScaler IP Address	NetScaler HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
[redacted]	AppDB		Load Balancing	test_ssl[redacted]		svc2[redacted]	
[redacted]	AppDB		Load Balancing	testvser[redacted]		svc2[redacted]	
[redacted]	AppDB	[redacted]	Load Balancing	p1_lb1#[redacted]		svc1#[redacted]	
[redacted]	AppDB	[redacted]	Load Balancing	p2_lb1#[redacted]		svc2#[redacted]	
[redacted]	NewBlrNS		Load Balancing	DAY_VS[redacted]		svc10[redacted]	
[redacted]	NewBlrNS		Load Balancing	SSL_VS#[redacted]		svc1#[redacted]	
[redacted]	NewBlrNS		Load Balancing	enable_[redacted]		svc1#[redacted]	
[redacted]	NewBlrNS		Load Balancing	test_ne[redacted]		svc1#[redacted]	

b. Select **Schedule Report** to create a schedule to generate and export reports at regular intervals. Specify the report generation recurrence settings and create an email profile to which the report is exported.

   i. **Recurrence** - Select **Daily**, **Weekly**, or **Monthly** from the drop-down list box.

   ii. **Recurrence time** - Enter the time in the Hour: Minute in 24-hour format.

   iii. **Email** - Select the check box and then select the profile from the drop-down list box, or click **Add** to create an email profile.

   iv. **Slack** - Select the check box and then select the profile from the drop-down list box, or click **Add** to create an email profile.

   Click **Enable Schedule** to schedule your report and then, click **OK**. By clicking the **Enable Schedule** check box, you can generate the selected reports.

Network reporting

You can optimize resource usage by monitoring your network reporting on NetScaler Console. You may have a distributed deployment with many applications deployed at multiple locations. To ensure optimal performance of your applications, you have also deployed multiple Citrix Application Delivery Controller (NetScaler) instances to load balance, content switch, or compress the traffic. Network performance can impact the application performance. To continue to maintain the performance of your applications, you must regularly monitor your network performance and make sure that all resources are used optimally.

NetScaler Console allows you to generate reports for instances at a global level and entities such as the virtual servers and network interfaces. The virtual servers for which you can generate reports are as follows:

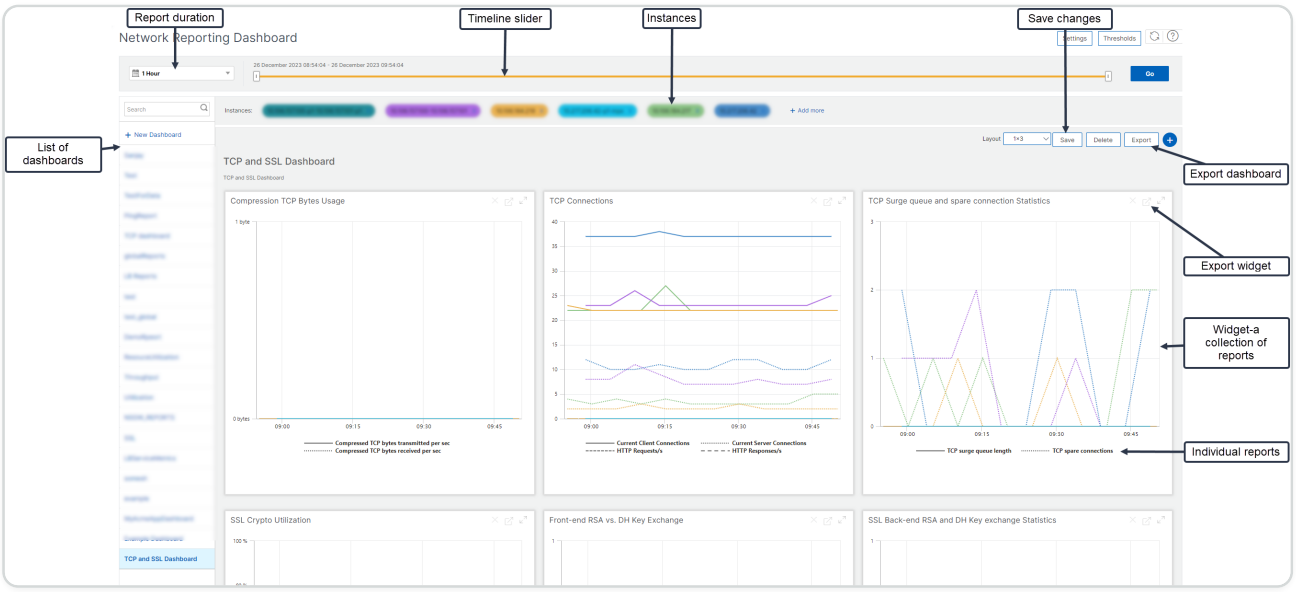
- Load balancing servers, services, and service groups
- Content switching servers
- Cache redirection servers
- Global service load balancing (GSLB)
- Authentication
- NetScaler Gateway

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can create multiple dashboards for various instances, virtual servers, and other entities in NetScaler Console.

Network reporting dashboard

The following image calls out the various features in the dashboard:



- The left side panel lists all the custom dashboards that are created in NetScaler Console. You can click one of them to view the various reports that the dashboard is composed of. For example, a TCP and SSL dashboard contains various reports related to TCP and SSL protocols.
- You can customize each dashboard with multiple widgets to display various reports. A widget represents a report on the dashboard, that is a collection of more related reports. For example, a compression TCP Bytes Usage report has reports for compressed TCP bytes transferred and received per second.
- You can display reports for one hour, one day, one week, or for one month. You can use the timeline slider option to customize the duration of reports being generated on the NetScaler Console.
- You can remove a report by clicking "X". You can also export the report as a .pdf, .jpeg, .png, or .csv format to your system. You can also schedule a time and recurrence of when to generate the report. You can also configure an email distribution list to which you want to send the reports.
- The Instances section at the top of the dashboard lists the IP addresses of all the instances for which the report is generated.
- You can either remove instances by clicking "X" or add more instances to the reports. But, currently NetScaler Console allows you to view reports for 10 instances.

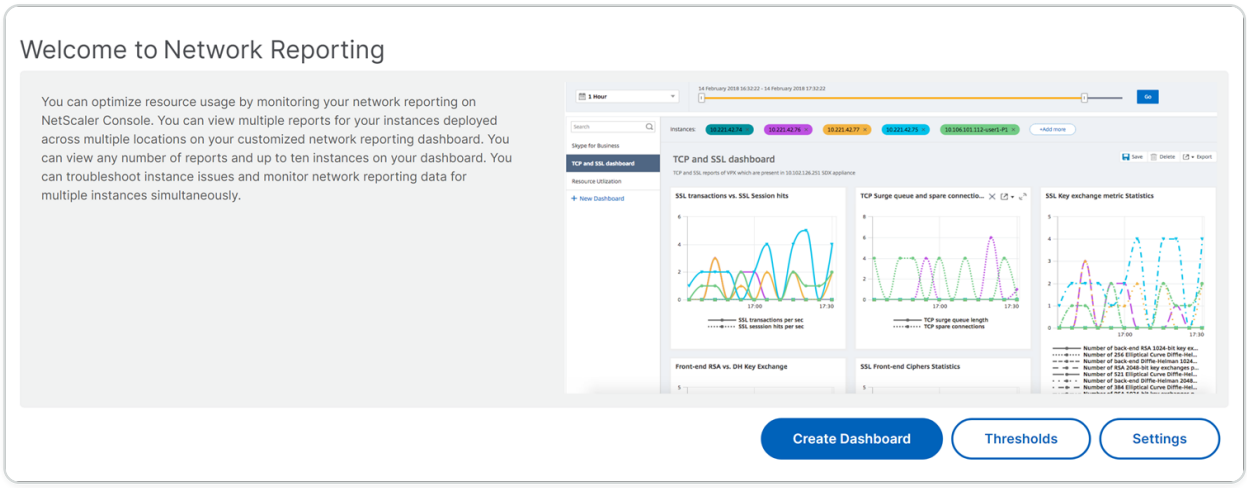
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You can also export the entire dashboard as a .pdf, .jpeg, .png, or .csv format to your system. Any changes made to the dashboard must be saved. Click Save to save the changes.

The following section explains in detail the tasks to create a dashboard, generate reports, and to export reports.

To view or to create a dashboard:

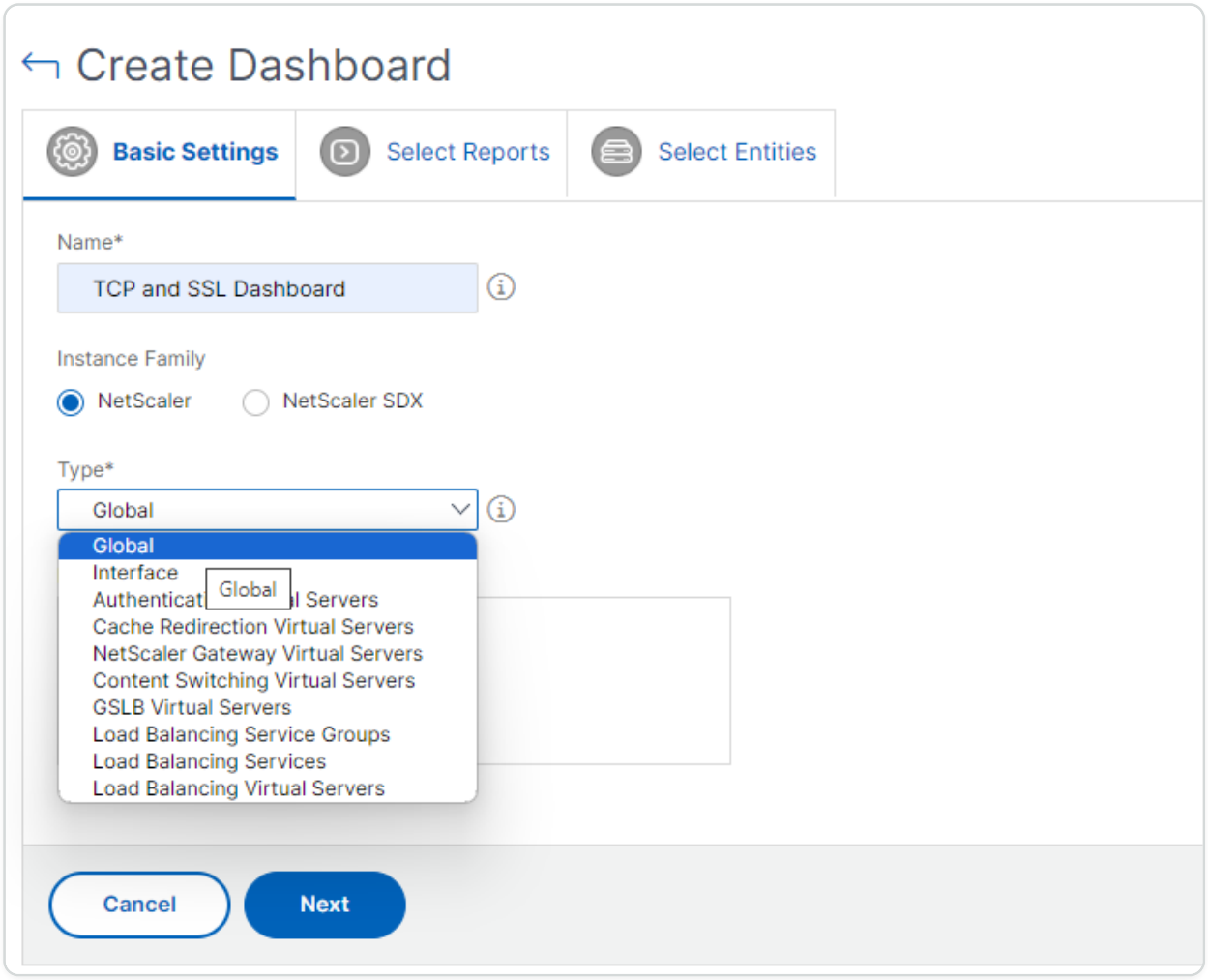
1. In NetScaler Console, navigate to **Infrastructure > Network Reporting**.



2. To view the existing dashboards, click **View Dashboard**. The Network Reporting **Dashboard** page opens where you can view all your dashboards and report widgets.
3. To create a dashboard, click **Create Dashboard**.

   The **Create Dashboard** page opens.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. In the **Basic Settings** tab, enter the following details:

   a. **Name**. Type the name of the dashboard.

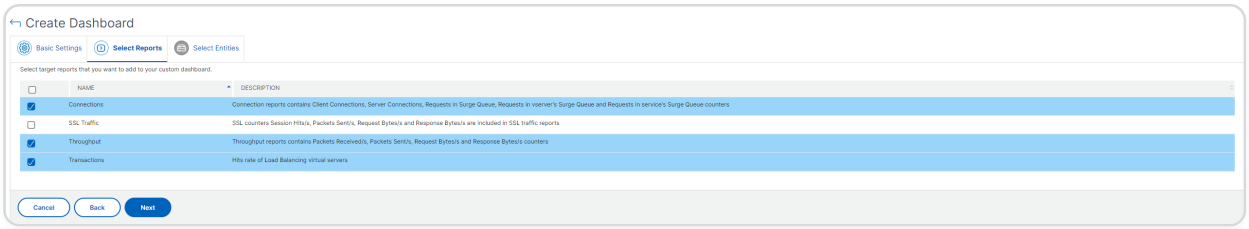
   b. **Instance Family**. Select the type of instance - NetScaler or NetScaler SDX.

   a. **Type**. Select the entity type for which you want to generate reports. In this example, select load balancing virtual servers.

   b. **Description**. Type a meaningful description for the dashboard.

5. Click **Next**.

6. In the **Select Reports** tab, select the reports required. In this example, you can select transactions, connections, and throughput. Click **Next**.

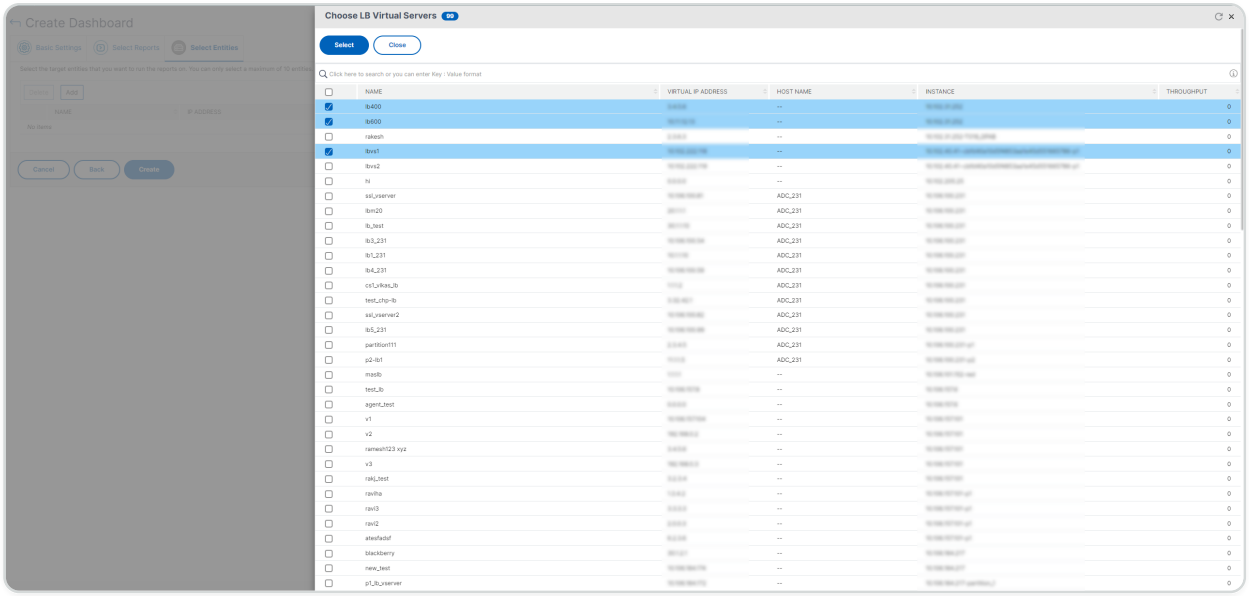


7. In the **Select Entities** tab, click **Add**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

A window appears with the entities list depending on the selected entity type in the **Basic Settings** tab. In this example, the **Choose LB Virtual Servers** window appears.

8. Select the entities that you want to monitor.



9. Click **Create**.

The dashboard is created and displays all the reports that you have selected.

NOTE

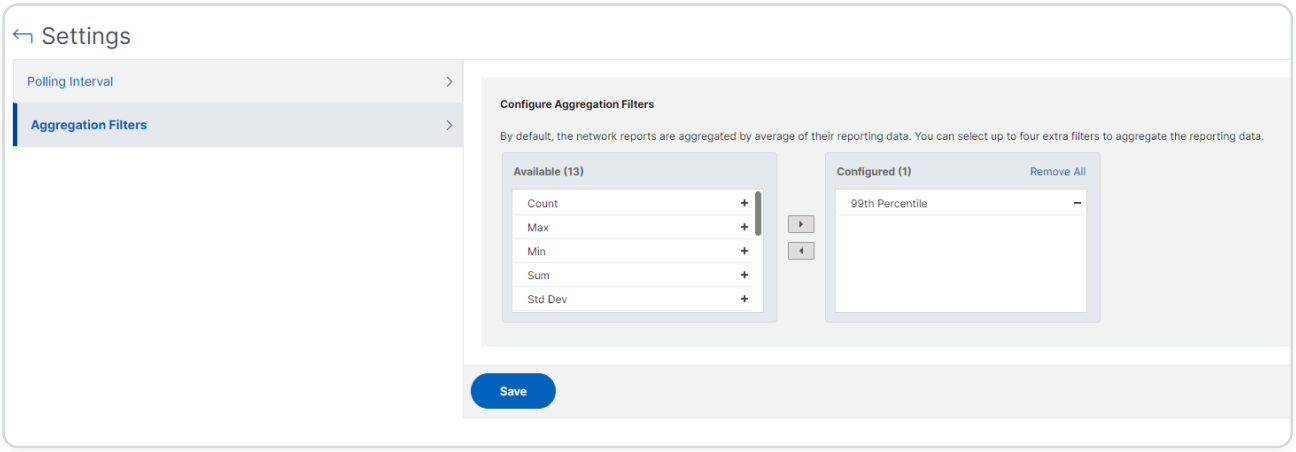
Currently, any changes that you make to legends or filters cannot be saved.

View network reporting data by applying aggregations

You can apply aggregations to the network performance data and view application performance on the dashboard. You can also export the results based on your requirement. Using these aggregations applied to the data, you can analyze and check if all resources are used optimally. Navigate to **Network > Network Reporting** and select the time duration 1 day or later to get the **View By** option.

In the existing average data, you can apply aggregations by selecting the option from the **View By** list. When you apply aggregation, the data is updated for each metric in the dashboard. Click **Settings** and select **Aggregation Filters**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following are the aggregations that you can add:

- Count
- Max
- Min
- Sum
- Std Dev
- Variance
- Mode
- Median
- 25th Percentile
- 75th Percentile
- 95th Percentile
- 99th Percentile
- First
- Last

You can add up to 4 aggregation options to the dashboard. After you add the aggregation options, NetScaler Console takes approximately 1 hour to generate reports for the selected aggregation options.

Exporting network reports

While you can export widget reports in .pdf, .png, .jpeg, or .csv formats, you can export the entire dashboards in only .pdf, .jpeg, or .png formats.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

You cannot export reports in NetScaler Console if you have read-only permissions. You need an edit permission to create a file in NetScaler Console and to export the file.

To export dashboard reports:

1. Navigate to **Infrastructure > Network Reporting**
2. Click **View Dashboards** to view all the dashboards that you've created.
3. In the left pane, click a dashboard. In this example, click **Dashboard 1**.
4. Click the export button at the top right corner of the page.
5. Under the **Export Now** tab, select the required format, and then click **Export**.

   On the **Export** page, you can do one of the following:
6. Select **Export Now** tab. To view and save the report in PDF, JPEG, PNG, or CSV format.
7. Select **Schedule Export** tab. To schedule the report daily, weekly, or monthly and send the report over an email or slack message.

   You can schedule an export of the **Network Reporting Dashboard** page on a recurrent basis. For example, you can set an option to generate a dashboard report every week for the previous one hour at a particular time. The report is generated every week then and shows the status of the dashboard. The report overrides the time and date stamp, if set by the user.

NOTE

- If you select Weekly recurrence, select the weekdays on which you want the report to be scheduled.
- If you select Monthly recurrence, enter all the days that you want the report to be scheduled separated by commas.

While scheduling network reports, you can customize the heading of the report by entering a text string in the **Subject** field. The report created at the scheduled time has this string as its name.

For example, for network reports originating from a particular virtual server, you can type in the subject as "authentication-reports-10.106.118.120," where 10.106.118.120 is the IP address of the monitored virtual server.

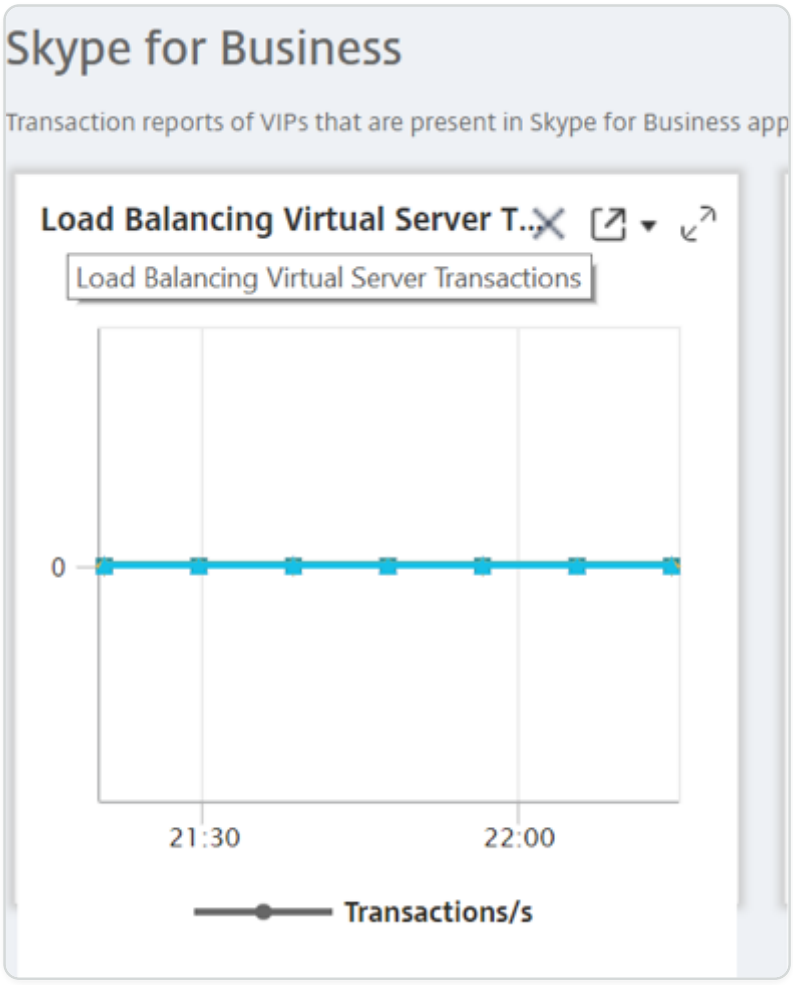
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

Currently, this option is available only when you schedule the export of reports. You cannot add a heading to the report when you export them instantly.

To export widget reports:

1. Navigate to **Infrastructure > Network Reporting**.
2. Click **View Dashboards** to view all the dashboards that you have created.
3. In the left pane, click a dashboard. In this example also click **Skype for Business**.
4. Select a widget. For example, select **Load Balancing Virtual Server Transactions**.
5. Click the export button at the top right corner of the page
6. Under the **Export Now** tab, select the required format, and then click **Export**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

How to manage Thresholds for Network Reports on NetScaler Console

To monitor the state of a NetScaler instance, you can set thresholds on counters and receive notifications when a threshold is exceeded. On NetScaler Console, you can configure thresholds and view, edit, and delete them.

For example, you can receive an email notification when the Connections counter for a content switching virtual server reaches a specified value. You can define a threshold for a specific instance type. You can also choose the reports you want to generate for specific counter metrics from your chosen instance.

When the value of a counter exceeds or falls below (as specified by the rule) the threshold value, an event of the specified severity is generated to signify a performance related issue. When the counter value returns to a value that you consider normal, the event is cleared. These events can be viewed by navigating to **Infrastructure > Events > Reports**. On the **Reports** page, you can click the **Events by Severity** donut to view events by their severity.

You can also associate an action with a threshold such as sending an email or SMS message when the threshold is breached.

To create a threshold:

1. In NetScaler Console, navigate to **Infrastructure > Network Reporting > Thresholds**. Under **Thresholds**, click **Add**.
2. On the **Create Threshold** page, specify the following details:
    - **Name**. Name of the threshold.
    - **Instance Type**. A NetScaler instance.
    - **Report Name**. Name of the performance report that provides information about this threshold.
3. You can also set rules to specify when an event is to be generated or cleared. You can specify the following details under the **Configure Rule** section:
    - **Metric**. Select the metric for which you want to set a threshold.
    - **Comparator**. Select a comparator to check whether the monitored value is greater than or equal to or less than or equal to the threshold value.
    - **Threshold Value**. Type the value for which the event severity is calculated. For example, you might want to generate an event with critical event severity if the monitored value for

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Current Client Connections reaches 80 percent. In this case, type 80 as the threshold value. You can view "critical severity" events by navigating to **Infrastructure > Events** > **Reports**. On the **Reports** page, you can click the **Events by Severity** donut to view events by their severity.

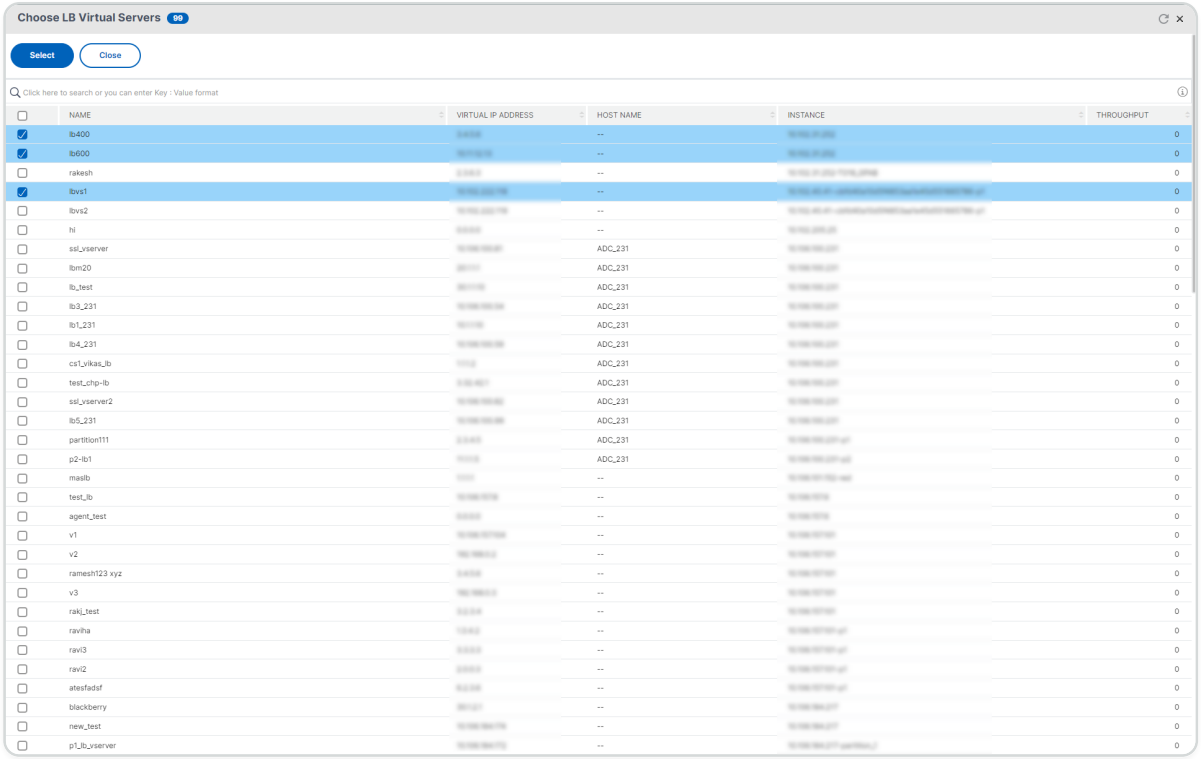
- **Clear Value**. Type the value that indicates when to clear the value. For example, you might want to clear the Current Client Connections threshold when the monitored value reaches 50 percent. In this case, type 50 as the clear value.
- **Event Severity**. Select the security level that you want to set for the threshold value.

4. You can choose instances and entities to be set with the threshold value. In the **Instances** section, choose one of the following options:

   - **All Instances**. The threshold is set for all the instances.
   - **Specific Instances**. The threshold is set for specific instances. Use the right arrow to move instances from the **Available** list to the **Configured** list. The threshold is set for the instances in the **Configured** list.
   - **Specific Entities**. The threshold is set for specific entities.

     Click **Add** to select the entities.

     A window appears with the entities list depending on the selected report type in the **Report Name** field. In this example, the **Choose LB Virtual Servers** window appears.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

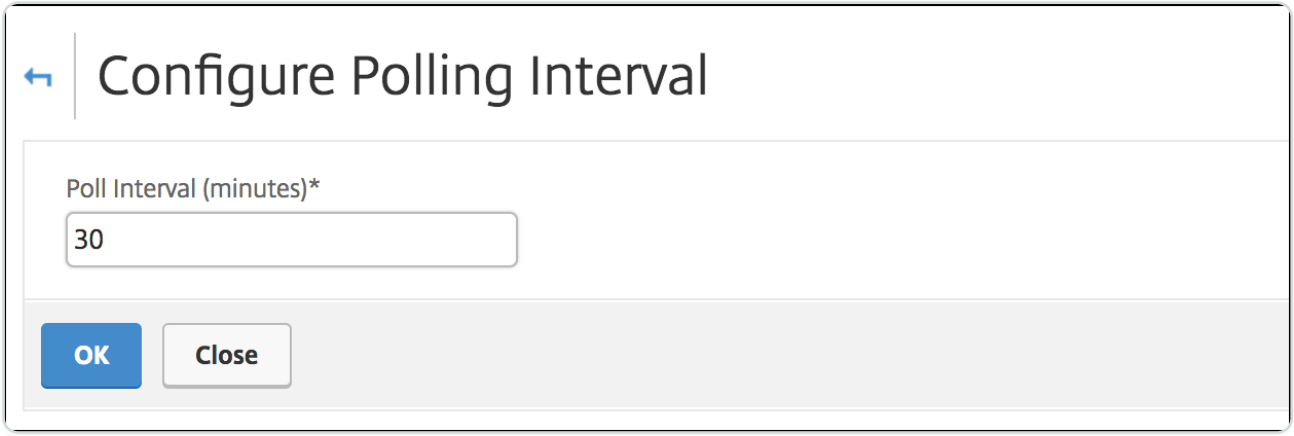
Select the entities for which you want to set a threshold. Click **Select**. The selected entities appear in the **Instances** section.

5. You can choose to have a message appear when the threshold is reached. In the **Event Message** section, type the message in the message box. NetScaler Console appends the monitored value and the threshold value to this message.
6. In the **Notification Settings** section, select **Enable Threshold** to enable the threshold to generate alarms. Optionally, you can select **Notify through Email** to receive notifications through various channels like email, Slack, ServiceNow, or PagerDuty when the threshold is reached.
7. Click **Create**.

Set Performance Polling Interval for Network Reports

By default, every 5 minutes, NITRO calls collect performance data for network reporting. The NetScaler Console retrieves instance statistics such as counter information and aggregates them based on per minute, per hour, per day, or per week. You can view this aggregated data in predefined reports.

To set the performance polling interval, navigate to **Infrastructure > Network Reporting** and click **Configure Polling Interval**. Your polling interval cannot be less than 5 minutes or more than 60 minutes.



Configuring Network Reporting Prune Settings

You can configure the purge interval of network reporting data in NetScaler Console. This interval limits the amount of network reporting data being stored in the NetScaler Console server's database. By default, pruning happens every 24 hours (at 01.00 hours) for the network reporting historical data.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

The value that you can specify cannot exceed 90 days or be less than 1 day.

Provisioning

This section covers the following topics:

- App-based provisioning in AWS
- App-based provisioning in Azure
- Provisioning NetScaler VPX instances
  - AWS
  - Microsoft Azure
  - Google Cloud
  - VMware vCenter
- NetScaler Global Load Balancing for public clouds

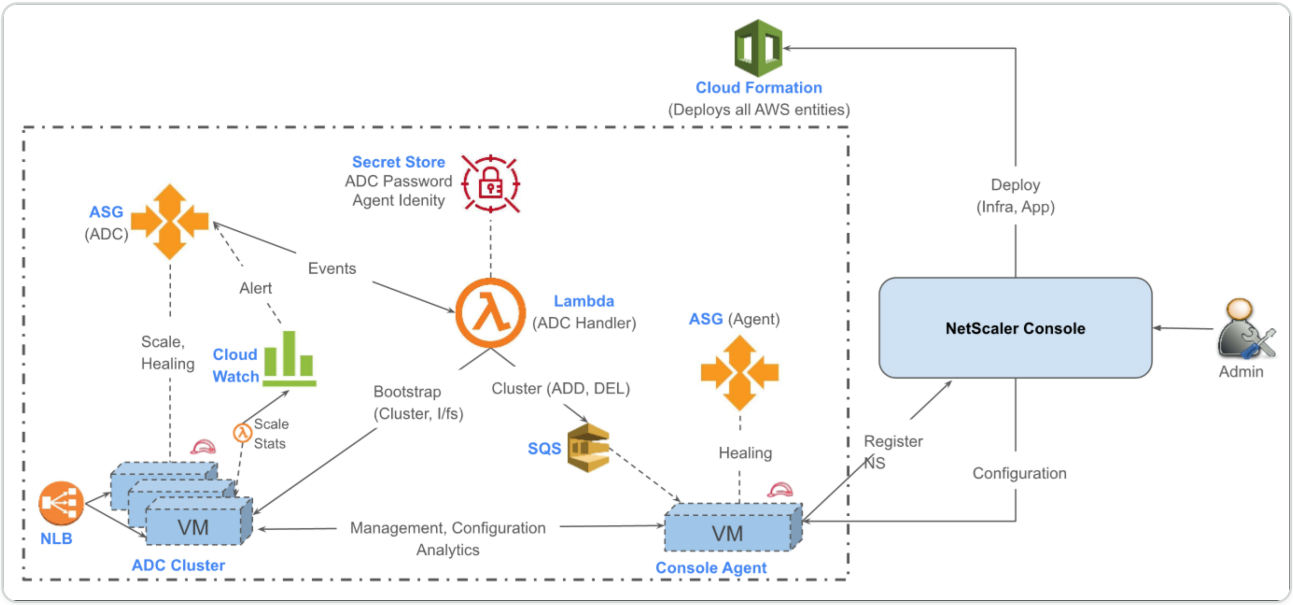
App-based provisioning in AWS

NetScaler Console service introduces "App based" provisioning, designed to streamline and simplify NetScaler deployments on cloud data centers and deliver applications from them.

NetScaler Console service accepts the customer's cloud credentials and sets up the infrastructure required for application delivery by orchestrating the launching of NetScaler, agents and the necessary cloud entities on AWS. NetScaler administrators can leverage both Flexed and Cloud marketplace licenses for their NetScaler, ensuring flexibility in licensing options.

Administrators can then deliver applications on their cloud by defining delivery settings in a straightforward, app centric manner from NetScaler Console service. It then takes care of configuring both ADCs and AWS infrastructure to deliver their applications. Once the applications are delivered, NetScaler administrators gain access to the rich analytics and monitoring features of the NetScaler Console service to effectively manage and monitor their applications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Prerequisites

Subscribe to the following products in the AWS Marketplace.

- NetScaler VPX - Subscribe to one of the following variants:
  - NetScaler VPX BYOL - Subscribe if you have purchased flexed licenses, and they are available in NetScaler Console service for licensing NetScaler instances.
  - NetScaler VPX Premium - 1000 Mbps Subscribe if you want a subscription based license from the AWS Marketplace.
  - NetScaler Agent Service
- Select a VPC - Select a VPC for setting up the infrastructure for application delivery. The VPC should have a CIDR of /22 or more. During the infrastructure deployment process dedicated subnets for ADC infrastructure are created consuming /24 address space for each Availability zone selected. Select a VPC from the list based on your deployment:
  - Dedicated VPC that is separate from the applications, if you want your deployment to be similar to a DMZ.
  - Same VPC where the applications are also present.
- NAT Gateway - The delivery infrastructure, such as the Console agent, that is autoprovisioned must have access to NetScaler Console service over the internet. A NAT gateway can provide this access. If you already have a NAT gateway you can also reuse that for delivery infrastructure by selecting it during the deployment. If a NAT gateway is not selected, the deployment process creates one.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cloud access profile

A cloud access profile is used to give permissions of the customer's AWS account to NetScaler Console service. While creating a cloud access profile the administrator must run a CloudFormationTemplate (CFT) in AWS. The CFT creates IAM roles and policies in the customer's AWS account.

1. Navigate to **Infrastructure > Provisioning > App based > Cloud Access Profiles**.
2. Follow the on-screen directions to create a cloud access profile for your subscription.

NOTE:

To create this profile, the NetScaler administrator must also be the AWS account administrator and must have the necessary permissions to create IAM entities.

App environment

App Environment represents the delivery infrastructure set up in a VPC for delivering the applications. When an administrator creates an App Environment in the NetScaler Console service, all the resources for delivering and monitoring applications, including gateways, security groups, subnets, NetScaler instances, and Console agents, are deployed as part of an App Environment. See the FAQ section for more information.

1. Navigate to **InfraStructure > Provisioning > App based > Environments**.
2. Follow the on-screen directions to create an App Environment.

NOTE:

The service does not make any changes to the resources created by the customer in their VPC. It only provisions the necessary infrastructure to deliver and monitor the applications.

Application delivery

Application delivery is the core component of the App based provisioning feature and contains the mandatory application delivery and security information. As part of application delivery configuration you define the following entities:

- The endpoint representing how the application is accessed by the clients, such as protocol, port, certificates, and ciphers. For example, an SSL profile of an endpoint represents the set of

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SSL configurations that includes the supported ciphers and protocols. A predefined A+ SSL profile is available by default.

- The services that represent an application's component, which must be accessed based on the specific HTTP request. For example, a component for an ecommerce application could be an order service, a catalog service, or a payment service that are installed in different application servers and requests must be routed based on the URL accessed. The service profile of an application service represents how the delivery infrastructure can access and monitor the application service, such as load balancing, SSL, and health check settings.
- The content policy that defines how the L7 content is inspected and modified when a request arrives for a specific service. It is used to take a predefined action on the HTTP requests based on headers, URLs, or IP addresses. Some of the actions could be header enrichment, redirecting requests, or dropping requests.

1. Navigate to **InfraStructure > Provisioning > App based > App Delivery**.
2. Follow the on-screen directions to create a new application.

FAQs

What entities are created by NetScaler Console service for delivering an application in the cloud?

NetScaler Console service creates the following entities in the customer's VPC:

- NetScaler VPX cluster in each Availability Zone.
  - The VPX instances are deployed as an EC2 Autoscale™ group.
  - A single node cluster is created during App Environment creation. This cluster can scale up to a maximum of 8 nodes.
- Console agent in each Availability Zone.
- Subnets: One subnet each for management, client, and server networks.
- Security groups: One security group each for management, client, and server NICs.
  - Management security group: This security group is associated with the management NICs of the NetScaler instances and agents. It consists of rules to allow communication between NetScaler instances, agents, and any other control plane traffic.
  - Client security group: This security group is associated with the client NICs of the NetScaler instances and is used to allow the data traffic to the NetScaler virtual servers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Server security group: This security group is associated with the server NICs of the NetScaler instances and does not contain any default rules.

- Route tables

    - Client route table: This route table facilitates the internet-bound traffic. It includes a route directing traffic to the Internet Gateway associated with the VPC, which enables connectivity to the internet for resources within the VPC.
    - Management route table: This route table facilitates traffic originating from NetScaler and agents for Network Address Translation (NAT) by the NAT Gateway.

- NAT gateway in each Availability Zone: A NAT gateway enables NetScaler and Console agents to access the internet.

  NOTE:

  A NAT gateway is not created if you want to reuse an existing NAT gateway in their VPC.

- Secrets manager: A secret manager is used to:

    - Store the agent token and URL that is used for registering the agent with NetScaler Console service.
    - Store the ADC password for authentication.

- Lambda functions

    - ClusterLambdaFunction: This lambda function is responsible for the creation and management of the NetScaler cluster.
    - StatsLambdaFunction: This lambda function is created for collecting metrics from NetScaler that are used for autoscaling.

What are the metrics used to Autoscale NetScaler?

The following metrics are used to Autoscale NetScaler:

- The minimum number of instances in the Autoscale group is 1 and the maximum is 8.
- Scale-Out by 1 capacity unit. That is, cpu_use > 70% or throughput > 70% for 5 consecutive periods of 60 seconds.
- Scale-In by 1 capacity unit. That is, cpu_use =< 30% and throughput =< 30% for 5 consecutive periods of 60 seconds.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How can an administrator identify the resources created by NetScaler Console service in the cloud?

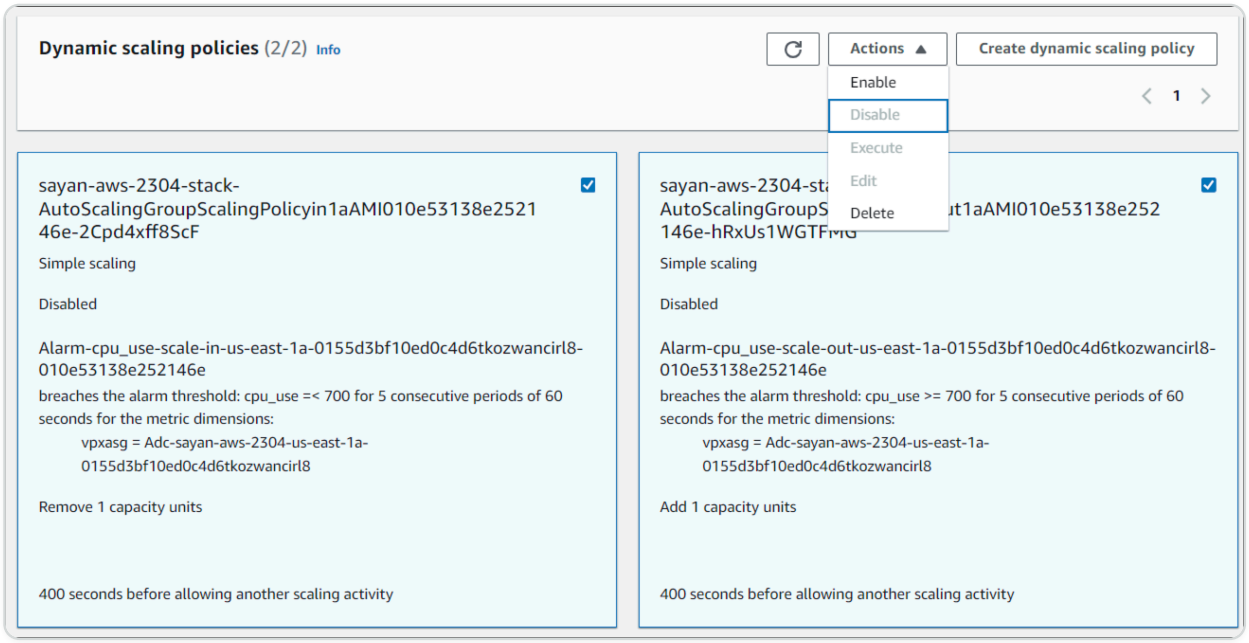
All AWS resources are created by default with the tag “UsedFor: AppDeliveryByNetScaler”. In addition, the resources are tagged using the tags specified during the App Environment creation workflow.

How can a NetScaler administrator upgrade NetScaler in an App Environment?

Perform the following steps to upgrade NetScaler:

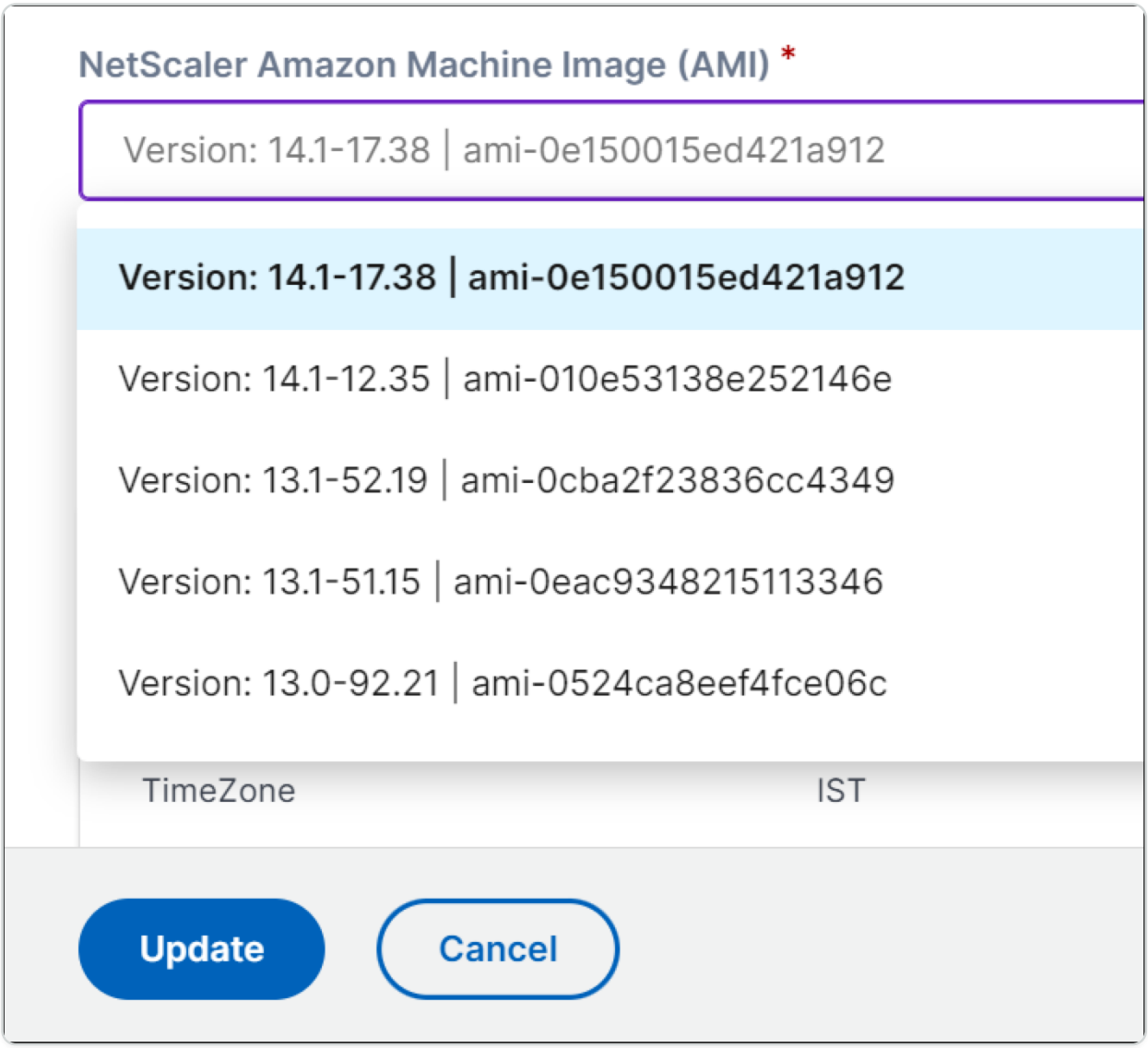
- From the AWS console, disable dynamic scaling for the Autoscale group created for the App Environment.

  Naming convention: `Adc-<App Environment Name>-<Availability Zone>-<random alphanumeric string>`

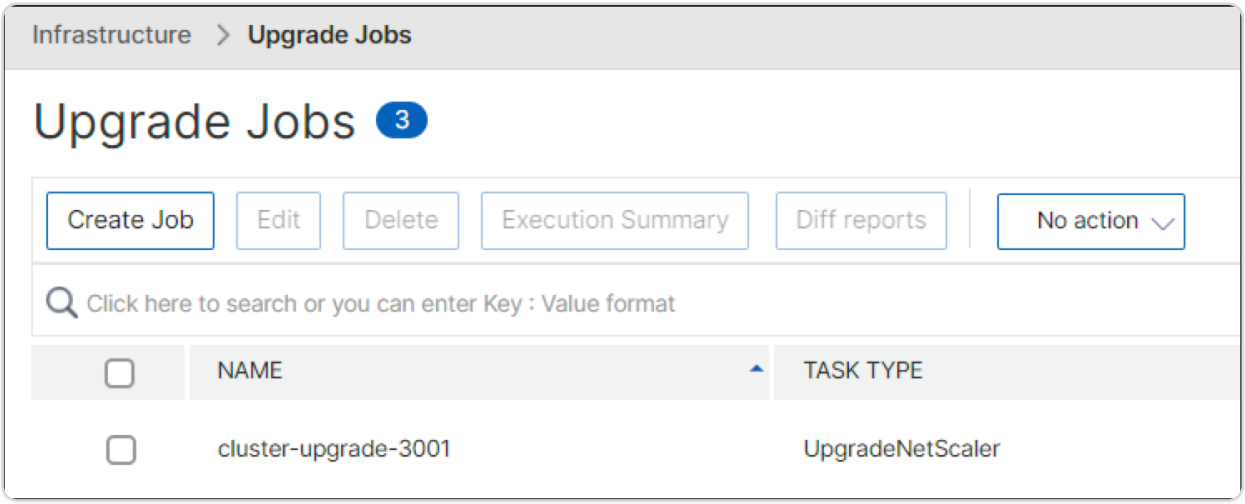


- From the NetScaler Console service, update the AMI details to the ADC version to which the NetScaler is being upgraded to, using the **Edit** option for the App Environment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- From NetScaler Console service, upgrade ADCs using the **Upgrade Job** feature.



- From the AWS Console, re-enable dynamic scaling for the Autoscale group.

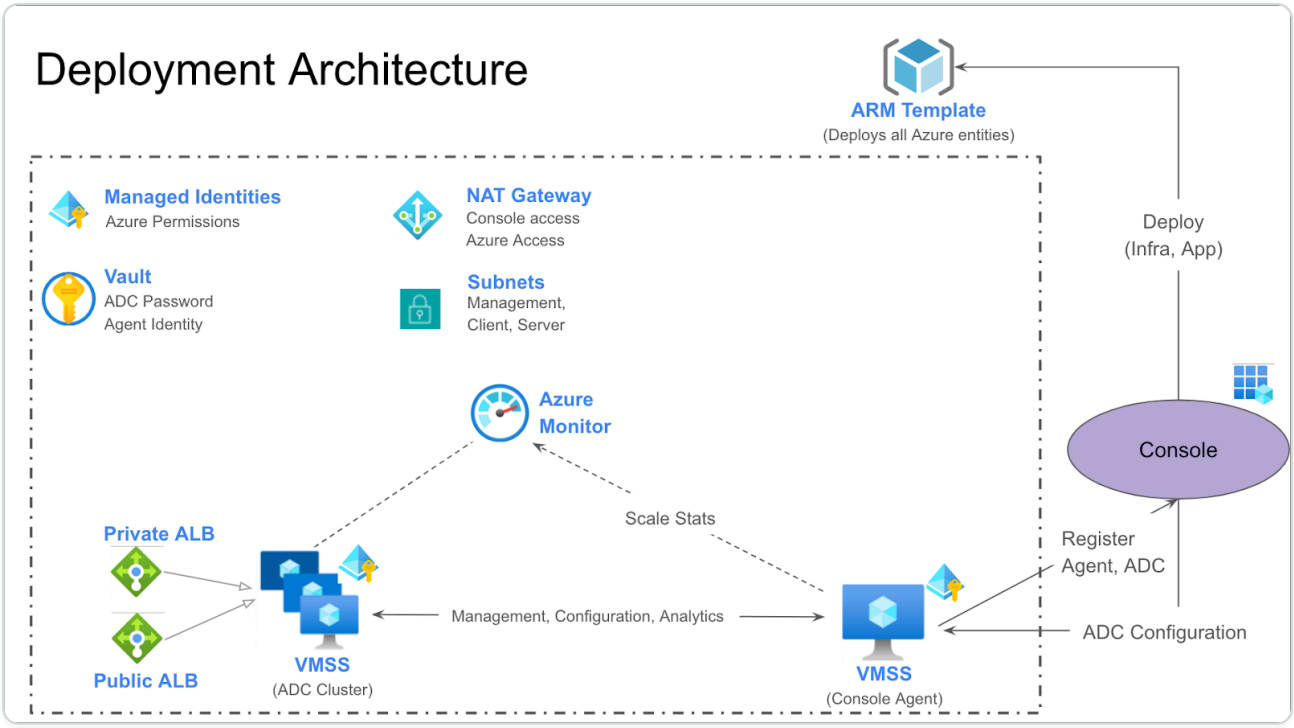
© 1997–2026 Citrix Systems, Inc. All rights reserved.

App-based provisioning in Azure

NetScaler Console service introduces "App based" provisioning, designed to streamline and simplify NetScaler deployments on cloud data centers and deliver applications from them.

NetScaler Console service accepts the customer's cloud credentials and sets up the infrastructure required for application delivery by orchestrating the launching of NetScaler instances, NetScaler Console Agents and the necessary cloud entities in Azure. NetScaler administrators can leverage both Flexed and Cloud Marketplace licenses for their NetScaler instances, ensuring flexibility in licensing options.

Administrators can then deliver applications present in their cloud by defining delivery settings in a straightforward, app centric manner from NetScaler Console service. The service then takes care of configuring both ADCs and Azure infrastructure to deliver their applications. Once the applications are delivered, NetScaler administrators gain access to the rich analytics, and monitoring features of NetScaler Console service to effectively manage and monitor their applications.



Prerequisites

Configure programmatic deployment for the following products in Azure Marketplace:

- NetScaler VPX - Configure programmatic deployment for one of the following variants:
  - NetScaler VPX BYOL - Subscribe if you have purchased flexed licenses and they are available in NetScaler Console service for licensing NetScaler instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - NetScaler VPX Premium - 1 Gbps - Subscribe if you want a subscription based license from the Azure Marketplace.
    - NetScaler Agent Service

- Select a VNet - Select a VNet for setting up the infrastructure for application delivery. The VNet should have a CIDR of /22 or more. During the infrastructure deployment process, dedicated subnets for ADC infrastructure are created consuming /24 address space. Select a VNet from the list based on your deployment:
    - Dedicated VNet that is separate from the applications, if you want your deployment to be similar to a DMZ.
    - Same VNet where the applications are also present.

Cloud access profile

A cloud access profile is used to give permissions of the customer's Azure account to NetScaler Console service. While creating a cloud access profile the administrator must download and run a powershell script in Azure CLI. The script creates Service Principals in the customer's Azure account with owner permissions at the subscription level.

1. Navigate to **Infrastructure > Provisioning > App based > Cloud Access Profiles**.
2. Follow the on-screen directions to create a cloud access profile for your subscription.

NOTE:

To create this profile, the NetScaler administrator must also be the Azure subscription owner.

App environment

App Environment represents the delivery infrastructure set up in a VNet for delivering the applications. When an administrator creates an App Environment in the NetScaler Console service, all the resources for delivering and monitoring applications, including gateways, security groups, subnets, NetScaler instances, and NetScaler Console agents, are deployed as part of an App Environment. See the FAQ section for more information.

1. Navigate to **InfraStructure > Provisioning > App based > Environments**.
2. Follow the on-screen directions to create an App environment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Application delivery

Application delivery is the core component of the App-based provisioning feature and contains the mandatory application delivery and security information. As part of application delivery configuration you define the following entities:

- The endpoint representing how the application is accessed by the clients, such as protocol, port, certificates, and ciphers. For example, an SSL profile of an endpoint represents the set of SSL configurations that includes the supported ciphers and protocols. A predefined A+ SSL profile is available by default.
- The services that represent an application's component, which must be accessed based on the specific HTTP request. For example, a component for an ecommerce application could be an order service, a catalog service, or a payment service that are installed in different application servers and requests must be routed based on the URL accessed. The service profile of an application service represents how the delivery infrastructure can access and monitor the application service, such as load balancing, SSL, and health check settings.
- The content policy that defines how the L7 content is inspected and modified when a request or a response arrives for a specific service. It is used to take a predefined action on the HTTP requests based on headers, URLs, or IP addresses. Some of the actions could be header enrichment, redirecting requests, or dropping requests.

1. Navigate to **InfraStructure > Provisioning > App based > App Delivery**.
2. Follow the on-screen directions to create a new application.

FAQs

What are the entities created by NetScaler Console service for delivering an application in the cloud?

NetScaler Console service creates the following entities in the customer's VNet:

- NetScaler VPX cluster.
  - The VPX instances are deployed as a Virtual Machine Scale Set (VMSS).
  - A single node cluster is created during App Environment creation. This cluster can scale up to a maximum of 10 nodes.
- A NetScaler Console agent.
- Subnets: One subnet each for management, client, and server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Security groups: One security group each for management, client, and server NICs of NetScaler.
  - Management security group: This security group is associated with the management NICs of the NetScaler instances and NetScaler Console agents. It consists of rules to allow communication between NetScaler instances, NetScaler Console agents, and any other control plane traffic.
  - Client security group: This security group is associated with the client NICs of the NetScaler instances and is used to allow the data traffic to the NetScaler virtual servers.
  - Server security group: This security group is associated with the server NICs of the NetScaler instances and does not contain any default rules.
- NAT gateway: A NAT gateway enables NetScaler Console agent to access NetScaler Console service and NetScaler instances to access the internet.
- Azure Key Vault: Store any NetScaler and agent secrets in the vault.

What are the metrics used to Autoscale NetScaler?

The following metrics are used to Autoscale NetScaler:

- The minimum number of instances in the VMSS is 1 and the maximum is 10.
- Scale-Out by 1 capacity unit. That is, cpu_use > 70% or throughput > 70% for 5 consecutive periods of 60 seconds.
- Scale-In by 1 capacity unit. That is, cpu_use =< 30% and throughput =< 30% for 5 consecutive periods of 60 seconds.

How can an administrator identify the resources created by NetScaler Console service in the cloud?

All Azure resources are created with the tag “UsedFor: AppDeliveryByNetScaler” by default. In addition, the resources are tagged using the tags specified during the App Environment creation workflow.

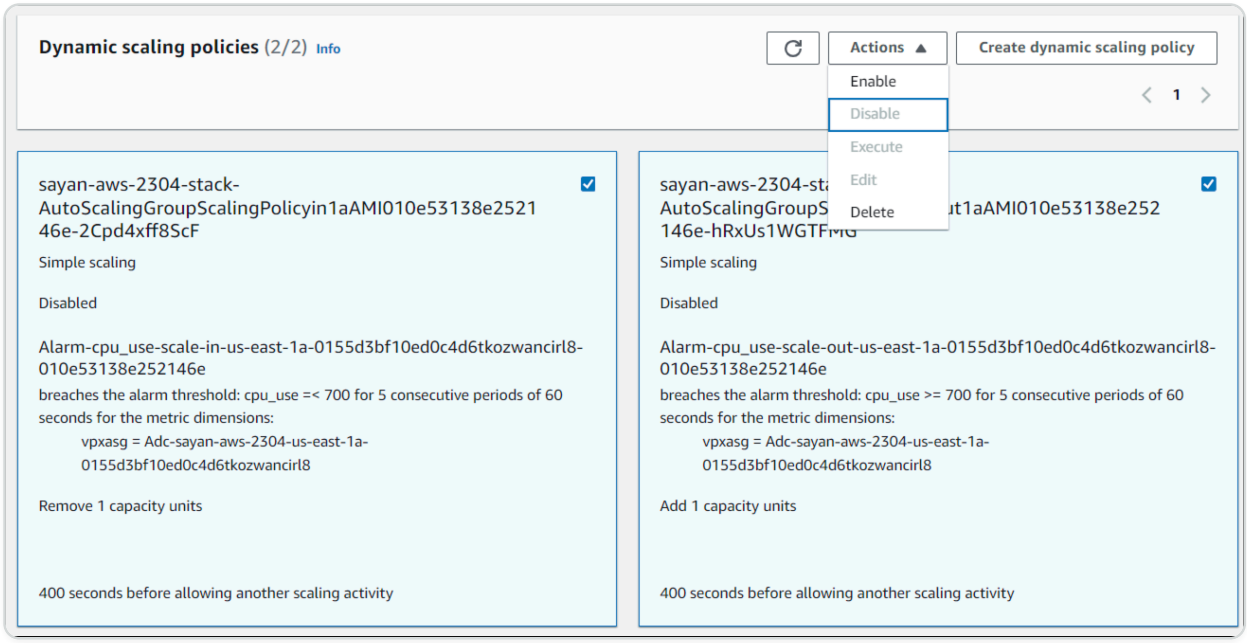
How can a NetScaler administrator upgrade NetScaler in an App Environment?

Perform the following steps to upgrade NetScaler:

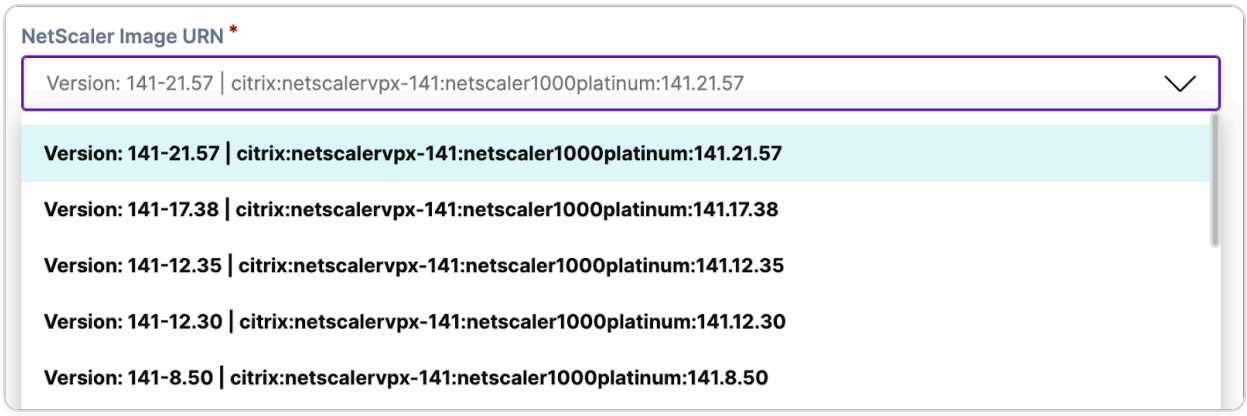
- From the Azure console, disable scaling for the VMSS by setting the scaling policy values to the current number of instances in the VMSS for the App Environment.

  Naming convention: `vmss-adc-<App Environment Name>`

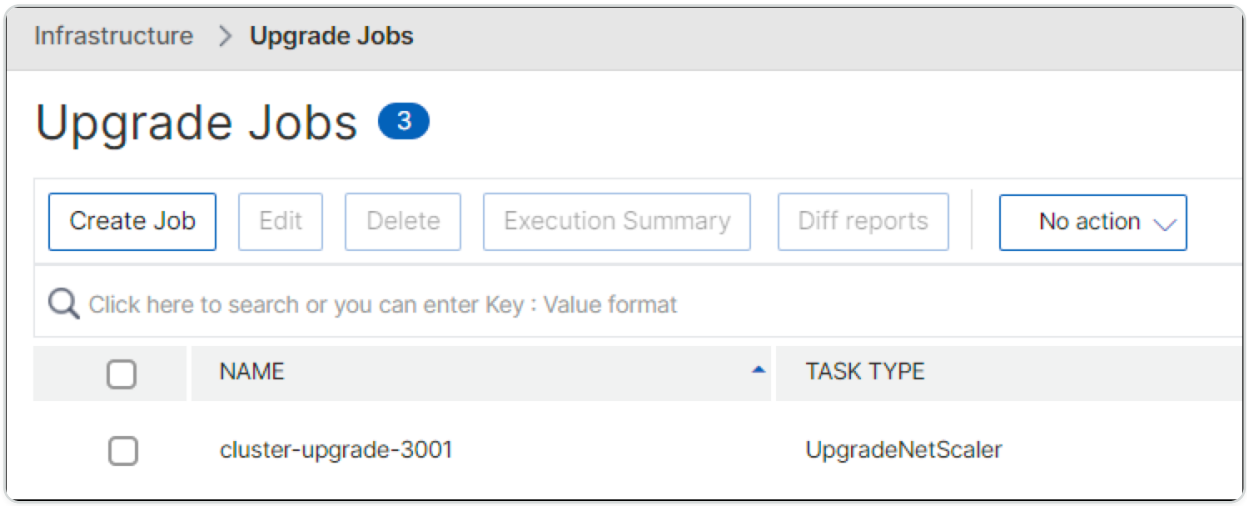
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- From the NetScaler Console service, edit the App Environment and select the version to upgrade to.



- From NetScaler Console service, upgrade ADCs to the version selected in the pervious step by using the **Upgrade Job** feature.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

- From the Azure Console, re-enable dynamic scaling for the VMSS. The instance limit must be set to the initial values. That is, minimum=1, maximum=10, default=1.

Provisioning NetScaler VPX instances

You can use NetScaler Console to automate the deployment, setup, and management of NetScaler VPX instances across public cloud and virtualization platforms. Provisioning NetScaler VPX instances using NetScaler Console combines the elasticity and flexibility of the cloud with the optimization, security, and control features of NetScaler.

With NetScaler Console monitoring your NetScaler instances, you gain visibility into the health, performance, and security of your applications, and you can manage your application delivery infrastructure across hybrid and multi-cloud environments.

You can provision NetScaler VPX instances on the following platforms:

- AWS
- Microsoft Azure
- Google Cloud
- VMware vCenter

Provisioning NetScaler VPX Instances on AWS

When you move your applications to the cloud, the components that are part of your application increase, become more distributed, and need to be dynamically managed.

With NetScaler VPX instances on AWS, you can seamlessly extend your L4-L7 network stack to AWS. With NetScaler VPX, AWS becomes a natural extension of your on-premises IT infrastructure. You can use NetScaler VPX on AWS to combine the elasticity and flexibility of the cloud, with the same optimization, security, and control features that support the most demanding websites and applications in the world.

With NetScaler Console monitoring your NetScaler instances, you gain visibility into the health, performance, and security of your applications. You can automate the setup, deployment, and management of your application delivery infrastructure across hybrid multi-cloud environments.

AWS terminology

The following section provides a brief description of the AWS terms used in this document:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TERM	DEFINITION
Amazon Machine Image (AMI)	A machine image, which provides the information required to launch an instance, which is a virtual server in the cloud.
Elastic Compute Cloud (EC2)	A web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers.
Elastic network interface (ENI)	A virtual network interface that you can attach to an instance in a VPC.
Instance type	Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instance types comprise varying combinations of CPU, memory, storage, and networking capacity and give you the flexibility to choose the appropriate mix of resources for your applications.
Identity and Access Management (IAM) role	An AWS identity with permission policies that determine what the identity can and cannot do in AWS. You can use an IAM role to enable applications running on an EC2 instance to securely access your AWS resources.
Security groups	A named set of allowed inbound network connections for an instance.
Subnets	A segment of the IP address range of a VPC that EC2 instances can be attached to. You can create subnets to group instances according to security and operational needs.

Prerequisites

This document assumes the following:

- You possess an AWS account.
- You have created the required VPC and selected the availability zones.
- You have added the agent in AWS.

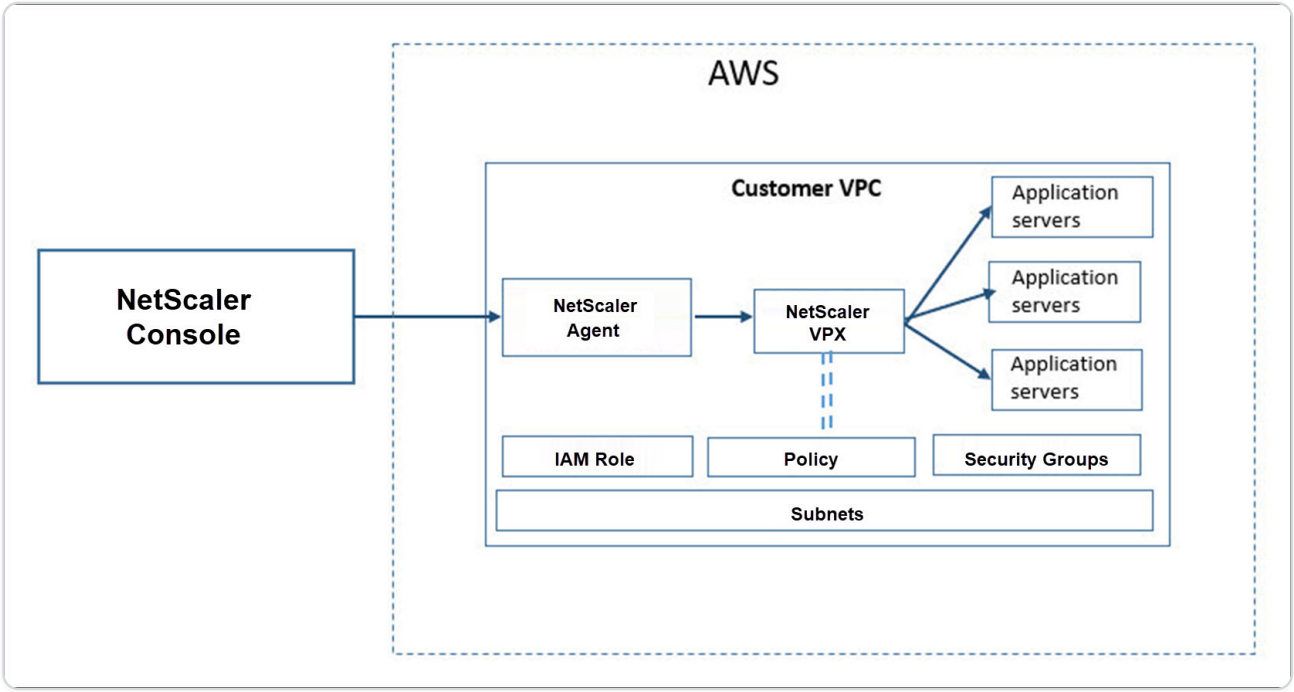
© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information on how to create an account and other tasks, see AWS Documentation.

For more information on how to install an agent on AWS, see Install a NetScaler agent on AWS.

Architecture Diagram

The following image provides an overview of how NetScaler Console connects with AWS to provision NetScaler VPX instances in AWS.



Configuration tasks

Perform the following tasks on AWS before you provision NetScaler VPX instances in NetScaler Console:

- Create subnets
- Create security groups
- Create an IAM role and define a policy

Perform the following tasks on NetScaler Console to provision the instances on AWS:

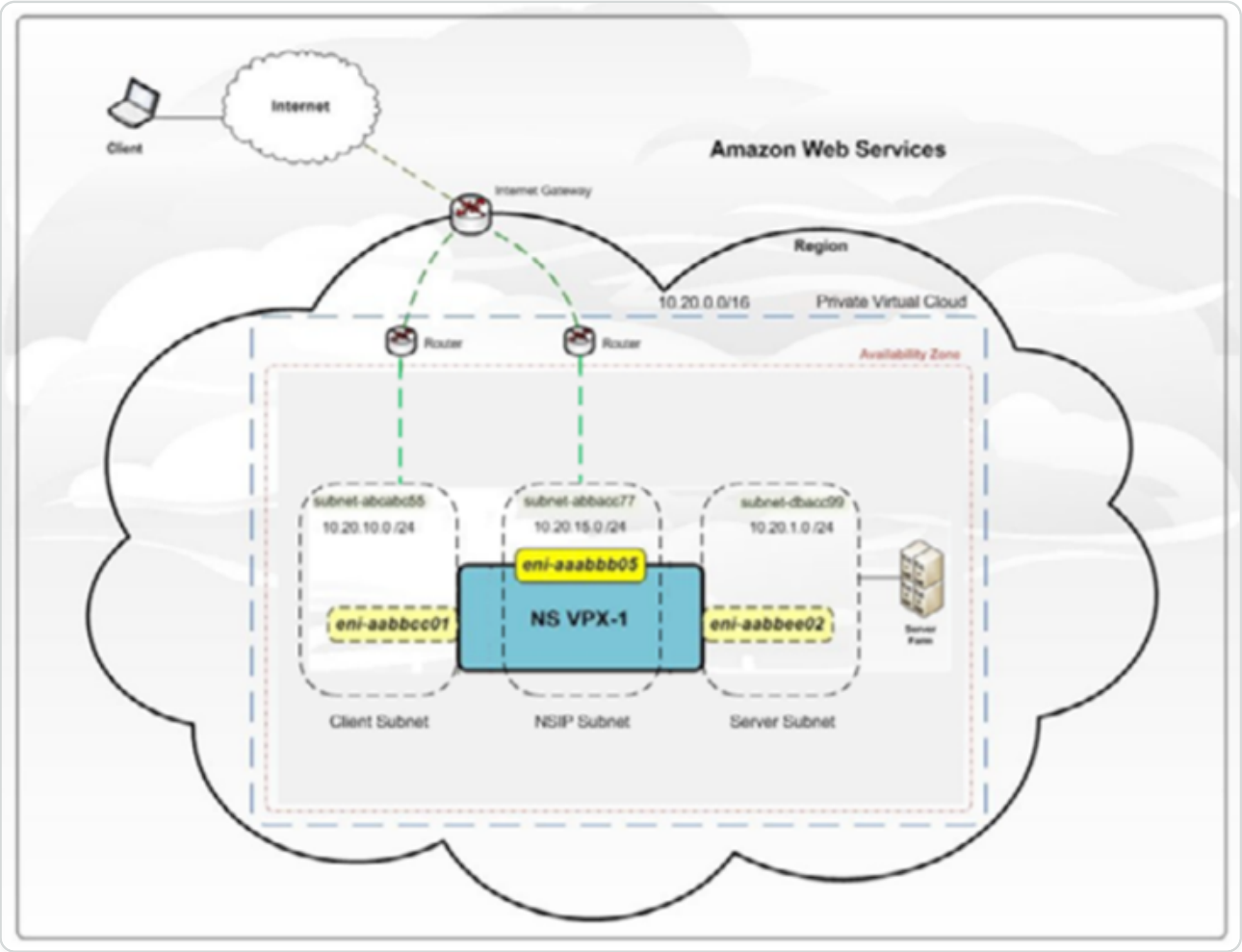
- Create site
- Provision NetScaler VPX instance on AWS

TO CREATE SUBNETS

Create three subnets in your VPC. The three subnets that are required to provision NetScaler VPX instances in your VPC - are management, client, and server. Specify an IPv4 CIDR block from the range that is defined in your VPC for each of the subnets. Specify the availability zone in which you

© 1997–2026 Citrix Systems, Inc. All rights reserved.

want the subnet to reside. Create all the three subnets in the same availability zone. The following image illustrates the three subnets created in your region and their connectivity to the client system.



For more information on VPC and subnets, see VPCs and Subnets.

TO CREATE SECURITY GROUPS

Create a security group to control inbound and outbound traffic in the NetScaler VPX instance. A security group acts as a virtual firewall for your instance. Create security groups at the instance level, and not at the subnet level. It is possible to assign each instance in a subnet in your VPC to a different set of security groups. Add rules for each security group to control the inbound traffic that is passing through the client subnet to instances. You can also add a separate set of rules that control the outbound traffic that passes through the server subnet to the application servers. Although you can use the default security group for your instances, you might want to create your groups. Create three security groups - one for each subnet. Create rules for both incoming and outgoing traffic that you want to control. You can add as many rules as you want.

For more information on security groups, see Security Groups for your VPC.

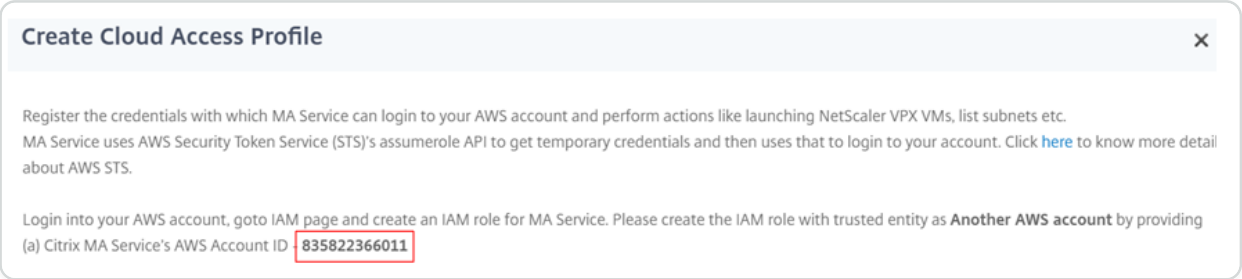
© 1997–2026 Citrix Systems, Inc. All rights reserved.

TO CREATE AN IAM ROLE AND DEFINE A POLICY

Create an IAM role so that you can establish a trust relationship between your users and the Citrix trusted AWS account and create a policy with Citrix permissions.

1. In AWS, click **Services**. In the left side navigation pane, select **IAM > Roles**, and click **Create role**.
2. You are connecting your AWS account with the AWS account in NetScaler Console. So, select **Another AWS account** to allow NetScaler Console to perform actions in your AWS account.

   Type in the 12-digit NetScaler Console AWS account ID. The Citrix ID is 835822366011. You can also find the Citrix ID in NetScaler Console when you create the cloud access profile.

3. Enable **Require external ID** to connect to a third-party account. You can increase the security of your role by requiring an optional external identifier. Type an ID that can be a combination of any characters.
4. Click **Permissions**.
5. In the **Attach permissions policies** page, click **Create policy**.
6. You can create and edit a policy in the visual editor or by using JSON.

   The list of permissions from Citrix is provided in the following box:

```
{

"Version": "2012-10-17",

"Statement":

[

    {

         "Effect": "Allow",

        "Action": [
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "ec2:DescribeInstances",
            "ec2:DescribeImageAttribute",
            "ec2:DescribeInstanceAttribute",
            "ec2:DescribeRegions",
            "ec2:DescribeDhcpOptions",
            "ec2:DescribeSecurityGroups",
            "ec2:DescribeHosts",
            "ec2:DescribeImages",
            "ec2:DescribeVpcs",
            "ec2:DescribeSubnets",
            "ec2:DescribeNetworkInterfaces",
            "ec2:DescribeAvailabilityZones",
            "ec2:DescribeNetworkInterfaceAttribute",
            "ec2:DescribeInstanceStatus",
            "ec2:DescribeAddresses",
            "ec2:DescribeKeyPairs",
            "ec2:DescribeTags",
            "ec2:DescribeVolumeStatus",
            "ec2:DescribeVolumes",
            "ec2:DescribeVolumeAttribute",
            "ec2:CreateTags",
            "ec2:DeleteTags",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "ec2:CreateKeyPair",
            "ec2:DeleteKeyPair",
            "ec2:ResetInstanceAttribute",
            "ec2:RunScheduledInstances",
            "ec2:ReportInstanceStatus",
            "ec2:StartInstances",
            "ec2:RunInstances",
            "ec2:StopInstances",
            "ec2:UnmonitorInstances",
            "ec2:MonitorInstances",
            "ec2:RebootInstances",
            "ec2:TerminateInstances",
            "ec2:ModifyInstanceAttribute",
            "ec2:AssignPrivateIpAddresses",
            "ec2:UnassignPrivateIpAddresses",
            "ec2:CreateNetworkInterface",
            "ec2:AttachNetworkInterface",
            "ec2:DetachNetworkInterface",
            "ec2:DeleteNetworkInterface",
            "ec2:ResetNetworkInterfaceAttribute",
            "ec2:ModifyNetworkInterfaceAttribute",
            "ec2:AssociateAddress",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "ec2:AllocateAddress",
            "ec2:ReleaseAddress",
            "ec2:DisassociateAddress",
            "ec2:GetConsoleOutput"
        ],
            "Resource": "*"
    }
]
}
```

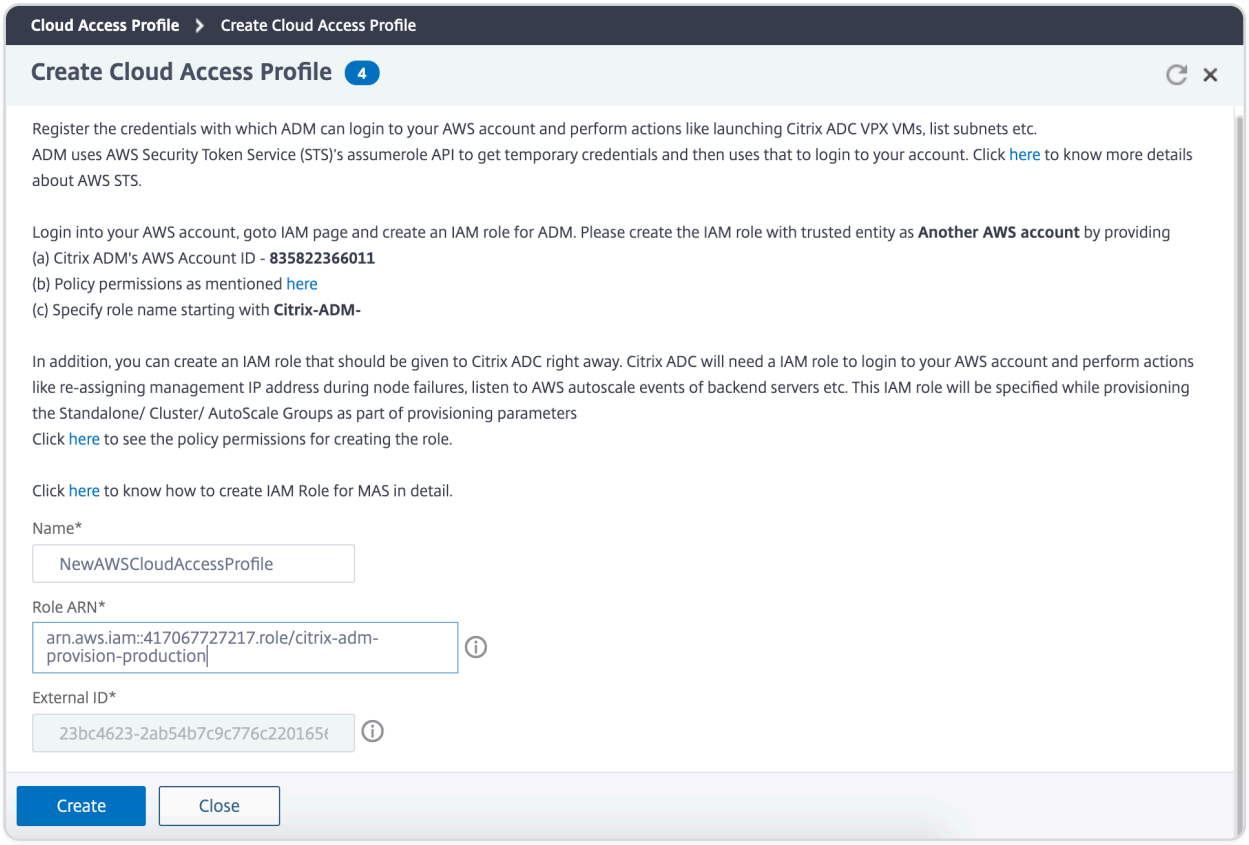
7. Copy and paste the list of permissions in the JSON tab and click **Review policy**.
8. In **Review policy** page, type a name for the policy, enter a description, and click **Create policy**.

TO CREATE A SITE IN NETSCALER CONSOLE

Create a site in NetScaler Console and add the details of the VPC associated with your AWS role.

1. In NetScaler Console, navigate to **Infrastructure > Sites**.
2. Click **Add**.
3. Select the service type as AWS and enable **Use existing VPC as a site**.
4. Select the cloud access profile.
5. If the cloud access profile doesn't exist in the field, click **Add** to create a profile.
    a. In the **Create Cloud Access Profile** page, type the name of the profile with which you want to access AWS.
    b. Type the ARN associated with the role that you have created in AWS.
    c. Type the external ID that you provided while creating an Identity and Access Management (IAM) role in AWS. See step 4 in To create an IAM role and define a policy task. Ensure that the IAM role name that you specified in AWS starts with "Citrix-ADM-" and it correctly appears in the Role ARN.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The details of the VPC, such as the region, VPC ID, name and CIDR block, associated with your IAM role in AWS are imported in NetScaler Console.

6. Type a name for the site.
7. Click **Create**.

TO PROVISION NETSCALER VPX ON AWS

Use the site that you have created earlier to provision the NetScaler VPX instances on AWS. Provide the agent details to provision those instances that are bound to that agent.

1. In NetScaler Console, navigate to **Infrastructure > Instances > NetScaler**.
2. In the **VPX** tab, click **Provision**.

   This option displays the **Provision NetScaler VPX on Cloud** page.
3. Select **Amazon Web Services (AWS)** and click **Next**.
4. In the **Basic Parameters** tab,

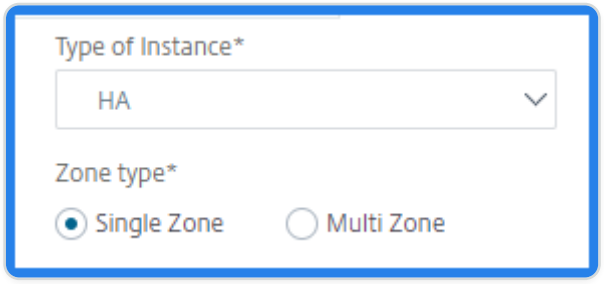
   a. Select the **Type of Instance** from the list.

   - **Standalone:** This option provisions a standalone NetScaler VPX instance on AWS.
   - **HA:** This option provisions the high availability NetScaler VPX instances on AWS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To provision the NetScaler VPX instances in the same zone, select the **Single Zone** option under **Zone Type**.

To provision the NetScaler VPX instances across multiple zones, select the **Multi Zone** option under **Zone type**. In the **Provision Parameters** tab, make sure to specify the network details for each zone that are created on AWS.



b. Specify the name of an NetScaler VPX instance.

c. In **Site**, select the site that you created earlier.

d. In **Agent**, select the agent that is created to manage the NetScaler VPX instance.

e. In **Cloud Access Profile**, select the cloud access profile created during site creation.

f. In **Device Profile**, select the profile to provide authentication.

NetScaler Console uses the device profile when it requires to log on to the NetScaler VPX instance.

g. Click **Next**.

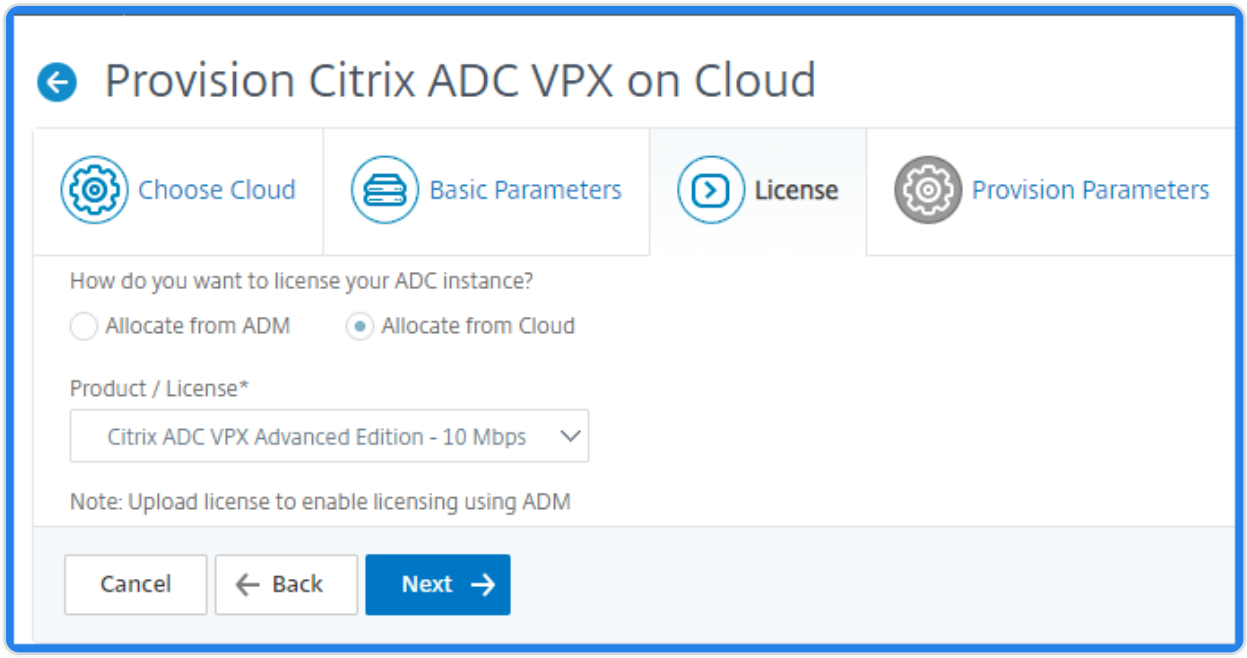
5. In the **License** tab, Select one of the following modes to apply license to a NetScaler instance:

- **Using NetScaler Console**: The instance that you want to provision checks out the licenses from the NetScaler Console.
- **Using the AWS Cloud**: The **Allocate from Cloud** option uses the NetScaler® product licenses available in the AWS marketplace. The instance that you want to provision uses the licenses from the marketplace.

If you choose to use licenses from the AWS marketplace, specify the product or license in the **Provision Parameters** tab.

For more information, see Licensing Requirements.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. In the **License** tab if you select the **Allocate from NetScaler Console**, specify the following:

   - License Type - Select either bandwidth or virtual CPU licenses:

     Bandwidth Licenses: You can select one of the following options from the **Bandwidth License Types** list:

     - **Pooled Capacity:** Specify the capacity to allocate to an instance.

       From the common pool, the NetScaler instance checks out one instance license and only as much bandwidth is specified.

     - **VPX Licenses:** When a NetScaler VPX instance is provisioned, the instance checks out the license from the NetScaler Console.

     Virtual CPU Licenses: The provisioned NetScaler VPX instance checks out licenses depending on the number of CPUs running in the instance.

     NOTE

     When the provisioned instances are removed or destroyed, the applied licenses return to the NetScaler Console license pool. These licenses can be reused to provision new instances.

   a. In **License Edition**, select the license edition. The NetScaler Console uses the specified edition to provision instances.

7. Click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. In the **Provision Parameters** tab,

    a. Select the **Citrix IAM Role** created in AWS. An IAM role is an AWS identity with permission policies that determine what the identity can and cannot do in AWS.

    b. In the **Product** field, select the NetScaler product version that you want to provision.

    c. Select the EC2 instance type from the **Instance Type** list.

    This list displays the supported AMI instance types for the selected NetScaler instance.

    d. Select the **Version** of NetScaler that you want to provision. Select both **Major** and **Minor** version of NetScaler.

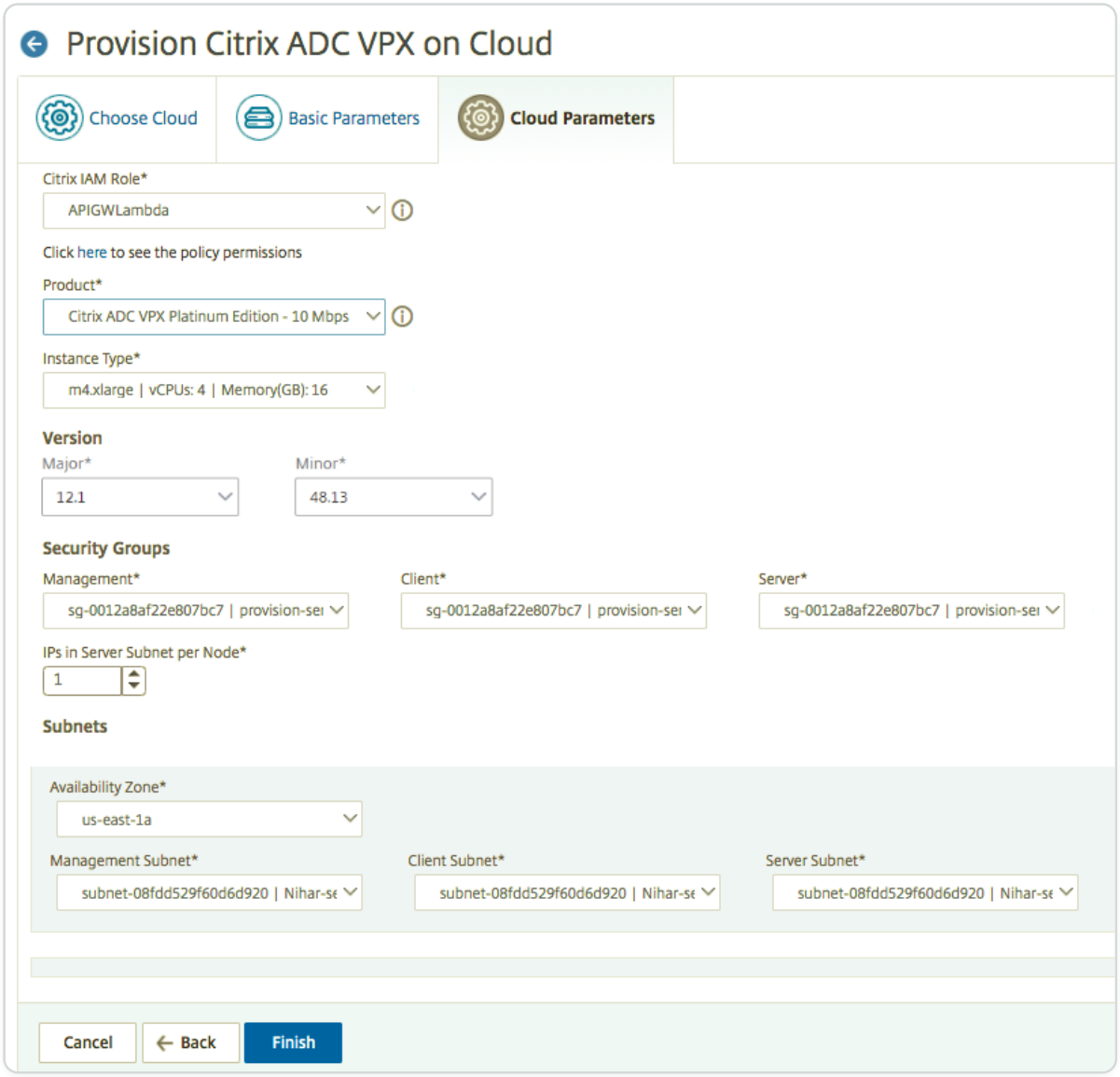
    e. In **Security Groups**, select the Management, Client, and Server security groups that you have created in your virtual network.

    f. In **IPs in server Subnet per Node**, select the number of IP addresses in server subnet per node for the security group.

    g. In **Subnets**, select the Management, Client, and Server subnets for each zone that are created in AWS. You can also select the region from the **Availability Zone** list.

    h. Click **Finish**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The NetScaler VPX instance is now provisioned on AWS.

NOTE

Currently, NetScaler Console doesn't support deprovisioning of NetScaler instances from AWS.

TO VIEW THE NETSCALER VPX PROVISIONED IN AWS

1. From the AWS home page, navigate to **Services** and click **EC2**.
2. On the **Resources** page, click **Running Instances**.
3. You can view the NetScaler VPX provisioned in AWS.

The name of the NetScaler VPX instance is the same that you provided while provisioning an instance in the NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TO VIEW THE NETSCALER VPX PROVISIONED IN NETSCALER CONSOLE

1. In NetScaler Console, navigate to **Infrastructure > Instances > NetScaler**.
2. Select **NetScaler VPX** tab.
3. The NetScaler VPX instance provisioned in AWS is listed here.

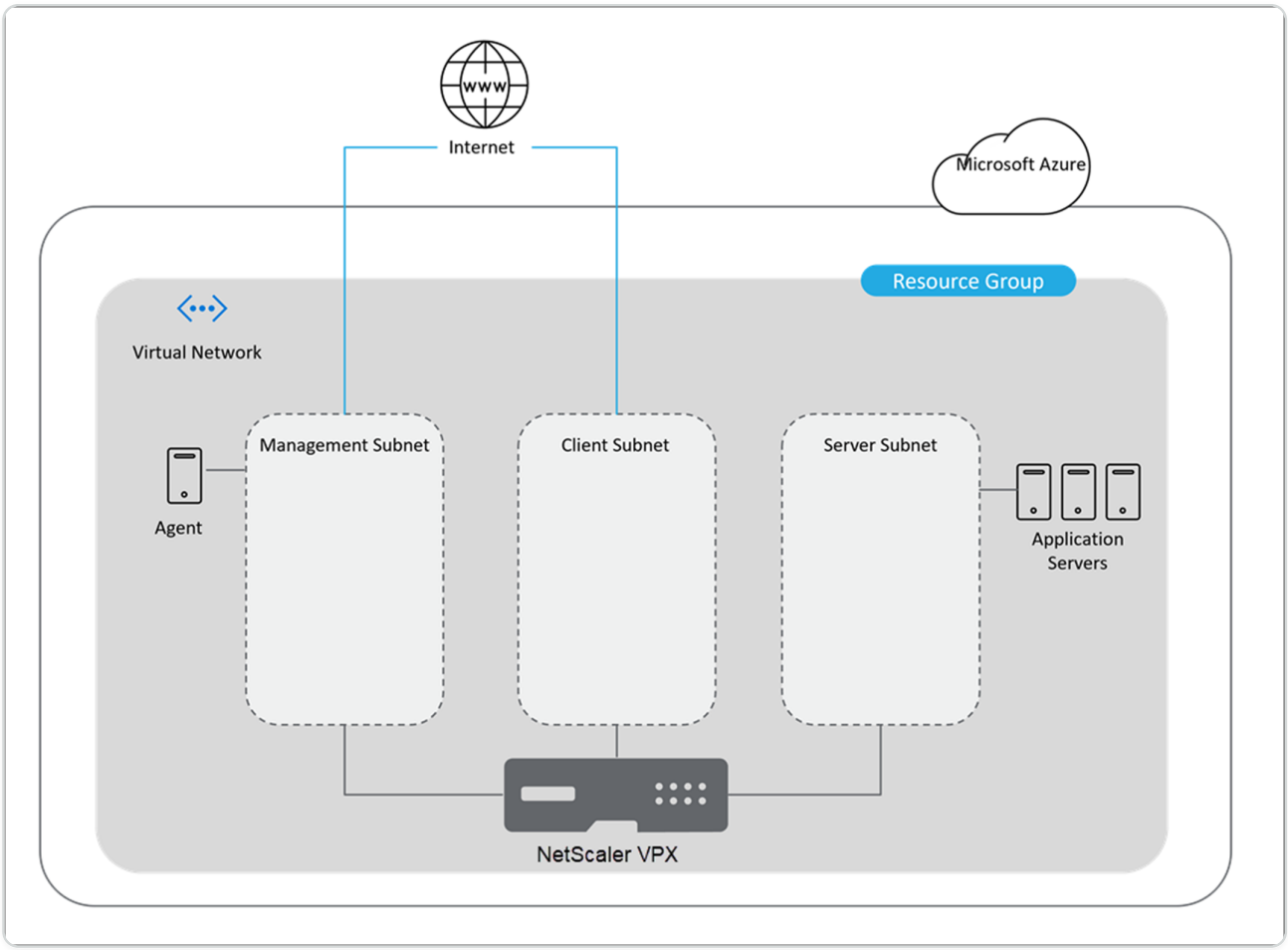
Provisioning NetScaler VPX instances on Microsoft Azure

Applications or services hosted on Azure require secure traffic management and efficient optimization of network resources along with cloud benefits. NetScaler VPX instances provisioned on Microsoft Azure provide secure traffic management, optimized resource consumption, and reduced web application ownership costs.

NetScaler Console allows you to automate the deployment, setup, and management of the NetScaler VPX instances on Azure. Provisioning NetScaler VPX instances using NetScaler Console combines the elasticity and flexibility of cloud with the control features of NetScaler.

NetScaler Console Deployment Architecture

The following image provides an overview of how NetScaler Console connects with Azure to provision NetScaler VPX instances in Microsoft Azure.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

You require to have three subnets to provision and manage the NetScaler VPX instance in Microsoft Azure. A security group must be created for each subnet. The rules specified in the NetScaler Gateway govern the communication across the subnets.

The agent helps you to provision and manage the NetScaler VPX instance.

Prerequisites

This section describes the prerequisites that you must complete in Microsoft Azure and NetScaler Console before you provision NetScaler VPX instances.

This document assumes the following:

- You possess a Microsoft Azure account that supports the Azure Resource Manager deployment model.
- You have a resource group in Microsoft Azure.

For more information on how to create an account and other tasks, see Microsoft Azure Documentation.

SET UP MICROSOFT AZURE COMPONENTS

Perform the following tasks in Azure before you provision NetScaler VPX instances in NetScaler Console.

1. Create a virtual network.
2. Create security groups.
3. Create subnets.
4. Subscribe to NetScaler VPX license in Microsoft Azure.
5. Create and register an application.
6. Set up an agent.

Create a virtual network

1. Log on to your Microsoft Azure portal.
2. Select **Create a resource**.
3. Select **Networking** and click **Virtual Network**.
4. Specify the required parameters.
    - In **Resource group**, you must specify the resource group where you want to deploy the NetScaler VPX product.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- In **Location**, you must specify the locations that support availability zones such as:
  - Central US
  - East US2
  - France Central
  - North Europe
  - Southeast Asia
  - West Europe
  - West US2

NOTE

The application servers present in this resource group.

5. Click **Create**.

For more information, see Azure Virtual Network in Microsoft Documentation.

Create security groups

Create three security groups in your virtual network (VNet) - one each for the management, client, and server connections. Create a security group to control inbound and outbound traffic in the NetScaler VPX instance. You can add as many rules as you want.

- **Management:** A security group in your account dedicated for the management of NetScaler VPX. NetScaler has to contact Azure services and requires internet access. Inbound rules are allowed on the following TCP and UDP ports.
  - TCP: 80, 22, 443, 3008–3011, 4001
  - UDP: 67, 123, 161, 500, 3003, 4500, 7000

NOTE

Ensure that the security group allows the agent to access the VPX.

- **Client:** A security group in your account dedicated for client-side communication of NetScaler VPX instances. Typically, inbound rules are allowed on the TCP ports 80, 22, and 443.
- **Server:** A security group in your account dedicated for server-side communication of NetScaler VPX.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information on how to create a security group in Microsoft Azure, see Create, change, or delete a network security group.

Create subnets

Create three subnets in your virtual network (VNet) - one each for the management, client, and server connections. Specify an address range that is defined in your VNet for each of the subnets. Specify the availability zone in which you want the subnet to reside.

- **Management:** A subnet in your Virtual Network (VNet) dedicated for management. NetScaler has to contact Azure services and requires internet access.
- **Client:** A subnet in your Virtual Network (VNet) dedicated for the client side. Typically, NetScaler receives client traffic for the application via a public subnet from the internet.
- **Server:** A subnet where the application servers are provisioned. All your application servers are present in this subnet and receives application traffic from the NetScaler through this subnet.

NOTE

Specify an appropriate security group to the subnet while creating a subnet.

For more information on how to create a subnet in Microsoft Azure, see Add, change, or delete a virtual network subnet.

Subscribe to the NetScaler VPX license in Microsoft Azure

1. Log on to your Microsoft Azure portal.
2. Select **Create a resource**.
3. In the **Search the marketplace** bar, search `NetScaler` and select the required product version.
4. In the **Select a software plan** list, select one of the following license types:
    - Bring your own license
    - Advanced
    - Premium

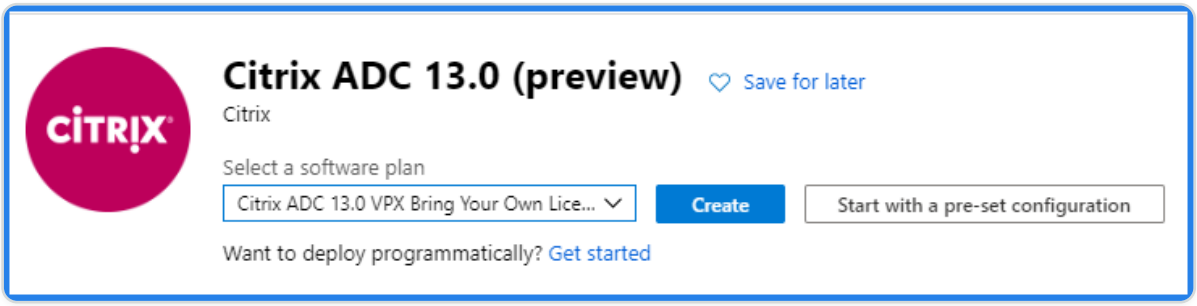
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

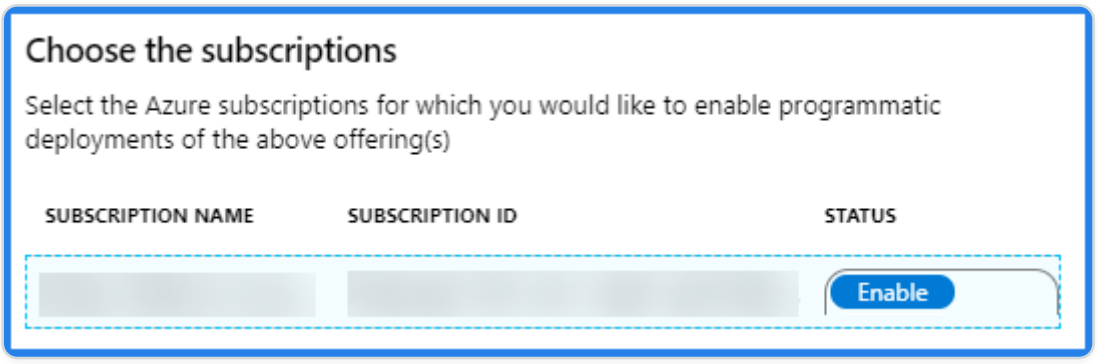
- If you choose the **Bring your own license** option, the instance that you want to provision checks out the licenses from the NetScaler Console while provisioning NetScaler instances.
- In NetScaler Console, the **Advanced** and **Premium** are the equivalent license types for **Enterprise** and **Platinum** respectively.

5. Ensure the programmatic deployment is enabled for the selected NetScaler product.

   a. Beside **Want to deploy programmatically?**, click **Get Started**.



   b. In **Choose the subscriptions**, select **Enable** to deploy the selected NetScaler VPX edition programmatically.



IMPORTANT

Enabling the programmatic deployment is required to provision NetScaler VPX instances in Azure.

   c. Click **Save**.

   d. Close **Configure Programmatic Deployment**.

6. Click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create and register an application

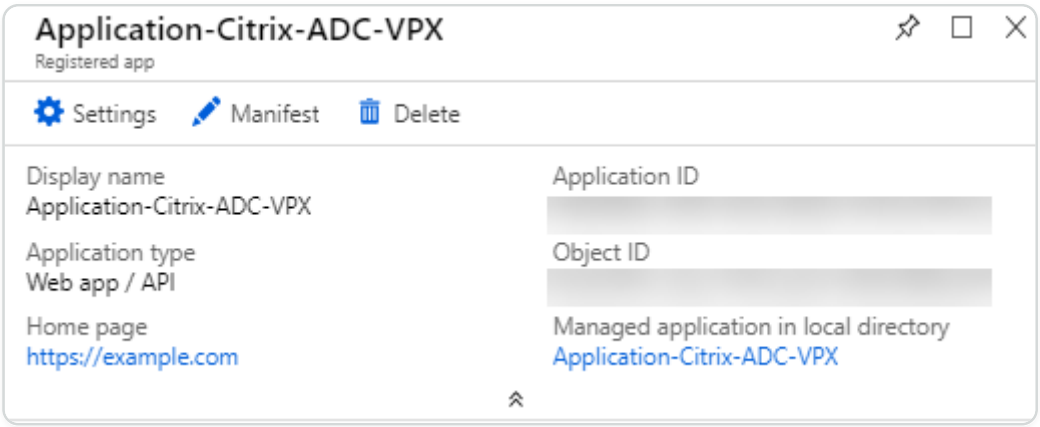
NetScaler Console uses this application to provision NetScaler VPX instances in Azure.

To create and register an application in Azure:

1. In Azure portal, select **Azure Active Directory**. This option displays your organization's directory.
2. Select **App registrations**:
    a. In **Name**, specify the name of the application.
    b. Select the **Application type** from the list.
    c. In the **Sign-on** URL, specify the application URL to access the application.
3. Click **Create**.

For more information on App registrations, see Microsoft Documentation.

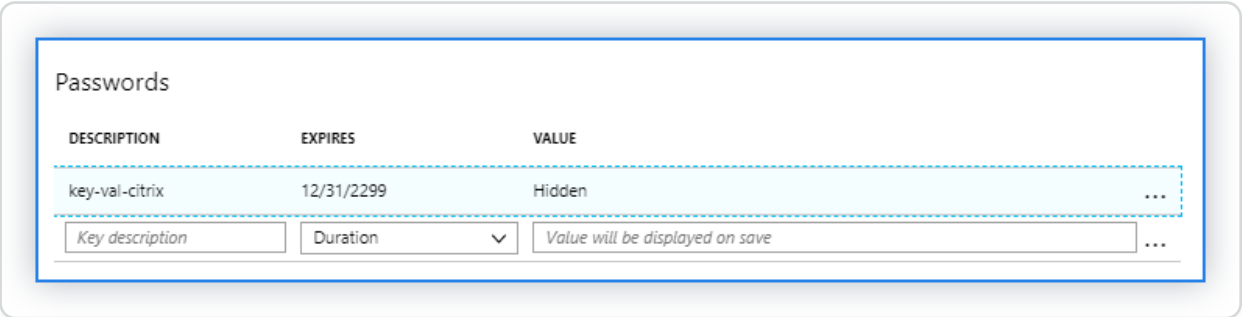
Azure assigns an application ID to the application. The following is an example application registered in Microsoft Azure:



Copy the following IDs and provide these IDs when you are configuring a Cloud Access Profile in NetScaler Console:

- **Application ID:** For steps to retrieve the application or client ID.
- **Directory ID:** For steps to retrieve the directory or tenant or object ID.
- **Key:** For steps to retrieve the key value or client secrets ID.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Subscription ID:** Copy the subscription ID from your storage account.

For more information, see Microsoft Documentation.

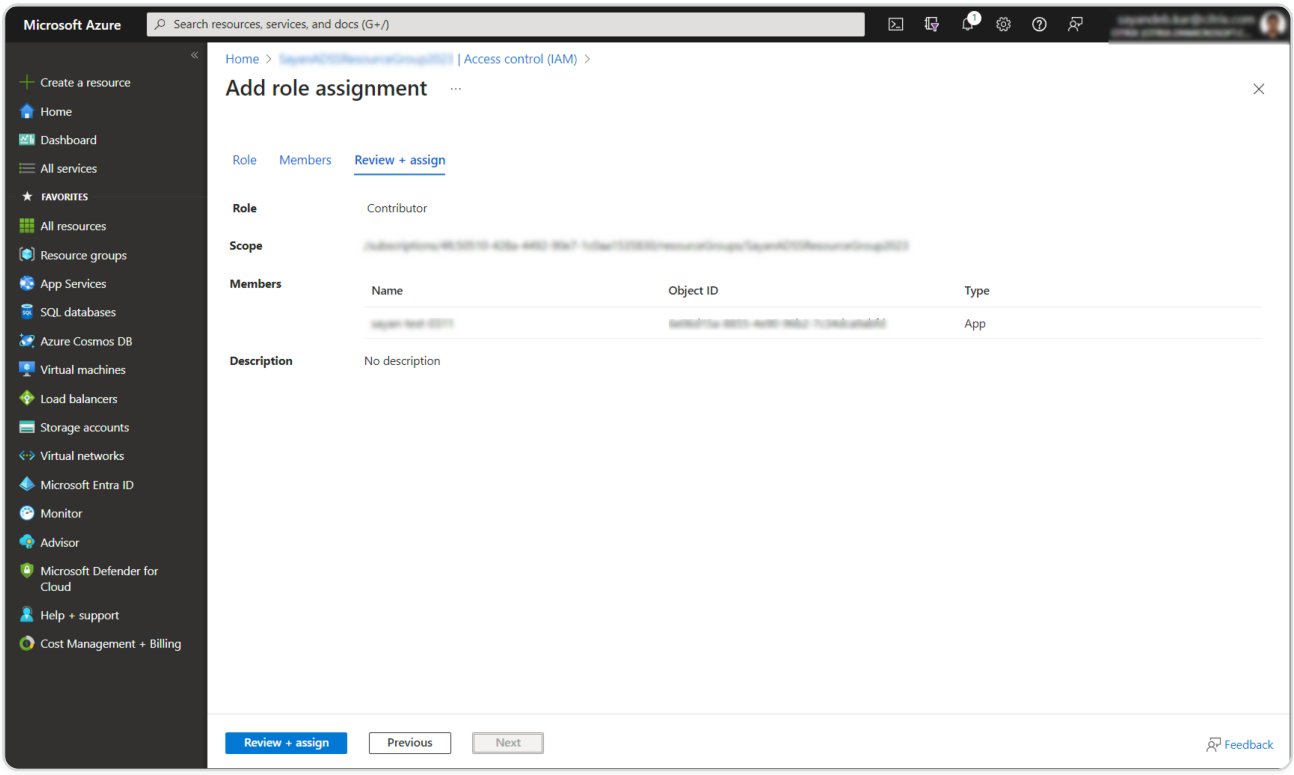
Assign the role permission to an application

NetScaler Console uses the application-as-a-service principle to provision NetScaler instances in Microsoft Azure. This permission is applicable only to the selected resource group.

To assign a role permission to your registered application, you have to be the owner of the Microsoft Azure subscription.

1. In the Azure portal, select **Resource groups**.
2. Select the resource group to which you want to assign role permission.
3. Select **Access control (IAM)**.
4. In **Role assignments**, click **Add**.
5. Select **Owner** from the **Role** list.
6. Select the application that is registered for provisioning NetScaler instances. See, Create, and register an application.
7. Click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Set up a NetScaler agent

Install an agent in the management subnet. This agent works as an intermediary between the NetScaler Console and the managed instances in Microsoft Azure. For more information on how to install an agent on Microsoft Azure, see Install a NetScaler agent on the Microsoft Azure cloud.

SET UP NETSCALER CONSOLE COMPONENTS

Perform the following tasks in Azure before you provision NetScaler VPX instances in NetScaler Console:

1. Create a site.
2. Attach the site to a Citrix service agent.

Create a site in NetScaler Console

Create a site in NetScaler Console and add the VNet details associated with your Microsoft Azure resource group.

1. In NetScaler Console, navigate to **Infrastructure > Instances > Sites** .
2. Click **Add**.
3. In the **Select Cloud** pane,
    a. Select **Data Center** as a **Site type**.
    b. Choose **Azure** from the **Type** list.
    c. Check the **Fetch VNet from Azure** check box.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This option helps you to retrieve the existing VNet information from your Microsoft Azure account.

d. Click **Next**.

4. In the **Choose Region** pane,

   a. In **Cloud Access Profile**, select the profile created for your Microsoft Azure account. If there are no profiles, create a profile.

   b. To create a cloud access profile, click **Add**.

   c. In **Name**, specify a name to identify your Azure account in NetScaler Console.

   d. In **Tenant Active Directory ID / Tenant ID**, specify the Active Directory ID of the tenant or the account in Microsoft Azure.

   e. Specify the **Subscription ID**.

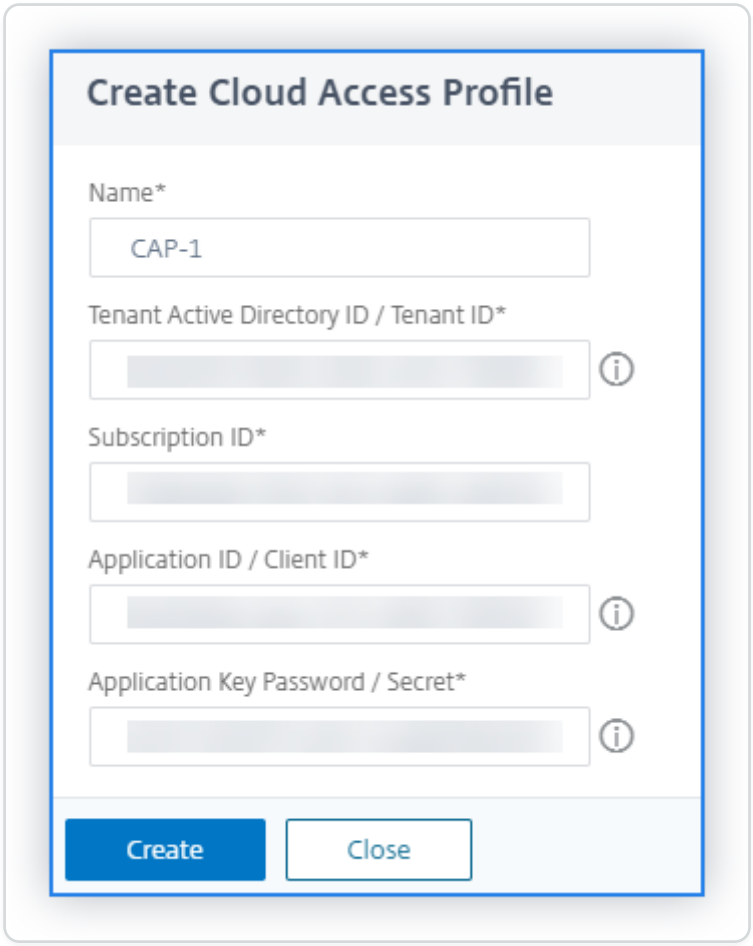
   f. Specify the **Application ID/Client ID**.

   g. Specify the **Application Key Password / Secret**.

   h. Click **Create**.

   For more information, see Create and register an application and Mapping Cloud access profile to the Azure application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



i. In **VNet**, select the virtual network containing NetScaler VPX instances that you want to manage.

j. Specify a **Site Name**.

k. Click **Finish**.

Mapping cloud access profile to Azure application

NETSCALER CONSOLE TERM	MICROSOFT AZURE TERM
Tenant Active Directory ID / Tenant ID	Directory ID
Subscription ID	Subscription ID
Application ID/Client ID	Application ID
Application Key Password / Secret	Keys or Certificates or Client Secrets

Attach the site to an agent

1. In NetScaler Console, navigate to **Infrastructure > Instances > Agents**.
2. Select the agent for which you want to attach a site.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Click **Attach Site**.
4. Select the site from the list that you want to attach.
5. Click **Save**.

Configuration tasks

Use the site that you have associated with your Microsoft Azure resource group to provision the NetScaler VPX instances. Provide the agent details to provision those instances that are bound to that agent.

1. In NetScaler Console, navigate to **Infrastructure > Instances > NetScaler**.
2. In the **VPX** tab, click **Provision**.

   This option displays the **Provision NetScaler VPX on Cloud** page.
3. Select **Microsoft Azure** and click **Next**. Specify the required parameters to provision an instance.

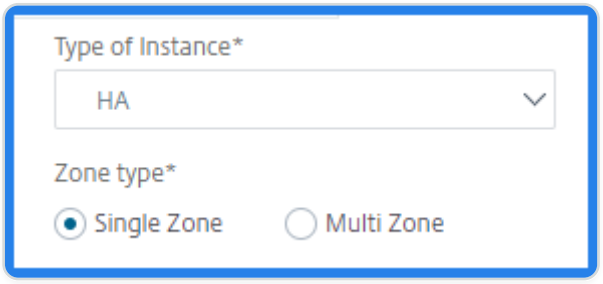
CONFIGURE BASIC PARAMETERS

1. In the **Basic Parameters** tab, specify the following:

   - **Type of Instance**: Select one of the following options from the list.
     - **Standalone** - This option provisions a standalone NetScaler VPX instance on Microsoft Azure.
     - **HA:** This option provisions the high availability NetScaler VPX instances on Microsoft Azure.

       To provision the NetScaler VPX instances in the same zone, select the **Single Zone** option under **Zone Type**.

       To provision the NetScaler VPX instances across multiple zones, select the **Multi Zone** option under **Zone type**. In the **Cloud Parameters** tab, make sure to specify the network details for each zone that are created on Microsoft Azure.

   - **Name** - Specify the name of an NetScaler VPX instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

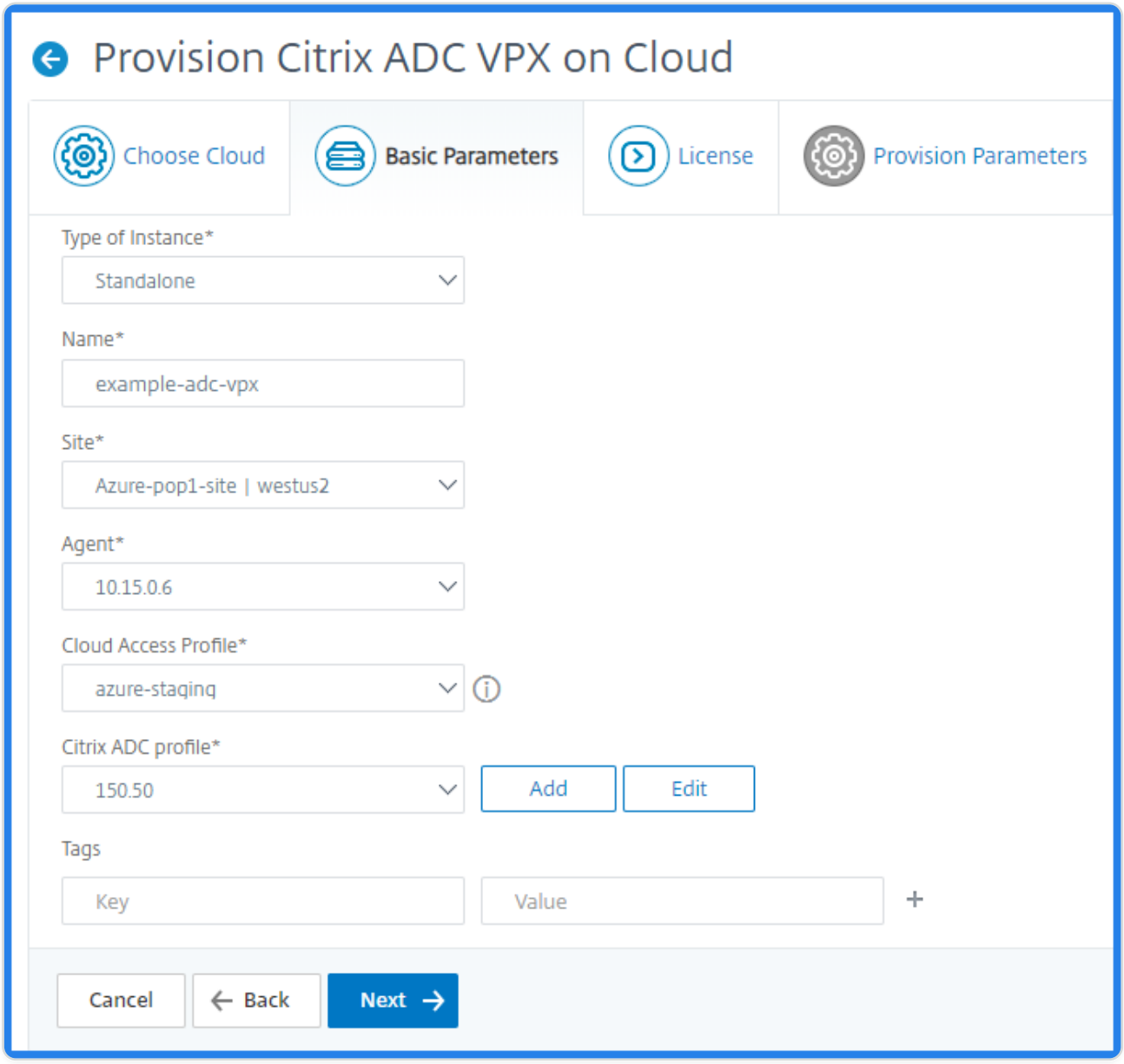
- **Site** - Select the site that you created earlier.
- **Agent** - select the agent that is created to manage the NetScaler VPX instance.
- **Cloud Access Profile** - Select the cloud access profile created during site creation.
- **NetScaler Profile** - Select the profile to provide authentication.

  NetScaler Console uses the device profile when it requires to log on to the NetScaler VPX instance.

  NOTE

  Ensure the selected device profile conforms to Microsoft Azure password rules.

2. Click **Next**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONFIGURE LICENSES

Select one of the following modes to apply license to a NetScaler instance:

- **Using NetScaler Console**: The instance that you want to provision checks out the licenses from the NetScaler Console.
- **Using Microsoft Azure**: The **Allocate from Cloud** option uses the NetScaler® product licenses available in the Azure Marketplace. The instance that you want to provision uses the licenses from the marketplace.

  If you choose to use licenses from Azure Marketplace, specify the product or license in the **Provision Parameters** tab.

For more information, see Licensing Requirements.

USE LICENSES FROM NETSCALER CONSOLE

To use this option, ensure that you have subscribed to the NetScaler product with the **Bring your own license** software plan in Azure. See, Subscribe to the NetScaler VPX license in Microsoft Azure.

1. In the **License** tab, select **Allocate from NetScaler Console**.
2. In **License Type**, select one of the following options from the list:
   - **Bandwidth Licenses:** You can select one of the following options from the **Bandwidth License Types** list:
     - **Pooled Capacity:** Specify the capacity to allocate to an instance.

       From the common pool, the NetScaler instance checks out one instance license and only as much bandwidth is specified.
     - **VPX Licenses:** When a NetScaler VPX instance is provisioned, the instance checks out the license from the NetScaler Console.
   - **Virtual CPU Licenses:** The provisioned NetScaler VPX instance checks out licenses depending on the number of CPUs running in the instance.

NOTE

When the provisioned instances are removed or destroyed, the applied licenses return to the NetScaler Console license pool. These licenses can be reused to provision new instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. In **License Edition**, select the license edition. The NetScaler Console uses the specified edition to provision instances.
4. Click **Next**.

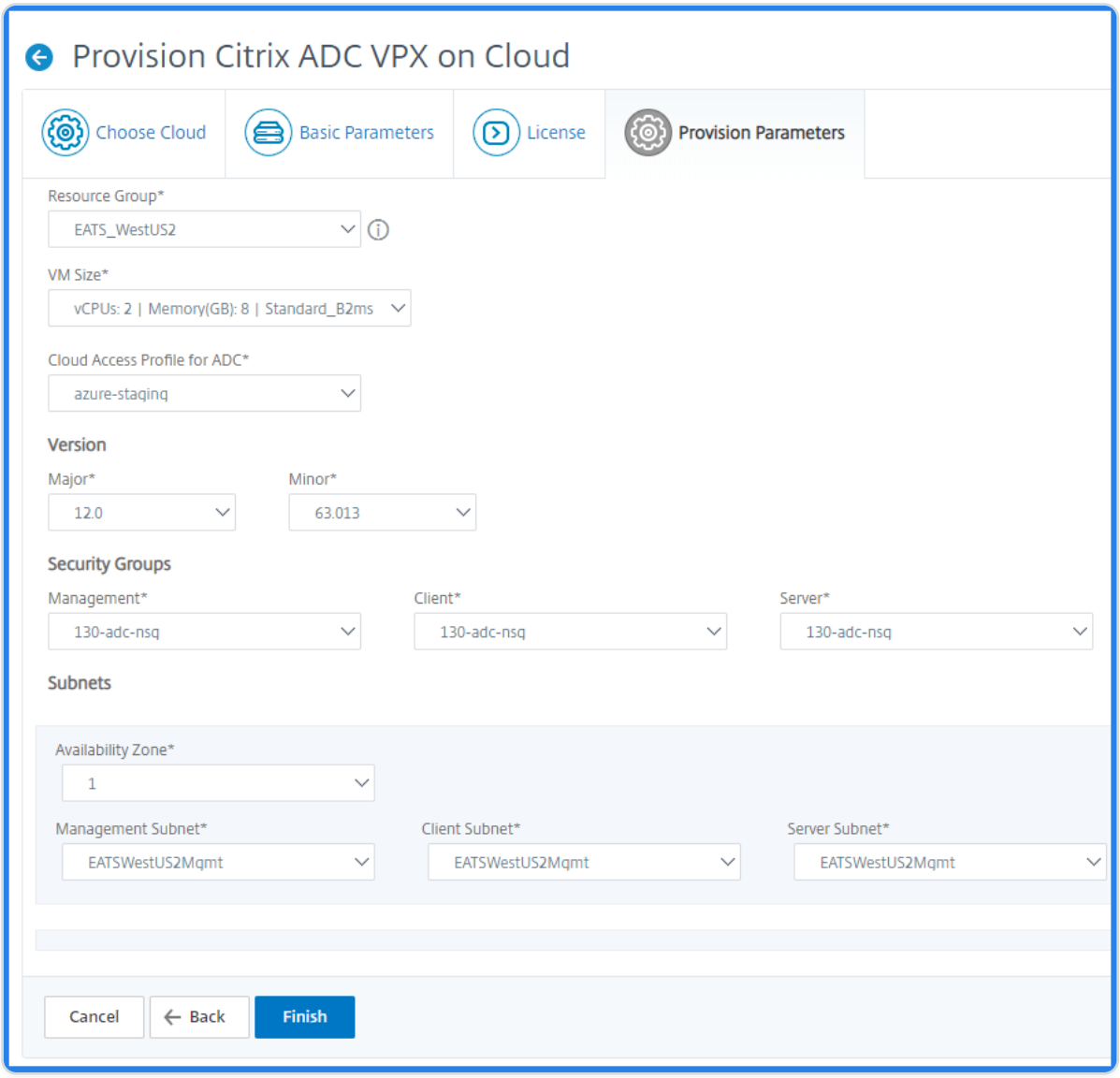
CONFIGURE PROVISION PARAMETERS

1. In the **Provision Parameters** tab, specify the following:
    a. Select the **Resource Group** in which you want to provision the NetScaler VPX instance.
    b. Select the supported **VM size** from the list.

    > **NOTE**
    >
    > This list displays the supported VM sizes for the selected NetScaler product.

    c. Select the Cloud Access Profile for NetScaler.
    d. Select the **Version** of NetScaler that you want to provision. Select both **Major** and **Minor** version of NetScaler.
    e. In **Security Groups**, select the Management, Client, and Server security groups that you have created in your virtual network.
    f. In **Subnets**, specify the required number of availability zones in Azure.
    g. In **Subnets**, select the Management, Client, and Server subnets that you have created in your virtual network.
    h. Click **Finish**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The NetScaler VPX instance is now provisioned on Microsoft Azure.

View the provisioned NetScaler VPX instances

To view in NetScaler Console:

1. In NetScaler Console, navigate to **Infrastructure > Instances > NetScaler**.
2. Select the **NetScaler VPX** tab.

   The NetScaler VPX instance provisioned in Microsoft Azure is listed here.

To view in Microsoft Azure:

1. Log on to your Azure portal.
2. Navigate to the resource group that is created to provision the NetScaler VPX instance.

   This page displays the provisioned NetScaler VPX instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

The name of the NetScaler VPX instance is the same that you provided while provisioning an instance in the NetScaler Console.

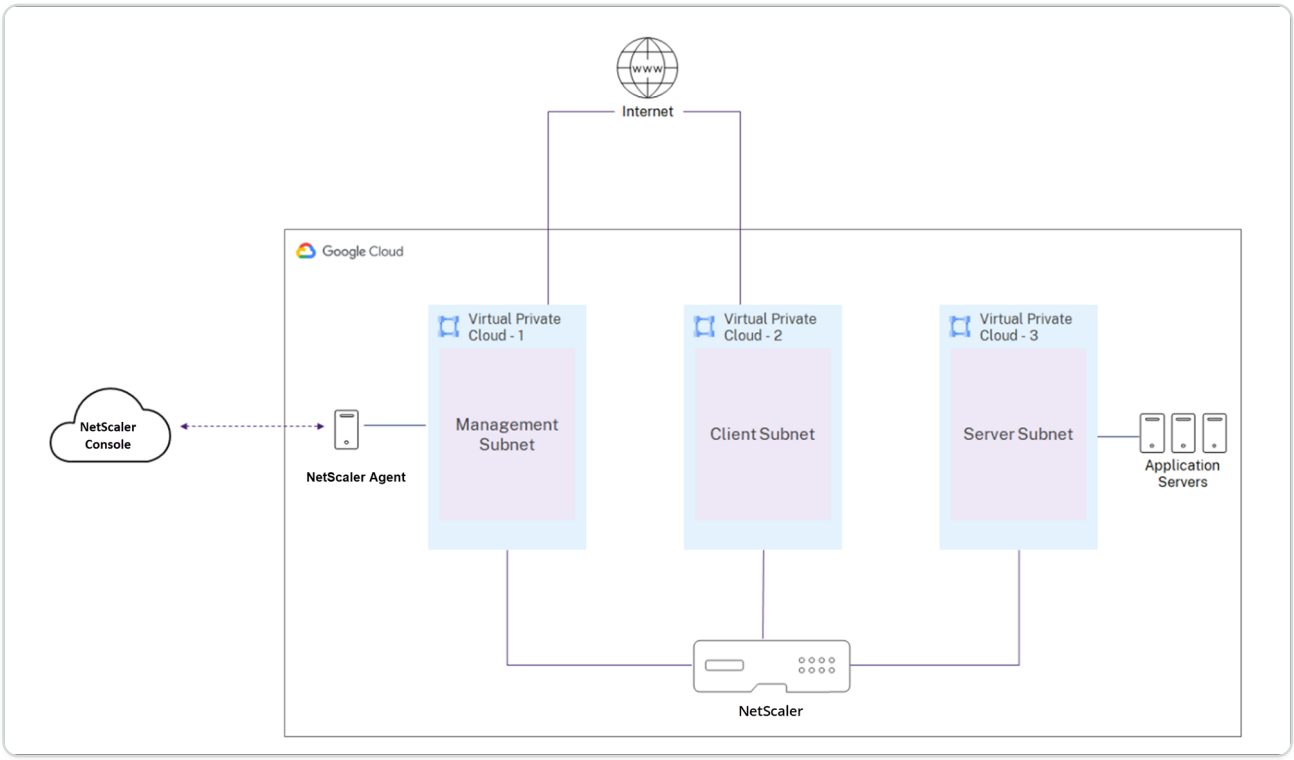
Provisioning NetScaler VPX instances on Google Cloud

Applications or services hosted on Google Cloud require secure traffic management and efficient optimization of network resources along with cloud benefits. NetScaler VPX instances provisioned on Google Cloud provide secure traffic management, optimized resource consumption, and reduced web application ownership costs.

NetScaler Console allows you to automate the deployment, setup, and management of the NetScaler VPX instances on Google Cloud. Provisioning NetScaler VPX instances using NetScaler Console combines the elasticity and flexibility of cloud with the control features of NetScaler.

NetScaler Console Deployment Architecture

The following image provides an overview of how NetScaler Console connects with Google Cloud to provision NetScaler VPX instances in Google Cloud.



You require three Virtual Private Cloud (VPC) networks to provision and manage the NetScaler VPX instance in Google Cloud. A VPC network contains a subnet and firewall. The firewall has rules that govern the incoming and outgoing traffic to a subnet.

The agent helps you to provision and manage the NetScaler VPX instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prerequisites

This section describes the prerequisites that you must complete in Google Cloud and NetScaler Console before you provision NetScaler VPX instances.

This document assumes you possess a Google Cloud account. For more information on how to create an account, see Google Cloud Documentation.

SET UP GOOGLE CLOUD COMPONENTS

Before you provision NetScaler VPX instances in NetScaler Console, do the following tasks in Google Cloud:

1. Enable APIs
2. Create a Service Account
3. Create a VPC network
4. Create a firewall
5. Subscribe to the NetScaler VPX license in Google Cloud

Enable APIs

NetScaler Console requires programmatic access to deploy and provision the required resources in Google Cloud. So, enable the following APIs on your Google Cloud project:

- Compute Engine API
- Cloud DNS API

For more information about how to enable APIs in Google Cloud, see Enabling APIs.

Create a Service Account

The NetScaler Console uses a Service Account to access your Google Cloud resources. Do the following to create a service account:

1. Log in to your Google Cloud account.
2. Go to **IAM & Admin > Service Accounts**.
3. Click **+CREATE SERVICE ACCOUNT**.

   Create two service accounts, one service account is used for NetScaler Console. And, another is used for NetScaler instances. Do the following steps to create a service account.

   a. Specify the name, ID, and description and click Create.

   b. Assign the following predefined roles:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- IAM roles required for NetScaler Console

```
roles/iam.serviceAccountUser

roles/compute.instanceAdmin.v1

roles/compute.networkAdmin

roles/dns.admin
```

- IAM roles required for the NetScaler instances that are created by NetScaler Console:

```
roles/compute.instanceAdmin.v1

roles/compute.networkAdmin
```

These roles allow your service account to access Google Cloud resources.

c. Click **Done**.

Create a VPC network

Create three subnets in your VPC network - one each for the management, client, and server connections. Select the custom option to create a subnet. Specify an address range for each of the subnets. Specify the region in which you want the subnet to reside.

- **Management**: A subnet in your management VPC Network dedicated for management. NetScaler has to contact Google Cloud services and requires internet access.
- **Client**: A subnet in your client VPC network dedicated for the client side. Typically, NetScaler receives client traffic for the application via a public subnet from the internet.
- **Server**: A subnet where the application servers are provisioned. All your application servers are present in this subnet and receives application traffic from the NetScaler through this subnet. For more information on how to create a subnet in Google Cloud, see VPC network overview.

Create a firewall

The firewall has rules that control the inbound and outbound traffic in the NetScaler VPX instance. You can add as many rules as you want. To Autoscale NetScaler instances, you must create three firewalls:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Management**: A firewall is dedicated for the management of NetScaler VPX. NetScaler has to contact Google Cloud services and requires internet access. Inbound rules are allowed on the following TCP and UDP ports.
  - TCP: 80, 22, 443, 3008–3011, 4001, 27000, 7279
  - UDP: 67, 123, 161, 500, 3003, 4500, 7000

  NOTE

  Ensure that the firewall allows the agent to be able to access the VPX.

- **Client**: A firewall is dedicated for client-side communication of NetScaler VPX instances. Typically, inbound rules are allowed on the TCP ports 80, 22, and 443.
- **Server**: A firewall is dedicated for server-side communication of NetScaler VPX. For more information on how to create a firewall in Google Cloud, see VPC firewall rules overview.

Subscribe to the NetScaler VPX license in Google Cloud

1. Log on to your Google Cloud portal.
2. In **Marketplace**, search NetScaler and select the required product version.
3. Select one of the following license types:
   - Customer Licensed
   - Enterprise
   - Platinum

   NOTE

   If you select the **Customer Licensed** option, the Autoscale group checks out the licenses from the NetScaler Console while provisioning NetScaler instances.

SET UP NETSCALER CONSOLE COMPONENTS

Before provisioning NetScaler VPX instances in NetScaler Console, do the following tasks in NetScaler Console:

1. Create a site.
2. Provision NetScaler agent on Google Cloud.
3. Attach the site to a NetScaler agent.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a site

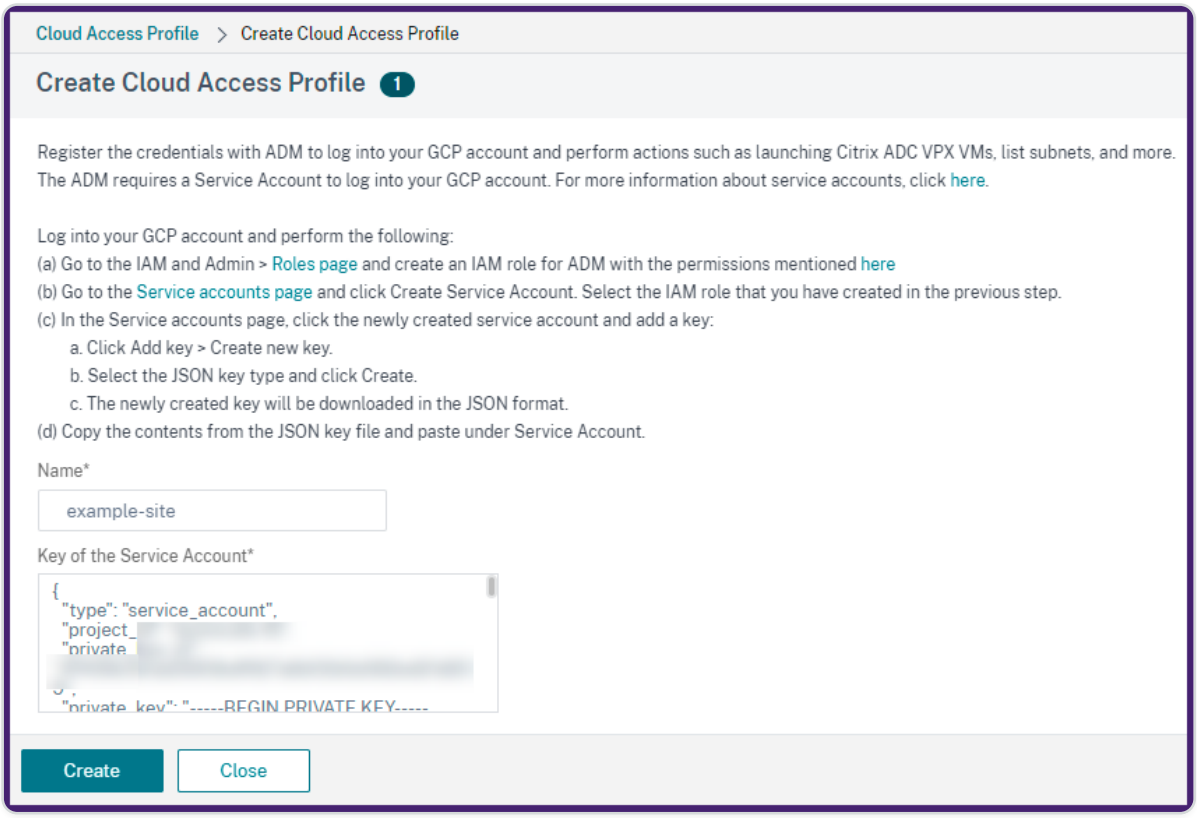
Create a site in NetScaler Console and add the VNet details associated with your Google Cloud.

1. In NetScaler Console, navigate to **Infrastructure > Sites**.
2. Click **Add**.
3. In the **Select Cloud** pane,
    a. Select **Data Center** as a Site type.
    b. Choose **Google Cloud** from the Type list.
    c. Check the **Fetch regions from the Google Cloud** check box.

        This option helps you to retrieve the existing regions information from your Google Cloud account.

    d. Click **Next**.
4. In the **Choose Region** pane,
    a. In **Cloud Access Profile**, select the profile created for your Google Cloud account. If there are no profiles, create a profile.
    b. To create a cloud access profile, click **Add**.
    c. In **Name**, specify a name to identify your Google Cloud account in NetScaler Console.
    d. In **Key of the Service Account**, specify the Service Account JSON created in Google Cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



e. Click **Create**.

   For more information, see Create a Service Account.

f. In **Regions**, select the region that contains the VPC network containing NetScaler VPX instances that you want to manage.

g. Specify a **Site Name**.

h. Click **Finish**.

Provision NetScaler agent on Google Cloud

The agent works as an intermediary between the NetScaler Console and the discovered instances in the data center or on the cloud.

1. Navigate to **Infrastructure > Instances > Agents**.
2. Click **Provision**.
3. Select **Google Cloud** and click **Next**.
4. In the **Provision Parameters** tab, specify the following:

   - **Name** - specify the agent name.
   - **Site** - select the site you have created to provision an agent and NetScaler VPX instances.
   - **Cloud Access Profile** - select the cloud access profile from the list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Zone** - Select the zones in which you want to create the Autoscale™ groups. Depending on the cloud access profile that you have selected, the zones of that profile are populated.
- **Network**- Select the VPC network where you want to create Autoscale groups.
- **Subnet** - Select the management subnet to provision an agent.
- **Tags** - Type the key-value pair for the Autoscale group tags. A tag consists of a case-sensitive key-value pair. These tags enable you to organize and identify the Autoscale groups easily. The tags are applied to both Google Cloud and NetScaler Console.

5. Click **Finish**.

Alternatively, you can install the agent from Google Cloud Marketplace. For more information, see Install a NetScaler agent on the Google Cloud.

Attach the site to a NetScaler agent

1. In NetScaler Console, navigate to **Infrastructure > Instances > Agents**.
2. Select the agent for which you want to attach a site.
3. Click **Attach Site**.
4. Select the site from the list that you want to attach.
5. Click **Save**.

Configuration tasks

To provision a standalone NetScaler VPX instance on Google Cloud, do the following steps:

1. In NetScaler Console, navigate to **Infrastructure > Instances > NetScaler**.
2. Click **Provision**.
3. Select **Google Cloud** and click **Next**. Specify the required parameters to provision an instance.
4. Specify the basic parameters, licenses, and provision parameters.

CONFIGURE BASIC PARAMETERS

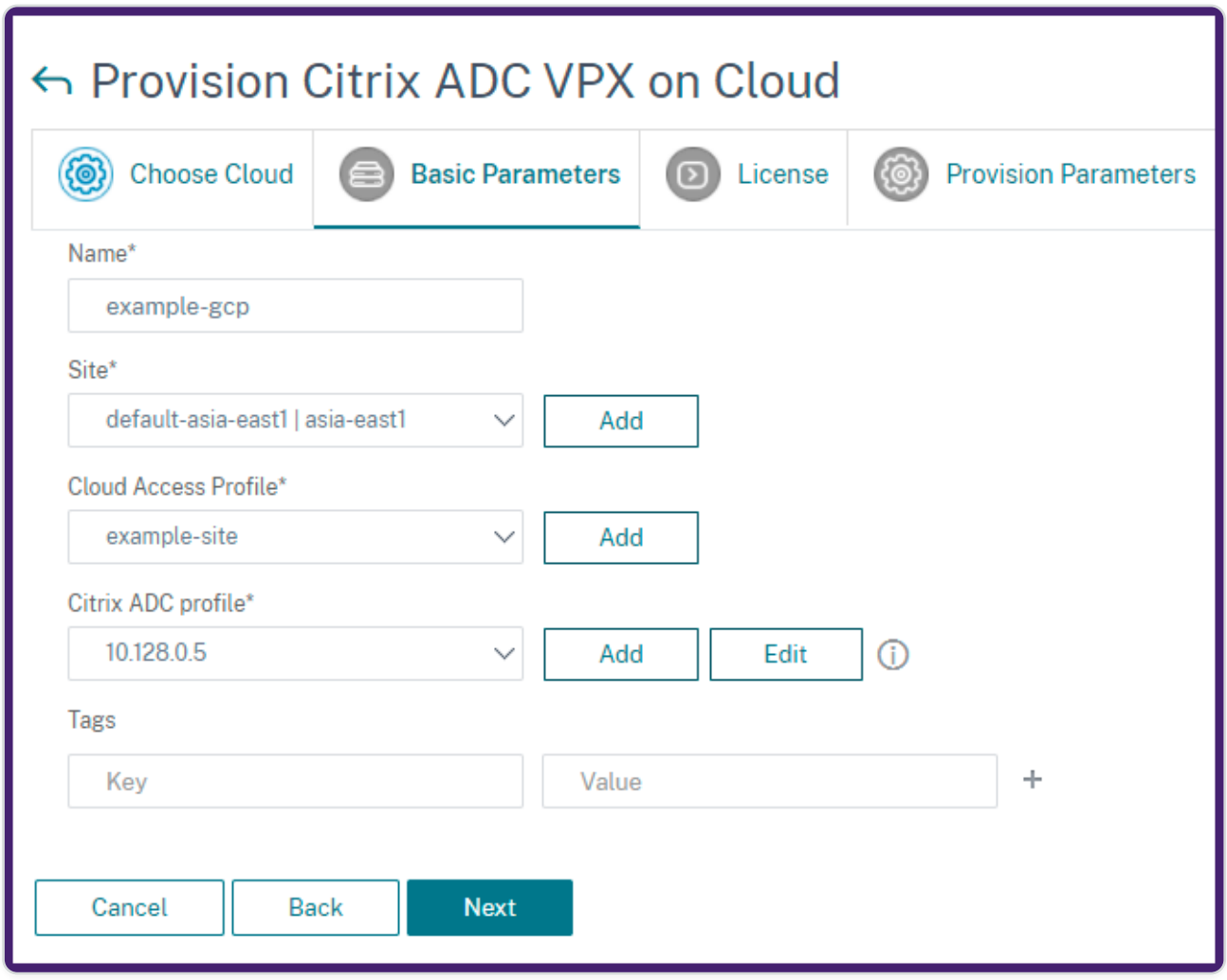
1. In the **Basic Parameters** tab, specify the following:

   - **Name** - Specify the name of an NetScaler VPX instance.
   - **Site** - Select the site that you created earlier.
   - **Agent** - select the agent that is created to manage the NetScaler VPX instance.
   - **Cloud Access Profile** - Select the cloud access profile created during site creation.
   - **NetScaler Profile** - Select the profile to provide authentication.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console uses the device profile when it requires to log on to the NetScaler VPX instance.

2. Click **Next**.



CONFIGURE LICENSES

Select one of the following modes to apply license to a NetScaler instance:

- **Using NetScaler Console**: The instance that you want to provision checks out the licenses from the NetScaler Console.
- **Using Google Cloud**: The **Allocate from Cloud** option uses the NetScaler® product licenses available in the Google Cloud Marketplace. The instance that you want to provision uses the licenses from the marketplace.

  If you choose to use licenses from Google Cloud Marketplace, specify the product or license in the **Provision Parameters** tab.

For more information, see Licensing Requirements.

Use licenses from NetScaler Console

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To use this option, ensure that you have subscribed to the NetScaler product with the **Bring your own license** software plan in Google Cloud. See, Subscribe to the NetScaler VPX license in Google Cloud.

1. In the **License** tab, select **Allocate from NetScaler Console**.
2. In **License Type**, select one of the following options from the list:
    - **Bandwidth Licenses:** You can select one of the following options from the **Bandwidth License Types** list:
        - **Pooled Capacity:** Specify the capacity to allocate to an instance.

          From the common pool, the NetScaler instance checks out one instance license and only as much bandwidth is specified.
        - **VPX Licenses:** When a NetScaler VPX instance is provisioned, the instance checks out the license from the NetScaler Console.
    - **Virtual CPU Licenses:** The provisioned NetScaler VPX instance checks out licenses depending on the number of CPUs running in the instance.

    NOTE

    When the provisioned instances are removed or destroyed, the applied licenses return to the NetScaler Console license pool. These licenses can be reused to provision new instances.
3. In **License Edition**, select the license edition. The NetScaler Console uses the specified edition to provision instances.
4. Click **Next**.

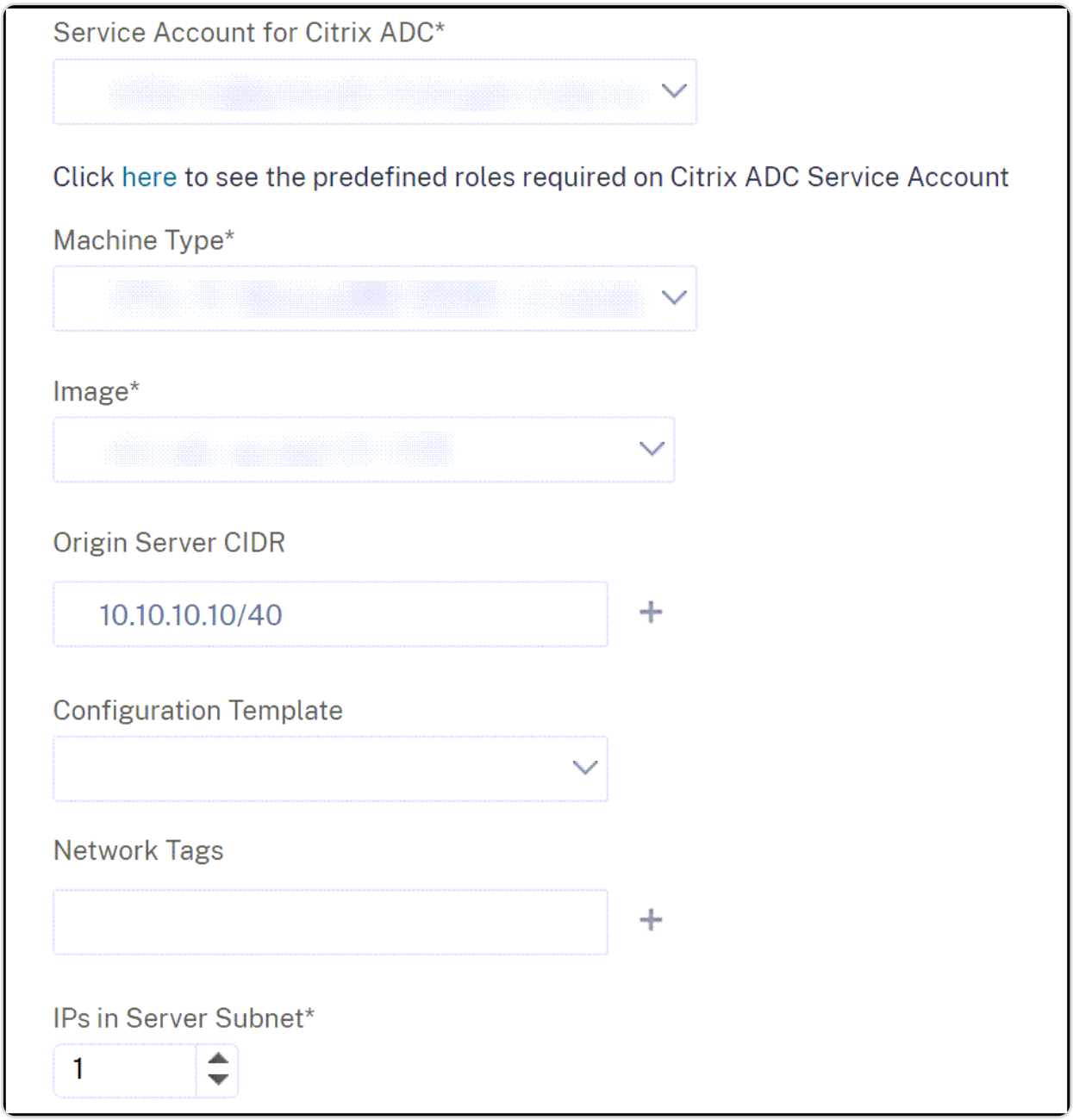
CONFIGURE PROVISION PARAMETERS

1. In the **Provision Parameters** tab, specify the following:
    - **NetScaler Service Account**: Select the service account that you have created in Google Cloud. The NetScaler Console uses a Service Account to access your Google Cloud resources.
    - **Product / License**: Select the NetScaler product version that you want to provision. For more information, see Subscribe to the NetScaler VPX license in Google Cloud.
    - **Machine types**: Select the required machine type from the list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This list displays the supported machine types for the selected NetScaler image.

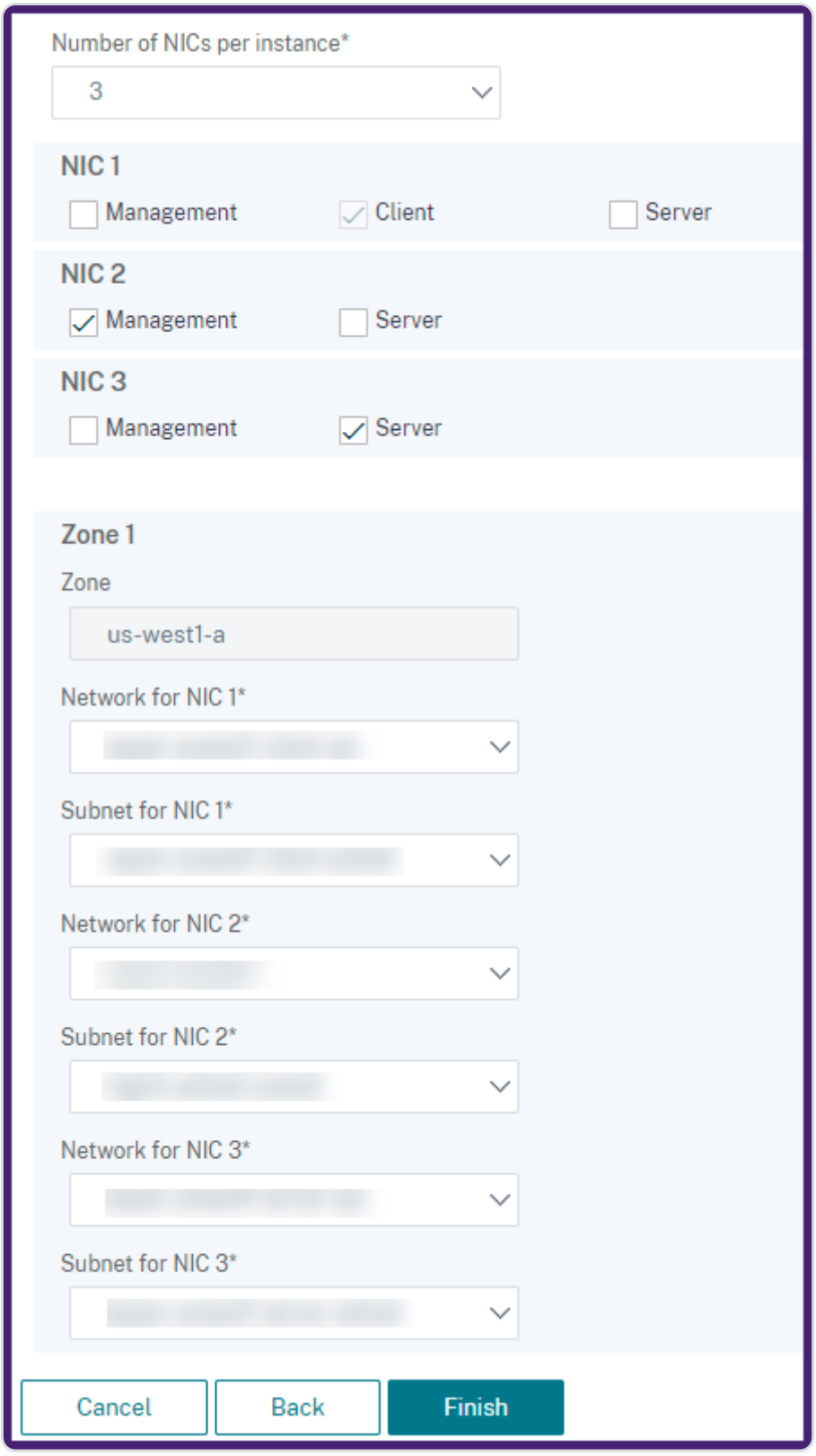
- **Image**: Select the required NetScaler version image. Click **Add New** to add a NetScaler image.
- **Configuration Template** – Select the configuration template that you want to use to deploy on the NetScaler instances.
- **IPs in Server Subnet per instance** – Specify how many SNIP addresses each instance can have in the server subnet.



In this tab, you can also specify and configure the required NICs. Each NIC contains a dedicated firewall and subnet.

For more information, see Create a VPC network and Create a firewall.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Click **Finish**.

View the provisioned NetScaler VPX instances

To view in NetScaler Console:

1. In NetScaler Console, navigate to **Infrastructure > Instances > NetScaler**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Select the **NetScaler VPX** tab.

   The NetScaler VPX instance provisioned in Google Cloud is listed here.

To view in Google Cloud:

1. Log on to your Google Cloud portal.
2. Navigate to the **Resources** tab that displays the provisioned NetScaler VPX instance.

NOTE

The name of the NetScaler VPX instance is the same that you provided while provisioning an instance in the NetScaler Console.

Provision NetScaler VPX instances on VMware ESX

You can use NetScaler Console to automate a NetScaler VPX instance deployment and management in VMware ESX. When you use NetScaler Console to provision a NetScaler VPX instance on VMware ESX, the instance is readily available to manage in the NetScaler Console GUI.

The NetScaler Console uses NetScaler templates of the already deployed instances to provision a new instance in VMware ESX. It stores the datacenter of the VMware vCenter where the required VMware ESX server details are present in a site. Also, it uses cloud access profile to access the VMware vCenter and deploy the VPX on the VMware ESX.

Prerequisites

Before you provision a NetScaler VPX instance in VMware ESX, ensure to complete the following:

1. Install a supported VMware ESXi version (6.0, 6.5, and 6.7).
2. Install VMware Client on a management workstation that meets the minimum system requirements.
3. Download the NetScaler VPX setup files.
4. Convert NetScaler VPX files into templates in ESX.
5. Create permissions for NetScaler Console to access VMware vCenter.
6. Create a site in NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

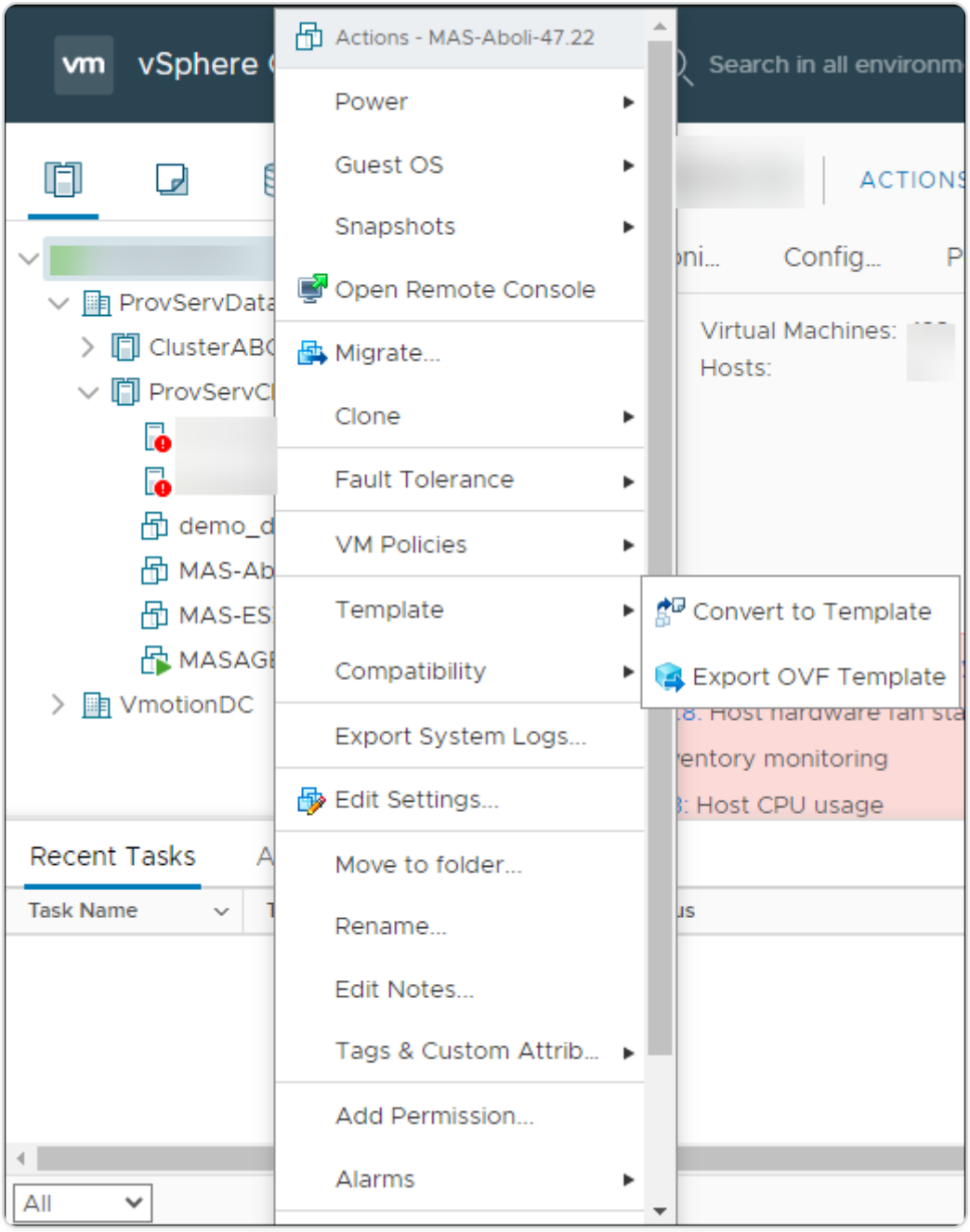
Convert NetScaler VPX files into templates

The NetScaler Console uses the NetScaler template in ESX converted by a NetScaler VPX file. Perform the following steps to convert VPX files into templates.

1. Deploy a NetScaler VPX instance on VMware using the NetScaler setup files.

   For the first time, use NetScaler setup files to deploy the VPX instance. For more information, see Install NetScaler VPX instance on VMware.

2. Right-click the deployed VM and select **Template**.
3. Click **Convert to Template**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create permissions for NetScaler Console to access VMware vCenter

To enable NetScaler Console for provisioning and management in VMware vCenter, follow these steps:

1. Create a custom role with privileges
    a. Login to VMware vCenter and navigate to the **Roles** section.
    b. Create a custom role tailored for NetScaler Console.
    c. Assign the following privileges:

```
Datastore.AllocateSpace

Resource.AssignVMToPool

VirtualMachine.Config.AdvancedConfig

VirtualMachine.Inventory.CreateFromExisting

VirtualMachine.Inventory.Delete

VirtualMachine.Interact.PowerOff

VirtualMachine.Interact.PowerOn

VirtualMachine.Provisioning.DeployTemplate
```

2. Create a user
    a. Once the role is defined, navigate to the **Users and Groups** section.
    b. Create a user for NetScaler Console to access the VMware vCenter.
    c. Provide a password for the newly created user.
3. Associate the role with the user
    a. Navigate to the **Global Permissions** section and associate the custom role with the user.
    b. This association provides privileges for NetScaler Console to perform necessary actions on VMware vCenter.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The listed privileges are the minimum requirements for NetScaler Console to access the VMware vCenter. Creating a user with limited privileges is optional. If any user has privileges that include a superset of the specified privileges, the user can provide those credentials instead.

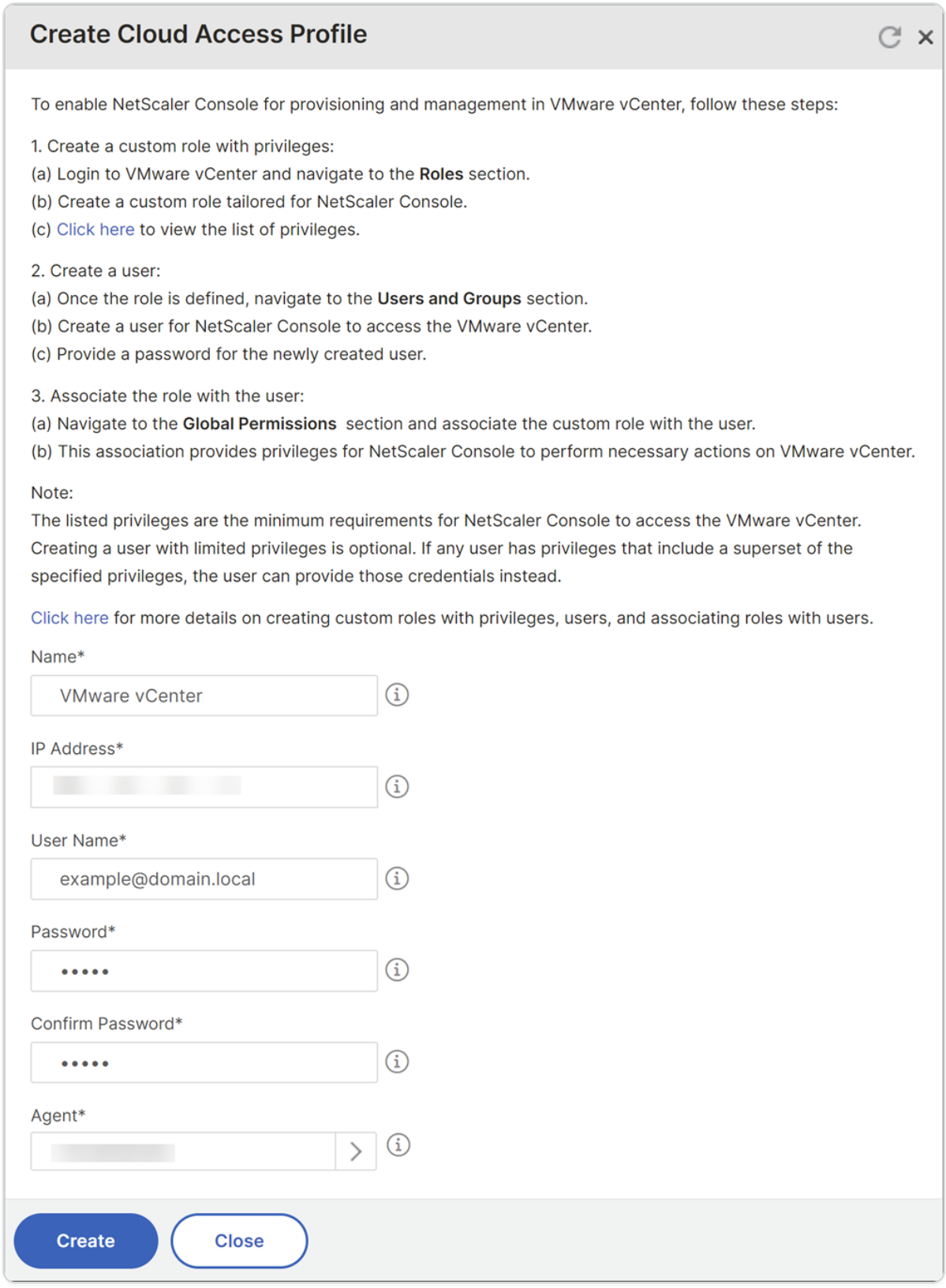
For more information about configuring user roles with privileges in VMware vCenter, see Configure User access.

Create a site in NetScaler Console

Create a site in NetScaler Console and add the VMware ESX details.

1. In NetScaler Console, navigate to **Infrastructure > Instances > Sites**.
2. Click **Add**.
3. In the **Select Cloud** pane,
    a. Select **Data Center** as a **Site type**.
    b. Choose **VMware vCenter** from the **Type** list.
    c. Click **Next**.
4. In the **Choose Region** pane,
    a. In the **Cloud Access Profile** pane, select the profile created for your VMware ESX. If there are no profiles, create a profile.
    b. To create a cloud access profile, click **Add** and specify the following:
        - **Name** – Specify a name to identify your cloud access profile in NetScaler Console.
        - **IP address** – Specify the IP address of the VMware vCenter.
        - **Username** – Specify the user name to access the VMware vCenter.
        - **Password** – Specify the password to access the VMware vCenter and confirm the password.
        - **Agent** - Select the agent registered with NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



c. In **Network (Datacenter)**, select the data center where you have the NetScaler VPX templates.

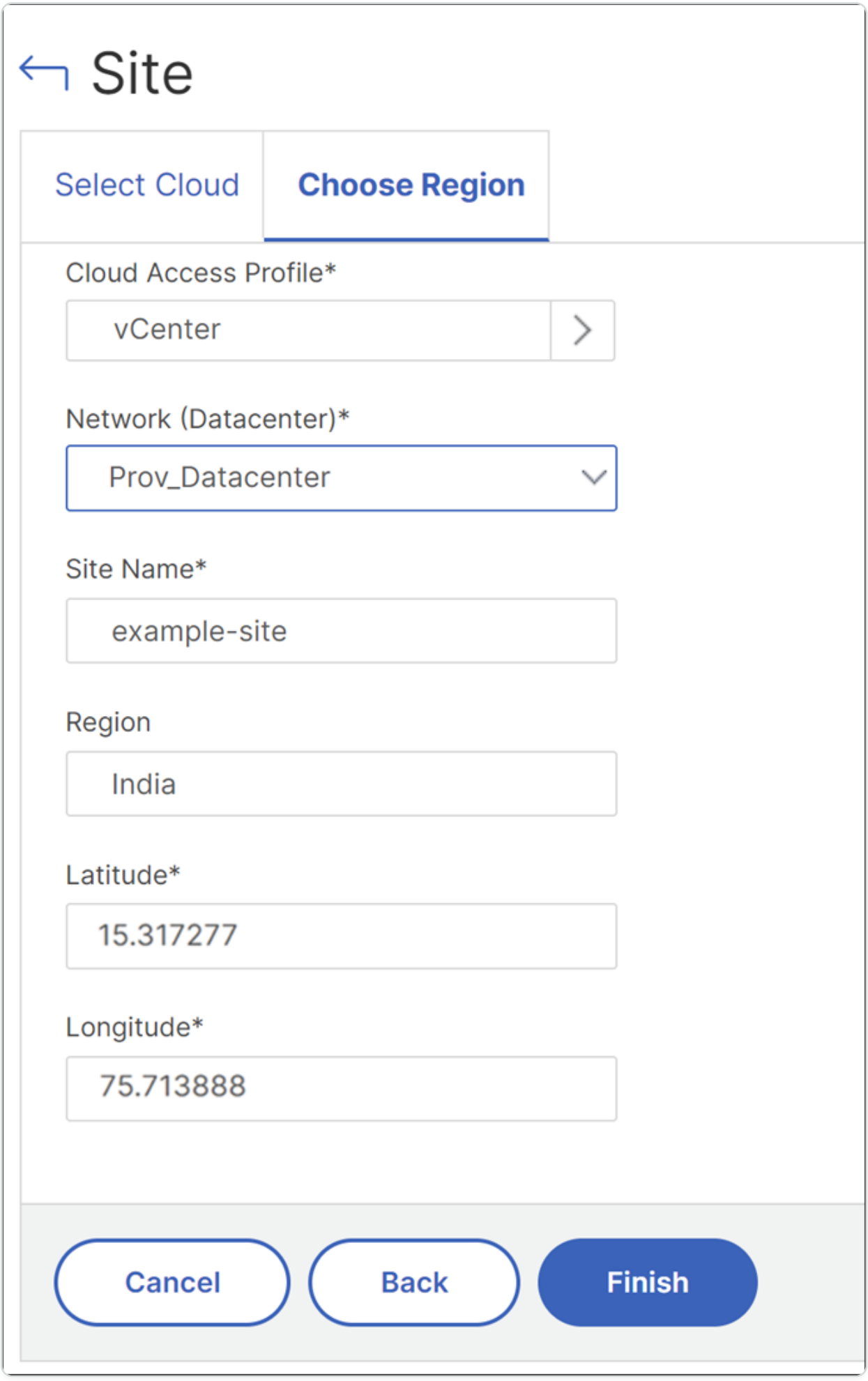
d. Specify the **Site Name**.

e. Specify the **Region**, **Latitude**, and **Longitude** to identify the geo-location of your data center.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

f. Click **Finish**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Provision NetScaler VPX instance on VMware ESX

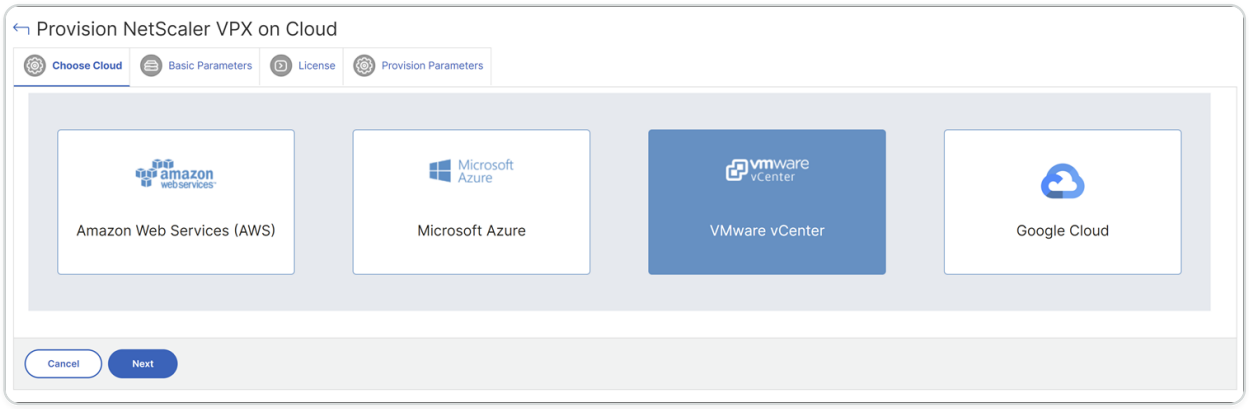
Use the site that you have associated with your VMware ESX to provision the NetScaler VPX instances.

NOTE:

Currently, the NetScaler Console supports only to provision standalone NetScaler instances.

1. In NetScaler Console, navigate to **Infrastructure > Instances > NetScaler**.
2. In the **VPX** tab, click **Provision**.

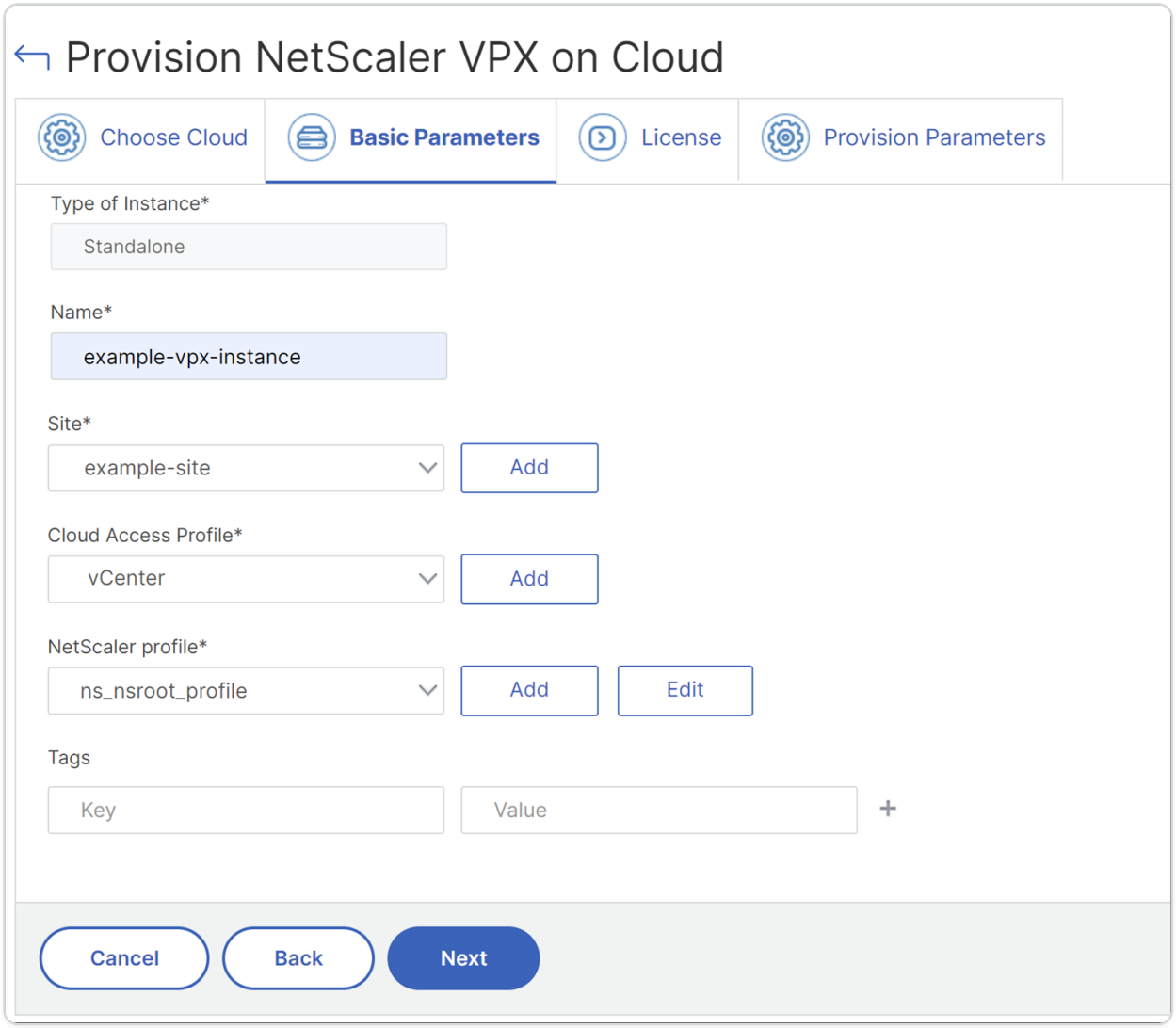
   This option displays the **Provision NetScaler VPX on Cloud** page.
3. In the **Choose Cloud** tab, select **VMware vCenter** and click **Next**.



4. In the **Basic Parameters** tab, specify the following:

   - **Name** – Specify the name of an instance.
   - **Site** – Select the site that you have created earlier.
   - **Cloud Access Profile** – Select the cloud access profile created during site creation.
   - **NetScaler profile** – Select the NetScaler profile to provide authentication.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Click **Next**.
6. In the **License** tab, the **Allocate from Cloud** option is automatically selected and uses the NetScaler product licenses available in the VMware vCenter. The VPX instance you want to provision uses licenses from the VMware vCenter.

    a. **License Type** – Select the license type as bandwidth or virtual CPU licenses.

        i. For bandwidth license type, you can select one of the following options from the **Bandwidth License Type** list:

        - **Pooled Capacity** - Specify the capacity to allocate to an instance in the **Bandwidth capacity to be allocated for each NetScaler instance**.

          From the common pool, the NetScaler instance checks out one instance license and only as much bandwidth is specified.
        - **VPX Licenses** - When a NetScaler VPX instance is provisioned, the instance checks out the license from the NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

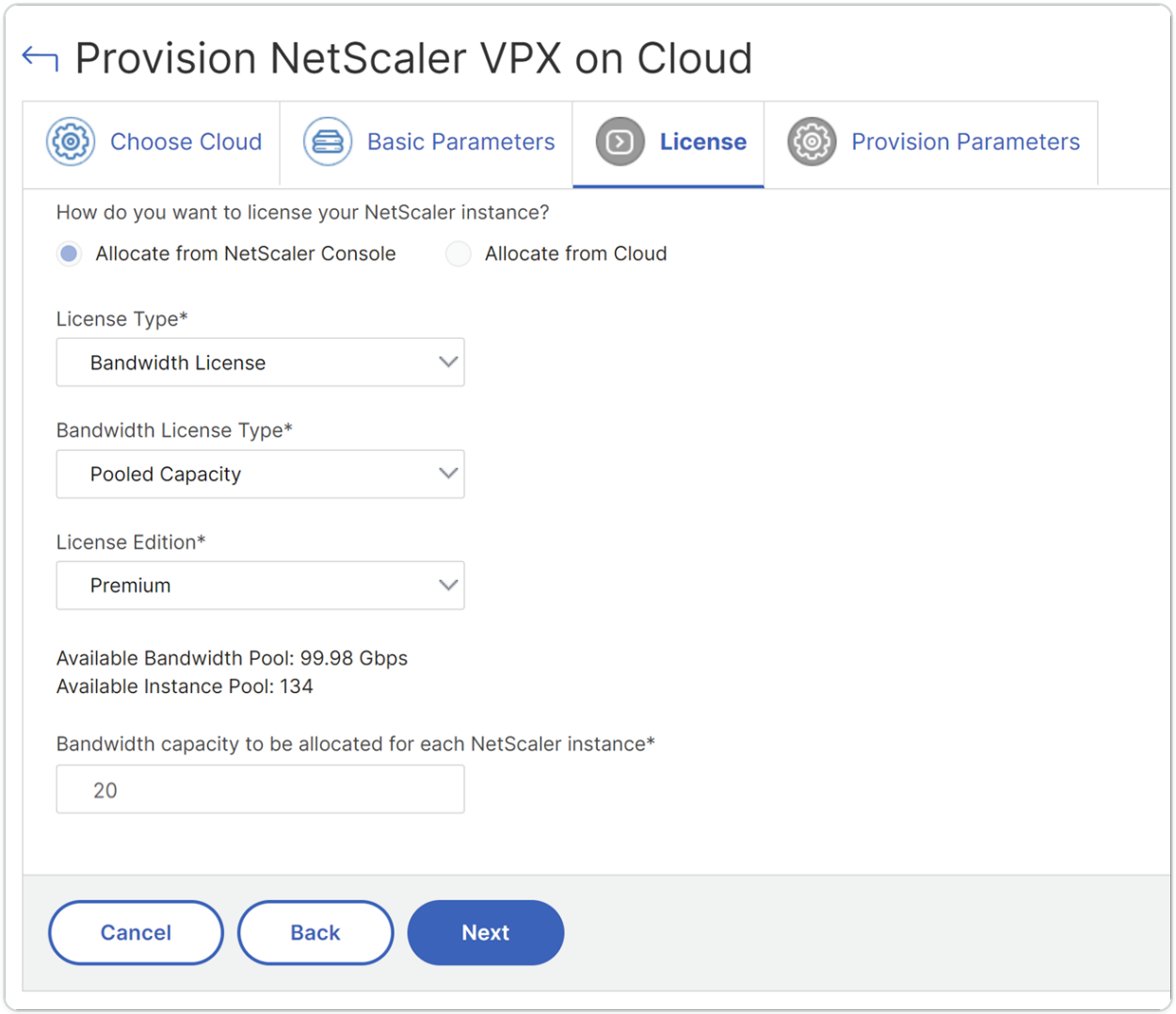
ii. **Virtual CPU Licenses**: The provisioned NetScaler VPX instance checks out licenses depending on the number of CPUs running in the instance.

NOTE:

When the provisioned VPX instances are removed or destroyed, the applied licenses return to the NetScaler Console license pool. These licenses can be reused to provision new VPX instances.

b. **License Edition** – Select the license edition from the list.

NetScaler Console uses the specified edition to provision the VPX instances.

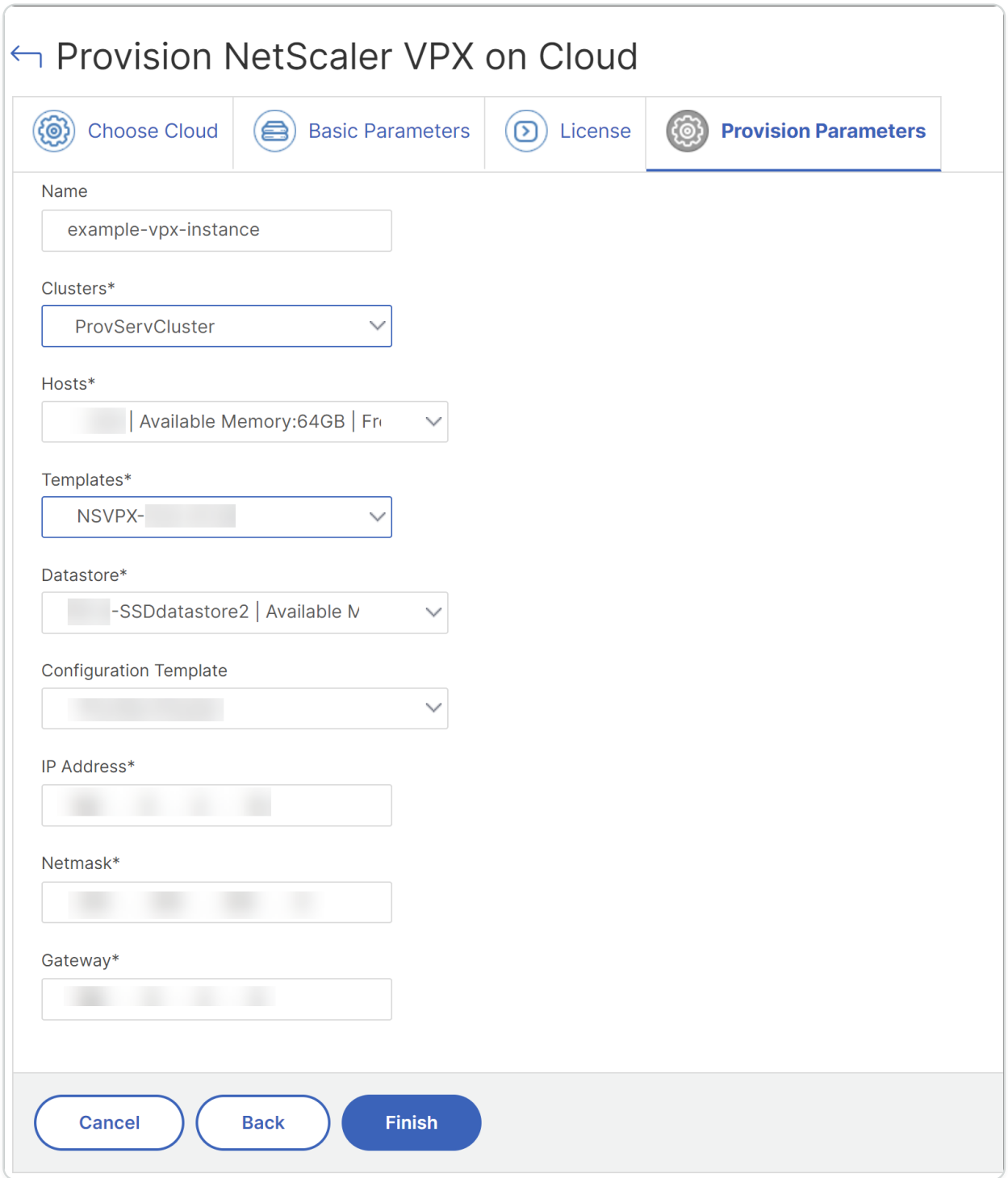


7. Click **Next**.
8. In the **Provision Parameters** tab, specify the following details:

- **Clusters** – Select the cluster where you want to provision an instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Hosts** – Select the required host from the list.
- **Templates** – Select the template from the list that you want to apply to an instance.
- **Datastore** – Select the datastore from the list.
- **Configuration Template** - Select the configuration template from the list.
- **IP address** – Specify an IP address to an instance.
- **Net mask** – Specify a net mask to an instance.
- **Gateway** – Specify a gateway to an instance.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. Click **Finish** to provision a VPX instance.

NetScaler Global Load Balancing for Hybrid and Multi-Cloud Deployments

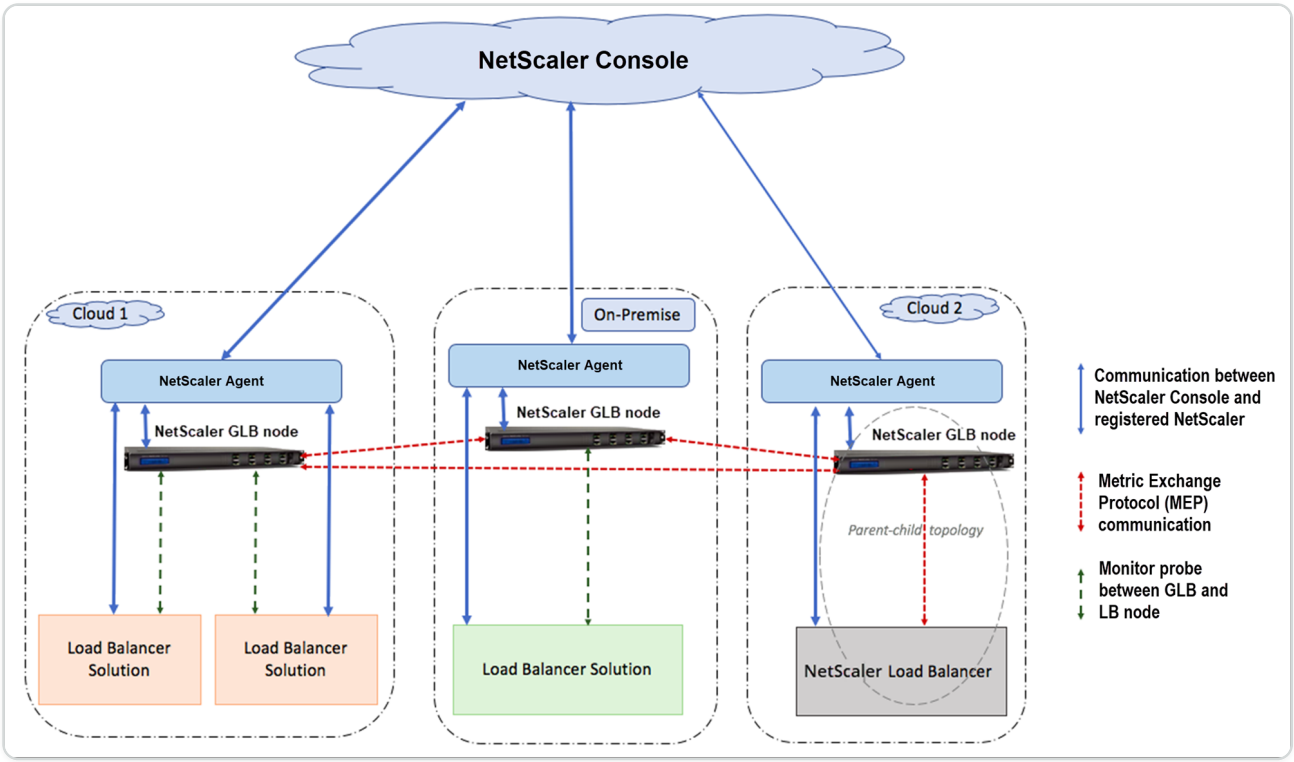
The NetScaler hybrid and multi-cloud global load balancing (GLB) solution enables you to distribute application traffic across multiple data centers in hybrid clouds, multiple clouds, and on-premises deployment. The NetScaler hybrid and multi-cloud GLB solution helps you to manage your load balancing setup in hybrid or multi-cloud without altering the existing setup. Also, if you have an on-premises setup, you can test some of your services in the cloud by using the NetScaler hybrid and multi-cloud GLB solution before completely migrating to the cloud. For example, you can route only a small percentage of your traffic to the cloud, and handle most of the traffic on-premises. The NetScaler hybrid and multi-cloud GLB solution also enables you to manage and monitor NetScaler instances across geographic locations from a single, unified console.

A hybrid and multi-cloud architecture can also improve the overall enterprise performance by avoiding "vendor lock-in" and using different infrastructure to meet the needs of your partners and customers. With multiple cloud architectures, you can manage your infrastructure costs better as you now have to pay only for what you use. Also scale your applications better as you now use the infrastructure on demand. It also provides the ability to quickly switch from one cloud to another to take advantage of the best offerings of each provider.

Architecture of the NetScaler Hybrid and Multi-Cloud GLB Solution

The following diagram illustrates the architecture of the NetScaler hybrid and multi-cloud GLB feature.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The NetScaler GLB nodes handle the DNS name resolution. Any of these GLB nodes can receive DNS requests from any client location. The GLB node that receives the DNS request returns the load balancer virtual server IP address as selected by the configured load balancing method. Metrics (site, network, and persistence metrics) are exchanged between the GLB nodes using the metrics exchange protocol (MEP), which is a proprietary Citrix protocol. For more information on the MEP protocol, see Configuring the Metrics Exchange Protocol.

The monitor configured in the GLB node monitors the health status of the load balancing virtual server in the same data center. In a parent-child topology, metrics between the GLB and NetScaler nodes are exchanged by using MEP. However, configuring monitor probes between a GLB and NetScaler LB node is optional in a parent-child topology.

The agent enables communication between the NetScaler Console and the managed instances in your data center. For more information on agents and how to install them, see Getting Started.

NOTE

This document makes the following assumptions:

- If you have an existing load balancing setup, it is up and running.
- A SNIP address or a GLB site IP address is configured on each of the NetScaler GLB nodes. This IP address is used as the data center source IP address when exchanging metrics with other data centers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- An ADNS or ADNS-TCP service is configured on each of the NetScaler GLB instances to receive the DNS traffic.
- The required firewall and security groups are configured in the cloud service providers.

SECURITY GROUPS CONFIGURATION

You must set up the required firewall/security groups configuration in the cloud service providers. For more information about AWS security features, see AWS documentation. For more information about Microsoft Azure Network Security Groups, see Microsoft Azure documentation.

In addition, on the GLB node, you must open port 53 for ADNS service/DNS server IP address and port 3009 for GSLB site IP address for MEP traffic exchange. On the load balancing node, you must open the appropriate ports to receive the application traffic. For example, you must open port 80 for receiving HTTP traffic and open port 443 for receiving HTTPS traffic. Open port 443 for NITRO communication between the agent and NetScaler Console.
For the dynamic round trip time GLB method, you must open port 53 to allow UDP and TCP probes depending on the configured LDNS probe type. The UDP or the TCP probes are initiated using one of the SNIPs and therefore this setting must be done for security groups bound to the server side subnet.

Capabilities of the NetScaler Hybrid and Multi-Cloud GLB Solution

Some of the capabilities of the NetScaler hybrid and multi-cloud GLB solution are described in this section:

Compatibility with other load balancing solutions

The NetScaler hybrid and multi-cloud GLB solution supports various load balancing solutions, such as the NetScaler load balancer, Nginx, and other third-party load balancers.

NOTE

Load balancing solutions other than NetScaler are supported only if proximity-based and non-metric based GLB methods are used and if parent-child topology is not configured.

GLB Methods

The NetScaler hybrid and multi-cloud GLB solution supports the following GLB methods.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Metric-based GLB methods. Metric-based GLB methods collect metrics from the other NetScaler nodes through the metrics exchange protocol.
  - Least Connection: The client request is routed to the load balancer that has the fewest active connections.
  - Least Bandwidth: The client request is routed to the load balancer that is currently serving the least amount of traffic.
  - Least Packets: The client request is routed to the load balancer that has received the fewest packets in the last 14 seconds.
- Non-metric based GLB methods
  - Round Robin: The client request is routed to the IP address of the load balancer that is at the top of the list of load balancers. That load balancer then moves to the bottom of the list.
  - Source IP Hash: This method uses the hashed value of the client IP address to select a load balancer.
- Proximity-based GLB methods
  - Static Proximity: The client request is routed to the load balancer that is closest to the client IP address.
  - Round-Trip Time (RTT): This method uses the RTT value (the time delay in the connection between the client's local DNS server and the data center) to select the IP address of the best performing load balancer.

For more information on the load balancing methods, see Load Balancing Algorithms.

GLB Topologies

The NetScaler hybrid and multi-cloud GLB solution supports the active-passive topology and parent-child topology.

- Active-passive topology - Provides disaster recovery and ensures continuous availability of applications by protecting against points of failure. If the primary data center goes down, the passive data center becomes operational. For more information about GSLB active-passive topology, see Configuring GSLB for Disaster Recovery.
- Parent-child topology – Can be used if you are using the metric-based GLB methods to configure GLB and LB nodes and if the LB nodes are deployed on a different NetScaler instance. In a parent-child topology, the LB node (child site) must be a NetScaler appliance

© 1997–2026 Citrix Systems, Inc. All rights reserved.

because the exchange of metrics between the parent and child site is through the metrics exchange protocol (MEP).

For more information about parent-child topology, see Parent-Child Topology Deployment Using the MEP Protocol.

IPv6 Support

The NetScaler hybrid and multi-cloud GLB solution also supports IPv6.

Monitoring

The NetScaler hybrid and multi-cloud GLB solution supports built-in monitors with an option to enable the secure connection. However, if LB and GLB configurations are on the same NetScaler instance or if parent-child topology is used, configuring monitors is optional.

Persistence

The NetScaler hybrid and multi-cloud GLB solution supports the following:

- Source IP based persistence sessions, so that multiple requests from the same client are directed to the same service if they arrive within the configured time-out window. If the time-out value expires before the client sends another request, the session is discarded, and the configured load balancing algorithm is used to select a new server for the client's next request.
- Spillover persistence so that the backup virtual server continues to process the requests it receives, even after the load on the primary falls below the threshold. For more information, see Configuring Spillover.
- Site persistence so that the GLB node selects a data center to process a client request and forwards the IP address of the selected data center for all subsequent DNS requests. If the configured persistence applies to a site that is DOWN, the GLB node uses a GLB method to select a new site, and the new site becomes persistent for subsequent requests from the client.

Configuration by using the NetScaler Console StyleBooks

You can use the default Multi-cloud GLB StyleBook on NetScaler Console to configure the NetScaler instances with hybrid and multi-cloud GLB configuration.

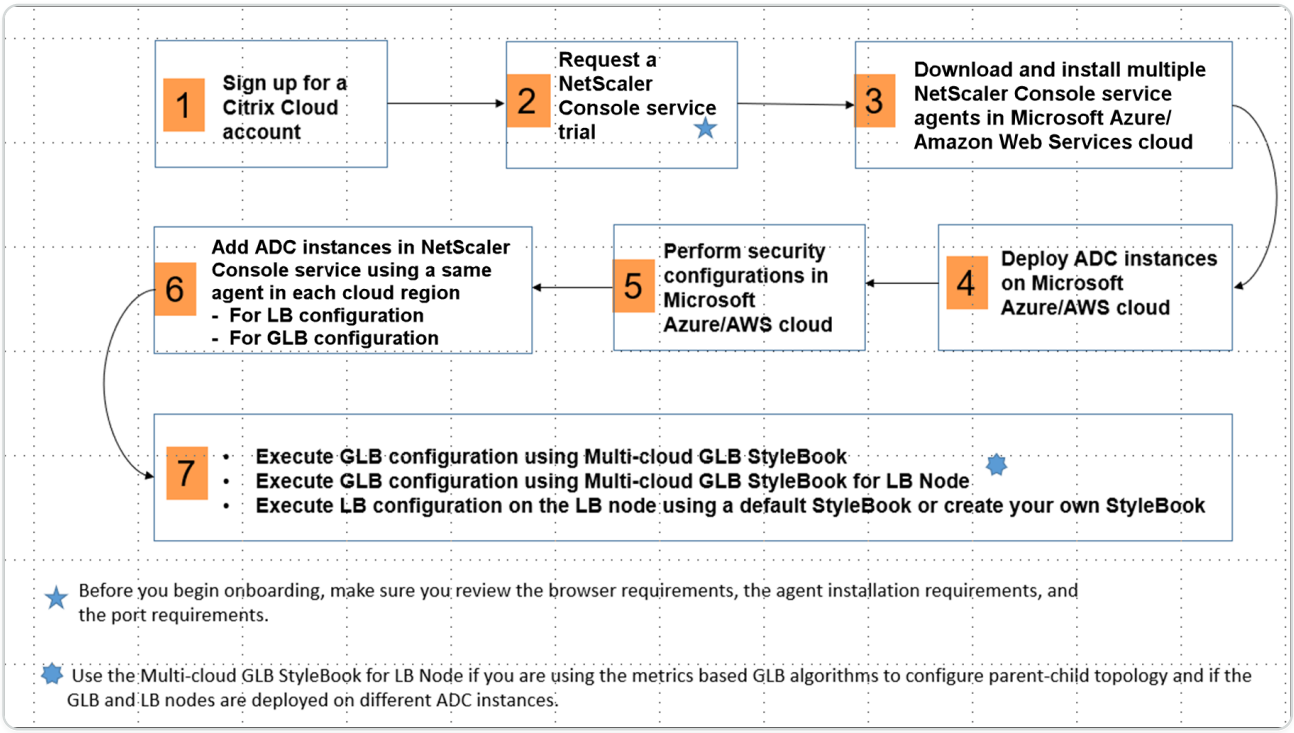
You can use the default Multi-cloud GLB StyleBook for LB Node StyleBook to configure the NetScaler load balancing nodes which are the child sites in a parent-child topology that handle the application traffic. Use this StyleBook only if you want to configure LB nodes in case of a parent-child topology. However, each LB node must be configured separately using this StyleBook.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Workflow of the NetScaler Hybrid and Multi-Cloud GLB Solution Configuration

You can use the shipped Multi-cloud GLB StyleBook on NetScaler Console to configure the NetScaler instances with hybrid and multi-cloud GLB configuration.

The following diagram shows the workflow for configuring the NetScaler hybrid and multi-cloud GLB solution. The steps in the workflow diagram are explained in more detail after the diagram.



Perform the following tasks as a cloud administrator:

1. Sign up for a Citrix Cloud™ account.

   To start using NetScaler Console, create a Citrix Cloud company account or join an existing one that has been created by someone in your company.

2. After you log on to Citrix Cloud, click **Manage** on the **NetScaler Console** tile to set up the NetScaler Console for the first time.
3. Download and install multiple agents.

   You must install and configure the agent in your network environment to enable communication between the NetScaler Console and the managed instances in your data center or cloud. Install an agent in each region, so that you can configure LB and GLB configurations on the managed instances. The LB and GLB configurations can share a single agent. For more information on the above three tasks, see Getting Started.

4. Deploy load balancers on Microsoft Azure/AWS cloud/on-premises data centers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Depending on the type of load balancers that you are deploying on cloud and on-premises, provision them accordingly. For example, you can provision NetScaler VPX instances in a Microsoft Azure Resource Manager (ARM) portal, in an Amazon Web Services (AWS) virtual private cloud and in on-premises data centers. Configure NetScaler instances to function as LB or GLB nodes in standalone mode, by creating the virtual machines and configuring other resources. For more information on how to deploy NetScaler VPX instances, see the following documents:

- Launching the NetScaler VPX for AWS AMI.
- Configuring NetScaler VPX in a Standalone Mode in Azure Resource Manager.

5. Perform security configurations.

   Configure network security groups and network ACLs in ARM or AWS to control inbound and outbound traffic for your instances and subnets.

6. Add NetScaler instances in NetScaler Console.

   NetScaler instances are network appliances or virtual appliances that you want to discover, manage, and monitor from NetScaler Console. To manage and monitor these instances, you must add the instances to the service and register both LB (if you are using NetScaler for LB) and GLB instances. For more information on how to add NetScaler instances in the NetScaler Console, see Getting Started.

7. Implement the GLB and LB configurations using default NetScaler Console StyleBooks.

   - Use **Multi-cloud GLB StyleBook** to run the GLB configuration on the selected GLB NetScaler instances.
   - Implement the load balancing configuration. (You can skip this step if you already have LB configurations on the managed instances.)

   You can configure load balancers on NetScaler instances in one of two ways:

   - Manually configure the instances for load balancing the applications. For more information on how to manually configure the instances, see Setting Up Basic Load Balancing.
   - Use StyleBooks. You can use one of the NetScaler Console StyleBooks (HTTP/SSL LoadBalancing StyleBook or HTTP/SSL LoadBalancing (with Monitors) StyleBook) to create the load balancer configuration on the selected NetScaler instance. You can also create your own StyleBooks. For more information on StyleBooks, see StyleBooks.

8. Use **Multi-cloud GLB StyleBook for LB Node** to configure GLB parent-child topology in any of the following cases:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If you are using the metric-based GLB algorithms (Least Packets, Least Connections, Least Bandwidth) to configure GLB and LB nodes and if the LB nodes are deployed on a different NetScaler instance.
- If site persistence is required.

Using StyleBooks to Configure GLB

You can use the Multi-cloud GLB StyleBook to configure GLB configurations on NetScaler instances that are provisioned in your data centers. Make sure that you have configured the site IP address on the NetScaler GLB instance in each data center.

You can also use this StyleBook to create a parent site that accepts child sites that you might add later in the GLB nodes. To configure multi-cloud GLB configuration on NetScaler instances.

1. Navigate to **Applications** > **Configuration**, and click **Create New**.
2. The **Choose StyleBook** page displays all the StyleBooks available for your use in the NetScaler Console. Scroll down and select **Multi-cloud GLB StyleBook**.

   The Multi-cloud GLB StyleBook is used to configure GLB for an application that is deployed in multiple clouds and on-premises sites. The StyleBook appears as a user interface page on which you can enter the values for all the parameters defined in this StyleBook.

   NOTE

   The terms data center and sites are used interchangeably in this document.

3. Set the following parameters:

   - **Application Name**. Enter the name of the application deployed on the GLB sites.
   - **GLB Algorithm**. Choose the global load balancing algorithm (method) for selecting the site that serves a client. The options that are available in the drop-down list box are LEASTCONNECTION, LEASTBANDWIDTH, LEASTPACKETS, ROUNDROBIN, STATICPROXIMITY, SOURCEIPHASH, and RTT.
   - **Geo Database File**. If you selected STATICPROXIMITY as the GLB algorithm, enter the complete path and name of the database file that contains the static proximity data. Make sure the database file is present on all GLB NetScaler instances at the specified location. Alternatively, you can retain the default file.
   - **Protocol**. Select the application protocol of the deployed application from the drop-down list box.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Persistence Settings**. Persistence configured on a virtual server maintains the states of connections on the servers represented by that virtual server (for example, connections used in e-commerce). Persistence overrides the load balancing methods once the virtual server is selected. If persistence configuration is applied to a service that is DOWN, the instance uses the load balancing methods to select a new service, and the new service becomes persistent for subsequent requests from the client.
- **Persistence Type**. Select the persistence type to use for this application. For example, if you select persistence as SOURCEIP, after the initial selection of the site hosting the application, all subsequent requests from the same client are sent to that site for access to the application's services.
- **Persistence Timeout**. If you selected SOURCEIP as the persistence type, enter the number of minutes before the persistence session expires after the last client request. The range is from 2 to 1440 minutes. The minutes are resolved in seconds.

4. **Spillover Settings**. Configure the spillover feature to forward the spillover connections to a secondary or backup virtual server when, for example, the connection limit or bandwidth limit of the primary virtual server has reached the threshold value.

   - **Spillover Method**. From the drop-down list box, select the method of spillover. For example, CONNECTION spillover method monitors the number of connections that are active on the primary server. If the spillover threshold is reached for this method, new connections are diverted to the first available virtual server in the backup chain. The HEALTH spillover method allows you to spillover if the threshold drops below a configured threshold. For example, less than 70%.

     NOTE

     Except HEALTH spillover method, other methods are applicable only when NetScaler is used as load balancer instance.

   - **Spillover Threshold.** Enter a threshold value for the spillover method that you have selected.
   - **Spillover Persistence.** Enable Spillover Persistence if you want the backup virtual server to continue to process the requests it receives, even after the load on the primary falls below the threshold.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Spillover Persistence Timeout**. Configure the time period for which Spillover persistence is in effect. The minimum value is 2 minutes and the maximum value is 1440 minutes. The minutes are resolved in seconds.

5. **Persistence/Spillover Persistence ID**. If you have selected SOURCEIP as persistence type or if Spillover persistence is enabled, enter a unique number to identify the same domain on all the GLB appliances. The range is from 1 to 65535.

   - **Health Check of GLB service end points (Optional)**
   - **Health Check Type**. From the drop-down list box, select the type of probe used for checking the health of the load balancer VIP address that represents the application on a site.
   - **Secure Mode**. (Optional) Select **Yes** to enable this parameter if SSL based health checks are required.
   - **HTTP Request**. (Optional) If you selected HTTP as the health-check type, enter the full HTTP request used to probe the VIP address.
   - **List of HTTP Status Response Codes**. (Optional) If you selected HTTP as the health check type, enter the list of HTTP status codes expected in responses to HTTP requests when the VIP is healthy.

6. **GLB Domain Names**. This section allows you to configure the list of DNS domain names associated with this application. Click the plus icon (**+**) to create a DNS domain name for the application.
7. **GLB Sites**. This section allows you to configure the list of sites on which this application is deployed.

   The GLB site is the top-level entity for the GLB communications. The information specified when configuring the site is used for linking local sites to remote sites and sharing monitoring data by using the Citrix Metrics Exchange Protocol (MEP). The IP address is owned by the GLB NetScaler instance and uses TCP port 3009. The GLB Sites section in the StyleBook allows you to specify as many GLB sites as needed.

   Click the plus icon (**+**) to add sites.

   - **Site Name**. Enter the name of the site.
   - **Site IP Address**. Enter the IP address that the site uses as its source IP address when exchanging metrics with other sites. This IP address is assumed to be already configured on the GLB instance in each site.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Site Public IP Address**. (Optional) Enter the Public IP address of the site that is used to exchange metrics, if that site's IP address is NAT'ed.

8. **Child Sites**. Click the plus icon (+) to configure the required child sites.

   - **Child Site name**. Enter the name of the site.
   - **Child Site IP Address**. Enter the IP address of the child site. Here, use the private IP address or SNIP of the NetScaler node that is being configured as a child site.
   - **Site Public IP Address**. (Optional) Enter the Public IP address of the site that is used to exchange metrics, if that site's IP address is NAT'ed.

9. **Services Site Persistence**. Select the type of persistence used from the drop-down list box to be used for the GLB services on the site.

   - Select ConnectionProxy to allow the site to create a connection to the GLB site that inserted the site cookie, proxy the client request to the original site, receive a response from the original GLB site, relay the response back to the client, and close the connection.
   - Select `HTTPRedirect` to allow the site to redirect the request to the site that originally inserted the cookie. For more information on persistence, see Configuring Persistent Connections.

10. **Active GLB Services**: This section allows you to configure the list of active services on the sites where the application is deployed.

    Service IP. Enter the IP address of the GLB service on this site.

    - **Service Public IP Address**. If the virtual IP address is private and has a public IP address NAT'ed to it, specify the public IP address.
    - **Service Port**. Enter the port of the GLB service on this site.
    - **Service Weight**. Enter the weight that is assigned to the GLB service.

    NOTE

    You can assign relative weights to the services, depending on the percentage of traffic that needs to be sent to the cloud and the percentage of traffic that must be handled on-premises. For example, if you have assigned a weight of 3 to the cloud-based GLB service and 7 to the on-premises GLB service, 30% of the traffic is directed to the cloud and 70% is handled on-premises.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Site Name**. Enter the name of the site on which the GLB service is located.
- **Site Prefix**. Enter a prefix for the site on which the GLB service is configured. This is applicable when site persistence is enabled and the method is `httpredirect`. The site prefix value must be unique across all the GLB services of an application.
- **Max Client Connections**. Enter the maximum client connections that are configured in the GLB service, if you have selected DYNAMICCONNECTION as a spillover method in **Spillover Persistence** settings. If you do not provide a value, by default the system assigns a number to the maximum client connections that can be configured.

11. **Passive GLB Services**: This section allows you to configure the list of passive services on the sites where the application is deployed with an active-passive topology. Provide information for all the backup GLB services similar to the information that you provided for active GLB services.
12. Click **Target Instances** and select the NetScaler instances configured as GLB instances on each site on which to deploy the GLB configuration.
13. Click **Create** to create the GLB configuration on the selected NetScaler instances. You can also click **Dry Run** to check the objects that would be created in the target instances. The StyleBook configuration (config pack) that you have created appears in the list of configurations on the Configurations page. You can examine, update, or remove this configuration (config pack) by using the NetScaler Console GUI.

Using StyleBooks to Configure GLB on NetScaler LB Nodes

You can use the **Multi-cloud GLB StyleBook for LB Node** if you are using the metric-based GLB algorithms (Least Packets, Least Connections, Least Bandwidth) to configure GLB and LB nodes and if the LB nodes are deployed on a different NetScaler instance.

You can also use this StyleBook to configure additional child sites for an existing parent site. This StyleBook configures one child site at a time. So, create as many configurations (config packs) from this StyleBook as there are child sites. The StyleBook applies the GLB configuration on the child sites. You can configure a maximum of 1024 child sites.

NOTE

Use Multi-cloud GLB StyleBook to configure the parent sites.

This StyleBook makes the following assumptions:

- A SNIP address or a GLB site IP address is configured.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The required firewall and security groups are configured in the cloud service providers.

Configuring a Child Site in a Parent-Child Topology by using Multi-cloud GLB StyleBook for LB Node

1. Navigate to **Applications** > **Configuration**, and click **Create New**.
2. The **Choose StyleBook** page displays all the StyleBooks available for your use in NetScaler Console. Scroll down and select **Multi-cloud GLB StyleBook for LB Node.**

   The StyleBook appears as a user interface page on which you can enter the values for all the parameters defined in this StyleBook.

   NOTE

   The terms data center and sites are used interchangeably in this document.

3. Set the following parameters:

   - **Application Name**. Enter the name of the GLB application deployed on the GLB sites for which you want to create child sites.
   - **Protocol**. Select the application protocol of the deployed application from the drop-down list box.
   - **LB Health Check (Optional)**

     - **Health Check Type**. From the drop-down list box, select the type of probe used for checking the health of the load balancer VIP address that represents the application on a site.
     - **Secure Mode**. (Optional) Select **Yes** to enable this parameter if SSL based health checks are required.
     - **HTTP Request**. (Optional) If you selected HTTP as the health-check type, enter the full HTTP request used to probe the VIP address.
     - **List of HTTP Status Response Codes**. (Optional) If you selected HTTP as the health check type, enter the list of HTTP status codes expected in responses to HTTP requests when the VIP is healthy.

4. Configuring parent site.

   Provide the details of the parent site (GLB node) under which you want to create the child site (LB node).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Site Name**. Enter the name of the parent site.
- **Site IP Address**. Enter the IP address that the parent site uses as its sourceIP address when exchanging metrics with other sites. This IP address is assumed to be already configured on the GLB node in each site.
- **Site Public IP Address**. (Optional) Enter the Public IP address of the parent site that is used to exchange metrics, if that site's IP address is NAT'ed.

5. Configuring child site.

   Provide the details of the child site.

   - **Site name**. Enter the name of the site.
   - **Site IP Address**. Enter the IP address of the child site. Here, use the private IP address or SNIP of the NetScaler node that is being configured as a child site.
   - **Site Public IP Address**. (Optional) Enter the Public IP address of the child site that is used to exchange metrics, if that site's IP address is NAT'ed.

6. Configuring active GLB services (optional)

   Configure active GLB services only if the LB virtual server IP address is not a public IP address. This section allows you to configure the list of local GLB services on the sites where the application is deployed.

   - **Service IP**. Enter the IP address of the load balancing virtual server on this site.
   - **Service Public IP Address**. If the virtual IP address is private and has a public IP address NAT'ed to it, specify the public IP address.
   - **Service Port**. Enter the port of the GLB service on this site.
   - **Site Name**. Enter the name of the site on which the GLB service is located.

7. Click **Target Instances** and select the NetScaler instances configured as GLB instances on each site on which to deploy the GLB configuration.
8. Click **Create** to create the LB configuration on the selected NetScaler instance (LB node). You can also click **Dry Run** to check the objects that would be created in the target instances. The StyleBook configuration that you have created appears in the list of configurations on the Configurations page. You can examine, update, or remove this configuration by using the NetScaler Console GUI.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Orchestration

The NetScaler Console orchestration features enable you to manage container orchestration platforms that are integrated with NetScaler. You can monitor and manage the Kubernetes cluster used for service graph.

The following topics help you manage orchestration:

- Kubernetes

Manage the Kubernetes cluster for Service Graph

Kubernetes (K8s) is an open source container orchestration platform that automates the deployment, scaling, and management of cloud-native applications.

NOTE

- NetScaler Console supports the visibility of clusters for Service graph with Kubernetes version 1.14–1.23.

You can specify the following aspects of Kubernetes integration in NetScaler Console:

- **Cluster** – You can register or unregister Kubernetes clusters for which NetScaler Console monitors all microservices and populates the Service graph. When you register a cluster in NetScaler Console, specify the Kubernetes API server information. Then, select an agent that can reach the Kubernetes cluster.

Before you begin

To monitor and visualize your microservices on Kubernetes clusters and get started on Service Graph, ensure you have:

- Kubernetes cluster in place.
- The agent installed and configured to enable communication between NetScaler Console and Kubernetes cluster or managed instances. You can use the managed instances that are present in your data center or cloud.
- Kubernetes cluster registered in NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure NetScaler agent to register with Kubernetes cluster

To enable communication between Kubernetes cluster and NetScaler Console, you must install and configure an agent. You can deploy an agent on the following platforms:

- Hypervisor (ESX, XenServer®, KVM, Hyper-V)
- Public Cloud Services (such as Microsoft Azure, AWS)

Follow the procedure to configure an agent.

NOTE

You can also use an existing agent if one is already deployed.

Configure the NetScaler Console with a secret token to manage a Kubernetes cluster

For NetScaler Console to be able to receive events from Kubernetes, you need to create a service account in Kubernetes for NetScaler Console. And, configure the service account with the necessary RBAC permissions in the Cluster.

1. Create a service account for NetScaler Console. For example, the service account name can be `citrixadm-sa`. To create a service account, see Use Multiple Service Accounts.
2. Use the `cluster-admin` role to bind the NetScaler Console account. This binding grants a `ClusterRole` across the cluster to a service account. The following is an example command to bind a `cluster-admin` role to the service account.

   ```
   kubectl create clusterrolebinding citrixadm-sa-admin --
   clusterrole=cluster-admin --serviceaccount=default:citrixadm-sa
   ```

   After binding the NetScaler Console account to the `cluster-admin` role, the service account has the cluster-wide access. For more information, see `kubectl` create `clusterrolebinding`.
3. Obtain the token from the created service account.

   For example, run the following command to view the token for the `citrixadm-sa` service account:

   ```
   kubectl describe sa citrixadm-sa
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Run the following command to obtain the secret string of the token:

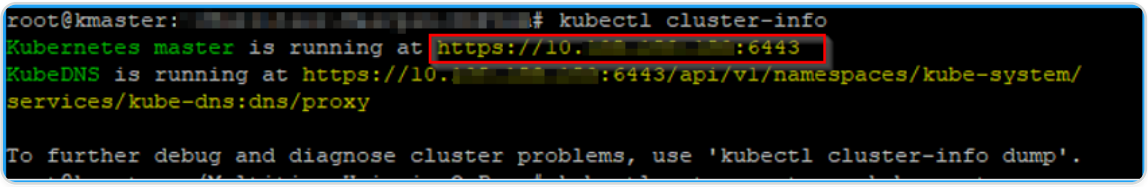
```
kubectl describe secret <token-name>
```

Add the Kubernetes cluster in NetScaler Console

After you configure an agent and configure static routes, you must register the Kubernetes cluster in NetScaler Console.

To register the Kubernetes cluster:

1. Log on to NetScaler Console with administrator credentials.
2. Navigate to **Orchestration** > **Kubernetes** > **Cluster**. The Clusters page is displayed.
3. Click **Add**.
4. In the **Add Cluster** page, specify the following parameters:
   a. **Name** - Specify a name of your choice.
   b. **API Server URL** - You can get the API Server URL details from the Kubernetes Master node.
      i. On the Kubernetes master node, run the command `kubectl cluster-info`.



      ii. Enter the URL that displays for **"Kubernetes master is running at."**
   c. **Authentication Token** - Specify the authentication token string obtained while you configure NetScaler Console to manage a Kubernetes cluster. The authentication token is required to validate access for communication between Kubernetes cluster and NetScaler Console. To generate an authentication token:
      i. On the Kubernetes master node, run the following commands:

```
kubectl describe secret <token-name>
```

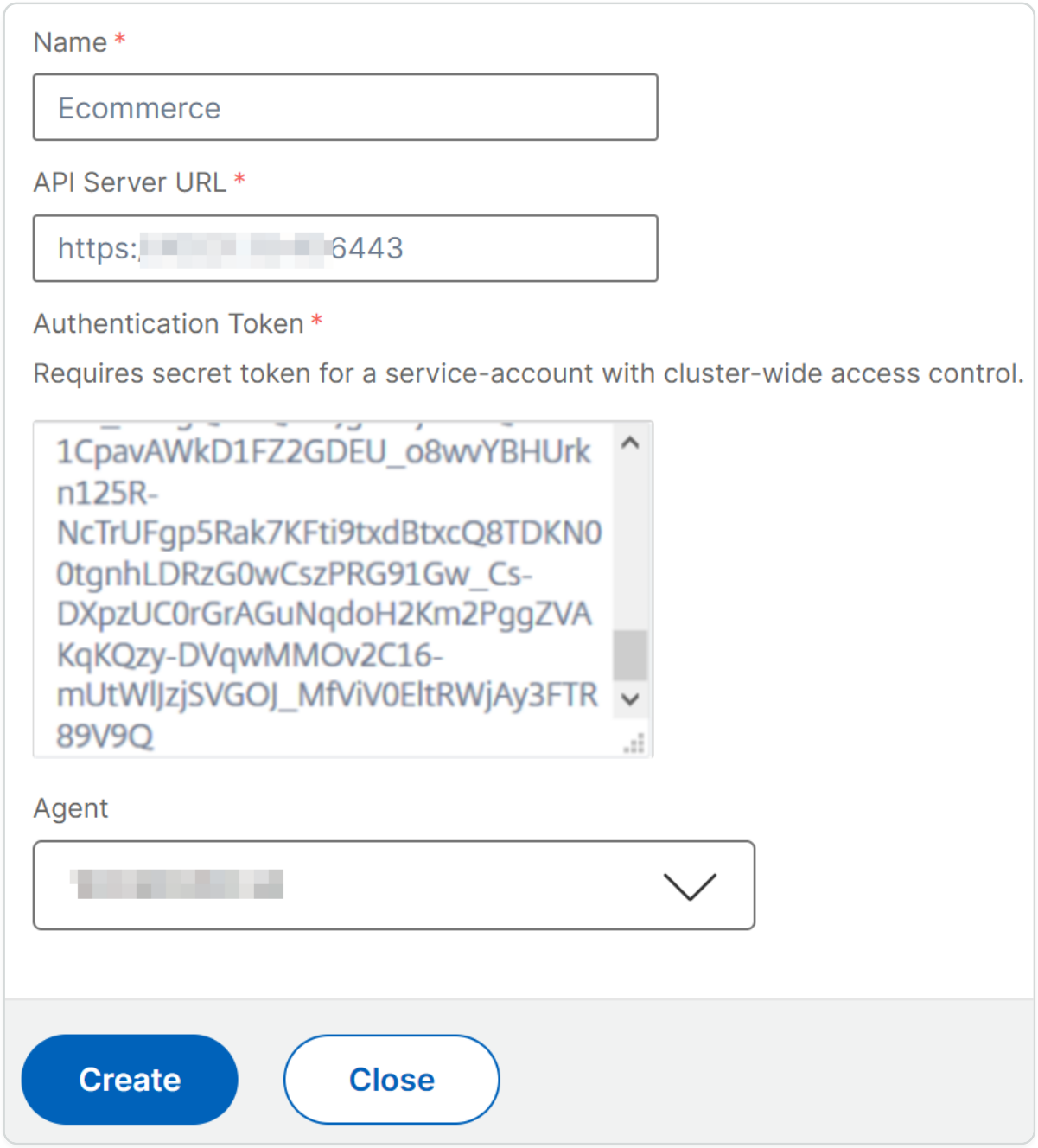
      ii. Copy the token that is generated and paste it as the Authentication Token

      For more information, see Kubernetes documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. Select the agent from the list.

e. Click **Create**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler® licenses

The NetScaler Console licensing features enable you to manage and monitor your NetScaler licenses. You can activate and manage licenses, apply best practices, configure Flexed licensing, view license dashboards and reports, and manage legacy licenses.

The following topics help you manage NetScaler licenses:

- License Activation Service
- Best Practices
- License Management
- Minimum and maximum capacity checkout
- NetScaler agent behavior
- Flexed licensing
- Configure license
- License dashboard
- License reporting
- Transition to Flexed licensing
- Scenarios for Flexed or Pooled license expiry and connectivity issues behavior
- Configure NetScaler Console server only as the Flexed or Pooled license server
- Legacy licenses

© 1997–2026 Citrix Systems, Inc. All rights reserved.

License Activation Service

IMPORTANT:

File-based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (Citrix Platform License/Universal Hybrid Multi-Cloud), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Supported from early September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Note: LAS support for Console on-prem is from release 14.1-51.x onwards. However, file-based licensing is deprecated as of April 15 2026 from Console on-prem releases 14.1-51.x onwards and 13.1-60.x onwards. If you upgrade to Console on-prem release 14.1-51.x or release 13.1-60.x or later, you can continue using file-based licensing until 15th April 2026. However you must upgrade to Console on-prem release 14.1-51.x or later, and switch to LAS before 15th April 2026 because Console on-prem 13.1 does not support LAS.

All the other forms of legacy NetScaler licenses such as NetScaler virtual CPU licensing (Pooled vCPU), NetScaler VPX Check-In and Check-Out (CICO), perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS-based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don’t apply where prohibited by law or regulation.
Before starting your transition to LAS, we recommend reading LAS for NetScaler. This ensures that you understand the general prerequisites, the supported or unsupported license types, the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

accurate workflow for your specific license and deployment types along with other important information.

License Activation Service (LAS) is a cloud-based licensing solution that replaces traditional file-based licensing. LAS introduces new modules to activate Citrix and NetScaler products, providing a streamlined, modern approach to license management.

NOTES:

- LAS is a license mechanism, not a license type.
- File-based licensing refers to the older method of licensing using manual entitlements. In this document, ‘File-based licensing’ and ‘manually managed entitlements’ are used interchangeably as they describe the same concept.

The following are the key benefits of LAS:

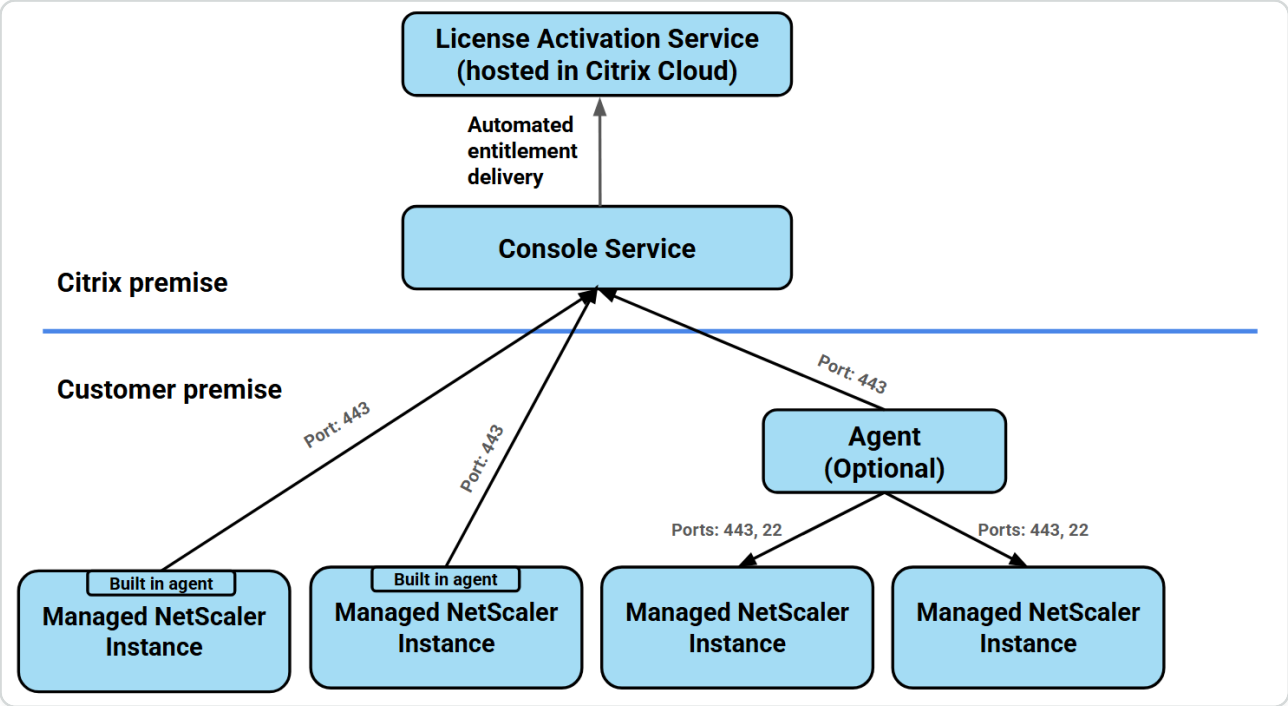
- Automated entitlement delivery through an entitlement blob.
- An external agent for licensing communication is optional.
- LAS eliminates the need for Z-Cap software license files on the NetScaler MPX™ and SDX instances.

NOTE:

If you are new to NetScaler Console, begin with Getting Started.

The following diagram is for LAS with Console service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Prerequisites

To use LAS, ensure that you have completed the following prerequisites:

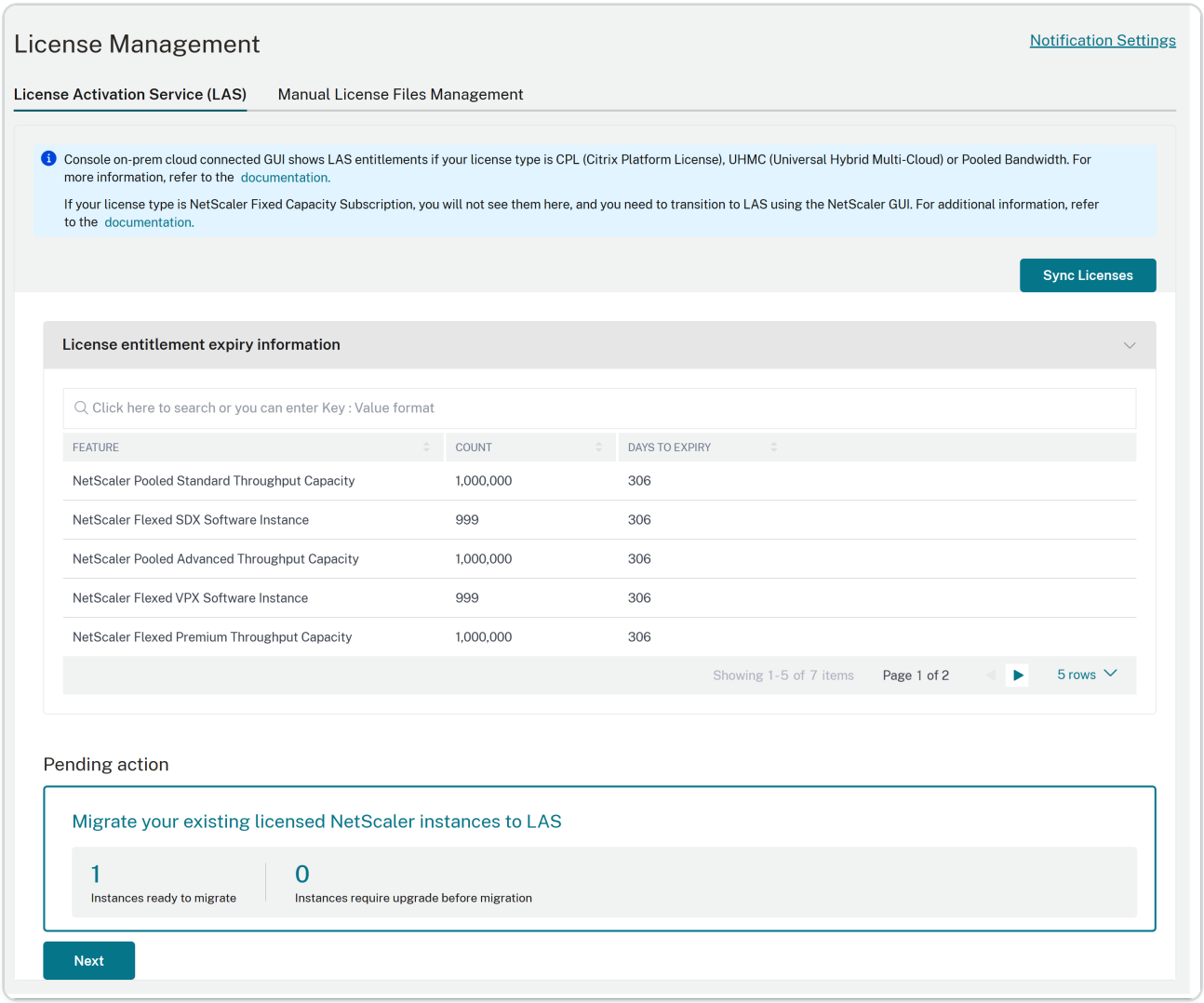
- You must have a valid Citrix Cloud account. For more information about existing cloud accounts or to onboard new cloud accounts, see Account Management.
- The Organization ID (Org ID) linked to the Citrix Cloud account used for the LAS activation workflow must possess valid purchased entitlements. To view the current entitlements, see Entitlements.
- The NetScaler instance is running a LAS-compatible version.
- The NetScaler instance is added as a managed instance in NetScaler Console.

Automatic enablement and compatibility

LAS is automatically enabled on the NetScaler Console service. Once enabled, all NetScaler Flexed and Pooled license entitlements appear in the NetScaler Console GUI.

You can view your entitlements by navigating to **NetScaler Licensing > License management > License Activation Service (LAS)** tab.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTES:

- The new Sync Licenses option allows you to manually trigger this synchronization on demand, ensuring entitlements are up to date immediately.
- The default frequency for entitlement synchronization is once every 8 hours if LAS entitlements have not been synchronized with NetScaler Console service and once every 24 hours there after. For on-demand synchronization, click `Sync Now`.

NetScaler version compatibility for LAS

To use LAS, your NetScaler instances must be running one of the following minimum versions:

- NetScaler: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console service: Supported from early September 2025.

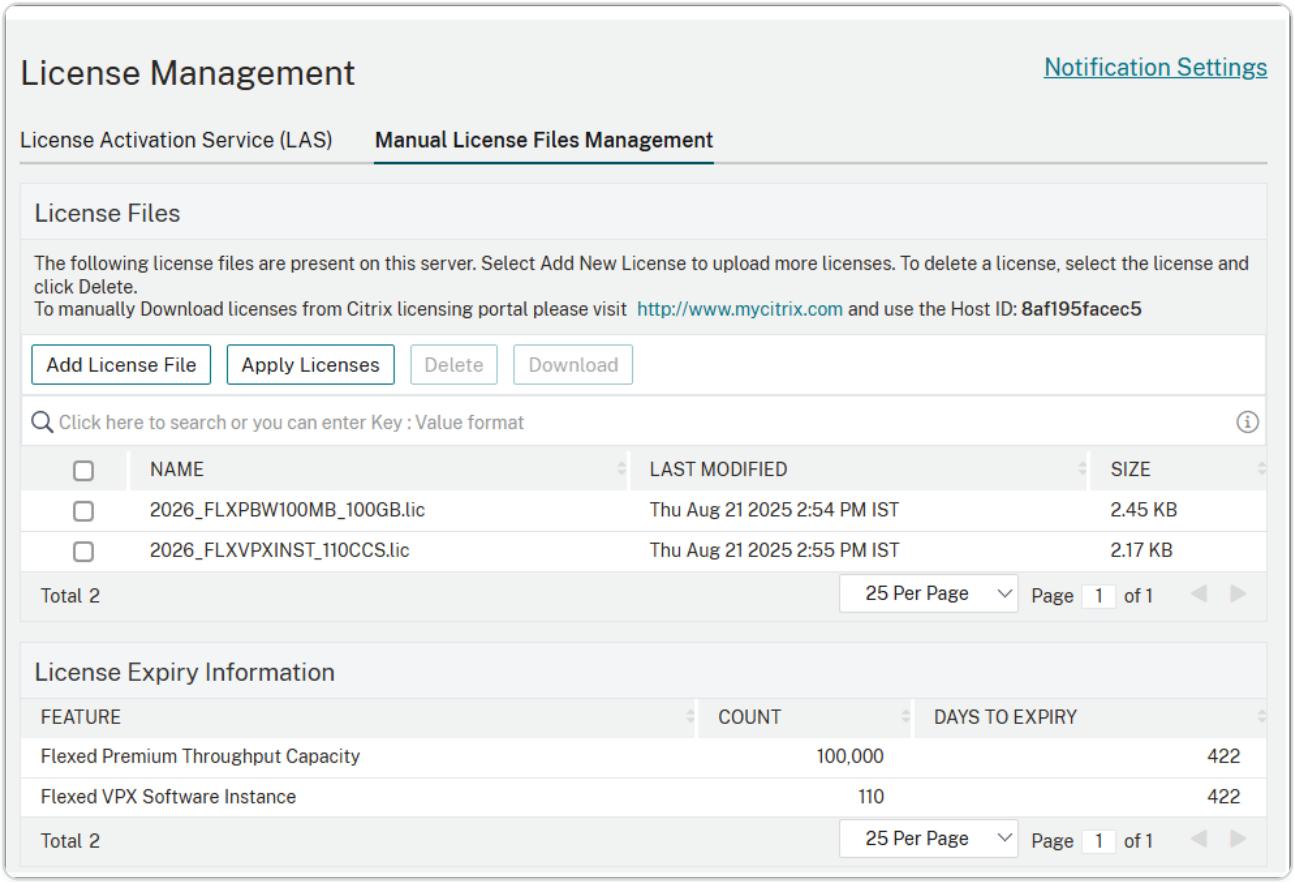
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler Console on-prem: 14.1-51.x

NOTES:

- To use LAS, ensure that you have completed the following prerequisites:
  - The NetScaler instance is running a LAS-compatible version.
  - The NetScaler instance is added as a managed instance in NetScaler Console.
- For SDX appliances, upgrade the Management Service (SVM) to a LAS-supported build and transition to LAS-based licensing. The VPX build version does not impact LAS compatibility.

With file-based licensing, your applied entitlements and configurations are visible under **NetScaler Licensing > License management> Manual License File management**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

LAS supports Flexed licensing (UHMC/CPL), Pooled bandwidth licensing, and Fixed-term bandwidth licensing. All other forms of legacy NetScaler licenses, such as Pooled vCPU and CICO, are not supported with LAS.

Transition to LAS

When you navigate to **NetScaler Licensing > License management > License Activation Service (LAS)**, the NetScaler GUI dynamically updates based on the compatibility of your NetScaler instances.

A message appears in the GUI if you do not have any NetScaler instances that are on LAS-compatible versions. The message prompts you to upgrade or add a NetScaler instance.

NOTE:

If some of your NetScaler instances are upgraded to a compatible version, you can use LAS for those specific instances.

When one or more NetScaler instances are compatible with LAS, they are categorized into one of two groups:

- License NetScaler instances with LAS
- Migrate the licensed NetScaler instances to LAS

The GUI adjusts dynamically depending on whether you are a first-time LAS user (with zero instances migrated) or an existing user (who has already moved some instances to LAS and is now adding more).

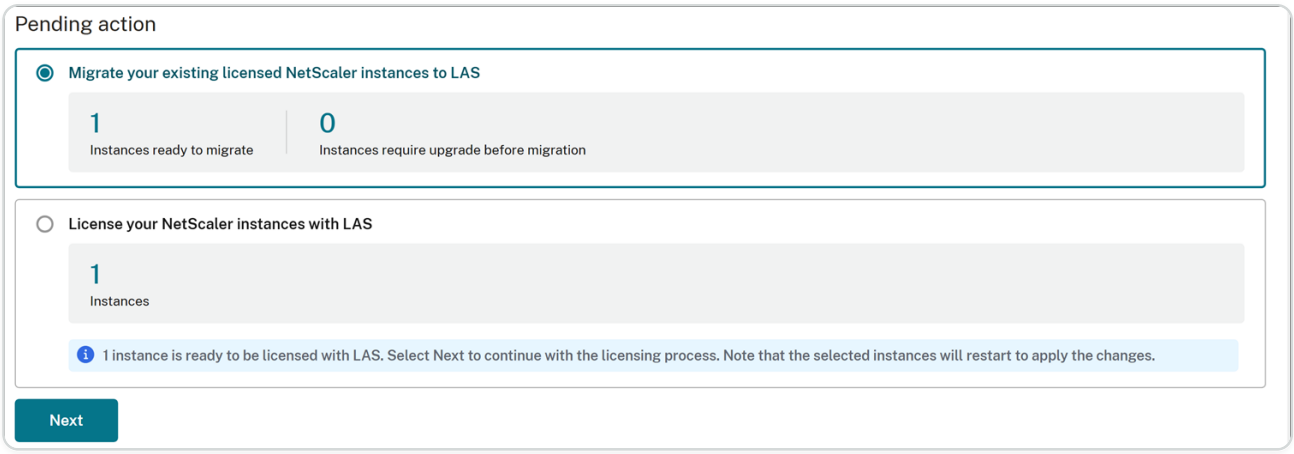
NOTE:

Delete the local file-based licenses on the SVM once licensing or migration to LAS is complete. The file-based licenses are located in the SVM folder `/mpsconfig/license` and must be deleted from this folder using the shell prompt. This note applies to the **License with LAS** and **Migrate to LAS** workflows for both first-time and existing users.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

First-Time LAS user

The following image is displayed for the first-time user:



License NetScaler instances with LAS

The **License NetScaler instances with LAS** section lists NetScaler instances that are currently unlicensed or that do not use a Flexed bandwidth or Pooled bandwidth file-based license.

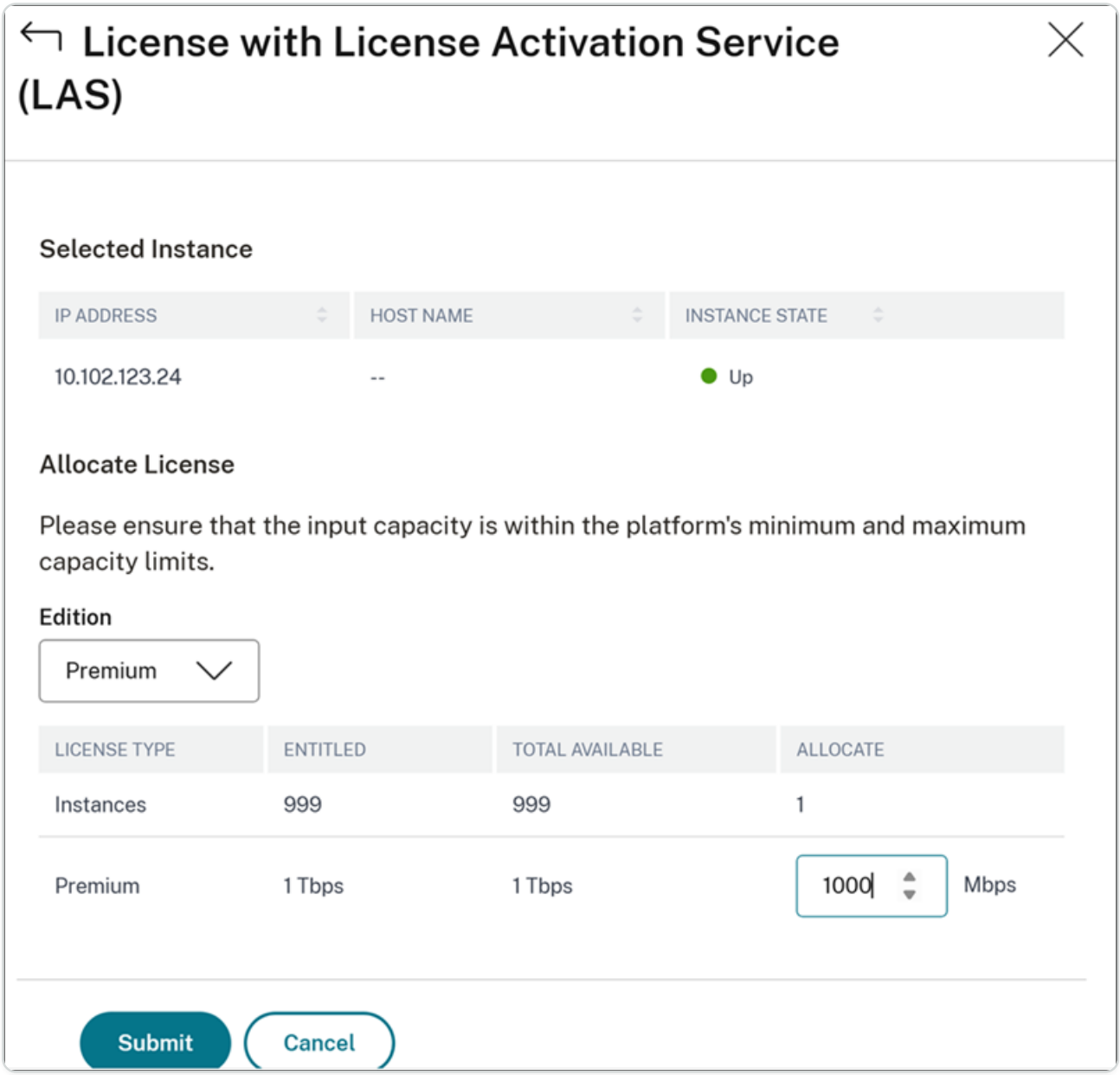
To license an instance, perform the following steps:

1. Select **License NetScaler instances with LAS**, and click **Next**.
2. Select an instance, and click **Continue**.
3. Enter the details and click **Submit**. Repeat this process for each instance.

NOTE:

The selected instances restart for the license to take effect, except for SDX instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Migrate existing licensed instances to LAS

The **Migrate your existing licensed instances to LAS** section lists all NetScaler instances with Flexed or Pooled file-based licenses. They are categorized as follows:

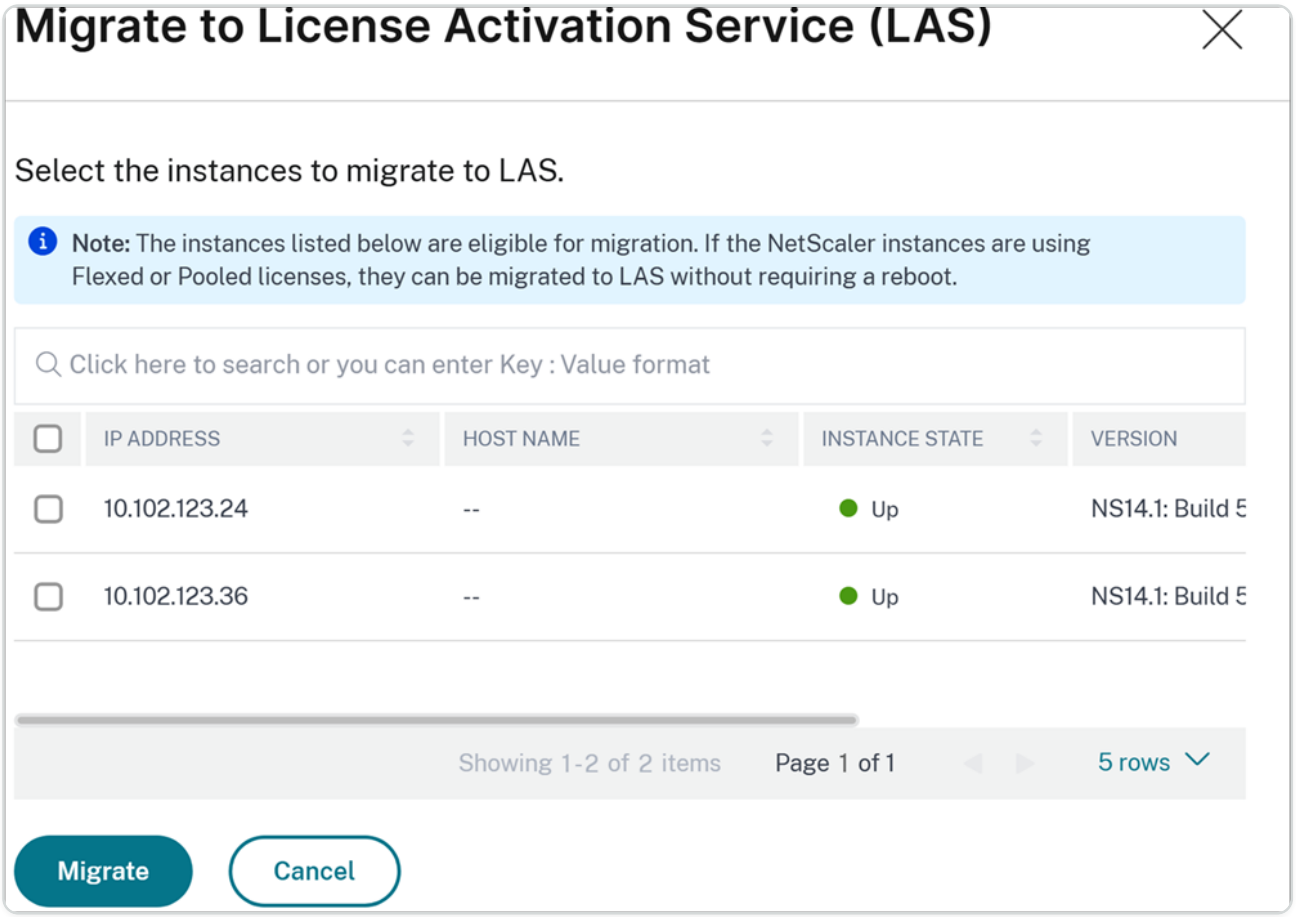
- **Instances ready to migrate:** Lists the instances that are on LAS-compatible versions or builds and are ready to be migrated to LAS.

To migrate, perform the following steps:

```
1.  Select **Migrate your existing licensed NetScaler instances to LAS**
and click **Next**.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Select the instances and click **Migrate**.



- **Instances require upgrade before migration:** List the instances that are to be upgraded to a compatible version or builds before migration.

  Prerequisite:

  To use LAS-based licensing, the edition of your NetScaler instance must match the edition of your Pooled or Flexed file-based license. Ensure that you change the instance's edition to match the new license before you begin the migration.

  a. Select **Migrate your existing licensed NetScaler instances to LAS**, click **Upgrade**.

  b. In **Upgrade NetScaler** page, select the instance and upgrade the instances to versions or builds compatible with LAS.

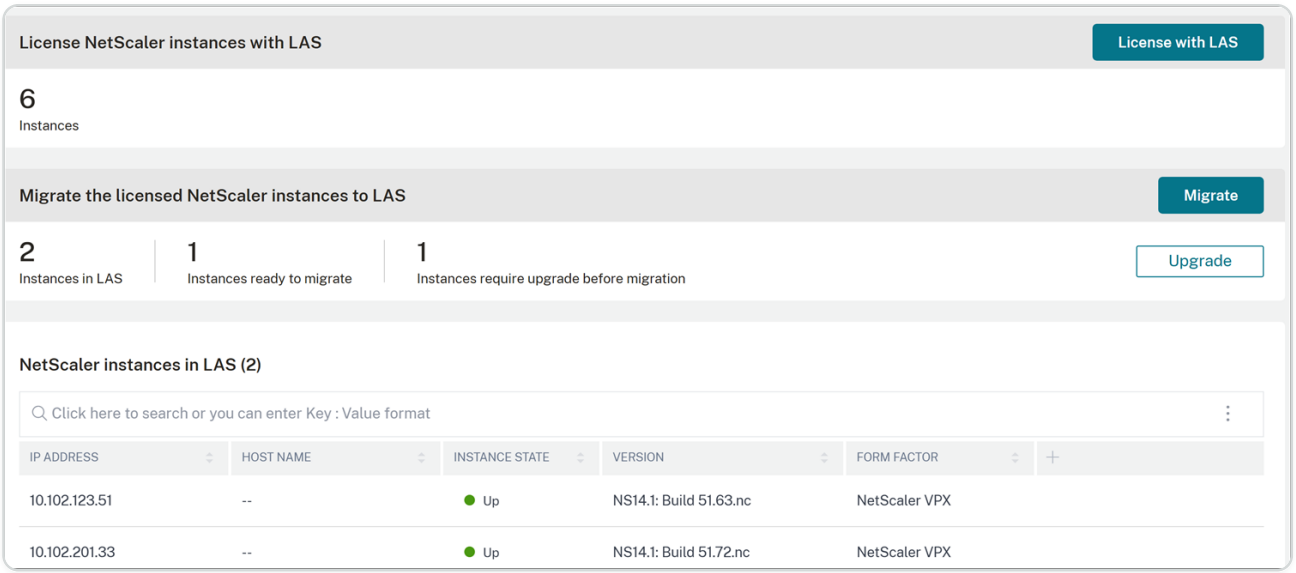
NOTE:

For NetScaler instances in the "Migrate to LAS" workflow and are transitioning from legacy file-based to LAS-based Pooled bandwidth or Flexed licensing, reboot is not required.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Existing LAS user

The following image is displayed for the existing user:



Note: To view the CPX instances licensed with LAS, see the Flexed Dashboard GUI. CPX instances are not listed under **NetScaler instance with LAS**.

License NetScaler instances with LAS

The **License NetScaler instances with LAS** section lists NetScaler instances that are currently unlicensed or use any license other than a Flexed bandwidth or Pooled bandwidth file-based license.

To license an instance, perform the following steps:

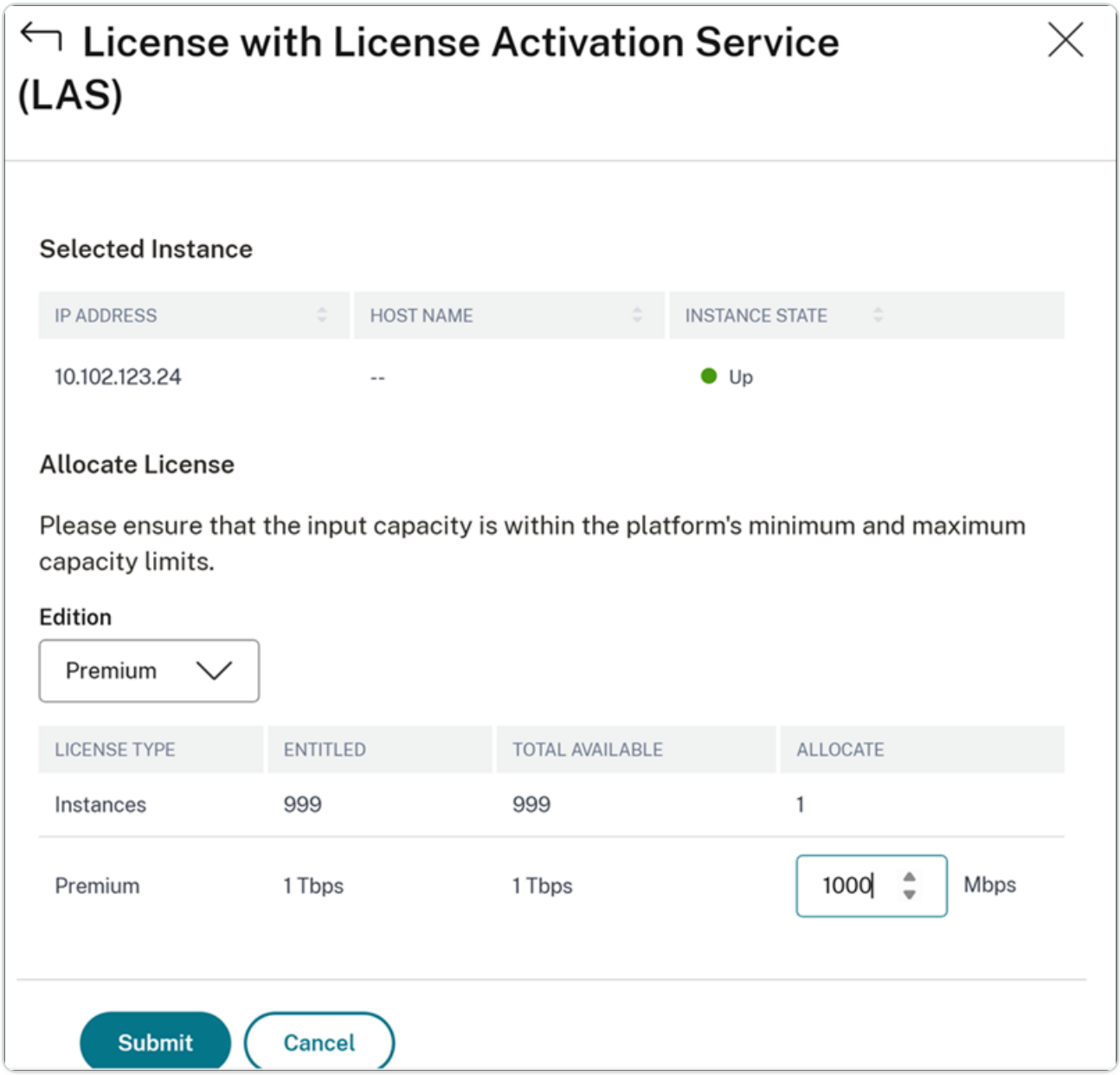
1. Under **License with License Activation Service (LAS)**, click **License with LAS**.
2. Select an instance, and click **Continue**.
3. Enter the details and click **Submit**.

   Repeat the steps for each NetScaler instance you want to license with LAS.

NOTE:

The selected instances restart for the license to take effect.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Migrate the licensed NetScaler instances to LAS

The **Migrate the licensed NetScaler instances to LAS** section lists all NetScaler instances with a Flexed or Pooled file-based license. They are categorized as follows:

- **Instances in LAS**: Lists the instances that are already using LAS-based licensing.
- **Instances ready to migrate**: Lists instances that are compatible instances ready for migration.

  To migrate, perform the following steps:

  a. Select **Migrate the licensed NetScaler instances to LAS**, click **Migrate**.

  b. Select one or more NetScaler instances, and migrate the selected instances to LAS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Instances require upgrade before migration:** Lists instances that are to be upgraded to a compatible version. To upgrade, perform the following steps:

  Prerequisite:

  To use LAS-based licensing, the edition of your NetScaler instance must match the edition of your Pooled or Flexed license. Ensure that you change the instance's edition to match the new license before you begin the migration.

  a. Select **Migrate the licensed NetScaler instances to LAS**, click **Upgrade**.
  b. Select one or more NetScaler instances, and upgrade the instances to a compatible version or build.

NOTE:

For NetScaler instances in the "Migrate to LAS" workflow and are transitioning from legacy file-based to LAS-based Pooled bandwidth or Flexed licensing, reboot is not required.

Information sent to LAS during LAS licensing workflow

This section details all information sent as part of the request for an activation blob to LAS during every initial request and each LAS activation blob refresh request. The following table summarizes the parameters sent to LAS during the licensing workflow.

PARAMETER	DESCRIPTION	NEED FOR IT IN LAS WORKFLOW
lsguid	Unique ID of Console service tenant	LAS binding parameter
lsid	Unique ID of Console service tenant	LAS binding parameter
pubkey	Public key of Console service deployment	Ensures that LAS has authorized this Console
ccid	Citrix Cloud ID that is used to onboard Console service	LAS binding parameter
lsbuild	Build version or sample value	LAS activation requirement

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	DESCRIPTION	NEED FOR IT IN LAS WORKFLOW
hostname	Console service hostname (POP name)	LAS activation requirement
lpeid	Unique ID of NetScaler that is activated.	LAS binding parameter
lpehostname	Hostname of NetScaler that is activated	LAS binding parameter
burnin_date	Software burn-in date of NetScaler	LAS binding parameter
products	The features that LAS validates to generate the activation license	LAS entitlement validation parameter

Best Practices for monitoring your LAS transitioned NetScaler Console service environment

This document focuses on the best practices that you can follow to monitor your NetScaler environments that use LAS. This document applies to deployments that use LAS with Console service.

Prerequisites

- Read the LAS for NetScaler page, including the FAQ for LAS with Console service.
- Read the License Activation Service and complete your LAS migration.
- Ensure that you set up the relevant notifications, and monitor the NetScaler GUI and CLI regularly.

NOTE:

We intend to make continuous improvements to notifications and keep this documentation updated accordingly.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Monitoring LAS activation blob expiry

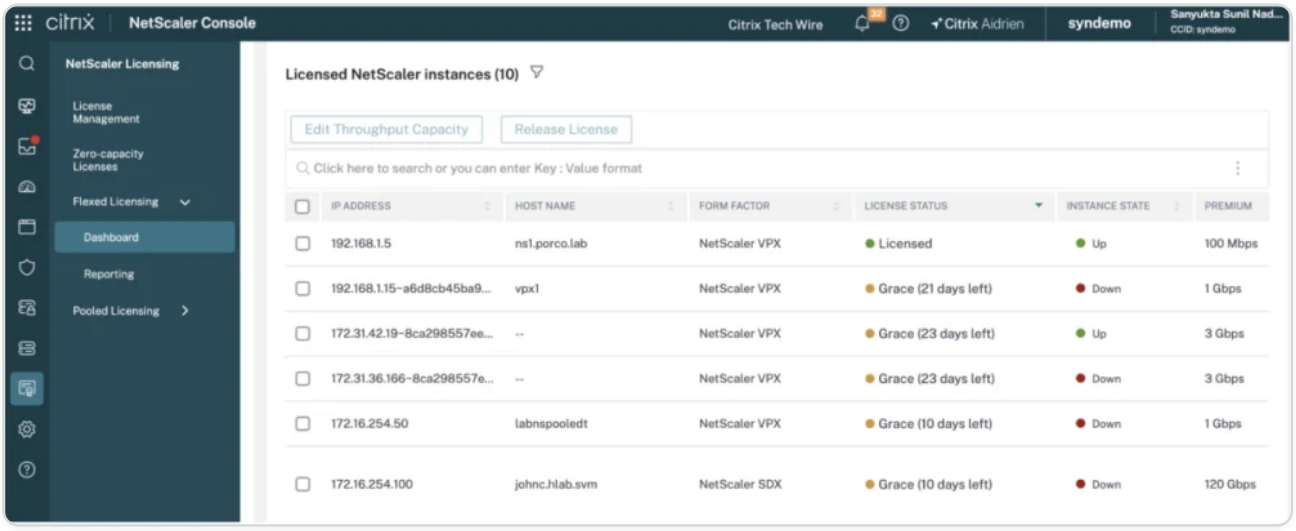
For NetScaler Console service, the LAS activation blob is provided directly by LAS to the NetScaler instances that use NetScaler Console service as their licensing server. The blob is valid for 30 days or until the license entitlement expires, whichever comes first and is refreshed every eight hours.

If connectivity between NetScaler and NetScaler Console service breaks, NetScaler Console service cannot refresh the NetScaler instance's LAS activation blob. NetScaler Console service retries every eight hours, and after three failed attempts (8 hours x 3 = 24 hours), NetScaler goes into **Grace** status. The NetScaler Console service GUI then shows such NetScaler instances in the grace status.

This section details the notifications triggered when a LAS activation blob is nearing expiry (less than 30 days), which indicates that the deployment requires attention. To resolve this, verify and repair any connectivity issues, or contact Citrix Support for assistance.

View NetScaler instances by using the GUI

To view NetScaler instances that are in grace status, navigate to **Console Service GUI > NetScaler Licensing > Flexed Licensing > Dashboard**.



View NetScaler instance status by using the CLI

To view NetScaler instances in **Grace** status and the remaining grace period duration, run the `sh licenseserver` command.

Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
> sh licenseserver

     License Server: 10.102.123.31 Status: Disconnected

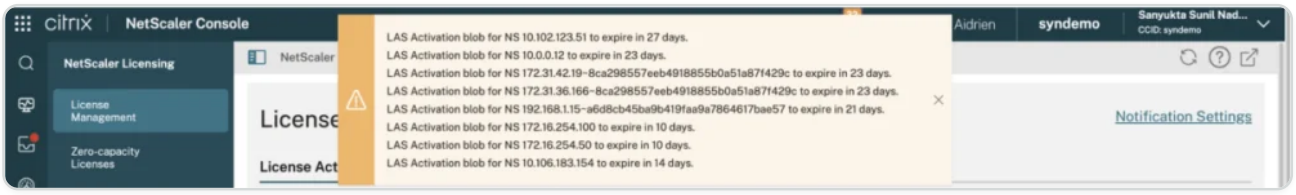
        Grace: Yes         Grace Time Left: 652

Done
```

Notifications

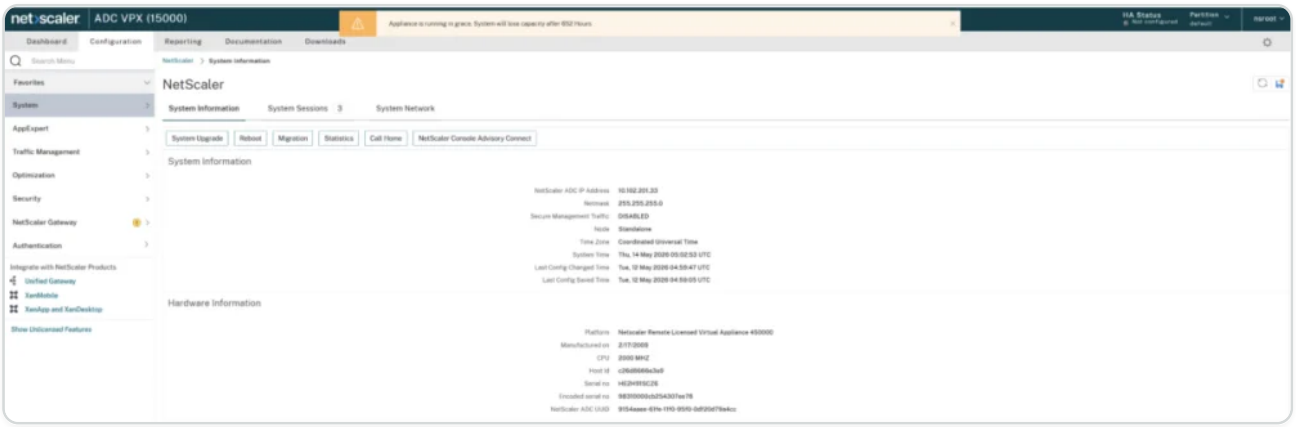
Banner on NetScaler Console service:

The NetScaler Console service GUI displays a banner listing NetScaler instances whose LAS activation blob expires in x days, where x is less than 30 days.



Banner on NetScaler GUI:

The NetScaler Console service GUI displays a banner if the NetScaler instance is in grace status.



SNMP traps generated by NetScaler for grace status:

If NetScaler instances are in grace status, NetScaler generates the following SNMP traps:

- `pooledLicenseGraceStarted`: Triggered when the instance has entered the grace period.
- `pooledLicenseGraceNormal`: Triggered when the grace period of 30 days ends, which means that the deployment is impacted and the instance becomes unlicensed.
- `pooledLicenseGracePeriodOver`: Triggered when the grace period is over.

Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
May 15 05:17:21 <local0.info> 10.102.201.33  05/15/2026:11:17:21 GMT  0-
PPE-2 : default SNMP TRAP_SENT 0 0 :  pooledLicenseGraceStarted
(nsPartitionName = default)

May 15 05:17:21 <local0.info> 10.102.201.33  05/15/2026:11:17:21 GMT  0-
PPE-2 : default SNMP TRAP_SENT 0 0 :  pooledLicenseGraceNormal
(nsPartitionName = default)

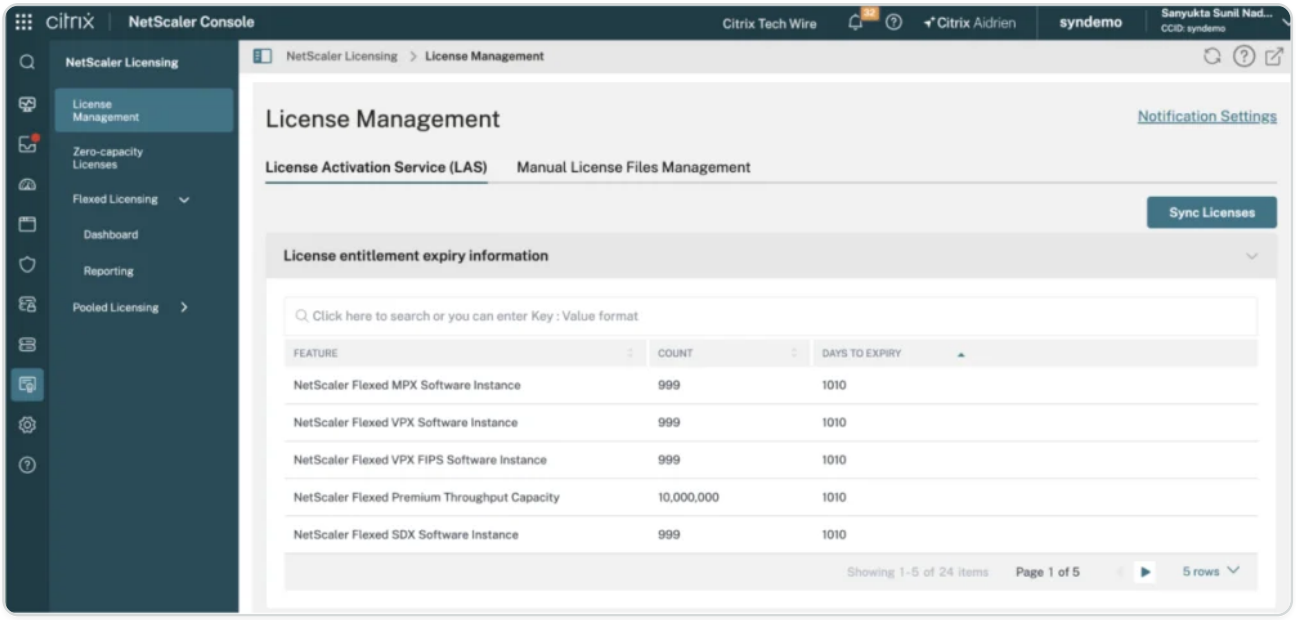
May 15 05:17:21 <local0.info> 10.102.201.33  05/15/2026:11:17:21 GMT  0-
PPE-2 : default SNMP TRAP_SENT 0 0 :  pooledLicenseGracePeriodOver
(nsPartitionName = default)
```

Monitoring license entitlement expiry

The **License entitlement expiry date** refers to the customer license entitlement or contract expiry date.

To view license entitlement expiry information by using the GUI, navigate to **Console Service GUI > NetScaler Licensing > License Management > LAS**.

The **Days to expiry** shows entitlement expiry date for the corresponding license.



Notifications

NetScaler Console service GUI banner:

The NetScaler Console service GUI shows a banner indicating that the license entitlement is nearing expiry in x days.

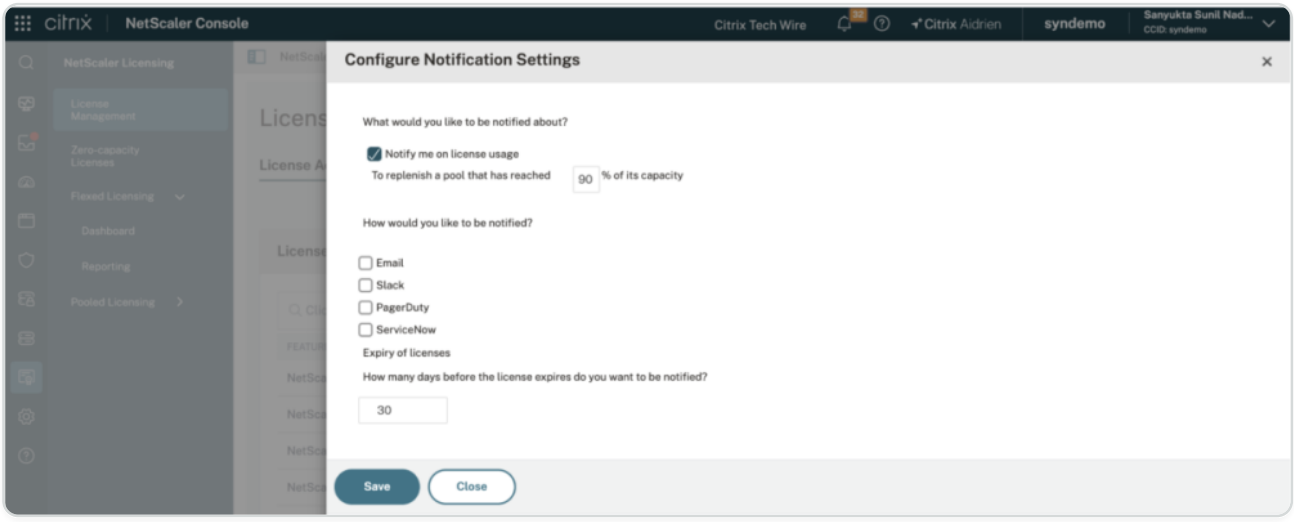
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Flexed Premium Throughput Capacity license entitlement of 1000000 Mbps expires in 14 days.
Flexed VPX FIPS Instance license entitlement of 999 instances expires in 14 days.
Flexed VPX Software Instance license entitlement of 999 instances expires in 14 days.
Flexed MPX Software Instance license entitlement of 999 instances expires in 14 days.
Flexed SDX Software Instance license entitlement of 999 instances expires in 14 days.

Email-based notifications:

To configure notifications for license entitlement expiry:

1. Navigate to **Console Service GUI > NetScaler Licensing > License Management > Notification Settings**.
2. Enter the required value in **How many days before the license expires do you want to be notified?**.



License management

IMPORTANT:

File-based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler versions that are LAS compatible are:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Supported from early September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Note: LAS support for Console on-prem is from release 14.1-51.x onwards. However, file-based licensing is deprecated as of April 15 2026 from Console on-prem releases 14.1-51.x onwards and 13.1-60.x onwards. If you upgrade to Console on-prem release 14.1-51.x or release 13.1-60.x or later, you can continue using file-based licensing until 15th April 2026. However you must upgrade to Console on-prem release 14.1-51.x or later, and switch to LAS before 15th April 2026 because Console on-prem 13.1 does not support LAS.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don’t apply where prohibited by law or regulation.

LAS-based license

With License Activation Service (LAS), the entitlements are automatically reflected in the NetScaler Console UI, so no manual action is required.

License server ports

The LAS uses port 443 for all licensing communication.

NOTE:

To use LAS, add your NetScaler instance as a managed instance.

License expiry information

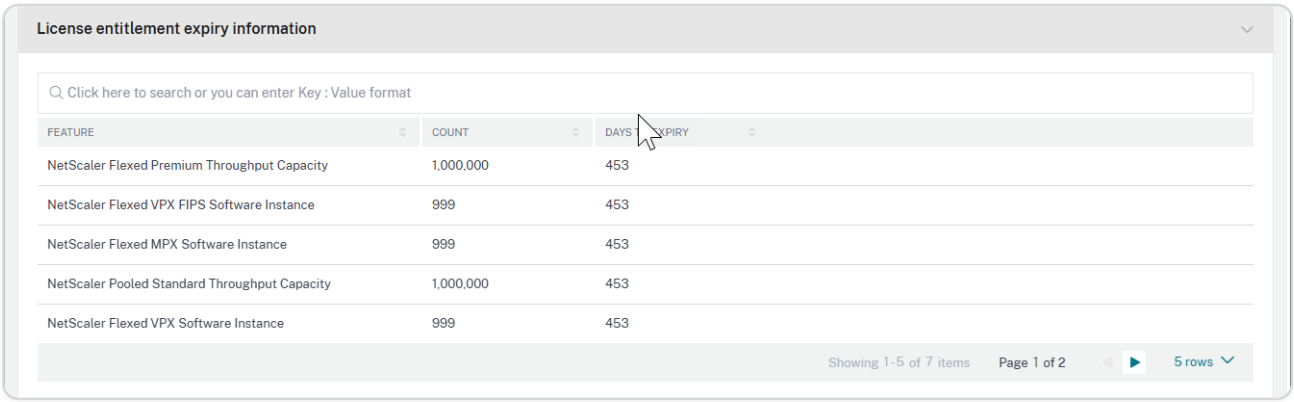
View license expiry

1. Navigate to **NetScaler Licensing > License Management**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. The **License entitlement expiry information** section provides details on licenses nearing expiration.

    - **Feature**: Type of license that is going to expire.
    - **Count**: Number of instances or Bandwidth (in Mbps) that are affected.
    - **Days to expiry**: Number of days before license expiry (contract end date).



NOTE:

Newly purchased Pooled or Flexed entitlements automatically appear in the **License entitlement expiry information** section.

License expiry behavior

When a license managed through the NetScaler Console expires, the associated NetScaler instance stops processing traffic, and its configuration might be lost.

Notification email and a pop-up banner on license end date

In the NetScaler Console GUI, a pop-up message appears related to the license end date. By default, you get a pop-up message in the GUI (every time after login) starting 30 days (default) before the license end date.

You can configure the number of days in **Notification settings > Expiry of license setting**.

As an administrator, you also receive a notification email for the license end date if email notification is configured in **Notifications settings**. A notification email is sent in the frequency of 60, 30, 20, and 10 days before the license end date.

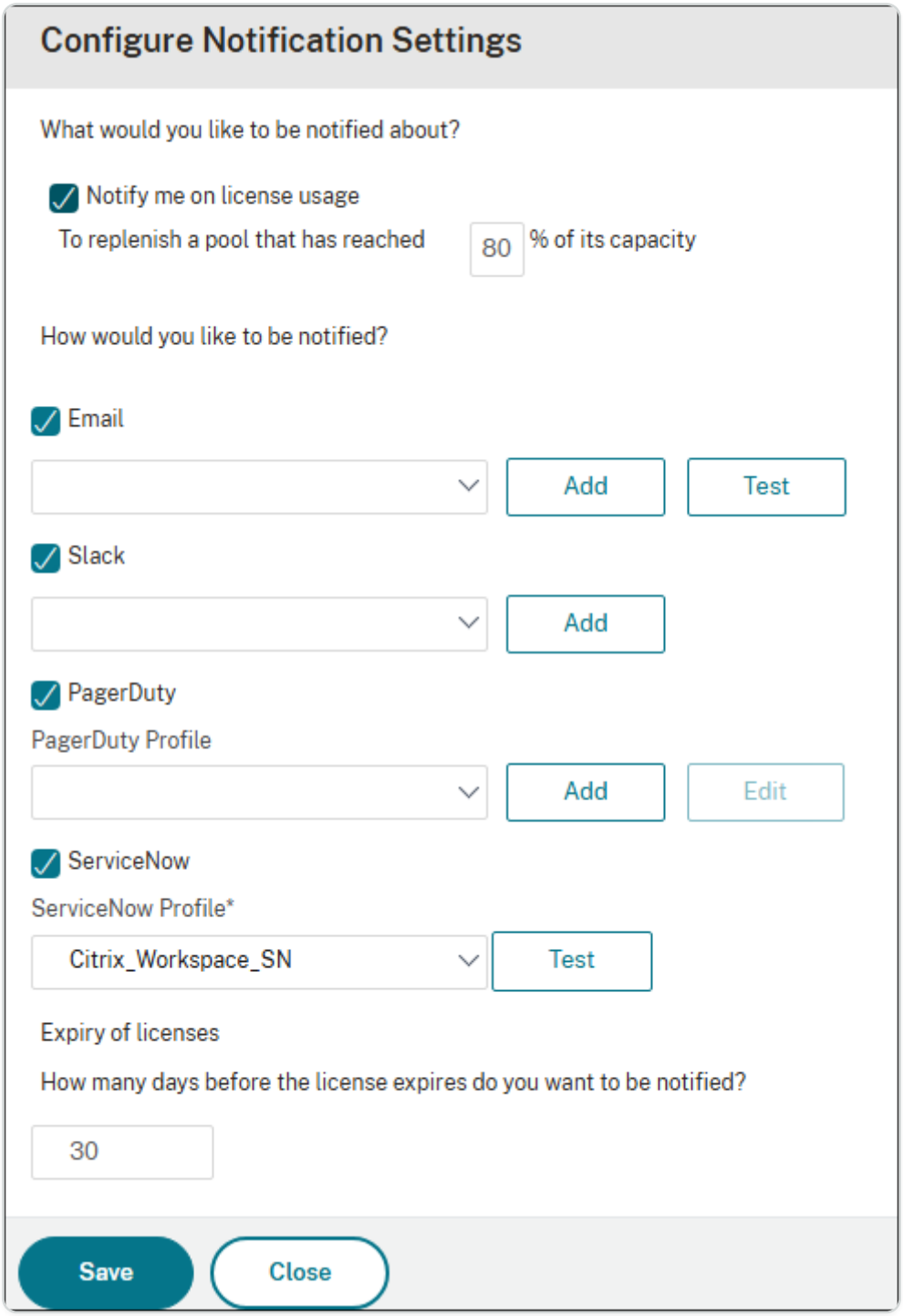
Notification settings

To set up notifications for expiring Flexed or Pooled licenses managed by LAS, follow these steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigate to **NetScaler Licenses > License Management > Notification Settings**.
2. In the **Notification Settings** section, select **Notify me on license usage**. Set the alert threshold as a percentage of flexed or pooled license capacity to be allocated to send a notification.
3. Choose the type of notification that you want to send when licenses reach the threshold, or are about to expire by selecting the appropriate checkbox. The notification types are as follows.
    - **Email**: Email profile or distribution list for sending notifications. For more information, see Create an email distribution list.
    - **Slack**: Slack profile details for sending notifications.
    - **PagerDuty**: PagerDuty profile for sending notifications.
    - **ServiceNow**: The Citrix ServiceNow profile is specified by default and is the only available option. For more information about creating these profiles, see Configure notifications
    - Select a notification type and click **Add** to add details. You can also test each notification system before saving your settings.
4. Specify the **Days to Expiry**, which is the number of days before which you would like to be notified about the license expiry.
5. Click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Create an email distribution list

Perform the following steps to create an email distribution list:

1. Select **Email** and click **Add**.
2. In **Create Email Distribution List**, specify the following details:
   - **Name** - Specify the distribution list name.
   - **To** - Specify the email addresses to which the NetScaler Console sends the message.
   - **Cc** - Specify the email addresses to which the NetScaler Console copies the message.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Bcc** - Specify the email addresses to which the NetScaler Console blind carbon copies (does not display the email address) the message.

3. Click **Create**.

Create a Slack profile

Perform the following steps to create a Slack profile:

1. In **Slack**, click **Add**.
2. In **Create Slack Profile**, specify the following details:

   - **Notifications** - When enabled, sends alerts and event notifications directly to a designated Slack channel.
   - **Notifications with attachments** - When enabled, detailed information about triggered alerts and events is sent as an email attachment or a JSON payload within a webhook.
   - **Profile Name** - Specify the profile name. This name appears in the Slack profile list.
   - **Channel Name** - Specify the Slack channel name to which the NetScaler Console sends the notification.
   - **Webhook URL** - Specify the Webhook URL of the channel. Incoming Webhooks are a simple way to post messages from external sources into Slack. The URL is internally linked to the channel name. All event notifications that are sent to this URL are posted on the designated Slack channel. An example of a webhook is as follows: `<https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK>`.

Create a PagerDuty profile

PagerDuty enables you to configure notifications through email, push notifications, and phone calls on a registered number. Before you add a PagerDuty profile in NetScaler Console, ensure that you have completed the required configurations in PagerDuty. To get started with PagerDuty, see the PagerDuty documentation.

Perform the following steps to create a PagerDuty profile:

1. In **PagerDuty**, click **Add**.
2. In **Create PagerDuty Profile**, specify the following details:

   - **Profile Name** - Specify a profile name. This name is used by different modules, such as event rules and SSL notifications to send PagerDuty alerts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Integration Key** - Specify the integration key. You can obtain this key from your PagerDuty portal. When creating a service in PagerDuty for integration, use the **Generic Events API Integration** option.

3. Click **Create**.

For more information, see Services and Integrations in the PagerDuty documentation.

View the ServiceNow profile

To enable ServiceNow notifications for the NetScaler events, you must integrate NetScaler Console with the ServiceNow using ITSM connector. For more information, see Integrate NetScaler Console with the ServiceNow instance.

Perform the following steps to view and verify the ServiceNow profile:

1. In **ServiceNow**, **Citrix_Workspace_SN** profile is selected by default.
2. Click **Test** to auto-generate a ServiceNow ticket and verify the configuration.

Note

> For information about the different types of NetScaler licenses, see Licensing overview.

RBAC support for LAS

You can use Role-Based Access Control (RBAC) to manage LAS application access with the following levels of control:

- **Feature level**: Restrict visibility of the licensing feature for specific administrators.
- **Instance level**: Limit authorized administrators to apply licenses only to selected NetScaler instances.

For configuration details, see Role-based access control.

Manually managed entitlements (file-based licenses)

The following sections are applicable for manually managed entitlement (file-based licensing).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

When you purchase a Universal Hybrid Multi-Cloud (UHMC) or a Citrix Platform License (CPL), the NetScaler licenses delivered are referred to as Flexed licenses. For more information, see UHMC/CPL offerings.

License files

NetScaler Flexed license includes the following files that you must download from the MyCitrix portal. For more information about transitioning from your current type of NetScaler licensing to Flexed Licensing, see Transition to Flexed licensing.

The license files present on your NetScaler are listed in this section.

FILE NAME CONTAINS	DESCRIPTION	DOWNLOAD INFORMATION	WHERE TO UPLOAD/APPLY THE LICENSE
NetScaler Flexed VPX SW Instance	Entitles you to VPX/ CPX/BLX software instances	Download this file using your NetScaler Console host ID	On NetScaler Console
NetScaler Flexed MPX SW Instance	Entitles you to MPX software instances	Download this file using your NetScaler Console host ID	On NetScaler Console
NetScaler Flexed SDX SW Instance	Entitles you to SDX software instances	Download this file using your NetScaler Console host ID	On NetScaler Console
NetScaler Flexed Platinum BW	Entitles you to Flexed Platinum throughput capacity	Download this file using your NetScaler Console host ID	On NetScaler Console
NetScaler Flexed VPX FIPS SW Instance	Entitles you to VPX FIPS software instances	Download this file using your NetScaler Console host ID	On NetScaler Console
Zero Capacity MPX-Z Platform License	Entitles you to make your NetScaler MPX HW/NetScaler MPX	Download this file	On NetScaler MPX

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FILE NAME CONTAINS	DESCRIPTION	DOWNLOAD INFORMATION	WHERE TO UPLOAD/APPLY THE LICENSE
	FIPS HW participate in Flexed licensing		
Zero Capacity SDX-Z Platform License	Entitles you to make your NetScaler SDX HW/NetScaler SDX FIPS HW participate in Flexed licensing	Download this file	On NetScaler SDX

Important points to note

- You can upload license to multiple NetScaler Console service tenants or multiple NetScaler Console on-prem instances.
- If you are transitioning to flexed license from pooled license and your MPX and SDX instances already have Z-Cap perpetual licenses, then applying the Z-Cap licenses received with flexed license is not required. However, if the current Z-Cap licenses that are applied on NetScaler MPX or NetScaler SDX are valid for a specific duration, then you must apply the Z-Cap licenses received with the flexed license.
- MPX-Z or SDX-Z platform licenses delivered as part of flexed licenses are perpetual. After the MPX-Z or SDX-Z platform license file is applied on the specific instances, it can be used until the instance End of Life (EOL).
- You must apply the flexed licenses on NetScaler Console for the NetScaler form factor that you are using in your deployment. For example:

  Apply the following licenses if you are using NetScaler SDX form factor:

  |License File|Apply on| |-|-| |NetScaler Flexed SDX SW Instance|NetScaler Console| |NetScaler Flexed VPX SW Instance|NetScaler Console| |NetScaler Flexed Platinum BW|NetScaler Console| |ADC Zero Capacity SDX-Z Platform|NetScaler SDX|

  Apply the following licenses if you are using NetScaler MPX form factor:

  |License File|Apply on| |-|-| |NetScaler Flexed MPX SW Instance|NetScaler Console| |NetScaler Flexed Platinum BW|NetScaler Console| |ADC Zero Capacity MPX-Z Platform|NetScaler MPX|

  Apply the following licenses if you are using NetScaler VPX, NetScaler BLX, or NetScaler CPX form factor:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

|License File|Apply on| |-|-| |NetScaler Flexed VPX SW Instance|NetScaler Console| |NetScaler Flexed Platinum BW|NetScaler Console|

Apply the following licenses if you are using NetScaler VPX FIPS form factor

|License File|Apply on| |-|-| |NetScaler Flexed VPX FIPS SW Instance|NetScaler Console| | NetScaler Flexed Platinum BW|NetScaler Console|

Apply a license file

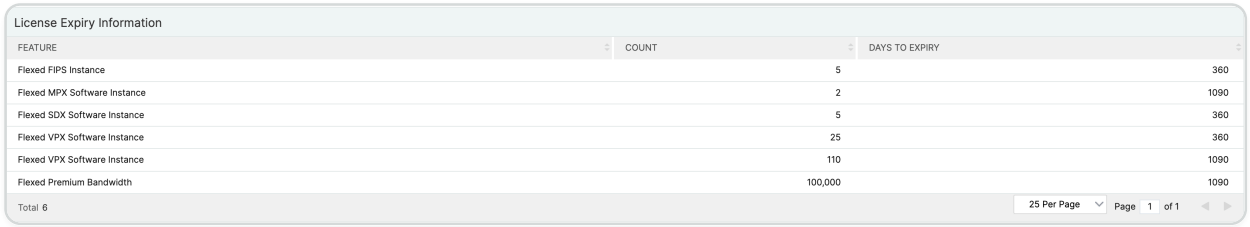
You can add, delete, and download licenses. You must apply licenses before they can be used.

1. Navigate to **NetScaler Licensing > License Management**.
2. In the **License Files** section, click **Add License File** and select one of the following options:
   - **Upload license files from a local computer**: If a license file is already present on your local computer, you can upload it to the NetScaler Console.
   - **Use license access code**: Specify the license access code for the license that you have purchased from Citrix. Click **Get Licenses** and then click **Finish**.
3. Click Finish. The license files are added to NetScaler Console. The **License Expiry Information** section lists the licenses present in NetScaler Console, count, and the remaining days to expiry.

NOTE:

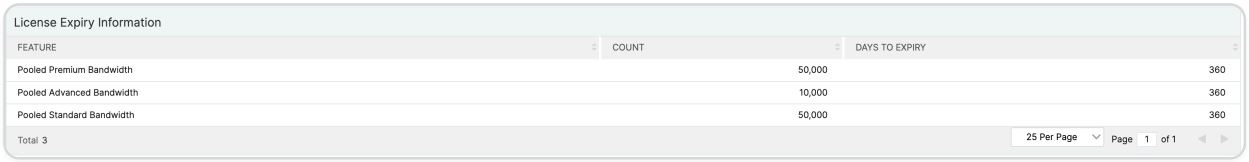
The license end date is the date till your contract is valid and you must renew it before the end date.

The following screenshot shows the number of Flexed NetScaler VPX, NetScaler MPX, NetScaler SDX, and NetScaler VPX FIPS software instance licenses, Flexed premium bandwidth capacity present, and the days to expiry (contract end date).



The following screenshot shows the Pooled Standard, Advanced, and Premium bandwidth available and the days to expiry (contract end date).

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Select a license file and click **Apply licenses**.

Delete a license file

To delete a license file, select one or more files and click **Delete**. When you delete a license, you must first add the license and only then you can apply it.

Download a license file

To download a license file, select a file and click **Download**. You can save the license file offline as a backup.

License server port settings

Ports are used by NetScaler instances to communicate with the license server. Click the **Edit** icon and specify values for the following parameters:

- **License Server Port**: The proxy server port used by NetScaler instances to access the Citrix licensing portal for license allocation. Default value: 27000.
- **Vendor Daemon Port**: The license server port used by NetScaler instances to communicate with the license server. Default value: 7279.

License expiry information

You can configure the license expiry threshold for flexed or pooled capacity licenses. When the threshold is set, NetScaler Console sends notifications through email when a license is due to expire. An SNMP trap and a notification are also sent when the license has expired on NetScaler Console.

An event is generated when a license expiry notification is sent and this event can be viewed on NetScaler Console from **Infrastructure > Events**.

View license expiry

1. Navigate to **NetScaler Licensing > License Management**.
2. In the **License Settings** page, under the **License Expiry Information** section, you can find the details of the licenses that are going to expire:
    - **Feature**: Type of license that is going to expire.
    - **Count**: Number of virtual servers or instances that are affected.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Days to expiry**: Number of days before license expiry (contract end date).

NOTE:

When you add new licenses to the pool, the NetScaler instances use the new licenses on the expiry of their existing licenses.

Notification email and a pop-up banner on license end date

In the NetScaler Console GUI, a pop-up message appears related to the license end date. As an administrator, you also receive a notification email for the license end date. By default, you get a pop-up message in the GUI (every time after login) 60 days before the license end date and a notification email in the frequency of 60, 30, 20, and 10 days before the license end date.

License expiry behavior

NetScaler instances with expired licenses managed through NetScaler Console stop to process traffic and might result in configuration loss.

Notification settings

Specify the settings based on which notifications will be sent out about license allocation and days to expiry.

1. In the **Notification Settings** section, click the **Edit** icon and select **Notify me on license usage**. Set the alert threshold as a percentage of flexed or pooled license capacity to be allocated to send a notification.
2. Choose the type of notification that you want to send when licenses reach the threshold, or are about to expire by selecting the appropriate checkbox. The notification types are as follows.

   - **Email**: Email profile or distribution list for sending notifications. For more information, see Create an email distribution list.
   - **Slack**: Slack profile details for sending notifications.
   - **PagerDuty**: PagerDuty profile for sending notifications.
   - **ServiceNow**: The Citrix ServiceNow profile is specified by default and is the only available option. For more information about creating these profiles, see Configure notifications

   Select a notification type and click **Add** to add details. You can also test each notification system before saving your settings.
3. Specify the **Days to Expiry**, which is the number of days before which you would like to be notified about the license expiry.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Click **Save**.

Create an email distribution list

Perform the following steps to create an email distribution list:

1. Select **Email** and click **Add**.
2. In **Create Email Distribution List**, specify the following details:
    - **Name** - Specify the distribution list name.
    - **Email Server** - Select the email server that sends the email notification. To add an email server, click Add. Specify the server name/IP address and port. Select Authentication to mandate authentication to access the email server. Select Secure if the email server supports SSL authentication. Click Create.
    - **From** - Specify the email address from which the NetScaler Console sends the message.
    - **To** - Specify the email addresses to which the NetScaler Console sends the message.
    - **Cc** - Specify the email addresses to which the NetScaler Console copies the message.
    - **Bcc** - Specify the email addresses to which the NetScaler Console blind carbon copies (does not display the email address) the message.
3. Click **Create**.

Create a Slack profile

Perform the following steps to create a Slack profile:

1. In **Slack**, click **Add**.
2. In **Create Slack Profile**, specify the following details:
    - **Profile Name** - Specify the profile name. This name appears in the Slack profile list.
    - **Channel Name** - Specify the Slack channel name to which the NetScaler Console sends the notification.
    - **Webhook URL** - Specify the Webhook URL of the channel. Incoming Webhooks are a simple way to post messages from external sources into Slack. The URL is internally linked to the channel name. All event notifications that are sent to this URL are posted on the designated Slack channel. An example of a webhook is as follows: `<https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK>`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a PagerDuty profile

PagerDuty enables you to configure notifications through email, push notifications, and phone calls on a registered number. Before you add a PagerDuty profile in NetScaler Console, ensure that you have completed the required configurations in PagerDuty. To get started with PagerDuty, see the PagerDuty documentation.

Perform the following steps to create a PagerDuty profile:

1. In **PagerDuty**, click **Add**.
2. In **Create PagerDuty Profile**, specify the following details:
    - **Profile Name** - Specify a profile name. This name is used by different modules, such as event rules and SSL notifications to send PagerDuty alerts.
    - **Integration Key** - Specify the integration key. You can obtain this key from your PagerDuty portal. When creating a service in PagerDuty for integration, use the **Generic Events API Integration** option.
3. Click **Create**.

For more information, see Services and Integrations in the PagerDuty documentation.

View the ServiceNow profile

To enable ServiceNow notifications for the NetScaler events, you must integrate NetScaler Console with the ServiceNow using ITSM connector. For more information, see Integrate NetScaler Console with the ServiceNow instance.

Perform the following steps to view and verify the ServiceNow profile:

1. In **ServiceNow**, **Citrix_Workspace_SN** profile is selected by default.
2. Click **Test** to auto-generate a ServiceNow ticket and verify the configuration.

NOTE:

For information about the different types of NetScaler licenses, see Licensing overview.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Minimum and maximum capacity for checkout

IMPORTANT:

File-based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler® versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Supported from early September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Note: LAS support for Console on-prem is from release 14.1-51.x onwards. However, file-based licensing is deprecated as of April 15 2026 from Console on-prem releases 14.1-51.x onwards and 13.1-60.x onwards. If you upgrade to Console on-prem release 14.1-51.x or release 13.1-60.x or later, you can continue using file-based licensing until 15th April 2026. However you must upgrade to Console on-prem release 14.1-51.x or later, and switch to LAS before 15th April 2026 because Console on-prem 13.1 does not support LAS.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don’t apply where prohibited by law or regulation.
NetScaler Flexed licensing uses NetScaler Console configured as a license server to manage Flexed licenses: bandwidth pool licenses and instance pool licenses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When checking out licenses from bandwidth and instance pool, NetScaler form factor and hardware model number on a zero-capacity hardware determines:

- The minimum bandwidth and the number of instances that a NetScaler instance must check out before being functional.
- The maximum bandwidth and the number of instances that a NetScaler can check out.
- The minimum bandwidth unit for each bandwidth check out. The minimum bandwidth unit is the smallest unit of bandwidth that a NetScaler has to check out from a pool. Any check-out must be an integer multiple of the minimum bandwidth unit. For example, if the minimum bandwidth unit of a NetScaler is 1 Gbps, 1000 Mbps can be checked out, but not 200 Mbps or 150.5 Gbps. The minimum bandwidth unit is different from the minimum bandwidth requirement. A NetScaler instance can only operate after it is licensed with at least the minimum bandwidth. Once the minimum bandwidth is met, the instance can check out more bandwidth in multiples of the minimum bandwidth unit.

Tables 1 through 5 summarize the maximum bandwidth/instances, minimum bandwidth/instances, and minimum bandwidth unit for all supported NetScaler instances. Table 6 summarizes the license requirement for different form factors for all supported NetScaler instances. The following tables refer to system requirements.

NOTE:

The minimum bandwidth checkout unit for NetScaler CPX/BLX/VPX is 10 Mbps. The minimum bandwidth checkout unit for NetScaler MPX/SDX is 1 Gbps.

Table 1. Supported Flexed capacity for MPX

PRODUCT LINE	MINIMUM BANDWIDTH (GBPS)	MAXIMUM BANDWIDTH (GBPS)	MINIMUM BANDWIDTH UNIT
MPX 5900Z	1	10	1 Gbps
MPX 8900Z	5	30	1 Gbps
MPX 8900Z FIPS	5	20	1 Gbps
MPX 9100Z	10	95	1 Gbps
MPX 9100Z FIPS	10	95	1 Gbps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRODUCT LINE	MINIMUM BANDWIDTH (GBPS)	MAXIMUM BANDWIDTH (GBPS)	MINIMUM BANDWIDTH UNIT
MPX 14000Z	20	100	1 Gbps
MPX 14000Z-40G	20	100	1 Gbps
MPX 14000Z-40S	40	100	1 Gbps
MPX 14000Z FIPS	30	80	1 Gbps
MPX 15000Z	20	120	1 Gbps
MPX 15000Z-50G	20	120	1 Gbps
MPX 15000Z FIPS	30	120	1 Gbps
MPX 16000Z	30	250	1 Gbps
MPX 22000Z	40	120	1 Gbps
MPX 24000Z	100	150	1 Gbps
MPX 25000Z	100	160	1 Gbps
MPX 25000Z-40G	100	200	1 Gbps
MPX 26000Z	100	200	1 Gbps
MPX 26000Z-50S	100	200	1 Gbps
MPX 26000Z-100G	100	200	1 Gbps

Table 2A. Supported Flexed capacity for NetScaler SDX version earlier than build 13.0-47.x

PRODUCT LINE	MINIMUM BANDWIDTH (GBPS)	MAXIMUM BANDWIDTH (GBPS)	MINIMUM INSTANCES	MAXIMUM INSTANCES	MINIMUM BANDWIDTH UNIT
SDX 8900Z	10	30	2	7	1 Gbps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRODUCT LINE	MINIMUM BANDWIDTH (GBPS)	MAXIMUM BANDWIDTH (GBPS)	MINIMUM INSTANCES	MAXIMUM INSTANCES	MINIMUM BANDWIDTH UNIT
SDX 14000Z	20	100	5	25	1 Gbps
SDX 14000Z-40G	40	100	20	25	1 Gbps
SDX 15000Z	20	120	5	55	1 Gbps
SDX 15000Z-50G	20	120	5	55	1 Gbps
SDX 22000Z	40	120	80	80	1 Gbps
SDX 24000Z	100	150	80	80	1 Gbps
SDX 25000Z	100	200	20	115	1 Gbps
SDX 25000Z-40G	100	200	20	115	1 Gbps
SDX 26000Z	100	200	20	115	1 Gbps
SDX 26000Z-50S	100	200	20	115	1 Gbps
SDX 26000Z-100G	100	200	20	115	1 Gbps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Table 2B. Supported Flexed capacity for NetScaler SDX version 13 (build 13.0-47.x and later), version 13.1 (build earlier than 51.x), and version 14.1 (build earlier 12.x)

PRODUCT LINE	MINIMUM BANDWIDTH (GBPS)	MAXIMUM BANDWIDTH (GBPS)	MINIMUM INSTANCES	MAXIMUM INSTANCES	MINIMUM BANDWIDTH UNIT
SDX 8900Z	5	30	1	7	1 Gbps
SDX 9100Z	10	95	2	7	1 Gbps
SDX 14000Z	10	100	2	25	1 Gbps
SDX 14000Z-40G	20	100	10	25	1 Gbps
SDX 15000Z	10	120	2	55	1 Gbps
SDX 15000Z-50G	10	120	2	55	1 Gbps
SDX 16000Z	15	250	10	55	1 Gbps
SDX 22000Z	20	120	40	80	1 Gbps
SDX 24000Z	50	150	40	80	1 Gbps
SDX 25000Z	50	200	10	115	1 Gbps
SDX 25000Z-40G	50	200	10	115	1 Gbps
SDX 26000Z	50	200	10	115	1 Gbps
SDX 26000Z-50S	50	200	10	115	1 Gbps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRODUCT LINE	MINIMUM BANDWIDTH (GBPS)	MAXIMUM BANDWIDTH (GBPS)	MINIMUM INSTANCES	MAXIMUM INSTANCES	MINIMUM BANDWIDTH UNIT
SDX 26000Z-100G	50	200	10	115	1 Gbps

Table 2C. Supported Flexed capacity for NetScaler SDX version 13.1 (build 51.x and later), and version 14.1 (build 12.x and later)

PRODUCT LINE	MINIMUM BANDWIDTH (GBPS)	MAXIMUM BANDWIDTH (GBPS)	MINIMUM INSTANCES	MAXIMUM INSTANCES	MINIMUM BANDWIDTH UNIT
SDX 8900Z	5	30	1	7	1 Gbps
SDX 9100Z	10	95	1	7	1 Gbps
SDX 14000Z	10	100	1	25	1 Gbps
SDX 14000Z-40G	20	100	1	25	1 Gbps
SDX 15000Z	10	120	1	55	1 Gbps
SDX 15000Z-50G	10	120	1	55	1 Gbps
SDX 16000Z	15	250	1	55	1 Gbps
SDX 22000Z	20	120	1	80	1 Gbps
SDX 24000Z	50	150	1	80	1 Gbps
SDX 25000Z	50	200	1	115	1 Gbps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRODUCT LINE	MINIMUM BANDWIDTH (GBPS)	MAXIMUM BANDWIDTH (GBPS)	MINIMUM INSTANCES	MAXIMUM INSTANCES	MINIMUM BANDWIDTH UNIT
SDX 25000Z-40G	50	200	1	115	1 Gbps
SDX 26000Z	50	200	1	115	1 Gbps
SDX 26000Z-50S	50	200	1	115	1 Gbps
SDX 26000Z-100G	50	200	1	115	1 Gbps

NOTES:

- The minimum purchase quantity can be different from the minimum system requirement.
- On NetScaler SDX running build 14.1-12.x and later, with a Flexed license, the restriction to check out a minimum number of instance licenses is removed. That is, you can check out a minimum of one instance license.

Table 3. Supported minimum/maximum bandwidth and minimum/maximum instances for NetScaler CPX instances

PRODUCT LINE	MAXIMUM BANDWIDTH (GBPS)	MINIMUM BANDWIDTH (MBPS)	MINIMUM INSTANCES	MAXIMUM INSTANCES	MINIMUM BANDWIDTH UNIT
CPX	10	10	1	1	10 Mbps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Table 4. Supported minimum/maximum bandwidth and minimum/maximum instances for NetScaler VPX instances on Hypervisors and Cloud services

HYPERVISOR/CLOUD SERVICE	MAXIMUM BANDWIDTH (GBPS)	MINIMUM BANDWIDTH (MBPS)	MINIMUM INSTANCES	MAXIMUM INSTANCES	MINIMUM BANDWIDTH UNIT
Citrix Hypervisor	40 Gbps	10 Mbps	1	1	10 Mbps
VMware ESXI	100 Gbps	10 Mbps	1	1	10 Mbps
Linux KVM	100 Gbps	10 Mbps	1	1	10 Mbps
Microsoft Hyper-V	3 Gbps	10 Mbps	1	1	10 Mbps
AWS	30 Gbps	10 Mbps	1	1	10 Mbps
Azure	10 Gbps	10 Mbps	1	1	10 Mbps
Google Cloud	10 Gbps	10 Mbps	1	1	10 Mbps

Note

The minimum purchase quantity is different from the minimum system requirement.

Table 5. Supported minimum/maximum bandwidth and minimum/maximum instances for NetScaler BLX instances

PRODUCT LINE	MAXIMUM BANDWIDTH (GBPS)	MINIMUM BANDWIDTH (MBPS)	MINIMUM INSTANCES	MAXIMUM INSTANCES	MINIMUM BANDWIDTH UNIT
BLX	100	10	1	1	10 Mbps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Table 6. Zero capacity license requirement for different form factors

PRODUCT LINE	ZERO CAPACITY HARDWARE
MPX	License required
SDX	License required
VPX	-
CPX	-
BLX	-

NetScaler agent behavior

IMPORTANT:

File-based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (Citrix Platform License/Universal Hybrid Multi-Cloud), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Supported from early September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Note: LAS support for Console on-prem is from release 14.1-51.x onwards. However, file-based licensing is deprecated as of April 15 2026 from Console on-prem releases 14.1-51.x onwards and 13.1-60.x onwards. If you upgrade to Console on-prem release 14.1-51.x or release 13.1-60.x or later, you can continue using file-based licensing until 15th April 2026.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

However you must upgrade to Console on-prem release 14.1-51.x or later, and switch to LAS before 15th April 2026 because Console on-prem 13.1 does not support LAS.

All the other forms of legacy NetScaler licenses such as NetScaler virtual CPU licensing (Pooled vCPU), NetScaler VPX Check-In and Check-Out (CICO), perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS-based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don't apply where prohibited by law or regulation.
The NetScaler agent works as an intermediary between NetScaler Console and the discovered instances across different data centers and public clouds. NetScaler Console service requires a minimum of one agent per tenant for Flexed or Pooled licensing to work. Multiple NetScaler agents can be deployed per site or multi-site, but only one agent can have the License Server Agent (LSA) role for the entire tenant deployment.

LAS-based licensing

When using LAS-based licensing, a built-in agent within NetScaler handles license communication. An external agent is an optional component that you can deploy within your architecture to serve as a proxy for licensing communication.

To configure the NetScaler built-in agent for LAS, see Configure the built-in agent to manage instances.

To enable agent failover, see netscaler-console-service/getting-started/initiate-built-in-agent.

NOTE:

If you are using a built-in agent, you can only transition to LAS-based licensing through the NetScaler Console GUI.

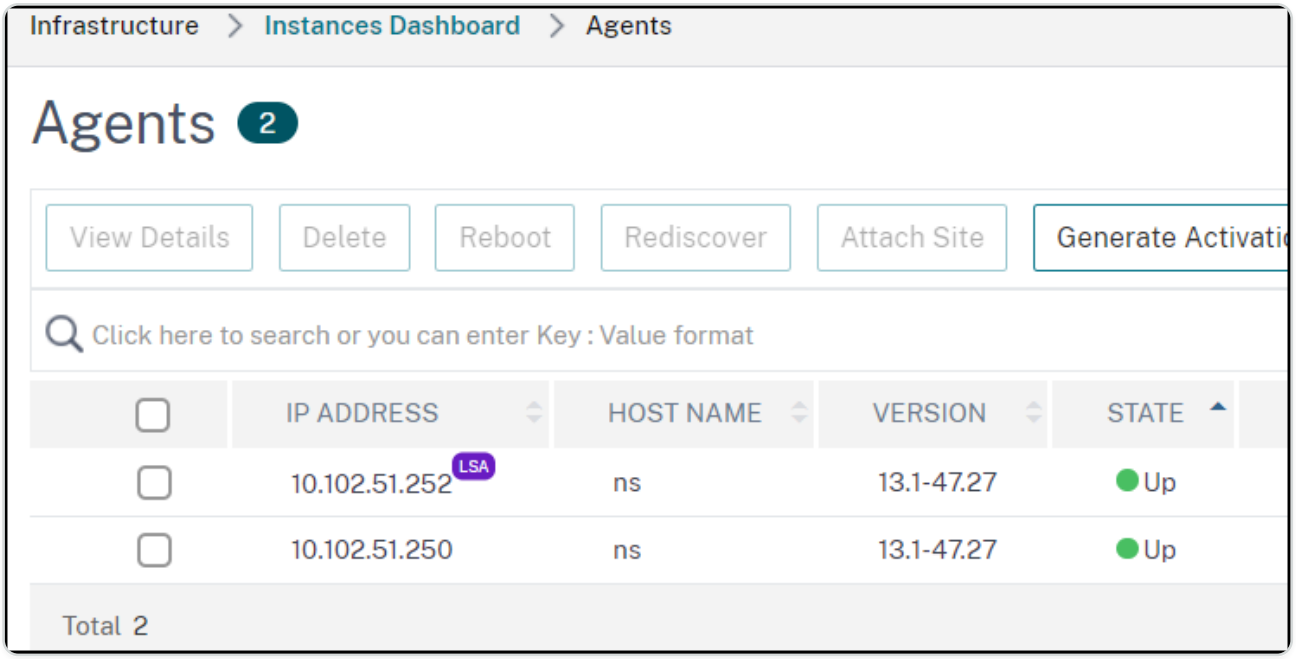
Manually managed entitlement (file-based licensing)

An LSA is an agent that works as a license server in NetScaler Console service based pooled licensing deployment. If the LSA goes down, the service waits for 24 hours to elect a new LSA.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Until then, the NetScaler instances using pooled or flexed license go in grace period. As an administrator, you can also manually elect an LSA.

The following example shows two agents deployed and one of them has the LSA role:



The following sections are applicable for manually managed entitlement (file-based licensing).

Manually select a NetScaler Console agent as LSA

Admins can manually select a NetScaler Console agent as the LSA for NetScaler Pooled licensing or NetScaler Flexed licensing. When the LSA is down, the NetScaler Console service waits for 24 hours before auto-electing the next LSA. The admin can manually elect the new LSA in the interim by using this feature. However, the admin must ensure that the status of the new LSA being elected is UP and its diagnostic status is OK.

When the admin manually selects a new LSA, it might take up to 5 minutes for the licensing functionality to work correctly. During this time, the NetScaler instances are in grace and any fresh checkout for a license fails.

To select an LSA:

1. Navigate to **Infrastructure > Instances Dashboard > Agents** and select an agent.
2. In the **Select Action** list, select **Set as LSA**.
3. Click **Yes** to confirm. The selected agent assumes the LSA role.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Multiple NetScaler agents behavior

In a deployment with a combination of multiple agents and multiple sites, the NetScaler agents follow the client/server architecture.

The first or oldest agent registered in an UP state is assigned the LSA role. Any other agents added later act as a proxy and communicate with the agent hosting the main LSA role for license allocation. Each agent hosting the proxy role communicates to the agent with the current LSA role through the NetScaler Console service.

NOTE:

There is no direct communication between the agent holding the LSA role and the other (non-LSA) agents. All the connections go through the NetScaler Console service only.

NetScaler agent failover behavior

The agent failover works in a multi-agent deployment in the following way.

Assume that there are two agents, AG1 and AG2, in the same data center.

- AG1 is configured to use ADC11, ADC12, ADC13 as the remote license host or LSA.
- AG2 is configured to use ADC21, ADC22, ADC23 as the remote license host or LSA.
- AG2 is acting as the license server.
    - If AG1 fails, ADC11, ADC12, and ADC13 automatically connect through AG2 for license reconciliation.
        - ADC11, ADC12, and ADC13 might still notice a small period of grace if a few heartbeats are missed, while this reconnection happens.
    - If AG2 fails, all ADCs continue to stay in grace until:
        - Either AG2 comes back up/is brought back up, or AG1 is selected as the new LSA either automatically after 24 hours by NetScaler Console service or manually by admin.
        - Or AG2 is deleted from the NetScaler Console service. Once deregistered, the NetScaler Console service designates AG1 as the agent with the LSA role.
        - After the election has completed, AG1 starts allocating and reconciling resources to the configured instances.

For questions related to LSA, see FAQs on License Server Agent.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure license server through NetScaler built-in agent

If you have a License Server Agent (LSA) configured in one site and want to use the same LSA from other sites, you can use a NetScaler built-in agent. While using the built-in agent, you must configure the license server using the following command on the NetScaler instance.

```
add licenseserver 127.0.0.1 -port 27000
```

In this configuration, NetScaler can reach the License Server Agent (LSA) through Console service.

NOTE:

NetScaler built-in agent cannot be assigned the LSA role.

Flexed license

IMPORTANT:

File-based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Supported from early September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Note: LAS support for Console on-prem is from release 14.1-51.x onwards. However, file-based licensing is deprecated as of April 15 2026 from Console on-prem releases 14.1-51.x onwards and 13.1-60.x onwards. If you upgrade to Console on-prem release 14.1-51.x or release 13.1-60.x or later, you can continue using file-based licensing until 15th April 2026.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> However you must upgrade to Console on-prem release 14.1-51.x or later, and switch to LAS before 15th April 2026 because Console on-prem 13.1 does not support LAS.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don't apply where prohibited by law or regulation.
NetScaler Flexed licensing is the new licensing framework aimed at simplifying the license management process. Your Flexed license includes software instance licenses (VPX/CPX/BLX, SDX, MPX, and VPX FIPS) and bandwidth capacity licenses. You must apply the Flexed license on NetScaler Console service or NetScaler ADM on-prem. You must also apply the MPX Z-Cap and SDX Z-Cap license on NetScaler MPX and NetScaler SDX hardware respectively. You can then allocate them across all NetScaler form factors deployed in cloud or on-prem.

Las-based licensing - When using LAS-based licensing, your flexed entitlements are automatically pulled into the NetScaler Console service and displayed in the user interface.

Manually managed entitlements (file-based licensing):

When using manually managed entitlements (file-based licensing), perform the following steps:

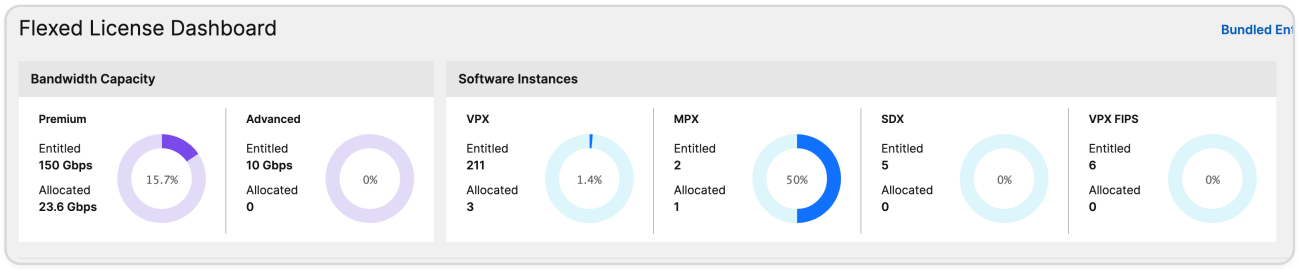
1. Apply the Flexed license to your NetScaler Console service or your NetScaler Console On-prem.
2. Apply the specific MPX Z-Cap and SDX Z-Cap licenses to your NetScaler MPX™ and SDX hardware, respectively.
3. Once the licenses are applied, you can allocate them across all NetScaler form factors, regardless of whether they are deployed in the cloud or on-premises.

A Flexed license also offers analytics for unlimited virtual servers.

If you had Pooled licenses earlier and bought a Flexed license, you can view your license details in the Flexed license dashboard. The combined bandwidth and instances appear in the Flexed license dashboard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Bandwidth license typically includes only the Premium edition unless you had a Pooled Standard or Advanced license earlier, in which case Standard, Advanced, and Premium editions appear in the Flexed license dashboard.



For more details see the Flexed license dashboard.

You can use Flexed licensing to maximize bandwidth utilization by ensuring the necessary bandwidth allocation to an instance and not more than its need. Increase or decrease the bandwidth allocated to an instance at run time without affecting the traffic.

Zero-capacity hardware

When managed through NetScaler Flexed licensing, MPX and SDX instances are referred to as “zero-capacity hardware” because these instances cannot function until they check resources out of the bandwidth pool. Thus, these platforms are also referred to as MPX-Z, and SDX-Z appliances.

Zero-capacity hardware requires a Z-cap license to check out bandwidth from the common pool.

NOTE:

- The zero capacity license installation works the same way as other NetScaler local licenses. For more information about how to obtain and install a zero capacity license, see Licensing guide for NetScaler.
- When using LAS-based licensing, you do not need to apply Z-Cap licenses.

Manage and install Z-cap licenses

You must install a Z-cap license manually, by using the hardware serial number or the license access code. After a Z-cap license is installed, it is locked to the hardware and cannot be shared across NetScaler hardware instances on demand. However, you can manually move the Z-cap license to another NetScaler hardware instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler MPX instances running the NetScaler software release 11.1 build 54.14 or later and NetScaler SDX instances running 11.1 build 58.13 or later support NetScaler Flexed licensing. For more information, see Tables 1 and 2 in Minimum and maximum capacity for Flexed and Pooled licensing.

Standalone NetScaler VPX instances

NetScaler VPX instances running NetScaler software release 11.1 Build 54.14 and later on the following hypervisors support Flexed licenses:

- VMware ESX 6.0
- Citrix Hypervisor™
- Linux KVM

NetScaler VPX instances running NetScaler software release 12.0 Build 51.24 and later on the following hypervisors and cloud platforms support Flexed licensing:

- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

NetScaler VPX instances running NetScaler software release 13.0 and 13.1 (all versions) on the following hypervisors and cloud platforms support Flexed licensing:

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM
- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

Standalone NetScaler CPX instances

NetScaler CPX instances deployed on a Docker host support Flexed licensing. Unlike zero-capacity hardware, NetScaler CPX does not require a Z-cap license. A single NetScaler CPX instance consuming up to 1 Gbps throughput checks-out only 1 instance and no bandwidth from

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the license pool. For example, consider that you have 20 NetScaler CPX instances with a 20 Gbps bandwidth pool. If one of the NetScaler CPX instances consumes 500 Mbps throughput, the bandwidth pool remains 20 Gbps for the remaining 19 NetScaler CPX instances.

If the same NetScaler CPX instance starts to consume 1500 Mbps throughput, the bandwidth pool has 19.5 Gbps for the remaining 19 NetScaler CPX instances.

For Flexed licensing, you can add more bandwidth only in multiples of 10 Mbps.

Standalone NetScaler BLX instances

NetScaler BLX instances support Flexed licensing. A NetScaler BLX instance does not require a Z-cap license. To process traffic, a NetScaler BLX instance must check out bandwidth and an instance license from the pool.

Bandwidth Pool

The bandwidth pool is the total bandwidth that can be shared by NetScaler instances, both physical and virtual. The bandwidth pool comprises a pool for the Premium software edition. If you shift from Pooled to Flexed licensing, you might find a mix of Standard, Advanced, and Premium software editions. A given NetScaler MPX/VPX/CPX/BLX instance cannot have bandwidth from different pools checked out concurrently. The bandwidth pool from which it can check out bandwidth depends on its software edition for which it is licensed.

Instance pool

There are three types of software instance pools:

- VPX/CPX/BLX software instance
- MPX software instance (same pool applies for MPX FIPS)
- SDX software instance (same pool applies for SDX FIPS)
- VPX FIPS software instance

When checked out from the pool, a license unlocks the software instance's resources, including CPUs/PEs, SSL cores, packets per second, and bandwidth.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure license

IMPORTANT:

File-based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (Citrix Platform License/Universal Hybrid Multi-Cloud), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Supported from early September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Note: LAS support for Console on-prem is from release 14.1-51.x onwards. However, file-based licensing is deprecated as of April 15 2026 from Console on-prem releases 14.1-51.x onwards and 13.1-60.x onwards. If you upgrade to Console on-prem release 14.1-51.x or release 13.1-60.x or later, you can continue using file-based licensing until 15th April 2026. However you must upgrade to Console on-prem release 14.1-51.x or later, and switch to LAS before 15th April 2026 because Console on-prem 13.1 does not support LAS.

All the other forms of legacy NetScaler licenses such as NetScaler virtual CPU licensing (Pooled vCPU), NetScaler VPX Check-In and Check-Out (CICO), perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS-based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don’t apply where prohibited by law or regulation.
The NetScaler Flexed or pooled licensing allows you to share bandwidth or instance licenses across different NetScaler form factors. When an instance no longer requires the resources, it

© 1997–2026 Citrix Systems, Inc. All rights reserved.

checks the allocated capacity back into the common pool. Reuse the released capacity on other NetScaler instances that need resources.

NOTE:

If you have pooled licenses, and have now purchased and applied Flexed licenses, the combined entitlement appears in the Flexed license dashboard.

You can use Flexed or pooled licensing to maximize the bandwidth utilization by ensuring the necessary bandwidth allocation to an instance and not more than its need. Increase or decrease the bandwidth allocated to an instance at run time without affecting the traffic. With the Pooled capacity licenses, you can automate the instance provisioning.

LAS-based licensing

When using LAS, an external agent is optional. The license entitlements are automatically pulled into the NetScaler Console service and reflected on the NetScaler console GUI.

Prerequisite

- Ensure port 443 is available for instances to check out licenses from NetScaler Console. For more information, see System requirements.

Step 1 - Validate Entitlement Reflection

1. Navigate to **Licensing Management > LAS** to validate that your NetScaler entitlements are reflected.

Step 2 - Add NetScaler instance to the console service

1. Add your NetScaler instance to the console service.

For more information, see Add NetScaler instances.

```
-  **Using an External Agent**: If you are using an external agent for
proxying licensing communication, you must explicitly add the NetScaler
instances to the Console.



-  **Using a Built-in Agent**: If you are using a built-in agent, the
NetScaler instance is automatically added to the NetScaler Console service
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> when you configure the agent. For more informatiion about built-in agent, see Configure Built-in Agent for NetScaler Console On-Prem.

Step 3 - Activate your license with LAS

1. Navigate to **Licensing Management > LAS**.
2. Click **License with LAS** or **Migrate to LAS**.
3. Select an instance, and click **Continue**.

   For more information, see License Activation Service.

Step 4 - Edit flexed throughput capacity for NetScaler instances

1. Navigate to **NetScaler Licensing > Flexed Licensing > Dashboard > LAS managed entitlements**.
2. In the **Licensed NetScalers section**, select an instance and click **Edit Throughput Capacity**.
3. Enter the desired throughput value in the **Allocate*** column.
4. Click **Submit**.

Special Licensing for Unlicensed MPX Appliances with an external agent

When using an external agent with an unlicensed MPX, HTTPS connections to the Console Service are not supported. As a result, step 2 is not feasible. Instead navigate to the NetScaler to complete the following steps.

1. Navigate to **System > Licenses > ADC License > Manage Licenses > Add New License**.
2. In the Licenses page, select the **Use remote licensing** radio button, and choose **LAS** mode from Remote Licensing Mode.
3. In the **Server Name/IP address** field, enter the IP address of your NetScaler Console external agent.
4. Enter your NetScaler agent credentials to register the instance and then click **Continue**.

NOTES:

- Select the **Validate Certificate** checkbox only if you have uploaded a valid digital certificate (issued by a Certificate Authority (CA)) on the NetScaler agent.
- One of the agents in NetScaler Console serves as the license server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. In the **Device Profile Name** field, provide the instance profile that NetScaler Console uses to access the instance. This profile holds the user name and password for the instances you want to add. The default profile is ns_nsroot_profile. However, if you have changed the default administrator credentials, ensure to create and specify a custom instance profile name.
6. In the **Allocate Licenses** section, select the license edition and specify the required bandwidth. The first time you allocate licenses in NetScaler, you can later modify or release the allocation directly from the NetScaler Console GUI.
7. Click **Get Licenses**.

NOTE:

If you change the license edition, warm restart the instance. The configuration changes do not take effect until you restart the instance.

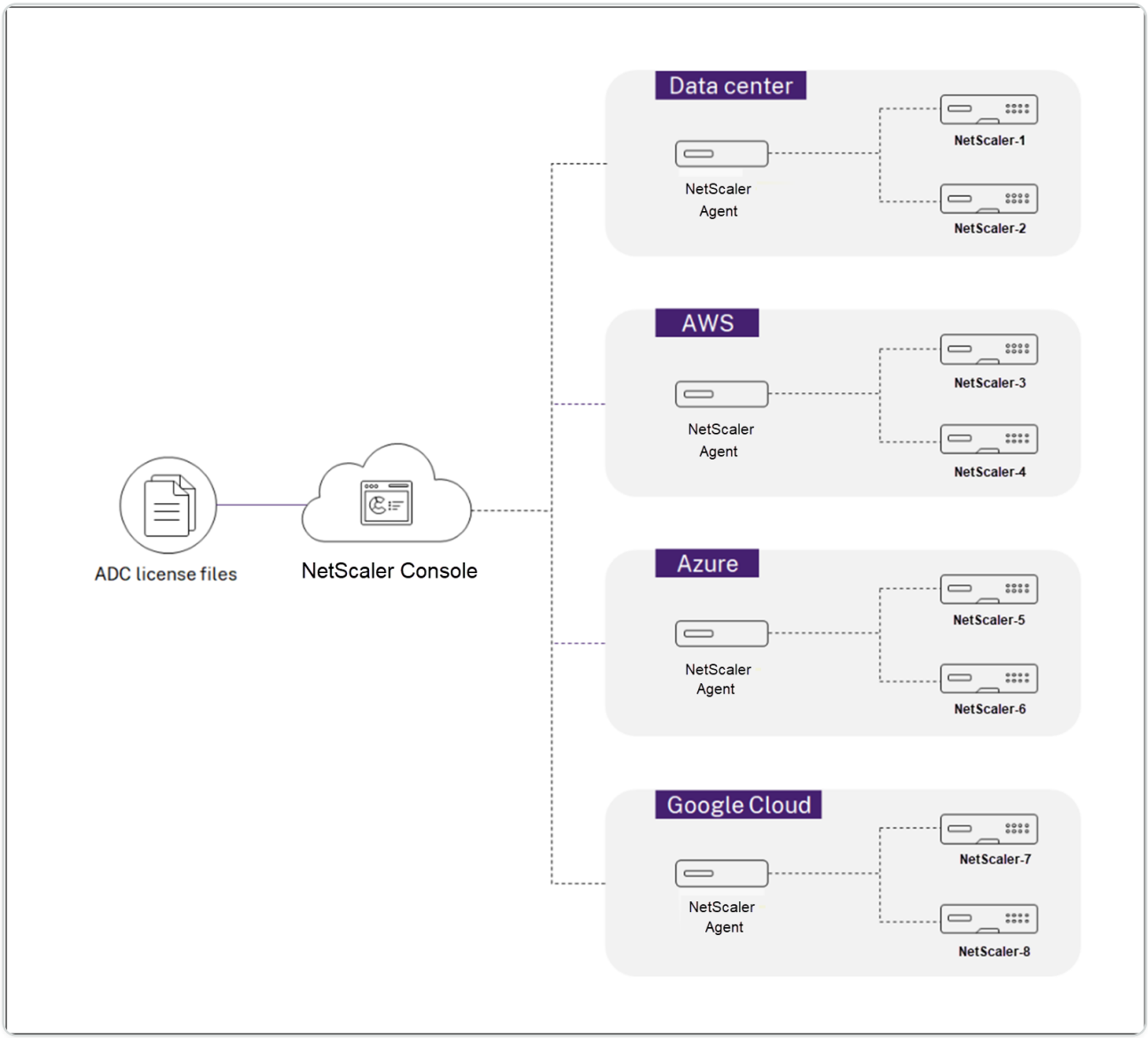
Manually managed entitlements (file-based licensing)

To use NetScaler Flexed or pooled licensing, you must attach an NetScaler Console agent to an NetScaler instance. NetScaler instances check in and check out licenses from NetScaler Console through an agent.

You can also use Pooled capacity licenses for NetScaler FIPS instances. You can perform the following tasks in NetScaler Console:

1. Upload the Flexed or pooled license files (bandwidth pool or software instance pool) to the license server.
2. Allocate licenses from the license pool to NetScaler instances on demand.
    - Check out the licenses from NetScaler instances (MPX-Z /SDX-Z/VPX/CPX/BLX) based on the minimum and maximum capacity of the instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can download Flexed or pooled licenses, including bandwidth, instance, and Z-cap licenses from citrix.com. For more information, see Licensing guide for NetScaler.

Before you begin

Ensure that the following prerequisites are met before you configure Flexed licensing:

- Install and register an agent in NetScaler Console. To install and register an agent, see Getting started.
- Ensure that all registered agents are in the UP state for Flexed licensing to work properly. If agents are in DOWN state but not yet decommissioned or terminated, bring them to UP state. If DOWN agents are decommissioned or terminated or not in use anymore, delete them from NetScaler Console.
- The `27000` and `7279` ports are available to check out licenses from NetScaler Console to an instance. See, System requirements.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 1 - Apply licenses in NetScaler Console

1. Navigate to **NetScaler Licensing > License Management**.
2. In the **License Files** section, select **Add License File** and select one of the following options:
   - **Upload license files from a local computer**. If a license file is already present on your local computer, you can upload it to NetScaler Console.
   - **Use license access code**. Specify the license access code for the license that you have purchased from Citrix. Then, select **Get Licenses**. Then select **Finish**.

   NOTE:

   At any time, you can add more licenses to NetScaler Console from **License Settings**.
3. Click **Finish**.

   The license files are added to NetScaler Console. The **License Expiry Information** section lists the licenses present in the NetScaler Console and the remaining days to expiry.
4. In **License Files**, select a license file that you want to apply and click **Apply licenses**.

   This action enables NetScaler instances to use the selected license as a Flexed or pooled license.

Step 2 - Register NetScaler Console as a license server and allocate licenses

You can register the NetScaler Console as a license server to a NetScaler instance using an agent.

Register an NetScaler Console agent using the GUI

In the NetScaler Console GUI, register the NetScaler Console agent associated with an NetScaler instance.

1. Log in to NetScaler GUI.
2. Navigate to **System > Licenses > Manage Licenses**.
3. Click **Add New License**.
4. Select **Use remote licensing** and under **Remote Licensing Mode**, select **Pooled Licensing** from the list.
5. In the **Server Name/IP address** field, specify the associated NetScaler Console agent IP address that is registered with NetScaler Console.
6. The default license port is 27000.

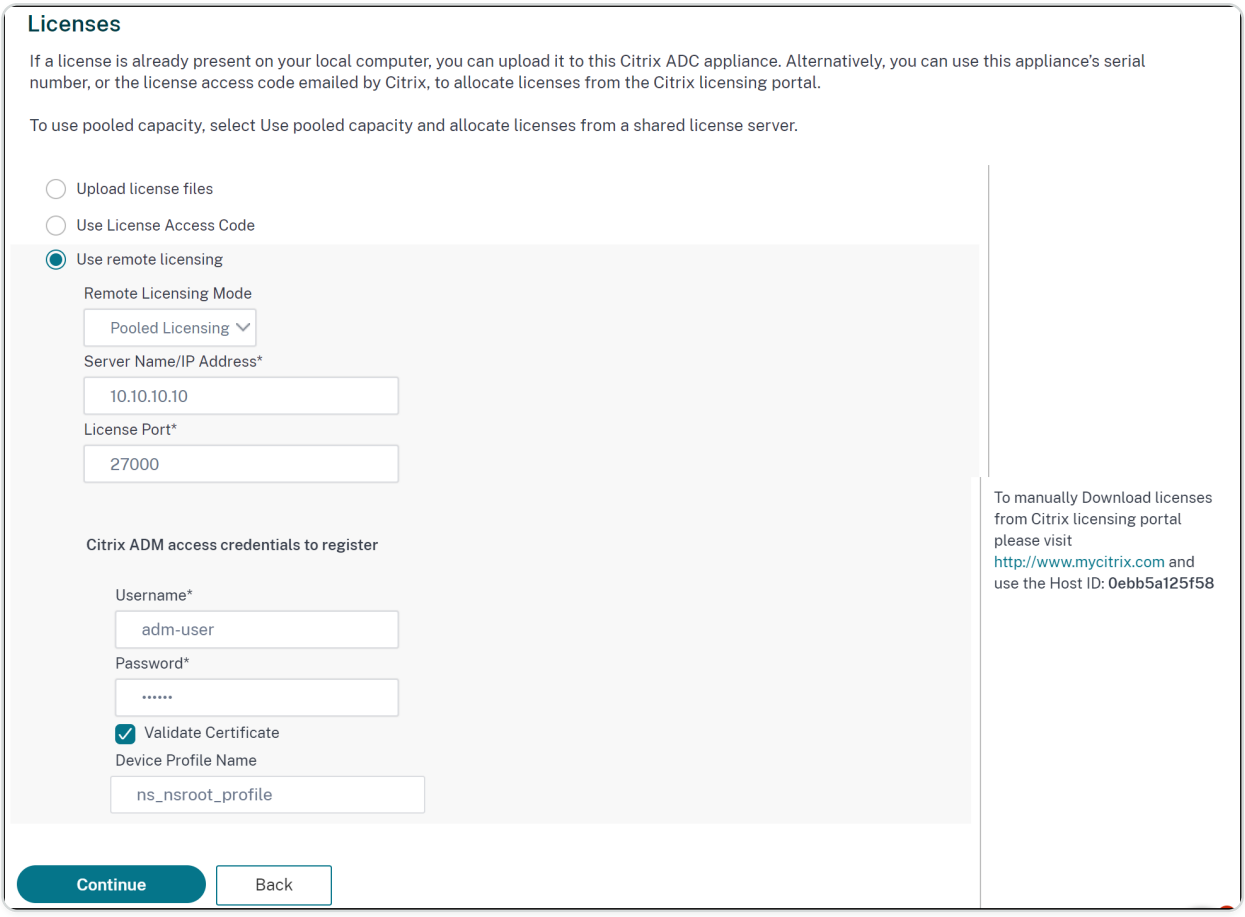
© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. Enter your NetScaler agent credentials to register an instance with NetScaler Console and click **Continue**. In NetScaler Console, one of the agents is the license server.

   NOTES:

   - Select the **Validate Certificate** checkbox only if you have uploaded a valid digital certificate (issued by a Certificate Authority (CA)) on the NetScaler agent. In NetScaler Console, navigate to Infrastructure > Instances > Agents and from the Select Action list, select Install Certificate to upload the certificate.
   - Device registration might fail if NetScaler is reachable only through an NAT IP. You can still check out the license, but NetScaler Console displays those NetScaler instances as unmanaged instances.

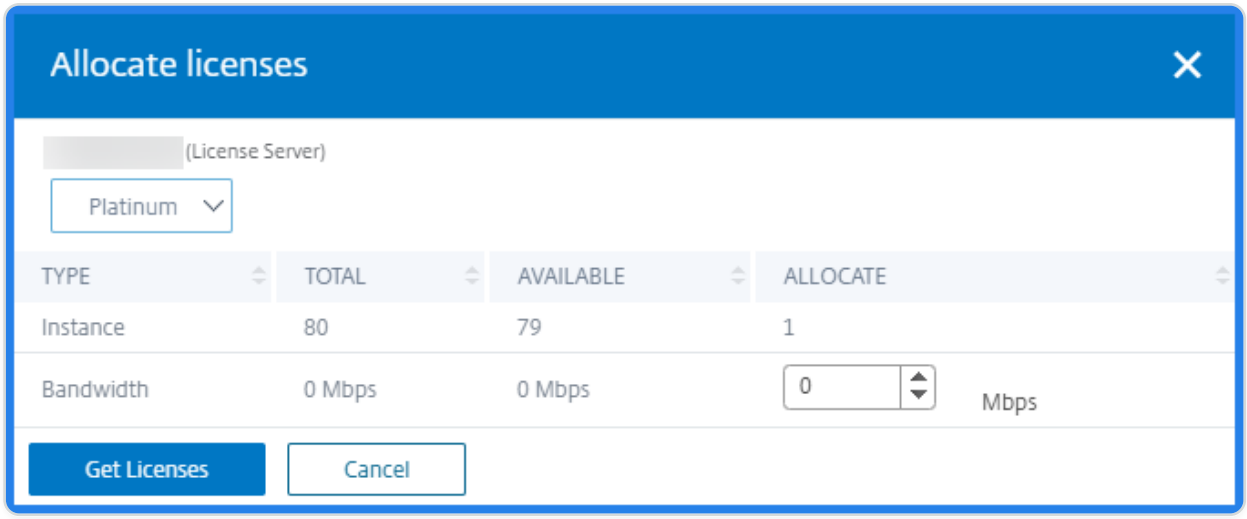
8. Under **Device Profile Name**, specify the instance profile that NetScaler Console can use to access the instance. This instance profile contains the user name and password of the instances that you want to add to NetScaler Console. The default profile is **ns_nsroot_profile**. If you have changed the default admin credentials of your instances, you can define a custom instance profile name.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. In **Allocate licenses**, select the license edition and specify the required bandwidth.

   For the first time, allocate licenses in NetScaler. You can later change or release the license allocation from the NetScaler Console GUI.



10. Click **Get Licenses**.

IMPORTANT

Warm restart the instance if you change the license edition. The configuration changes do not take effect until you restart the instance.

Add an agent using the CLI

If a NetScaler instance has no GUI, use the following CLI commands to add an agent associated with an instance:

1. Log in to the NetScaler console.
2. Add the associated agent's IP address that is registered with the NetScaler Console:

```
> add ns licenseserver <adm-agent-IP-address> -port <adm-agent-license-port-number>
```

3. View the license bandwidth available in the license server:

```
> sh ns licenseserverpool
```

4. Allocate the license bandwidth from the required license edition:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
> set ns capacity -unit gbps -bandwidth <specify-license-bandwidth>
edition <specify-license-edition>
```

IMPORTANT

Warm restart the instance if you change the license edition.

`reboot -w`

The configuration changes do not take effect until you restart the instance.

Step 3 - Based on license type proceed to the relevant license procedure

Edit Flexed Throughput Capacity for NetScaler instances

1. Navigate to **NetScaler Licensing > Flexed Licensing > Dashboard**.
2. In the **Licensed NetScalers** section, select an instance and click **Edit Throughput Capacity**.
3. In the **Edit Throughput Capacity** page, enter a number in the **Allocate** column.
4. Click **Submit**.

Allocate Pooled licenses to NetScaler instances

To allocate Pooled capacity licenses from the NetScaler Console GUI:

1. Log in to NetScaler Console.
2. Navigate to **Infrastructure > Pooled Licensing > Bandwidth Licenses > Pooled Capacity**.

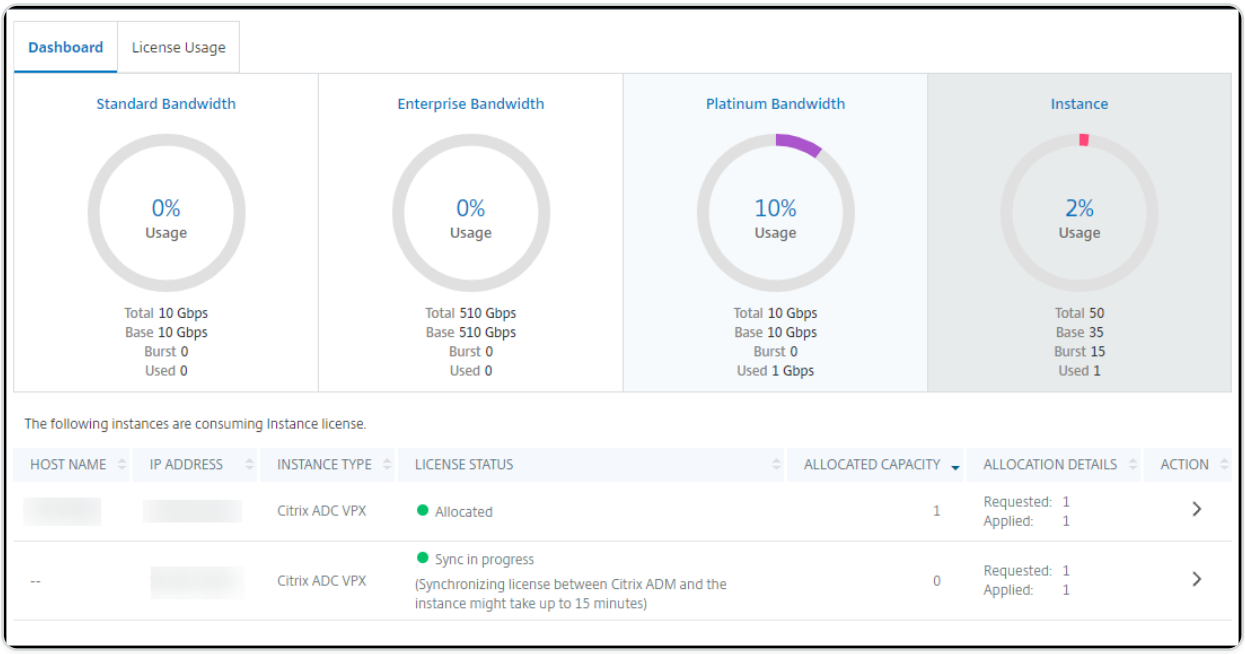
   The FIPS instance capacity appears only if you upload FIPS instance licenses to NetScaler Console.
3. Click the license pool that you want to manage.

   NOTE:

   The **Allocated Capacity** field does not reflect the changed bandwidth immediately. The bandwidth change takes effect after the NetScaler warm restart.

   In **Allocation Details**, the **Requested** and **Applied** fields are updated when you change the instance's bandwidth allocation.
4. Select a NetScaler instance from the list of available instances by clicking the **>** button.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The License status column displays corresponding license allocation status messages.

NOTE:

The **Unmanaged Instances** tab displays the instances that are discovered but not managed in NetScaler Console.

5. Click **Change allocation** or **Release allocation** to modify the license allocation.
6. A pop-up window with the available licenses in the License Server appears.
7. You can choose the bandwidth or instance allocation to the instance by setting the Allocate list options. After making your selections, click **Allocate**.
8. You can also change the allocated license edition from the list options in the **Change License Allocation window**.

NOTE:

Warm restart an instance if you change the license edition.

Configure flexed or pooled capacity on NetScaler instances

You can configure Pooled capacity licenses on the following NetScaler instances:

- NetScaler MPX-Z instances
- NetScaler SDX-Z instances
- NetScaler VPX instances

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler high-availability pair

NetScaler MPX-Z

MPX-Z is the Flexed-capacity enabled NetScaler MPX appliance. MPX-Z supports bandwidth pool for only Premium edition licenses.

MPX-Z requires a license before it can connect to the License Server. You can install the MPX-Z license by using one of the following ways:

- Uploading the license file from a local computer.
- Using the instance's hardware serial number.
- The License Access Code from the **System** > **Licenses** section of the instance's GUI.

If you remove the MPX-Z license, MPX becomes unlicensed. The instance licenses are released to the license server.

You can dynamically modify the bandwidth of an MPX-Z instance without a restart. A restart is required only if you want to change the license edition.

NOTE:

When you restart the instance, it automatically checks out the Flexed licenses required for its configured capacity.

NetScaler SDX-Z

SDX-Z is the Flexed-capacity enabled NetScaler SDX appliance. SDX-Z supports bandwidth and instance pool for the Premium edition licenses.

SDX-Z requires a license before it can connect to the License Server. You can install the SDX-Z license by using one of the following ways:

- Uploading the license file from a local computer.
- Using the instance's hardware serial number.
- The License Access Code from the **System** > **Licenses** section of the instance's GUI.

If you remove the SDX-Z license, SDX becomes unlicensed. The instance licenses are released to the license server.

You can dynamically modify the bandwidth of an SDX-Z instance without a restart. A restart is required only if you want to change the license edition.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

When you restart the instance, it automatically checks out the Flexed licenses required for its configured capacity.

License requirements for NetScaler high-availability pair (Common for both LAS and file-based licensing)

NOTE:

These requirement are applicable for both manually managed entitlement (file-based licensing) and LAS.

When you configure a NetScaler high-availability (HA) pair, ensure that both the primary and secondary instances meet the following requirements:

Before you begin, ensure that the NetScaler Console server is configured as a license server. For more information, see Configure NetScaler Console as a license server

When you allocate the bandwidth to an NetScaler HA pair, the NetScaler Console checks out the allocated bandwidth to the primary instance. You must repeat the process for the secondary instance.

To allocate pool licenses to a NetScaler HA pair, see (#Edit Flexed Throughput Capacity for NetScaler instances)

The **Flexed Capacity** page displays the instances and their allocated capacity separately.

NetScaler Flexed licensing states (Common for both LAS and file-based licensing)

The Flexed licensing states indicate the license requirement on an NetScaler instance. The NetScaler instances configured with Flexed licensing display one of the following states:

- **Allocated**: Instance is running with proper license capacity.
- **Grace**: Instance is running on a grace license. **Note**: This state is applicable only for manually managed entitlement (file-based licensing).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Connection lost**: Communication from NetScaler Console to the instance is not working. **Note**: If the connection between NetScaler and Console Service is lost for 24 hours or longer, the NetScaler state changes to Grace.

License dashboard

IMPORTANT:

File-based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Supported from early September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Note: LAS support for Console on-prem is from release 14.1-51.x onwards. However, file-based licensing is deprecated as of April 15 2026 from Console on-prem releases 14.1-51.x onwards and 13.1-60.x onwards. If you upgrade to Console on-prem release 14.1-51.x or release 13.1-60.x or later, you can continue using file-based licensing until 15th April 2026. However you must upgrade to Console on-prem release 14.1-51.x or later, and switch to LAS before 15th April 2026 because Console on-prem 13.1 does not support LAS.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other

© 1997–2026 Citrix Systems, Inc. All rights reserved.

remedies Citrix may have at law or equity. These requirements don’t apply where prohibited by law or regulation.

Read the following note before proceeding further.

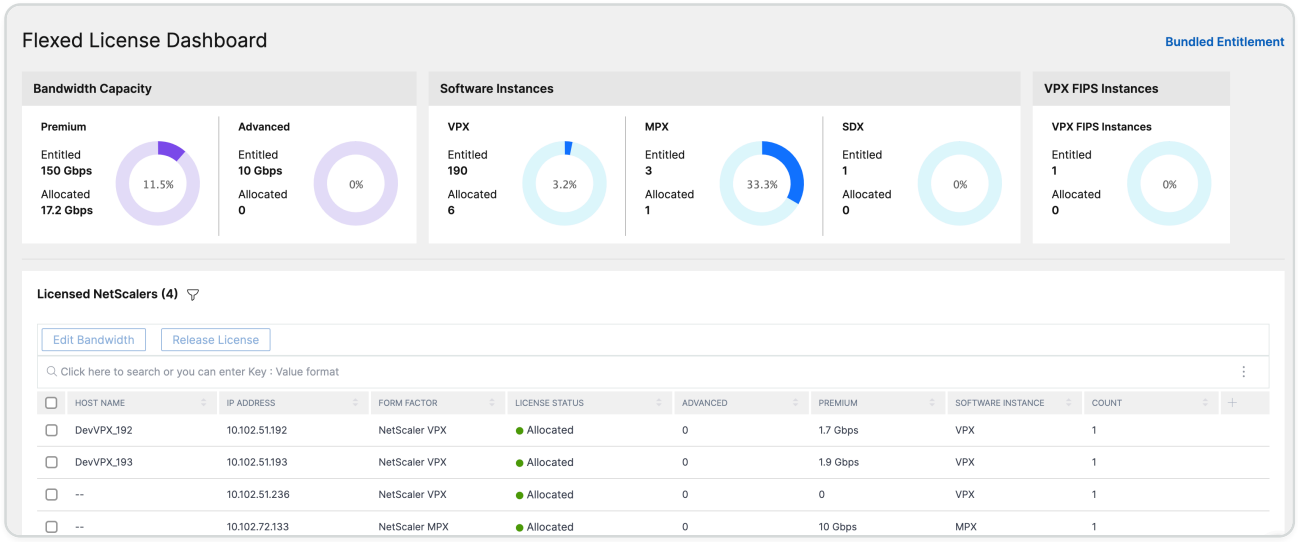
NOTES:

- If you had pooled licenses earlier, and now purchased and applied Flexed licenses, the combined entitlement now appears in the Flexed license dashboard.
- If you have only pooled licenses, check the Pooled license dashboard.
- If you have only Flexed licenses, or both Flexed and Pooled licenses, check the Flexed license dashboard.
- **Point to note based on licensing method:**
  - To view LAS-based licensing licenses, navigate to **NetScaler licenses > Flexed Licensing > Dashboard > LAS managed entitlements tab**
  - To view manually managed entitlements (file-based licensing) licenses, navigate to **NetScaler licenses > Flexed Licensing > Dashboard > Manually managed entitlements tab**
  - If you use both license mechanism refer to both tabs.

The flexed license dashboard gives you a comprehensive view of the bandwidth capacity and instances purchased by you.

Bandwidth capacity across editions and instance details for different form factors, such as MPX, VPX, and SDX are displayed on this page. MPX and MPX FIPS have the same license file. Similarly, SDX and SDX FIPS have the same license file. However, VPX FIPS has a different file from VPX and is displayed separately. Also, VPX (including VPX on SDX), BLX, and CPX require VPX licenses and are part of the entitlement and allocation for VPX. A flexed license supports only the premium edition. However, if you bought flexed licenses, and had pooled standard or advanced bandwidth capacity earlier, the details related to bandwidth capacity (standard or advanced) are also listed in the flexed license dashboard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



VPX (including VPX on SDX), BLX, and CPX form factors require NetScaler Flexed VPX SW Instance license file. That is these form factors are a part of the entitlement and allocation for Flexed VPX SW Instance licenses.

Details about your licensed NetScaler instances are available in the **Licensed NetScalers** section. You can select an instance and edit the bandwidth or release the license on that instance.

You can filter the results based on the following parameters:

- Filter by Bandwidth/throughput capacity
  - Premium
  - Advanced
  - Standard
- Form Factor
  - NetScaler MPX
  - NetScaler VPX
  - NetScaler SDX
- License status
  - Connection lost
  - Grace
  - Allocated

Edit the allocated throughput capacity on a NetScaler instance

1. Navigate to **NetScaler Licensing > Flexed Licensing > Dashboard**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. In the **Licensed NetScalers** section, select an instance and click **Edit Throughput Capacity**.
3. In the **Edit Throughput Capacity** page, enter a number in the **Allocate** column.
4. Click **Submit**.

Release licenses on a NetScaler instance

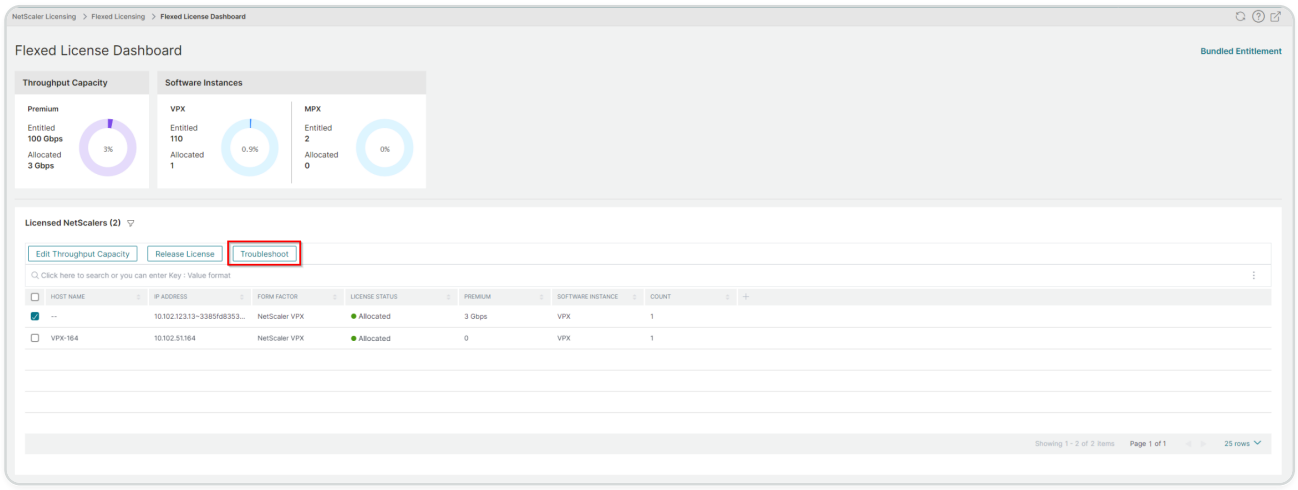
To transfer licenses to another instance, you must release the license on the current instance and then apply the license to the new instance. Selecting **Release License** does the following:

- Releases all the licenses, which are checked out on that instance, to the license server.
- Deletes the license server configuration on that instance.

If you select **Yes**, your NetScaler instance becomes unlicensed and cannot process any traffic.

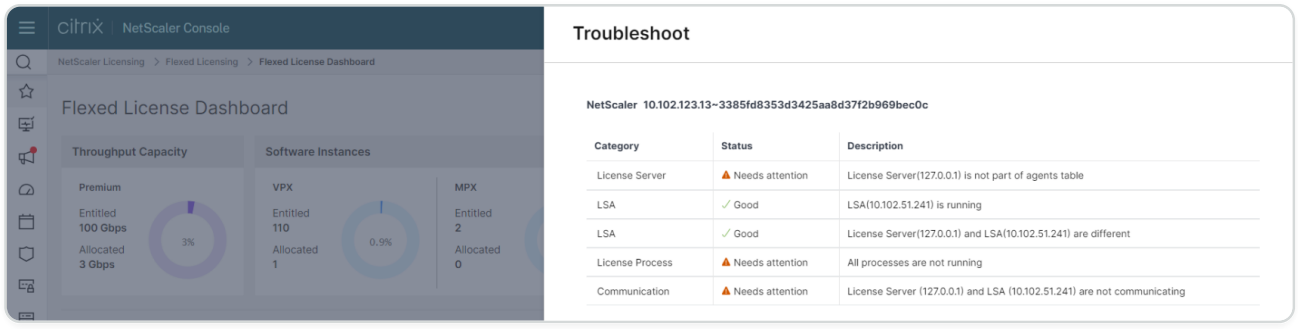
Troubleshoot licensing issues

You can use the **Troubleshoot** option to view and analyze few licensing related issues.



Some possible licensing issues are communication from Console to the instances, availability of the License Server Agents (LSA), and so on. The **Troubleshoot** option provides the list of issue categories such as License server, LSA, Processes, Communication, and their status. As an administrator, if you find any licensing issues, you can analyze these categories and troubleshoot.

The following is an example scenario that needs attention:



© 1997–2026 Citrix Systems, Inc. All rights reserved.

License reporting

IMPORTANT:

File-based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Supported from early September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Note: LAS support for Console on-prem is from release 14.1-51.x onwards. However, file-based licensing is deprecated as of April 15 2026 from Console on-prem releases 14.1-51.x onwards and 13.1-60.x onwards. If you upgrade to Console on-prem release 14.1-51.x or release 13.1-60.x or later, you can continue using file-based licensing until 15th April 2026. However you must upgrade to Console on-prem release 14.1-51.x or later, and switch to LAS before 15th April 2026 because Console on-prem 13.1 does not support LAS.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don’t apply where prohibited by law or regulation.
In this dashboard, you can view details about:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If you had pooled licenses earlier, and now purchased and applied Flexed licenses, the combined entitlement now appears in the Flexed license dashboard.

- Software instance (VPX, MPX, and SDX, and VPX FIPs) entitlement and allocation
- Bandwidth/throughput-capacity entitlement, allocation, and actual usage
- Peak and average allocation across all managed or selected instances
- Peak and average usage across all managed or selected instances

FEATURES (FOR NETSCALER INSTANCES)	DESCRIPTION
Entitlement	The total instance entitlements for software instance types (VPX, SDX, MPX).
Allocation	The total instance allocation for software instance types (VPX, SDX, MPX).

FEATURES (FOR BANDWIDTH/ THROUGHPUT-CAPACITY)	DESCRIPTION
Entitlement	The total bandwidth/throughput-capacity entitlements across all managed NetScaler instances. The total entitlements are calculated from the licenses applied in License management (**NetScaler Licensing > License Management**).
Allocation	The bandwidth/throughput-capacity that are allocated to **Licensed NetScalers** in Flexed License Dashboard (**NetScaler Licensing > Flexed Licensing > Dashboard**).
Usage	The total throughput consumed by the NetScaler instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

A flexed license supports only the premium edition. However, if you have bought and applied flexed licenses, and had pooled standard or advanced bandwidth capacity earlier, the details related to bandwidth/throughput-capacity (standard or advanced) are also listed. For example, you have applied 1000 Gbps Flexed license (which is premium) and also have an active Pooled license of 100 Gbps Advanced Bandwidth, then the reporting dashboard shows both Premium 1000 Gbps and 100 Advanced Bandwidth.

The following example helps you understand how the dashboard displays the peak usage and average usage:

Consider that there are 3 managed NetScaler instances (NetScaler A, NetScaler B, and NetScaler C) with Flexed license (Premium bandwidth) and the selected duration is 1 day. For calculations, NetScaler Console considers datapoints (in Mbps) for each hour per NetScaler instance. For 1 day, there are 24 datapoints for each NetScaler instance. So, for 3 NetScaler instances, there are (24 * 3) datapoints.

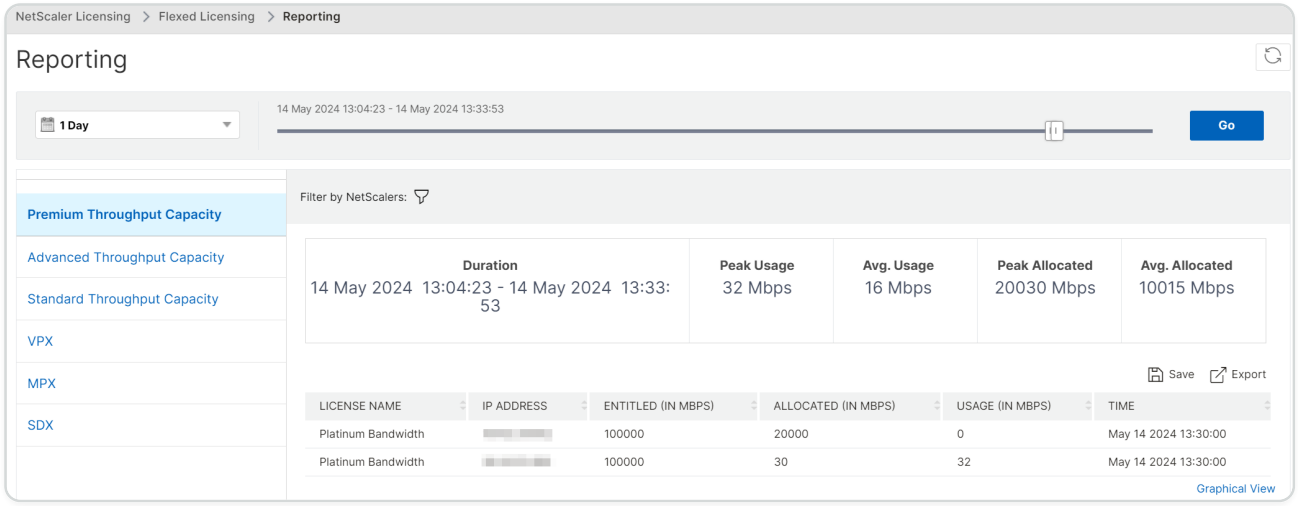
- **Peak usage** = The sum of the highest datapoint (Mbps) from the 24 hours of all NetScaler instances. For example, if the highest datapoint from the 24-hour duration for NetScaler A is 30 Mbps, NetScaler B is 45 Mbps, and NetScaler C is 120 Mbps, then the peak usage is displayed as 195 Mbps (30 + 45 + 120).
- **Average usage** = The sum of all the 24 hours datapoints divided by 24 for each NetScaler instance. So, for 3 NetScaler instances, the total average of all 3 NetScaler instances divided 3. For example, if NetScaler A average is 25 Mpbs, NetScaler B average is 20 Mpbs, and NetScaler C average is 45 Mbps, the average usage is displayed as 30 Mbps (25 + 20 + 35 divided by 3).

Similarly, the peak and average allocation details are displayed using the same logic.

You can select the duration from the list, starting from an hour to a year, and view the details in both tabular view and graphical view.

The following example shows the tabular view for the instances using Flexed license (Premium bandwidth):

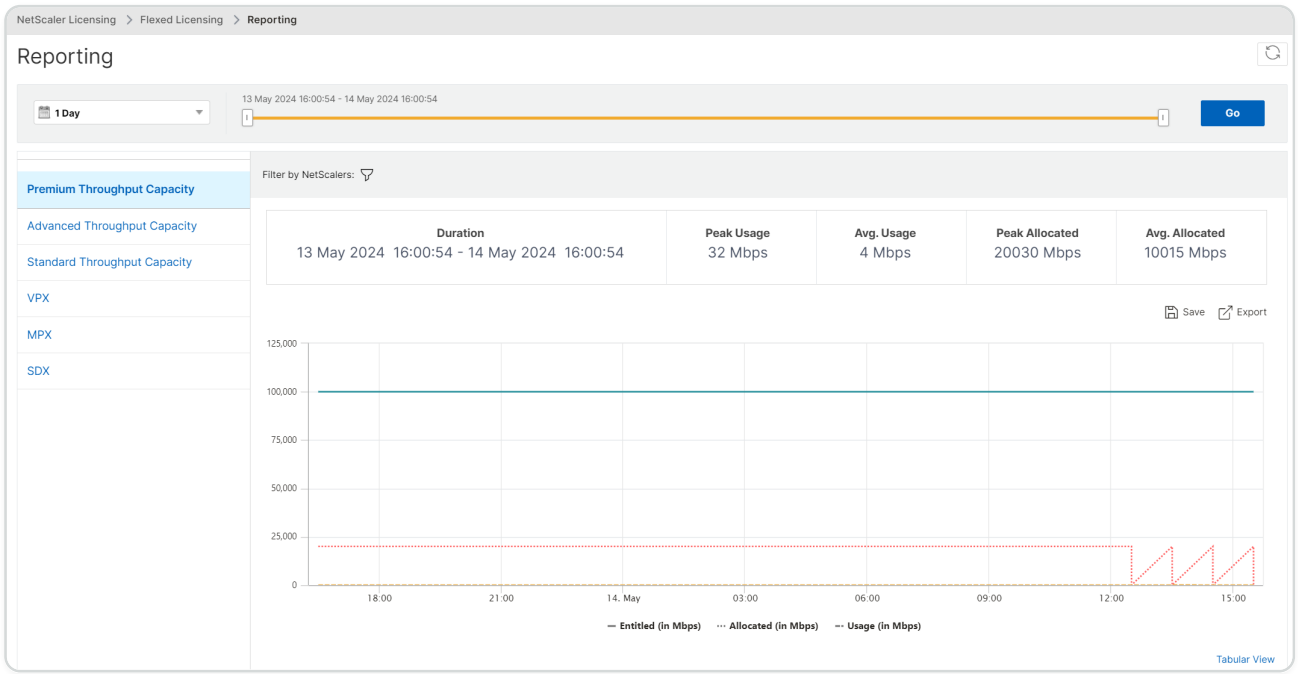
© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following details appear on the dashboard:

- **Peak usage** - The highest usage (in Mbps) for the selected duration.
- **Average usage** - The average usage (in Mbps) for the selected duration.
- **Peak allocated** - The highest allocation for the selected duration.
- **Average allocation** - The average allocation for the selected duration.
- **Filter** - You can select one or more instances to view the usage and allocation details for the specific instances.
- **Export** - You can export details in PDF, JPEG, and PNG format.

The following example shows the graphical view for the instances using Flexed license (Premium bandwidth):



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Transition to Flexed licensing

IMPORTANT:

File-based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler® versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Supported from early September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Note: LAS support for Console on-prem is from release 14.1-51.x onwards. However, file-based licensing is deprecated as of April 15 2026 from Console on-prem releases 14.1-51.x onwards and 13.1-60.x onwards. If you upgrade to Console on-prem release 14.1-51.x or release 13.1-60.x or later, you can continue using file-based licensing until 15th April 2026. However you must upgrade to Console on-prem release 14.1-51.x or later, and switch to LAS before 15th April 2026 because Console on-prem 13.1 does not support LAS.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don’t apply where prohibited by law or regulation.
Read the following note before proceeding further.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

You must switch to the Flexed licensing before the expiry of your current license. While planning the transition keep the following steps in mind, and plan a maintenance window if the steps involve a license reconfiguration or NetScaler reboot.

LAS-based licenses

NOTE:

Ensure your NetScaler (ADC and SDX) instances are on LAS-compatible versions.

Information related to migration for the following license, see Migrate existing licensed instances.

- Flexed licensing (file-based licenses) to Flexed licensing (LAS-based licenses)
- Pooled licensing (file-based licenses) to Flexed licensing (LAS-based licenses)

Information related to transition for the following license, see License Activation Service.

- Pooled vCPU licensing (file-based licenses) to Flexed licensing (LAS-based licenses)
- Fixed subscription or Perpetual licensing (file-based licenses) to Flexed licensing (LAS-based licenses)
- Fixed vCPU licensing (file-based licenses) to Flexed licensing (LAS-based licenses)
- CICO licensing (file-based licenses) to Flexed licensing (LAS-based licenses)
- Self-Managed licensing (file-based licenses) to Flexed licensing (LAS-based licenses)
- Self-Managed vCPU licensing (file-based licenses) to Flexed licensing (LAS-based licenses)

Manually managed entitlements (file-based licenses)

The following sections describe the steps to transition from existing license types to Flexed licensing (file-based licenses).

Pooled bandwidth license to Flexed licensing

Some steps are common to MPX, SDX, and VPX. These steps are listed first, followed by the steps specific to MPX, SDX, or VPX.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Common steps for VPX/MPX/SDX

1. Upload and apply Flexed licenses on NetScaler Console. See License files.
2. If you have a Z-Cap software license that is valid for a specific period, apply that license on NetScaler hardware (MPX/SDX).

For VPX/MPX

The following additional steps are needed:

1. If you have a Pooled Premium (Platinum) bandwidth license, the license automatically switches to Flexed after the expiry of the old license.
2. If you have a Pooled Standard or Pooled Advanced bandwidth license, manually check out Premium bandwidth and warm reboot NetScaler.

For SDX

NOTE:

Ensure that you switch to the Flexed licensing before the expiry of your current license.

The following additional steps are needed:

1. Check out the required instance and bandwidth license from Flexed licensing to SDX. SDX reboot is not required.
2. If all VPX on SDX have a Premium edition, the license automatically switches to Flexed after the expiry of the old license.
3. Change the edition for all the VPX (on SDX) with Standard or Advanced to Premium. These VPX instances are automatically rebooted.
4. Reduce the Standard and Advanced bandwidth capacity on SDX to zero.

Pooled vCPU to Flexed licensing

For VPX

1. Upload and apply Flexed licenses on NetScaler Console. See License files.
2. Remove the existing license server using the NetScaler GUI. NetScaler is unlicensed until all the steps are completed.
3. Add the license server with Flexed/Pooled option.
4. Check out the required instance and bandwidth licenses to NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Warm reboot NetScaler.

Fixed subscription or Perpetual license to Flexed licensing

Some steps are common to MPX, SDX, and VPX. These steps are listed first, followed by the steps specific to MPX, SDX, or VPX.

Common steps for VPX/MPX/SDX

1. Onboard to NetScaler Console.
2. Deploy the NetScaler agent.
3. Upload and apply Flexed licenses on NetScaler Console. See License files.
4. Apply Z-Cap software license on NetScaler hardware (MPX/SDX).

For VPX/MPX

The following additional steps are needed:

1. Check out the required instance and bandwidth licenses to NetScaler.
2. Warm reboot NetScaler.
3. Delete the Fixed subscription license after NetScaler reboots.

For SDX

The following additional steps are needed:

1. Check out the required instance and bandwidth license from Flexed licensing on SDX.
2. If all VPX on SDX have the premium edition, SDX reboot is not required.
3. If any VPX has the Advanced or Standard edition, that VPX must be shifted to the premium edition. The VPX automatically reboots.
4. Apply Z-Cap software license on NetScaler SDX.
5. Check out the required instance and bandwidth license from Flexed licensing on SDX.
6. Delete the Fixed subscription license after NetScaler reboots.

Fixed vCPU to Flexed licensing

For VPX

1. Onboard to NetScaler Console.
2. Deploy the NetScaler agent.
3. Upload and apply Flexed licenses on NetScaler Console. See License files.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Configure the license server on NetScaler in Flexed/Pooled mode.
5. Check out the required instance and bandwidth licenses to NetScaler.
6. Warm reboot NetScaler.
7. Delete the Fixed license after NetScaler reboots.

CICO to Flexed licensing

For VPX

1. Upload and apply Flexed licenses on NetScaler Console. See License files.
2. Remove the existing license server using the NetScaler GUI. NetScaler is unlicensed until all the steps are completed.
3. Add the license server with Flexed/Pooled option.
4. Check out the required instance and bandwidth licenses to NetScaler.
5. Warm reboot NetScaler.

Self Managed bandwidth license to Flexed licensing

Some steps are common to MPX, SDX, and VPX. These steps are listed first, followed by the steps specific to MPX, SDX, or VPX.

Common steps for VPX/MPX/SDX

1. Upload and apply Flexed licenses on NetScaler Console. See License files.
2. If you have a Z-Cap software license that is valid for a specific period, apply that license on NetScaler hardware (MPX/SDX).

For VPX/MPX

1. If you have a Self Managed Premium license, change the license mode using the NetScaler GUI from Self Managed Pool to Flexed/Pooled.
2. NetScaler reboot is not required.
3. If you have a Self Managed Standard or Advanced license, remove the existing license server using the NetScaler GUI.
4. Add the license server with the Flexed/Pooled option.
5. Check out the Flexed Premium bandwidth capacity to VPX/MPX.
6. Warm reboot NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For SDX

1. If all VPX on SDX have a Self Managed Premium license, change the license mode using the NetScaler GUI from Self Managed Pool to Flexed/Pooled.
2. NetScaler reboot is not required.
3. If some VPX on SDX have a Self Managed Standard or Advanced license, contact Citrix Support.

Self Managed vCPU to Flexed licensing

For VPX

1. Upload and apply Flexed licenses on NetScaler Console. See License files.
2. Remove the existing license server using the NetScaler GUI. NetScaler is unlicensed until all the steps are completed.
3. Add the license server with Flexed/Pooled option.
4. Check out the required instance and bandwidth licenses to NetScaler.
5. Warm reboot NetScaler.

Scenarios for Flexed or Pooled license expiry and connectivity issues behavior

IMPORTANT:

File-based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler® versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Supported from early September 2025.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler Console on-prem: 14.1-51.x

  Note: LAS support for Console on-prem is from release 14.1-51.x onwards. However, file-based licensing is deprecated as of April 15 2026 from Console on-prem releases 14.1-51.x onwards and 13.1-60.x onwards. If you upgrade to Console on-prem release 14.1-51.x or release 13.1-60.x or later, you can continue using file-based licensing until 15th April 2026. However you must upgrade to Console on-prem release 14.1-51.x or later, and switch to LAS before 15th April 2026 because Console on-prem 13.1 does not support LAS.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don’t apply where prohibited by law or regulation.

LAS-based licenses

Before the term expires

If the license is renewed before its expiration:

- The NetScaler instance seamlessly switches to the new license after the old one expires, provided the device is up and running.
- A restart is not required.
- The NetScaler does not need a manual capacity reconfiguration.

After the term expires

If the license is not renewed before its term expires, the NetScaler instance stops normal operations.

- It loses its configuration.
- All traffic processing shuts down completely.

Scenarios for connectivity issues behavior

If connectivity between a NetScaler and the NetScaler Console service is lost, the device enters a 30-day grace period.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

During the grace period, licensing functions normally. However, on the thirty-first day, the following occurs:

- NetScaler VPX™, CPX, BLX, and MPX instances undergo a forced reboot and become unlicensed.
- The throughput for all VPX instances on a NetScaler SDX™ is reduced to 1 Mbps.

Manually managed license (file-based license)

This document presents different scenarios of license expiry and connectivity issues behavior in NetScaler MPX, NetScaler SDX, and NetScaler VPX/NetScaler BLX/NetScaler CPX.

Components of Flexed licenses

- Software instance (VPX/BLX/CPX, SDX, MPX, VPX FIPS)
- Bandwidth capacity

Scenario: MPX form factor

You are using Flexed or Pooled licensing and the licenses are due to expire soon. The following scenarios explain the behavior when a new license is uploaded on NetScaler Console before and after the term expires, or when a license file is not present.

Before the term expires

If the new license is uploaded before the term expires and the old license is still valid, two different pools of capacity (old and new) are available.

- If NetScaler is up and running, it switches to the new Flexed or Pooled license seamlessly after the old license expires.
- A restart is not required.
- NetScaler does not require a manual capacity reconfiguration.

After the term expires

NetScaler instance stops its normal operations after the license expiry, including configuration loss and complete shutdown of traffic processing.

Before or after term expiry if license edition of old and new are different

If the license edition of old and new are different, then irrespective of before or after the term expires, you must perform the following:

- Bandwidth must be manually reconfigured. In NetScaler GUI:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Navigate to **System > Licenses > Manage Licenses**.

b. Click **Release Allocation** to release the allocation.

c. Click **Change Allocation** to reallocate the bandwidth and change the bandwidth to premium.

- Restart NetScaler.

Scenario: SDX form factor

You are using Flexed or Pooled licensing and the licenses are due to expire soon. The following scenarios explain the behavior when a new license is uploaded on NetScaler Console before and after the term expires, or when a license file is not present.

Before the term expires

If the new license is uploaded before the term expires and the old license is still valid, two different pools of capacity (old and new) are available.

- If NetScaler is up and running, it switches to the new Flexed or Pooled license seamlessly after the old license expires.
- A restart is not required.
- NetScaler does not require a manual capacity reconfiguration.

After the term expires

NetScaler instance stops its normal operations after the license expiry, including configuration loss and complete shutdown of traffic processing.

If license edition of old and new are different

Before the term expires

- Ensure that both old and new license files exist on the Console.
- Bandwidth must be manually reconfigured. In the NetScaler SDX GUI:

  a. Navigate to **System > Licenses > Manage Licenses**.

  b. Click **Release Allocation** to release the allocation.

  c. Click **Change Allocation** to reallocate the bandwidth and change the bandwidth to premium.

- Change all the edition of VPX to premium to reboot the VPX instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Click **Change Allocation** and retain only premium bandwidth. Delete all other bandwidth allocations.

After the term expires

NetScaler instance stops its normal operations after the license expiry, including configuration loss and complete shutdown of traffic processing.

- Delete the VPX instances on SDX.
- Click **Change allocation** to reallocate the bandwidth for SDX on Console.
- Reprovision the VPX with premium edition on SDX.

Scenario: VPX/BLX/CPX form factor

You are using Flexed or Pooled licensing and the licenses are due to expire soon. The following scenarios explain the behavior when a new license is uploaded on NetScaler Console before and after the term expires, or when a license file is not present.

Before the term expires

If the new license is uploaded before the term expires, and the old license is still valid, two different pools of capacity (old and new) are available.

- If NetScaler is up and running, it switches to the new Flexed or Pooled license seamlessly after the old license expires.
- A restart is not required.
- NetScaler does not require a manual capacity reconfiguration.

After the term expires

NetScaler instances with expired licenses managed through NetScaler Console stop to process traffic and might result in configuration loss.

Before or after term expiry if license edition of old and new are different

If the license edition of old and new are different, then irrespective of before or after the term expires, you must perform the following:

- Bandwidth must be manually reconfigured. In NetScaler VPX/BLX/CPX GUI:
  a. Navigate to **System > Licenses > Manage Licenses**.
  b. Click **Release Allocation** to release the allocation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Click **Change Allocation** to reallocate the bandwidth and change the bandwidth to premium.

- Restart VPX/BLX/CPX instance.

Scenarios for connectivity issues behavior

If connectivity breaks between NetScaler and agent, or agent and NetScaler Console service, the behavior is as follows:

- NetScaler goes into grace for 30 days.
- During this grace period, licensing functionality continues to work until the thirtieth day.
- On the thirty-first day,
  - NetScaler VPX/NetScaler CPX/NetScaler BLX and NetScaler MPX undergo a forced reboot and become unlicensed.
  - The throughput on all the VPX on NetScaler SDX is decreased to 1 Mbps.

Configure NetScaler Console server only as the Flexed or Pooled license server

IMPORTANT:

File-based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (Citrix Platform License/Universal Hybrid Multi-Cloud), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Supported from early September 2025.
- NetScaler Console on-prem: 14.1-51.x

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:** LAS support for Console on-prem is from release 14.1-51.x onwards. However, file-based licensing is deprecated as of April 15 2026 from Console on-prem releases 14.1-51.x onwards and 13.1-60.x onwards. If you upgrade to Console on-prem release 14.1-51.x or release 13.1-60.x or later, you can continue using file-based licensing until 15th April 2026. However you must upgrade to Console on-prem release 14.1-51.x or later, and switch to LAS before 15th April 2026 because Console on-prem 13.1 does not support LAS.

All the other forms of legacy NetScaler licenses such as NetScaler virtual CPU licensing (Pooled vCPU), NetScaler VPX Check-In and Check-Out (CICO), perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS-based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don’t apply where prohibited by law or regulation.
As an administrator, you can configure the NetScaler Console only for the Pooled licensing feature. With this configuration, the NetScaler Console only receives licensing data from NetScaler instances.

Sometimes, you might have the regulatory mandate that requires restricting NetScaler instances’ data from leaving the regulatory zone. In such situations, you can deploy a local instance of an NetScaler Console server in your regulatory zone to use management, monitoring, and analytics capabilities. When you take the same approach to use the Pooled licenses feature, you have to split Pooled licenses across various NetScaler Console license servers. This approach does not provide you the flexibility to allocate Pooled licenses across your globally deployed NetScaler instances.

Therefore, configure the NetScaler Console only for the Pooled licensing feature. The NetScaler Console receives only licensing data from all NetScaler instances. So, you can adhere to the regulatory mandate and dynamically allocate Pooled capacity licenses across globally deployed NetScaler instances.

This document explains how to configure the NetScaler Console only for the Pooled licensing feature.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

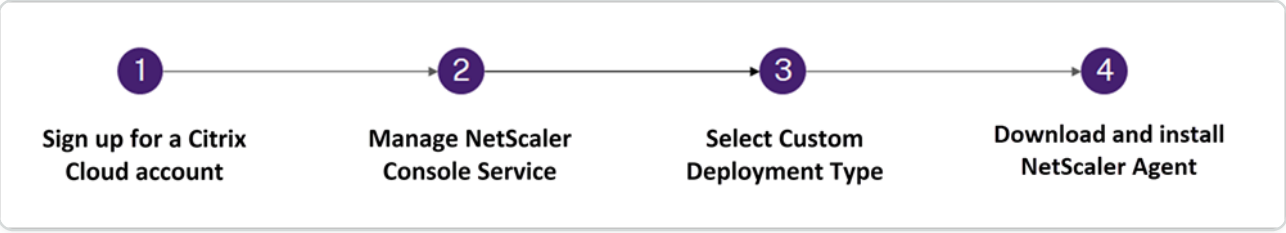
Prerequisites

Before you configure the NetScaler Console only for the Pooled licensing feature, complete the first time onboarding and setting up the NetScaler Console. Ensure to review the agent specifications in System requirements.

IMPORTANT

When you first time onboard or set up the NetScaler Console, ensure the following:

- The Custom Deployment option is selected.
- NetScaler instances to be added after you complete step 4 in this configuration procedure



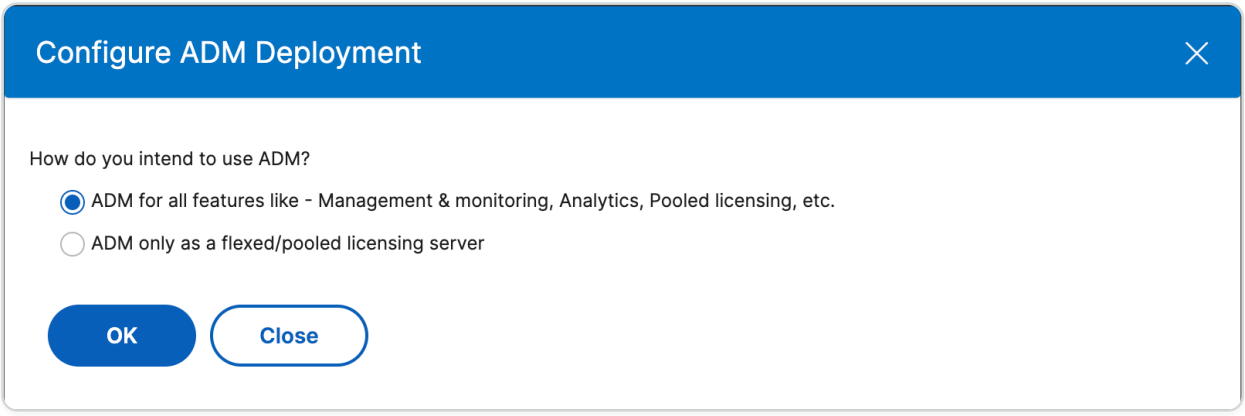
For more information about onboarding and setting up the NetScaler Console, see Getting started.

After you complete the onboarding steps, configure the NetScaler Console only for the Pooled licensing feature.

How to configure NetScaler Console only as the Flexed or Pooled license server

Do the following to configure the NetScaler Console only for the licensing feature:

1. Navigate to **Settings > Global Settings > System Configurations > System Deployment**.
2. In **NetScaler Console Deployment**, select **NetScaler Console only as a flexed/pooled licensing server**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Click **OK**.

   This action retains only the Pooled licensing feature and disables the following NetScaler Console features:

   - NetScaler Console backup
   - Event management
   - SSL certificate management
   - Network reporting
   - Network functions
   - Configuration audit

   NOTE

   By default, the NetScaler Console analytics feature is disabled. Make sure to disable this feature if you have enabled it.

   In the confirmation box, click **Yes**.

   The NetScaler Console GUI now displays only the Pooled licensing feature. And, the remaining features do not appear.

4. After you configure NetScaler Console only for the licensing feature, add NetScaler instances in the **Infrastructure > Instances** page.

NOTE

- You can add a NetScaler instance in the NetScaler Console and other NetScaler Console servers as well. When you change the password of such NetScaler instances, ensure to update the password on all NetScaler Console servers where the instance is discovered. This note applies when the NetScaler Console is configured only to use the pooled licensing feature.
- A user can still do some operations of the disabled features in the NetScaler Console GUI. For example, event polling and NetScaler backup. As a super administrator, If you want to restrict such operations, disable user accesses for other administrators using an appropriate access policy. For more information, see Configure Access Policies on NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Legacy licenses

The legacy licensing options enable you to manage the earlier NetScaler licensing models, such as Pooled capacity, check-in and check-out licensing, and virtual CPU licensing. You can also upgrade perpetual licenses and troubleshoot Pooled capacity license issues for NetScaler® deployments.

The following topics help you manage legacy licenses:

- NetScaler Pooled capacity
- Upgrading a perpetual license in NetScaler MPX to ADC Pooled capacity
- Upgrade a perpetual license in NetScaler SDX to ADC Pooled capacity
- NetScaler VPX check-in and check-out licensing
- NetScaler virtual CPU licensing
- FAQs and other resources
- Troubleshoot Pooled capacity license issues

Pooled capacity

IMPORTANT:

File-based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler® versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Supported from early September 2025.
- NetScaler Console on-prem: 14.1-51.x

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:** LAS support for Console on-prem is from release 14.1-51.x onwards. However, file-based licensing is deprecated as of April 15 2026 from Console on-prem releases 14.1-51.x onwards and 13.1-60.x onwards. If you upgrade to Console on-prem release 14.1-51.x or release 13.1-60.x or later, you can continue using file-based licensing until 15th April 2026. However you must upgrade to Console on-prem release 14.1-51.x or later, and switch to LAS before 15th April 2026 because Console on-prem 13.1 does not support LAS.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don’t apply where prohibited by law or regulation.
Pooled capacity in NetScaler is a licensing framework that comprises a common bandwidth and instance pool that is hosted on and served by NetScaler Console. From this common pool, each NetScaler instance in your data center, regardless of platform or form factor, checks out one instance license and only as much bandwidth as it needs. The license file and the bandwidth are not bound to the instance. When the instance no longer requires these resources, it checks them back in to the common pool, making the resources available to other instances that need them.

NOTE

In NetScaler Console, one of the agents is the license server.

This licensing framework maximizes bandwidth utilization by ensuring that instances are not allocated bandwidth more than their requirement. The ability of the NetScaler instances to check licenses and bandwidth in and out of a common pool also enables you to automate instance provisioning.

You can increase or decrease the bandwidth allocated to an instance at run time without impacting traffic. You can also transfer the licenses in the pool from one instance to another.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Upgrade a perpetual license in NetScaler MPX to NetScaler Pooled capacity

IMPORTANT:

File-based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler® versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Supported from early September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Note: LAS support for Console on-prem is from release 14.1-51.x onwards. However, file-based licensing is deprecated as of April 15 2026 from Console on-prem releases 14.1-51.x onwards and 13.1-60.x onwards. If you upgrade to Console on-prem release 14.1-51.x or release 13.1-60.x or later, you can continue using file-based licensing until 15th April 2026. However you must upgrade to Console on-prem release 14.1-51.x or later, and switch to LAS before 15th April 2026 because Console on-prem 13.1 does not support LAS.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don’t apply where prohibited by law or regulation.
NetScaler MPX appliance with perpetual license can be upgraded to NetScaler Pooled capacity license. Upgrading to NetScaler Pooled capacity license enables you to allocate licenses from the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

license pool to NetScaler appliances on demand. NetScaler can use one license at a time which is either use perpetual license or use the pooled license. A customer can make a switch from a pooled license to a perpetual license. As long as the perpetual license is valid, you can reconfigure the NetScaler and remove the pooled licensing config. When a customer makes a switch from perpetual license to pooled license or pooled to perpetual license, all the NetScaler instances are restarted.

You can also configure the NetScaler Pooled capacity license for NetScaler instances configured in high availability mode. To configure NetScaler Pooled capacity license for NetScaler MPX instances in high availability mode, see Upgrading the perpetual license in NetScaler MPX high availability pair to NetScaler Pooled capacity.

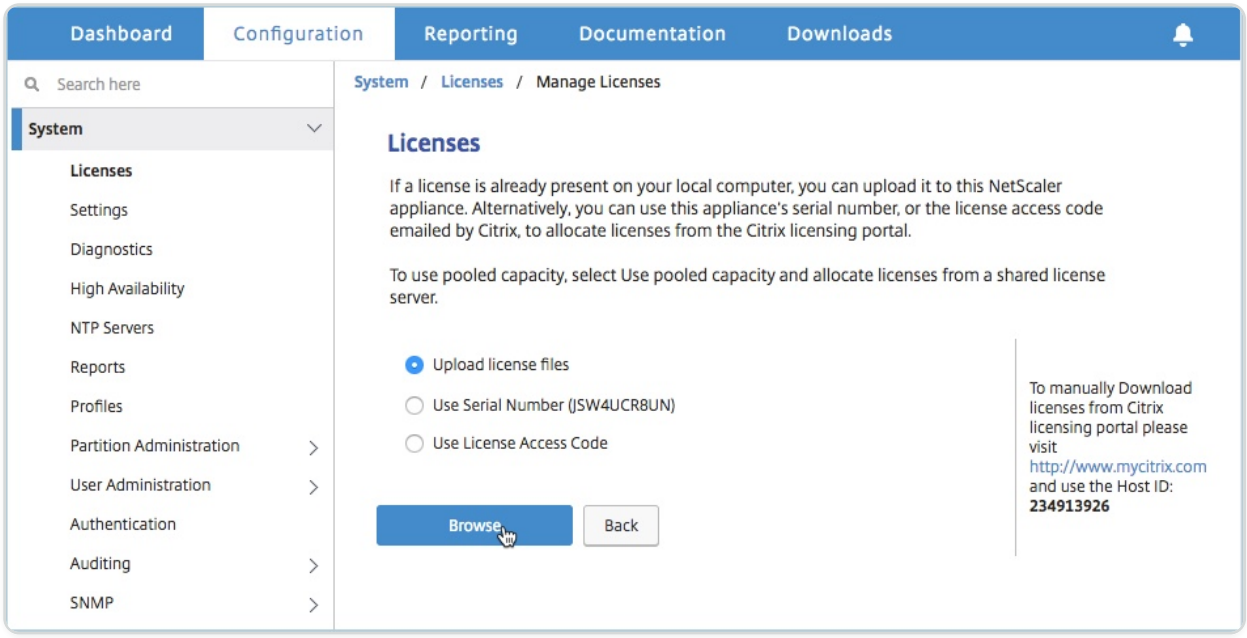
NOTE

For upgrading NetScaler MPX appliance to NetScaler Pooled capacity license, you need to upload the MPX-Z license to the appliance.

To upgrade to NetScaler Pooled capacity:

1. In a Web browser, type the IP address of the NetScaler appliance, such as `<http://192.168.100.1>`.
2. In **User Name** and **Password** fields, type the administrator credentials.
3. On the **Welcome** page, click **Continue**.
4. Upload the zero capacity license (MPX-Z license). On the Configuration tab, navigate to **System** \> **Licenses**.
5. In the details pane, click **Manage Licenses**, click Add **New License**.
6. In the **Licenses** page, select **Upload license files** and click **Browse** to select the zero capacity license from your local machine.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

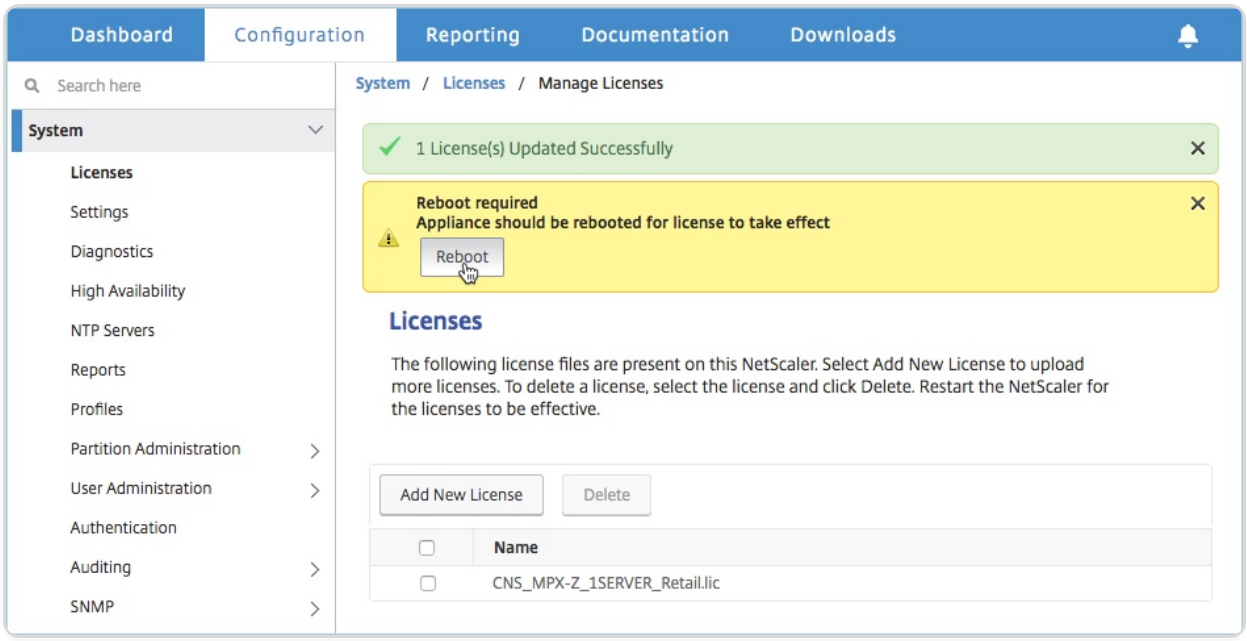


7. After the license is uploaded, click **Reboot** to reboot the appliance.

WARNING

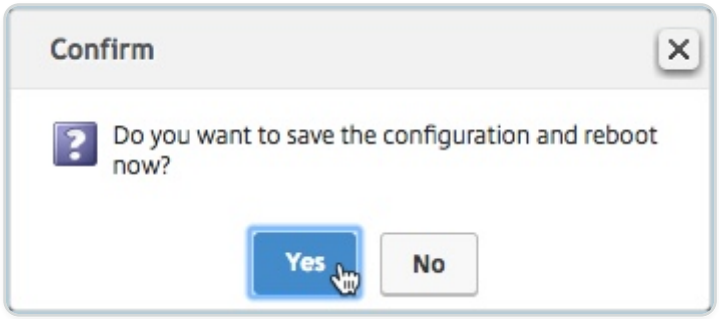
After applying the MPX-Z license, the features including SSL offloading on the appliance become unlicensed. The appliance stops processing HTTPS requests.

If the **Secure Access Only** option is enabled on the appliance before the upgrade, you cannot connect to the appliance through NetScaler Console GUI using HTTPS.

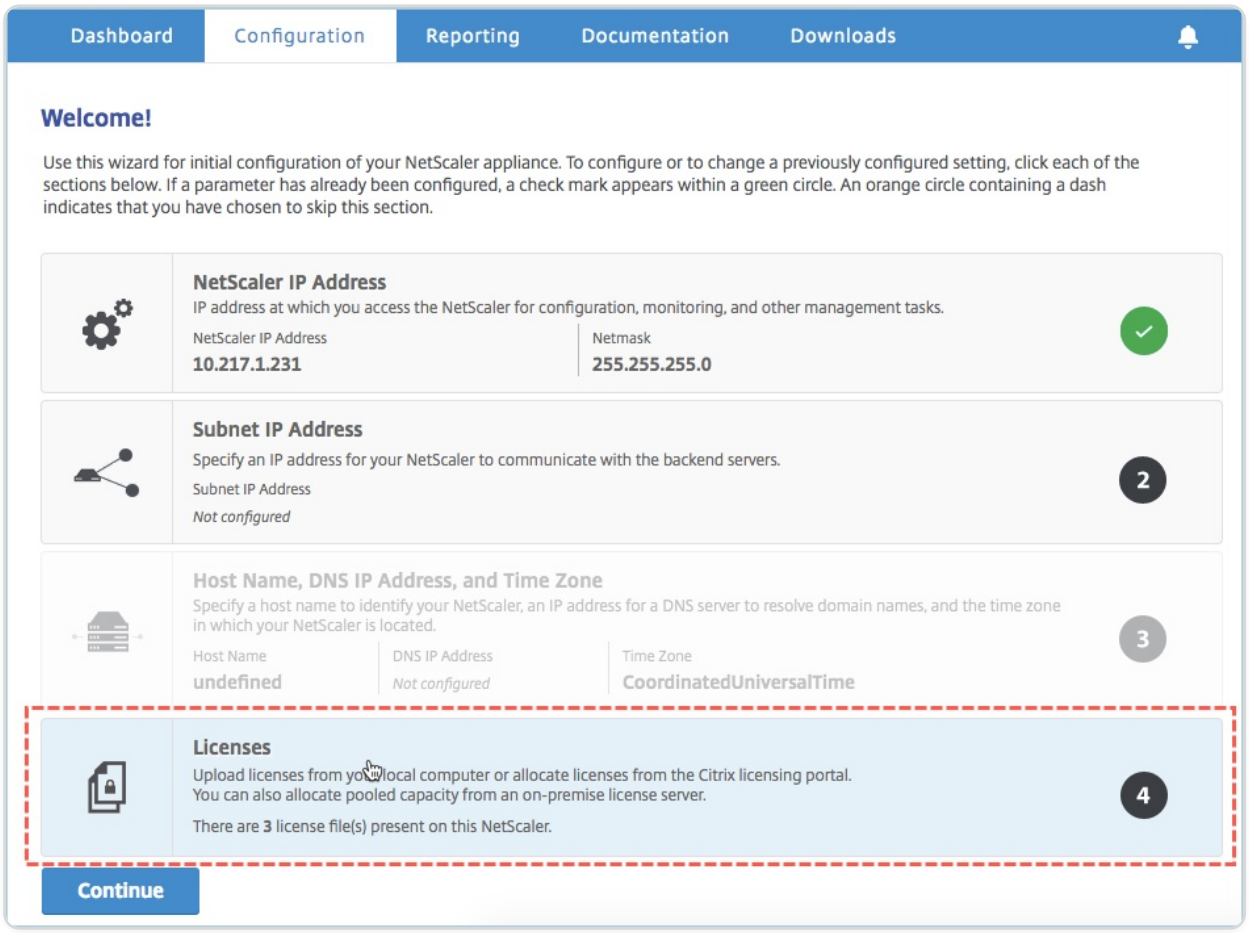


8. On the **Confirm** page, click **Yes**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

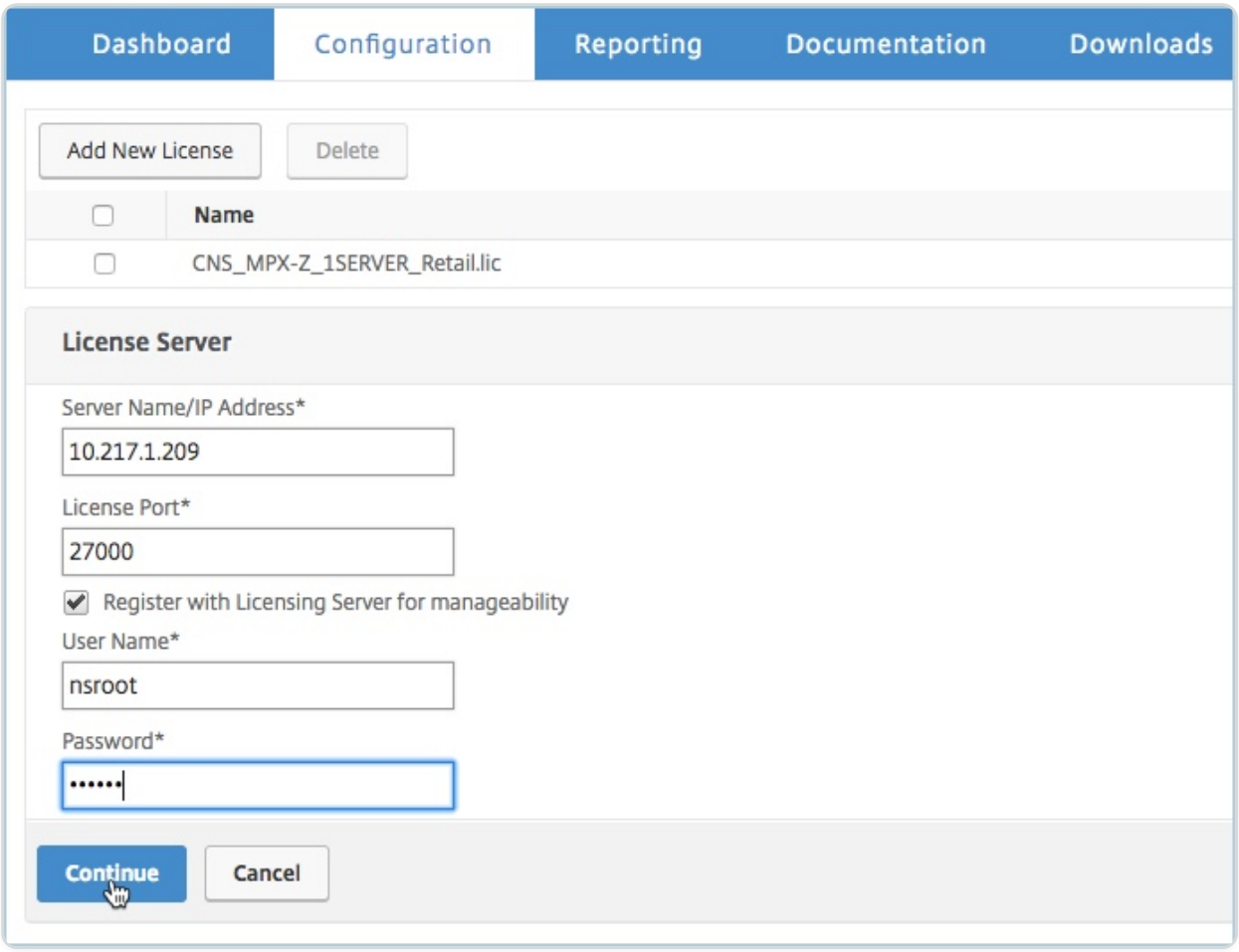


9. After the appliance reboots, logon to the appliance.
10. On the Welcome page, click the **Licenses** section.



11. In the **License Server** section, do the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



a. In the **Server Name/IP Address** field, enter the license server details.

b. In the **License Port** field, enter the license server port. Default value: 27000.

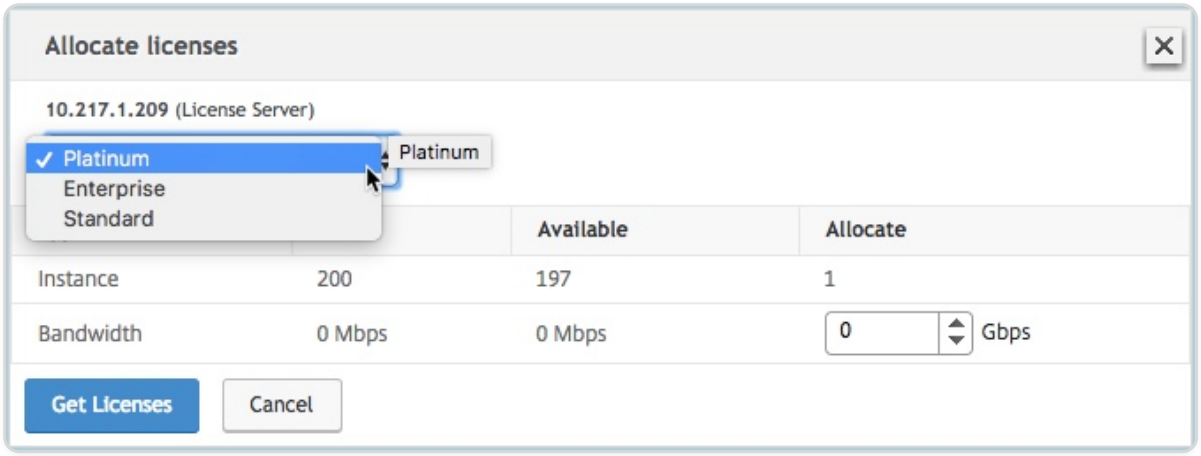
c. If you want to manage your instance's pool licenses through NetScaler Console, select the **Register with Licensing Server for manageability** checkbox and enter NetScaler Console credentials.

d. Click **Continue**.

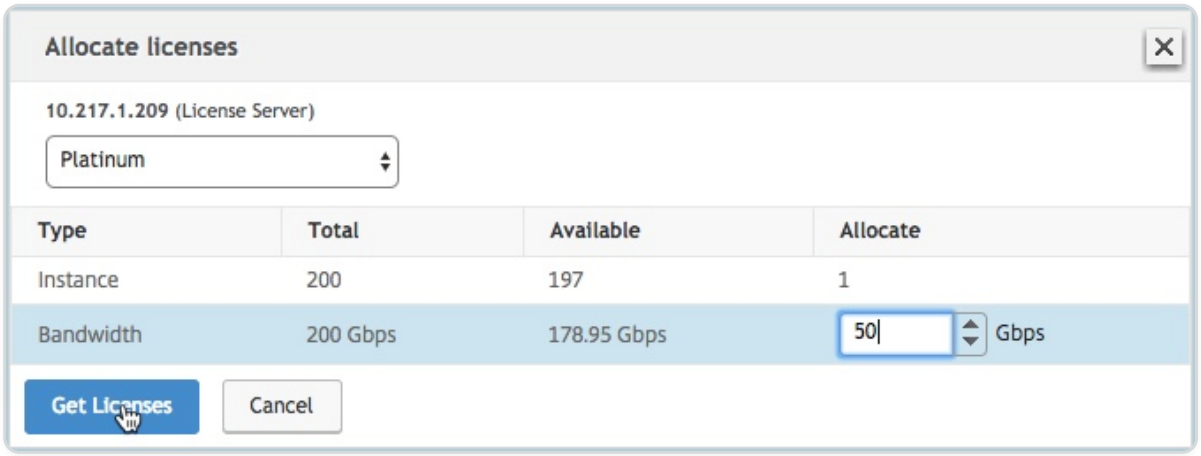
12. In the Allocate licenses window, do the following:

    a. Select the license edition from the drop-down list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

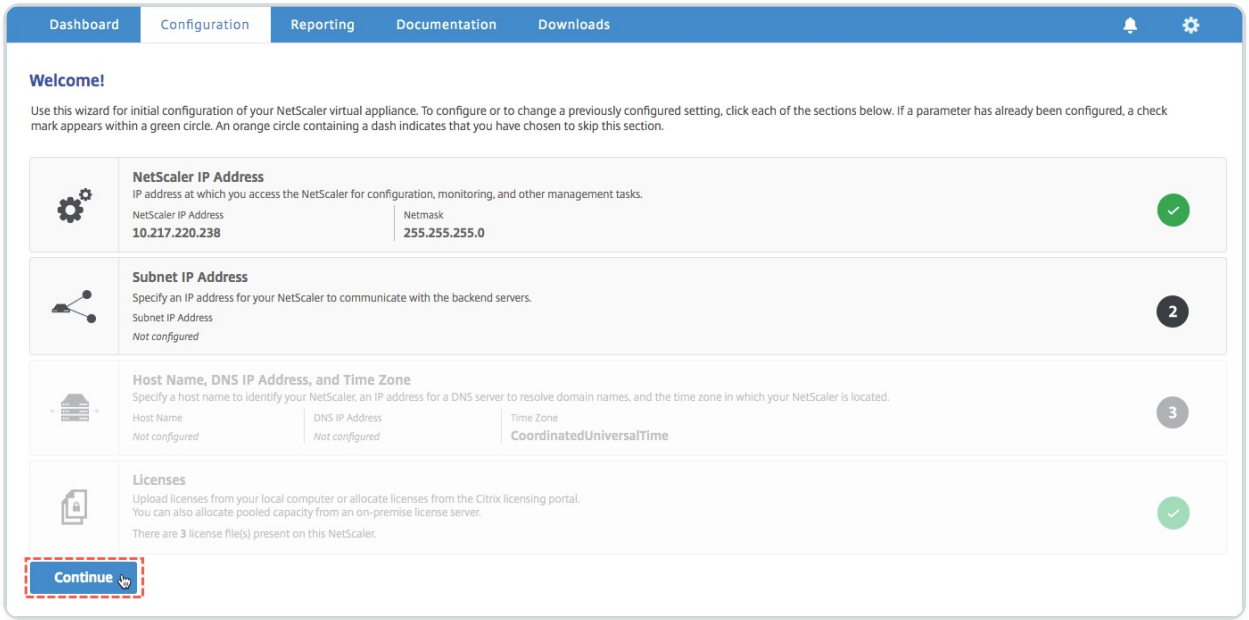


b. Allocate the bandwidth to the NetScaler appliance from the **Allocate** menu and click **Get Licenses**.



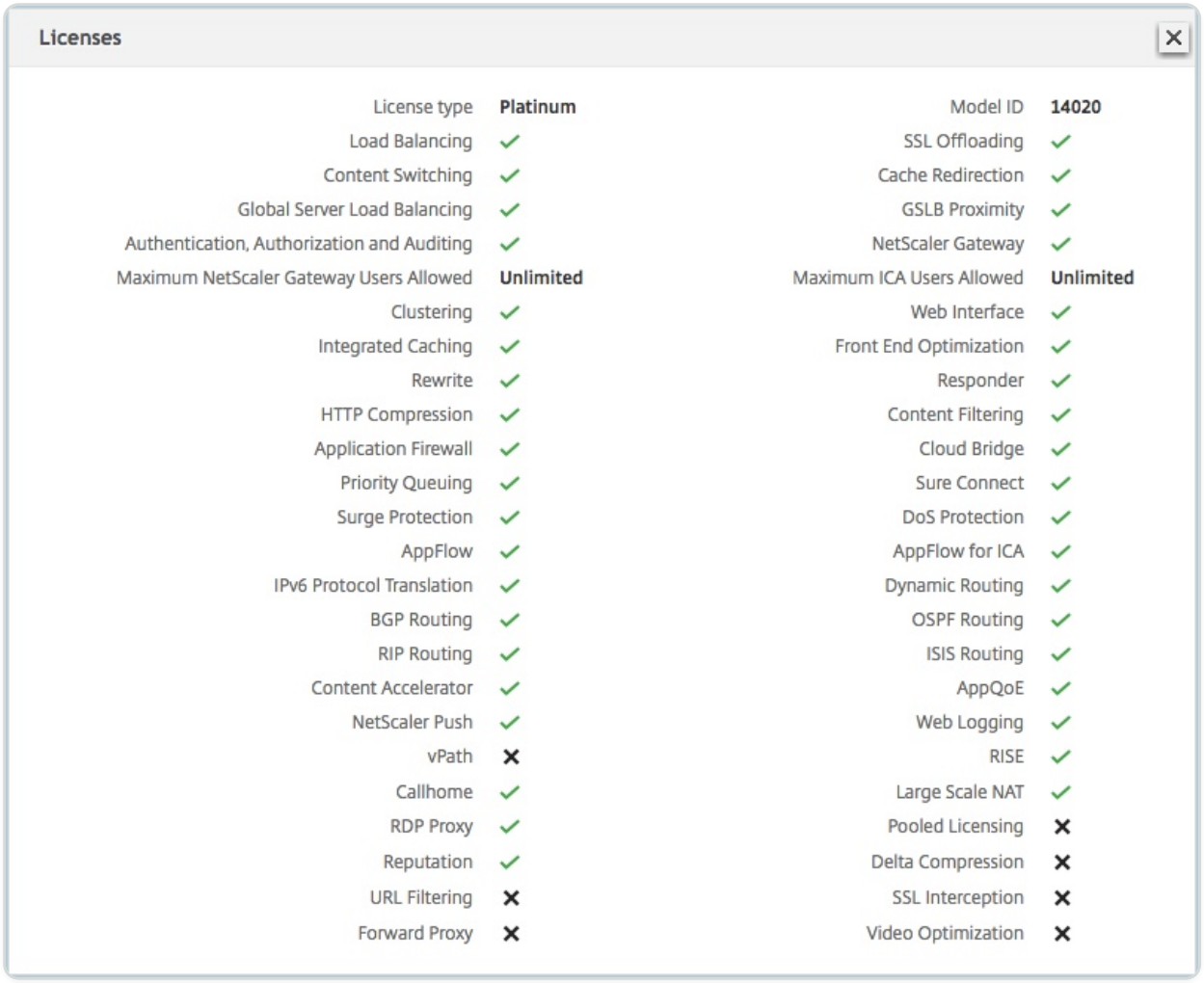
c. When prompted, click **Reboot** to reboot the appliance.

13. Once the NetScaler MPX appliance reboots, logon to the NetScaler MPX appliance. On the **Welcome** page, click **Continue**.

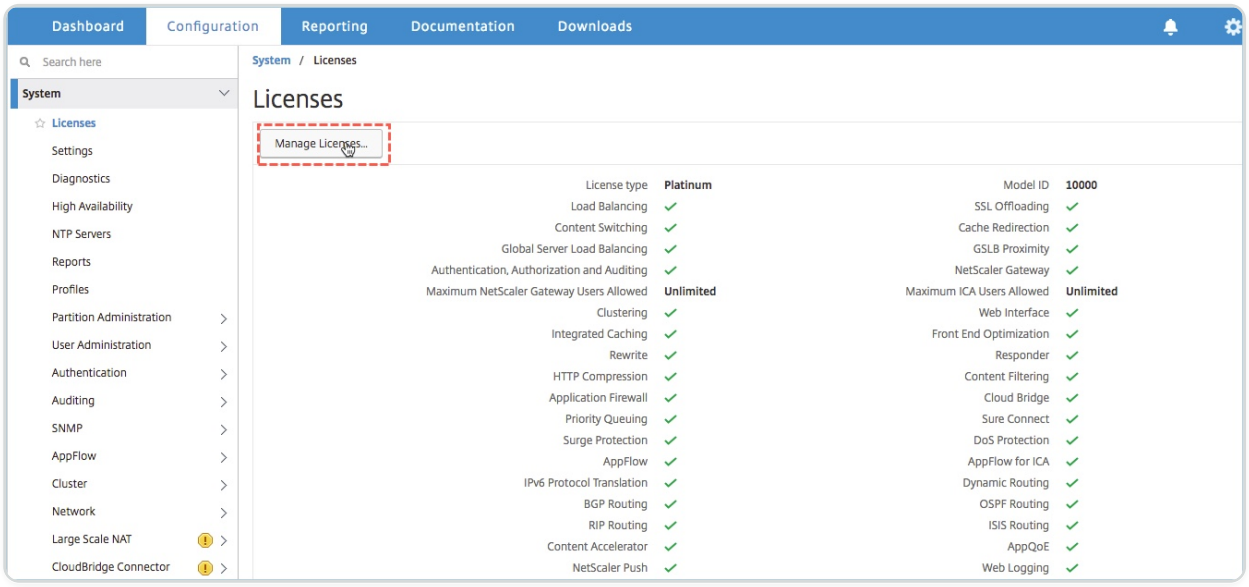


The **Licenses** page lists all the licensed features.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

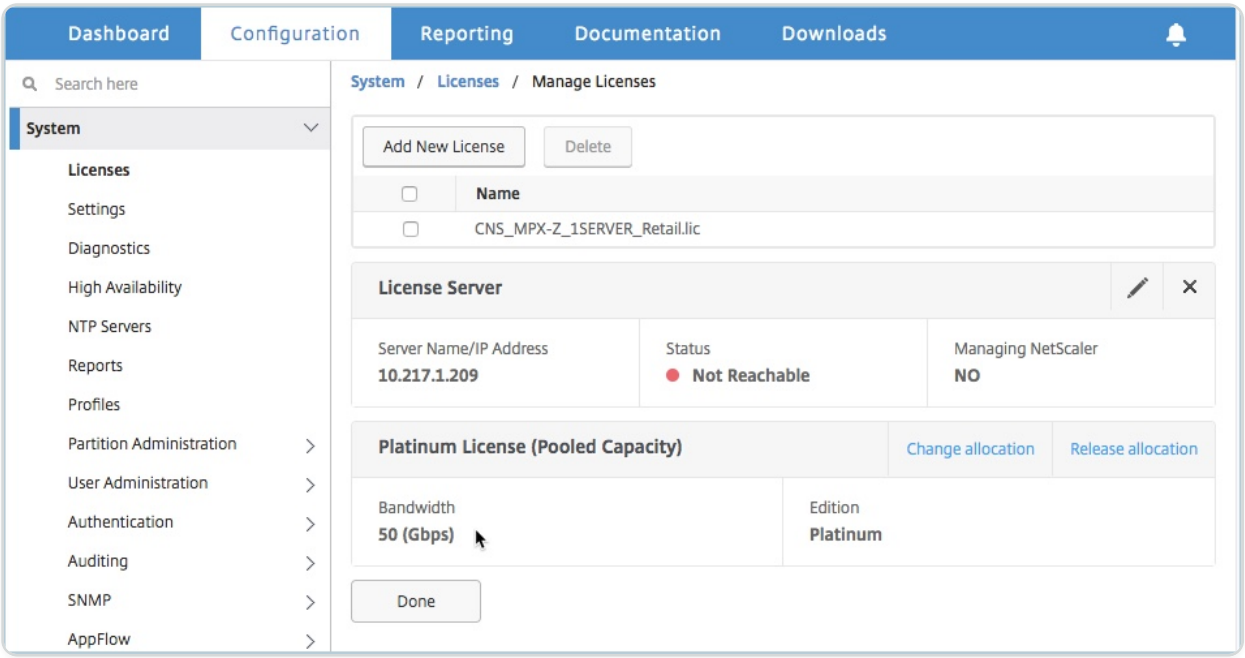


14. Navigate to **System \> Pooled Licensing** and click **Manage Licenses**.



On the **Manage Licenses** page, you can view the details of the license server, license edition and the allocated bandwidth.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Upgrading the perpetual license in NetScaler MPX high availability pair to NetScaler Pooled capacity

For the NetScaler MPX appliances configured in high availability mode, you have to configure NetScaler Pooled capacity on both the primary and secondary NetScaler instances in the HA pair. You need to allocate licenses of the same capacity to both the primary and secondary NetScaler instances in the HA pair. For example, if you want 1 Gbps capacity from each instance in the HA pair, you need to allocate 2 Gbps capacity from the common pool so that you can allocate 1 Gbps capacity each to the primary and secondary NetScaler instances in the HA pair.

IMPORTANT

For upgrading NetScaler MPX appliance to use NetScaler Pooled capacity license, you need to upload the MPX-Z to the appliance.

Prerequisites

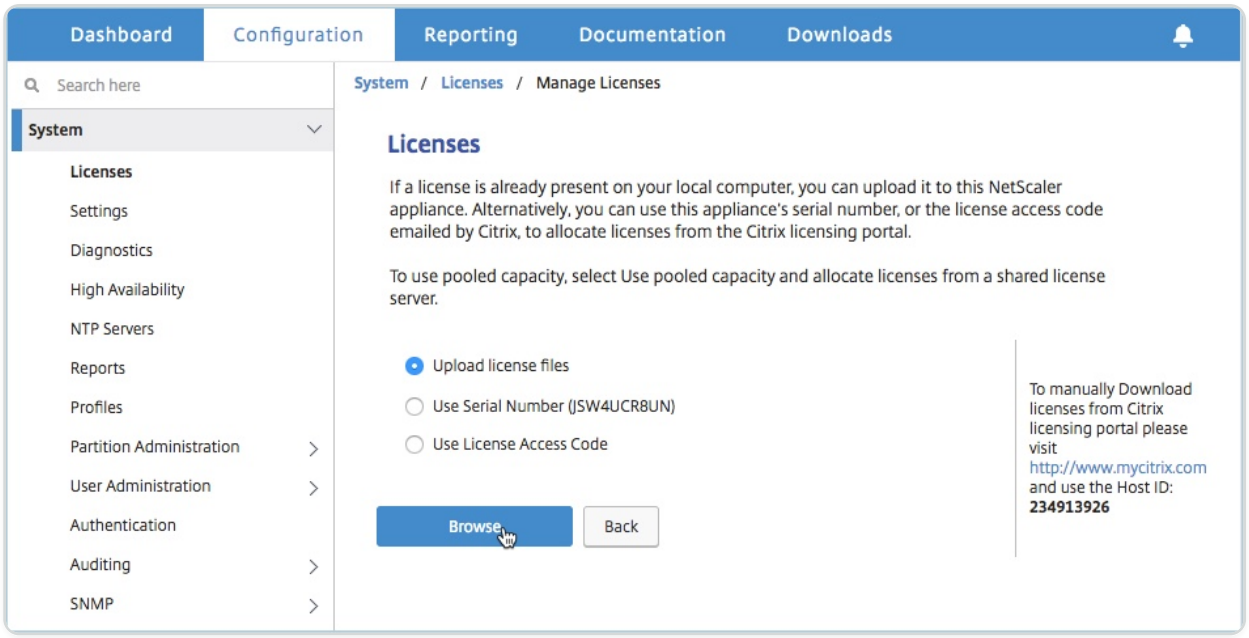
Make sure that you upload the MPX-Z license to both the primary and secondary instances in the HA pair.

To upload the MPX-Z license to the NetScaler MPX instances in the HA pair:

1. In a Web browser, type the IP address of the appliance, such as `<http://192.168.100.1>`.
2. In **User Name** and **Password** fields, type the administrator credentials.
3. On the **Welcome** page, click **Continue**.

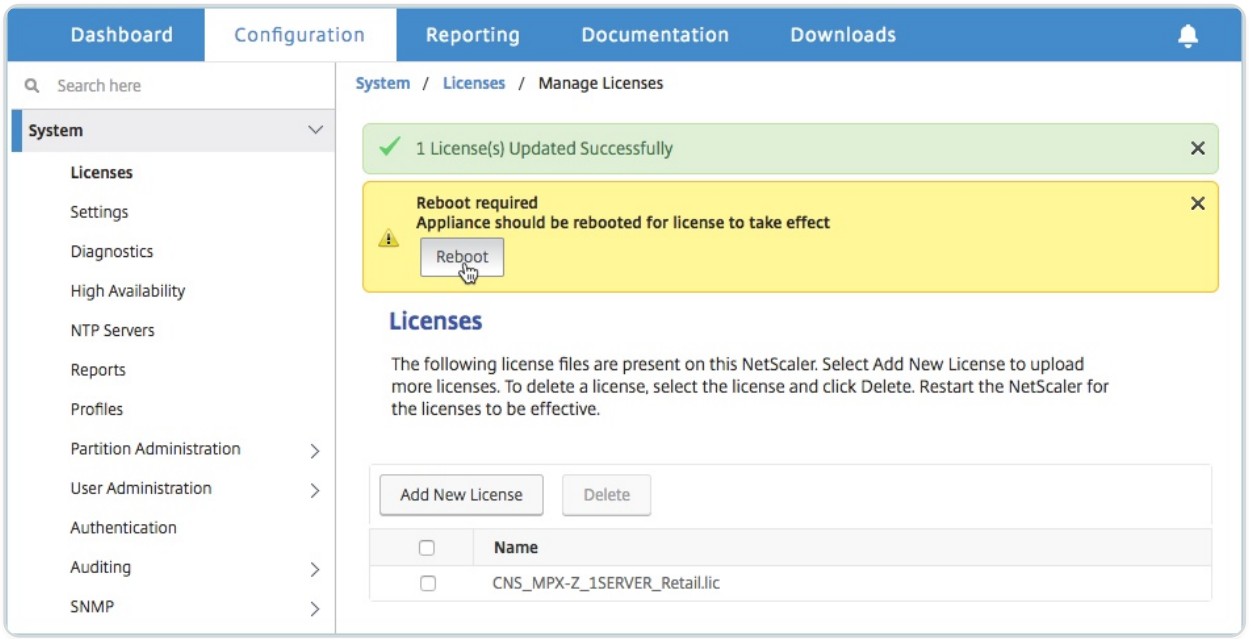
© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Upload the zero capacity license (MPX-Z license). On the **Configuration** tab, navigate to **System \> Licenses**.
5. In the details pane, click **Manage Licenses**, click **Add New License**.
6. In the **Licenses** page, select **Upload license files** and click **Browse** to select the zero capacity license from your local machine.



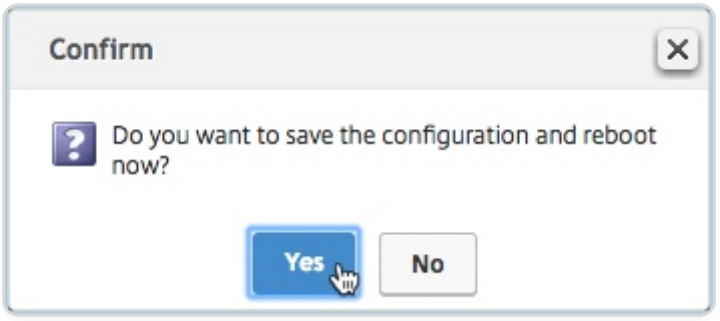
Once the license is uploaded you are prompted to reboot the appliance.

7. Click **Reboot** to reboot the appliance.



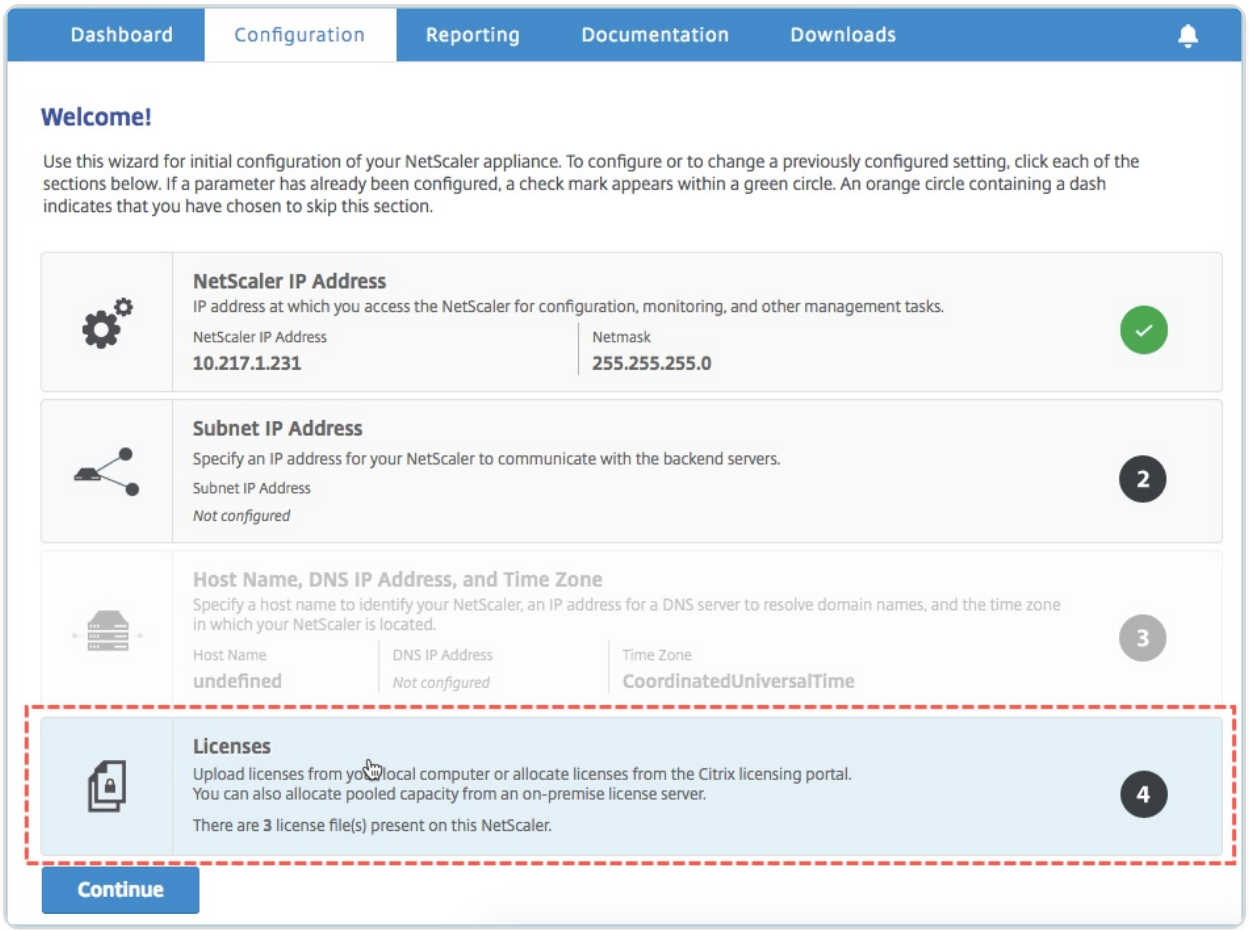
8. On the **Confirm** page, click **Yes**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



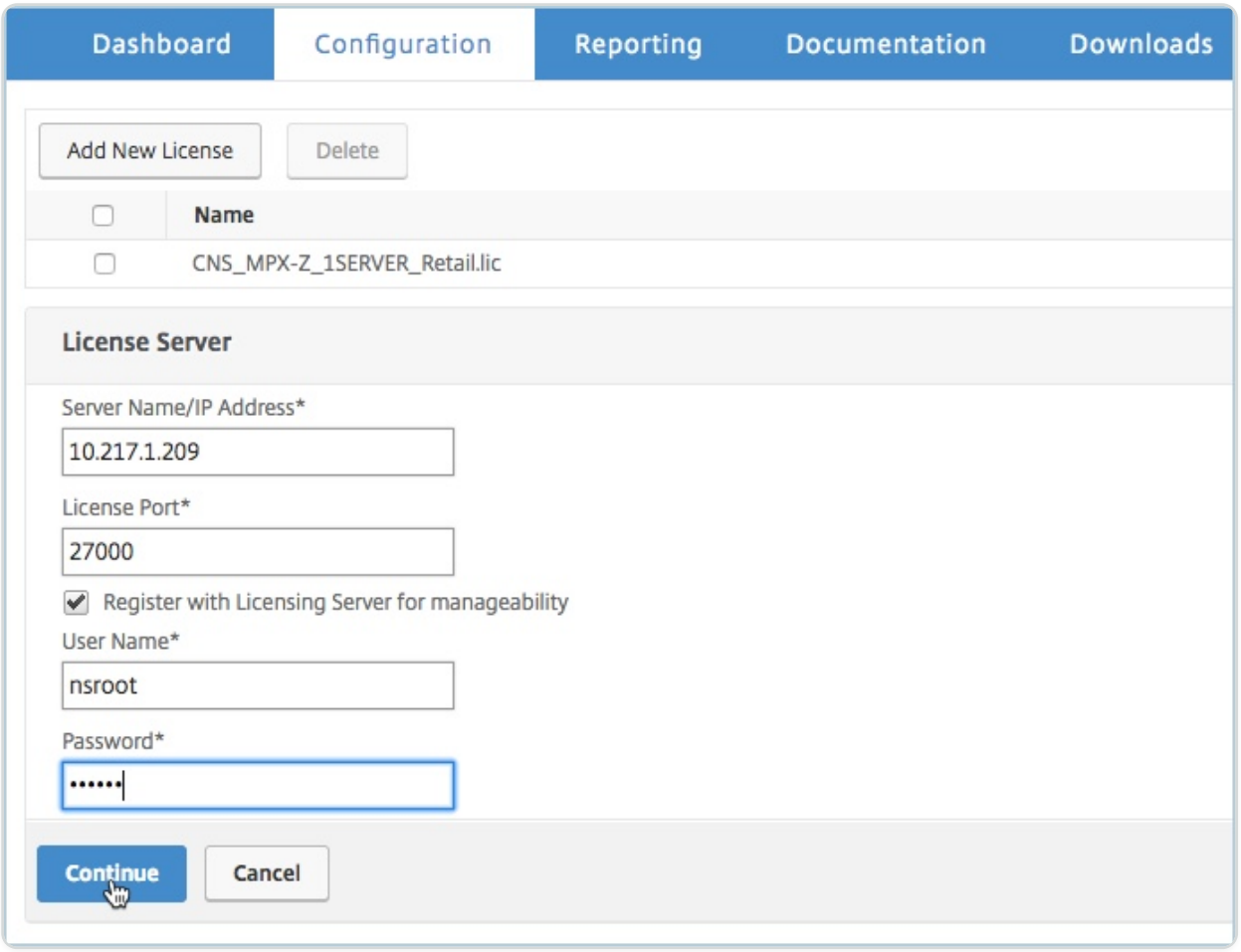
To upgrade an exisiting HA setup to NetScaler Pooled capacity:

1. Log on to the secondary NetScaler MPX Instance. In a Web browser, type the IP address of the NetScaler appliance, such as `<http://192.168.100.1>`.
2. In **User Name** and **Password** fields, type the administrator credentials.
3. On the **Welcome** page, click the **Licenses** section.



4. In the **License Server** section, do the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



a. In the **Server Name/IP Address** field, enter the license server details.

b. In the **License Port** field, enter the license server port. Default value: 27000.

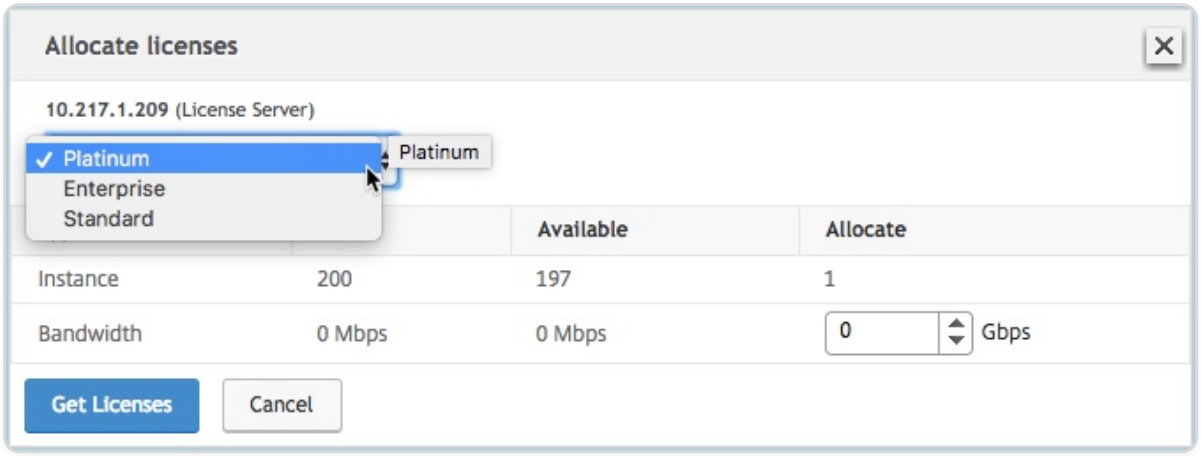
c. If you want to manage your instance's pool licenses through NetScaler Console, select the **Register with Licensing Server for manageability** checkbox and enter NetScaler Console credentials.

d. Click **Continue**.

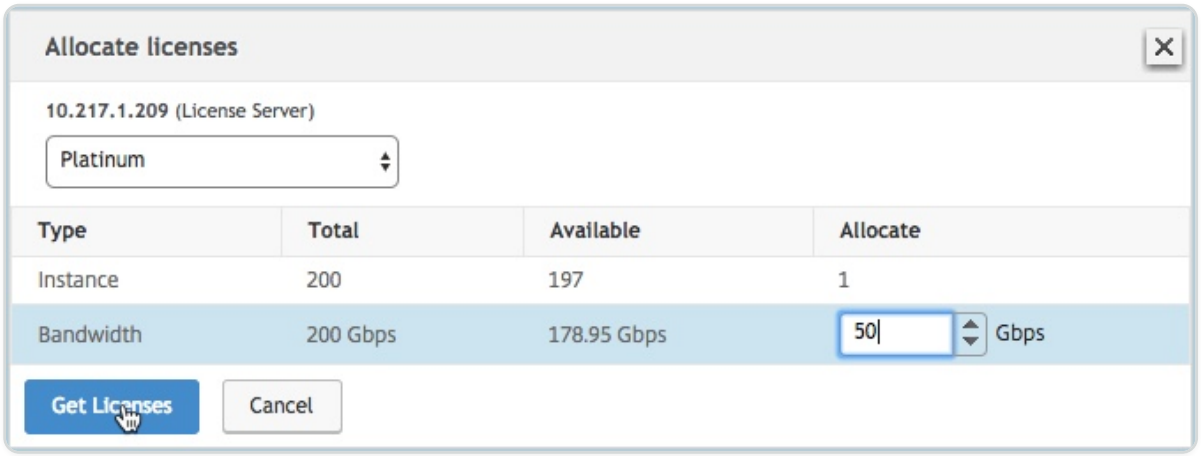
5. In the **Allocate licenses** window, do the following:

   a. Select the license edition from the drop-down list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



b. Allocate the bandwidth to the NetScaler appliance from the **Allocate** menu and click **Get Licenses**.



c. When prompted, click **Reboot** to reboot the appliance.

   After the secondary NetScaler MPX appliance reboots, it becomes the primary NetScaler MPX appliance in the HA pair.

6. Log on to the existing primary NetScaler MPX appliance and reboot the appliance. Perform the following:

   a. In a Web browser, type the IP address of the NetScaler appliance, such as `<http://192.168.100.1>`.

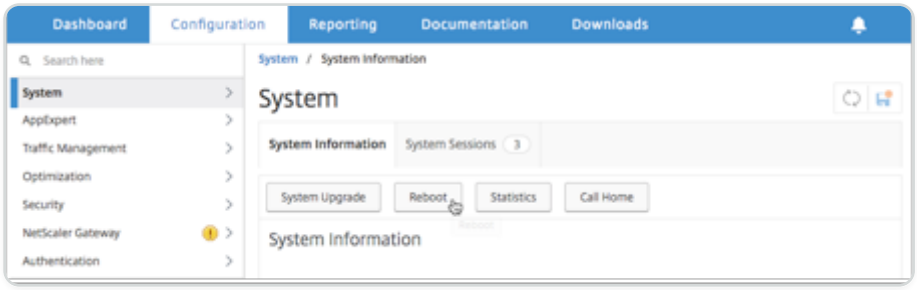
   b. In **User Name** and **Password** fields, type the administrator credentials.

   c. On the **Welcome** page, click **Continue**.

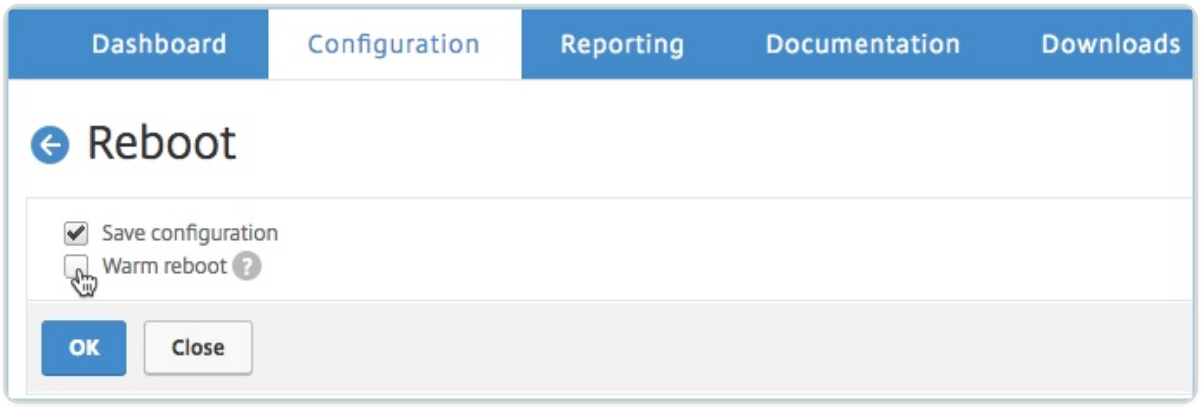
   d. On the **Configuration** tab, click **System**.

   e. On the **System** page, click **Reboot**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



f. On the **Reboot** page, select **Warm reboot** and click **OK**.



After the primary NetScaler MPX appliance reboots, it becomes the secondary NetScaler MPX appliance in the HA pair. If required, you can change the primary and secondary instances in the HA pair to your original HA pair configuration by using the following command on any instance in the HA pair:

```
> force ha failover
```

Upgrade a perpetual license in a NetScaler SDX to NetScaler Pooled capacity

IMPORTANT:

File-based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The minimum required NetScaler® versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Supported from early September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Note: LAS support for Console on-prem is from release 14.1-51.x onwards. However, file-based licensing is deprecated as of April 15 2026 from Console on-prem releases 14.1-51.x onwards and 13.1-60.x onwards. If you upgrade to Console on-prem release 14.1-51.x or release 13.1-60.x or later, you can continue using file-based licensing until 15th April 2026. However you must upgrade to Console on-prem release 14.1-51.x or later, and switch to LAS before 15th April 2026 because Console on-prem 13.1 does not support LAS.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don’t apply where prohibited by law or regulation.
A NetScaler SDX with perpetual license can be upgraded to NetScaler Pooled capacity license. Upgrading to NetScaler Pooled capacity license enables you to allocate licenses from the license pool to NetScaler appliances on demand. NetScalercan use one license at a time which is either use perpetual license or use the Pooled license. A customer can make a switch from a Pooled license to a perpetual license. As long as the perpetual license is valid, a customer can reconfigure the NetScalerand remove the Pooled licensing config. When a customer makes a switch from perpetual license to Pooled license or pooled to perpetual license, all the NetScaler instances are restarted.

You can also configure the NetScaler Pooled capacity license for NetScaler instances configured in a high-availability mode.

NOTE

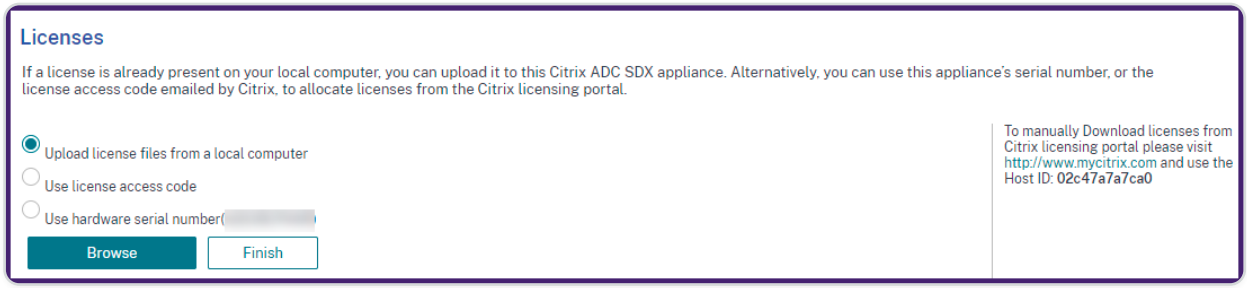
For upgrading the SDX appliance to NetScaler Pooled capacity license, you must upload the SDX-Z license to the appliance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ensure you have the permission to add NetScaler instances in NetScaler Console.

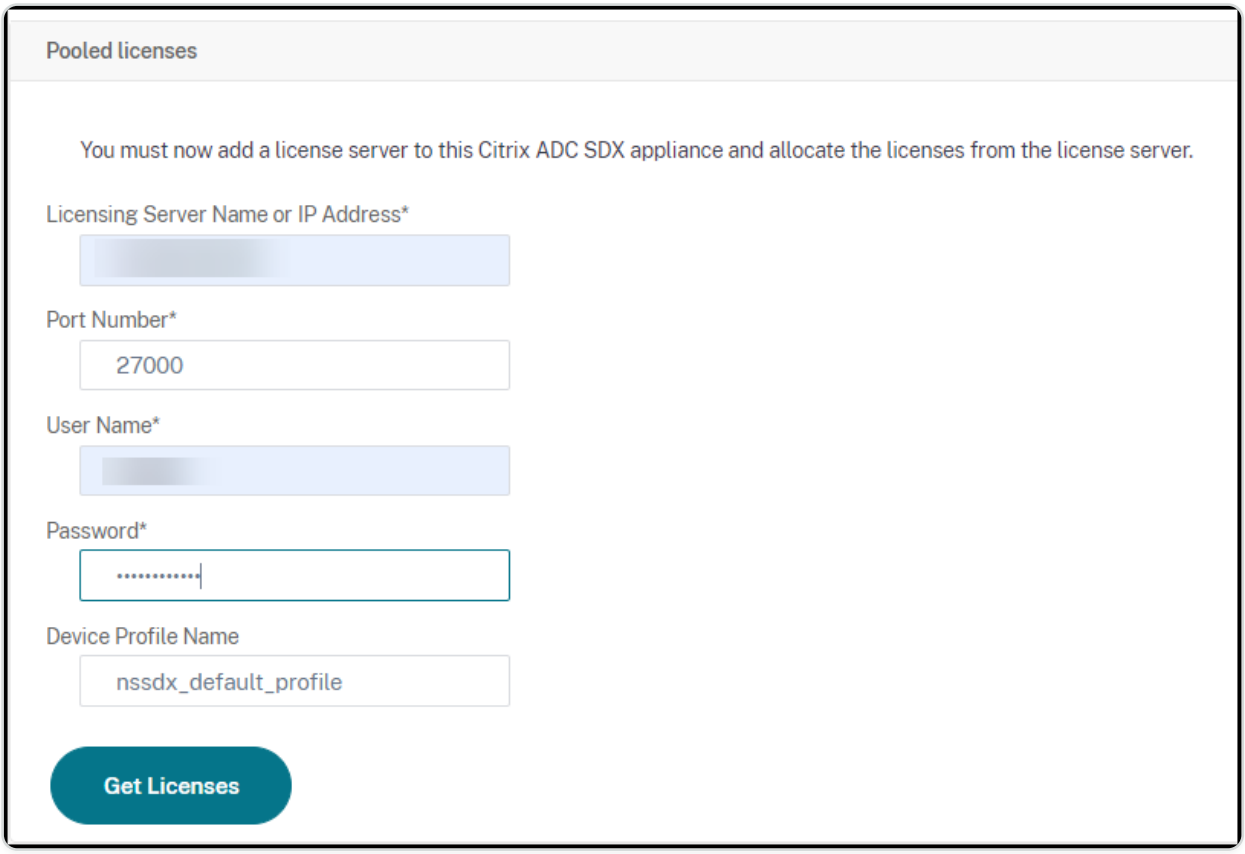
To upgrade to NetScaler pooled capacity:

1. In a Web browser, type the IP address of the SDX appliance, such as `<http://192.168.100.1>`.
2. In **User Name** and **Password** fields, type the administrator credentials.
3. On the **Welcome** page, click **Continue**.
4. Upload the zero-capacity license. On the Configuration tab, navigate to **System** > **Licenses**.
5. On the **Manage Licenses** page, click **Add License File**.
6. In the **Licenses** page, select **Upload license files from a local computer** and click **Browse** to select the zero-capacity license from your local machine. Then, click **Finish**.



   Once the zero-capacity license is applied successfully, a **Pooled Licenses** section appears on the **Licenses** page.
7. In the **Pooled licenses** section, do the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



a. In the **Licensing Server Name or IP Address** field, enter the license server details.

   If you want to configure NetScaler Console server as a license server, specify NetScaler Console server's IP address.

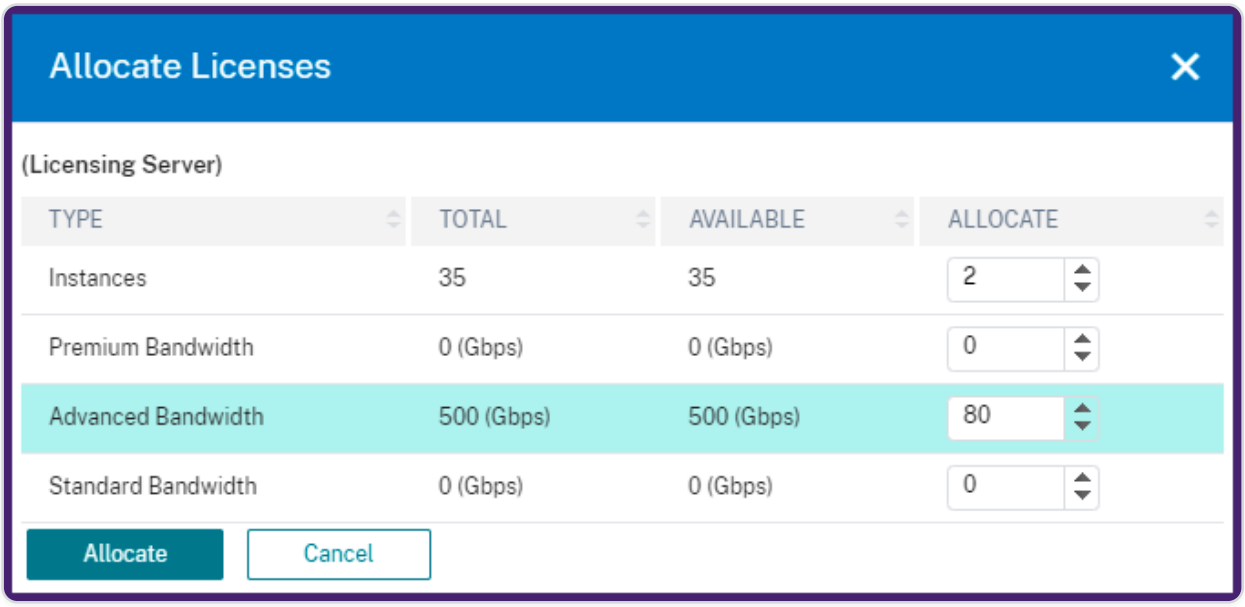
   If you are using an agent to communicate with the NetScaler Console server, specify the agent's IP address.

b. In the **Port Number** field, enter the license server port. Default value: 27000.

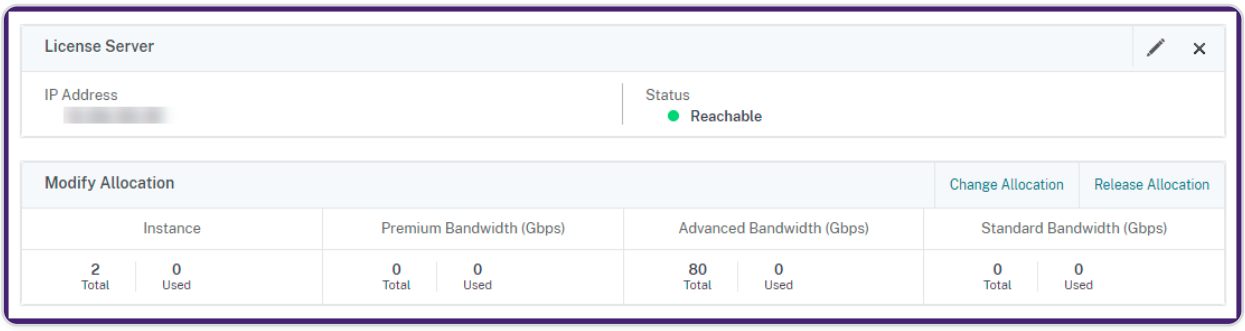
c. Click **Get Licenses**.

8. In the **Allocate Licenses** window, specify the required instances and bandwidth and click **Allocate**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



On the **Manage Licenses** page, you can view the details of the license server, license edition, and the allocated instances and bandwidth from the pool.



NOTE

Upgrading a perpetual license to Pooled capacity does not require restarting the SDX appliance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler VPX check-in and check-out licensing

IMPORTANT:

File-based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler® versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Supported from early September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Note: LAS support for Console on-prem is from release 14.1-51.x onwards. However, file-based licensing is deprecated as of April 15 2026 from Console on-prem releases 14.1-51.x onwards and 13.1-60.x onwards. If you upgrade to Console on-prem release 14.1-51.x or release 13.1-60.x or later, you can continue using file-based licensing until 15th April 2026. However you must upgrade to Console on-prem release 14.1-51.x or later, and switch to LAS before 15th April 2026 because Console on-prem 13.1 does not support LAS.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don’t apply where prohibited by law or regulation.
You can allocate NetScaler VPX licenses to NetScaler VPX instances on demand from NetScaler Console. The licenses are stored and managed by NetScaler Console, which has a licensing framework that provides scalable and automated license provisioning. A NetScaler VPX instance,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

when provisioned, can check out the license from the NetScaler Console, or check back in its license to NetScaler Console when an instance is removed or destroyed.

Install licenses in NetScaler Console

To install license files on the NetScaler Console:

1. Navigate to **NetScaler Licensing > License Management**.
2. In the **License Files** section, click **Add License File** and select one of the following options:
   - **Upload license files from a local computer**: If a license file is already present on your local computer, you can upload it to the Console.
   - **Use license access code**: Specify the license access code for the license that you have purchased from Citrix. Click **Get Licenses** and then click **Finish**.
3. Click Finish. The license files are added to NetScaler Console.

> **NOTE**
>
> Make sure you are connected to the internet before using the license access code for installing the licenses.

Allocate NetScaler VPX license to a NetScaler VPX instance by using the NetScaler GUI

1. Log in to the NetScaler VPX instance and navigate to **System > Licenses > Manage Licenses**, click **Add New License**, and select **Use remote licensing**.
2. Enter the details of the license server in the **Server Name/IP Address** field.

   Note

   > If you want to manage your instance's NetScaler VPX licenses through the NetScaler Console, select the **Register with NetScaler MA Service** checkbox and enter the NetScaler Console credentials.
3. Click **Continue**.
4. In the **Allocate licenses** window, select the type of license. The window displays the total and the available virtual CPUs and also the CPUs that can be allocated. Click **Get Licenses**.
5. Click **Reboot** on the next page to apply for the license.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

You can also release the current license and check out from a different edition. For example, you are already running a Standard edition license on your instance. You can release that license and then check out from Advanced edition.

6. You can change or release the license allocation by navigating to **System > Licenses > Manage Licenses**, and selecting **Change allocation** or **Release allocation**.
7. If you click **Change allocation**, a pop-up window shows the licenses available on the license server. Select the required license, click **Get Licenses**.

Allocate a NetScaler VPX license to a NetScaler VPX instance by using the NetScaler CLI

1. In an SSH client, enter the IP address of the NetScaler instance, and log on by using administrator credentials.
2. To add a licensing server, enter the following command:

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <port number >]
```

```
> add ns licenseserver 10.102.29.97 -port 27000
 Done
```

3. To show the available licenses on the licensing server, enter the following command:

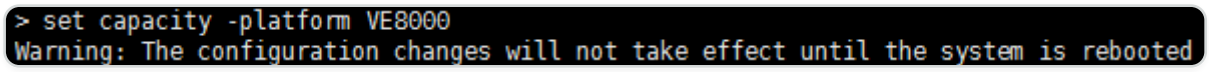
```
sh licenseserverpool
```

```
> sh licenseserverpool
        Instance Total                  : 0
        Instance Available              : 0
        Standard Bandwidth Total        : 0 Mbps
        Standard Bandwidth Availabe     : 0 Mbps
        Enterprise Bandwidth Total      : 0 Mbps
        Enterprise Bandwidth Available  : 0 Mbps
        Platinum Bandwidth Total        : 0 Mbps
        Platinum Bandwidth Available    : 0 Mbps
        VPX25S Total                    : 1
        VPX25S Available                : 1
        VPX200E Total                   : 1
        VPX200E Available               : 1
        VPX1000S Total                  : 1
        VPX1000S Available              : 1
        VPX8000E Total                  : 2
        VPX8000E Available              : 1
 Done
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. To assign a license to a NetScaler VPX instance, enter the following command:

```
set capacity –platform V\[S/E/P\]\[Bandwidth\]
```



Configure expiry checks for NetScaler VPX check-in/check-out licenses

You can now configure the license expiry threshold for NetScaler VPX licenses. By setting thresholds, NetScaler Console sends notifications via email or SMS when a license is due to expire. An SNMP trap and a notification are also sent when the license has expired on NetScaler Console.

An event is generated when a license expiry notification is sent and this event can be viewed on NetScaler Console.

For more information, see License management.

NetScaler virtual CPU licensing

IMPORTANT:

File-based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler® versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Supported from early September 2025.
- NetScaler Console on-prem: 14.1-51.x

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:** LAS support for Console on-prem is from release 14.1-51.x onwards. However, file-based licensing is deprecated as of April 15 2026 from Console on-prem releases 14.1-51.x onwards and 13.1-60.x onwards. If you upgrade to Console on-prem release 14.1-51.x or release 13.1-60.x or later, you can continue using file-based licensing until 15th April 2026. However you must upgrade to Console on-prem release 14.1-51.x or later, and switch to LAS before 15th April 2026 because Console on-prem 13.1 does not support LAS.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don’t apply where prohibited by law or regulation.
Data center administrators like you are moving to newer technologies that simplify network functions while offering lower costs and greater scalability. Newer data center architecture must include the following features in the least:

- Software-defined networking (SDN)
- Network functions virtualization (NFV)
- Network virtualization (NV)
- Micro-services

Such a movement also needs that the software requirements to be dynamic, flexible, and agile to meet the ever-changing business needs. Licenses are also expected to be managed by a central management tool with full visibility into the usage.

Virtual CPU licensing for NetScaler VPX

Earlier, NetScaler VPX licenses were allocated based on the bandwidth consumption by the instances. A NetScaler VPX is restricted to use a specific bandwidth and other performance metrics based on the license edition that it is bound to. To increase the available bandwidth, you must upgrade to a license edition that provides more bandwidth. In certain scenarios, the bandwidth requirement might be less, but the requirement is more for other L7 performance such as SSL TPS, compression throughput, and so on. Upgrading the NetScaler VPX license might not be suitable in such cases. But you might still have to buy a license with large bandwidth to unlock

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the system resources required for CPU-intense processing. NetScaler Console now supports allocating licenses to the NetScaler instance based on the virtual CPU requirements.

In the virtual CPU-usage-based licensing feature, the license specifies the number of CPUs that a particular NetScaler VPX is entitled to. So, the NetScaler VPX can check out licenses for only the number of virtual CPUs running on it from the license server. NetScaler VPX checks out licenses depending on the number of CPUs running in the system. NetScaler VPX does not consider the idle CPUs while checking out the licenses. Similar to pooled license capacity and CICO licensing functionalities, the NetScaler Console license server manages a separate set of virtual CPU licenses. Here also, the three editions managed for virtual CPU licenses are standard, Advanced, and Premium. These editions unlock the same set of features as those unlocked by the editions for bandwidth licenses.

There might be a change in the number of virtual CPUs or when there is a change in the license edition. In such a case, you must always shut down the instance before you initiate a request for a new set of licenses. Restart the NetScaler VPX after checking out the licenses.

To configure licensing server in NetScaler VPX using GUI

1. In NetScaler VPX, navigate to **System** > **Licenses** and click **Manage Licenses**.
2. On the **License** page, click **Add New License**.
3. On the **Licenses** page, select the **Use remote licensing** option.
4. Select **CPU licensing** from the **Remote Licensing Mode** list.
5. Type the IP address of the license server and the port number.
6. Click **Continue**.

   NOTE

   Always register NetScaler VPX instance with NetScaler Console. If not done already, enable Register with NetScaler Console and type NetScaler Console login credentials.

7. In the **Allocate licenses** window, select the type of license. The window displays the total and the available virtual CPUs and also the CPUs that can be allocated. Click **Get Licenses**.

   NOTE

   For a NetScaler HA pair, allocate virtual CPU licenses to each node separately.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Click **Reboot** on the next page to apply for the licenses.

> **NOTE**
>
> You can also release the current license and check out from a different edition. For example, you are already running the Standard edition license on your instance. You can release that license and then check out from the Advanced edition.

FAQs and other resources

> **IMPORTANT:**
>
> File-based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler® versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Supported from early September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Note: LAS support for Console on-prem is from release 14.1-51.x onwards. However, file-based licensing is deprecated as of April 15 2026 from Console on-prem releases 14.1-51.x onwards and 13.1-60.x onwards. If you upgrade to Console on-prem release 14.1-51.x or release 13.1-60.x or later, you can continue using file-based licensing until 15th April 2026. However you must upgrade to Console on-prem release 14.1-51.x or later, and switch to LAS before 15th April 2026 because Console on-prem 13.1 does not support LAS.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don't apply where prohibited by law or regulation.
This section lists the reference documentations on configuring and operating Pooled licensing. You can refer to these documents for assistance related to configuration and operation issues.

Configuration

1. Where do I find information about the overview and features of Pooled capacity?

   Answer: See Configure Pooled capacity.

2. How do I convert or migrate perpetual to Pooled licenses and the opposite way?

   Answer: Conversion from a perpetual license to a Pooled capacity license is a one-way license entitlement process. You cannot revert the Pooled capacity license back to perpetual.

3. How do I deploy the NetScaler Console server?

   Answer: Follow the Getting started document.

4. How do I add a license to an existing Pooled license and allocate it?

   Answer: Follow the License Management document.

5. How do I allocate/increase capacity and bandwidth on instances?

   Answer: Follow the License Management document.

License Server Agent

1. How do I assign the LSA role to a specific agent?

   Answer: The first agent deployed is assigned with the LSA role. If the LSA agent goes down, all the NetScaler instances connected to NetScaler Console for pooled licensing enter into a grace period for one day. The next day, NetScaler Console selects a new agent as the LSA. This behavior is enabled by default.

   Admins can manually select a NetScaler agent as an LSA within 24 hours, instead of waiting for the NetScaler Console service to auto-select an agent after 24 hours of the LSA being down.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

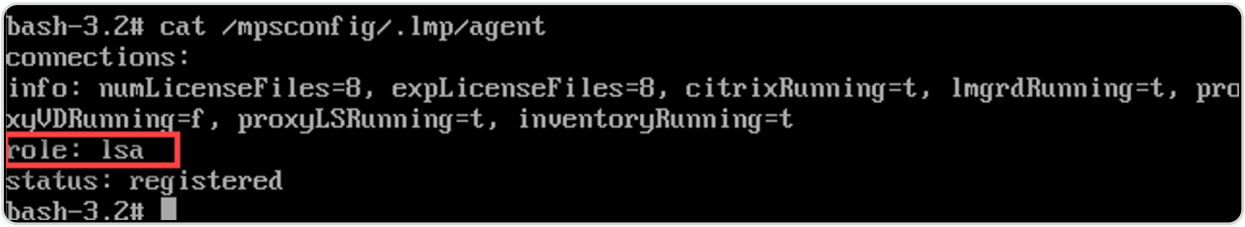
During this transition, NetScaler functionality is not impacted.

2. How can we determine which agent hosts the License Server role?

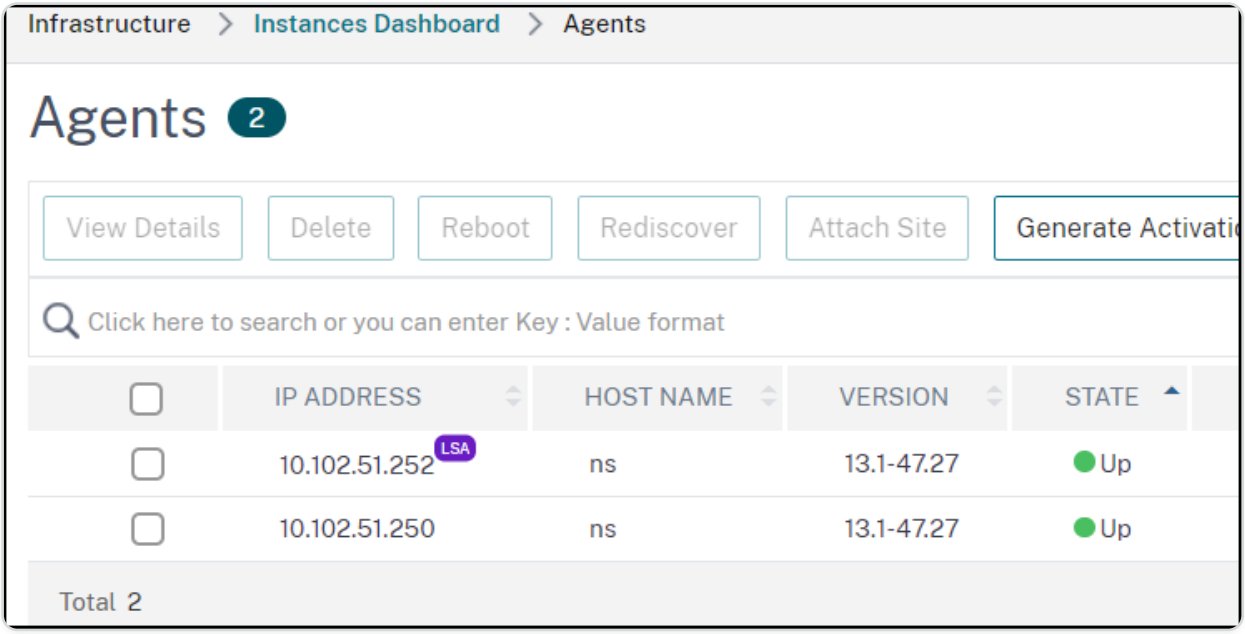
   Answer: To know which agent is hosting the LSA role, you can run the following command in the shell:

   ```
   cat /mpsconfig/.lmp/agent
   ```

   If the output value for “role” is **lsa**, then that agent is hosting the license server role.

   In the NetScaler Console GUI, you see LSA written next to the IP address of the designated agent.

3. What happens when the agent hosting the LSA role goes down?

   Answer: If the agent hosting the LSA role is offline, all the deployed NetScaler devices configured for pooled capacity licensing go into grace period. The grace period lasts for 30 days and the resources allocated to the NetScaler devices persist through this period. NetScaler instances in this state cannot allocate or modify license allocation until the agent hosting the LSA role comes online again or a new agent with the LSA role is designated.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. If the agent hosting the LSA role goes offline for an extended period, will there be a re-election?

   Answer: If the admin does not select a new LSA within 24 hours, the NetScaler Console service automatically selects the next agent that is UP as the new LSA after 24 hours of the LSA agent being down. The grace period of the NetScaler devices ends after the new LSA is elected.

Common issues

1. Instances running in grace mode due to connectivity failure, upgrade, split brain, and others.

   Answer: See the NetScaler Console license server behavior documented in Configuring NetScaler Pooled capacity.

2. Licenses not applying or reflecting on instances.

   Answer: See Troubleshoot Pooled capacity license issues.

3. License allocation is stuck in “sync in progress.”

   Answer: See Troubleshoot Pooled capacity license issues.

4. Error due to wrong host ID on license file.

   Answer: To identify a NetScaler Console server, you can assign the server a host name. The host name is displayed on the Universal license for NetScaler Console. For more information, see Assign a host name to a NetScaler Console server.

Migration

1. Is reallocation of bandwidth and instances required for VPX on SDX if migrating from one Console tenant to another Console tenant while using pooled or flexed licenses?

   Answer: If the licensing edition is the same on both the tenants and SDX can get earlier allocated capacity, then reallocation of bandwidth and instances is not required for VPX on SDX.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshoot Pooled capacity license issues

IMPORTANT:

File-based licensing system (also referred to as manually managed entitlements), traditionally used for activating various on-premises components, will be End of Life (EOL) on April 15, 2026. License Activation Service (LAS) is the next generation technology for product activations across the suite of Citrix products. LAS will be the only way to activate and license NetScaler instances after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.

The minimum required NetScaler® versions that are LAS compatible are:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Supported from early September 2025.
- NetScaler Console on-prem: 14.1-51.x

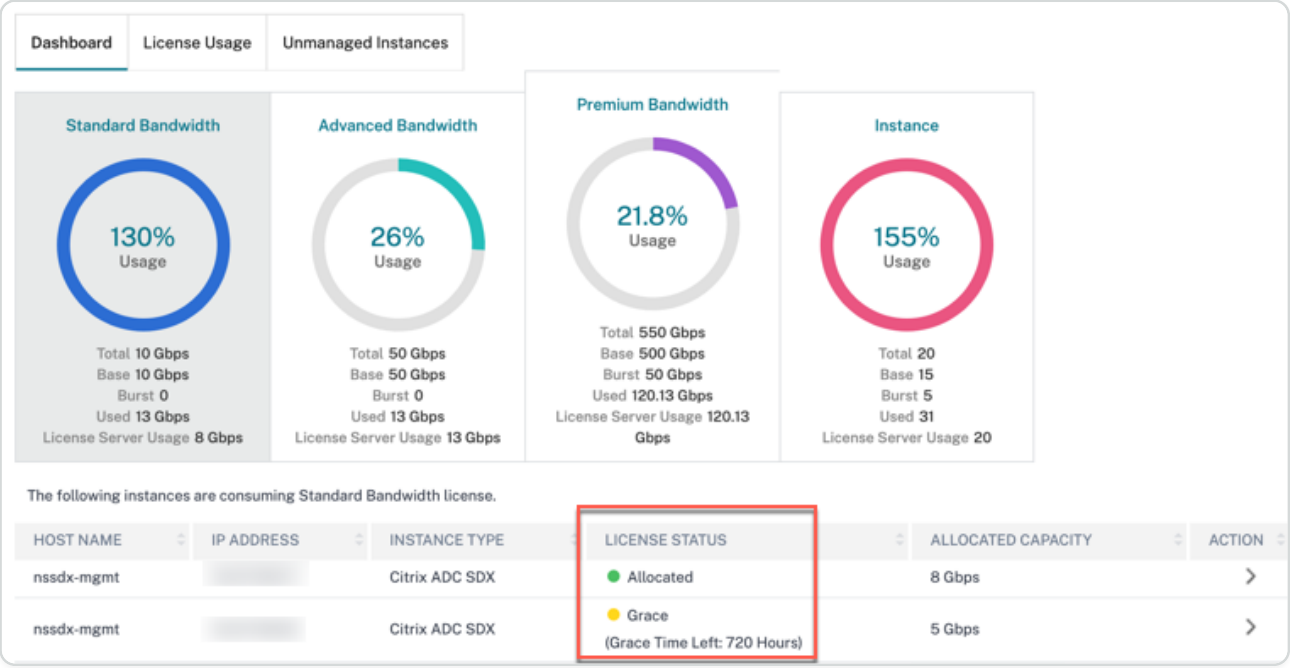
  Note: LAS support for Console on-prem is from release 14.1-51.x onwards. However, file-based licensing is deprecated as of April 15 2026 from Console on-prem releases 14.1-51.x onwards and 13.1-60.x onwards. If you upgrade to Console on-prem release 14.1-51.x or release 13.1-60.x or later, you can continue using file-based licensing until 15th April 2026. However you must upgrade to Console on-prem release 14.1-51.x or later, and switch to LAS before 15th April 2026 because Console on-prem 13.1 does not support LAS.

All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
LAS based licenses may not be available to customers where prohibited by law or regulations.
If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don’t apply where prohibited by law or regulation.
This section describes how to analyze and troubleshoot common Pooled capacity issues and also the troubleshooting scenarios are applicable for manually managed entitlement (file-based licenses).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Check license status

The NetScaler Console acts as a licensing server for your NetScaler Pooled capacity license. You can use the NetScaler Console GUI to check the status of the license. Navigate to **Infrastructure > Pooled Licensing > Throughput Capacity > License Usage**.



The following table lists the types of license status and what they mean

STATUS	WHAT IT MEANS
Allocated	The license state is fine.
Allocated: not applied on NetScaler	NetScaler might require reboot if license is checked-out or checked-in from NetScaler, but NetScaler hasn't rebooted yet.
Not allocated	License is not allocated in the NetScaler instance.
Grace	NetScaler instance is in the license grace period for 30 days
Sync in progress	NetScaler Console fetches information from NetScaler in a 2-minute intervals. Synchronizing licenses between NetScaler Console and NetScaler might take as long as 15 minutes. NetScaler Console might have

© 1997–2026 Citrix Systems, Inc. All rights reserved.

STATUS	WHAT IT MEANS
	rebooted or NetScaler Console HAS failover is triggered.
Partially allocated	NetScaler cannot accept the capacity allocated because it might be running at its maximum allocation. For example, NetScaler is running with 10 Gbps license pool capacity. When NetScaler reboots, the 10 Gbps is checked-in back to NetScaler Console license server. When NetScaler comes back online, it tries to check out the earlier allocated 10 Gbps automatically. Meanwhile, other NetScaler instances might have checked out that bandwidth. Partially Allocated appears if the license pool does not have enough capacity to allocate complete 10 Gbps or even partial capacity to this NetScaler.
Not managed	NetScaler is not added to NetScaler Console for manageability. This does not have impact on NetScaler licensing, but it can impact license monitoring from NetScaler Console.
Not managed	NetScaler is not added to NetScaler Console for manageability. This does not have impact on NetScaler licensing, but it can impact license monitoring from NetScaler Console.
Connection lost	NetScaler is not reachable from NetScaler Console for manageability. For example, there are network connectivity issues, NITRO is not working, or NetScaler password mismatches. If NITRO is not working or NetScaler password mismatches, this does not have an impact on NetScaler licensing. However, it can impact license monitoring from NetScaler Console.

Check server status

This section describes the common server status issues and possible reasons and fixes.

Issue: NetScaler displays the license server as unreachable and license status changes to grace.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Connection to license server (NetScaler Console or agent) has severed for more than 15 minutes. Verify if the license server is up and reachable.
- NetScaler is in grace mode.

Issue: NetScaler displays license server status as reachable but user attempt to change allocation has no effect. Clicking **Change Allocation** returns 0 0. This value might make it appear the configured capacity has been lost.

- Connection to the license server has recently gone down but the NetScaler still hasn't missed the second heartbeat. Therefore, it is not in Grace (yet). Verify if the license server is up and reachable.

Issue: NetScaler displays capacity and instance counts but the license server is **Reachable/ Unreachable**. Clicking **Change Allocation** returns some numbers but does not account for configured capacity.

- Connection to license server got restored but the NetScaler is still to miss the second heartbeat or send the reconnect probe.

Issue: NetScaler says Cannot connect to license server when configuring Pooled licensing with NetScaler Console

- Check firewall rules to ensure that ports 27000 and 7279 are open.
- The agent is not registered. For more information, see Getting Started.
- NetScaler Console does not have license files uploaded. For more information, see Configure NetScaler Pooled capacity
- NetScaler Console has the wrong license file.

Check usage report of license

Under **NetScaler Licensing > Pooled Licensing > Throughput Capacity > License Usage** in the NetScaler Console GUI, you can see the monthly peak of your license usage. You can use this report to increase your license usage or plan the purchase of an extra license.

The following are some details how the report is generated and can be used.

Polling: License data is polled from the NetScaler instances every 15 minutes.

Maintaining peaks per hour: NetScaler Console maintains only maximum license usage in an hour, per device.

Reporting: You can generate a GUI report for each instance, for a specific time range.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exporting: You can export reports either as in CSV format or XLS format.

Purging: NetScaler Console purges data on the first of every month at 12:10 a.m. The purge period is configurable (the default period is two months).

Counters and statistics for Pooled capacity licensing

The following counters, logs, and commands expose the NetScaler Pooled licensing metrics that indicate the behavior of both NetScaler Console and NetScaler instances in Pooled licensing mode.

- **SNMP traps**: available from NetScaler version 13.xx.
- **NSCONMSG counters for rate limiting**: available from NetScaler version 12.1 57.xx.
- **NetScaler Console counters** NetScaler Console Command Actions are available in NetScaler Cloud service.

SNMP traps

You can configure the following SNMP traps v.13 Pooled license alarms

- `POOLED-LICENSE-CHECKOUT-FAILURE`
- `POOLED-LICENSE-ONGRACE`
- `Configure POOLED-LICENSE-PARTIAL`

For more information about these alarms, see NetScaler SNMP OID Reference.

NSCONMSG Counter

Check the following `NCCONMSG` counters and what they mean:

- `allnic_err_rl_cpu_pkt_drops`: aggregate (all NICs) packet drops after CPU limit was reached
- `allnic_err_rl_pps_pkt_drops`: aggregate packet drops system wide after pps limit
- `allnic_err_rl_rate_pkt_drops`: aggregate rate drops system wide
- `allnic_err_rl_pkt_drops`: cumulative rate limiting drops due to rate, pps, and CPU
- `rl_tot_ssl_rl_enforced`: number of times SSL RL was applied (on new SSL connections)
- `rl_tot_ssl_rl_data_limited`: number of times the SSL throughput limit was reached
- `rl_tot_ssl_rl_sess_limited`: number of times the SSL TPS limit was reached

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console counters

When you choose the **Run Command Action** event action, you can create a command or a script that can be run on NetScaler Console for events matching a particular filter criterion. You can also set the following parameters for the **Run Command Action** script:

PARAMETER	DESCRIPTION
$source	This parameter corresponds to the source IP address of the received event.
$category	This parameter corresponds to the type of traps defined under the category of the filter.
$entity	This parameter corresponds to the entity instances or counters for which an event has been generated. It can include the counter names for all threshold-related events, entity names for all entity-related events, and certificate names for all certificate-related events.
$severity	This parameter corresponds to the severity of the event.
$failureobj	The failure object affects the way that an event is processed and ensures that the failure object reflects the exact problem as notified. This parameter can be used to track down problems quickly and to identify the reason for failure, instead of simply reporting raw events.

NOTE

During command execution, these parameters are replaced with actual values.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Settings

The NetScaler Console settings enable you to configure and manage the behavior of the service. You can manage role-based access control, data storage and retention, system alarms, observability integrations, notifications, and other global settings for NetScaler® deployments.

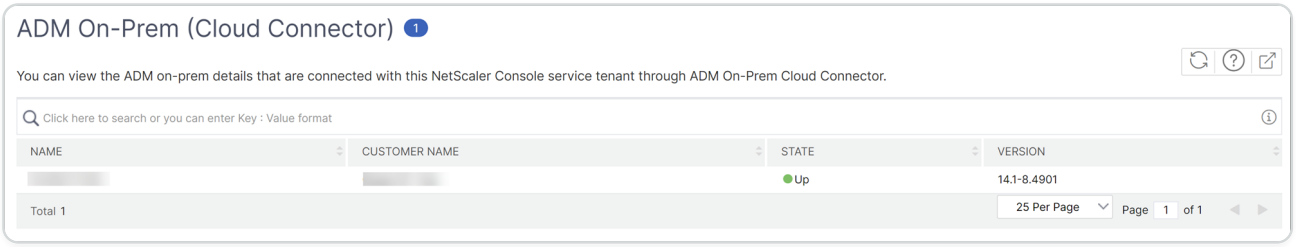
The following topics help you configure NetScaler Console settings:

- Console on-prem instances connected with Console service using Cloud Connect
- Console on-prem telemetry upload
- Configure analytics on virtual servers
- Configure Role-based access control
- Assign a net profile for the managed NetScaler instance
- Data Storage Management
- Data retention policy
- Configure and view system alarms
- Observability Integration
- Configure Analytics settings
- Configure notifications
- Export or schedule export reports
- Global Settings
- Configure action policies
- Audit log messages
- Configure IPAM

Console on-prem instances connected with Console service using Cloud Connect

In **Settings > NetScaler Console On-Prem**, you can view details of the NetScaler Console on-prem instances that are connected with the NetScaler Console service tenant through Cloud Connect.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Name** - The IP address of the NetScaler Console on-prem
- **Customer Name** - The name of the NetScaler Console service tenant
- **State** - The connectivity status between NetScaler Console on-prem instance and NetScaler Console service
- **Version** - The NetScaler Console on-prem instance build version

Console on-prem upload

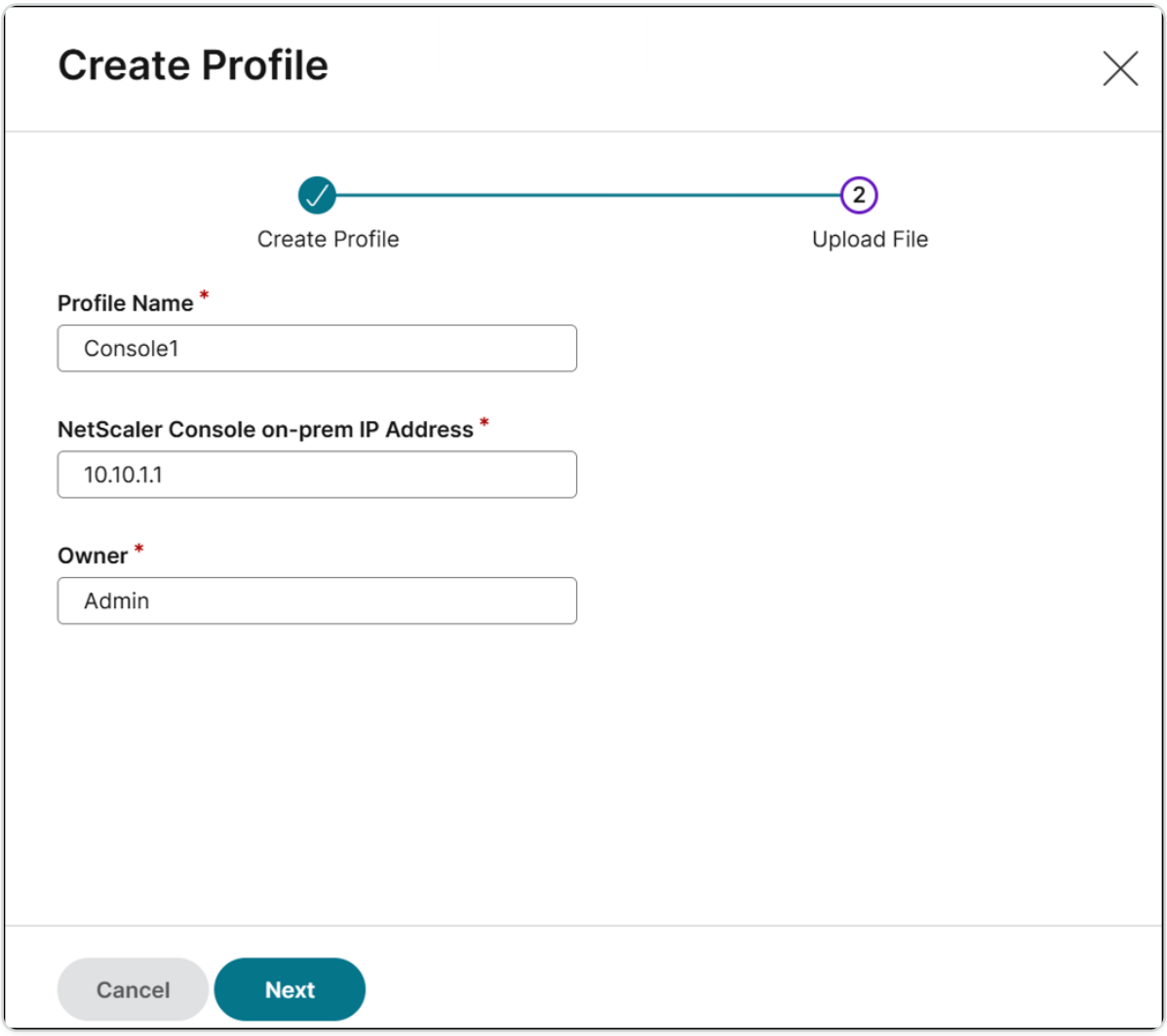
This page is applicable only for NetScaler® on-prem users who opted the manual mode to upload their telemetry data to NetScaler Console service. Ensure that you have downloaded the telemetry data from your NetScaler Console on-prem (click **Download Telemetry** from the **NetScaler Telemetry** homepage to download the bundle (.tgz) file that comprises the required telemetry data).

Starting from build **14.1-43.x**, you must create a profile for each NetScaler Console on-prem instance for uploading the telemetry file to the NetScaler Console service. You might have multiple NetScaler Console on-prem instances deployed globally. By creating a profile for each on-prem instance, you can upload the telemetry file for those on-prem instances and monitor the upload deadline separately.

To create a profile:

1. Navigate to **Settings > Console on-prem telemetry upload** and click **Create Profile**.
2. In the **Create Profile** page, specify the following:
    a. A profile name of your choice.
    b. The NetScaler Console on-prem IP address.
    c. The administrator name of the NetScaler Console on-prem.

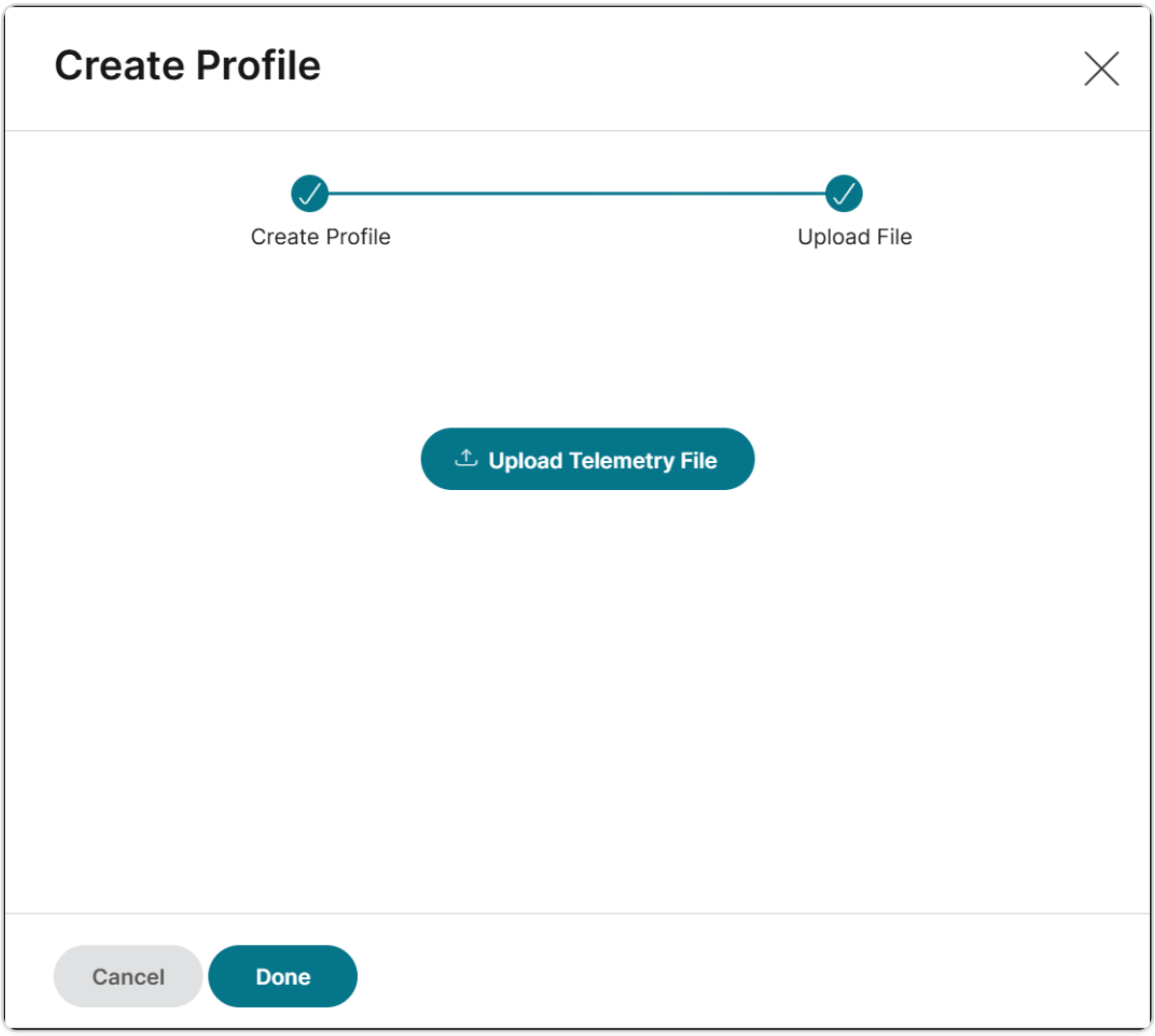
© 1997–2026 Citrix Systems, Inc. All rights reserved.



d. Click **Next**.

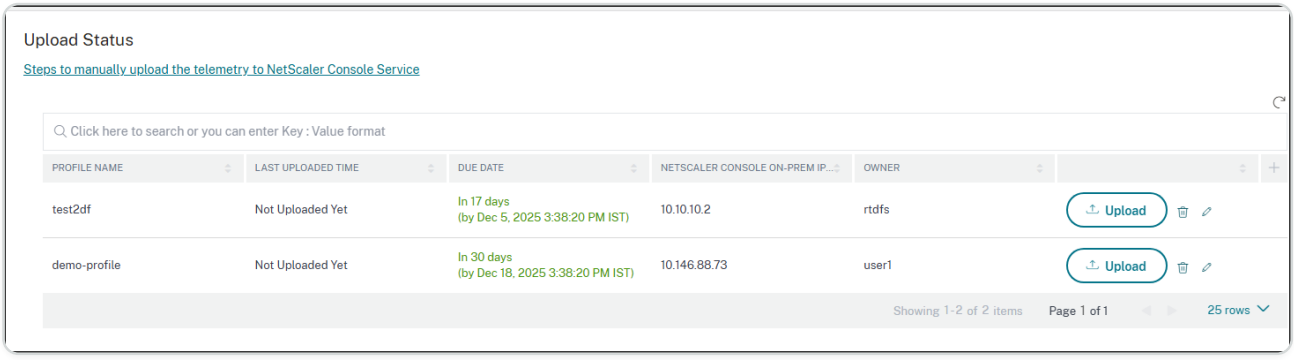
The profile name is created. You can either upload the telemetry file and click Done or upload it later.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



e. Repeat the procedure to create multiple profiles for all NetScaler Console on-prem instances.

After you create profiles, you can view the created profiles:



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If you are an existing NetScaler Console on-prem user and have previously uploaded the telemetry file to the NetScaler Console service, you must create a new profile and then upload the telemetry file. After creating the profile, you might observe a discrepancy between the NetScaler Console on-prem deadline and the NetScaler Console service deadline. Ensure that you upload the telemetry file to NetScaler Console service on or before the due date that is shown in your NetScaler Console on-prem. This discrepancy is aligned after you complete one upload using the new profile.

To upload your data telemetry in NetScaler Console service:

1. In **NetScaler Console on-prem upload** page, click **Upload Telemetry** from the created profile, and select the downloaded (.tgz) file to complete the upload process.
2. Complete the first upload within 30 days of selecting manual mode. Repeat the same procedure and upload the telemetry file every 90 days thereafter.

NOTES:

- The upload fails if the file is not in a valid (.tgz) format or the file does not pass the integrity checks. The recommendation is to download again and retry to upload. If the issue persists, contact Customer Care.
- The NetScaler Console service rejects the uploaded telemetry files older than 90 days. To retry, download a fresh telemetry file and upload it.
- You can disable the optional telemetry data. To disable, in NetScaler Console on-prem, you must first disable **Security Advisory** in the **NetScaler Telemetry** page, then navigate to **Settings > Administration > Enable or disable the Console feature data sharing**, and clear the **I agree to share Console feature usage data** checkbox.

To edit or delete a profile:

1. Navigate to **Settings > Console on-prem telemetry upload**, and select the profile that you want to edit or delete.
2. To edit, click the **Edit** icon. Update the required fields and click **Save**.
3. To delete, click the **Delete** icon.

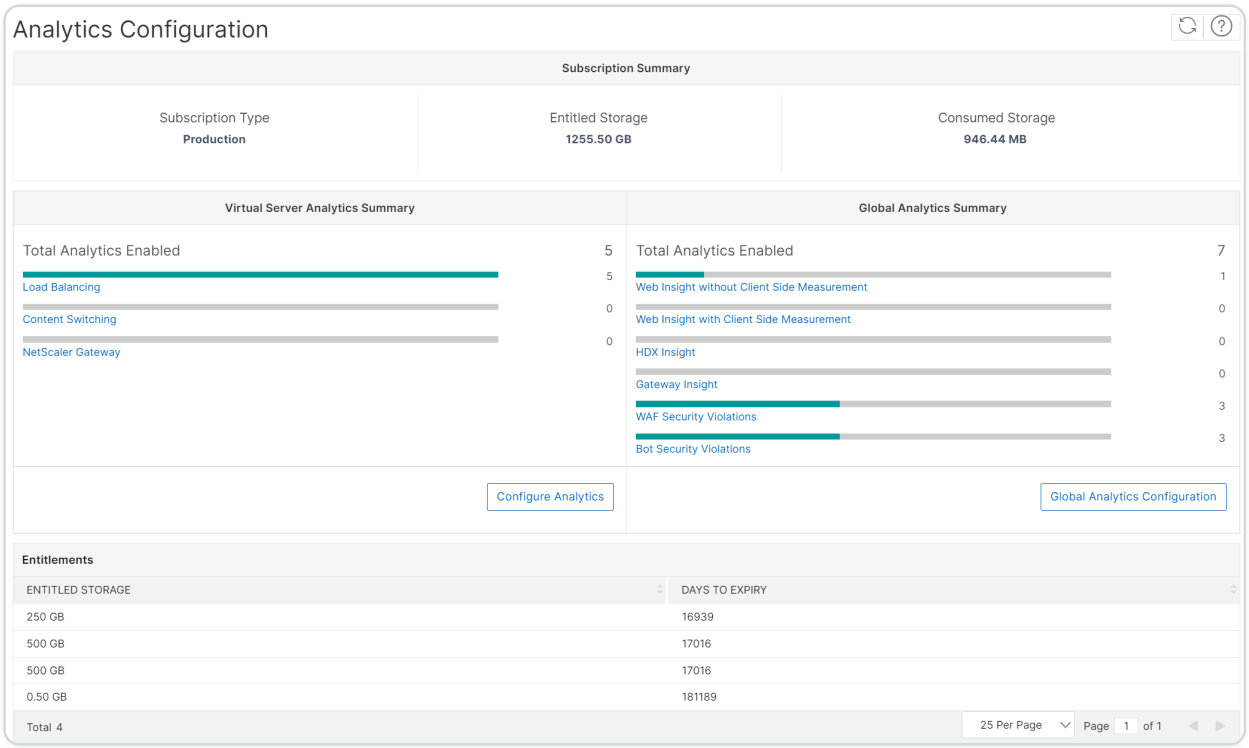
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure analytics on virtual servers

Starting from 14.1-21.x build, all the discovered virtual servers and the subsequent virtual servers are automatically licensed. You can proceed to configure analytics.

You can configure analytics in two ways. Navigate to **Settings > Analytics Configuration** to view:

- **Virtual Server Analytics Summary** - Enables you to configure analytics on the discovered virtual servers.
- **Global Analytics Summary** - Enables you to configure analytics on both discovered and subsequent virtual servers.



Configure analytics on the discovered virtual servers

NOTE:

Ensure that the virtual servers you want to enable analytics are in **UP** status.

1. Under **Virtual Server Analytics Summary**, click **Configure Analytics**.

   The **All Virtual Servers** page is displayed. You can:

   - Enable analytics
   - Edit analytics

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Disable analytics

NOTE:

The supported virtual servers to enable analytics are Load Balancing, Content Switching, and NetScaler Gateway.

2. Select the virtual servers and then click **Enable Security & Analytics**.

NOTE

Alternatively, you can enable analytics for an instance:

a. Navigate to **Infrastructure > Instances > NetScaler** and then select the instance type. For example, VPX.

b. Select the instance and from the **Select Action** list, select **Configure Analytics**

c. On the **Configure Analytics on Virtual Servers** page, select the virtual server and click **Enable Security & Analytics**.

3. On the **Enable Security & Analytics** window:

a. Select the insight types.

NOTE:

Starting from 14.1-44.x build, **Web Transaction Analytics** is available at the virtual server level. To enable, select the **Detailed Web Transactions** option under **Web Insight**.

b. Under **Advanced Settings (optional)**:

- Select **Logstream** as Transport Mode.

NOTE:

For NetScaler 12.0 or earlier, **IPFIX** is the default option for Transport Mode. For NetScaler 12.0 or later, you can either select **Logstream** or **IPFIX** as Transport Mode.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information about IPFIX and Logstream, see Logstream overview.

- **Enable HTTP X-Forwarded-For** - Select this option to identify the IP address for the connection between client and application, through HTTP proxy or load balancer.
- **Custom Header** - Define a custom header such as X-Real-IP, X-Client-IP, or any other custom header to fetch the actual client IP address instead of the proxy IP address. Ensure that the managed NetScaler instance is 14.1–38.24 or later build.
- **NetScaler Gateway** - Select this option to view analytics for NetScaler Gateway.

c. The Expression is true by default.

d. Click **OK**.

NOTE:

- For admin partitions, only **Web Insight** is supported.
- For virtual servers such as Cache Redirection, Authentication, and GSLB, you cannot enable analytics. An error message is displayed.

After you click **OK**, NetScaler Console processes to enable analytics on the selected virtual servers.

NOTE

NetScaler Console uses NetScaler SNIP for Logstream and NSIP for IPFIX. If there is a firewall enabled between NetScaler agent and NetScaler instance, ensure you open the following port to enable NetScaler Console to collect AppFlow traffic:

TRANSPORT MODE	SOURCE IP	TYPE	PORT
IPFIX	NSIP	UDP	4739
Logstream	SNIP	TCP	5557

Edit analytics

To edit analytics on the virtual servers:

1. Select the virtual servers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

Alternatively, you can also edit analytics for an instance:

a. Navigate to **Infrastructure > Instances > NetScaler** and then select the instance type. For example, VPX.

b. Select the instance and click **Edit Security & Analytics**.

2. Click **Edit Security & Analytics**
3. Edit the parameters that you want to apply on the **Edit Analytics Configuration** window.
4. Click **OK**.

Disable analytics

To disable analytics on the selected virtual servers:

1. Select the virtual servers.
2. Click **Disable Analytics**.

NetScaler Console disables the analytics on the selected virtual servers.

The following table describes the features of NetScaler Console that supports IPFIX and Logstream as the transport mode:

FEATURE	IPFIX	LOGSTREAM
Web Insight	Supported	Supported
WAF Security Violations	Supported	Supported
Gateway Insight	Supported	Supported
HDX Insight	Supported	Supported
SSL Insight	Not supported	Supported
CR Insight	Supported	Supported
IP Reputation	Supported	Supported
AppFirewall	Supported	Supported

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE	IPFIX	LOGSTREAM
Client Side Measurement	Supported	Supported
Syslog/Auditlog	Supported	Supported

Configure global analytics

You can enable global analytics by either creating a custom policy or a global policy.

NOTES:

- You can create only up to 10 policies. The policies can be a combination of nine custom policies and one global policy, or 10 custom policies.
- If you have both (custom and global) policies, the insights that are selected in both policies are applied on the virtual servers. If you want to remove any insights, you must remove them manually.

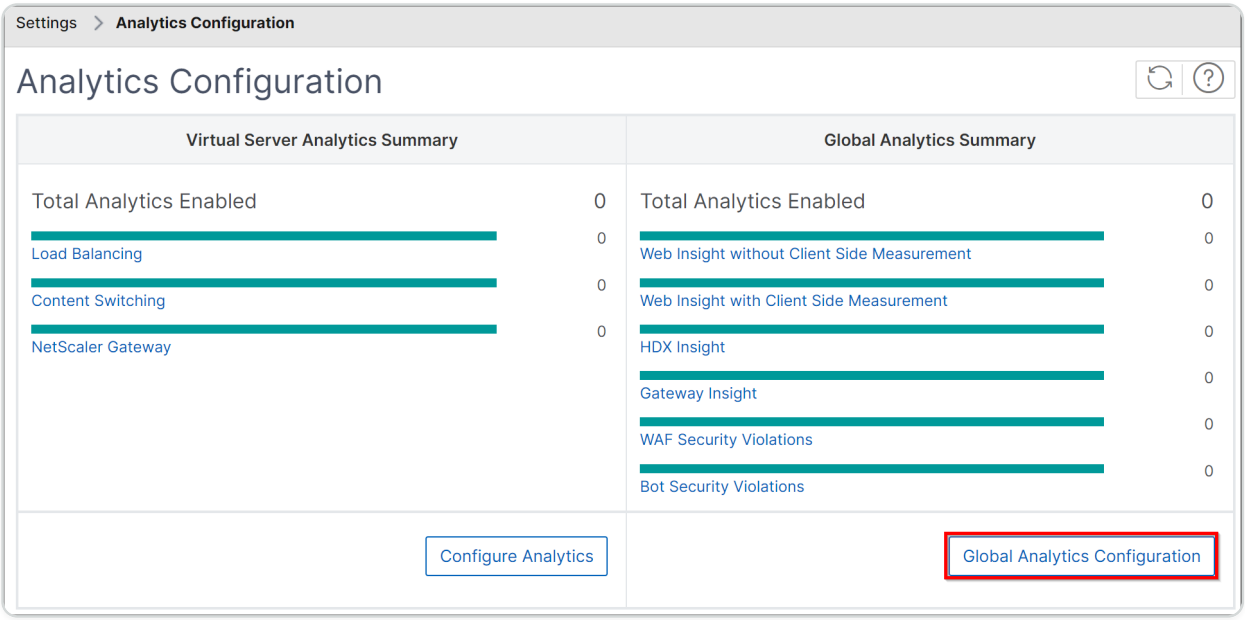
Custom policy

Using a custom policy, you can control instances or virtual servers that only require specific insights. You might have hundreds of virtual servers configured through various NetScaler instances managed in your NetScaler Console. In some scenarios, you might want to apply selective insights (for example, Bot Security Violations and WAF Security Violations) only to some of the virtual servers or instances. For such scenarios, you can configure a custom policy, select specific analytics features, and apply it to the relevant instances and virtual servers.

To configure a custom policy:

1. Under **Global Analytics Summary**, click **Global Analytics Configuration**.

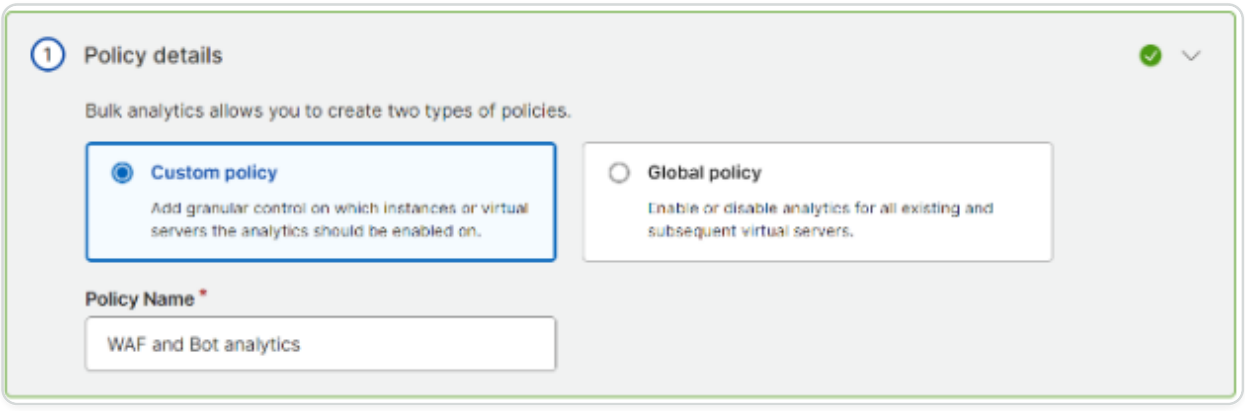
© 1997–2026 Citrix Systems, Inc. All rights reserved.



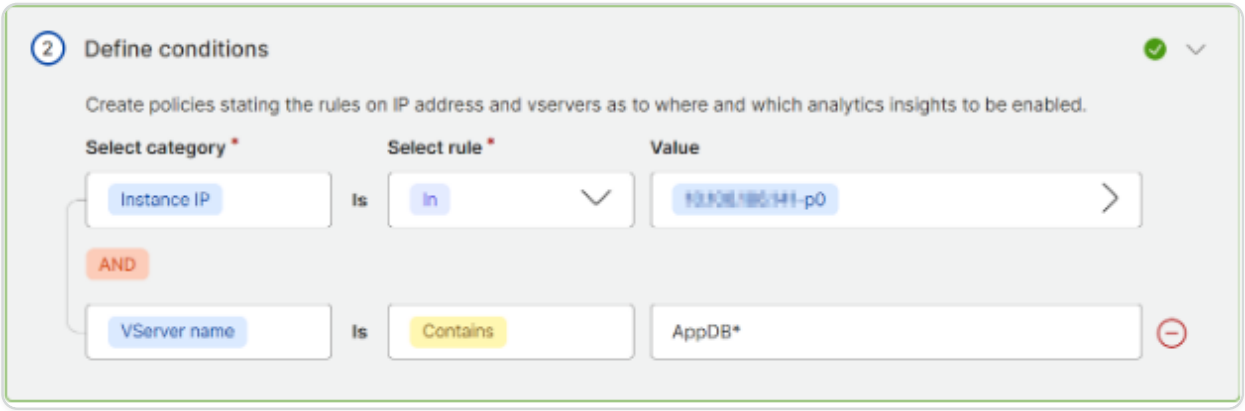
2. Under **Policy details**, select **Custom policy** and specify a policy name of your choice.

NOTE:

You cannot edit the policy name later.



3. Under **Define Conditions**, create conditions by selecting the set of instance IPs or specific instances or virtual server name or both.

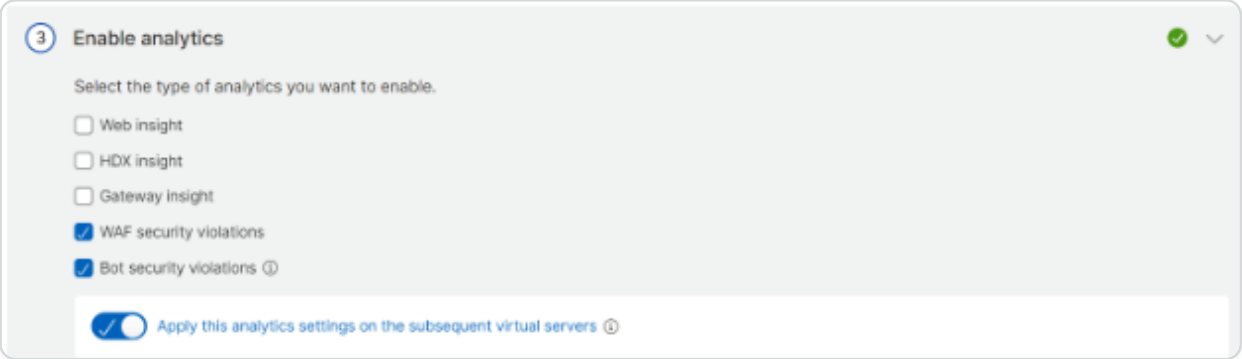


© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Under **Enable analytics**, select the analytics feature type.

   NOTE:

   If you enable **Apply this analytics settings on the subsequent virtual servers**, analytics will be applied to the subsequent virtual servers based on the defined analytics features.

5. Click **Save**.

   Points to note:

   - If you modify the policy by removing an existing insight and adding another insight, the updated policy is applied with the new insight. If you want to remove any insight, you must manually delete the already configured insights.

     Consider that you have created a custom policy with HDX insight and Web Insight. If you update the policy to remove HDX Insight and add Bot Security Violations, the virtual servers/instances are updated with HDX Insight, Web Insight, and Bot Security Violations. If you want to remove HDX Insight, you must manually remove using the edit analytics option.
   - The same logic is also applicable if you delete an existing policy and create another policy by adding the same instances or virtual servers.

Global policy

Using the global policy, you can enable analytics on both discovered and subsequent virtual servers. To create a global policy:

1. Under **Global Analytics Summary**, click **Global Analytics Configuration**.
2. Under **Policy details**, select **Global policy**.
3. Under **Enable analytics**, select the analytics feature type.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If you enable **Apply this analytics settings on the subsequent virtual servers**, analytics will be applied to the subsequent virtual servers based on the defined category.

4. Click **Save**.

After configuration, the analytics is enabled on both discovered and subsequent virtual servers.

Points to note

- Consider that you have configured the Global policy for the first time by selecting **Web Insight**, **HDX™ Insight**, and **Gateway Insight**. If you again change the analytics settings later and deselect **Gateway Insight**, the changes do not impact the virtual servers that are already enabled with analytics. You must manually remove the Gateway Insight on the virtual servers.
- Consider that you have 10 virtual servers and two of them are already enabled with analytics using the **Configure Analytics** option. In this scenario, when you configure the Global policy, the analytics are applied only on the remaining eight virtual servers.
- Consider that you have 10 virtual servers and you have manually disabled analytics for two virtual servers. In this scenario, when you configure the Global policy, the analytics are applied only on the remaining eight virtual servers and it skips the virtual servers that are manually disabled with analytics.

Migrate analytics

Starting from **14.1-40.x** build, when you enable analytics on virtual servers, the analytics are applied through profile-based configuration. Earlier, analytics was configured through an AppFlow policy. The profile-based configuration has the following benefits:

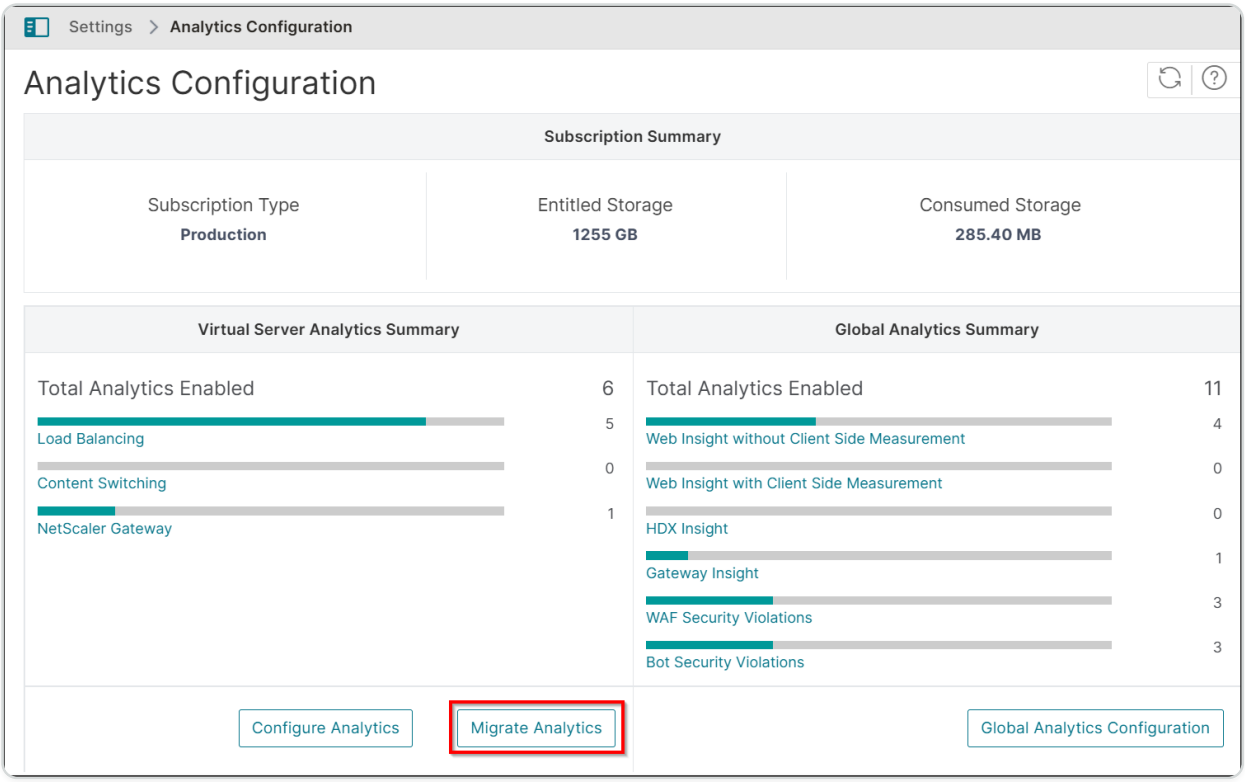
- Improved performance and flexibility
- Easier configuration and management

NOTE:

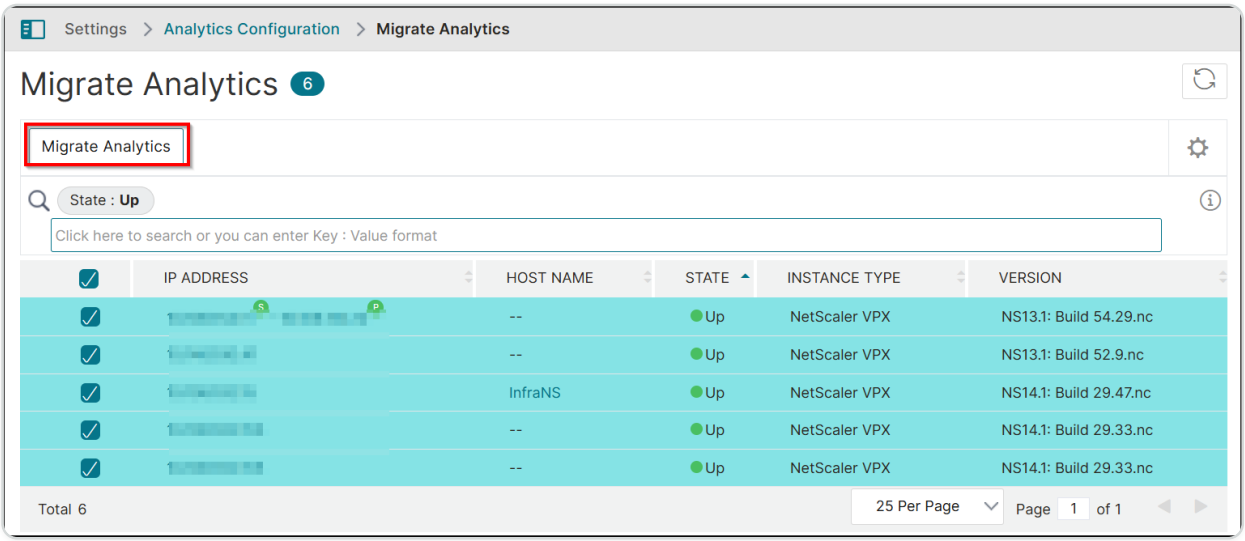
Enhancements related to analytics configurations are supported only through profile-based configuration. We recommend that you migrate all your existing virtual servers that are enabled for analytics to profile-based configuration.

1. Navigate to **Settings > Analytics Configuration** and then select **Migrate Analytics**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. In the **Migrate Analytics** page, you can view instances that have one or more virtual servers configured through AppFlow® policy.



A confirmation window appears. Click **Yes** to complete the migration.

Configure role-based access control

NetScaler Console provides fine-grained, role-based access control (RBAC) with which you can grant access permissions based on the roles of individual users within your enterprise.

In NetScaler Console, all users are added in Citrix Cloud. As the first user of your organization, you must first create an account in Citrix Cloud and then log on to the NetScaler Console GUI with the Citrix Cloud credentials. You are granted the super admin role, and by default, you have all access

© 1997–2026 Citrix Systems, Inc. All rights reserved.

permissions in NetScaler Console. Later you can create other users in your organization in Citrix Cloud.

Users who are created later and who log on to NetScaler Console as regular users are known as delegated admins. These users, by default, have all the permissions except user administration permissions. However, you can grant specific user administration permissions by creating appropriate policies and assigning them to these delegated users. The user administration permissions are at **Settings** > **Users & Roles**.

For more information on how to assign specific permissions, see How to Assign extra Permissions to Delegated Admin Users.

More information on how to create policies, roles, groups, and how to bind the users to groups is provided in the following sections.

Example:

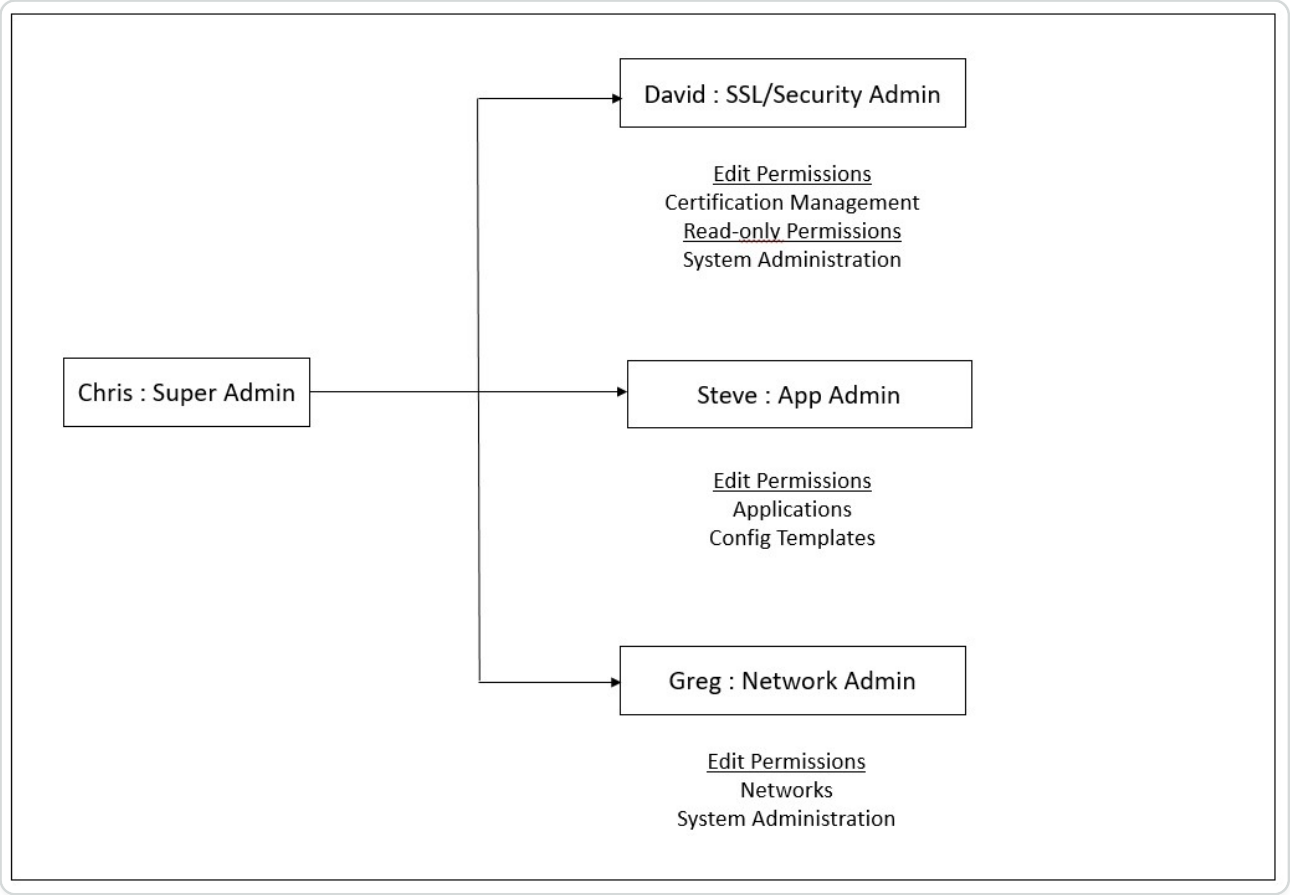
The following example illustrates how RBAC can be achieved in NetScaler Console.

Chris, the NetScaler group head, is the super administrator of NetScaler Console in his organization. He creates three administrator roles: security administrator, application administrator, and network administrator.

- David, the security admin, must have complete access for SSL Certificate management and monitoring but must have read-only access for system administration operations.
- Steve, an application admin, needs access to only specific applications and only specific configuration templates.
- Greg, a network admin, needs access to system and network administration.
- Chris also must provide RBAC for all users, irrespective of the fact that they are local or external.

The following image shows the permissions that the administrators and other users have and their roles in the organization.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



To provide role-based access control to his users, Chris must first add users in Citrix Cloud and only after that he can see the users in NetScaler Console. Chris must create access policies for each of the users depending on their role. Access policies are tightly bound to roles. So, Chris must also create roles, and then he must create groups as roles can be assigned to groups only and not to individual users.

Access is the ability to perform a specific task, such as view, create, modify, or delete a file. Roles are defined according to the authority and responsibility of the users within the enterprise. For example, one user might be allowed to perform all network operations, while another user can observe the traffic flow in applications and help in creating configuration templates.

Policies determine the user roles. After creating policies, you can create roles, bind each role to one or more policies, and assign roles to users. You can also assign roles to groups of users. A group is a collection of users who have permissions in common. For example, users who are managing a particular data center can be assigned to a group. A role is an identity granted to users by adding them to specific groups based on specific conditions. In NetScaler Console, creating roles and policies are specific to the RBAC feature in NetScaler. Roles and policies can be easily created, changed, or discontinued as the needs of the enterprise evolve, without having to individually update the privileges for every user.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Roles can be feature based or resource based. For example, consider an SSL/security administrator and an application administrator. An SSL/security administrator must have complete access to SSL Certificate management and monitoring features, but must have read-only access for system administration operations. Application administrators are able to access only the resources within their scope.

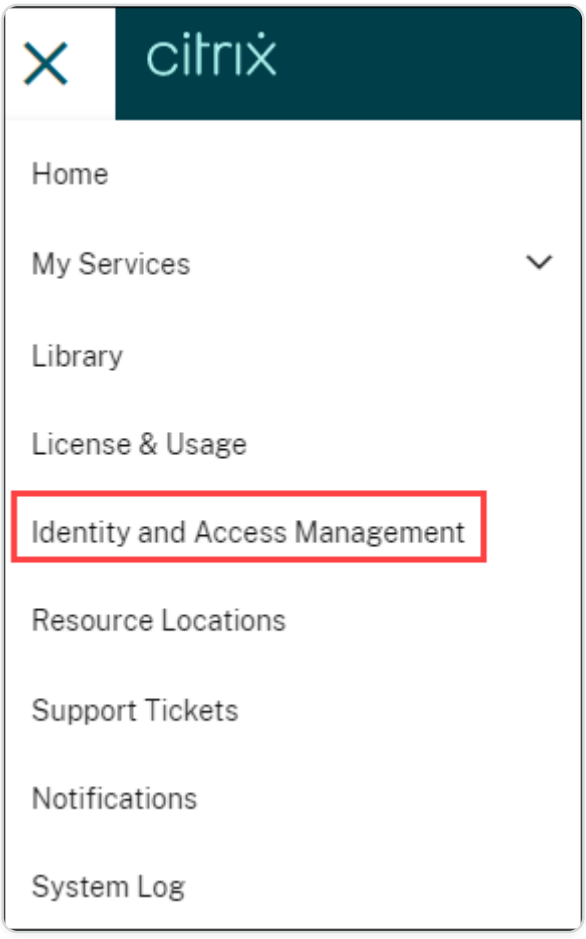
Therefore, in your role as Chris, the super admin, perform the following example tasks in NetScaler Console to configure access policies, roles, and user groups for David who is the security admin in your organization.

Configure Users on NetScaler Console

As a super admin, you can create more users by configuring accounts for them in Citrix Cloud and not in NetScaler Console. When the new users are added to NetScaler Console, you can only define their permissions by assigning the appropriate groups to the user.

To add new users in Citrix Cloud™:

1. In the NetScaler Console GUI, click the Hamburger icon at the top left, and select **Identity and Access Management**.



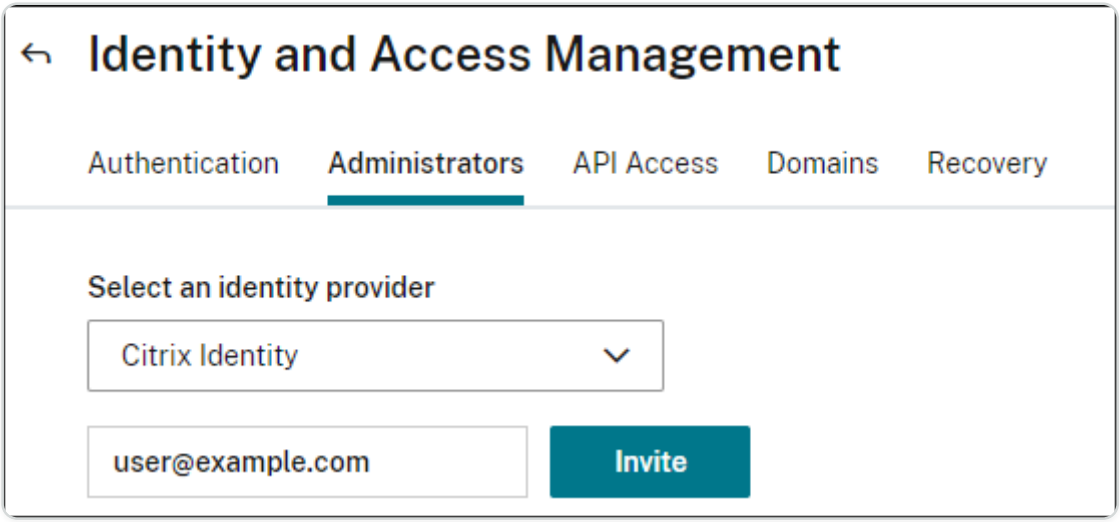
© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. On the Identity and Access Management page, select the **Administrators** tab.

   This tab lists the users that are created in Citrix Cloud.

3. Select the identity provider from the list.

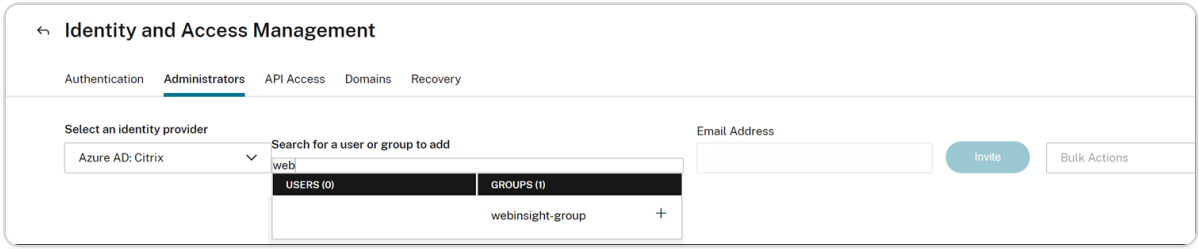
   - **Citrix Identity**: Type the email address of the user that you want to add in NetScaler Console and click **Invite**.



NOTE:

The user receives an email invite from Citrix Cloud. The user must click the link provided in the email to complete the registration process by providing their full name and password, and later log on to NetScaler Console using their credentials.

   - **Azure Active Directory (AD)**: This option appears only if your Azure AD is connected to Citrix Cloud, see Connect Azure Active Directory to Citrix Cloud. When you select this option to invite users or groups, you can specify only **Custom Access** for the selected user or group. The users can log in to NetScaler Console using their Azure AD credentials. And, you don't require to create a Citrix Identity for the users who are part of the selected Azure AD. If a user is added to the invited group, you don't require to send an invite for the newly added user. This user can access NetScaler Console using the Azure AD credentials.



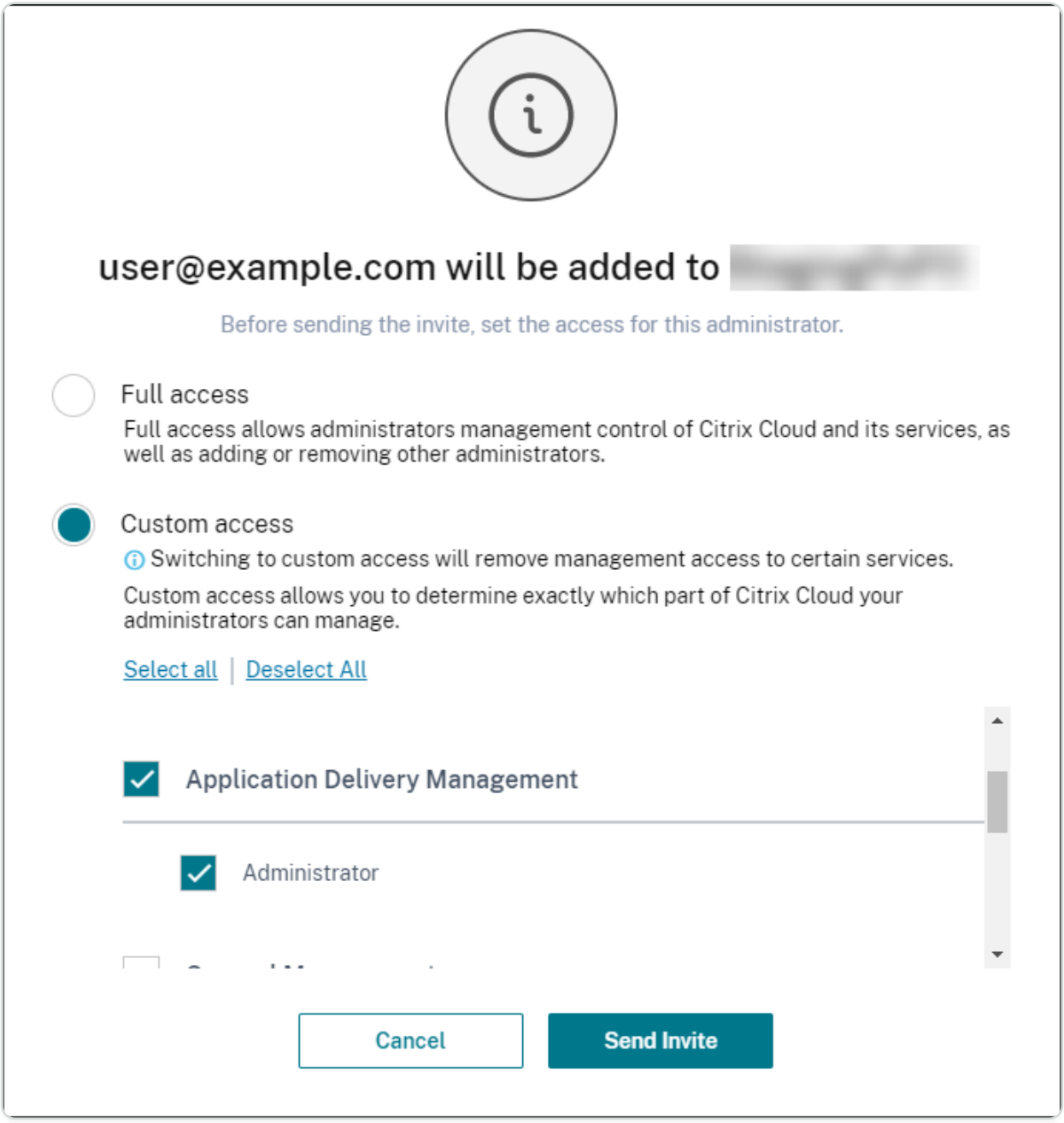
4. Select **Custom access** for the specified user or group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

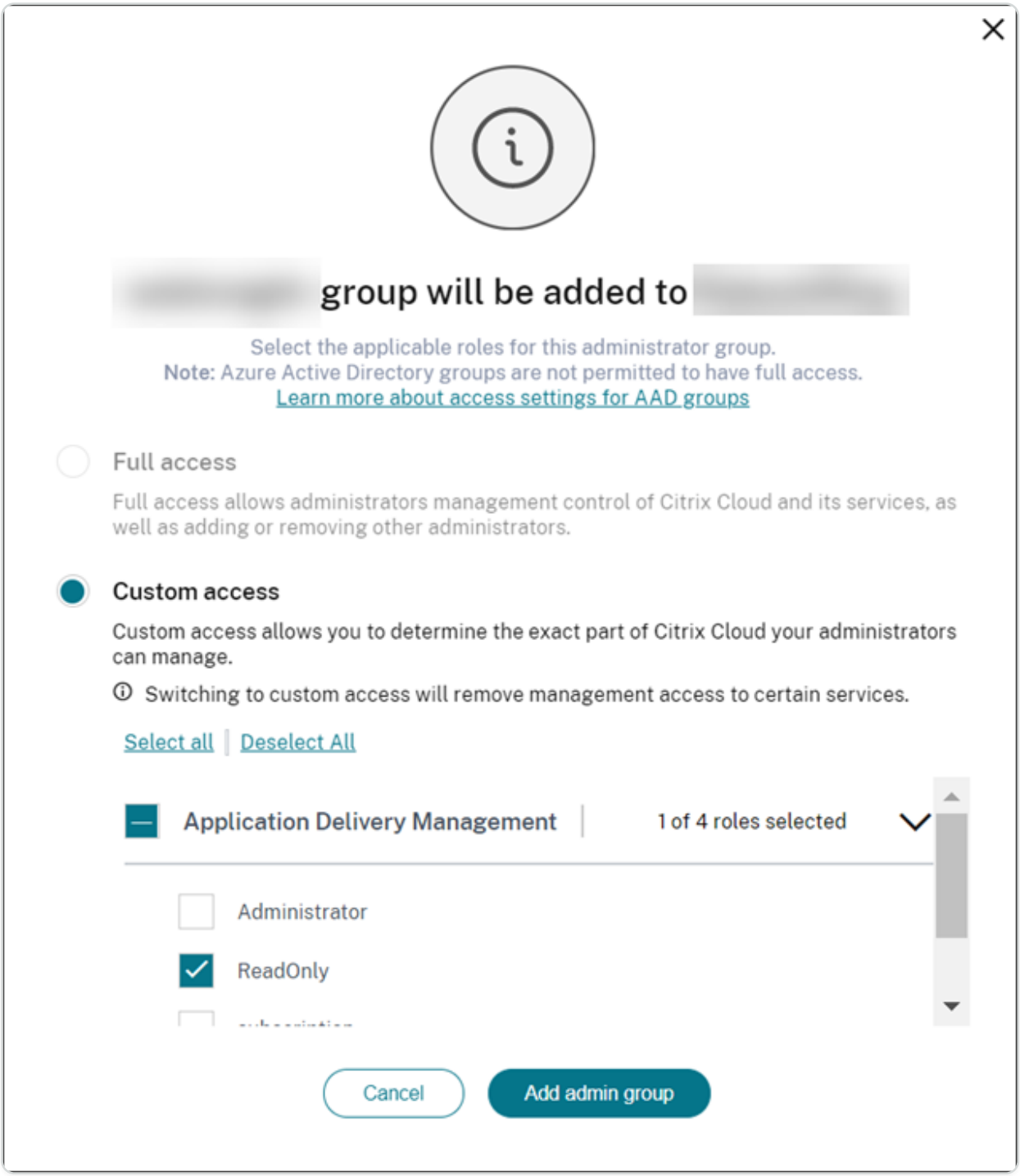
5. Select **Application Delivery Managment**.

   This option lists the user groups created in NetScaler Console. Select the group to which you want to add the user.

   |Citrix Identity|Azure AD| |-|-| |



© 1997–2026 Citrix Systems, Inc. All rights reserved.



| |Click **Send Invite**.|Click **Add Admin group**.|

As an admin, you see the new user in the NetScaler Console Users list only after the user logs on to NetScaler Console.

To Configure Users in NetScaler Console:

1. In the NetScaler Console GUI, navigate to **Settings** > **Users & Roles** > **Users**.
2. The user is displayed on the **Users** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. You can edit the privileges provided to the user by selecting the user and clicking **Edit**. You can also edit group permissions on the **Groups** page under the **Settings** node.

   NOTE:

   - The users are added in NetScaler Console from the Citrix Cloud only. Therefore, even though you have admin permissions, you cannot add or delete users in the NetScaler Console GUI. You can only edit the group permissions. Users can be added or deleted from Citrix Cloud.
   - The user details appear on the service GUI only after the user has logged on to the NetScaler Console at least once.

Configure Access Policies on NetScaler Console

Access policies define permissions. A policy can be applied to a user group or to multiple groups by creating roles. Policies determine the user roles. After creating policies, you must create roles, bind each role to one or more policies, and assign roles to user groups. NetScaler Console provides five predefined access policies:

- **admin_policy**. Grants access to all NetScaler Console nodes. The user has both view and edit permissions, can view all NetScaler Console content, and can do all edit operations. That is, the user can add, modify, and delete operations on the resources.
- **adminExceptSystem_policy**. Grants access to users for all nodes in NetScaler Console GUI, except access to the Settings node.
- **readonly_policy**. Grants read-only permissions. The user can view all content on NetScaler Console but is not authorized to do any operations.
- **appadmin_policy**. Grants administrative permissions for accessing the application features in NetScaler Console. A user bound to this policy can:
  - Add, modify, and delete custom applications
  - Enable or disable services, service groups, and the various virtual servers, such as content switching, and cache redirection
- **appreadonly_policy**. Grants read-only permission for application features. A user bound to this policy can view the applications, but cannot perform any add, modify, or delete, enable, or disable operations.

Though you cannot edit these predefined policies, you can create your own (user-defined) policies.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Earlier, when you assigned policies to roles and bound the roles to user groups, you can provide permissions for the user groups at node level in the NetScaler Console GUI. For example, you might only provide access permissions to the entire **Load Balancing** node. Your users had permission to access all entity-specific subnodes under **Load Balancing** (for example, virtual server, services, and others) or they did not have permission to access any node under **Load Balancing**.

In NetScaler Console 507.x build and later versions, the access policy management is extended to provide permissions for subnodes as well. Access policy settings can be configured for all subnodes such as virtual servers, services, service groups, and servers.

Currently, you can provide such a granular level access permission only for subnodes under a **Load Balancing** node and also for subnodes under the **GSLB** node.

For example, as an administrator, you might want to give the user an access permission for only to view virtual servers, but not the back end services, service groups, and application servers in the **Load Balancing** node. The users with such a policy assigned to them can access only the virtual servers.

To create user-defined access policies:

1. In the NetScaler Console GUI, navigate to **Settings** > **Users & Roles** > **Access Policies**.
2. Click **Add**.
3. On the **Create Access Policies** page, in the **Policy Name** field, enter the name of the policy, and enter the description in the **Policy Description** field.

   The **Permissions** section lists of all NetScaler Console features, with options for specifying read-only, enable-disable, or edit access.

   a. Click the (+) icon to expand each feature group into many features.
   b. Select the permission checkbox next to the feature name to grant permission to the users.

      - **View:** This option allows the user to view the feature in NetScaler Console.
      - **Enable-Disable:** This option is available only for the **Network Functions** features that allow enable or disable action on NetScaler Console. The user can enable or disable the feature. The user can also perform the **Poll Now** action.

        When you grant the **Enable-Disable** permission to a user, the **View** permission is also granted. You cannot deselect this option.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Edit:** This option grants the full access to the user. The user can modify the feature and its functions.

  If you grant the **Edit** permission, both **View** and **Enable-Disable** permissions are granted. You cannot deselect the auto-selected options.

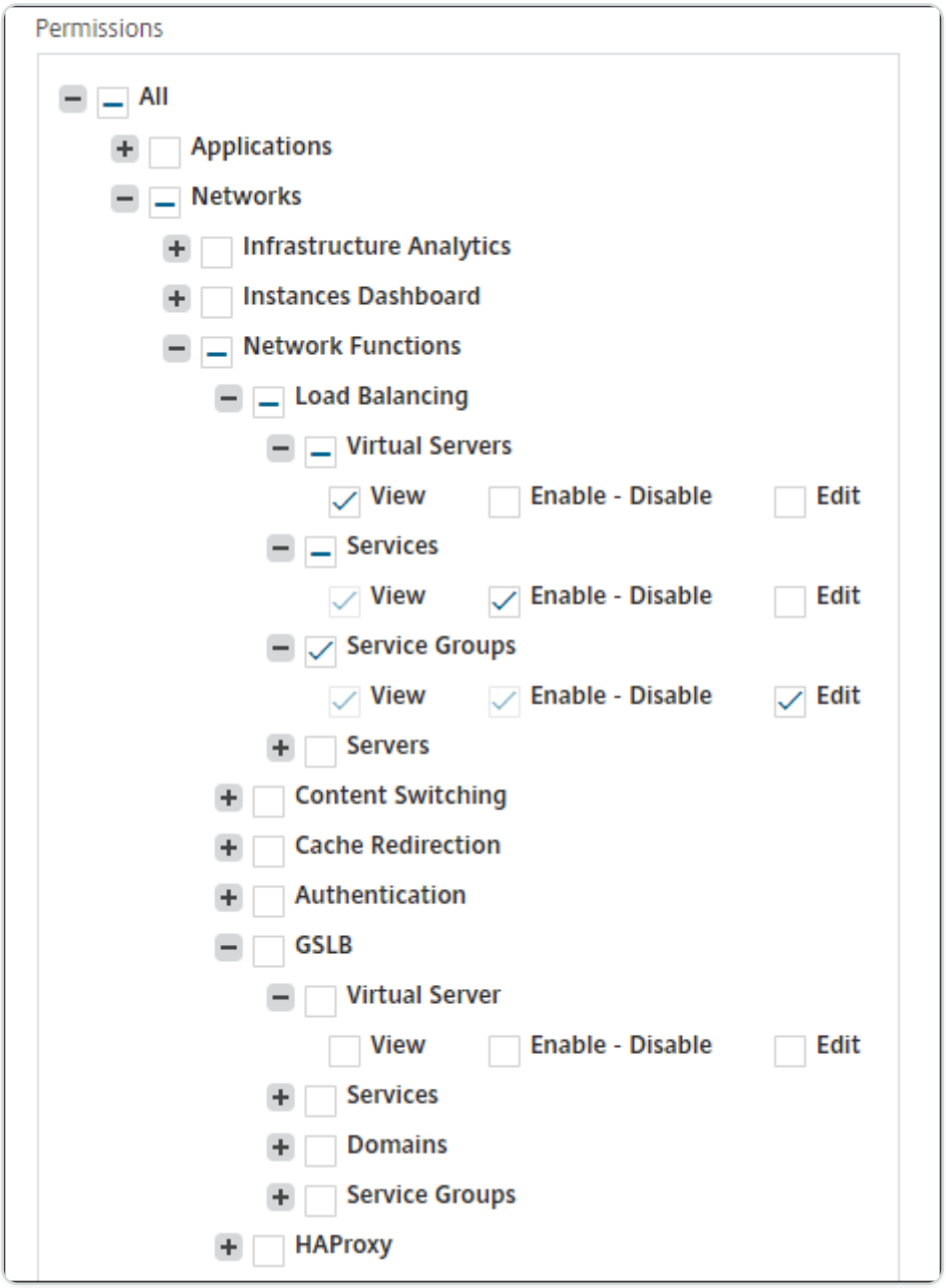
If you select the feature checkbox, it selects all the permissions for the feature.

NOTE:

Expand **Load Balancing** and **GSLB** to view more configuration options.

In the following image, the configuration options of the Load Balancing feature have different permissions:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **View** permission is granted to a user for the **Virtual Servers** feature. User can view the load balancing virtual servers in NetScaler Console. To view virtual servers, navigate to **Infrastructure > Network Functions > Load Balancing** and select the **Virtual Servers** tab.

The **Enable-Disable** permission is granted to a user for the **Services** feature. This permission also grants the **View** permission. The user can enable or disable the services bound to a load balancing virtual server. Also, the user can perform **Poll Now** action on services. To enable or disable services, navigate to **Infrastructure > Network Functions > Load Balancing** and select the **Services** tab.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

If a user has the **Enable-Disable** permission, the enable or disable action on a service is restricted in the following page:

a. Navigate to **Infrastructure > Network Functions**.

b. Select a virtual server and click **Configure**.

c. Select the **Load Balancing Virtual Server Service Binding** page. This page displays an error message if you select **Enable** or **Disable**.

The **Edit** permission is granted to a user for the **Service Groups** feature. This permission grants the full access where **View** and **Enable-Disable** permissions are granted. User can modify the service groups that are bound to a load balancing virtual server. To edit service groups, navigate to **Infrastructure > Network Functions > Load Balancing** and select the **Service Groups** tab.

4. Click **Create**.

NOTE:

Selecting **Edit** might internally assign dependent permissions that are not shown as enabled in the Permissions section. For example, when you enable edit permissions for fault management, NetScaler Console internally provides permission for configuring a mail profile or for creating SMTP server setups, so that the user can send the report as a mail.

Grant StyleBook permissions to users

You can create an access policy to grant StyleBook permissions such as import, delete, download, and more.

NOTE:

The View permission is automatically enabled when you grant other StyleBook permissions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure Roles on NetScaler Console

In NetScaler Console, each role is bound to one or more access policies. You can define one-to-one, one-to-many, and many-to-many relationships between policies and roles. You can bind one role to multiple policies, and you can bind multiple roles to one policy.

For example, a role might be bound to two policies, with one policy defining access permissions for one feature and the other policy defining access permissions for another feature. One policy might grant permission to add NetScaler instances in NetScaler Console, and the other policy might grant permission to create and deploy a StyleBook and to configure NetScaler instances.

When multiple policies define the edit and read-only permissions for a single feature, the edit permissions have priority over read-only permissions.

NetScaler Console provides five predefined roles:

- **admin_role**. Has access to all NetScaler Console features. (This role is bound to `adminpolicy`.)
- **adminExceptSystem_role**. Has access to the NetScaler Console GUI except for the Settings permissions. (This role is bound to adminExceptSystem_policy)
- **readonly_role**. Has read-only access. (This role is bound to `readonlypolicy`.)
- **appAdmin_role**. Has administrative access to only the application features in NetScaler Console. (This role is bound to appAdminPolicy).
- **appReadonly_role**. Has read-only access to the application features. (This role is bound to appReadOnlyPolicy.)

Though you cannot edit the predefined roles, you can create your own (user-defined) roles.

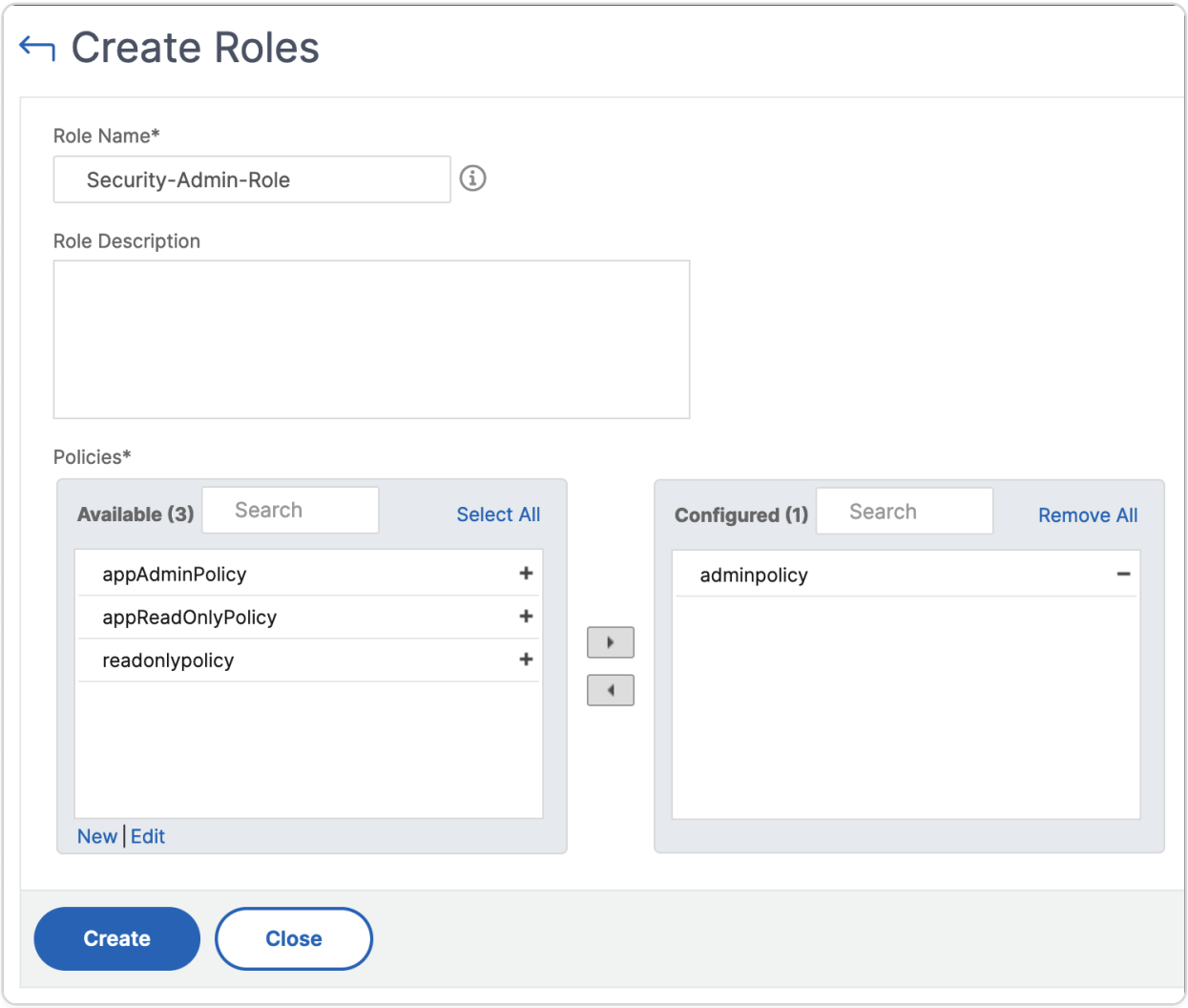
To create roles and assign policies to them:

1. In the NetScaler Console GUI, navigate to **Settings** > **Users & Roles** > **Roles**.
2. Click **Add**.
3. On **Create Roles** page, in the **Role Name** field, enter the name of the role, and provide the description in the **Role Description** field (optional.)
4. In the **Policies** section, add move one or more policies to the **Configured** list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The policies are pre-fixed with a tenant ID (for example, `maasdocfour`) that is unique to all tenants.



NOTE:

You can create an access policy by clicking **New**, or you can navigate to **Settings** > **Users & Roles** > **Access Policies,** and create policies.

5. Click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure Groups on NetScaler Console

In NetScaler Console, a group can have both feature-level and resource-level access. For example, one group of users might have access to only selected NetScaler instances; another group with only a selected few applications, and so on.

When you create a group, you can assign roles to the group, provide application-level access to the group, and assign users to the group. All users in that group are assigned the same access rights in NetScaler Console.

You can manage a user access in NetScaler Console at the individual level of network function entities. You can dynamically assign specific permissions to the user or group at the entity level.

NetScaler Console treats virtual server, services, service groups, and servers as network function entities.

- **Virtual server (Applications)** - Load Balancing(`lb`), GSLB, Context Switching (`CS`), Cache Redirection (`CR`), Authentication (`Auth`), and NetScaler Gateway (`vpn`)
- **Services** - Load balancing and GSLB services
- **Service Group** - Load balancing and GSLB service groups
- **Servers** - Load balancing Servers

To create a group:

1. In NetScaler Console, navigate to **Settings** > **Users & Roles** > **Groups**.
2. Click **Add**.

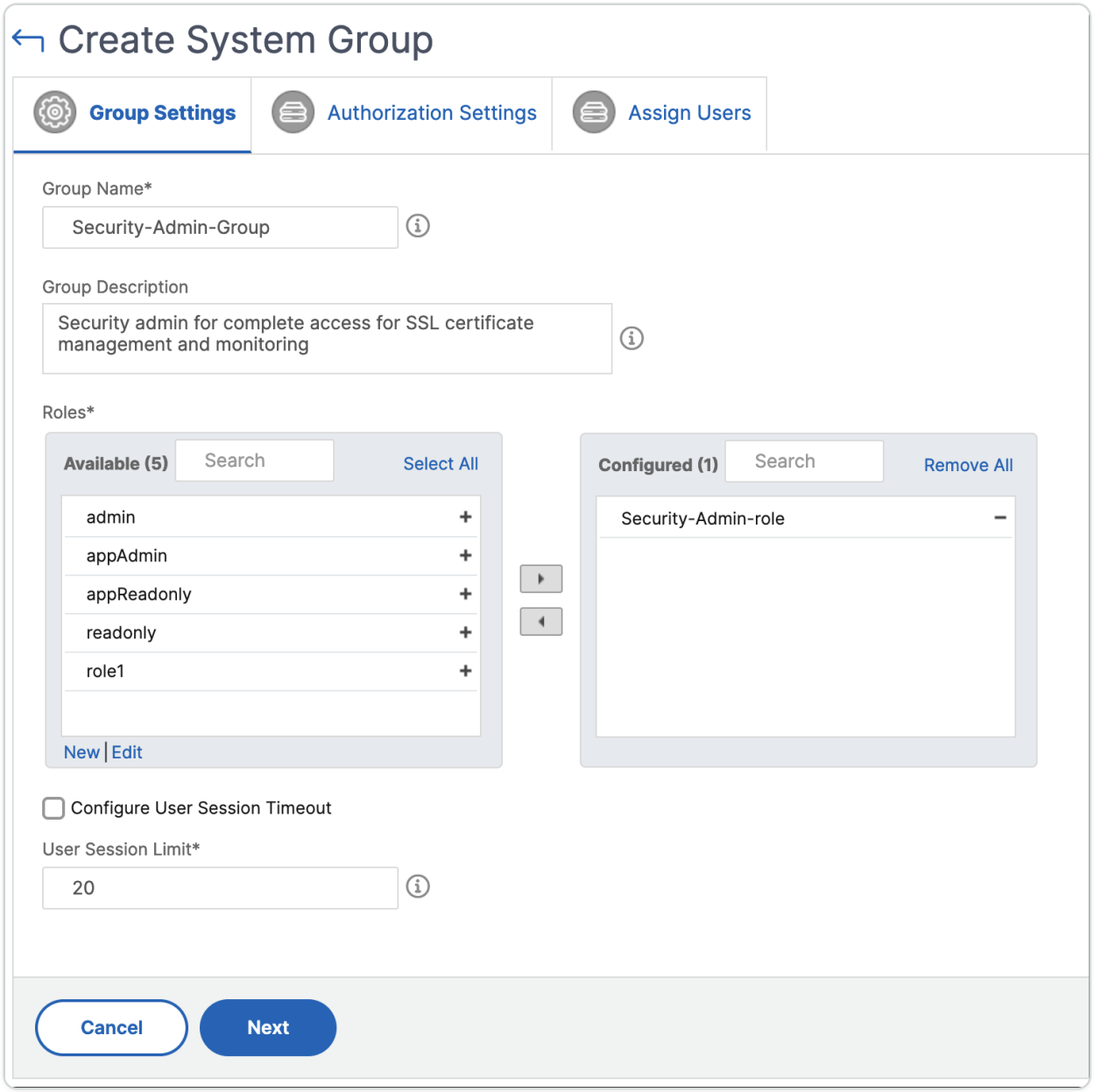
   The **Create System Group** page is displayed.
3. In the **Group Name** field, enter the name of the group.
4. In the **Group Description** field, type in a description of your group. Providing a good description helps you to understand the role and function of the group.
5. In the **Roles** section, move one or more roles to the **Configured** list.

   NOTE:

   The roles are pre-fixed with a tenant ID (for example, `maasdocfour`) that is unique to all tenants.
6. In the **Available** list, you can click **New** or **Edit** and create or modify roles.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Alternatively, you can navigate to **Settings > Users & Roles > Users**, and create or modify users.



7. Click **Next**.
8. In the **Authorization Settings** tab, you can choose resources from the following categories:

   - **Autoscale™ Groups**
   - **Instances**
   - **Applications**
   - **Configuration Templates**
   - **IPAM Providers and Networks**
   - **StyleBooks**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Config Packs**
- **Domain Names**

Select specific resources from the categories to which users can have access.

Autoscale Groups:

To select the specific Autoscale groups that a user can view or manage:

a. Clear the **All AutoScale Groups** checkbox and click **Add AutoScale Groups**.

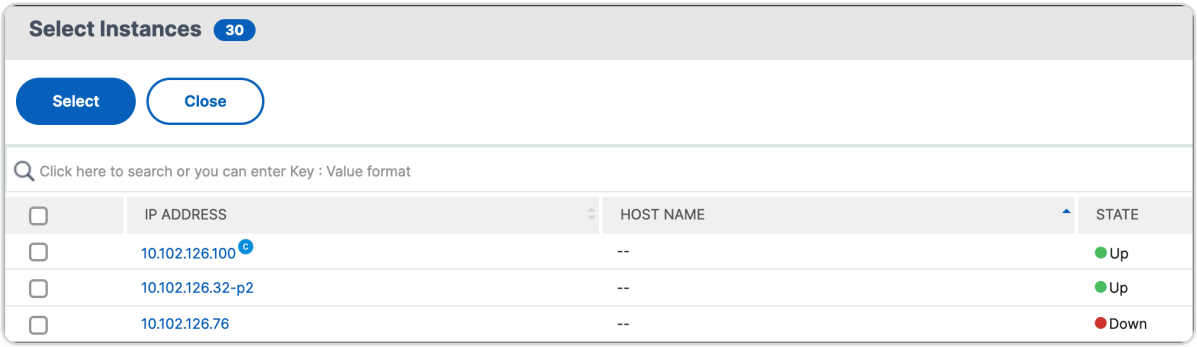
b. Select the required Autoscale groups from the list and click **OK**.

Instances:

To select the specific instances that a user can view or manage:

a. Clear the **All Instances** checkbox and click **Select Instances**.

b. Select the required instances from the list and click **OK**.

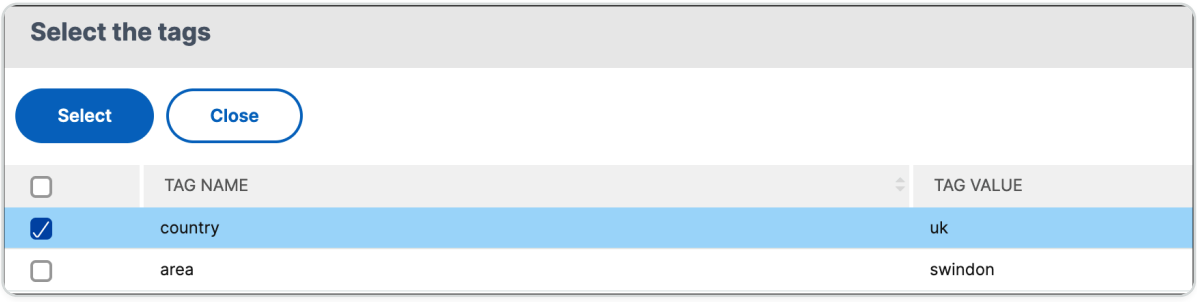


Tags:

To authorize users to view or manage specific instances based on associated tags:

a. Clear the **All Instances** checkbox and click **Select Tags**.

b. Select the required tags from the list and click **OK**.



Later, as you associate more instances with the selected tags, the authorized users automatically gain access to the new instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information about tags and associating tags to instances, see How to create tags and assign to instances.

Applications:

The **Choose Applications** list allows you to grant access to a user for the required applications.

You can grant access to applications without selecting their instances. Because applications are independent of their instances to grant user access.

When you grant a user access to an application, the user is authorized to access only that application regardless of instance selection.

This list provides you the following options:

- **All Applications:** This option is selected by default. It adds all the applications that are present in the NetScaler Console.
- **All Applications of selected instances:** This option appears only if you select instances from the **All Instances** category. It adds all the applications present on the selected instance.
- **Specific Applications:** This option allows you to add the required applications that you want users to access. Click **Add Applications** and select the required applications from the list.
- **Select Individual Entity Type:** This option allows you to select the specific type of network function entity and corresponding entities.

  You can either add individual entities or select all entities under the required entity type to grant access to a user.

  The **Apply on bound entities also** option authorizes the entities that are bound to the selected entity type. For example, if you select an application and select **Apply on bound entities also** , NetScaler Console authorizes all the entities that are bound to the selected application.

  NOTE:

  Ensure you have selected only one entity type if you want to authorize bound entities.

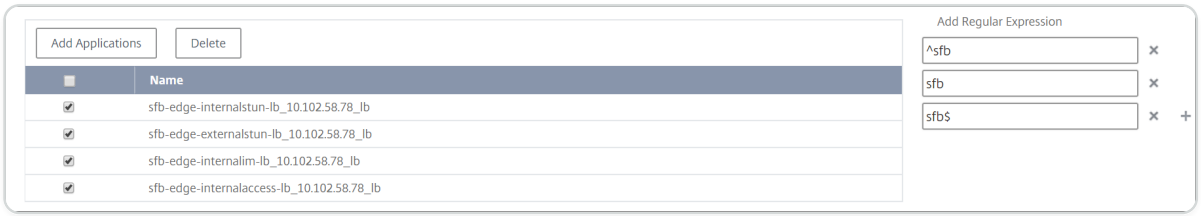
© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can use regular expressions to search and add the network function entities that meet the regex criteria for the groups. The specified regex expression is persisted in NetScaler Console. To add a regular expression, perform the following steps:

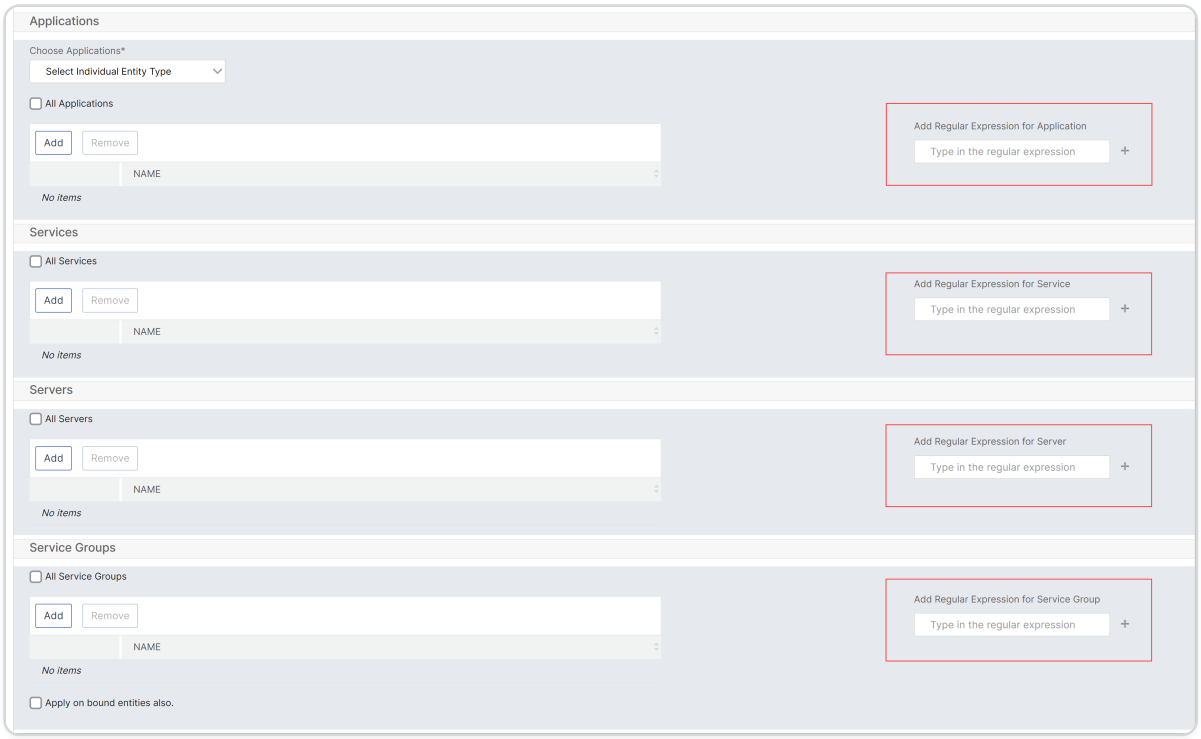
a. Click **Add Regular Expression**.

b. Specify the regular expression in the text box.

The following image explains how to use a regular expression to add an application when you select the **Specific Applications** option:



The following image explains how to use a regular expression to add network function entities when you choose the **Select the Individual Entity Type** option:



If you want to add more regular expressions, click the **+** icon.

NOTE:

The regular expression only matches the server name for the **Servers** entity type and not the server IP address.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you select the **Apply on bound entities also** option for a discovered entity, a user can automatically access the entities that are bound to the discovered entity.

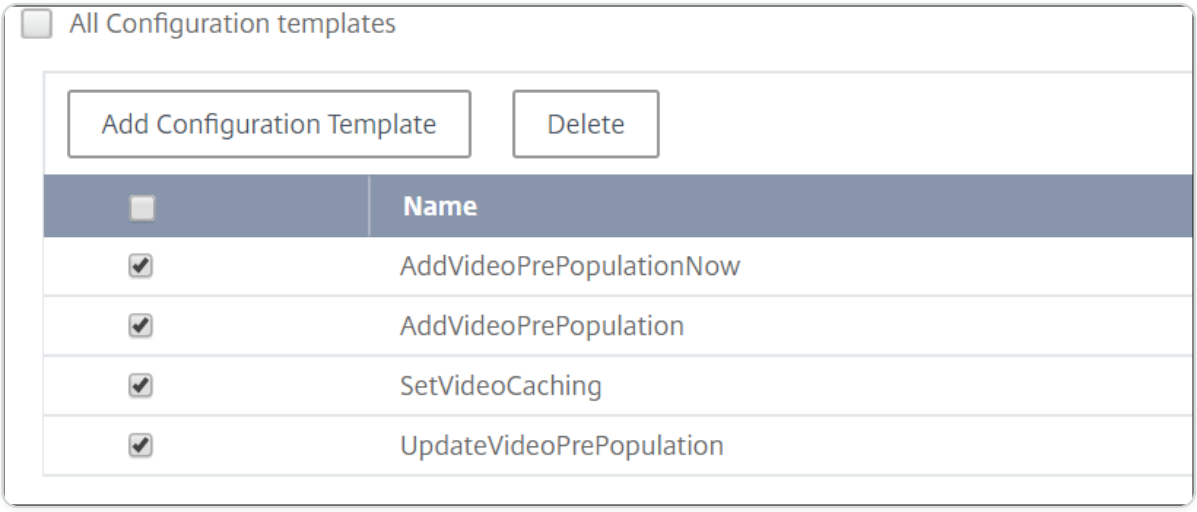
The regular expression is stored in the system to update the authorization scope. When the new entities match the regular expression of their entity type, NetScaler Console updates the authorization scope to the new entities.

Configuration Templates:

If you want to select the specific configuration template that a user can view or manage, do the following steps:

a. Clear **All Configuration templates** and click **Add Configuration Template**.

b. Select the required template from the list and click **OK**.



IPAM Providers and Networks:

If you want to add the specific IPAM providers and networks that a user can view or manage, perform the following:

- **Add providers** - Clear **All Providers** and click **Add Providers**. You can select the required providers and click **OK**.
- **Add networks** - Clear **All Networks** and click **Add Networks**. You can select the required networks and click **OK**.

StyleBooks:

If you want to select the specific StyleBook that a user can view or manage, do the following steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Clear the **All StyleBooks** checkbox and click **Add StyleBook to Group**. You can either select individual StyleBooks or specify a filter query to authorize StyleBooks.

   If you want to select the individual StyleBooks, select the StyleBooks from the **Individual StyleBooks** pane and click **Save Selection**.

   If you want to use a query to search StyleBooks, select the **Custom Filters** pane. A query is a string of key-value pairs where keys are `name`, `namespace`, and `version`.

   You can also use regular expressions as values to search and add StyleBooks that meet the regex criteria for the groups. A custom filter query to search StyleBooks supports both `And` and `Or` operation.

   Example:

   ```
   name=lb-mon|lb AND namespace=com.citrix.adc.stylebooks AND
   version=1.0
   ```

   This query lists the StyleBooks that meet the following conditions:

   - StyleBook name is either `lb-mon` or `lb`.
   - StyleBook namespace is `com.citrix.adc.stylebooks`.
   - StyleBook version is `1.0`.

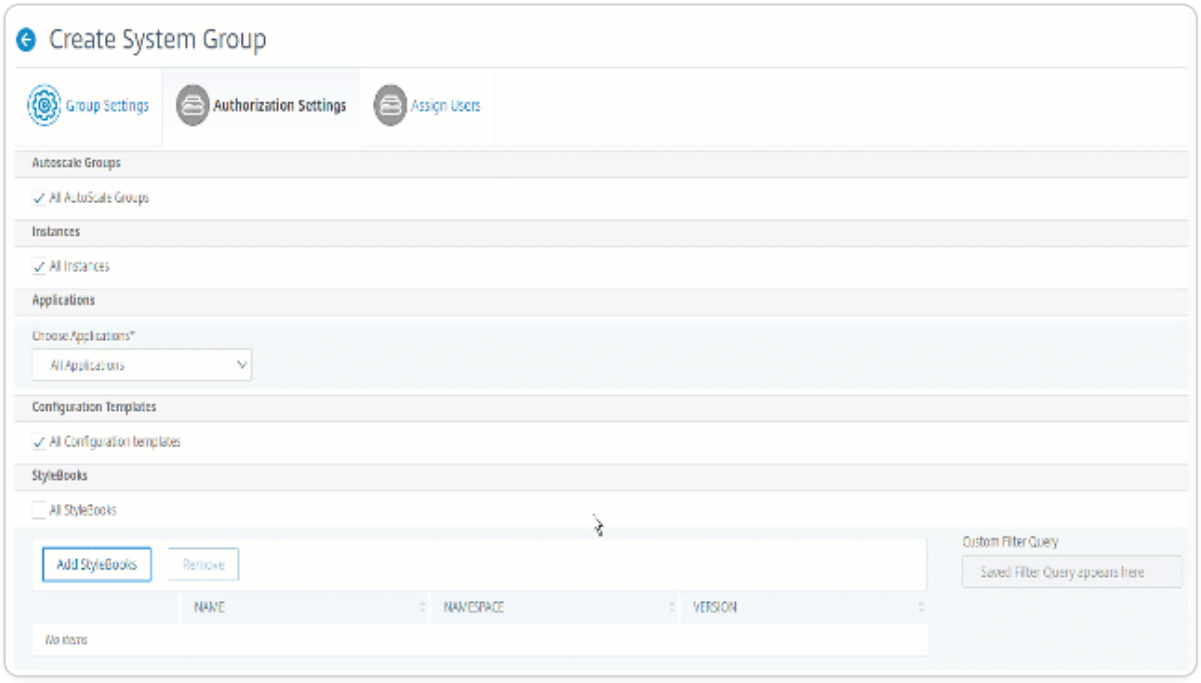
   Use an `Or` operation between value expressions that is defined to the key expression.

   Example:

   - The `name=lb-mon|lb` query is valid. It returns the StyleBooks having a name either `lb-mon` or `lb`.
   - The `name=lb-mon | version=1.0` query is invalid.

   Press `Enter` to view the search results and click **Save Query**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The saved query appears in the **Custom Filters Query**. Based on the saved query, the NetScaler Console provides user access to those StyleBooks.

b. Select the required StyleBooks from the list and click **OK**.

You can select the required StyleBooks when you create groups and add users to that group. When your user selects the permitted StyleBook, all dependent StyleBooks are also selected.

Config packs:

In the config packs, select one of the following options:

- **All Configurations**: This option is selected by default. It allows users to manage all the configurations in ADM.
- **All Configurations of the selected StyleBooks**: This option adds all the config packs of the selected StyleBook.
- **Specific Configurations**: This option allows you to add specific configurations of any StyleBook.
- **All Configurations created by the user group**: This option allows users to access only configurations created by users of the same group.

You can select the applicable config packs when you create groups and assign users to that group.

Domain Names:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you want to select the specific domain name that a user can view or manage, perform the following steps:

a. Clear the **All Domain Names** checkbox and click **Add Domain Name**.

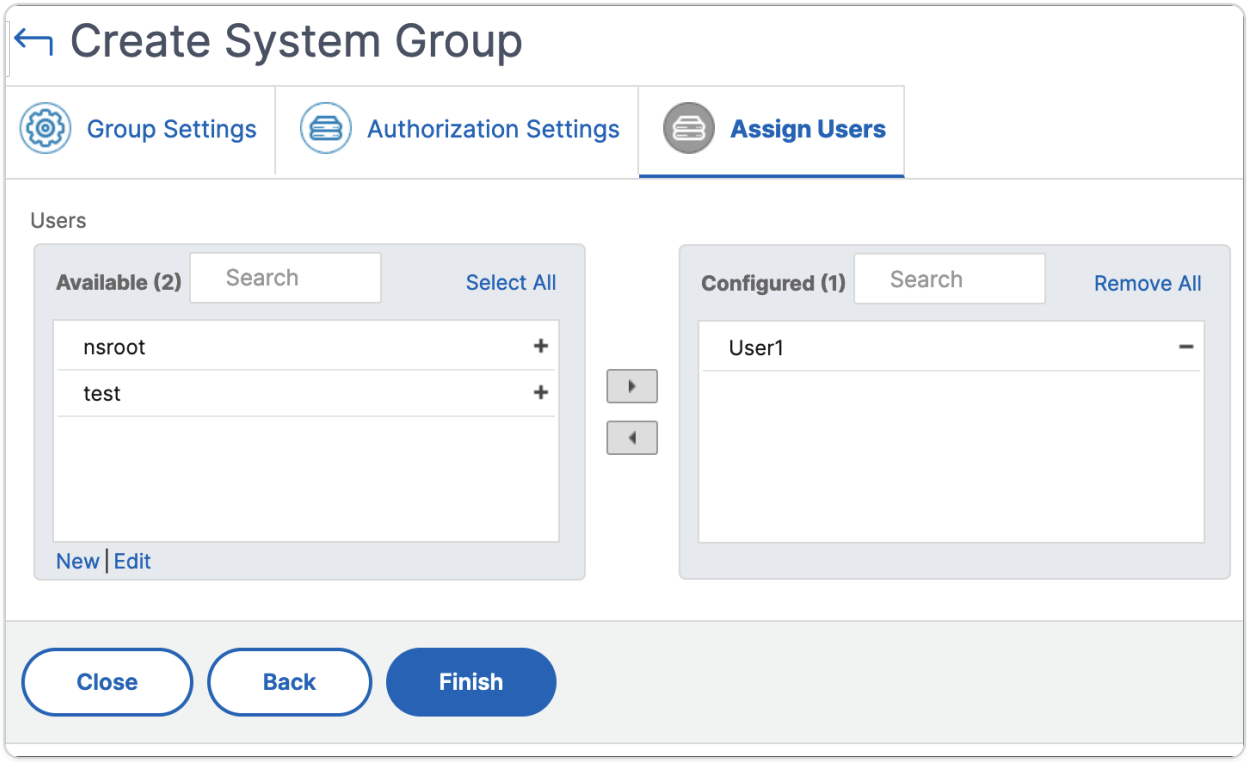
b. Select the required domain names from the list and click **OK**.

c. Click **Create Group**.

d. In the **Assign Users** section, select the user in the **Available** list, and add the user to the **Configured** list.

NOTE:

You can also add new users by clicking **New**.



a. Click **Finish**.

How user access changes based on the authorization scope

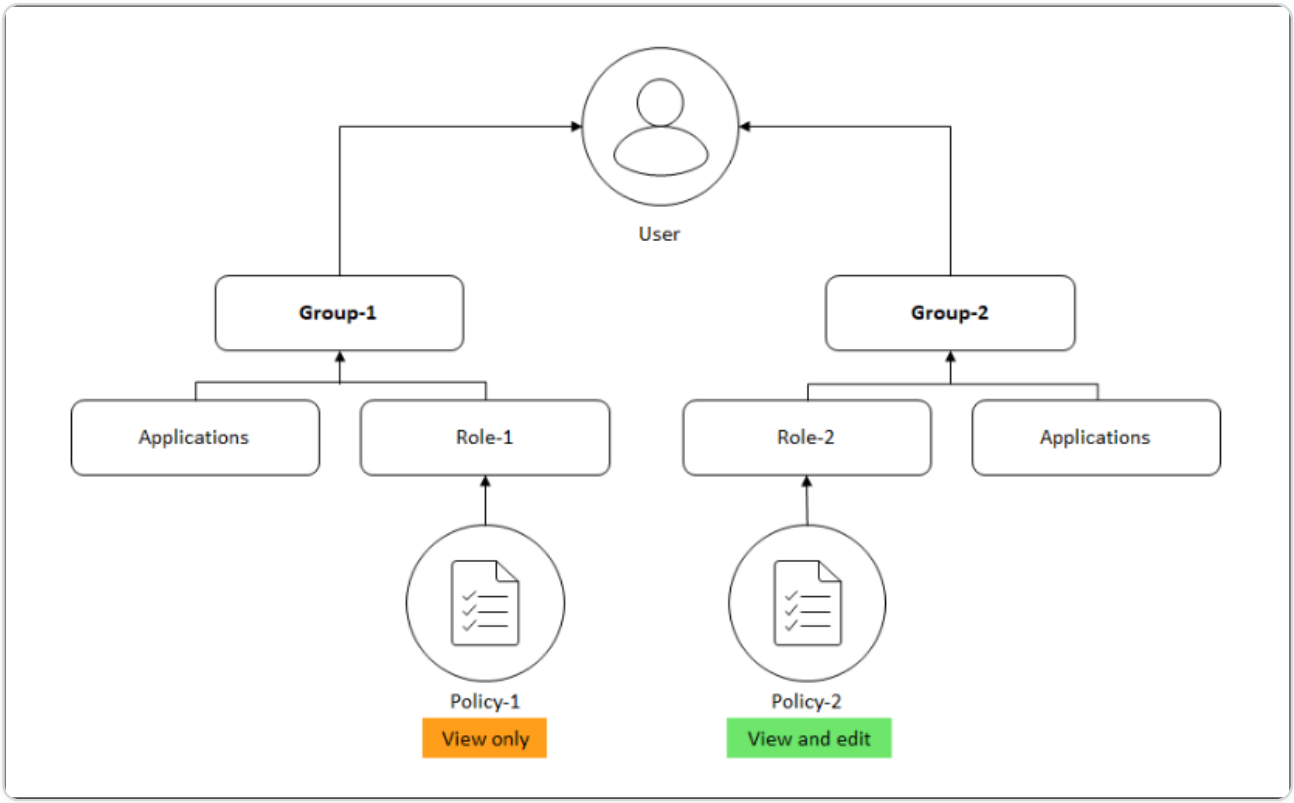
When an administrator adds a user to a group that has different access policy settings, the user is mapped to more than one authorization scopes and access policies.

In this case, the NetScaler Console grants the user access to applications depending on the specific authorization scope.

Consider a user who is assigned to a group that has two policies Policy-1 and Policy-2.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Policy-1** – View only permission to applications.
- **Policy-2** – View and Edit permission to applications.



The user can view the applications specified in Policy-1. Also, this user can view and edit the applications specified in Policy-2. The edit access to Group-1 applications are restricted as it is not under Group-1 authorization scope.

Limitations

The following NetScaler Console features do not fully support RBAC:

- **Analytics** - The analytics modules do not fully support RBAC. RBAC support is limited to an instance level, and it is not applicable at the application level in the Gateway Insight, HDX™ Insight, and Security Insight analytics modules.
  - Example 1: Instance-based RBAC (Supported). An administrator who has been assigned a few instances can see only those instances under **HDX Insight** > **Devices**, and only the corresponding virtual servers under **HDX Insight** > **Applications** because RBAC is supported at the instance level.
  - Example 2: Application-based RBAC (Not Supported). An administrator who has been assigned a few applications can see all virtual servers under **HDX Insight** > **Applications** but cannot access them, because RBAC is not supported at the applications level.
- **StyleBooks** – RBAC is not fully supported for StyleBooks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Consider a situation where many users have access to a single StyleBook but have access permissions for different NetScaler instances. Users can create and update config packs on their own instances since they do not have access to instances other than their own. But they can still view the config packs and objects created on NetScaler instances other than their own.

Assign a net profile for the managed NetScaler instance

When you enable analytics or metrics collector for the virtual servers in NetScaler Console, the AppFlow or metrics data from the NetScaler is exported to NetScaler Console through the NetScaler subnet IP address (SNIP). In some scenarios, the SNIP might be blocked because of the firewall in the network. In such scenarios, you might have to use a different IP address. For more information about net profile, see Use a specified source IP for back-end communication.

You can assign a net profile to a NetScaler instance through NetScaler Console for exporting AppFlow data from NetScaler to NetScaler Console.

Prerequisites

Ensure that:

- The NetScaler instance version is **13.0-48.4 or later**.
- Net profile is configured in NetScaler instances.

To assign a net profile in NetScaler Console:

1. Navigate to **Infrastructure > Instances > NetScaler**.
2. Select the instance, and from the **Select Action** list:
   - Click **Configure Net Profiles** to assign a net profile for AppFlow.
   - Click **Configure Net Profiles for Metrics Collector** to assign a net profile for metrics collector.
3. Select a net profile from the list and click **Apply**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

- For AppFlow, ensure that you disable analytics for all virtual servers before you assign a net profiles for the instance.
- For Metrics Collector, ensure that you disable metrics for all virtual servers before you assign a net profiles for the instance.

Data storage management

It's important to know which features are used in NetScaler Console and the data usage of each of these features. The **Data Storage Management** dashboard serves this purpose and functions as your visualization tool, enabling you to understand the total data stored in the NetScaler Console database across various features. The dashboard also indicates whether the consumed storage is within the specified limits or if it's more than the entitled storage.

As an admin, you can do the following tasks in the **Data Storage Management** dashboard:

- View the data storage consumption for the last 30 days - Data storage trends are stored in the NetScaler Console database for the last 30 days. These trends are available in graphical or tabular form. These trends show how much data has come in and how much data is stored after the scheduled pruning cycles in NetScaler Console.
- View data ingestion status - The data ingestion activity occurs as long as the consumed storage is within the limits of the entitled storage. When the consumed storage is more than the entitled storage, the data activity is paused.
- Send notifications - You can set notifications to be sent when consumed storage reaches 75% or 100% of the entitled storage, allowing users to manage their storage.
- Flexibility to manage data storage space - You can create more space within the stored data by pruning data that you consider suitable for removal or reduction.

Navigate to **Settings > Data Storage** to view your data storage dashboard.

The following sections outline how to use the **Data Storage Management** dashboard for effective data storage management:

- Understand your data storage - This section helps you understand how you can use the dashboard to view information about your data storage.

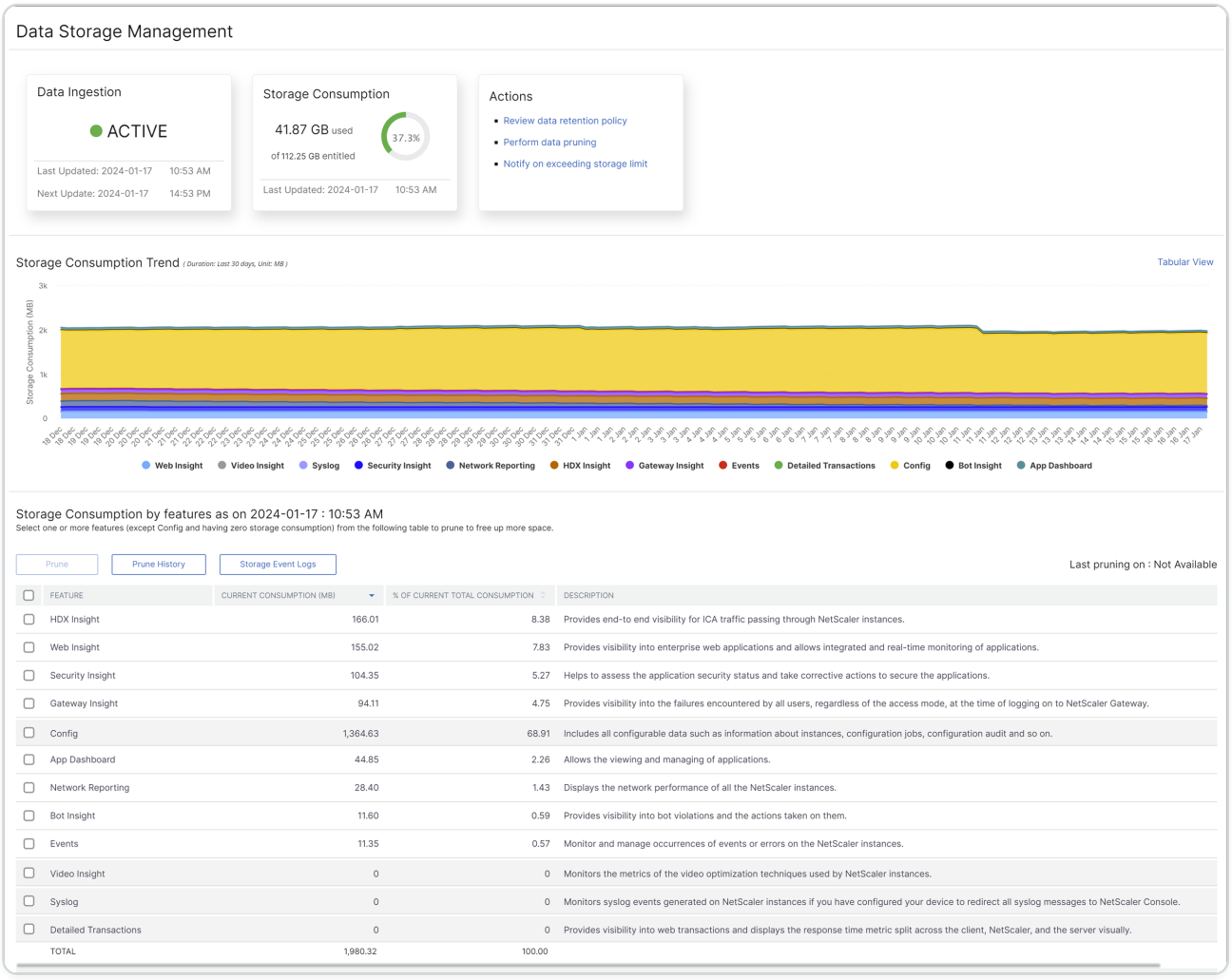
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Manage your data storage - This section provides information on what actions you can take in the dashboard to manage your data storage.

Understand your data storage

You can use the **Data Storage Management** dashboard in NetScaler Console to view data and graphs that help you track your data storage usage.

To monitor your data storage consumption, navigate to **Settings > Data Storage**.



The Data Storage Management dashboard indicates the following information:

- State of your data ingestion activity
- Total storage consumption
- Data Pruning status
- Storage consumption trends
- Storage consumption by features

© 1997–2026 Citrix Systems, Inc. All rights reserved.

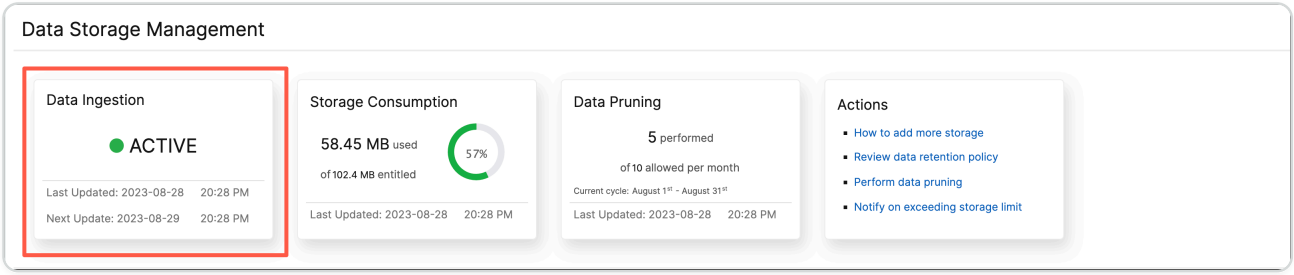
State of your data ingestion activity

Data ingestion refers to the process of importing large and assorted data from all the managed NetScaler instances across various features like Events, Syslogs, Network Reporting, and so on into the NetScaler Console storage.

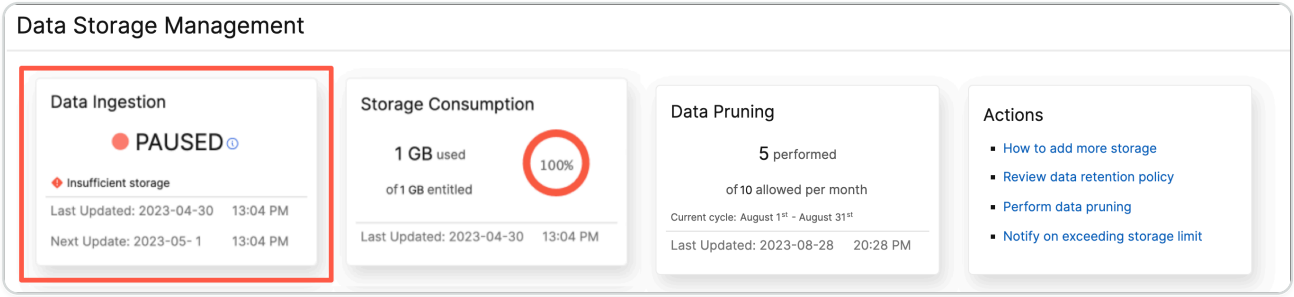
The data ingestion status indicates whether NetScaler Console is collecting statistics from NetScaler instances. The data ingestion activity continues as long as the consumed storage is within the entitled storage. When the consumption is more the entitled storage, the data ingestion is paused.

View the **Data Ingestion** tile to understand the current state of data ingestion. This tile displays either of the following two states:

- **Active** - The data ingestion activity is in progress.



- **Paused** - The data ingestion activity is paused since the consumed storage exceeds the entitled storage.



How to resume your paused data ingestion

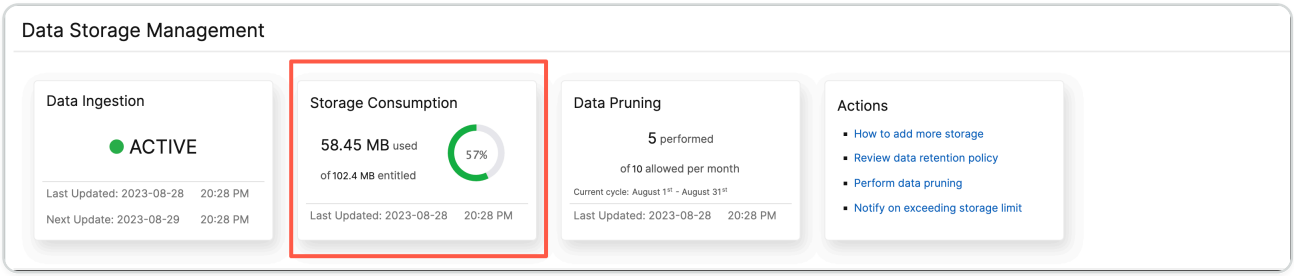
To resume your data ingestion activity, you can do either of the following actions:

- Add more data storage.
- Perform data pruning.

Total storage consumption

For a quick overview of your data storage, view the **Storage Consumption** tile.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **Storage Consumption** tile displays the total storage used by all the features in the deployment.

Hover over the donut chart to view the following:

Entitled Storage

The entitled storage is the total storage available for you to use as per your license. If you have an Express license, you get 500 MB of entitled storage. If you have an Advanced license, you get the sum of 500 MB of storage per purchased VIP and any additional storage that was bought directly without buying VIPs.

Consider the following scenarios:

- You bought 20 VIPs. You get 500 MB of free storage for each VIP. Your entitled storage is 20*500 = 10 GB.
- You bought 20 VIPs and an add-on storage of 5 GB. You get 500 MB of free storage for each VIP. Your entitled storage is 20*500 + 5 = 15 GB.

Consumed Storage

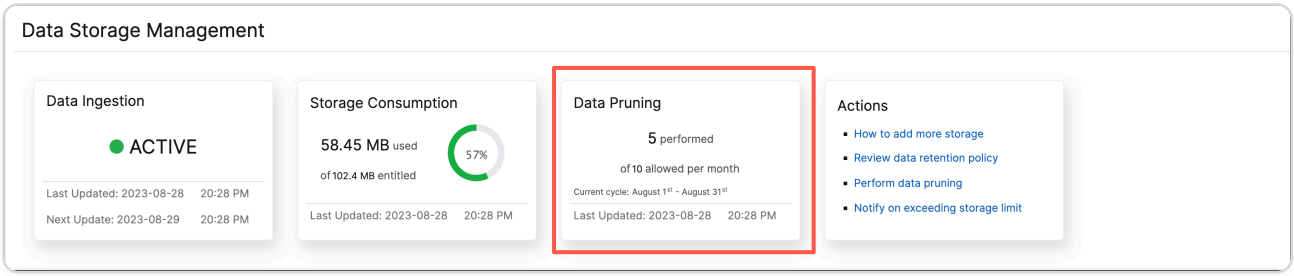
The consumed storage is the total storage used by all the features in the deployment. The following color coding criteria specify the amount of storage used by the features:

- **Green** - The consumed storage is less than 75% of entitled storage.
- **Amber** - The consumed storage is between 75% to 99% of entitled storage.
- **Red** - The consumed storage limit has reached or is above the current entitled storage.

Data pruning status

Pruning is the process of manually deleting data and freeing your storage space. You are allowed 10 data prunes in every calendar month. For example, you can delete your data 10 times from July 1 to July 31.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



To know how many data prunes you've already used up and how many you have left, view the **Data Pruning** tile.

NOTE:

Each pruning activity is counted as one data prune regardless of the number of features selected.

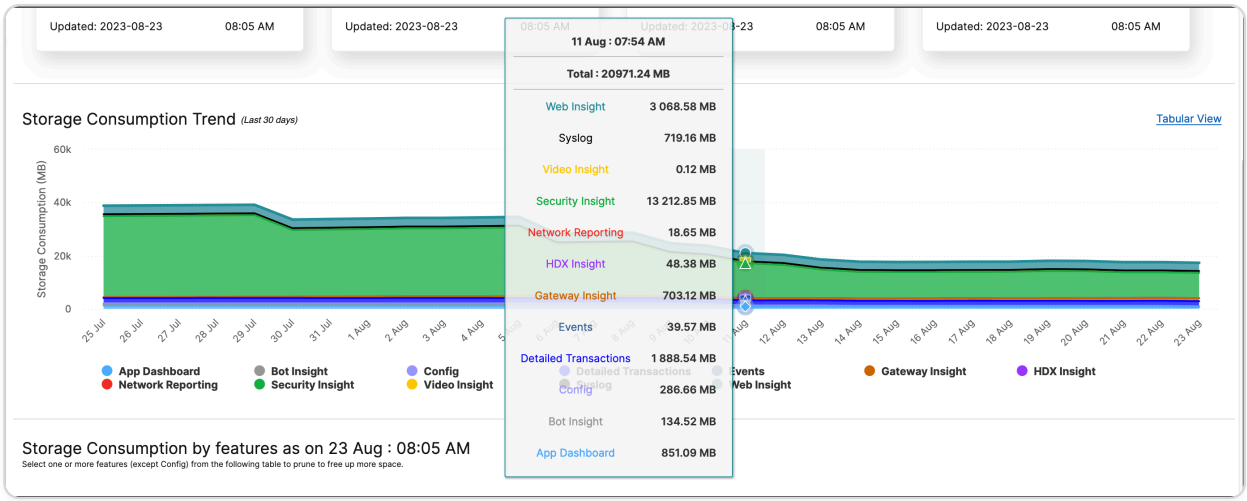
Storage consumption trends

To know how data is being consumed over the last 30 days, view the **Storage Consumption Trend** section.

Storage Consumption Trend provides insights into which features use the most or least storage over a time period and help you effectively manage your data storage consumption.

You can view the storage data trends in either of the following forms:

- **Graphical View** – Displays how the data storage is distributed across the different NetScaler Console features. Hover your mouse over the timeline to view the data storage information for any day of the month.

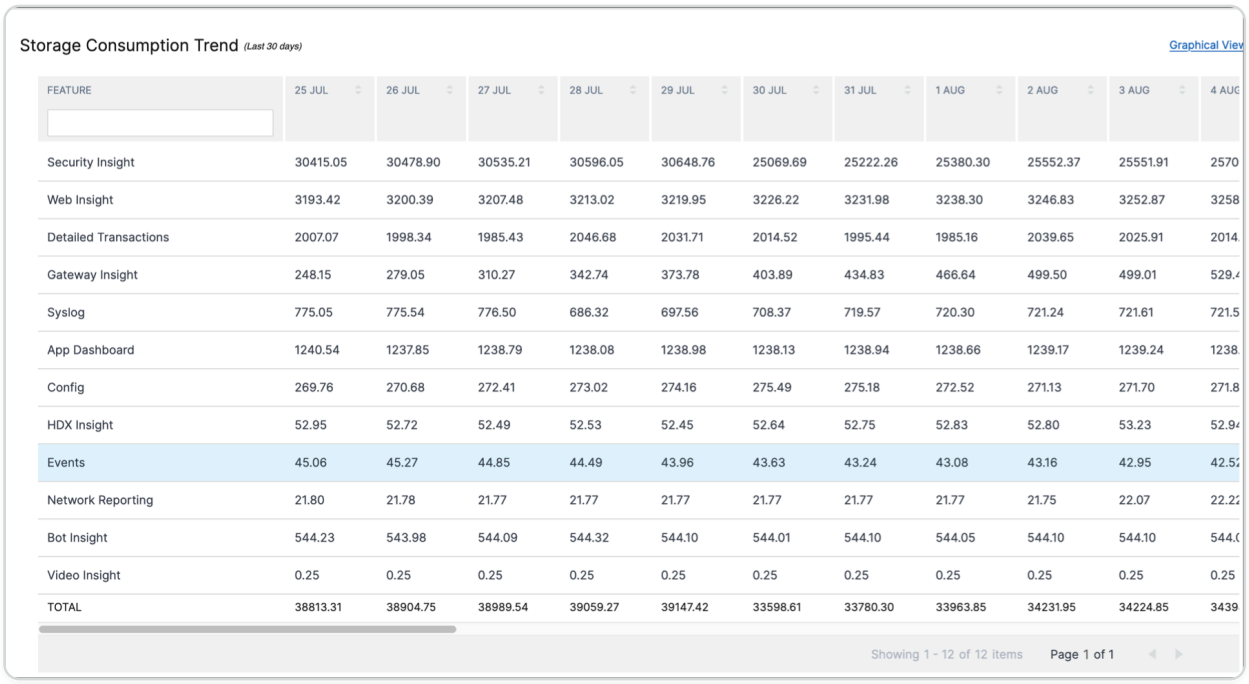


© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

The **Graphical View** is the default view.

- **Tabular View** – Click **Tabular View** to display the data storage information in a table form.



NOTE:

The tabular view allows you to filter the data by using the search field.

The following table describes the fields displayed in the **Storage Consumption Trend** section:

FEATURE	DESCRIPTION
Config	Includes all configurable data such as information about instances, configuration jobs, configuration audit and so on.
HDX Insight	Provides end-to-end visibility for ICA traffic passing through NetScaler.
Network Reporting	Displays the network performance of all the NetScaler instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FEATURE	DESCRIPTION
Web Insight	Provides visibility into enterprise web applications and allows integrated and real-time monitoring of applications.
Security Insight	Helps to assess the application security status and take corrective actions to secure the applications.
Gateway Insight	Provides visibility into the failures encountered by all users, regardless of the access mode, at the time of logging on to NetScaler Gateway.
Events	Monitor and manage occurrences of events or errors on the NetScaler instances.
App Dashboard	Allows the viewing and managing of applications.
Bot Insight	Provides visibility into bot violations and the actions taken on them.
Syslog	Monitors syslog events generated on NetScaler instances if you have configured your device to redirect all syslog messages to NetScaler Console.
Video Insight	Monitors the metrics of the video optimization techniques used by NetScaler instances.
Detailed Transactions	Provides visibility into web transactions and displays the response time metric split across the client, NetScaler, and the server visually.

Storage consumption by features

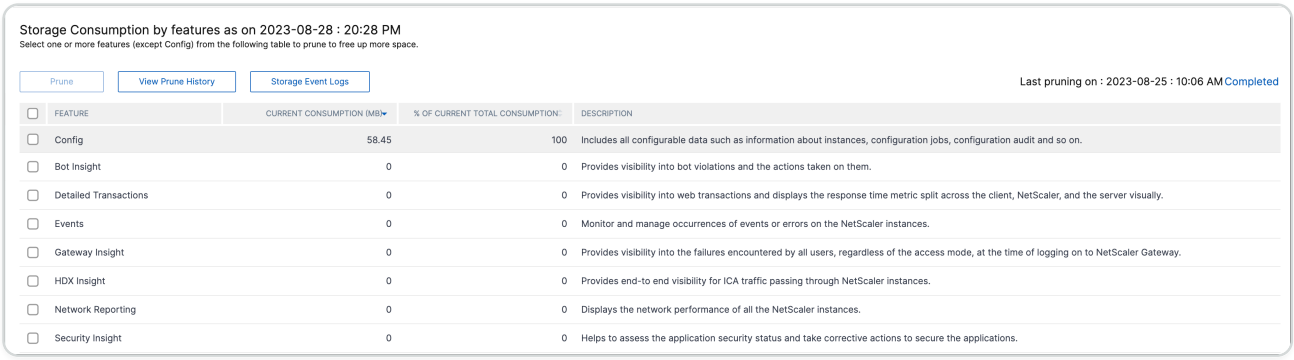
To know more about how the data storage is distributed across the different features, view the **Storage Consumption by features as on *dd mmm*** section.

Storage Consumption by features as on *dd mmm* helps you understand:

- The storage space used by all the different features in NetScaler Console

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The percentage of space the features consume on a particular day

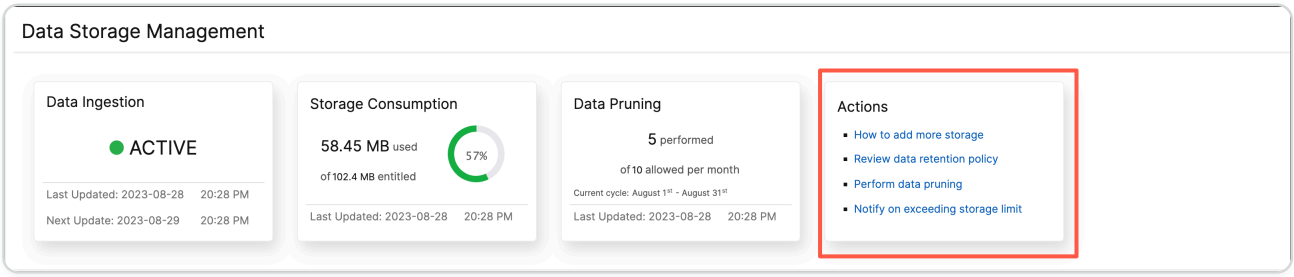


If you want to sort the table entries, the headers of the table. NetScaler Console alpha-numerically sorts the table from top to bottom based on the data in the chosen column. To sort the table in reverse order, click the column heading again.

For information on pruning your data, prune history, and Storage Event logs, see Manage your data storage.

Manage your storage space

You can use the **Data Storage Management** dashboard to observe your data storage usage and to take the necessary actions to clear space or increase storage when your data storage is over the licensed limit.



The **Actions** tile displays the list of recommended steps that you can take to manage your storage capacity:

- Review data retention policy
- Perform data pruning
- Notify on exceeding the storage limit

When your consumed storage reaches 100% of the licensed storage, the data ingestion activity is paused, and data is no longer stored in NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

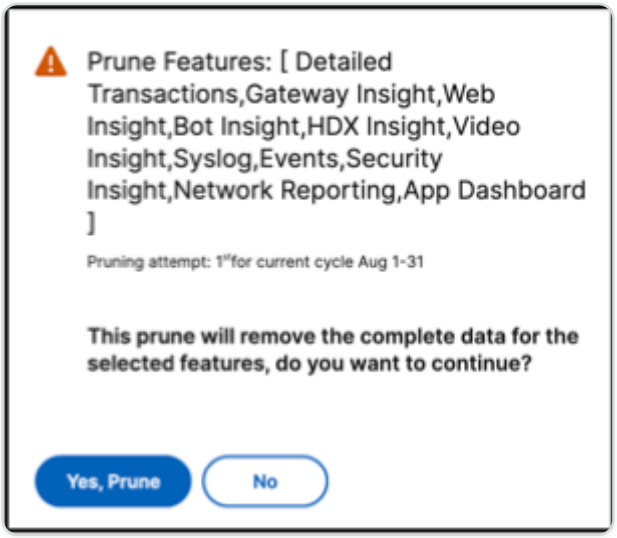
Perform data pruning

Prune your data to optimize storage resources and get more storage space. In addition to freeing up space, data pruning enhances data quality and accelerates processing times. We recommend you review and purge unnecessary data at regular intervals. This process makes sure that your resources are used judiciously and NetScaler Console is agile and responsive.

To prune your data:

1. In the **Data Storage Management** page, scroll down to the ***Storage Consumption by features as on yyyy-mm-dd*** section.
2. Select one or more features and click **Prune**. You can't select **Config** as it includes all the system configurations.

   A pop-up window prompts you to confirm if you want to delete all the data for the selected features. Click **Yes, Prune**.



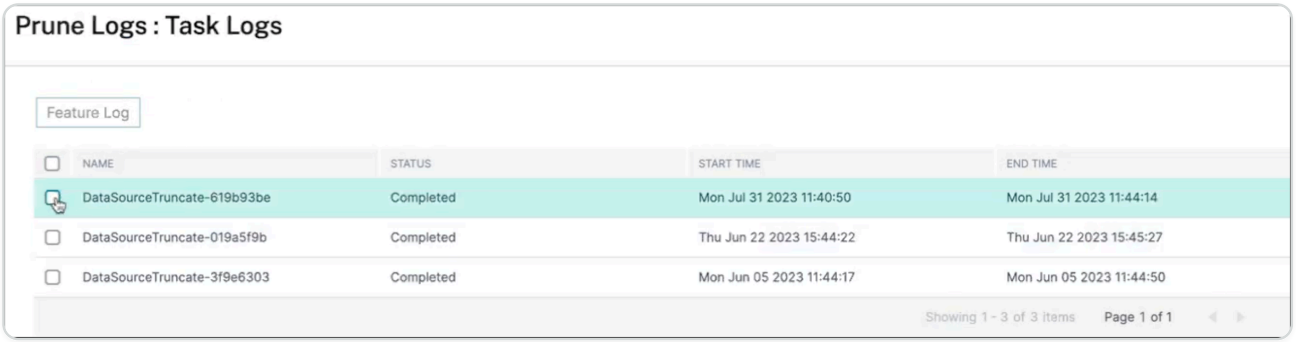
NOTE:

The pop-up window also displays information about your current pruning attempt.

View prune history

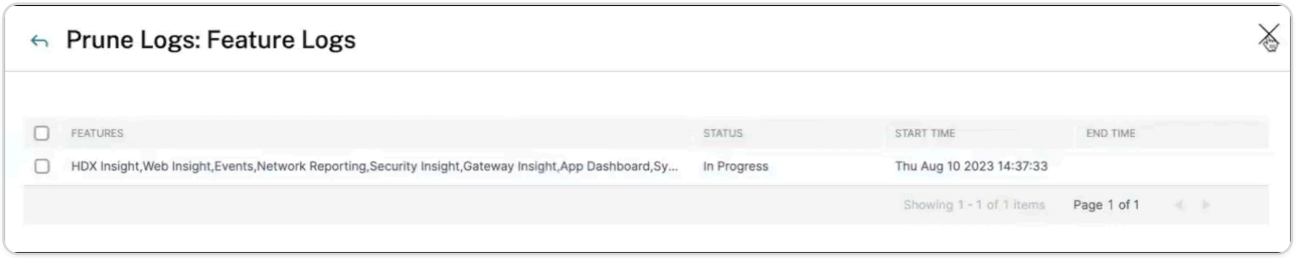
Click **View Prune History** to get details on the all the prune activities that you did in NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



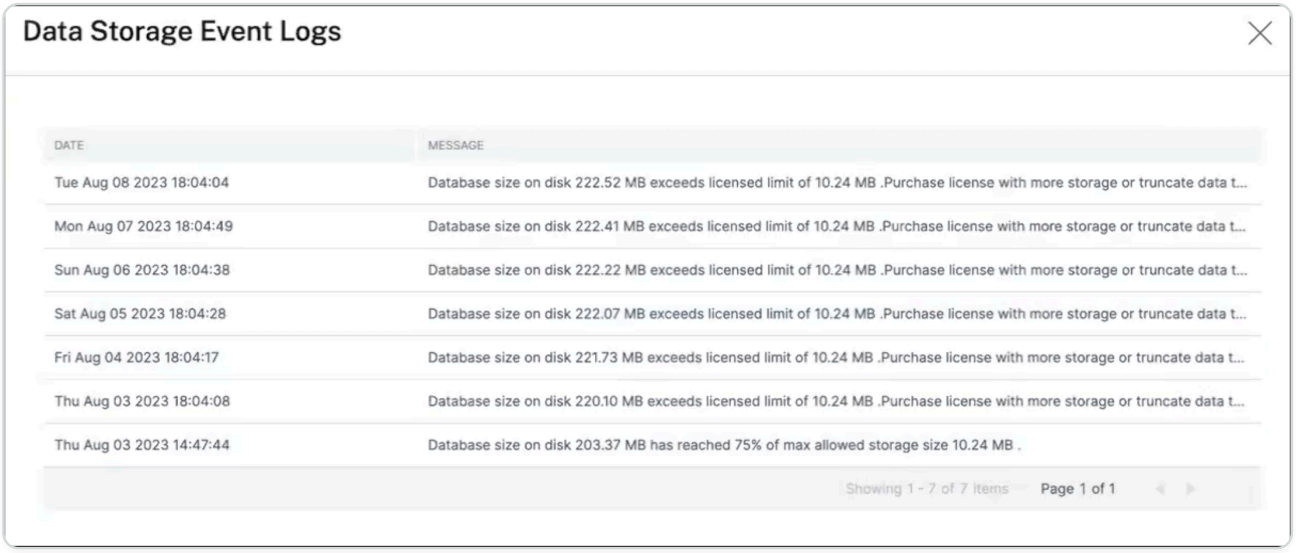
The **Prune Logs: Task Logs** page displays the list of all the prune tasks, including their respective statuses, start time, and end time.

To understand which features were removed in each of the prune operations, select a task and click **Feature Log**.



View storage event logs

Click **Storage Event Logs** to get insights into all the times that your data went over or reached 75% of your licensed limit.



Review data retention policy

The data retention policy refers to a set of rules and configurations that determine how NetScaler Console manages and maintains historical data over time. This policy outlines how long data is stored before the data is automatically deleted.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you want to reduce the storage space used by all the different features, you can change how long data is kept in NetScaler Console.

Use the **Data Retention policy** page to edit the data storage settings for:

- Event messages
- Syslog messages
- Network reporting data

For more information on the data storage settings, see Data Retention Policy.

Notify on exceeding storage limit

You can set up notifications for NetScaler Console to send you alerts when your data storage capacity exceeds the specified limits.

To view and configure your system notifications:

1. In the **Actions** tile, click **Notify on exceeding storage limit**.
2. In the **Configure System Notifications** page, under the **System Event Category**, make sure the **DataStorageExceeded** category is selected to receive notifications.

You can specify various parameters related to how and when notifications are sent to you or other users. Select the preferred communication method (for example, email, Slack, PagerDuty, and ServiceNow notifications) and define the recipients for the notifications.

For more information on how to set up the profiles and send notifications, see Configure Notifications.

Data retention policy

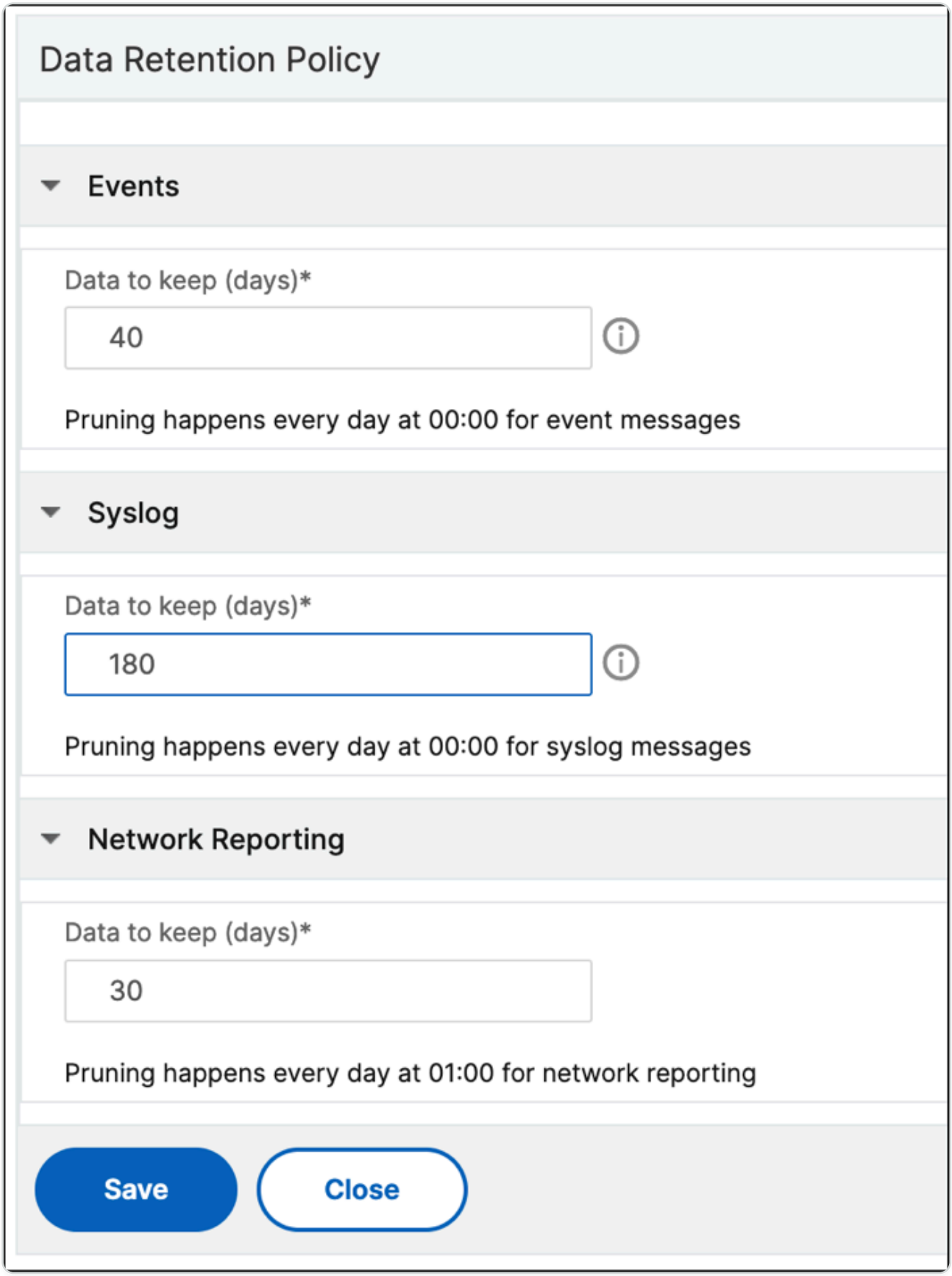
You can access system events, syslog messages, and network reporting data for a specific duration in NetScaler Console.

1. Navigate to **Settings > Data Storage > Data Retention Policy** to configure the data retention.
2. Click the edit button.
3. Enter the number of days that you want the data to be kept in NetScaler Console for each of the following options :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OPTIONS	DESCRIPTION
Events	Enables you to limit the event messages stored in NetScaler Console up to 40 days. The events are deleted from NetScaler Console after the retention policy is expired. The cleared events are deleted after one day.
Syslog	Enables you to limit the amount of syslog data stored in the database up to 180 days.
Network Reporting	Enables you to limit the network reporting data stored in NetScaler Console up to 30 days.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT:

You can't edit the data retention policy with an Express account.

When your account is converted to an Express account, the NetScaler Console retains the storage data up to 500 MB or one day data, whichever is the lesser. For more information, see Manage NetScaler Console resources using Express account.

Configure and view system alarms

You can enable and configure a set of alarms to monitor the health of your NetScaler Console servers. You must configure system alarms to make sure you are aware of any critical or major system issues.

For example, you might want to be notified if the CPU usage is high or if there are multiple login failures to the server. For some alarm categories, such as cpuUsageHigh or memoryUsageHigh, you can set thresholds and define the severity (such as Critical or Major) for each. For some categories, such as inventoryFailed or loginFailure, you can define only the severity. When the threshold is breached for an alarm category (for example, memoryUsageHigh) or when an event occurs corresponding to the alarm category (for example, loginFailure), a message is recorded in the system and you can view the message as syslog message. You can further set notifications to receive an email or SMS corresponding to your alarm settings.

You can assign or modify the severity of an alarm. The severity levels that you can assign are Critical, Major, Minor, Warning, and Informational.

Configure an alarm

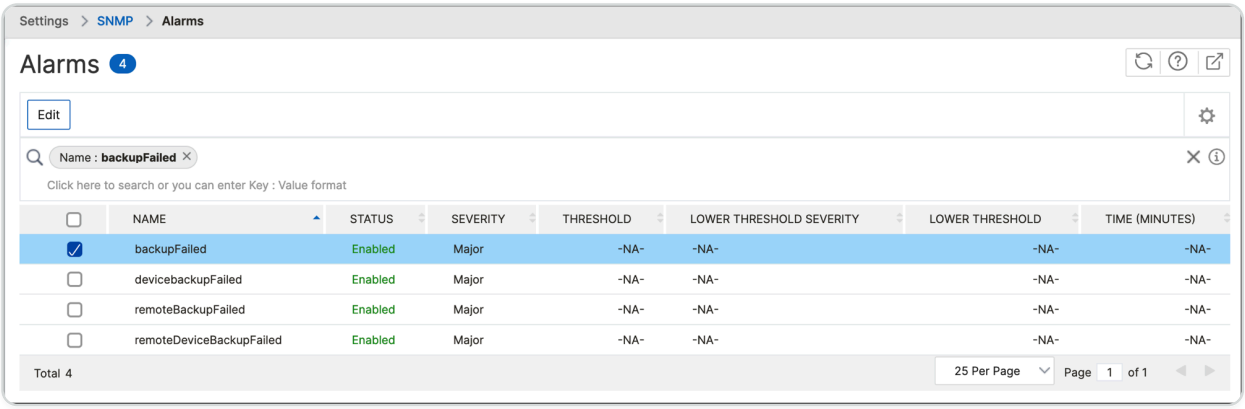
Consider a scenario where you want to monitor a failed backup attempt. You can enable the backupFailed alarm and assign a severity, such as Major, to it. Whenever NetScaler Console attempts to back up the system files and when the attempt fails, an alarm is triggered. You can view the message on the NetScaler Console log messages page or get notifications through email or SMS.

To configure the alarm, you must select the backupFailed alarm and specify the severity level as Major. The alarm is enabled by default.

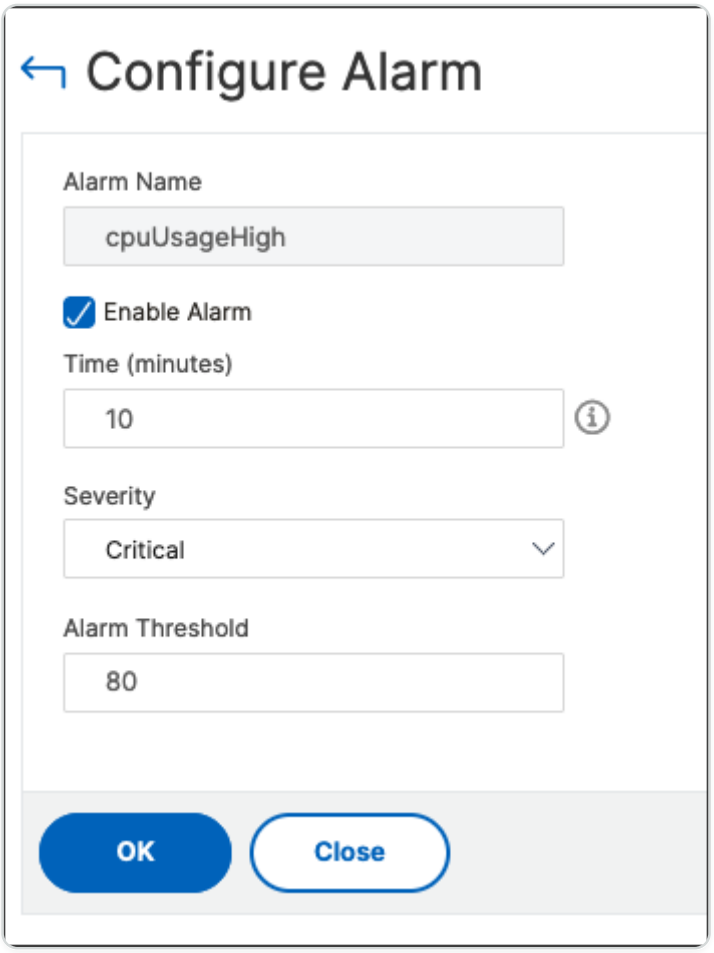
To configure and view a system alarm by using NetScaler Console:

1. Navigate to **Settings > SNMP**. Click **Alarms** in the upper-right corner.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Select the alarm you want to configure (for example, cpuUsageHigh) and click **Edit** to modify its settings.



3. In the **Configure Alarm** page, select **Enable Alarm** to create alerts and then specify the following:

   - **Time**. Type the time (in minutes) after which you want to trigger the alarm.
   - **Severity**. Select the severity level.
   - **Alarm Threshold**. Enter the value for which the alarm should be triggered and alerts sent to you.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

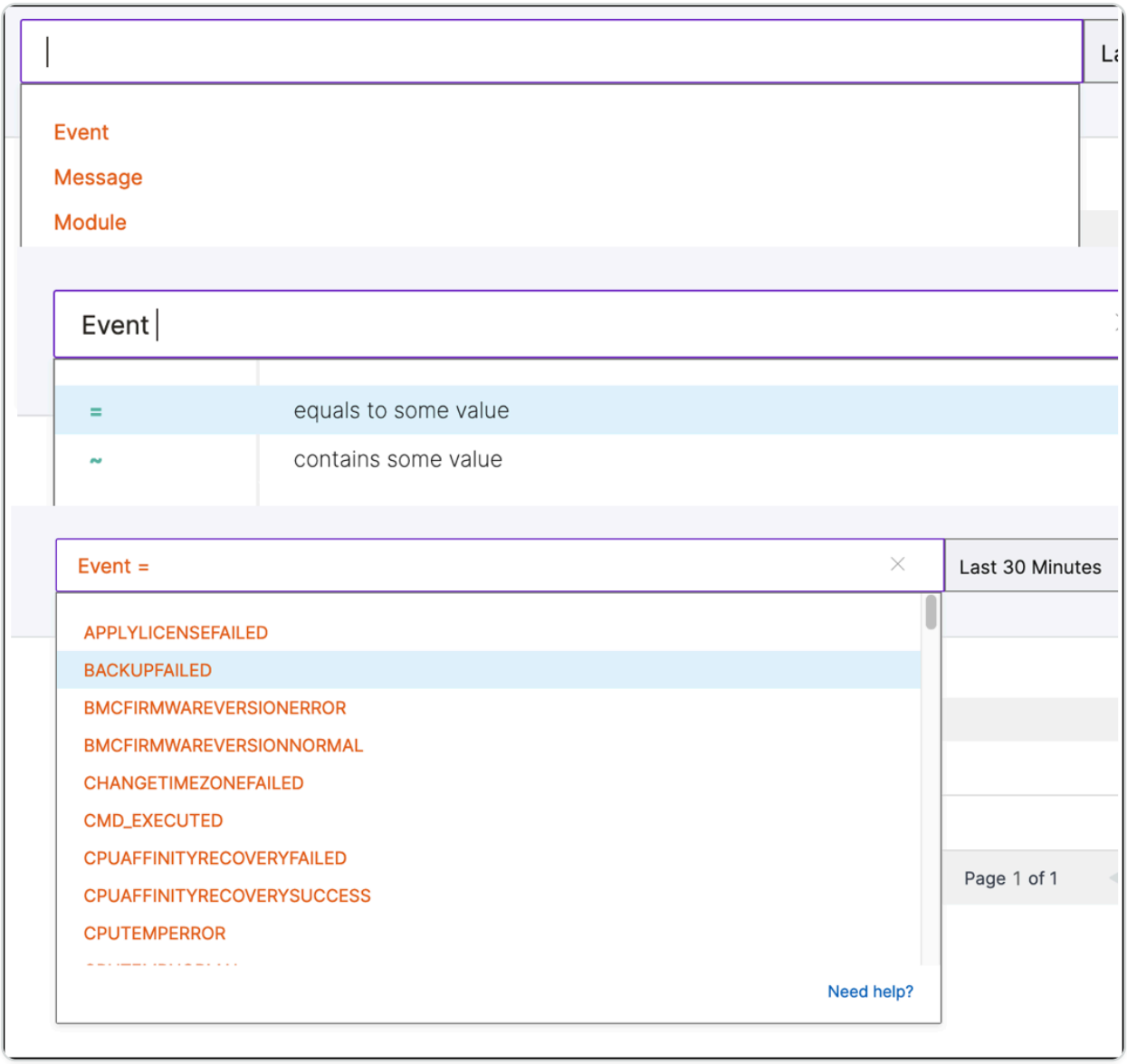
Click **OK**.

NOTE:

You cannot set the threshold for some alarms, for example, backupFailed. When the alarm is triggered, you can view the generated event as a syslog message.

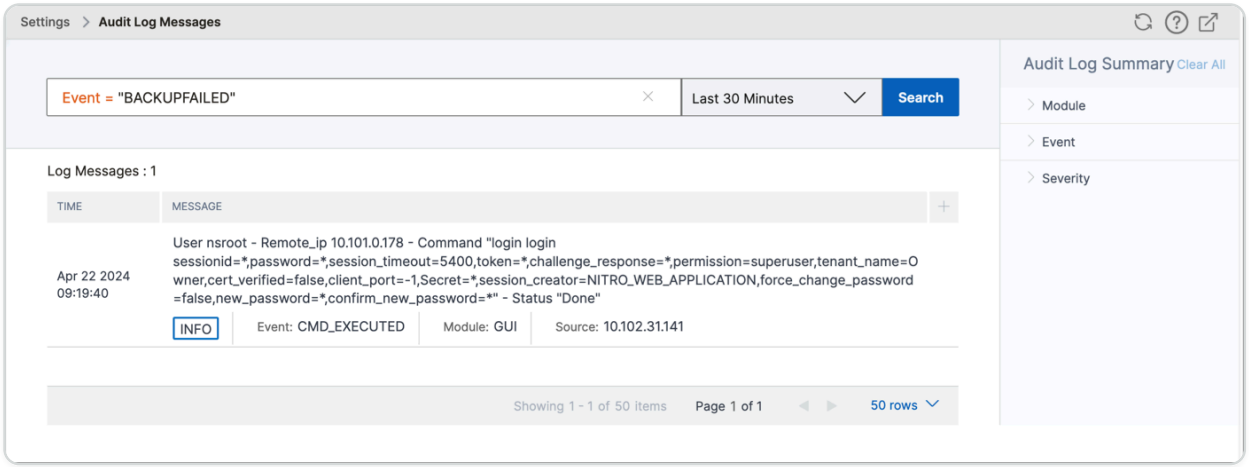
To view the event generated by alarm (for example, backupFailed):

1. Navigate to **Settings** > **Audit Log Messages**.
2. In the search field, select the type of alarm. In this example, select **Event**, **=** (equals to some value) and then **BACKUPFAILED**.



The event generated for a failed backup is displayed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can also set notifications to receive either an email or an SMS (Short Message Service) text when an alarm is triggered.

Add threshold limits to disk utilization alarms

Disk utilization alarms are triggered when the amount of disk space used on the NetScaler Console server exceeds a predefined threshold.

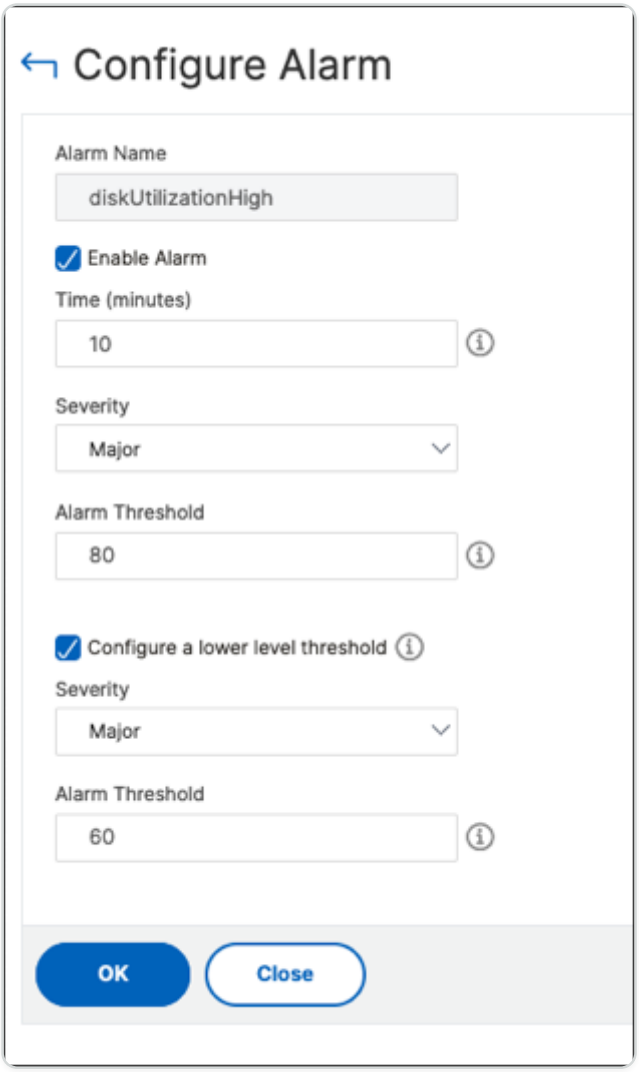
As an admin, when you receive alerts, you can choose to delete unnecessary data or allocate additional storage resources to prevent service disruptions or performance degradation.

Starting from release 14.1 build 25x, you can also add a lower-level threshold for disk utilization alarms. With this threshold value, you can set a lower-level limit to receive alerts before an upper threshold limit is breached.

To configure a lower-level threshold:

1. Navigate to **Settings > SNMP > Alarms** and in the search field, enter diskUtilizationHigh to view the disk utilization alarms.
2. Select the alarm and click **Edit**.
3. In the **Configure Alarm** page, select **Configure a lower-level threshold**. Enter the lower-level threshold limit.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For example, if you set a lower disk utilization threshold of 60 and an upper threshold of 80, you receive an alert when the disk usage exceeds 60% of the disk capacity. This setting allows you to take corrective actions before the disk utilization reaches 80%.

Observability Integration

Due to the increasing complexity of modern applications, administrators are facing challenges in:

- Monitoring and troubleshooting applications.
- Gaining visibility into the behavior of infrastructure and applications.

Observability bridges this gap by providing these insights into the entire infrastructure. Using the Observability Integration feature in NetScaler Console, you can:

- Integrate NetScaler Console with Splunk.
- Integrate NetScaler Console with New Relic.
- Integrate NetScaler Console with Microsoft Sentinel

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Configure NetScaler instances for the export of insights to Prometheus using the default schema.

Integration with Splunk

You can now integrate NetScaler Console with Splunk to view analytics for:

- WAF violations
- Bot violations
- SSL Certificate Insights
- Gateway Insights
- NetScaler® Console Audit Logs

Splunk add-on enables you to:

- Combine all other external data sources.
- Provide greater visibility of analytics in a centralized place.

NetScaler Console collects Bot, WAF, SSL, Gateway, audit logs events, and sends to Splunk periodically. The Splunk Common Information Model (CIM) add-on converts the events to CIM compatible data. As an administrator, using the CIM compatible data, you can view the events in the Splunk dashboard.

For a successful integration, you must:

- Configure Splunk to receive data from NetScaler Console
- Configure NetScaler Console to export data to Splunk
- View dashboards in Splunk

Configure Splunk to receive data from NetScaler Console

In Splunk, you must:

1. Setup the Splunk HTTP event collector endpoint and generate a token
2. Install the Splunk Common Information Model (CIM) add-on
3. Install the CIM normalizer (applicable only for WAF and bot insights)
4. Prepare a sample dashboard in Splunk

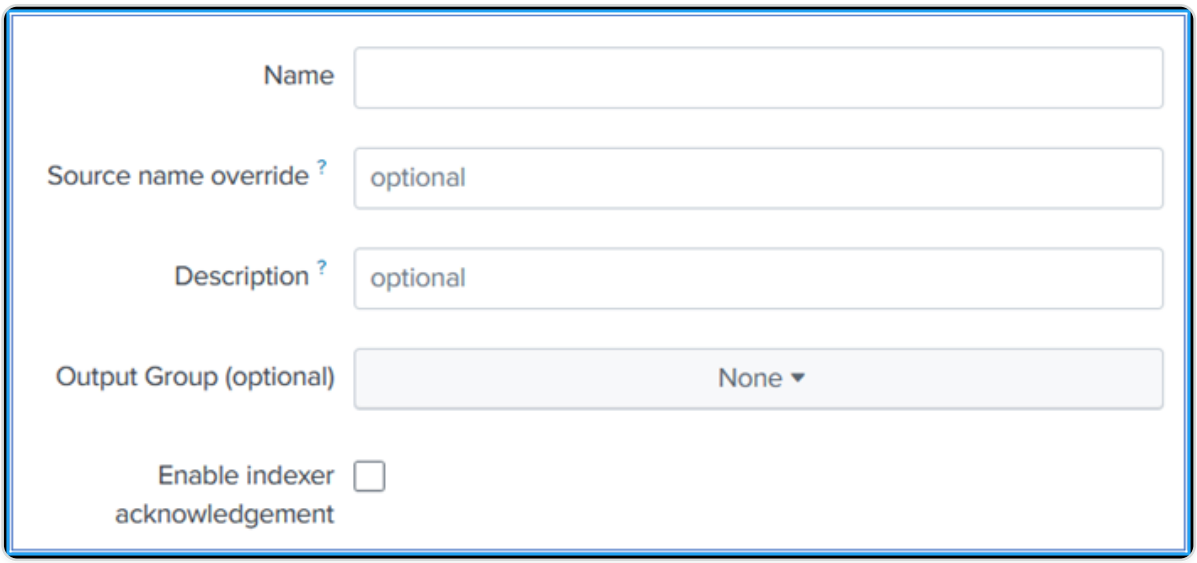
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Setup the Splunk HTTP event collector endpoint and generate a token

You must first setup the HTTP event collector in Splunk. This setup enables the integration between the NetScaler Console and Splunk to send the WAF or Bot data. Next, you must generate a token in Splunk to:

- Enable authentication between NetScaler Console and Splunk.
- Receive data through the event collector endpoint.

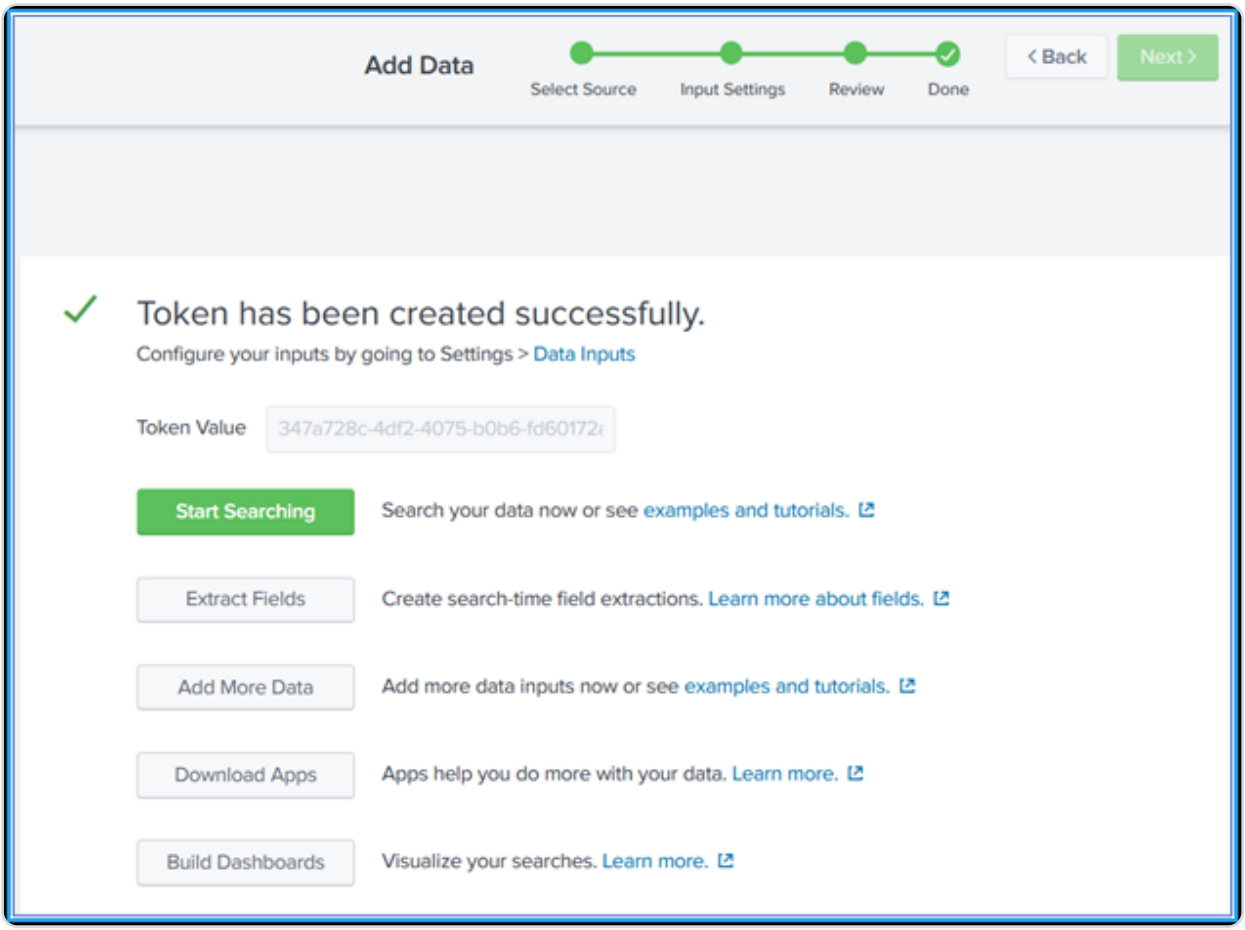
1. Log on to Splunk.
2. Navigate to **Settings > Data Inputs > HTTP event collector** and click **Add new**.
3. Specify the following parameters:
    a. **Name**: Specify a name of your choice.
    b. **Source name override (optional)**: If you set a value, it overrides the source value for HTTP event collector.
    c. **Description (optional)**: Specify a description.
    d. **Output Group (optional)**: By default, this option is selected as None.
    e. **Enable indexer acknowledgement**: NetScaler Console does not support this option. We recommend not to select this option.



4. Click **Next**.
5. Optionally, you can set additional input parameters in the **Input Settings** page.
6. Click **Review** to verify the entries and then click **Submit**.

    A token gets generated. You must use this token when you add details in NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Install the Splunk Common Information Model

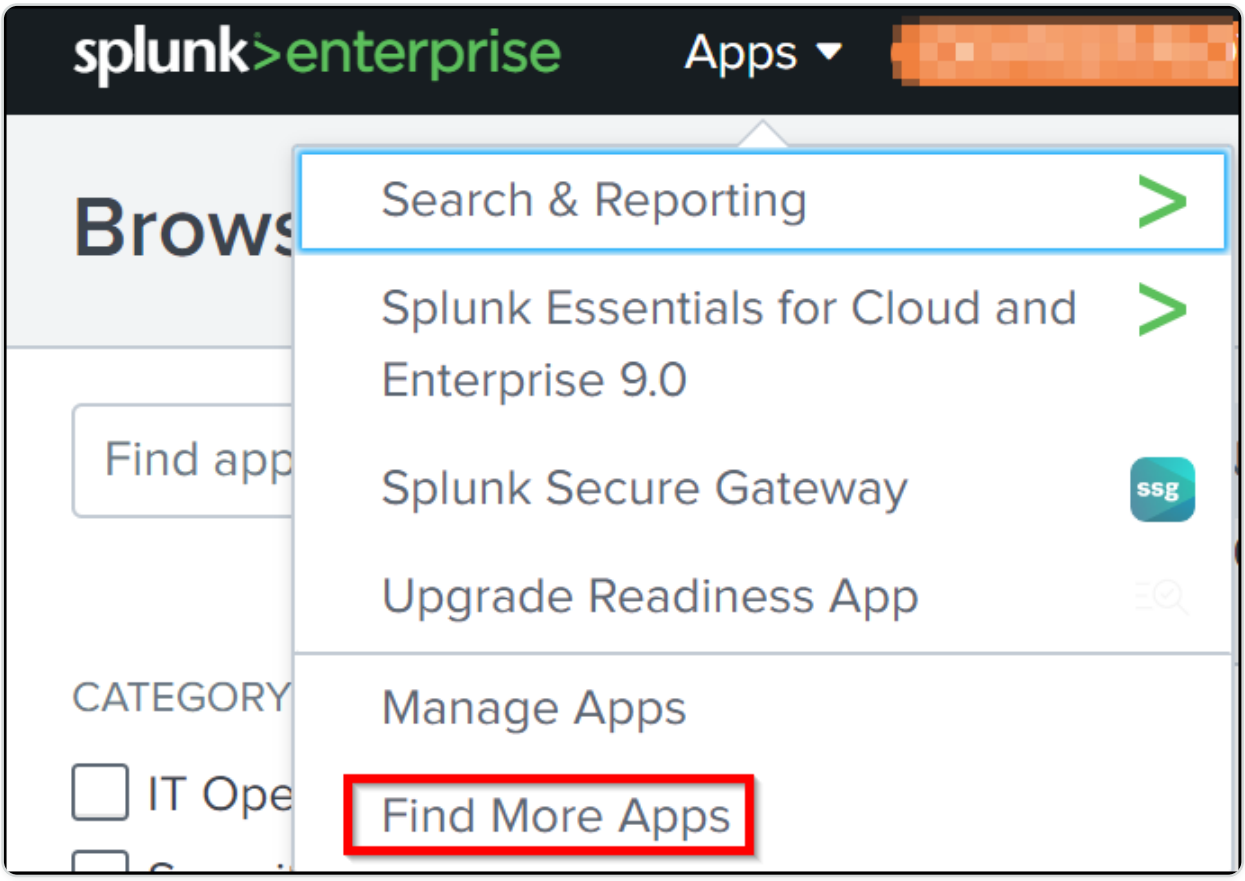
In Splunk, you must install the Splunk CIM add-on. This add-on ensures that the data received from NetScaler Console to normalize the ingested data and match a common standard using the same field names and event tags for equivalent events.

NOTE:

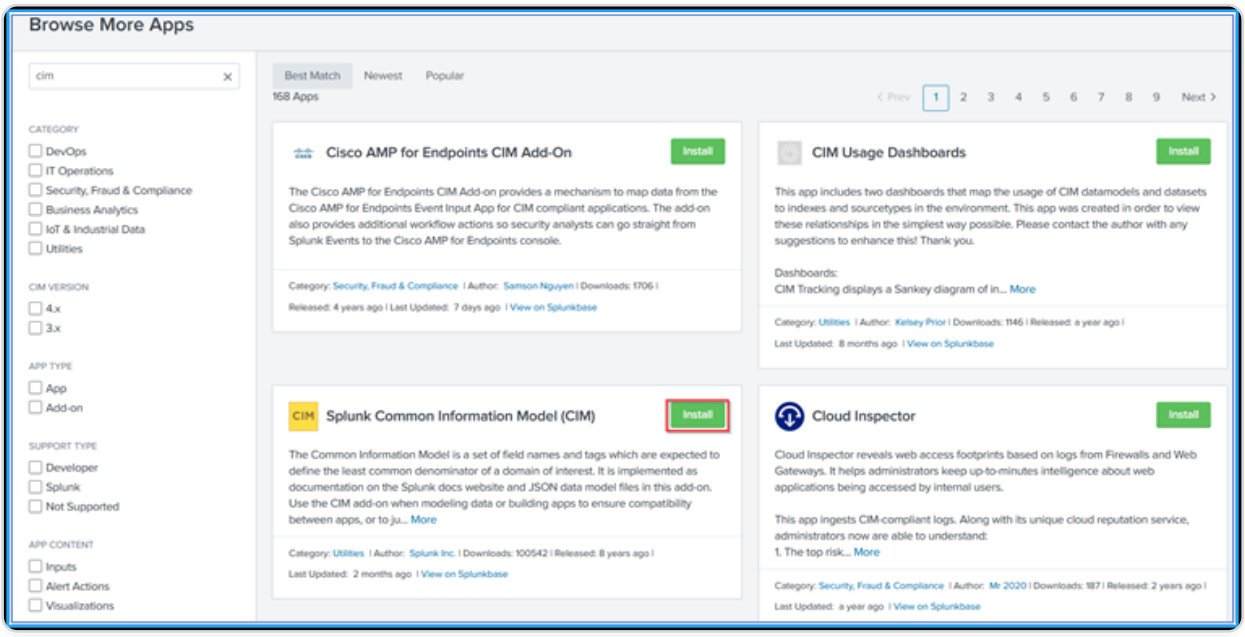
You can ignore this step if you have already installed the Splunk CIM add-on.

1. Log on to Splunk.
2. Navigate to **Apps > Find More Apps**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Type **CIM** in the search bar and press **Enter** to get the **Splunk Common Information Model (CIM)** add-on, and click **Install**.

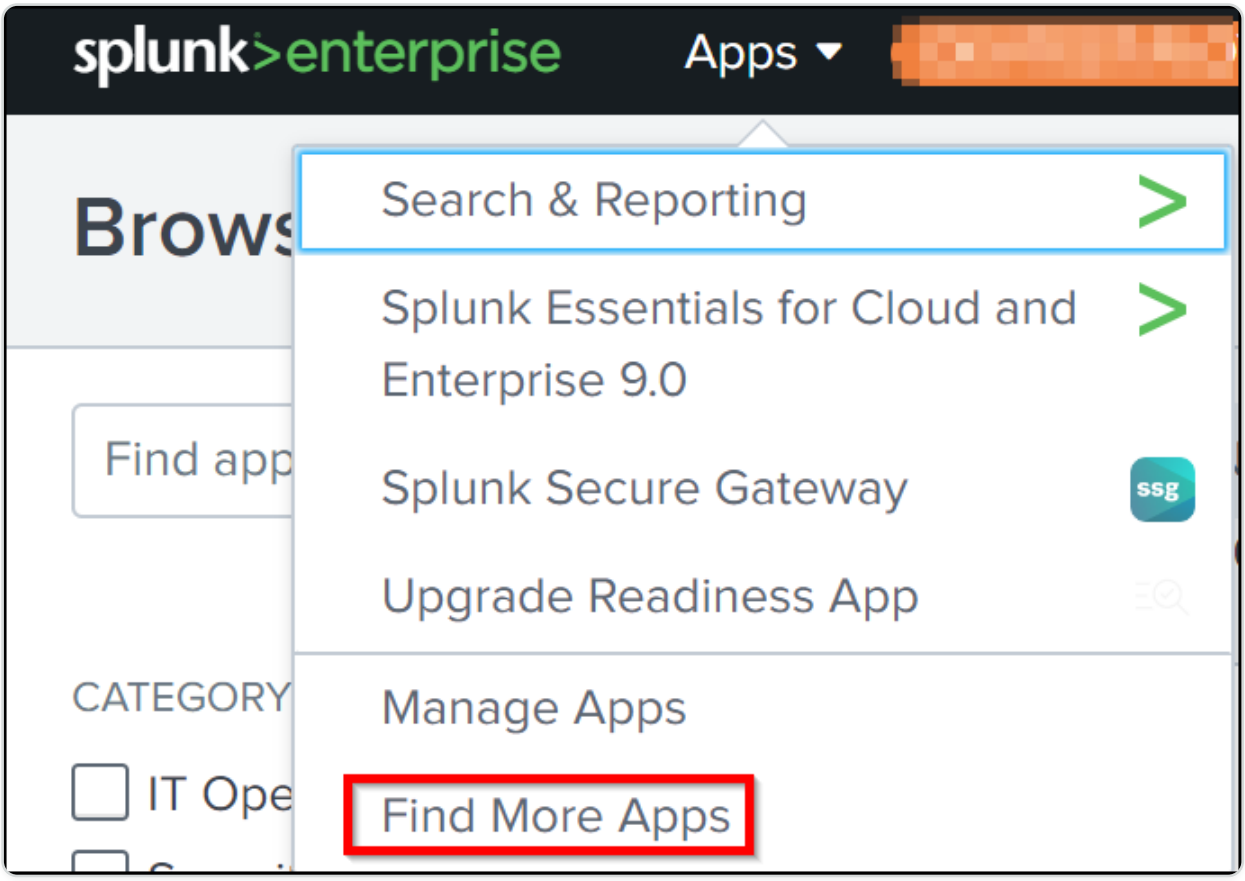


Install the CIM normalizer

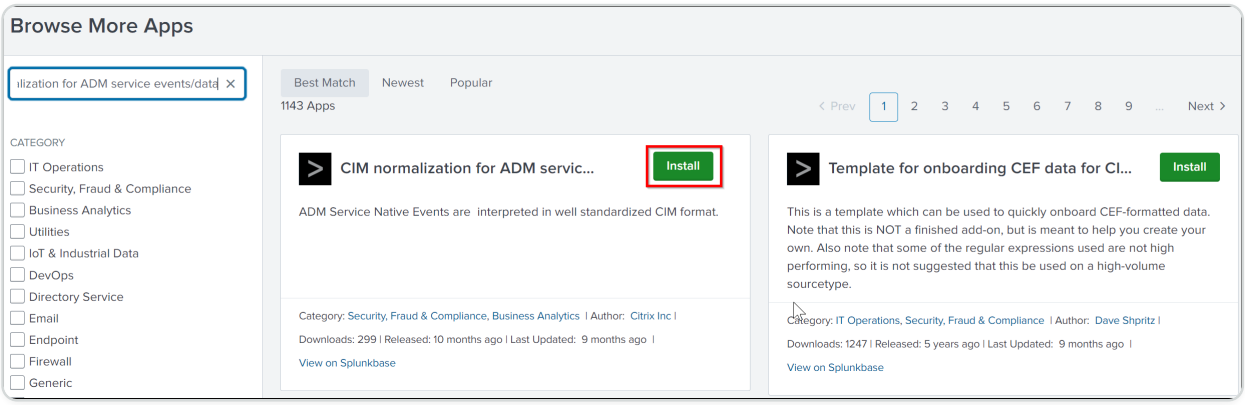
The CIM normalizer is an additional plug-in that you must install to view the WAF and bot insights in Splunk.

1. In the Splunk portal, navigate to **Apps > Find More Apps**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Type **CIM normalization for ADM service events/data** in the search bar and press **Enter** to get the add-on, and click **Install**.



Prepare a sample dashboard in Splunk

After you install the Splunk CIM, you must prepare a sample dashboard using a template for WAF and Bot, and SSL Certificate Insights. You can download the dashboard template (`.tgz`) file, use any editor (for example, notepad) to copy its contents, and create a dashboard by pasting the data in Splunk.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE:

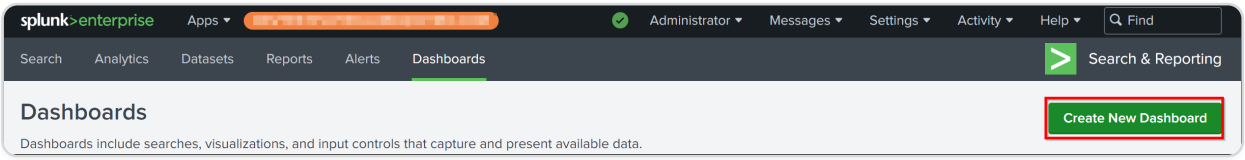
The following procedure to create a sample dashboard is applicable for both WAF and Bot, and SSL Certificate Insights. You must use the required `json` file.

1. Log on to the Citrix downloads page and download the sample dashboard available under Observability Integration.
2. Extract the file, open the `json` file using any editor, and copy the data from the file.

   NOTE:

   After you extract, you get two `json` files. Use `adm_splunk_security_violations.json` to create the WAF and Bot sample dashboard, and use `adm_splunk_ssl_certificate.json` to create the SSL certificate insight sample dashboard.

3. In the Splunk portal, navigate to **Search & Reporting > Dashboards** and then click **Create New Dashboard**.



4. In the **Create New Dashboard** page, specify the following parameters:

   a. **Dashboard Title** - Provide a title of your choice.

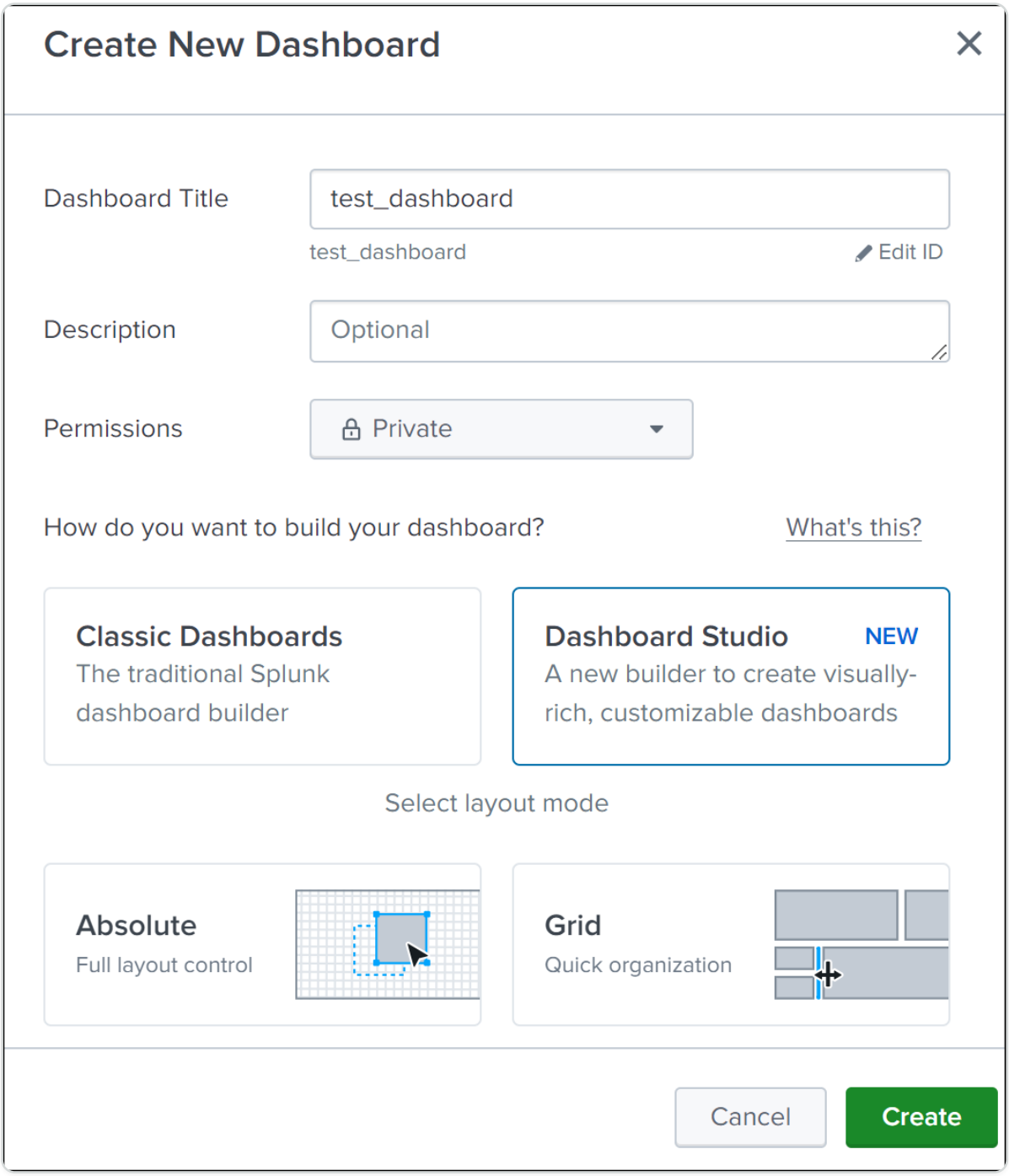
   b. **Description** - Optionally, you can provide a description for your reference.

   c. **Permission** - Select **Private** or **Shared in App** based on your requirement.

   d. Select **Dashboard Studio**.

   e. Select any one layout (**Absolute** or **Grid**), and then click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



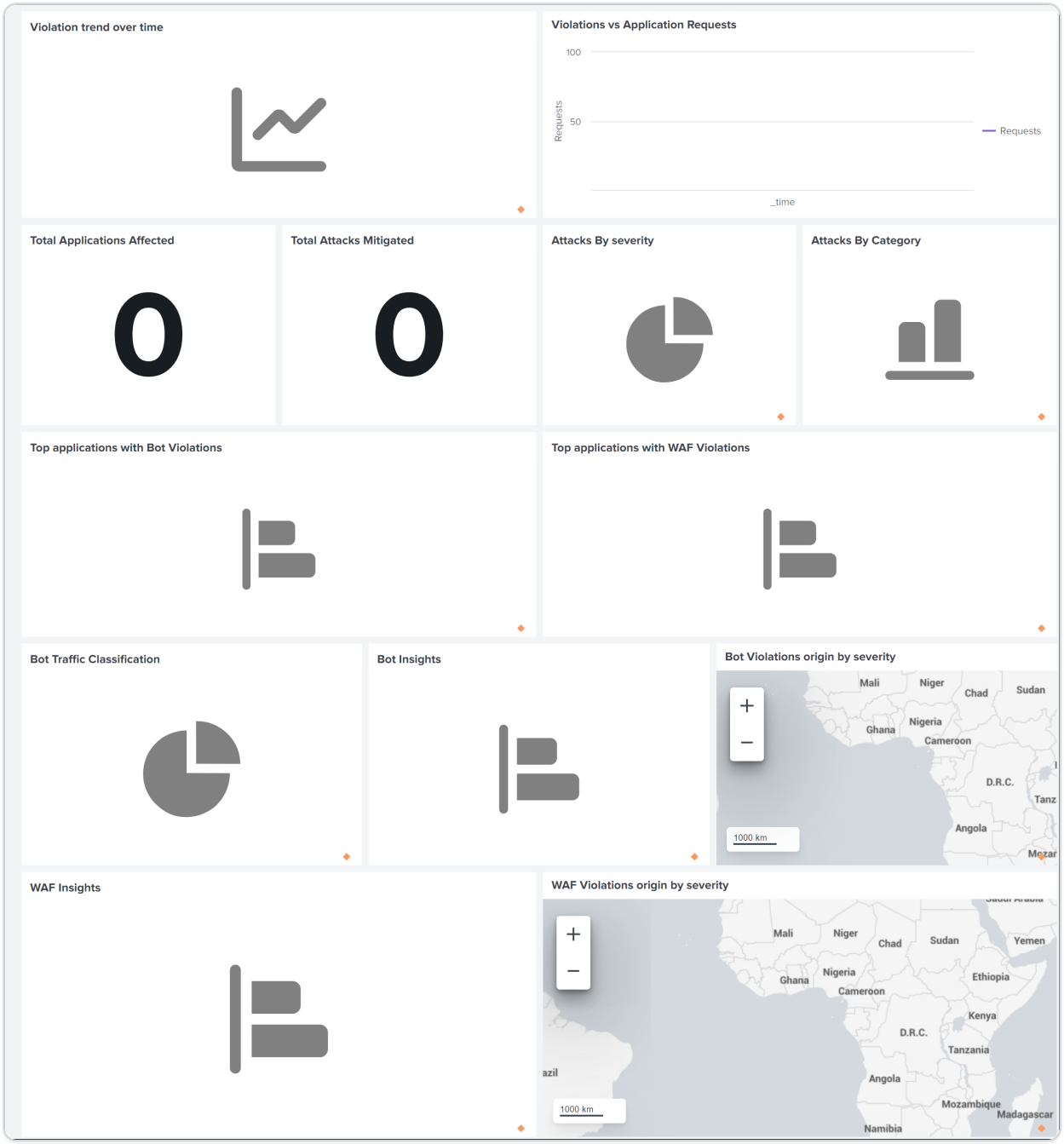
After you click **Create**, select the **Source** icon from the layout.



5. Delete the existing data, paste the data that you copied in step 2, and click **Back**.
6. Click **Save**.

   You can view the following sample dashboard in your Splunk.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Configure NetScaler Console to export data to Splunk

You now have everything ready in Splunk. The final step is to configure NetScaler Console by creating a subscription and adding the token.

Upon completion of the following procedure, you can view the updated dashboard in Splunk that is currently available in your NetScaler Console:

1. Log on to NetScaler Console.
2. Navigate to **Settings > Observability Integration**.
3. In the **Integrations** page, click **Add**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. In the **Create Subscription** page, specify the following details:

    a. Specify a name of your choice in the **Subscription Name** field.

    b. Select **NetScaler Console** as the **Source** and click **Next**.

    c. Select **Splunk** and click **Configure**. In the **Configure Endpoint** page:

        i. **End Point URL** – Specify the Splunk end point details. The end point must be in the `<https://SPLUNK_PUBLIC_IP:SPLUNK_HEC_PORT/services/collector/event>` format.

        NOTE:

        It is recommended to use HTTPS for security reasons.

        - **SPLUNK_PUBLIC_IP** – A valid IP address configured for Splunk.
        - **SPLUNK_HEC_PORT** – Denotes the port number that you have specified during the HTTP event endpoint configuration. The default port number is 8088.
        - **Services/collector/event** – Denotes the path for the HEC application.

        ii. **Authentication token** – Copy and paste the authentication token from Splunk.

        iii. Click **Submit**.

    d. Click **Next**.

    e. Click **Add Insights** and in the **Select Feature** tab, you can select the features that you want to export and click **Add Selected**.

    NOTE:

    If you have selected **NetScaler Console Audit Logs**, you can select **Daily** or **Hourly** for the frequency to export audit logs to Splunk.

    f. Click **Next**.

    g. In the **Select Instance** tab, you can either choose **Select All Instances** or **Custom select**, and then click **Next**.

    - **Select All Instances** - Exports data to Splunk from all the NetScaler instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Custom select** - Enables you to select the NetScaler instances from the list. If you select specific instances from the list, then the data is exported to Splunk only from the selected NetScaler instances.

h. Click **Submit**.

> **NOTE:**
>
> The data for the selected insights gets pushed to Splunk immediately after the violations are detected in NetScaler Console.

View dashboards in Splunk

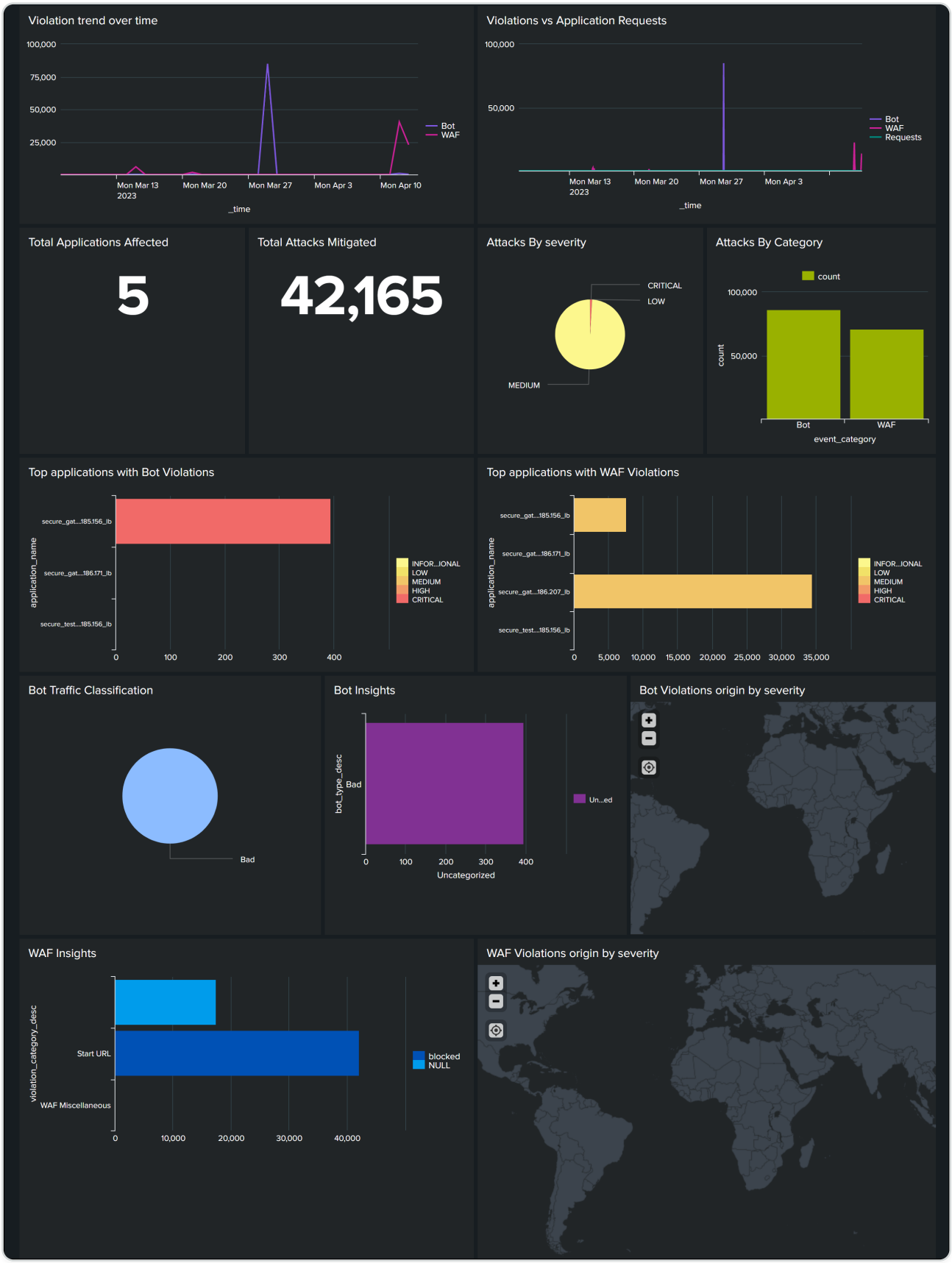
After you complete the configuration in NetScaler Console, the events appear in Splunk.

You are all set to view the updated dashboard in Splunk without any additional steps.

Go to Splunk and click the dashboard that you have created to view the updated dashboard.

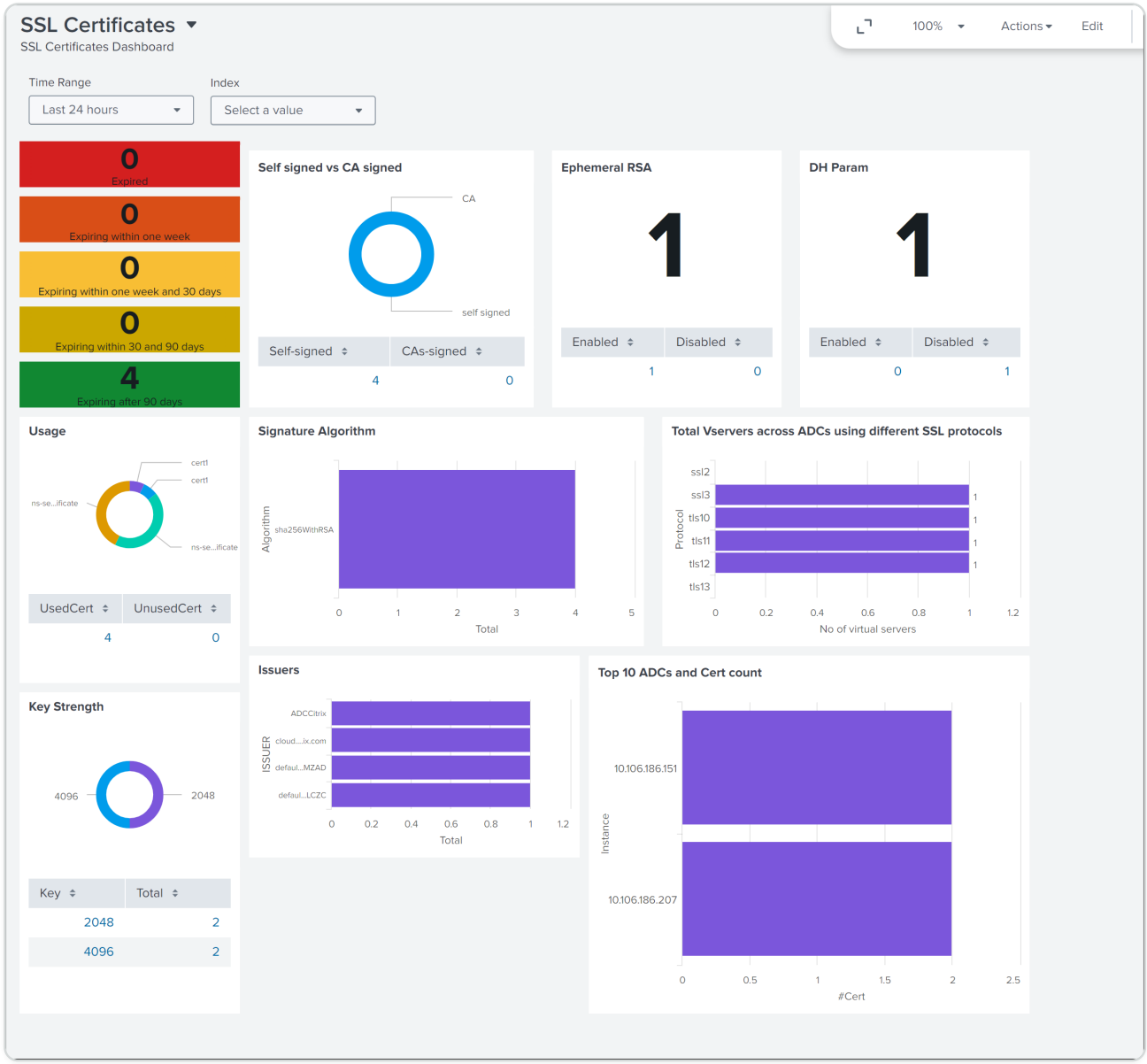
The following is an example for the updated WAF and Bot dashboard:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following dashboard is an example for the updated SSL Certificate Insights dashboard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Apart from the dashboard, you can also view data in Splunk after creating the subscription

1. In Splunk, click **Search & Reporting**.
2. In the search bar:
   - Type `sourcetype="bot"` or `sourcetype="waf"` and select the duration from the list to view bot/WAF data.
   - Type `sourcetype="ssl"` and select the duration from the list to view the SSL certificate insights data.
   - Type `sourcetype="gateway_insights"` and select the duration from the list to view the Gateway insights data.
   - Type `sourcetype= "audit_logs"` and select the duration from the list to view the audit logs data.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Integration with New Relic

You can now integrate NetScaler Console with New Relic to view analytics for WAF, Bot, SSL, Gateway Insights, and NetScaler Console audit logs in your New Relic dashboard. With this integration, you can:

- Combine all other external data sources in your New Relic dashboard.
- Get visibility of analytics in a centralized place.

NetScaler Console collects Bot, WAF, SSL, Gatewat Insights, and NetScaler Console audit logs events, and sends them to New Relic immediately. As an administrator, you can also view these events in your New Relic dashboard.

Prerequisites

For a successful integration, you must:

- Obtain a New Relic event endpoint in the following format:

  `https://insights-collector.newrelic.com/v1/accounts/<account_id>/events`

  For more information on configuring an event endpoint, see New Relic documentation.

  For more information on getting an account ID, see New Relic documentation.
- Obtain a New Relic key. For more information, see New Relic documentation.
- Add the key details in NetScaler Console

Add the key details in NetScaler Console

After you generate a token, you must add details in NetScaler Console to integrate with New Relic.

1. Log on to NetScaler Console.
2. Navigate to **Settings > Observability Integration**.
3. In the **Integrations** page, click **Add**.
4. In the **Create Subscription** page, specify the following details:
   a. Specify a name of your choice in the **Subscription Name** field.
   b. Select **NetScaler® Console** as the **Source** and click **Next**.
   c. Select **New Relic** and click **Configure**. In the **Configure Endpoint** page:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

i. **End Point URL** – Specify the New Relic end point details. The end point must be in the `https://insights-collector.newrelic.com/v1/accounts/<account_id>/events` format.

NOTE:

It is recommended to use HTTPS for security reasons.

d. **Authentication token** – Copy and paste the authentication token from New Relic.

i. Click **Submit**.

e. Click **Next**.

f. Click **Add Insights** and in the **Select Feature** tab, you can select the features that you want to export and click **Add Selected**.

NOTE:

If you have selected **NetScaler Console Audit Logs**, you can select **Daily** or **Hourly** for the frequency to export audit logs to New Relic.

g. Click **Next**.

h. In the **Select Instance** tab, you can either choose **Select All Instances** or **Custom select**, and then click **Next**.

- **Select All Instances** - Exports data to New Relic from all the NetScaler instances.
- **Custom select** - Enables you to select the NetScaler instances from the list. If you select specific instances from the list, then the data is exported to New Relic only from the selected NetScaler instances.

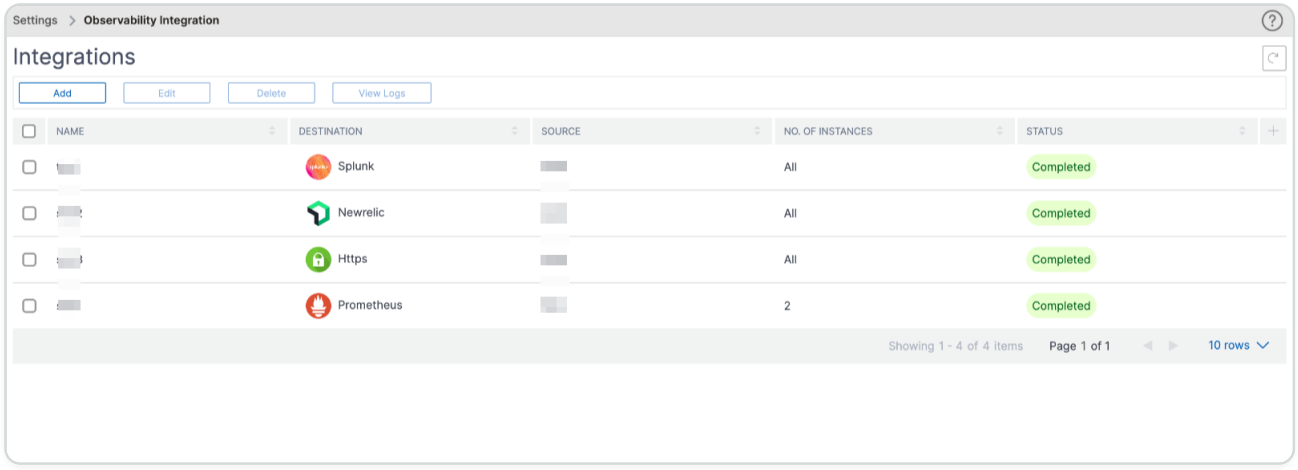
i. Click **Submit**.

NOTE:

- The data for the selected insights gets pushed to New Relic immediately after the violations are detected in NetScaler Console.

The configuration is complete. You can view details in the **Subscriptions** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



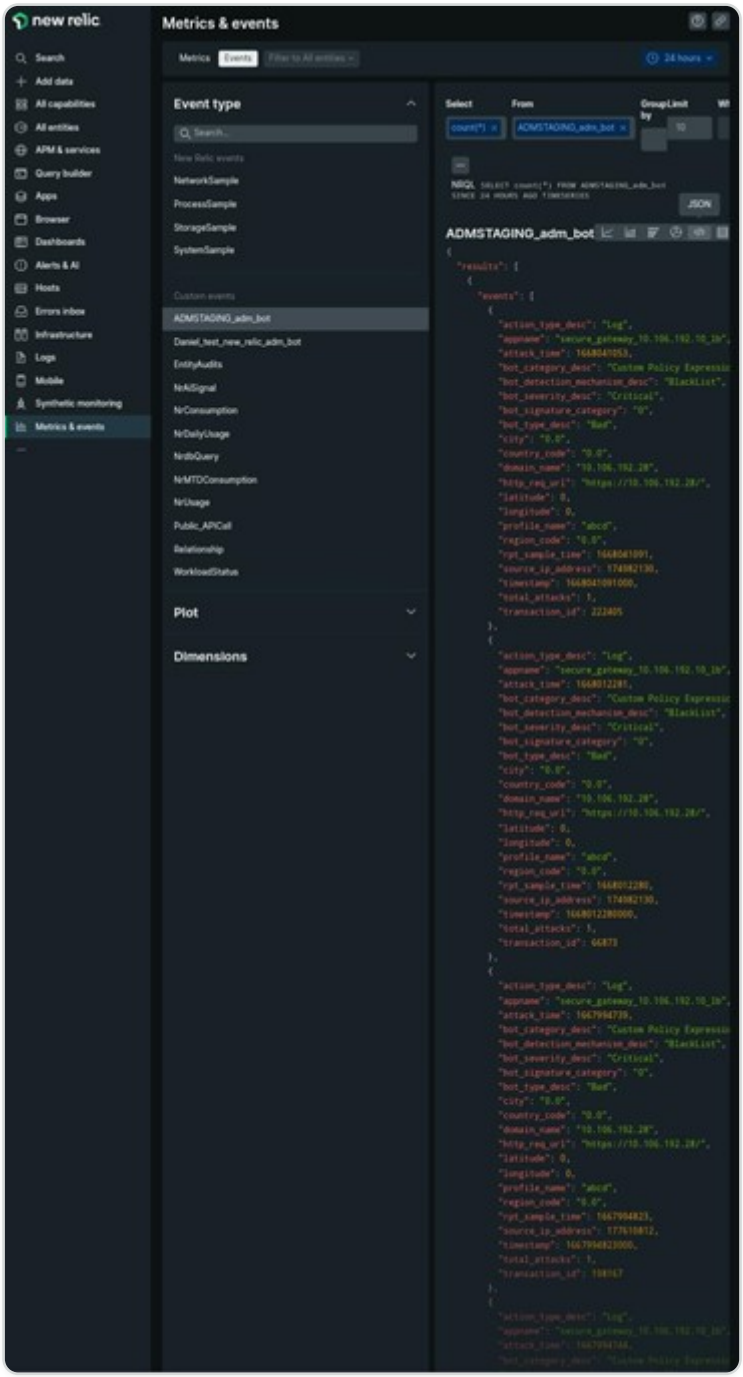
New Relic dashboard

When the events are exported in New Relic, you can view event details under **Metrics & events** in the following JSON format:

`<subsription_name>_adm_<event name>` where event name can be Bot, WAF, and so on.

In the following example, ADMSTAGING is the `<subscription_name>` and bot is the `<event_name>`.

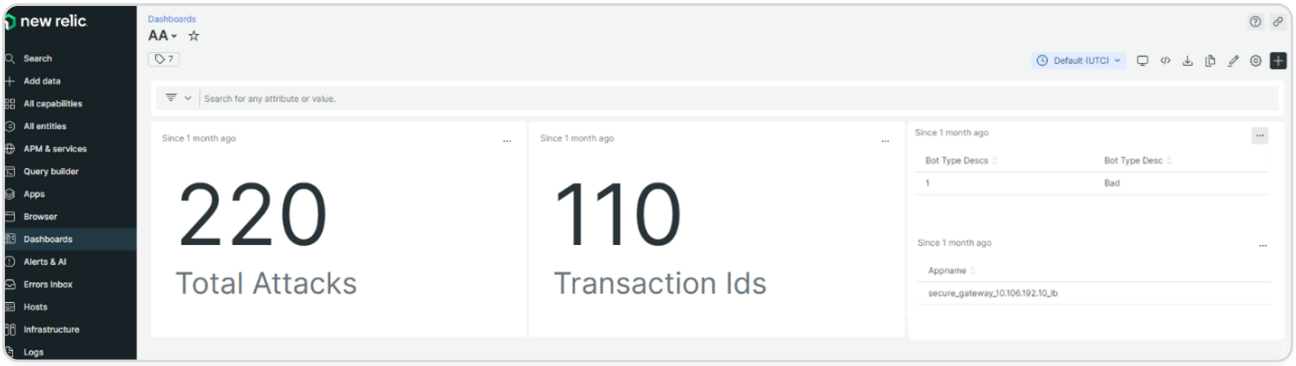
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Once you get the JSON data ingested into your New Relic dashboard, as an administrator, you can use the NRQL (New Relic Query Language) and create a custom dashboard with facets and widgets based on your choice by constructing queries around the ingested data. For more information, see `https://docs.newrelic.com/docs/query-your-data/nrql-new-relic-query-language/get-started/introduction-nrql-new-relics-query-language/`

The following is an example dashboard created using the NRQL:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



To create this dashboard, the following queries are required:

- Widget 1: Total Unique Attacks in events table

  ```
  SELECT count(total_attacks) from <event_name> since 30 days ago
  ```

- Widget 2: Unique Transaction IDs in event table

  ```
  SELECT uniqueCount(transaction_id) from <event_name> since 30 days ago
  ```

- Widget 3: Total Unique Bot Types and their counts

  ```
  SELECT uniqueCount(bot_type_desc), uniques(bot_type_desc) from <event_name> since 30 days ago
  ```

- Widget 4: Total unique App Names seeing Bot Violations

  ```
  SELECT uniques(appname) from <event_name> since 30 days ago
  ```

Integration with Microsoft Sentinel

You can integrate NetScaler Console with Microsoft Sentinel to export the following analytics from NetScaler Console to Microsoft Sentinel:

- WAF violations
- Bot violations
- SSL certificate insights
- Gateway insight
- NetScaler® Console audit logs

Microsoft Sentinel provides centralized data collection that gathers data from various sources such as applications, servers, and so on. As an administrator, you can view data and make decisions after the insights or violations are reported in Microsoft Sentinel.

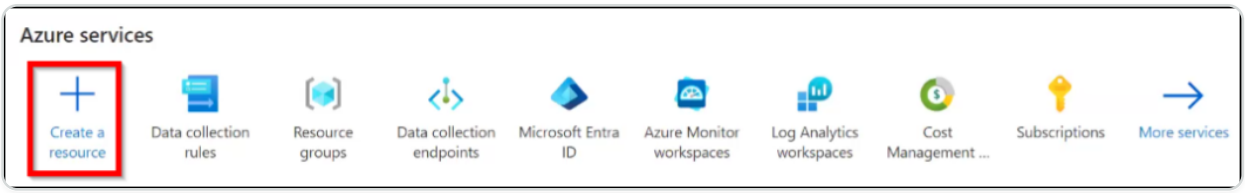
For a successful integration, ensure that you have an active Azure subscription and then follow the procedure under each section:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

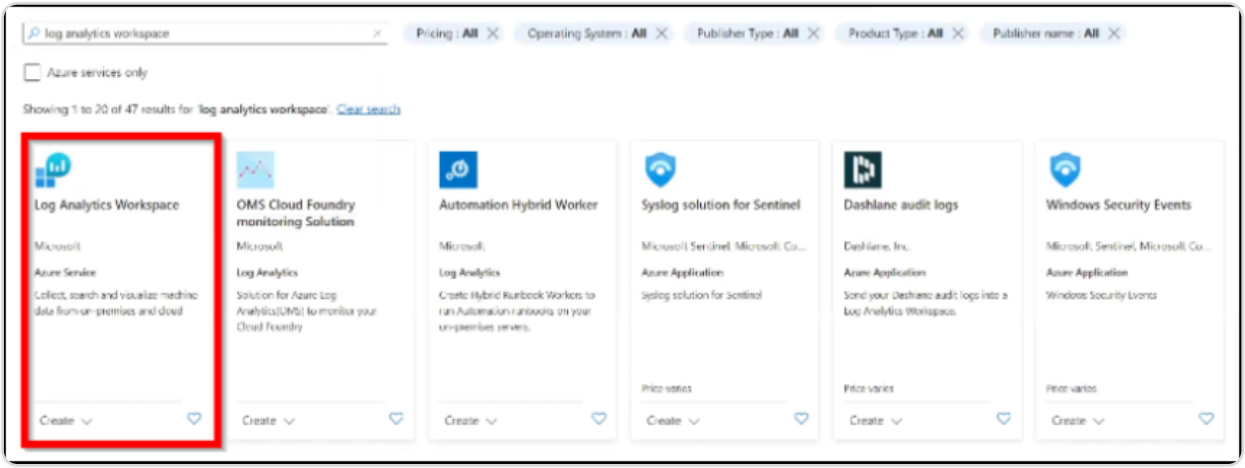
Configure the Log Analytics Workspace

A Log Analytics Workspace is required to store and analyze the collected data.

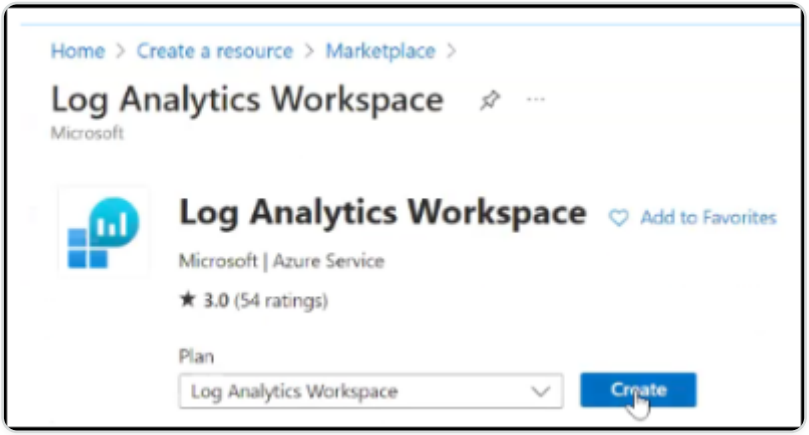
1. Login to Azure.
2. Click **Create a resource**.



3. In the search bar, type log analytics workspace and click **Create** under **Log Analytics Workspace**.



4. In the **Log Analytics Workspace** main page, click **Create**.



5. In the **Create Log Analytics workspace**:
   a. Select the active Subscription and the Resource group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

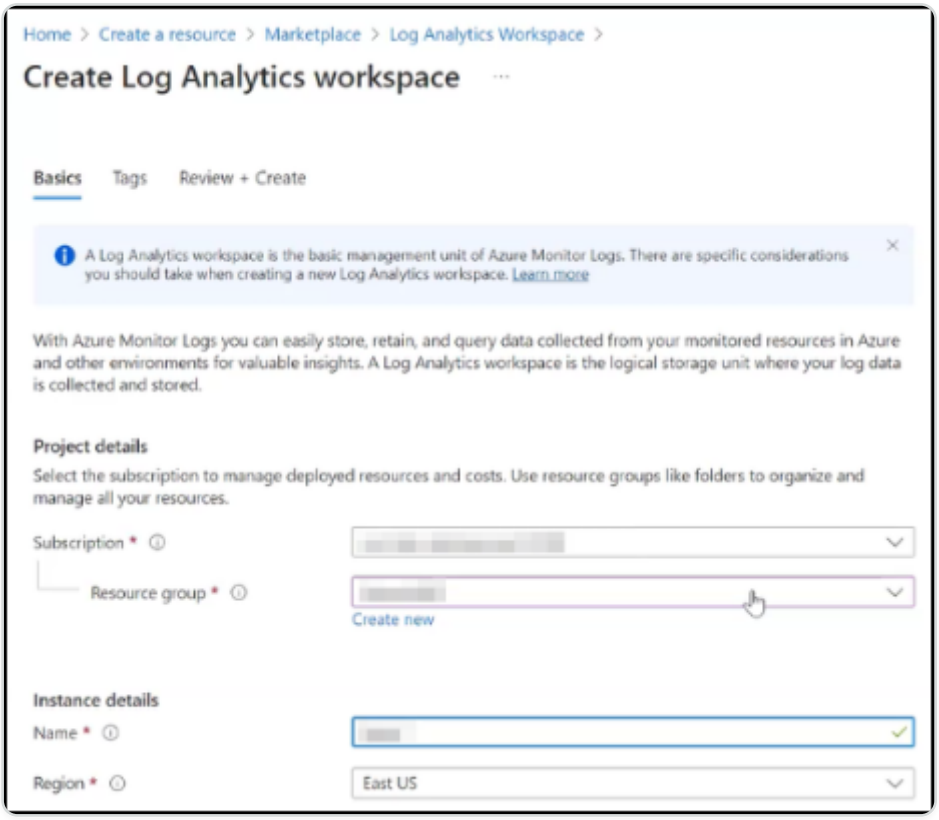
NOTE:

You can also click **Create new** to add a resource group if you have the privilege.

b. Specify a name of your choice.

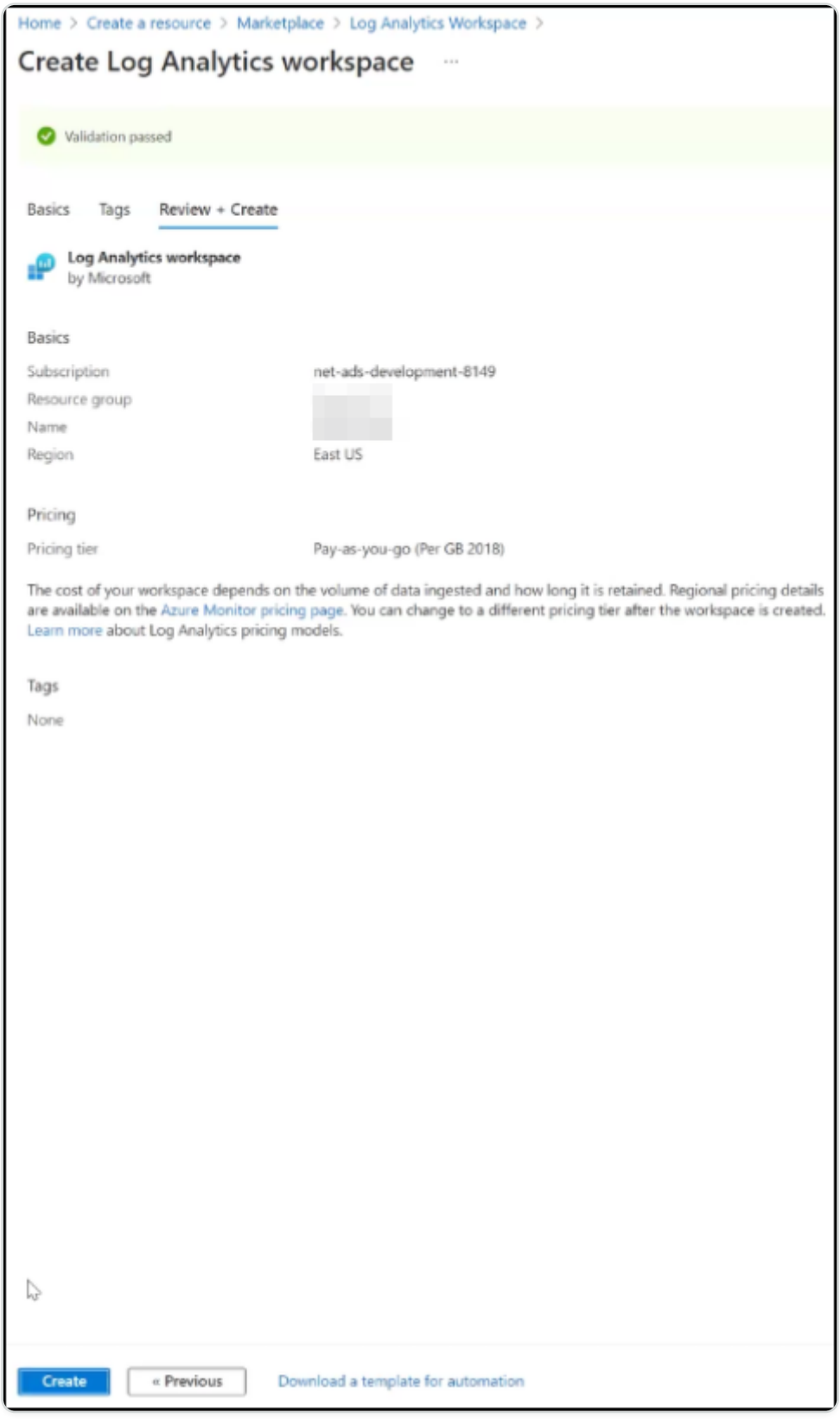
c. Select your region from the list.

d. Click **Review + Create**.



e. A validation passed message appears. Click **Create** to deploy the workspace.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



f. You can see the deployment in progress message. After you see the deployment complete message, click **Go to resource**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

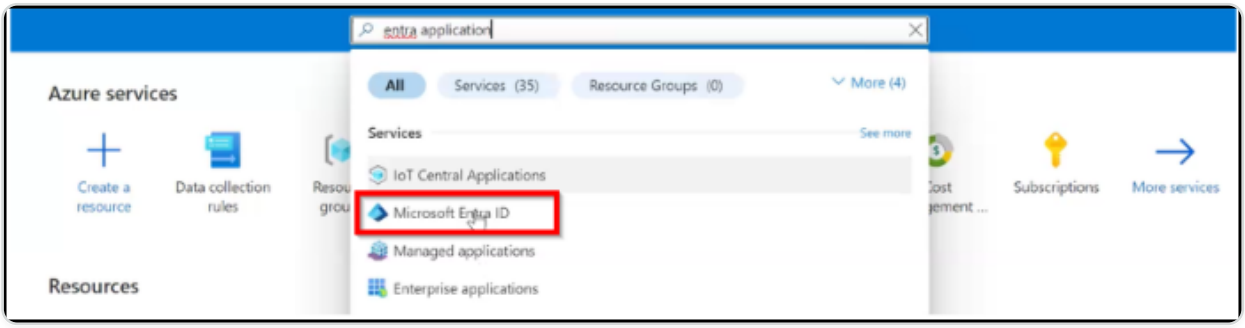


The workspace is successfully created.

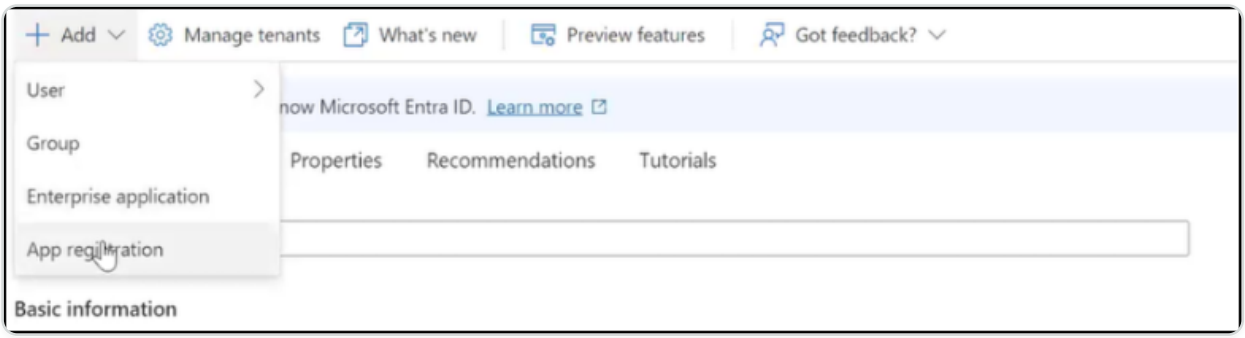
Create a Microsoft Entra application

You must create an Entra application associated with your Azure subscription to communicate on behalf of Log Analytics Workspace. After you create the application, you must also grant permission with **Microsoft Sentinel Contributor** role. The application also provides details such as **Client ID**, **Tenant ID**, and **Client Secret**. We recommend that you make a note of these details. These details are required when you create a subscription in NetScaler Console to complete the integration process.

1. In your Azure portal, type the keyword in the search bar.
2. Click **Microsoft Entra ID**.

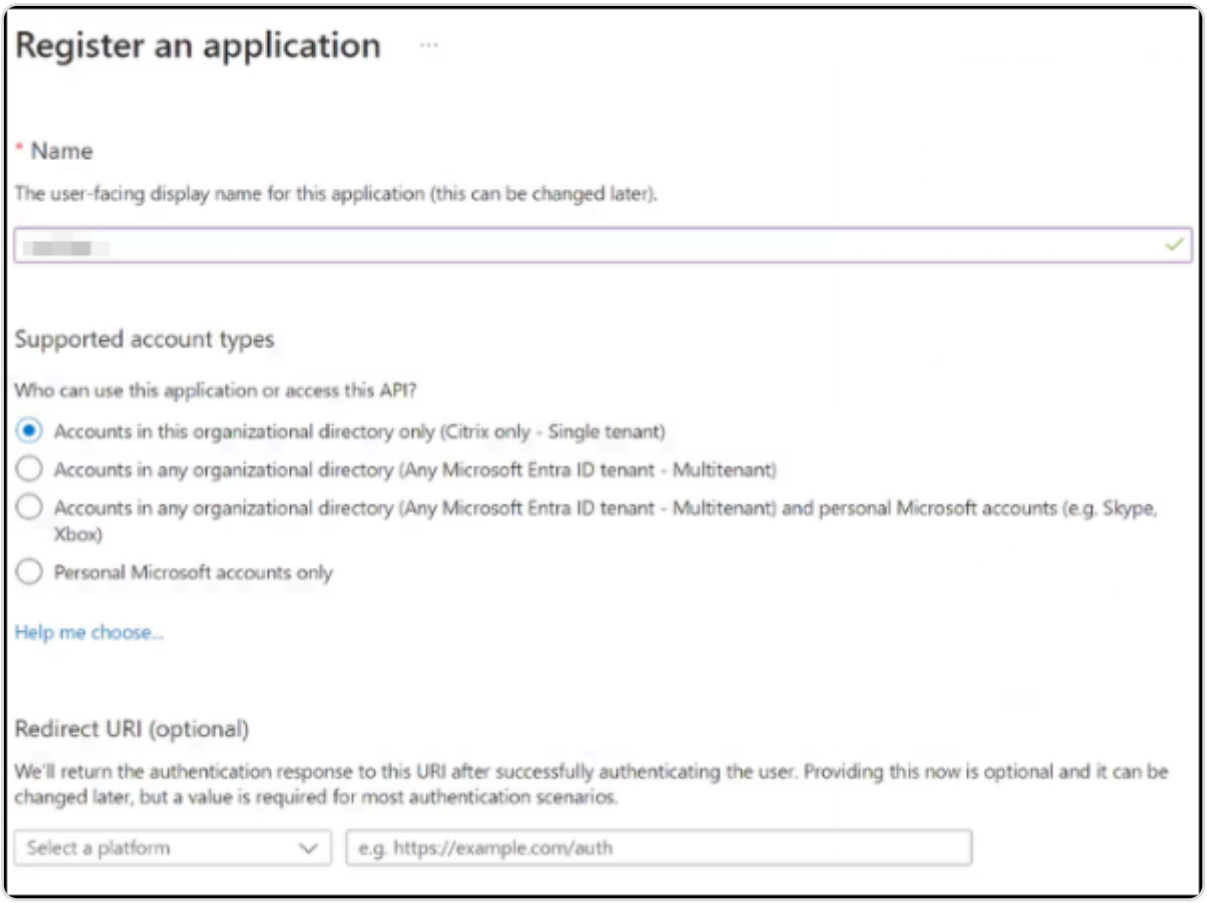


3. Click **Add** and select **App registration**.



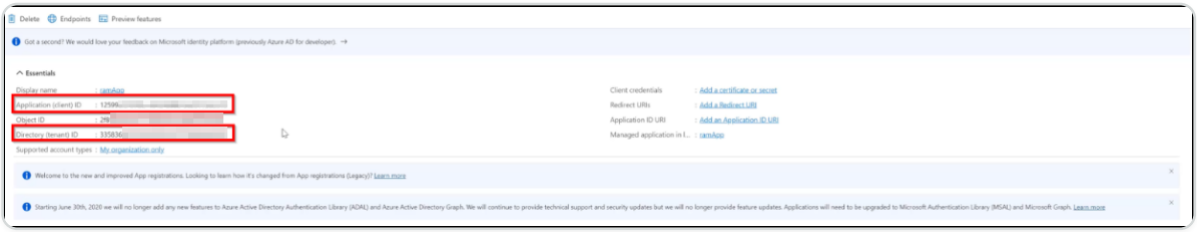
4. Specify a name for the app, select the default option under **Supported account types**, and then click **Register**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

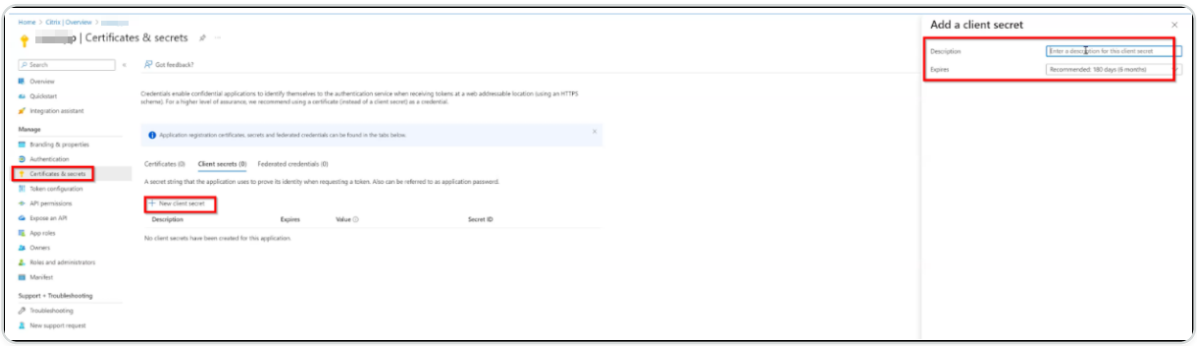


5. After you register the application:

   a. Make a note of **Client ID** and **Tenant ID**.

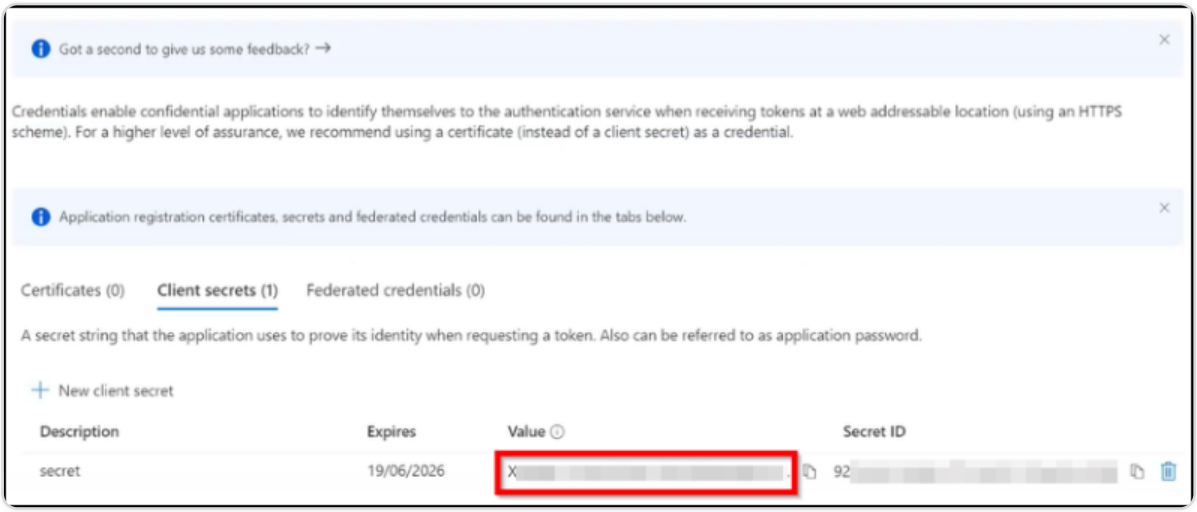


   b. Create a Secret ID for your application. Click **Certificates & secrets** and under **Client secrets**, click **New client secret**. Provide a description, validity, and then click **Add** to create a secret ID for your application.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. The details are displayed for your application. Ensure that you make a note of the ID displayed under **Value** immediately after the secret is created. This value gets hidden if you navigate to any other GUI option.



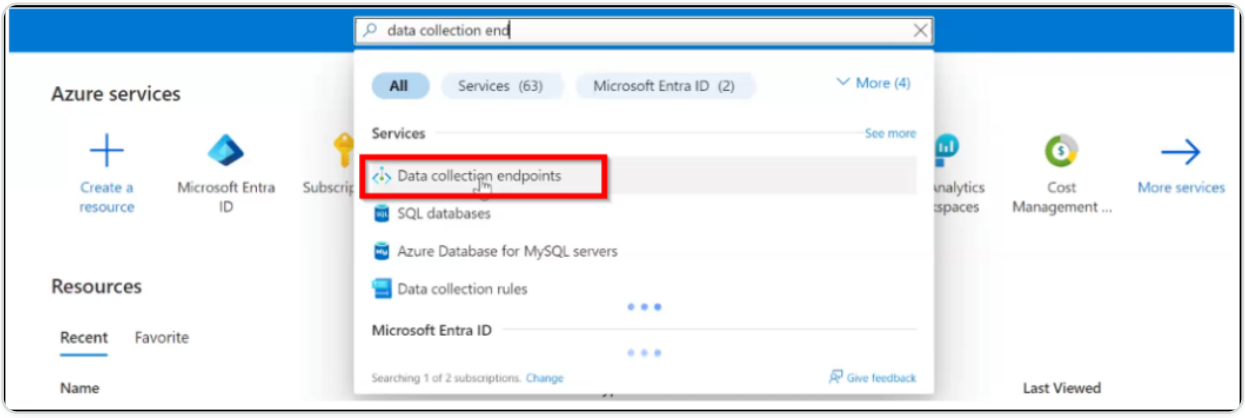
Send data to Microsoft Sentinel by using the Microsoft Entra ID data connector

Microsoft Entra ID logs provide comprehensive information about users, applications, and networks accessing your Entra tenant. For more information, see Send data to Microsoft Sentinel using the Microsoft Entra ID data connector.

Configure data collection endpoint

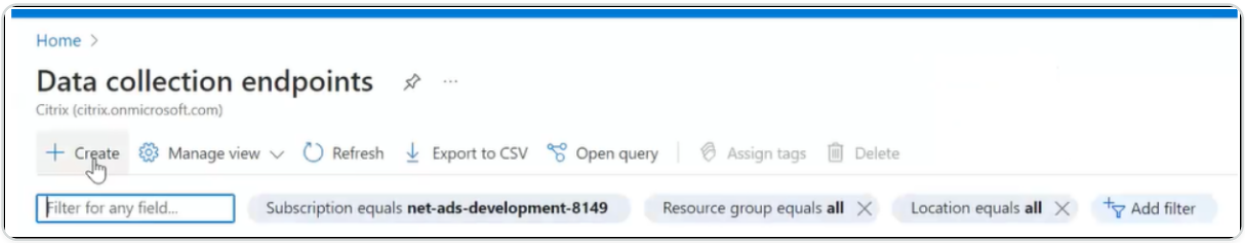
You must create a data collection endpoint to get the endpoint URL. This is required when you create a subscription in NetScaler Console.

1. In your Azure portal, under **Azure services**, select **Data collection endpoints** or type the keyword in the search bar.



2. Click **Create** in the **Data collection endpoints** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. In **Create data collection endpoint**:

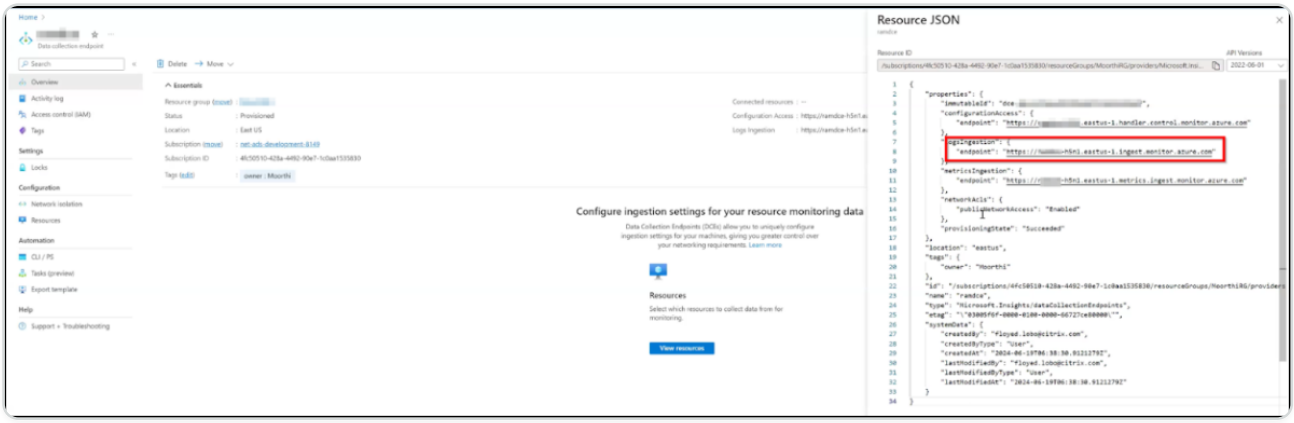
    a. Specify an endpoint name of your choice

    b. Select the **Subscription, Resource Group**, and **Region**.

    c. Click **Review + Create**.

    d. After you see the validation passed message, click **Create**.

You must make a note of the endpoint URL. In the **Data collection endpoint** main page, select the created endpoint, click **JSON view**, and make a note of the endpoint ID.



Create tables to export data

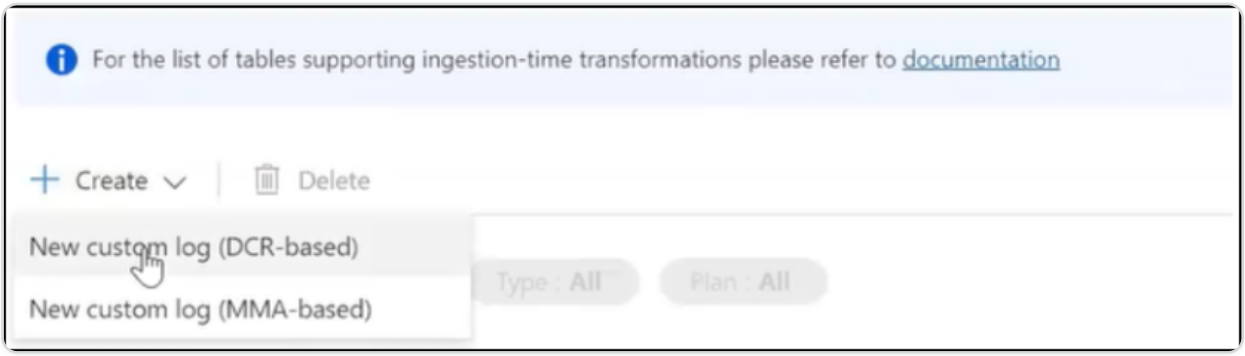
You must create a table and provide the JSON information for each insight that you want to export from NetScaler Console to Microsoft Sentinel. You can refer to the following details on the table requirements for each insight:

INSIGHTS	TOTAL NUMBER OF TABLES REQUIRED
SSL insights	3
WAF	1
Bot	1
Gateway insights	5

© 1997–2026 Citrix Systems, Inc. All rights reserved.

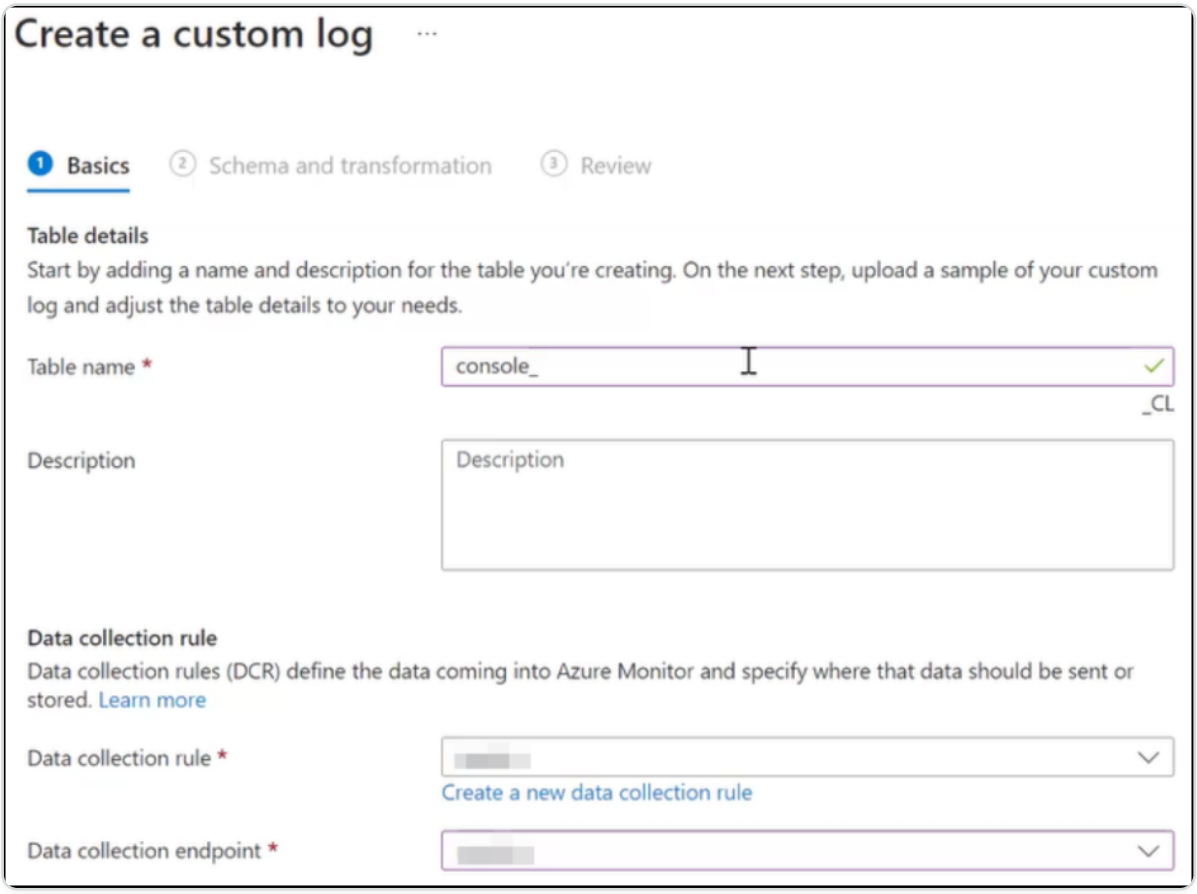
For each workspace, you can create a maximum of 10 tables. Beyond 10 tables, you must create another workspace.

1. Navigate to your workspace in the Azure portal and click **Tables** under **Settings**.
2. Click **Create** and select **New custom log (DCR-based)**



3. In **Create a custom log**:
    a. Specify a table name. The table name must be in the format **console_insightname**. For example: **console_ns_sslvserver**, **console_ns_ssl_certkey**. You can refer to step 4 to get the table names applicable for each insight.
    b. Provide a description to add more information about the table name. This is optional.
    c. Create a new data collection rule and add.
    d. Select the Data collection endpoint from the list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



e. Click **Next**.

4. In the **Schema and transformation** tab, you must upload the JSON sample logs for the insight that you want to export. You can use the following sample JSON for each insight and create a JSON file to upload:

INSIGHTS	JSON	TABLE NAME TO BE USED
SSL (1)	`{"id": "3eb05733-c326-493c-9aa0-f7db3a6b4277", "ns_ip_address": "10.106.186.141", "name": "zeta_192_168_110_250", "vsvr_ip_address": "", "vsvr_port": -1, "vsvr_type": "", "state": "", "partition_name": "", "display_name": "10.106.186.141",`	console_ns_sslvserver

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHTS	JSON	TABLE NAME TO BE USED
	"poll_time": 1716539986, "managed": "f", "ssl2": "f", "ssl3": "t", "tls10": "t", "tls11": "t", "tls12": "t", "dh": "f", "ersa": "t", "sslprofile": "", "tls13": "f", "dhkeyexpsizelimit": "DISABLED", "pushenctriggertimeout": 1, "sessionticket": "", "includesubdomains": "f", "sessionticketkeyrefresh": "", "ssllogprofile": "", "serverauth": "", "ssltriggertimeout": 100, "ersacount": 0, "strictcachecks": "NO", "dhfile": "", "sessreuse": "ENABLED", "redirectportrewrite": "DISABLED", "skipclientcertpolicycheck": "", "tls13sessionticketsperauthcontext": 1, "cipherredirect": "DISABLED", "dropreqwithnohostheader": "NO", "sessionticketlifetime": -1, "maxage": 0, "pushenctrigger": "Always", "strictsigdigestcheck":	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHTS	JSON	TABLE NAME TO BE USED
	"f", "sslredirect": "DISABLED", "sessionkeylifetime": -1, "alpnprotocol": "", "clientauthuseboundcachain": "", "sesstimeout": 120, "clientcert": "", "snihttphostmatch": "CERT", "preload": "NO", "prevsessionkeylifetime": -1, "sessionticketkeydata": "", "encrypttriggerpktcount": 45, "cleartextport": "", "ssliocspcheck": "", "hsts": "f", "sslinterception": "", "commonname": "", "sslireneg": "", "ocspstapling": "DISABLED", "quantumsize": 8192, "insertionencoding": "Unicode", "sslimaxsessperserver": -1, "cipherurl": "", "pushflag": 0, "zerorttearlydata": "DISABLED", "allowextendedmastersecret": "", "dhekeyexchangewithpsk": "NO", "clientauth": "DISABLED", "denysslreneg": "NONSECURE", "sendclosenotify":	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHTS	JSON	TABLE NAME TO BE USED
	"YES", "dhcount": 0, "snienable": "DISABLED", "table_name": "ns_sslvserver"}	
SSL (2)	{"id": "a6673ab2-0b59-47b9-b530-bc30fb2b937c", "ssl_certificate": "/nsconfig/ssl/ca-cert.pem", "ssl_key": "/nsconfig/ssl/ca-key.pem", "certkeypair_name": "athul-ca", "cert_format": "PEM", "days_to_expiry": 281, "ns_ip_address": "10.106.186.141", "status": "Valid", "device_name": "10.106.186.141", "file_location_path": "", "certificate_data": "", "key_data": "", "poll_time": 1717434335, "no_domain_check": "f", "version": 3, "serial_number": "7B34B6A6A1A79E0FF168242D7BCFF78F04C9EE66", "signature_algorithm": "sha256WithRSAEncryption", "issuer": "C=IN,ST=KA,L=BAN,O=CIT,OU=ADM,CN=A", "valid_from": "Mar 12 08:51:11 2024 GMT",	console_ns_ssl_certkey

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHTS	JSON	TABLE NAME TO BE USED
	"valid_to": "Mar 12 08:51:11 2025 GMT", "subject": "C=IN,ST=KA,L=BAN,O=CIT,OU=ADM,CN=A", "public_key_algorithm": "rsaEncryption", "public_key_size": 4096, "no_of_bound_entities": 0, "partition_name": "", "display_name": "10.106.186.141", "hostname": "athulsadc", "key_name": "", "subjaltname": "", "managed_by": "", "certificate_dn": "", "linkcertkeyname": "", "table_name": "ns_ssl_certkey"}	
SSL (3)	{"id": "2baffd1a-7ed6-4035-91e8-ad3a3125bff4", "certkeypair_name": "cert1", "ns_ip_address": "10.106.186.127", "poll_time": 1715671567, "partition_name": "", "display_name": "10.106.186.127", "hostname": "", "entity_name": "secure_gateway", "entity_type": "sslvserver",	console_ns_sslcertkey_binding

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHTS	JSON	TABLE NAME TO BE USED
	"table_name": "ns_sslcertkey_binding" }	
WAF	[{"ip_address": "10.106.185.156", "ctnsappname": "vserver_1", "severity": 2, "violation_type": 19, "violation_type_desc": "Start URL", "block_flags": 1, "transformed_flags": 0, "not_blocked_flags": 0, "country_code": "-NA-", "region_code": "-NA-", "city": "-NA-", "latitude": 200.0, "longitude": 200.0, "signature_category": "", "attack_category": 2, "attack_category_desc": "Broken Authentication and Session Management", "total_attacks": 1, "rpt_sample_time": 1704783773, "source_ip_address": 174766492, "attack_time": 1704783538, "profile_name": "appfw_cs_lb_prof", "session_id": "", "http_req_url": "https://10.106.192.54/csrf_ffc/ffc.html?	console_af_threat_exporter_data_l2

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHTS	JSON	TABLE NAME TO BE USED
	field10=asfasd", "violation_name": "-NA-", "violation_value": "-NA-", "violation_location": 4, "violation_threat_index": 5, "app_threat_index": 5, "http_method": 0, "violation_action": 3, "violation_action_desc": "Blocked", "severity_type": 2, "severity_type_desc": "Medium", "iprep_score": 0, "iprep_category": 0, "counter_value": 0, "appname": "vserver_1_10.106.185.156_lb", "violation_category": 12, "violation_category_desc": "Start URL", "source_ipv6_address": "", "true_client_ip": "\\N", "backend_vserver": "", "backend_appname": "", "transactionId": "0", "table_name": "af_threat_exporter_data_l2"}]	
Bot	{"ip_address": "10.106.186.122", "ctnsappname":	console_af_bot_attack_details_l2

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHTS	JSON	TABLE NAME TO BE USED
	"secure_gateway", "bot_type": "2", "bot_type_desc": "Bad", "action_type": "6", "action_type_desc": "Log", "country_code": "0.0", "region_code": "0.0", "city": "0.0", "bot_severity": "0", "bot_severity_desc": "Critical", "latitude": "0", "longitude": "0", "bot_detection_mechanism": "6", "bot_detection_mechanism_desc": "BlackList", "bot_category": "0", "bot_category_desc": "Uncategorized", "source_ip_address": "174758625", "bot_signature_category": "Custom Policy Expression", "appname": "secure_gateway_10.106.186.122_lb", "backend_vserver": "", "backend_appname": "", "total_attacks": "2", "rpt_sample_time": "1718783216", "table_name": "af_bot_attack_details_l2"}	
Gateway Insight (1)	{"adc_ip_address": "10.106.186.141", "auth_server": "", "client_ip": 174766732, "epa_method_type": 0,	console_af_vpn_error_details

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHTS	JSON	TABLE NAME TO BE USED
	"error_count": 14, "error_details": "Invalid credentials passed", "error_type": 1, "gateway_name": "vpn_vserver_142_6", "req_url": "", "resource": "", "rpt_sample_time": 1713505215, "sso_method_type": 0, "sta_ip": "", "table_name": "af_vpn_error_details", "username": "John"}	
Gateway Insight (2)	{"adc_ip_address": "10.102.71.166", "display_name": "10.102.71.166", "gateway_name": "firsthop", "ip_address": "10.102.71.168", "rpt_sample_time": "1718812158", "state": "Up", "table_name": "ns_vpnvserver"}	console_ns_vpnvserver
Gateway Insight (3)	{"adc_ip_address": "10.106.186.141", "gateway_name": "vpn_vserver_141_7", "rpt_sample_time": 1702011308, "sessions": 1, "table_name": "af_vpn_session_details", "users": 1}	console_af_vpn_session_details

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHTS	JSON	TABLE NAME TO BE USED
Gateway Insight (4)	`{"active_sessions": 59, "active_users": 1, "adc_ip_address": "10.106.186.136", "gateway_name": "vpnathul2", "rpt_sample_time": 1698919848, "table_name": "af_vpn_active_session_1"}`	console_af_vpn_active_session_1
Gateway Insight (5)	`{"adc_ip_address": "10.106.186.136", "entity_type": 3, "gateway_name": "vpnathul2", "hits": 3, "rpt_sample_time": 1698052438, "table_name": "af_vpn_error_reports"}`	console_af_vpn_error_reports
Audit logs	`{"system_gmt_time":1721868291, "source":"X.X.X.X", "severity":"INFO", "module":"DEVICECONFIG", "event_type":"CMD_EXECUTED", "message":"Sample Mesage", "instance_ip":"X.X.X.X", "app_name":""}`	console_syslog_messages

After uploading the JSON, you can view the following details:



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Click **Transformation editor**, enter the following query that is applicable for the appropriate insight, and click **Run** to accept the data starting from the poll time in NetScaler Console.

- **SSL** - `source | extend TimeGenerated = todatetime(poll_time) | project-rename sslvserver_id = id`
- **WAF** and **Bot** - `source | extend TimeGenerated = todatetime(rpt_sample_time)`
- **Gateway Insight** - `source | extend TimeGenerated = todatetime(rpt_sample_time)`



5. Click **Next** and click **Create** to complete.
6. Navigate to **Data collection rules**, click the DCR that you have created.
7. Under **Configuration**, click **Data sources** to view the created table.

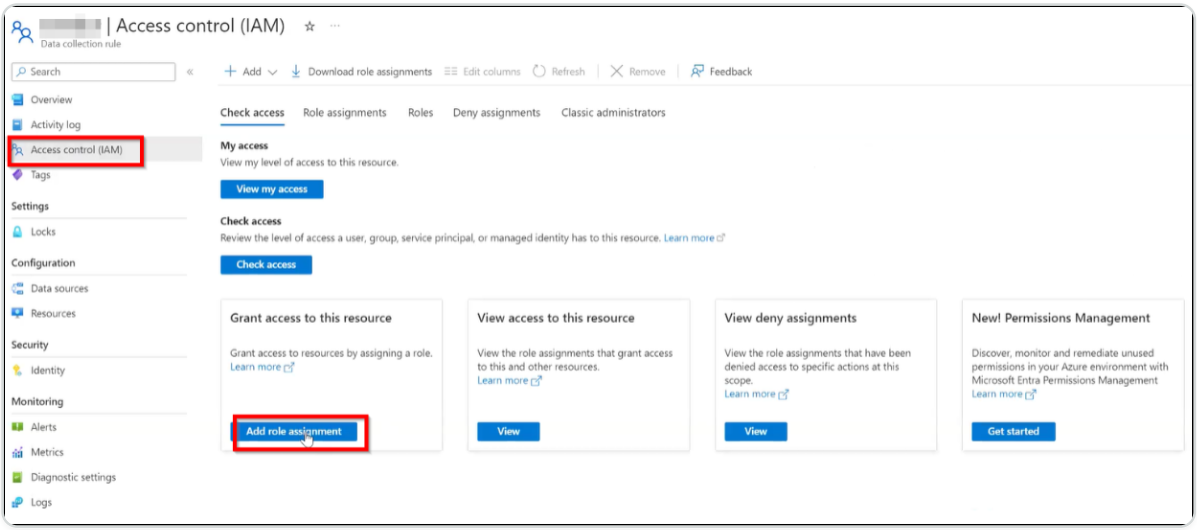


The DCR (Data collection rule) requires access to the **Monitoring Metrics Publisher** role.

a. Navigate to your DCR that you can access from your Azure portal under **Recents**.

b. Click **Access control (IAM)** from your DCR page and click **Add role assignment**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



c. In the search bar, type the keyword monitor to select **Monitoring Metrics Publisher** and click **Next**.

d. In the **Members** tab, click **Select Members** and select the Entra app that you created.

e. Click **Review + assign**.

You must make a note of the Data collection rules ID. Navigate to the Data collection rules page, select your DCR, and click the JSON view to make a note of the ID.



Create a subscription in NetScaler Console

You now have everything ready. The final step is to configure NetScaler Console by creating a subscription and adding the required details. To create a subscription in NetScaler Console, you need the following details that you have noted:

- Endpoint URL
- Data collection rules ID

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Tenant ID
- Client ID
- Client secret

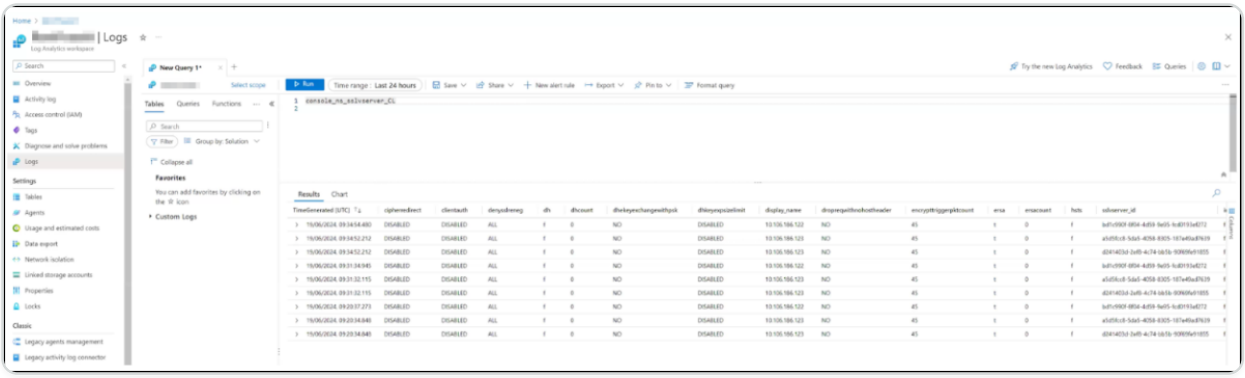
1. Login to NetScaler Console.
2. Navigate to **Settings > Observability Integration**.
3. In the **Integrations** page, click **Add**.
4. In the **Create Subscription** page, specify the following details:
    a. Specify a name of your choice in the Subscription Name field.
    b. Select **NetScaler Console** as the **Source** and click **Next**.
    c. Select **Microsoft Sentinel** and click **Configure**. In the **Configure Endpoint** page, enter all details, and click **Submit**.
    d. Click **Next**.
5. Click **Add Insights** and in the **Select Feature** tab, depending upon the tables that you have added in Microsoft Azure, select the features that you want to export and click **Add Selected**, and click **Next**.
6. In the **Select Instance** tab, you can either choose **Select All Instances** or **Custom select**, and then click **Next**.
    - **Select All Instances** - Exports data to Microsoft Sentinel from all the NetScaler instances.
    - **Custom select** - Enables you to select the NetScaler instances from the list. If you select specific instances from the list, then the data is exported to Microsoft Sentinel only from the selected NetScaler instances.
7. Click **Submit**.

View logs in Microsoft Azure

After you configure everything, we recommend that you wait until 30 minutes to view details in Microsoft Azure.

1. In your Azure portal, navigate to your **Log Analytics Workspace**.
2. Click **Logs**, provide the table name, and click **Run** to view results.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Configure NetScaler® instances for the export of insights to Prometheus using the default schema

NetScaler supports directly exporting metrics to Prometheus. You can use the rich set of metrics provided by NetScaler instance to monitor NetScaler health and application health. For example, you can gather metrics on CPU and memory usage to know the NetScaler health. Similarly, you can use metrics like the number of HTTP requests received per second or the number of active clients to monitor application health.

To export the metrics to Prometheus, you must configure an analytics profile with type as time series. For more information, see Monitor NetScaler, applications, and application security using Prometheus.

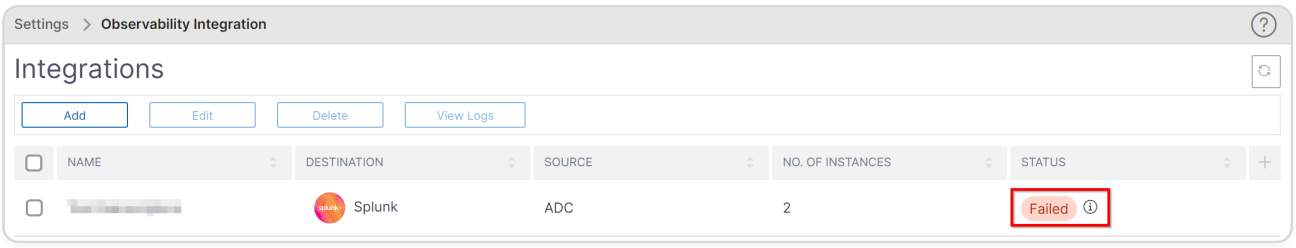
With the Observability Integration feature in NetScaler Console, you can configure the export of insights to Prometheus using the default schema.

1. Navigate to **Settings > Observability Integration**.
2. In the **Integrations** page, click **Add**.
3. In the **Create Subscription** page, specify the following details:
    a. Specify a name of your choice in the **Subscription Name** field.
    b. Select **NetScaler** as the **Source** and click **Next**.
    c. Select **Prometheus** as the Destination.
    d. Select **Default** for the default insights to the exported.
    e. Click **Add Instances** and select the instances for which you want to export insights to Prometheus.
    f. Click **Submit**.

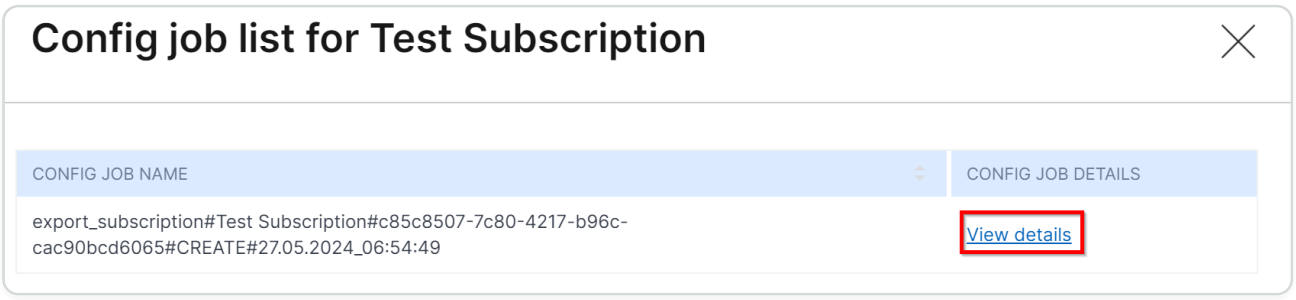
© 1997–2026 Citrix Systems, Inc. All rights reserved.

View logs for failed configurations

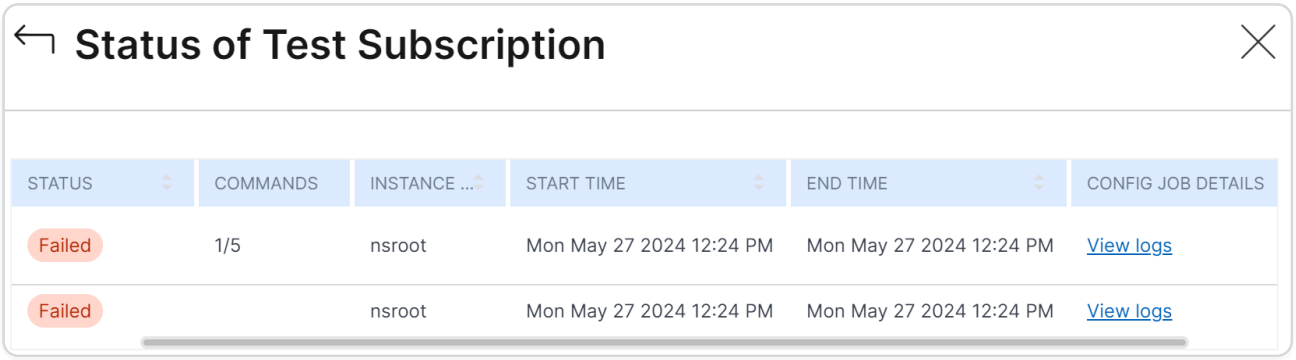
After you create a subscription, you can view the status of the created subscription at **Settings > Observability Integration**. If the status shows **Failed**, click to view details.



Click **View details** under **Config job details**.



Click **View logs** to view details of the issue.



Configure the export of NetScaler® metrics and audit logs to Splunk

NetScaler supports direct export of metrics to Splunk in the JSON format. NetScaler provides rich metrics to monitor your application health and application security health. By exporting the metrics provided by NetScaler to Splunk, you can visualize the metrics and get meaningful insights.

Audit logging enables you to log the NetScaler states and status information collected by various modules in NetScaler. By reviewing the logs, you can troubleshoot problems or errors and fix them.

For more information, see:

- Export audit logs directly from NetScaler to Splunk
- Export metrics directly from NetScaler to Splunk

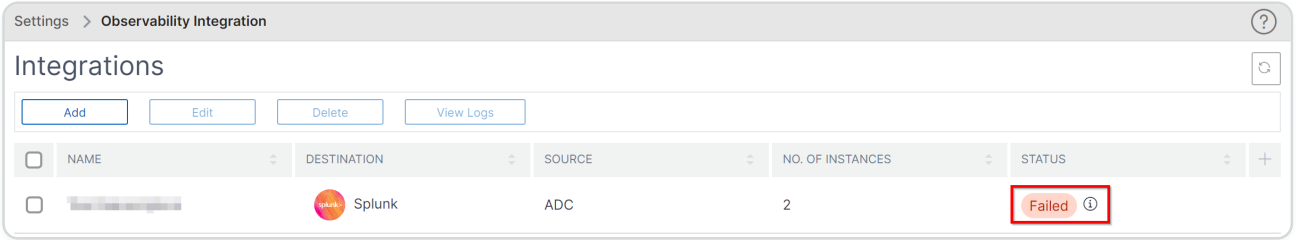
© 1997–2026 Citrix Systems, Inc. All rights reserved.

To configure the export of metrics and audit logs to Splunk through NetScaler Console:

1. Navigate to **Settings > Observability Integration**.
2. In the **Integrations** page, click **Add**.
3. In the **Create Subscription** page, specify the following details:
    a. Specify a name of your choice in the **Subscription Name** field.
    b. Select **NetScaler** as the **Source** and click **Next**.
    c. Select **Splunk** as the **Destination** and click **Configure**. In Configure Endpoint:
        - **Endpoint URL** - Specify the Splunk endpoint details. The end point must be in the `https://SPLUNK_PUBLIC_IP:SPLUNK_HEC_PORT/services/collector/event`` format.
        - **Authentication Token** - Copy and paste the authentication token from Splunk.
        - Click **Submit**.
    d. Click **Next**.
    e. Click **Add Insights** and select **NetScaler Metrics** and **NetScaler Audit Logs**, and then click **Add Selected**.
    f. Click **Next**.
    g. Click **Add Instances** and select the instances.
    h. Click **Submit**.

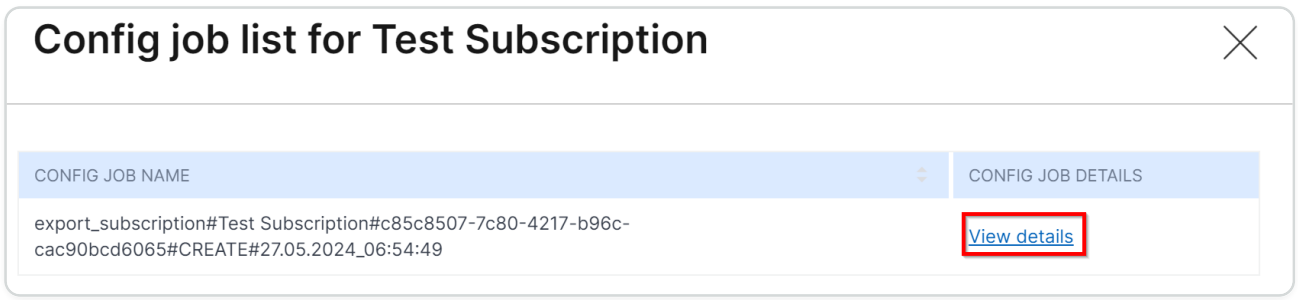
View logs for failed configurations

After you create a subscription, you can view the status of the created subscription at **Settings > Observability Integration**. If the status shows **Failed**, click to view details.

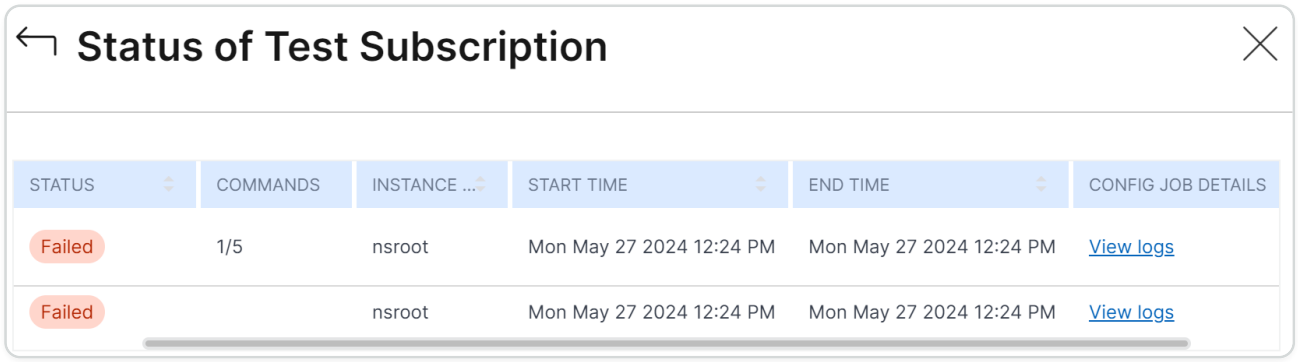


Click **View details** under **Config job details**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Click **View logs** to view details of the issue.



Configuring Analytics settings

Before you start using the Analytics feature on NetScaler Console to gain visibility into your instance and application data, it is recommended that you configure a few analytics settings to ensure optimal experience with this feature.

Creating Thresholds and Alerts for Analytics

You can set thresholds and alerts to monitor the analytics' metrics of the managed virtual servers configured on the discovered instances. When the value of a metric exceeds the threshold, NetScaler Console generates an event to signify a threshold breach.

You can also associate actions with the set thresholds. Actions include displaying an alert on the GUI, sending Email as configured.

For example, you can set a threshold to generate an event for HDX™ insight if any user's ICA RTT value exceeds 1 second. You can also enable alerts for the generated event, and send the threshold breach information to a configured Email list.

To create thresholds and alerts for analytics:

1. Navigate to **Settings** > **Analytics Settings** > **Thresholds**.
2. On the **Thresholds** screen, click **Add** to add a new threshold and configure alerts for the set thresholds.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. On the **Create Thresholds and Alerts** page, specify the following details:

    - **Name** – Name for configuring the threshold.
    - **Traffic Type** – Type of analytics traffic for which you want to configure the threshold. For example: HDX Insight, Security Insight.
    - **Entity** – Category or resource type for which you want to configure the threshold.
    - **Reference Key** – Automatically generated value based on the selected traffic type and entity.
    - **Duration** - Interval for which you want to configure the threshold.

4. To configure email notifications, select the check box for the set thresholds.
5. In the **Rules** section, specify the following:

    - **Metric** – Metric for the selected Traffic type to configure the threshold.
    - **Comparator** – Comparator to the selected metric (for example: \<, \>=).
    - **Value** – Value for the metric to set the threshold, and invoke alerts.

6. Click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create Threshold

Name*

test

Traffic Type*

HDX

Entity*

Applications

Reference Key

App Name

Duration*

Hour

Configure Rule

For more information about each metric, see documentation.

Add Rule | Delete

	METRIC
☐	Total Session Launch Count > 90000

Notification Settings

☐ Enable Threshold

Configure notifications

You can select a notification type to receive notifications for the following features:

- **Events** – List of events that are generated for NetScaler instances. For more information, see Add event rule actions.
- **Licenses** – List of licenses that are currently active, about to expire, and so on. For more information, see The NetScaler Console license expiry.
- **SSL Certificates** – List of SSL certificates that are added to NetScaler instances. For more information, see The SSL certificate expiry

NetScaler Console supports the following notification types:

- Email
- SMS
- Slack
- PagerDuty
- ServiceNow

For each notification type, the NetScaler Console GUI displays the configured distribution list or profile. The NetScaler Console sends notifications to the selected distribution list or profile.

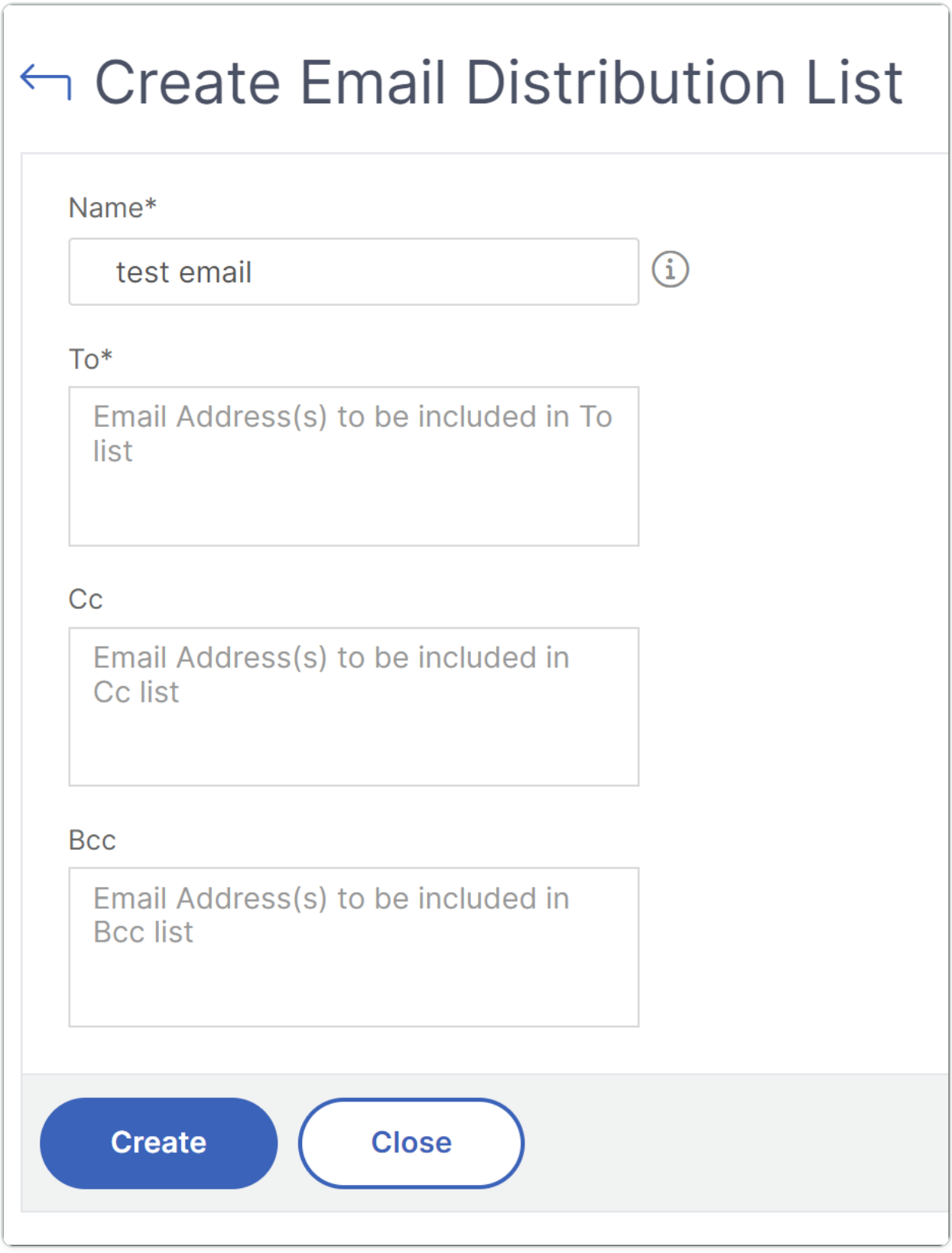
Create an email distribution list

To receive email notifications for NetScaler Console functions, you must add an email server and a distribution list.

Perform the following steps to create an email distribution list:

1. Navigate to **Settings > Notifications**.
2. In **Email**, click **Add**.
3. In **Create Email Distribution List**, specify the following details:
    - **Name** - Specify the distribution list name.
    - **To** - Specify the email addresses to which NetScaler Console has to send messages.
    - **Cc** - Specify the email addresses to which NetScaler Console has to send message copies.
    - **Bcc** - Specify the email addresses to which NetScaler Console has to send message copies without displaying the addresses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Click **Create**.

Repeat this procedure to create multiple email distribution lists. The **Email** tab displays all the email distribution lists present in NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create an SMS distribution list

To receive SMS notifications for NetScaler Console functions, you must add an SMS server and phone numbers.

Perform the following steps to configure SMS notification settings:

1. Navigate to **Settings > Notifications**.
2. In **SMS**, click **Add**.
3. In **Create SMS Distribution List**, specify the following details:
    - **Name** - Specify the distribution list name.
    - **SMS Server** - Select the SMS server that sends SMS notification.
    - **To** - Specify the phone number to which NetScaler Console has to send messages.
4. Click **Create**.

Repeat this procedure to create multiple SMS distribution lists. The **SMS** tab displays all the SMS distribution lists present in NetScaler Console.

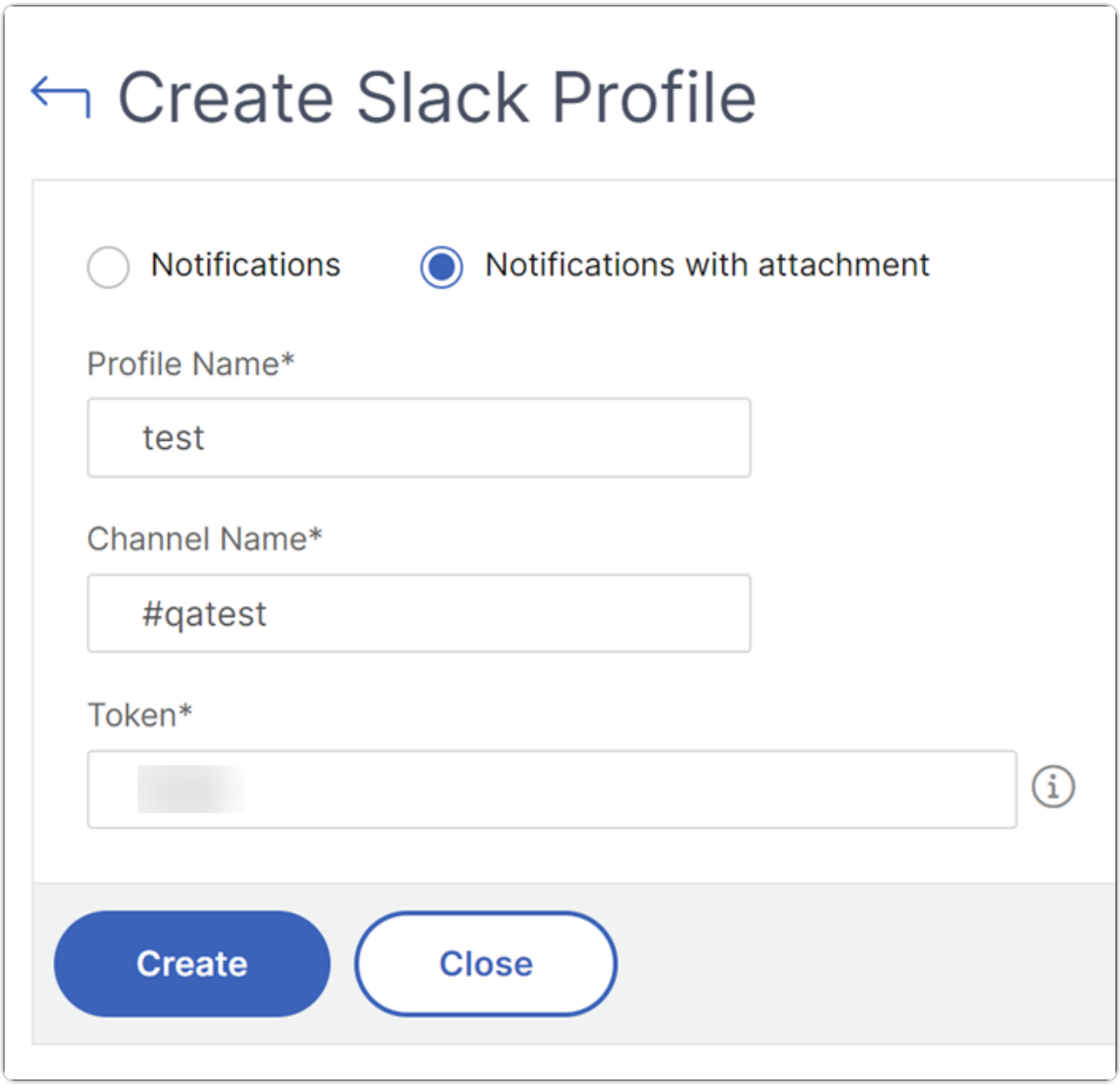
Create a Slack profile

To receive Slack notifications for NetScaler Console functions, you must create a slack profile.

Perform the following steps to create a Slack profile:

1. Navigate to **Settings > Notifications**.
2. In **Slack**, click **Add**.
3. In **Create Slack Profile**, specify the following details:
    - **Profile Name** - Specify the profile name. This name appears in the Slack profile list.
    - **Channel Name** - Specify the Slack channel name to which NetScaler Console has to send notifications.
    - **Webhook URL** - Specify the Webhook URL of the channel. Incoming Webhooks are a simple way to post messages from external sources into Slack. The URL is internally linked to the channel name. And, all event notifications are sent to this URL are posted on the designated Slack channel. An example of a webhook is as follows: `<https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Click **Create**.

Repeat this procedure to create multiple Slack profiles. The **Slack** tab displays all the Slack profiles present in NetScaler Console.

Create a PagerDuty profile

You can add a PagerDuty profile to monitor the incident notifications based on the PagerDuty configurations. PagerDuty enables you to configure notifications through email, SMS, push notification, and phone call on a registered number.

Before you add a PagerDuty profile in NetScaler Console, ensure you have completed the required configurations in PagerDuty. To get started with PagerDuty, see PagerDuty documentation.

Perform the following steps to create a PagerDuty profile:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigate to **Settings > Notifications**.
2. In **PagerDuty**, click **Add**.
3. In **Create PagerDuty Profile**, specify the following details:
   - **Profile Name** - Specify a profile name of your choice.
   - **Integration Key** - Specify the integration key. You can obtain this key from your PagerDuty portal.
4. Click **Create**.

For more information, see Services and Integrations in the PagerDuty documentation.

Repeat this procedure to create multiple PagerDuty profiles. The **PagerDuty** tab displays all the PagerDuty profiles present in NetScaler Console.

View the ServiceNow profile

When you want to enable ServiceNow notifications for NetScaler events and NetScaler Console events, you must integrate NetScaler Console with the ServiceNow using ITSM connector. For more information, see Integrate NetScaler Console with the ServiceNow instance.

Perform the following steps to view and verify the ServiceNow profile:

1. Navigate to **Settings > Notifications**.
2. In **ServiceNow**, select the **Citrix_Workspace_SN** profile from the list.
3. Click **Test** to auto-generate a ServiceNow ticket and verify the configuration.

   If you want to view ServiceNow tickets in the NetScaler Console GUI, select **ServiceNow Tickets**.

Export or schedule export reports

In NetScaler Console, you can export a comprehensive report for the selected NetScaler Console feature. This report provides you an overview of the mapping between the instances, partitions, and corresponding details.

NetScaler Console displays feature-specific scheduled export reports under individual NetScaler Console features, which you can view, edit, or delete. For example, to view the export reports of NetScaler instances, navigate to **Infrastructure > Instances > NetScaler** and click the export icon. You can export these reports in PDF, JPEG, PNG, and CSV file format.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

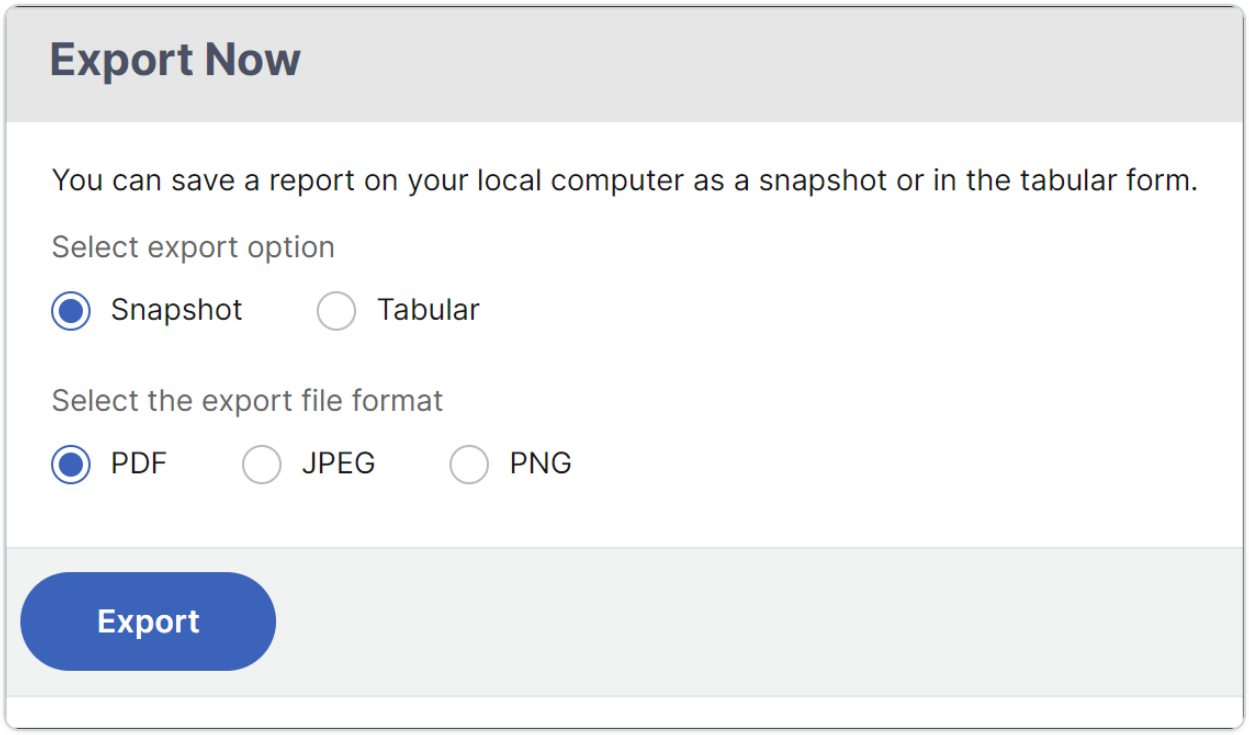
In **Export Reports**, you can perform the following actions:

- Export a report to a local computer
- Schedule export reports
- View, edit, or delete the scheduled export reports

Export a report

To export a report from the NetScaler Console to the local computer, perform the following steps:

1. Click the export icon at the top-right corner of the page.
2. Select **Export Now**.
3. Select one of the following the export options:
    - **Snapshot** - This option export NetScaler Console reports as a snapshot.
    - **Tabular** - This option export NetScaler Console reports in a tabular format. You can also choose how many data records to export in a tabular format



4. Select the file format that you want to save the report on your local computer.
5. Click **Export**.

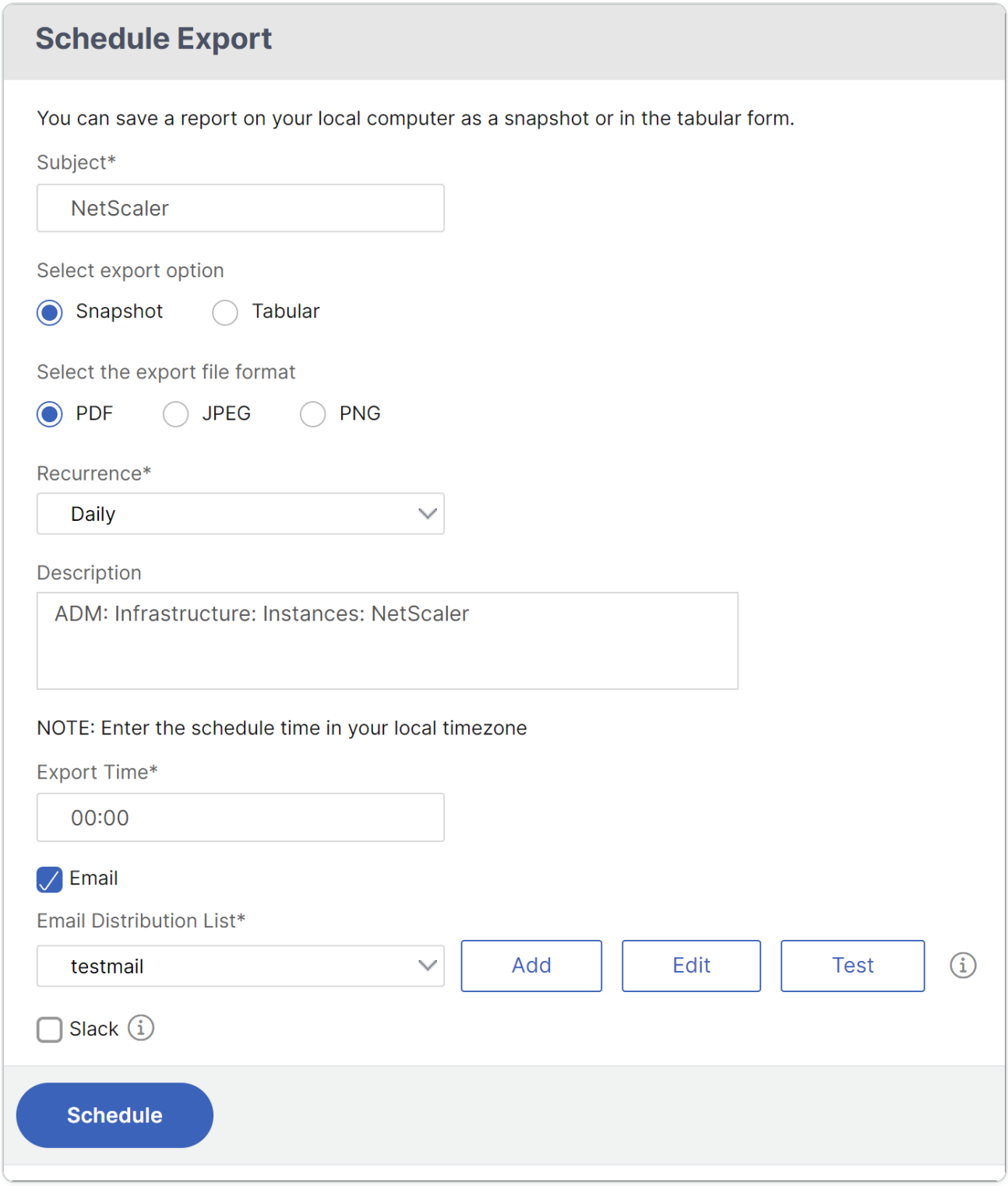
Schedule export report

To schedule the export report at regular intervals, specify the recurrence interval. NetScaler Console sends the exported report to the configured email or slack profile.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Click the export icon at the top-right corner of the page.
2. Select **Schedule Export** and specify the following:
    - **Subject** - By default, this field auto-populates the selected feature name. However, you can rewrite it with a meaningful title.
    - **Export option** - Export NetScaler Console reports in a snapshot or a tabular format. You can also choose how many data records to export in a tabular format
    - **Format** - Select the file format that you want to receive the report on the configured email or slack profile.
    - **Recurrence** - Select **Daily**, **Weekly**, or **Monthly** from the list.
    - **Description** - Specify the meaningful description to a report.
    - **Export Time** - Specify at what time you want to export the report.
    - **Email** - Select the check box and select the profile from the list box. If you want to add a profile, click **Add**.
    - **Slack** - Select the check box and select the profile from the list box. If you want to add a profile, click **Add**.
3. Click **Schedule**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



View and edit the scheduled export reports

To view the export reports, perform the following:

1. Click the export icon at the top-right corner of the page.

   The **Export Report** page displays all the feature-specific export reports .

2. Select the report that you want to edit and click **Edit**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Global Settings

The **Global Settings** in NetScaler Console let you configure system-wide options that apply across your managed NetScaler instances. Use these settings to manage instance settings, system configurations, email subscriptions, and to enable or disable NetScaler Console features.

You can configure the following global settings:

- Instance settings
- System configurations
- Email subscriptions
- Enable or disable NetScaler Console features

Instance settings

You can manage the discovered instances in NetScaler Console and configure the instance backup settings.

Manage the instance configuration

In **Settings > Global Settings > Instance Settings > Instance Management**, you can modify the following instance configurations:

- **Communication with instance(s)** - You can choose an HTTP or HTTPS communication channel between NetScaler Console and the discovered instances.
- **Enable Certificate Download** - Allows you to download the SSL certificates from a discovered instance.
- **Prompt Credentials for Instance Login** - When you access the instance through the NetScaler Console GUI, the instance login page appears. Specify your login credentials to access an instance.

Configure instance backup settings

In **Settings > Global Settings > Instance Settings > Instance Backup**, you can configure the backup settings for the discovered NetScaler instances in NetScaler Console.

In **Configure Instance Backup Settings**, select **Enable Instance Backups**.

- **Number of Backup Files to retain**: Specify the number of backup files to retain in the NetScaler Console. You can retain up to 3 backup files per NetScaler instance. The default is 1 backup file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Backup Scheduling Settings**- You can schedule an instance backup in two ways:
  - **Interval Based** - A backup file is created in NetScaler Console after the specified interval elapses. The default backup interval is 12 hours.
  - **Time Based** - Specify the time in `hours:minutes` format at which you want NetScaler Console to take the instance backup.
- **NetScaler settings** - With this option, you can initiate a backup based on the trap and to include GeoDB files with the backup. This setting applies to MPX,VPX,CPX, and BLX instances.
  - **Do instance backup when NetScalerConfigSave trap is received** - By default, NetScaler Console does not create a backup file when it receives the “NetScalerConfigSave” trap. But, you can enable the option to create a backup file whenever a NetScaler instance sends a `NetScalerConfigSave` trap to NetScaler Console.

    A NetScaler instance sends `NetScalerConfigSave` every time the configuration on the instance is saved.

    Specify **Backup on trap delay** in minutes. If the received `NetScalerConfigSave` trap persists for the specified minutes on NetScaler Console, NetScaler Console backs up the instance.
  - **Include GeoDB files** - By default, NetScaler Console does not back up the GeoDatabase files. You can enable the option to create a backup of these files also.
- **NetScaler SDX Settings** - To back up SDX instances, specify **Backup Timeout** in minutes. During an SDX instance backup, the connection between NetScaler Console and SDX is maintained for the specified period.

  For large SDX backup files, maintain the connection between NetScaler Console and SDX instance for a longer period to ensure backup completion.

  IMPORTANT:

  The backup fails if the connection times out.
- **External Transfer** - NetScaler Console allows you to transfer the NetScaler instance backup files to an external location:

  a. Specify the IP address of the location.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Specify the user name and the password of the external server to which you want to transfer the backup files.

c. Specify the transfer protocol and the port number.

d. Specify the directory path where the file must be stored.

e. If you want to delete the backup file after you transfer the file to an external server, select **Delete file from Application Delivery Management after transfer**.

Disable notifications for managed devices

Administrators can temporarily disable notifications for specific managed devices during maintenance and troubleshooting windows. By disabling notifications, you can avoid receiving unnecessary alerts and notifications concerning device-specific issues and status updates during these intervals.

Administrators can select individual devices, including primary, secondary, or specific cluster nodes. If a VPX instance is on SDX, then VPX and SDX are treated as separate entities for notification configuration. If the disable notifications window is configured for a device, then the configuration is applicable to device partitions as well.

During these intervals, events do get processed, but no notifications (email, Slack, PagerDuty) are sent to administrators for the selected devices. This behavior is applicable to both device-specific events (such as configuration changes, entity down alerts) and console-generated events (such as status polls, threshold breaches).

To disable notifications for specific managed devices, perform the following steps:

1. Navigate to **Settings > Administration > Instance Settings** and click **Notification Disable Windows**.
2. In **Notification Disable Windows**, click **Add**.
3. In **Add Notification Disable Windows**, click **Add Instances** and select the required instances. Click **Ok**.
4. Select the date and time for **Start Date**, **Start Time**, **End Date**, and **End Time**.
5. Add a comment (optional) and click **Create**. The disable notification window appears on the **Notification Disable Windows** page.

You can also edit or delete these disable notification windows. You can also click **History** to view the historical details of the disable notification windows.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

System configurations

You can modify the NetScaler Console agent's keep-alive interval and the NetScaler Console server timezone.

Set agent's keep-alive interval

NetScaler Console server and agent maintain the same TCP connection for the specified keep-alive interval. An agent uses this connection to send the managed instances data to the NetScaler Console server.

1. Navigate to **Settings > Global Settings**.
2. Select **Agent and Timezone** under **System Configurations**.
3. In **Agent**, specify the keep-alive interval between 30–120 seconds.
4. Click **Save**.

Set the NetScaler Console timezone

You can choose the timezone in which you want to display the time on the NetScaler Console webpage, notifications, and reports.

1. Navigate to **Settings > Global Settings**.
2. Select **Agent and Timezone** under **System Configurations**.
3. In **Time zone**, select local or GMT time zone to display time in NetScaler Console.
4. Click **Save**.

Email subscriptions

NetScaler Console sends in email notifications to all the inactive and the new users.

Inactive customers receive an email notification if:

- NetScaler instances are not configured
- The tenant license expires in less than 30 days

NOTE:

By default, all such inactive customers receive an email notification.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

New customers receive an email from NetScaler Console inviting them to onboard the NetScaler instances to NetScaler Console service where they are able to manage and monitor critical events on NetScaler instances, troubleshoot, and automate tasks like NetScaler configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

citrix

Manage, monitor, troubleshoot, automate with Citrix ADM Service



Hello [redacted] Org ID - [redacted] Customer name - [redacted]

Congratulations on getting started with ADM service successfully! You can now onboard your ADC instances to ADM service to :

- Monitor critical events on your ADC instances through alerts.
- Automate mundane tasks like ADC configuration.
- Get rich analytics pertaining to ADC and Applications health, performance, and security.

All this is easy to set up and we have resources below to get you started.

Onboard ADC instances on ADM service in 3 quick steps

Start with this brief video to know the exact steps to onboard ADC instances to ADM service quickly. Learn more

Onboard ADC Instances

Sign in using Citrix Cloud/ My Citrix credentials

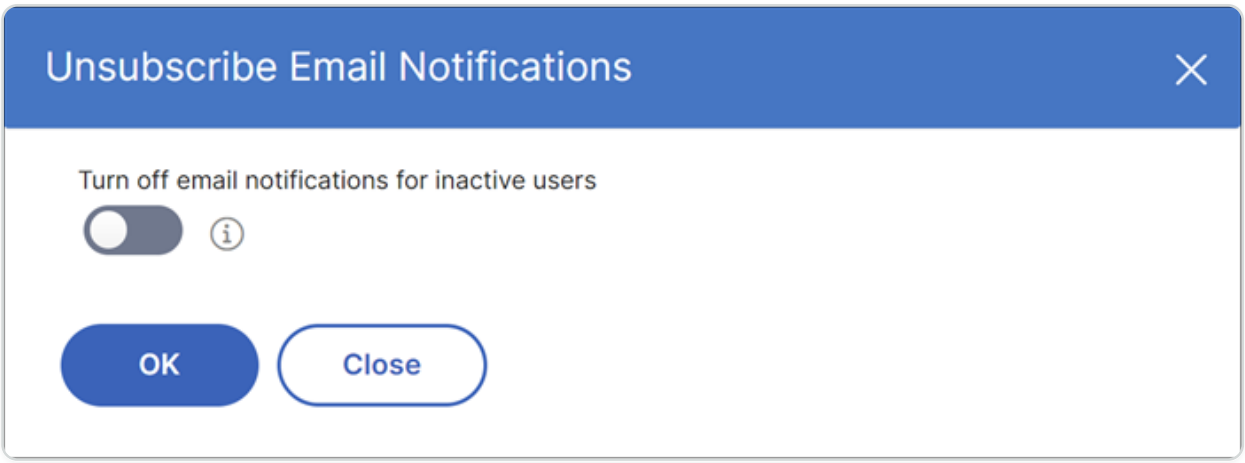
Your free ADM use cases resources

- Get bird's eye visibility into entire ADC infra and debug critical issues on your ADC instances.
- Manage the complete SSL cert lifecyle using Citrix ADM.
- Always stay on top of critical events with Citrix ADM ServiceNow integration.

Unsubscribe Email Notifications

You can subscribe or unsubscribe from the email notifications that you receive from NetScaler Console service. To **Unsubscribe Email Notifications**:

1. In NetScaler Console, navigate to **Settings > Global Settings > System Configurations**, and then click **Email Subscriptions**. The **Unsubscribe Email Notifications** window appears.



NOTE:

By default, the toggle button for turning off email notifications is in the off position and the email notifications are enabled for all inactive users.

2. In the **Unsubscribe Email Notifications** window, turn on the toggle button. Click **OK**.

You have now unsubscribed the email notifications and will not receive any emails to Onboard NetScaler instances.

Enable or disable features

As an administrator, you can enable or disable the following features in the **Settings > Global Settings > Configurable Features** page:

- **Agent failover** - The agent failover can occur on a site that has two or more active agents. When an agent becomes inactive (DOWN state) in the site, the NetScaler Console redistributes the NetScaler instances of the inactive agent with other active agents. For more information, see Configure NetScaler agent agents for multisite deployment.
- **Entity polling network function** - An entity is either a policy, virtual server, service, or action attached to a NetScaler instance. By default, NetScaler Console automatically polls configured network function entities every 60 minutes. For more information, see Polling overview.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Instance backup** - Back up the current state of a NetScaler instance and later use the backed-up files to restore the NetScaler instance to the same state. For more information, see Back up and restore NetScaler instances.
- **Instance configuration audit** - Monitor configuration changes across managed NetScaler instances, troubleshoot configuration errors, and recover unsaved configurations. For more information, see Create audit templates.
- **Instance events** - Events represent occurrences of events or errors on a managed NetScaler instance. Events received in NetScaler Console are displayed on the **Events Summary** page (**Infrastructure > Events**). And all active events are displayed in the Event Messages page (**Infrastructure > Events > Event Messages**). For more information, see Events.
- **Instance network reporting** - You can generate reports for instances at a global level. Also, for entities such as the virtual servers and network interfaces. For more information, see Network Reporting.
- **Instance SSL certificates** - NetScaler Console provides a centralized view of SSL certificates installed across all managed NetScaler instances. For more information, see SSL Dashboard.
- **Instance Syslog** - You can monitor the syslog events generated on your NetScaler instances if you have configured your device to redirect all syslog messages to NetScaler Console. For more information, see Configuring syslog on instances.

To enable a feature, perform the following steps:

1. Select the feature from the list that you want to enable.
2. Click **Enable**.

IMPORTANT:

If a feature is disabled, the user cannot perform the operations associated with that feature.

Configure an action policy to receive application event notifications

Apart from the existing analytics view of application events, you can configure an action policy to get application event notifications through Slack, Email, PagerDuty, or ServiceNow. The application events include performance issues, bot and WAF violations, and service graph violations. As an administrator, using the action policy, you can get event notifications in real time.

Using the action policy, you can:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Predefine certain conditions for the application events.
- Get notified for the following events through Slack, Email, PagerDuty, and ServiceNow:

EVENT CATEGORIES	EVENT SUB CATEGORIES	EVENTS
Security Violations	All Security Violations	All Bot Violations (For more information on the list of bot violations, see violation categories).
		All WAF Violations (WAF SQL Violations, WAF XSS Violations, and WAF Infer XML Violations)
	All Security Violations per Client	Bot Violations per Client
		WAF Violations per Client
		Note: To receive the WAF violation notification, the minimum violation transactions must be 20%. For example, out of 100 transactions, minimum 20 must be violation transactions.
Application Performance		App score violation
		Client network latency
		Server network latency
		Server processing time
		Response time
		Requests
		Bandwidth

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EVENT CATEGORIES	EVENT SUB CATEGORIES	EVENTS
		Service graph violation
Application Usage		Requests per second
		Throughput
		Data Volume

Configure an action policy

1. Navigate to **Settings > Action > Action Policies**.
2. Click **Add**.
3. In the **Create Action Policy** page:

   a. **Policy Name** – Provide a policy name of your choice.

   b. **Enabled** – This option is selected by default.

   c. If the **Following Event Occurs** – From the list, select an event.

   d. **And the Following Condition is Met** – From the list, select to define a condition for which you want to get notified. You can click **+** to add more conditions. To remove a condition, click **–**.

   You can configure the action policy using the following operators. The operators appear based on the conditions you select.

OPERATOR	DESCRIPTION
Equal to	Equals to a defined value
Not Equal to	Not equals to a defined value
Greater than	Greater than a defined value
Greater than or Equal to	Greater than or equal to a defined value
Less than	Lesser than a defined value
Less than or Equal to	Lesser than or equal to a defined value
Contains	Contains the defined term or value

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OPERATOR	DESCRIPTION
Starts with	Starts with a defined term or value
Ends with	Ends with a defined term or value
IN	Allows you to select multiple values

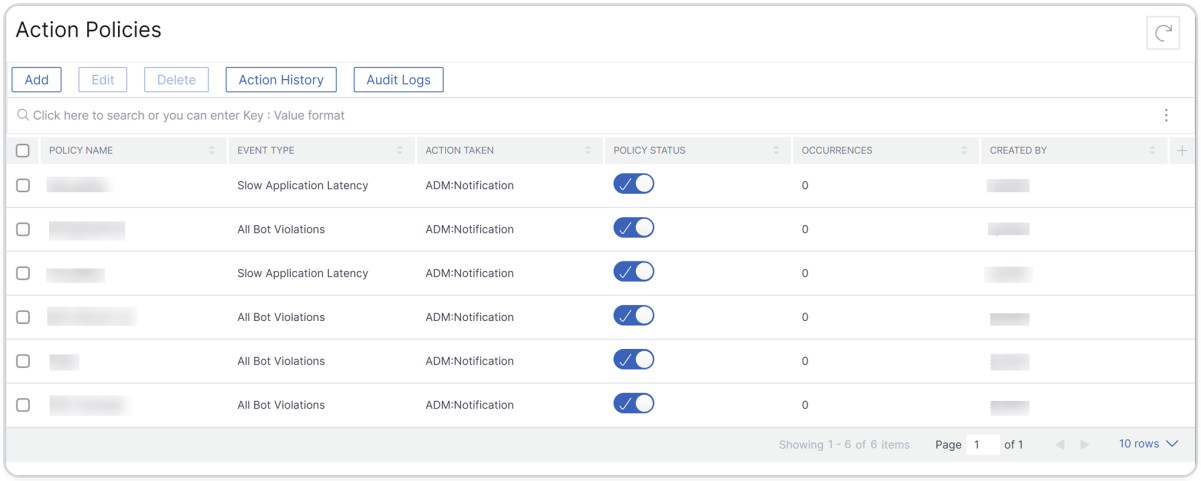
e. **Then Do the Following** – Select **Notify**. After you select **Notify**, the Notification Type option is displayed.

f. **Notification Type** – Select the notification type Email, Slack, PagerDuty, or ServiceNow. Depending upon the notification type you select, the corresponding option (Distribution list, Slack Profile, PagerDuty Profile, or ServiceNow profile) appears. Select a profile from the list.

   If you want to create a new profile, click **Add**.

g. Click **Create Policy**.

   The policy is configured. You can view the configured policy details.



After you configure the policy, you can select the policy and click:

- **Edit** to update or change the action policy. After you update, click Update Policy.
- **Delete** to remove the action policy. You can select multiple policies and click **Delete** to remove them.
- **Action History** to view details such as time, action taken, policy name, alert type, and alert message.

The following table describes the details of action policy configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VIOLATION NAME	CONDITION	DESCRIPTION
All Security Violations	Instance IP	IP address of the NetScaler instance. Select the IP address from the list.
	Violation Count	The violation count for which you want to get notified. For example, if you configure violation count as less or equal to 10, you will get notified if 10 or less bot violation transactions are received.
	Violation Ratio	This value indicates the total violations from specific transactions and the value must be between 0 and 1. For example, out of 100 transactions, 20 are violations and if you wanted to get notified for such a scenario, you must enter 0.2.
All Bot violations	Bot profile	The bot profile name that is used for configuring bot management on the NetScaler instance.
	Instance IP	IP address of the NetScaler instance. Select the IP address from the list.
	Violation Count	The violation count for which you want to get notified. For example, if you configure violation count as less or equal to 10, you will get notified if 10 or less bot violation transactions are received.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VIOLATION NAME	CONDITION	DESCRIPTION
	Violation Ratio	This value indicates the total violations from specific transactions and the value must be between 0 and 1. For example, out of 100 transactions, 20 are violations and if you wanted to get notified for such a scenario, you must enter 0.2.
All WAF Violations, WAF SQL Violation, WAF XSS Violation, WAF Infer XML Violation	WAF Profile	The WAF profile name that is used for configuring WAF security settings on the NetScaler instance.
	Instance IP	IP address of the NetScaler instance. Select the IP address from the list.
	Violation Count	The violation count for which you want to get notified. The minimum requirement for the WAF violations to get notified is 20%.
	Violation Ratio	This value indicates the total violations from specific transactions and the value must be between 0 and 1. For example, out of 100 transactions, 20 are WAF SQL violation transactions and if you want to get notified for such a scenario, you must enter 0.2.
All Security Violations per Client	Application Name	The custom application name. Select the application from the list. If you do not add this condition, then all applications from the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VIOLATION NAME	CONDITION	DESCRIPTION
		NetScaler instance are considered.
	Instance IP	IP address of the NetScaler instance. Select the IP address from the list.
	Client IP	The source from where the Bot originates. Specify the IP address.
	Total Attacks	The total attacks for which you want to get notified.
	Request URL	The URL that you want to configure to block. Specify the URL.
	Vserver name	The associated applications configured for custom applications. Select the application from the list. If you do not add this condition, then all applications from the NetScaler instance are considered.
Bot Violations per Client	Application Name	The custom application name. Select the application from the list. If you do not add this condition, then all applications from the NetScaler instance are considered.
	Instance IP	IP address of the NetScaler instance. Select the IP address from the list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VIOLATION NAME	CONDITION	DESCRIPTION
	Client IP	The source from where the Bot originates. Specify the IP address.
	Total Attacks	The total attacks for which you want to get notified.
	Violation Type	Select the bot violation from the list.
	Request URL	The URL that you want to configure to block. Specify the URL.
	Vserver name	The associated applications configured for custom applications. Select the application from the list. If you do not add this condition, then all applications from the NetScaler instance are considered.
WAF Violations per Client	Application Name	The custom application name. Select the application from the list. If you do not add this condition, then all applications from the NetScaler instance are considered.
	Instance IP	IP address of the NetScaler instance. Select the IP address from the list.
	Client IP	The source from where the Bot originates. Specify the IP address.
	Total Attacks	The total attacks for which you want to get notified.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VIOLATION NAME	CONDITION	DESCRIPTION
	Violation Type	Select the WAF violation from the list.
	Request URL	The URL that you want to configure to block. Specify the URL.
	Vserver name	The associated applications configured for custom applications. Select the application from the list. If you do not add this condition, then all applications from the NetScaler instance are considered.
App Score Violation	Performance Indicator	The app score components and their threshold values. Select the app score component from the list. For more information, see Select App Score components and set thresholds.
	Breach Count	The breach count for which you want to get notified. For example, if you configure breach count Equal to 5 for response time, you will get notified when the response time threshold is breached 5 times.
	Application Name	Click **Select Applications** to select the applications that you want to get the violation notified.
Client Network Latency	Client Network Average Latency	Specify the client latency (client to NetScaler) value in

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VIOLATION NAME	CONDITION	DESCRIPTION
		milliseconds for which you want to get notified.
	Client Network Latency Anomalies	Specify the anomaly count for the network latency that you want to get notified.
	Application Name	Click **Select Applications** to select the applications that you want to get the violation notified.
Server Network Latency	Server Network Average Latency	Specify the server latency (server to NetScaler) value in milliseconds for which you want to get notified.
	Server Network Latency Anomalies	Specify the anomaly count for the network latency that you want to get notified.
	Application Name	Click **Select Applications** to select the applications that you want to get the violation notified.
Response Time	Response Avg Time	Specify the value (in milliseconds) for which you want to get notified.
	Response Avg Time Anomalies	Specify the anomaly counts for which you want to get notified.
	Application Name	Click **Select Applications** to select the applications that you want to get notified. If you do not select any application, then it is applied in all applications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VIOLATION NAME	CONDITION	DESCRIPTION
Requests	Total Requests	Specify the total requests for which you want to get notified.
	Application Name	Click **Select Applications** to select the applications that you want to get notified. If you do not select any application, then it is applied in all applications.
Bandwidth	Total Bandwidth	Specify the bandwidth (MB) for which you want to get notified.
	Application Name	Click **Select Applications** to select the applications that you want to get notified. If you do not select any application, then it is applied in all applications.
Server Processing Time	Server Processing Average Time	Specify the server processing (server to NetScaler) value in milliseconds for which you want to get notified.
	Server Processing Time Anomalies	Specify the anomaly count for the server processing time that you want to get notified.
	Application Name	Click **Select Applications** to select the applications that you want to get the violation notified.
Service Graph Violation		Microservices that breach the configured thresholds. For more information, see Configure thresholds in service graph.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VIOLATION NAME	CONDITION	DESCRIPTION
Requests per second	Requests per second avg	The number of requests received by the application per second. Specify the average value to get notified.
	Requests per second avg anomalies	Specify the average anomaly count for which you want to get notified.
		Note: If you are using AND condition for this event, you can configure either Requests per second avg and Application Name or Requests per second anomaly average and Application Name.
	Application Name	Click **Select Applications** to select the applications that you want to get the violation notified.
Throughput	Throughput avg	The total data transmitted for a specific period. Specify the average value (in MB) to get notified.
	Throughput avg anomalies	Specify the average anomaly count for which you want to get notified.
		Note: If you are using AND condition for this event, you can configure either Throughput avg and Application Name or Throughput avg anomaly and Application Name.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VIOLATION NAME	CONDITION	DESCRIPTION
	Application Name	Click **Select Applications** to select the applications that you want to get the violation notified.
Data Volume	Total Data Volume	The total data that is to be transferred in a specific duration. Specify the value (in MB) to get notified.
	Data Volume Anomalies	Specify the anomaly count for which you want to get notified.
		Note: If you are using AND condition for this event, you can configure either Total Data Volume and Application Name or Data Volume Anomalies and Application Name.
	Application Name	Click **Select Applications** to select the applications that you want to get the violation notified.

Use the search bar

The search bar enables you to filter results. When you click the search bar, it gives you a list of search suggestions. You can select the component and filter the results based on your requirements.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use the audit logs option

Click **Audit Logs** and select the duration from the list to view the action policies that are created, modified, and deleted for the selected duration and click **Search**.

NOTE

The data storage policies are expected to change in the upcoming releases. With these changes, you cannot store historical data after it exceeds the storage limit. For now, it is recommended to add more storage or keep the storage within the license entitlement limits.

Use audit logs for managing and monitoring your infrastructure

You can use the NetScaler Console to track all events on NetScaler Console and syslog events generated on the NetScaler instances. These messages can help you manage and monitor your infrastructure. But log messages are a great source of information only if you review them, and NetScaler Console simplifies the way of reviewing log messages.

You can use filters to search NetScaler Console syslog and audit log messages. The filters help to narrow down your results and find exactly what you are looking for and in real time. The built-in Search Help guides you to filter the logs. Another way to view log messages is to export them in PDF, CSV, PNG, and JPEG formats. You can schedule the export of these reports to specified email addresses at various intervals.

You can review the following types of log messages from the NetScaler Console GUI:

- NetScaler instance related audit logs
- NetScaler Console related audit logs
- Application audit logs

NetScaler instance related audit logs

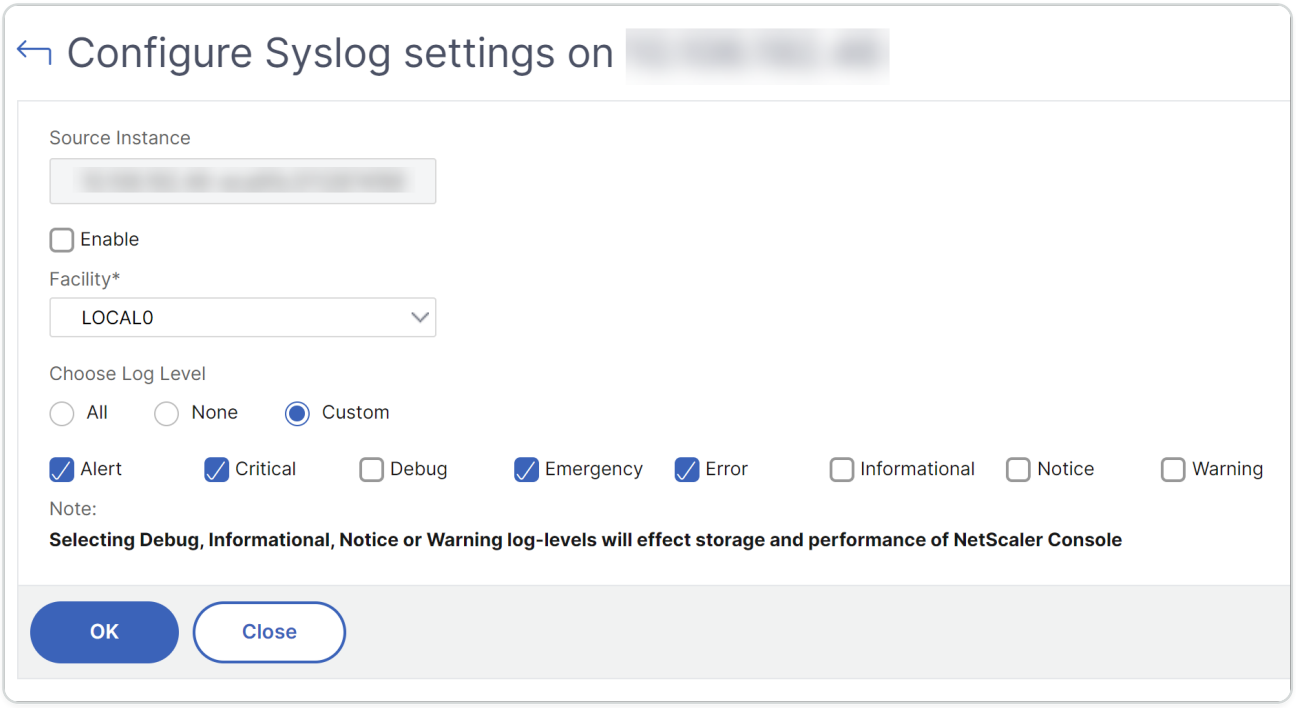
Before you can view NetScaler instance-related syslog messages from NetScaler Console, configure the NetScaler Console as the syslog server for your NetScaler instance. After the configuration is complete, all syslog messages are redirected from the instance to NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure NetScaler Console as a syslog server

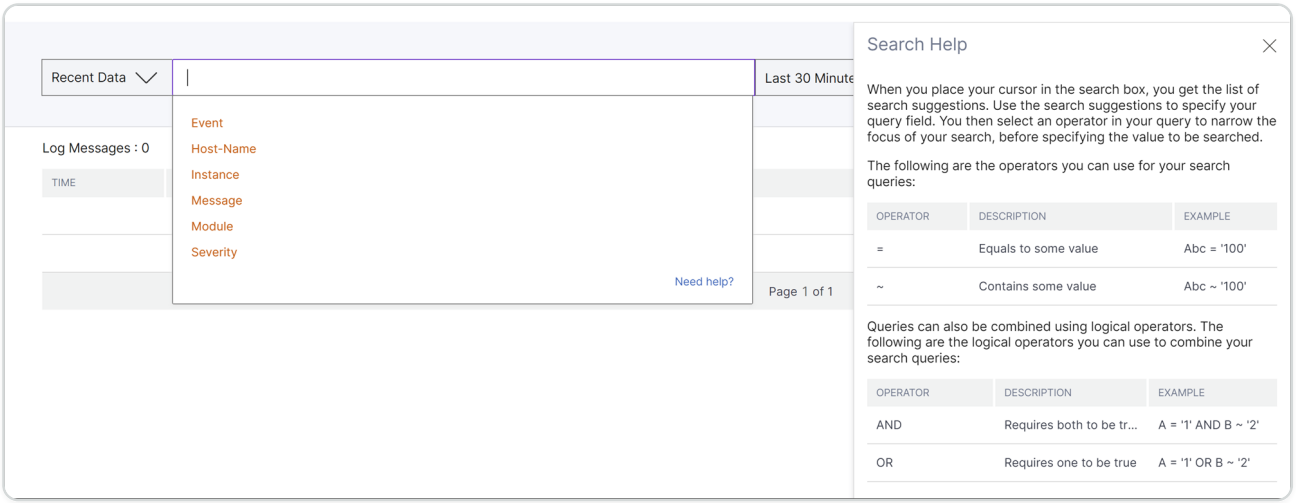
Follow these steps to configure NetScaler Console as the syslog server:

1. From the NetScaler Console GUI, navigate to **Infrastructure > Instances**.
2. Select the NetScaler instance from which you want the syslog messages to be collected and displayed in NetScaler Console.
3. In the **Select Action** list, select **Configure Syslog**.
4. Click **Enable**.
5. In the **Facility** drop-down list, select a local or user-level facility.
6. Select the required log level for the syslog messages.
7. Click **OK**.



These steps configure all the syslog commands in the NetScaler instance, and NetScaler Console starts receiving the syslog messages. You can view the messages by navigating to **Infrastructure > Events > Syslog Messages**. Click **Need Help?** to open the built-in search help. For more information, see View and Export syslog messages.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



To export the log messages, click the arrow icon on the upper right corner.

Next, click **Export Now** or **Schedule Export**. For more information, see Export syslog messages.

NetScaler Console related audit logs

Based on preconfigured rules, NetScaler Console generates audit log messages for all events on, helping you monitor the health of your infrastructure. To view all audit log messages present in the NetScaler Console, navigate to **Settings->Audit Log Messages**.

To export the log messages, click the arrow icon on the upper right corner.

Application related audit logs

You can view the audit log messages for all NetScaler Console applications or for a specific application.

- To view all audit log messages for all applications present in the NetScaler Console, navigate to **Infrastructure > Network Functions > Auditing**.
- To view audit log messages for any specific application in the NetScaler Console, navigate to **Applications > Dashboard > double-click the virtual server > Audit Log**.

Note

You can forward NetScaler Console audit log messages to an external server. For details, see View auditing information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure IP address management (IPAM)

NetScaler Console IPAM allows you to auto-assign and release IP addresses in NetScaler Console managed configurations. You can assign IPs from networks or IP ranges defined using the following IP providers:

- NetScaler Console built-in IPAM provider.
- Infoblox IPAM solution.

You can use NetScaler Console IPAM in:

- **StyleBooks**: Auto-Allocate IPs to virtual servers when you create configurations.
- **API gateway**: Auto-allocate an IP address to the API proxy.

You can also track the IP addresses in each network or the IP range managed by NetScaler Console.

If you encounter the following error while adding an external IPAM provider, it indicates that the NetScaler Console is unable to verify the SSL certificate for the external IPAM provider due to a missing or unrecognized Certificate Authority (CA) certificate:

```
certificate verify failed: unable to get local issuer certificate
```

To resolve this issue, you can manually add the required CA certificate to the NetScaler Console agent that is used for accessing the external IPAM provider. Adding the required CA certificate ensures that secure connections to the external IPAM provider are properly validated.

Log in to NetScaler Console agent that is used for accessing the external IPAM provider and add your CA certificate to the trusted certificate bundle `/var/mps/ca_certs/cacert.pem`.

Add an external IP address provider

NetScaler Console has a built-in IPAM provider to manage IPs and IP ranges. You can also use an external IP address provider to NetScaler Console.

IMPORTANT:

Before you begin, make sure that the following permissions are enabled in the external IP address provider:

- Ability to query networks that are present in the provider.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Reserve an IP address in the network.
- Free an IP address from the network.
- Retrieve the used IP addresses from a network.
- Retrieve available IP addresses from a network.

Perform the following steps to add an external IPAM provider solution in NetScaler Console:

1. Navigate to **Settings > IPAM**.
2. In **Providers**, click **Add**.
3. Specify the following details to add an IPAM provider:
   - **Name** - Specify the IP provider name to use in NetScaler Console.
   - **Vendor** - Select an IPAM vendor from the list.
   - **URL** - Specify the URL of the IPAM solution that assigns IP addresses in an NetScaler Console environment. Ensure to specify the URL in the following format:

     ```
     https://<host name>
     ```

     Example: `https://myinfoblox.example.com`
   - **Is it a private endpoint?** - If the Infoblox DDI is privately hosted, select this checkbox and then select an **Agent**.
   - **User Name** - Specify the user name to log in to the IPAM solution.
   - **Password** - Specify the password to log in to the IPAM solution.
4. Click **Add**.

Infoblox DDI as an external provider

Currently, NetScaler Console supports Infoblox DDI as an external provider. The Infoblox DDI can either be publicly accessible or hosted privately, accessible only within an enterprise's internal network. In the case of a privately hosted Infoblox DDI, you must select a NetScaler agent during the configuration process. The NetScaler agent acts as a proxy, to access the provider that resides within the enterprise’s intranet.

You can use NetScaler Console IPAM with the Infoblox provider to do the following actions:

- List IPAM networks
- Create, update, and delete IPAM networks

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Reserve and release an IP address from IPAM networks

Create an IPAM network

To create an NetScaler Console IPAM network using the Infoblox provider, a network with the same CIDR IP range must exist on Infoblox.

When you create an IPAM network within the NetScaler Console, you're only registering the use of Infoblox network within the NetScaler Console. The NetScaler Console then works together with Infoblox to manage IP addresses allocated from the network. The InfoBlox network can continue to be used outside of the NetScaler Console.

Similarly, If you delete the NetScaler Console IPAM network, the NetScaler Console de-registers the Infoblox network. This means that the NetScaler Console no longer interacts with Infoblox for IP address management in that network.

Infoblox DDI APIs

NetScaler Console IPAM uses the following Infoblox APIs to perform the respective actions:

- (/network) - Lists all available Infoblox networks
- (/network?network={id}) - Retrieves details of a specific Infoblox network
- (/ipv4address) - Lists all IPs on an Infoblox network
- (/record:host) - Retrieves details of a specific IP address
- (/{IP}) - Reserves and frees IPs on an Infoblox network

NOTE:

- The Infoblox DNS, DHCP, and IP address management (DDI) server IP and port must be accessible from the public network so that the NetScaler Console service can reach and connect to the Infoblox server.
- The Infoblox user account configured on NetScaler Console must have the required permissions to use the Infoblox APIs.

For more information on the Infoblox APIs, see the Infoblox REST API reference guide available at Infoblox DDI.

Add a network

Add a network to use IPAM with NetScaler Console managed configurations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigate to **Settings > IPAM**.
2. Under **Networks**, click **Add**.
3. Specify the following details:

   - **Network Name** - Specify the network name to identify the network in NetScaler Console.
   - **Provider** - Select the provider from the list.

     This list displays the providers added in NetScaler Console.
   - **Network Type** - Select **IP range** or **CIDR** from the list based on your requirement.
   - **Network Value** - Specify the network value.

     NOTE:

     NetScaler Console IPAM supports only IPv4 addresses.

     For **IP range**, specify the network value in the following format:

     ```
     <first-IP-address>-<last-IP-address>
     ```

     Example:

     ```
     10.0.0.20-10.0.0.100
     ```

     For **CIDR**, specify the network value in the following format:

     ```
     <IP-address>/<subnet-mask>
     ```

     Example:

     ```
     10.70.124.0/24
     ```
4. Click **Create**.

View allocated IP addresses

To view more details about allocated IP addresses from the IPAM network, do the following steps:

1. Navigate to **Settings > IPAM**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Under the **Networks** tab, click **View All Allocated IPs**.

   This pane displays IP address, provider name, provider vendor, and description. It also displays the resource details that reserved this IP address:

   - **Module**: Displays the NetScaler Console module that reserved the IP address. For example, if StyleBooks reserved the IP address, this column displays StyleBooks as the module.
   - **Resource Type**: Displays the resource type in that module. For the StyleBooks module, only the configurations resource type uses the IPAM network. So, it displays Configurations under this column.
   - **Resource ID**: Displays the exact resource id with a link. Click this link to access the resource that is using the IP address. For the configuration resource type, it displays the configuration pack ID as the resource ID.

NOTE:

If you want to release the IP address, select the IP address that you want to release and click **Release Allocated IPs**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How-to articles

NetScaler Console "How-to Articles" are simple, relevant, and easy to implement articles on the features available with the service. These articles contain information about some of the popular NetScaler Console features such as instance management, configuration management, event management, application management, StyleBooks, and certificate management.

Click a feature name in the following table to view the list of how-to articles for that feature.

TOPICS		
Instance management	Configuration management	Certificate management
StyleBooks	Event management	

Instance management

How to monitor globally distributed sites

How to manage admin partitions of NetScaler instances

How to add instances to NetScaler Console

How to create instance groups on NetScaler Console

How to poll NetScaler instances and entities in NetScaler Console

How to configure sites for Geomaps in NetScaler Console

How to force a failover to the secondary NetScaler instance

How to force a secondary NetScaler instance to stay secondary

How to change a NetScaler MPX or VPX root password

How to change a NetScaler SDX root password

Configuration management

How to use SCP (put) command in configuration jobs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How to upgrade NetScaler SDX instances by using NetScaler Console

How to schedule jobs created by using built-in templates in NetScaler Console

How to reschedule jobs that were configured by using built-in templates in NetScaler Console

Reuse run configuration jobs

How to upgrade NetScaler instances using NetScaler Console

How to create a configuration job on NetScaler Console

How to use variables in configuration jobs on NetScaler Console

How to use configuration templates to create audit templates on NetScaler Console

How to create configuration jobs from corrective commands on NetScaler Console

How to replicate running and saved configuration commands from one NetScaler instance to another on NetScaler Console

How to use configuration jobs to replicate configuration from one instance to multiple instances

How to use the master configuration template on NetScaler Console

Certificate management

How to configure an enterprise policy on NetScaler Console

How to install SSL certificates on a NetScaler instance from NetScaler Console

How to update an installed certificate from NetScaler Console

How to link and unlink SSL certificates by using NetScaler Console

How to create a certificate signing request (CSR) by using NetScaler Console

How to set up notifications for SSL certificate expiry from NetScaler Console

How to use the SSL dashboard on NetScaler Console

StyleBooks

How to use default StyleBooks in NetScaler Console

How to create your own StyleBooks

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How to use user-defined StyleBooks in NetScaler Console

How to use API to create configurations from StyleBooks

How to enable analytics and configure alarms on a virtual server defined in a StyleBook

How to create a StyleBook to upload SSL certificate and certificate key files to NetScaler Console

How to use Microsoft Skype for Business StyleBook in business enterprises

How to use Microsoft Exchange StyleBook in business enterprises

How to use Microsoft SharePoint StyleBook in business enterprises

How to use Microsoft ADFS Proxy StyleBook

How to use Oracle E-business StyleBook

How to use SSO Office 365 StyleBook

How to use SSO Google Apps StyleBook

Event management

How to set event age for events on NetScaler Console

How to schedule an event filter by using NetScaler Console

How to set repeated email notifications for events from NetScaler Console

How to suppress events by using NetScaler Console

How to use the events dashboard to monitor events

How to create event rules on NetScaler Console

How to modify the reported severity of events that occur on NetScaler instances

How to view the events summary in NetScaler Console

How to display event severities and skews of SNMP traps on NetScaler Console

How to export syslog messages using NetScaler Console

How to suppress Syslog messages in NetScaler Console

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FAQs

How many agents do I need to install?

The number of agents depends on the number of managed instances in a data center and the total throughput. Citrix recommends that you install at least one agent for every data center.

How can I install multiple agents?

You can install only one agent when you log on to the service for the first time. To add multiple agents, first complete the initial setup, and then navigate to **Settings** > **Setup Agents**.

Does NetScaler agent support AMD processors?

Yes.

Can I transition from a built-in agent to an external agent?

Yes, you can. For more information, see Transition from a built-in agent to an external agent.

How do I get a new activation code if I lose it?

If you are onboarding for the first time, access the service GUI, navigate to the **Set Up Agent** screen, and click **Generate Activation Code**.

While trying to install a second agent, to generate a new activation code, navigate to **Infrastructure > Instances > Agents > Generate Activation Code.**

How do I log on to the agent VM? What are the default credentials?

If your agent is installed on a hypervisor or Microsoft Azure cloud, the default logon credentials for the agent are `nsrecover/nsroot`, which opens the shell prompt of the agent.

If your agent is installed on AWS, the default credentials to log on to the agent is `nsrecover/instance id`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What are the resource requirements to install an agent on a hypervisor on-premises?

32 GB RAM, 8 Virtual CPU, 500 GB Storage, 1 Virtual Network Interfaces, 1 Gbps Throughput

Do I need to assign an extra disk to the agent while provisioning?

No, you do not have to add an extra disk. The agent is used only as an intermediary between the NetScaler Console and the instances in your enterprise data center or on the cloud. It does not store inventory or analytics data that would require an extra disk.

Can I reuse my activation code with multiple agents?

No, you cannot.

How do I rerun network settings if I have entered an incorrect value?

Access the agent console on your hypervisor, log on to the shell prompt by using the credentials nsrecover/nsroot, and then run the command `networkconfig`.

What do I do if my agent registration fails?

Ensure that:

- Your agent has access to the Internet (configure DNS).
- You have copied the activation code correctly.
- You have entered the service URL correctly.
- You have the required ports open.

Registration is successful, but how do I know if the agent is running fine?

After the agent is successfully registered, access NetScaler Console and navigate to the **Set Up Agent** screen. You can see the discovered agent on the screen. If the agent is running fine, a green icon appears. If it is not running, a red icon appears.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How can I connect agents to NetScaler Console using a proxy server?

You can connect agents to NetScaler Console using a proxy server. The script is available at `/mps` folder in agent. The agents forward all their data to the proxy server, which then sends the data to the NetScaler Console through the internet.

To forward data using the proxy server, type the proxy server details on the agent using the following script: `proxy_input.py`, and follow the instructions provided by the script to enter more information. The agent fetches this information while it connects to NetScaler Console using the proxy server.

You can authenticate your proxy server by providing your user name and password information. When the agent sends the data, the proxy server authenticates the user credentials before forwarding it to NetScaler Console.

For more information, see NetScaler Console as an API proxy server.

NOTE

NetScaler Console supports proxy servers with basic authentication enabled. NetScaler Console also supports proxy servers where authentication is disabled.

I do not see my Analytics Reports

Enable insight on your virtual servers to see the Analytics Reports. For details, see Enabling Analytics.

Which versions of NetScaler instances are supported in NetScaler Console?

For management and monitoring features, NetScaler instances running 10.5 and later are supported. Some features are only supported on certain NetScaler versions. For details, see System Requirements.

How do I export dashboard reports in NetScaler Console?

To export the report of any dashboard in NetScaler Console, click the **Export** icon on the top right side of this page. On the **Export** page, you can do one of the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Select **Export Now** tab. To view and save the report in PDF, JPEG, PNG, or CSV format. The report downloads to your system.
2. Select **Schedule Report** to set up schedules for generating and exporting reports at regular intervals. Specify the report generation recurrence settings and create an email profile to which the report is exported.

    a. **Recurrence** - Select **Daily**, **Weekly**, or **Monthly** from the drop-down list box.

    NOTE

    - If you select **Weekly** recurrence, ensure that you select the weekdays on which you want the report to be scheduled.
    - If you select **Monthly** recurrence, ensure that you enter all the days that you want the report to be scheduled separated by commas.

    b. **Recurrence time** - Enter the time as `Hour: Minute` in 24-hour format.

    c. **Email** - Select the check box and then select the profile from the drop-down list box, or click **Add** to create an email profile.

    d. **Slack** - Select the check box and then select the profile from the drop-down list box, or click **Add** to create an email profile.

    Click **Enable Schedule** to schedule your report and then, click **OK**. By clicking the **Enable Schedule** check box, you can generate the selected reports.

What does enabling client-side measurements do?

With client side measurements enabled, NetScaler Console captures load time and render time metrics for HTML pages, through HTML injection. Using these metrics, admins can identify L7 latency issues.

Is SSL traffic from Agent to NetScaler Console service taken through SSL inspection?

We recommend you to bypass the SSL inspection for Agent to the NetScaler Console service SSL traffic.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

index

- Analytics
- Dashboards
- WAF Insight
- Configure the learning profile
- Network violation details
- View WAF learning Actions Summary
- View relaxation rules, idle, and deny rules
- SSL Insight
- View analytics for Web transactions
- Detailed procedures to setup dual tier or service mesh lite topology
- Detailed procedures to setup service mesh topology
- Detailed procedures to setup single tier or unified ingress topology
- Data governance for NetScaler® telemetry program
- How to change the NetScaler MPX and VPX root password
- Previous releases

Analytics

NetScaler Console analytics provide an easy and scalable way to look into the various insights of the NetScaler instances' data to describe, predict, and improve the application's performance. You can use one or more analytics features simultaneously on NetScaler Console. Following table describes various analytics features that are supported on NetScaler Console:

ANALYTICS FEATURES	DESCRIPTIONS
Web Insight	Web Insight enables visibility into enterprise web applications and allows IT administrators to monitor all web applications being served by the NetScaler by providing integrated and real-time monitoring of applications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ANALYTICS FEATURES	DESCRIPTIONS
HDX insight	HDX Insight provides end-to-end visibility for ICA traffic passing through NetScaler. HDX Insight enables administrators to view real-time client and network latency metrics, historical reports, End-to-end performance data, and troubleshoot performance issues.
Gateway Insight	Gateway Insight provides visibility into the failures encountered by all users, regardless of the access mode, at the time of logging on to NetScaler Gateway.
Security Insight	Security Insight provides a single-pane solution to help you assess your application security status and take corrective actions to secure your applications.
SSL Insight	SSL Insight provides visibility into secure web transactions (HTTPS) and allows IT administrators to monitor all the secure web applications being served by the NetScaler by providing integrated and real-time and historic monitoring of secure web transactions.

Dashboards

NetScaler Console provides two dashboards, the **Outbound Traffic Dashboard** and **User Dashboard**. These dashboards display multiple charts that summarize the websites or applications accessed from the enterprise network and also the activities performed by the users in your network.

Outbound traffic dashboard

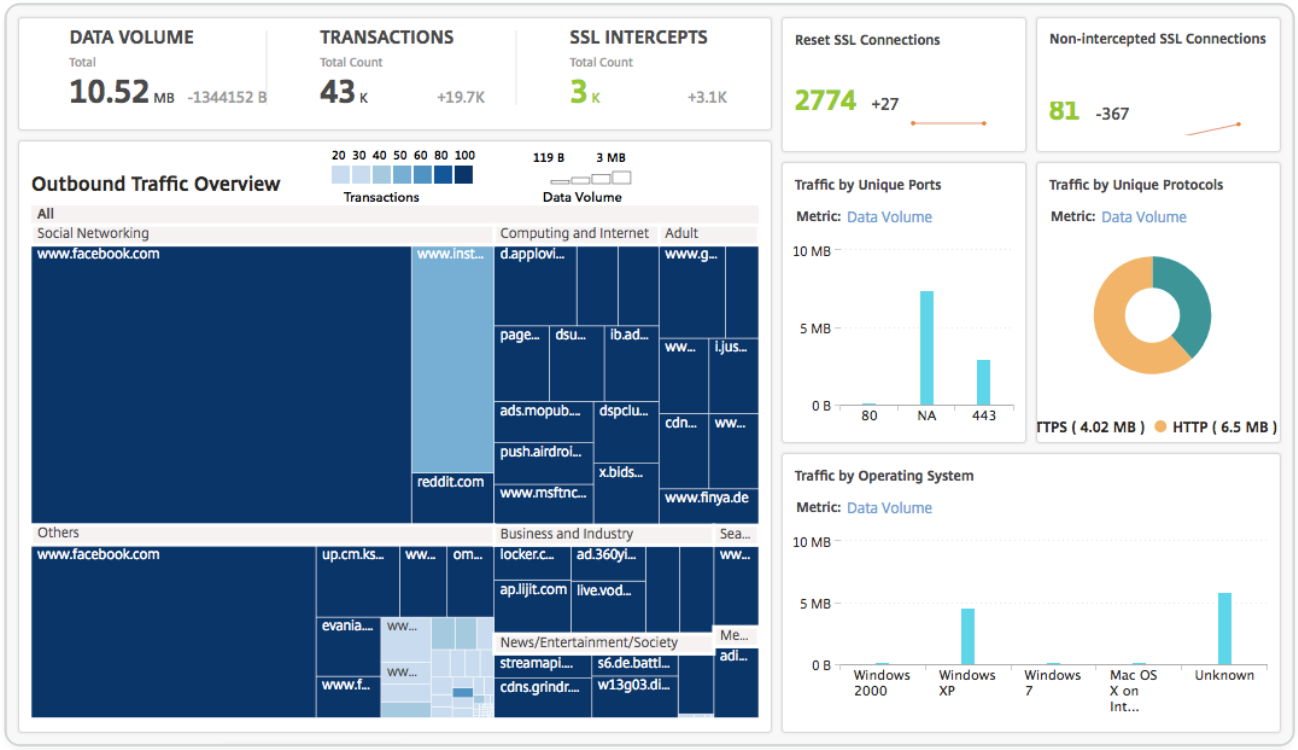
The **Outbound Traffic Dashboard** provides a summary of the URLs or Domains accessed from your network. It provides a holistic view of the all the URLs or Domains by number of transactions or data volume consumed by the URLs or Domains. It also provides details such as the following:

1. Amount of bandwidth consumed by the URLs or domains accessed from your network.
2. Number of transactions that occurred while accessing the URLs and domains from your network.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Number of SSL connections intercepted by the NetScaler appliance during the transactions.
4. Number of SSL connections not intercepted by NetScaler appliance during the transactions.
5. Number of SSL connections reset by the NetScaler appliance during the transactions.
6. Amount of web traffic transmitted, based on the port used to transmit the traffic, the protocol used by the web traffic, and the client operating systems used to transmit the traffic.

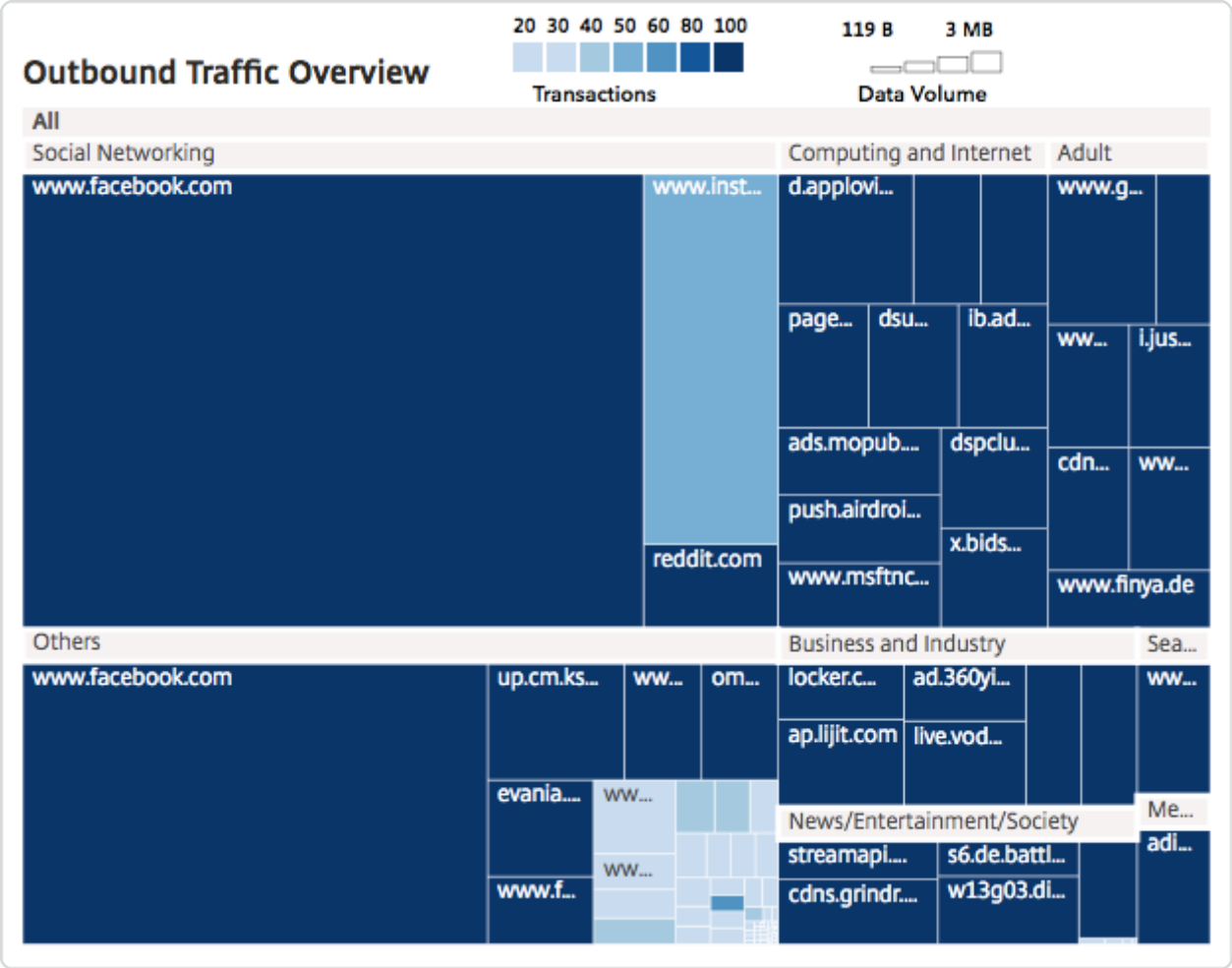
To access the Outbound Traffic Dashboard, navigate to **Security > Users & Endpoints > Outbound Traffic Dashboard**.



View the outbound traffic from the network

The **Outbound Traffic Dashboard** includes an **Outbound Traffic Overview** pane. In the **Outbound Traffic Overview** pane, NetScaler Console groups the accessed URLs or domains into categories, such as Shopping, News, Social Networking, and so on. The **Outbound Traffic Overview** pane displays the URLs or domains accessed from your network as nodes in the URL categories. The nodes are sized according to the data volume consumed by accessing the URL or domain. The color of the node indicates the number of transactions that occurred while accessing the URL or domain.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can click a category to filter the charts to display details related the category for the specified time frame.

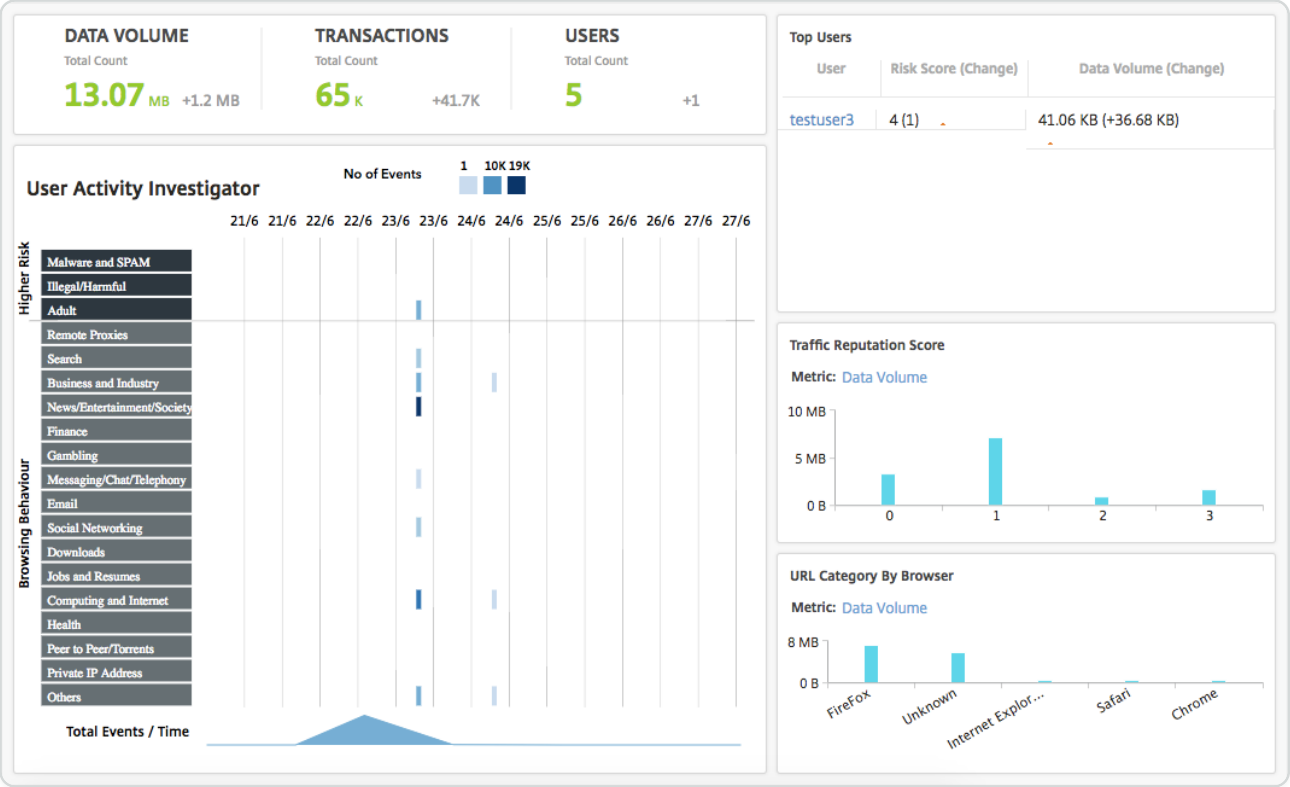
User dashboard

The **User Dashboard** displays a summary of the activities performed by the users in your enterprise. It provides key metrics that you can use to determine the following:

1. Browsing behavior of users in your enterprise.
2. URL categories accessed by the users in your enterprise.
3. Top five users, based on their risk scores and the bandwidth they consume. For more information about risk score, see Risk Score.
4. Browsers used to access the URLs or domains.
5. Amount web traffic generated by the users, based on the traffic reputation score.

To access the **User Dashboard**, navigate to **Users > Dashboard**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



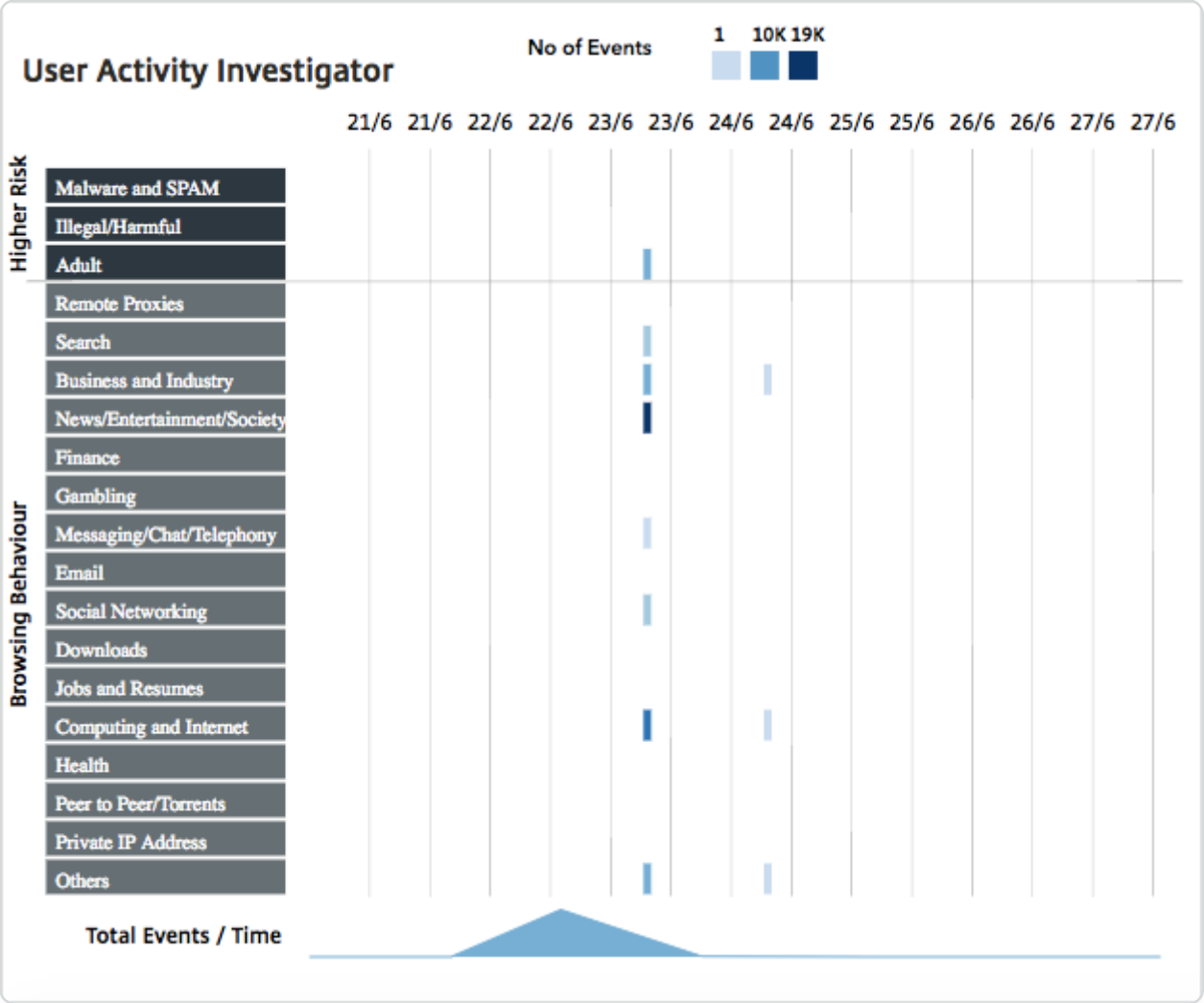
You can click a user in the **Top Users** pane to filter the charts to display details of the web activity performed by the user in the specified time frame.

User activity investigator

The **User Dashboard** includes a **User Activity Investigator** pane displaying various web activities performed by the users. It shows the URL categories accessed by the users during the selected time frame, and various events triggered per URL category. You can click the events to get the transaction level details.

The **User Activity Investigator** displays key information such as browsing behavior of the user, high risk activity by the user, and triggered events, per URL category. The events are shown as rectangular legends on the chart. Each of the legends is aggregated at one-minute intervals if the selected duration is one hour, and at one-hour intervals if the selected duration is one day.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



These legends are aggregated, and are color coded according to the number of events that have occurred. You can hover your mouse pointer on a legend to show details such as time and the number of events aggregated for the selected legend. You can customize the time period of the graph by selecting a time from the time-period list.

You can click the events to further drill down for the details of the transactions.

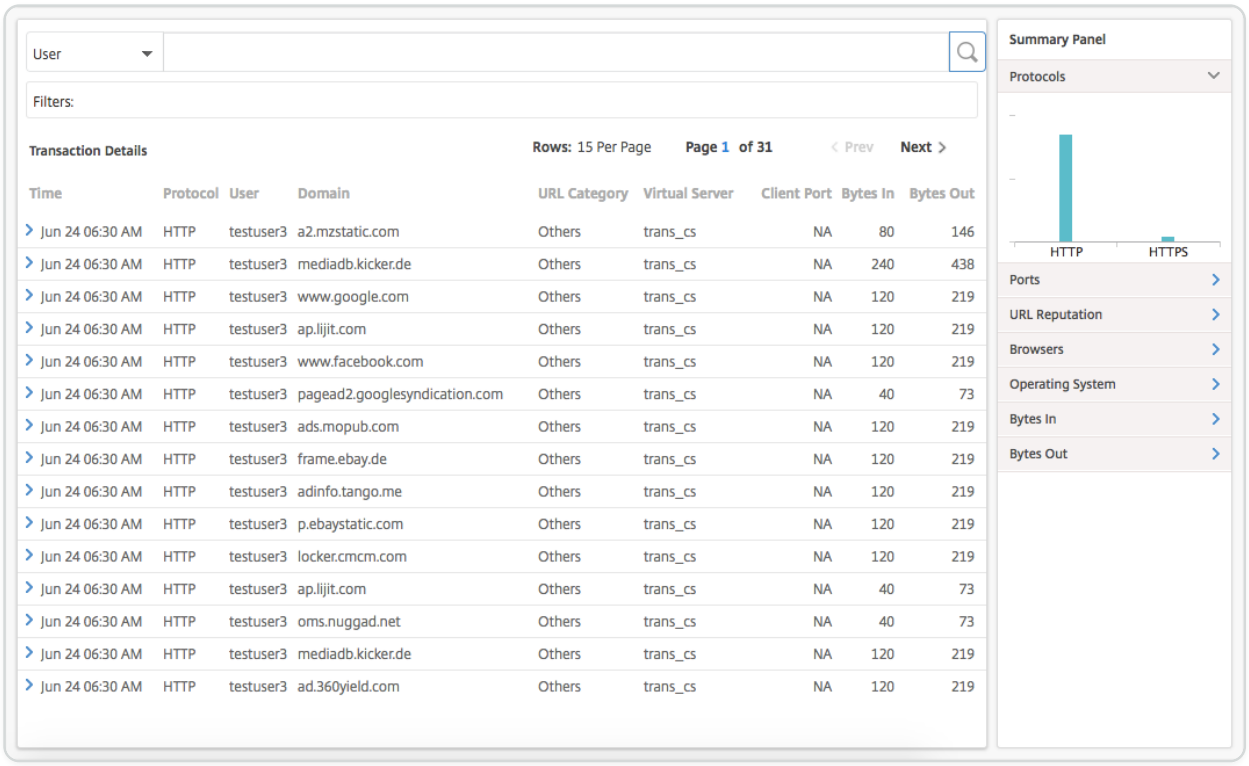
User transactions

The User Transactions page displays the details of the user transactions in your network. It provides transaction-level details such as:

1. Time at which the transaction occurred
2. Protocol used for the transaction
3. User name
4. Domain accessed by the user
5. URL category
6. Proxy server used to intercept the transaction

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. Client port details
8. Bytes In
9. Bytes Out



SUMMARY PANEL

The **Summary Panel** displays all the metrics of the transactions that are visible in the **Transaction Details** pane. This panel enables you to sort and view the transactions in the **Transaction Details** pane by selecting or deselecting the metrics. The **Summary Panel** displays the following metrics:

METRICS	DESCRIPTION
Protocols	Protocols used in the transactions
Ports	Ports used for the transactions
URL Reputation	URL reputation score
Browsers	Browsers used for the transactions
Operation System	Operating system used for the transactions
Bytes In	Amount of data received through the NetScaler Appliance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRICS	DESCRIPTION
Bytes Out	Amount of data sent through the NetScaler Appliance.

Risk score

Risk Score is a scoring system used in NetScaler Console to determine the risks associated with users in your enterprise. NetScaler Console assigns a risk score based on the URL reputation score assigned by the NetScaler appliance for the URLs accessed by the users in your network. For information on URL reputation score, see URL Reputation Score. The following table describes the Risk Scores assigned by NetScaler Console.

RISK SCORE	DESCRIPTION
1	The web activity of the user has no perceived threat or is not abnormal.
2	The web activity of the user has no perceived threat or is not abnormal, but the user is accessing "Unknown Sites," which do not have URL reputation scores.
3	No threat is detected in the web activity of the user, but the user has attempted to access sites that are potentially vulnerable or affiliated with sites that are potentially vulnerable.
4	Potentially compromised user.
5	The web activity of the user is abnormal and the user has accessed known malicious sites.

WAF Insight

Web and web service applications that are exposed to the Internet have become increasingly vulnerable to attacks. To protect applications from attack, you need visibility into the nature and extent of past, present, and impending threats, real-time actionable data on attacks, and recommendations on countermeasures. WAF Insight provides a single-pane solution to help you assess your application security status and take corrective actions to secure your applications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

WAF Insight is supported on NetScaler Console with all NetScaler appliances running on version 11.0 Build 65.31 and later.

How WAF insight works

WAF Insight is an intuitive dashboard-based security analytics solution that gives you full visibility into the threat environment associated with your applications. Security insight is included in NetScaler Console, and it periodically generates reports based on your Application Firewall and NetScaler system security configurations. The reports include the following information for each application:

- **Threat index.** A single-digit rating system that indicates the criticality of attacks on the application, regardless of whether the application is protected by a NetScaler appliance. The more critical the attacks on an application, the higher the threat index for that application. Values range from 1 through 7.

  The threat index is based on attack information. The attack-related information, such as violation type, attack category, location, and client details, gives you insight into the attacks on the application. Violation information is sent to NetScaler Console only when a violation or attack occurs. Many breaches and vulnerabilities lead to a high threat index value.
- **Safety index.** A single-digit rating system that indicates how securely you have configured the NetScaler instances to protect applications from external threats and vulnerabilities. The lower the security risks for an application, the higher the safety index. Values range from 1 through 7.

  The safety index considers both the application firewall configuration and the NetScaler system security configuration. For a high safety index value, both configurations must be strong. For example, if rigorous application firewall checks are in place but NetScaler system security measures, such as a strong password for the `nsroot` user, have not been adopted, applications are assigned a low safety index value.
- **Actionable information.** The information that you need for lowering the threat index and increasing the safety index, which significantly improves application security. For example, you can review information about violations, existing and missing security configurations for application firewall and other security features, the rate at which the applications are being attacked.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure WAF insight

NOTE:

You can get started with configuring protections through the **Unified Security** dashboard. For more information, see Unified Security dashboard

1. Navigate to **Infrastructure > Instances > NetScaler** and select the instance type. For example, VPX.
2. Select the instance and from the **Select Action** list, select **Configure Analytics**.
3. On the **Configure Analytics on virtual server** window:

    a. Select the virtual servers that you want to enable security insight and click **Enable Security & Analytics**.

    The **Enable Security & Analytics** window is displayed.

    b. Select **WAF Security Violations**

    c. Under **Advanced Options**, select **Logstream** or **IPFIX** as Transport Mode

    NOTE

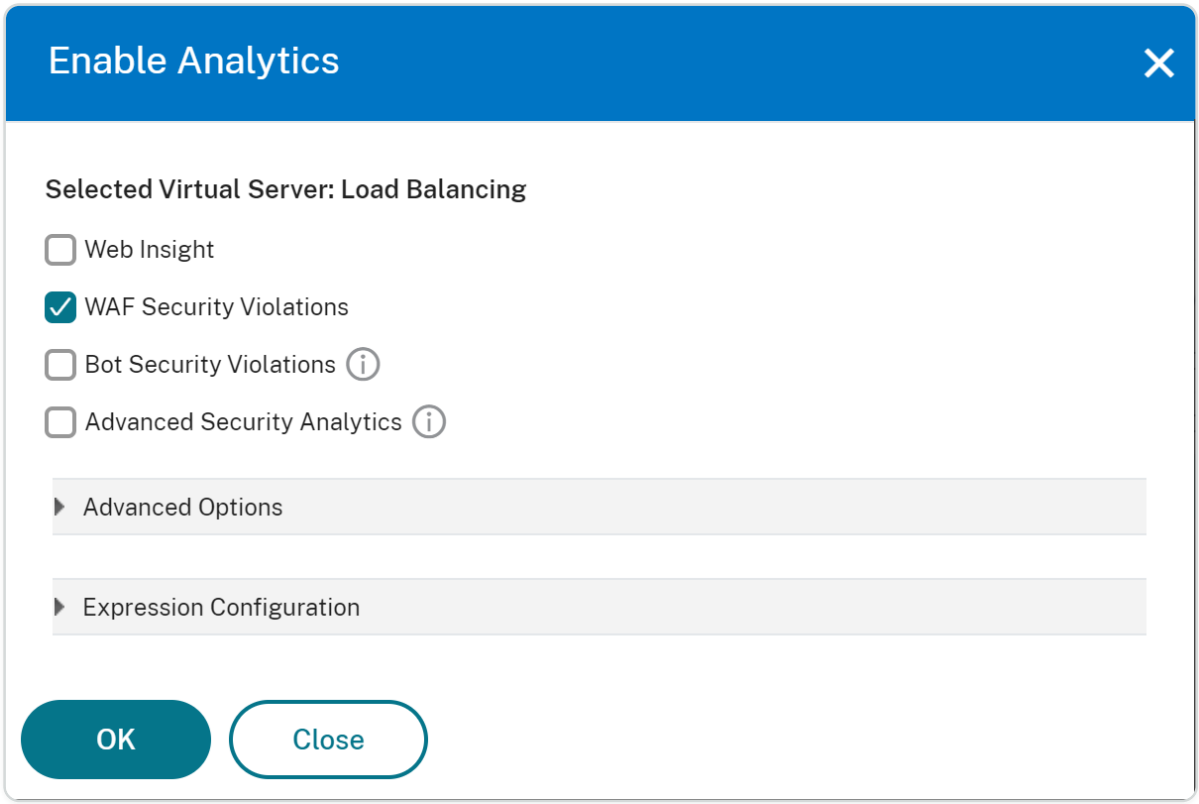
    For NetScaler 12.0 or earlier, **IPFIX** is the default option for Transport Mode. For NetScaler 12.0 or later, you can either select **Logstream** or **IPFIX** as Transport Mode.

    For more information about **IPFIX** and **Logstream**, see **Logstream overview**.

    d. The Expression is true by default

    e. Click **OK**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE

- If you are not on the Flexed license and you select virtual servers that are not licensed, then NetScaler Console first licenses those virtual servers and then enables analytics.

After you click **OK**, NetScaler Console processes to enable analytics on the selected virtual servers.

NOTE

When you create a group, you can assign roles to the group, provide application-level access to the group, and assign users to the group. NetScaler Console analytics now supports virtual IP address based authorization. Your users can now see reports for all Insights for only the applications (virtual servers) that they are authorized to. For more information on groups and assigning users to the group, see Configuring Groups on NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure geo locations for security insight reports

If you configure geo locations in NetScaler Console, WAF Insight reports include the exact geographic locations from which client requests originate. To enable geo locations, specify a private IP block or range of IP addresses for every geographic location in your organization. Add that information in the Geo Database file, along with the city/state/country name and the latitude and longitude coordinates of each location. Contact your NetScaler representative to obtain the Geo Database file, and then upload the file to the NetScaler instance.

To configure geo locations:

1. Copy the Geo Database file, Citrix_Netscaler_InBuilt_GeoIP_DB.csv, to any location on the NetScaler appliance.
2. Open the Geo Database file with a text editor, such as vi editor, and add an entry for every location in your organization.

   The entry must be in the following format:

   ```
   <start IP\>,<end IP\>,,<country\>,<state\>,,<city\>,,longitude,latitude
   ```

   For example,

   ```
   4.17.142.224,4.17.142.239,,US,New York,,Harrison,,73.7304,41.0568
   ```
3. Run the following commands to enable geo-location logging and logging in the CEF format:
   - **add locationFile** <Complete path with DB file\>
   - **set appfw settings** -geoLocationLogging ON
   - **set appfw settings** -CEFLogging ON

Monitor IP reputation

The IP Reputation feature provides attack-related information about malicious IP addresses. For example, it reports IP Reputation Score, IP Reputation category, IP Reputation attack time, Device IP, and details about the Client IP address.

IP Reputation score indicates the risk associated with an IP address. The score has the following ranges:

IP REPUTATION SCORE	LEVEL OF RISK
1–20	High Risk

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IP REPUTATION SCORE	LEVEL OF RISK
21–40	Suspicious
41–60	Moderate Risk
61–80	Low Risk
81–100	Trustworthy

To monitor IP Reputation:

1. Navigate to **Security > Security Violations**, and under **WAF**, select the application you want to monitor.
2. The **Threat Index** and **Safety Index** scores are displayed. Click **View Details**.
3. Under Application Firewall Configuration, you can view the IP reputation safety index score.

Thresholds

You can set and view thresholds on safety index and threat index of applications in WAF Insight.

To set a threshold:

1. Navigate to **Settings > Analytics Settings > Thresholds**, and select **Add**.
2. Select the traffic type as **Security** in the Traffic Type field, and enter required information in the other appropriate fields such as Name, Duration, and entity.
3. In the **Rule** section, use the Metric, Comparator, and Value fields to set a threshold.

   For example, "Threat Index" ">" "5"
4. Click **Create**.

WAF insight use cases

The following use cases describe how you can use security insight to assess the threat exposure of applications and improve security measures.

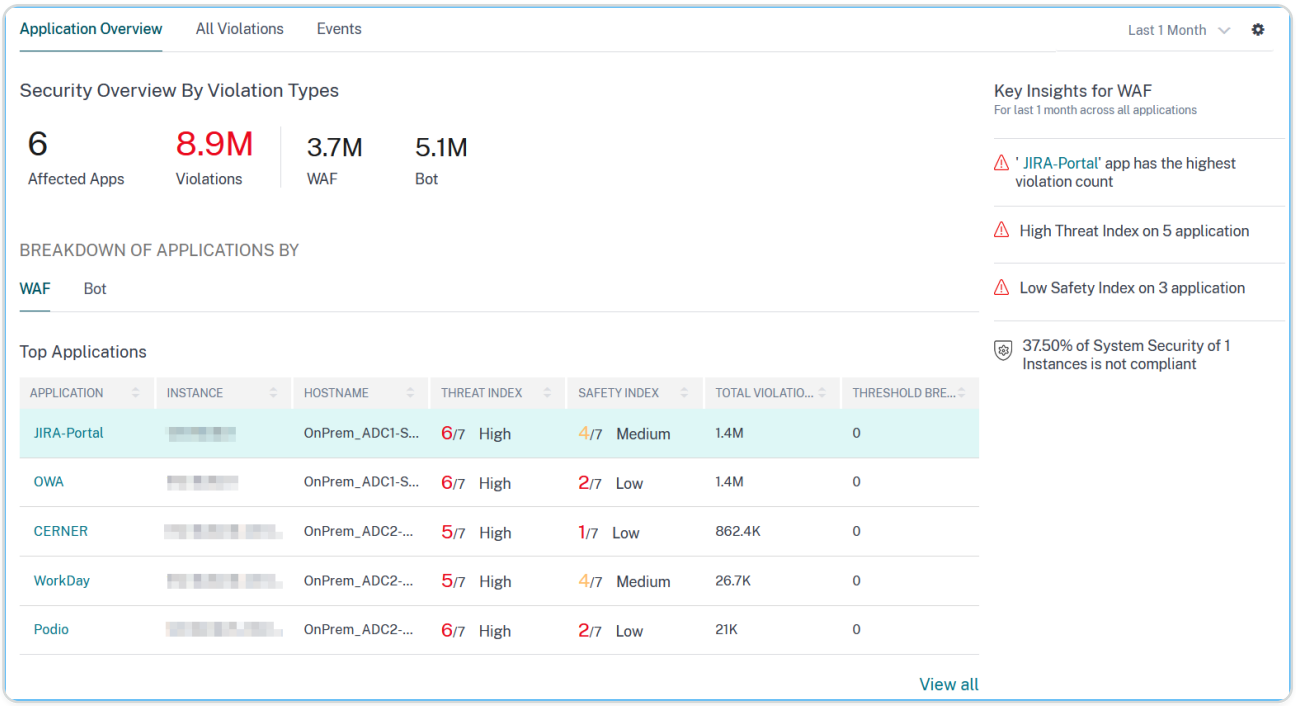
Obtain an overview of the threat environment

In this use case, you have a set of applications that are exposed to attacks, and you have configured NetScaler Console to monitor the threat environment. You must review the threat index, safety index, and the type and severity of any attacks that the applications might have experienced to focus first on the critical applications. The security insight dashboard provides a summary of the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

threats experienced by your applications over a time period of your choosing, and for a selected NetScaler device. It displays the list of applications, their threat and safety indexes, and the total number of attacks for the chosen time period.

To obtain a summary of the threat environment, log on to NetScaler Console, and then navigate to **Security > Security Violation** and under **WAF**, the top five applications are displayed based on the total violations affected. To view all applications, you can click **View All**.



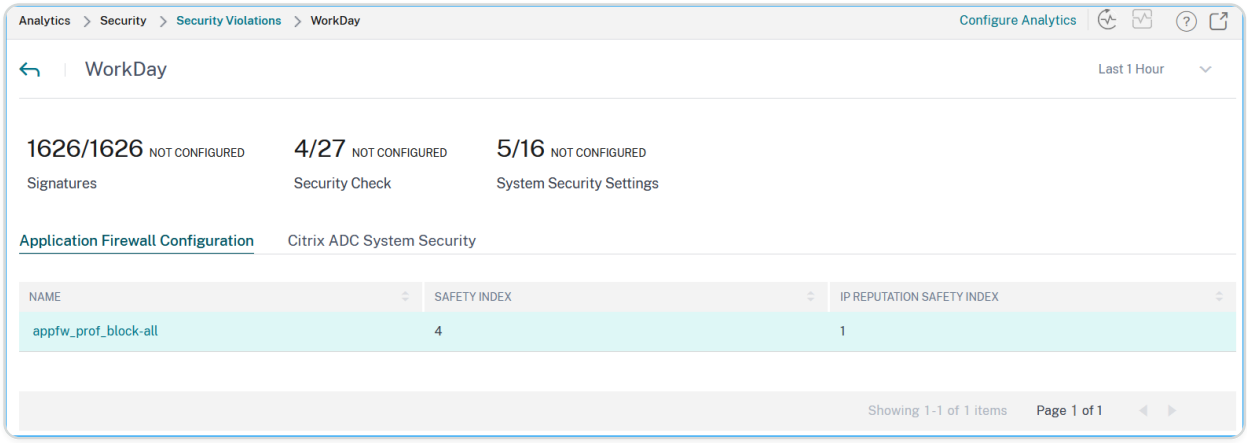
Determine the existing and missing security configuration for an application

After reviewing the threat exposure of an application, you want to determine what application security configurations are in place and what configurations are missing for that application. You can obtain this information by drilling down into the application summary.

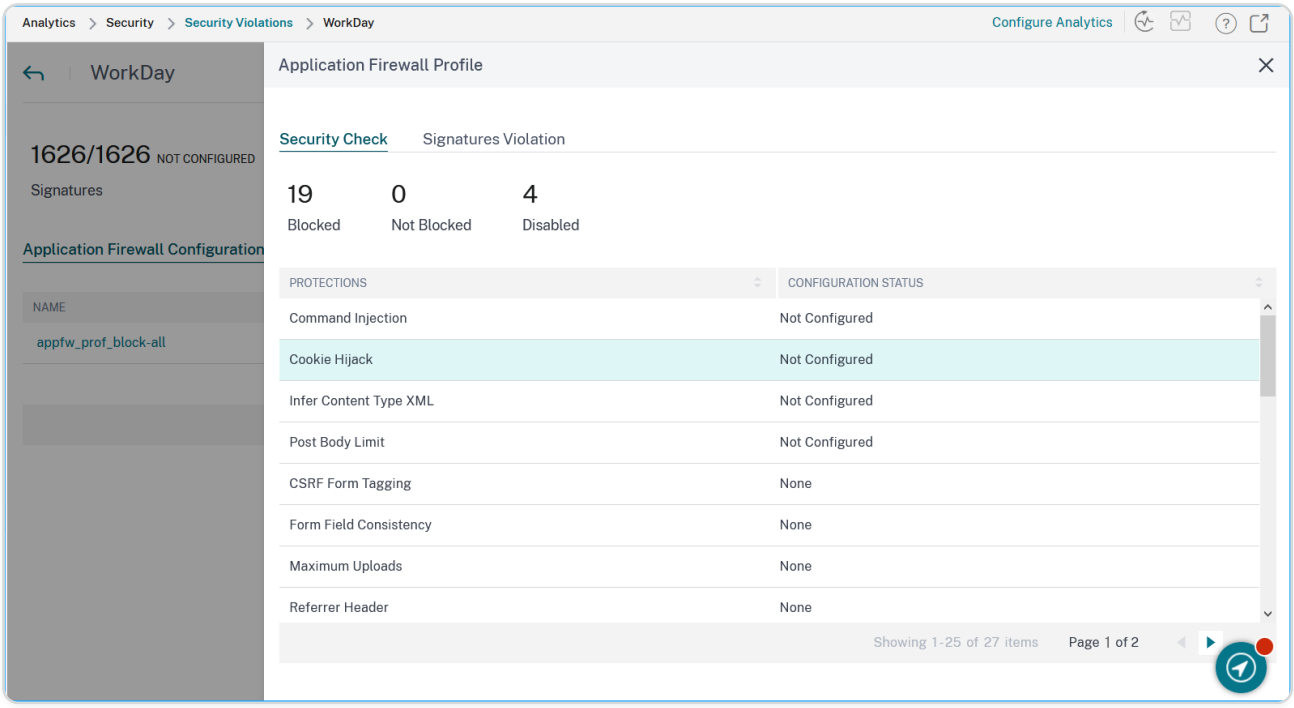
The summary gives you information about the effectiveness of the following security configurations:

- **Application Firewall Configuration.** Shows how many signature and security entities are not configured.
- **NetScaler Console System Security.** Shows how many system security settings are not configured.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



On the **Application Firewall Configuration** node, review the security check and security violation information.



Click the **NetScaler Console System Security** node and review the system security settings and Citrix recommendations to improve the application safety index.

Identify applications that require immediate attention

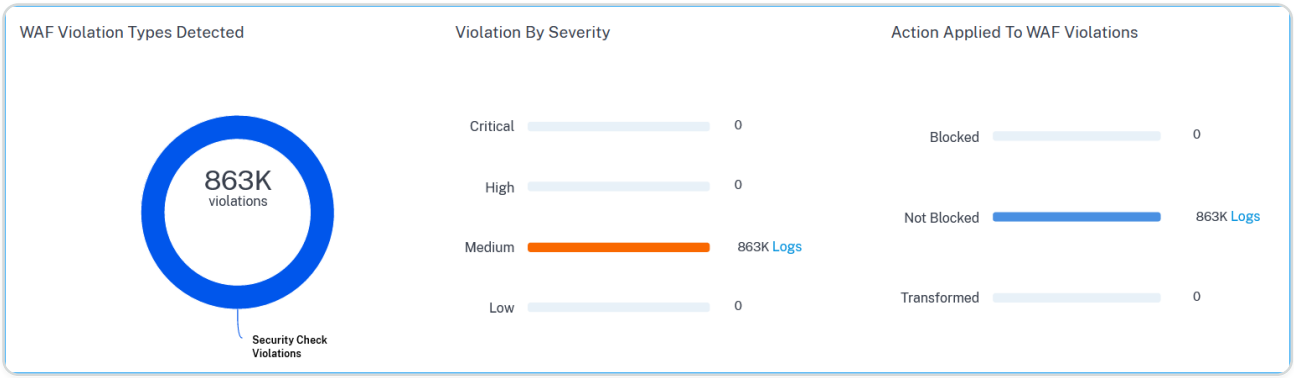
The applications that need immediate attention are the applications having a high threat index and a low safety index.

Determine the number of attacks in a given time

You might want to determine how many attacks occurred on a given application at a given point in time, or you might want to study the attack rate for a specific time period.

Under **WAF**, click any application to view the total WAF violations detected for the selected duration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Click **Logs** to view details for attacks based on severity and action taken. The logs page provides the following details:

- Attack time
- IP address of the client from which the attack happened
- Severity
- Category of violation
- URL from which the attack originated, and other details.

Configure the learning profile

You must configure a learning profile in NetScaler Console and select the **NetScaler profiles** to generate the relaxation rules list. Depending upon the traffic, you can configure profiles on NetScaler instances and configure a learning profile in NetScaler Console.

NOTE

Currently you can configure only 25 profiles.

You can configure learning profiles to generate the relaxation rules list for the selected:

- **Web applications** – Enables you to select the application for which you want to create the relaxation rules.
- **Profile names** – Enables you to select the WAF profile for which you want to create the relaxation rules.

After you create the learning profile, if NetScaler receives no incoming traffic for the configured security checks, you can also configure to remove the relaxation rules from NetScaler Console.

To configure a learning profile:

1. Navigate to **Security** > **WAF Learning** > **Learn Profiles**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Click **Add**.



3. In the **Add Profile Configuration** page, specify the following parameters:

   a. **Learn Profile Name** – Specify a name of your choice.

      Select the **Enable** option. By default, this option is selected. If you disable this option, the profile will not be active.

   b. **Learn Behavior** – Select the learn behavior to generate rule, remove rule, or both

      i. **Learn Rules** – Generates the exception rule and enables the administrator to either deploy or skip.

      ii. **Remove Idle Rules** – Removes the exception rule, when the configured idle time exceeds the threshold.

      iii. **Learn Rules & Remove Idle Rules** – Generates the exception rules and also removes when there is no incoming traffic

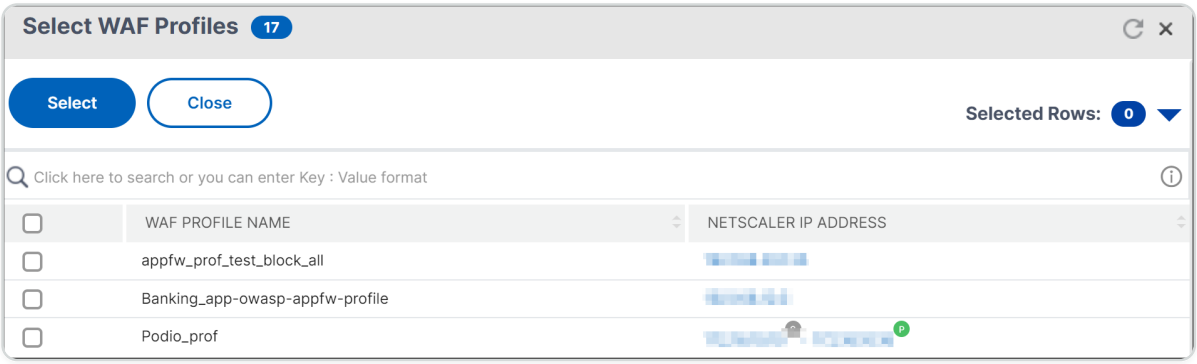
      NOTE

      - Remove rule option is only supported for **Start URL**, **Deny URL**, **HTML Cross-Site Scripting**, and **HTML SQL Injection** security checks.
      - When you select **Remove Rule** option, the supported security checks options are displayed.

   c. **Learning Group** – Select either **Profile Based** or **Application Based**.

   d. **Select WAF Profile** – This option is displayed when you select **Profile Based**. Select the required WAF profiles based on applications or profile names.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



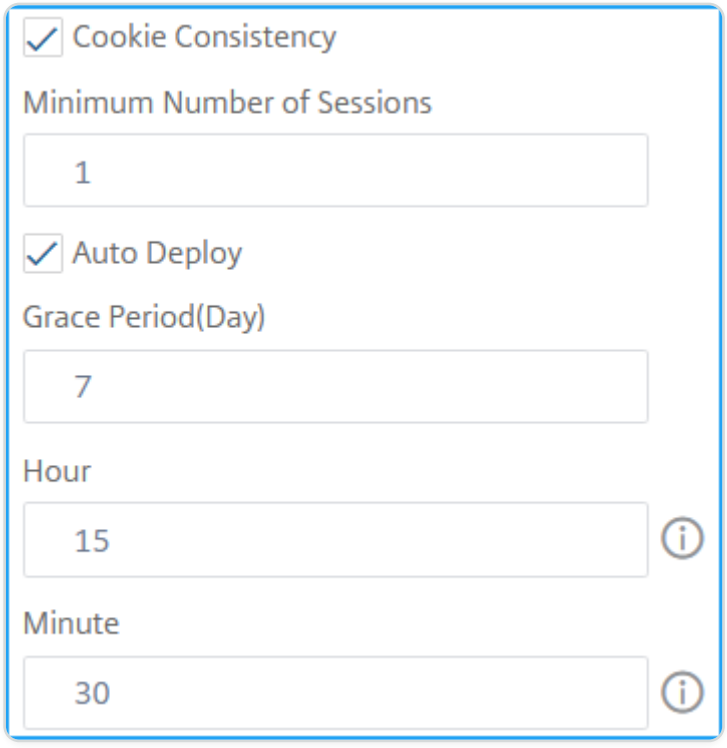
e. **Select Applications** - This option is displayed when you select **Application Based**. Select and add the applications from the list.

f. Under **Security Check**, select the security checks options that you want to take action for the violations reported in NetScaler Console. When you select an option, you must provide the following information:

   i. **Minimum number of sessions** – Specify the sessions. NetScaler Console monitors for the specified sessions to be occurred on the NetScaler instance to report it in the relaxation list.

   ii. **Auto Deploy** - This option enables the administrators to take an action (deploy or skip). You must specify the grace period (days, hour, and minute format), for which NetScaler Console will hold these violations in the Relaxation Rules list.

   The maximum grace period that you can specify is 30 days.



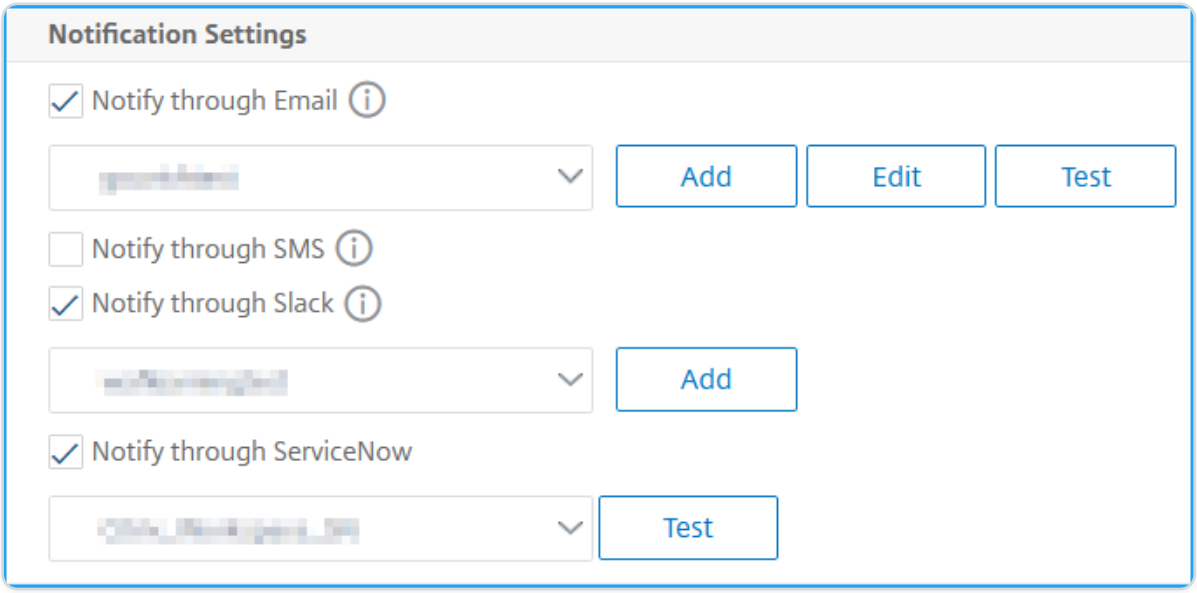
© 1997–2026 Citrix Systems, Inc. All rights reserved.

iii. If you have selected **Remove Rule** option, specify the **Idle Time (Day)** in days and hours. After this time period, if NetScaler receives no incoming traffic for this security check, the rule is automatically removed.

By default, the idle time is 7 days, but you can configure this time as no lesser than 23 hours.

g. On the **Notification Settings**, select the notification options that you want to get the violations notified. The available notification options are email, SMS, Slack, and ServiceNow.

After you select the notification options, you can either select from the existing distributed profile or create a profile.



h. Click **Create**.

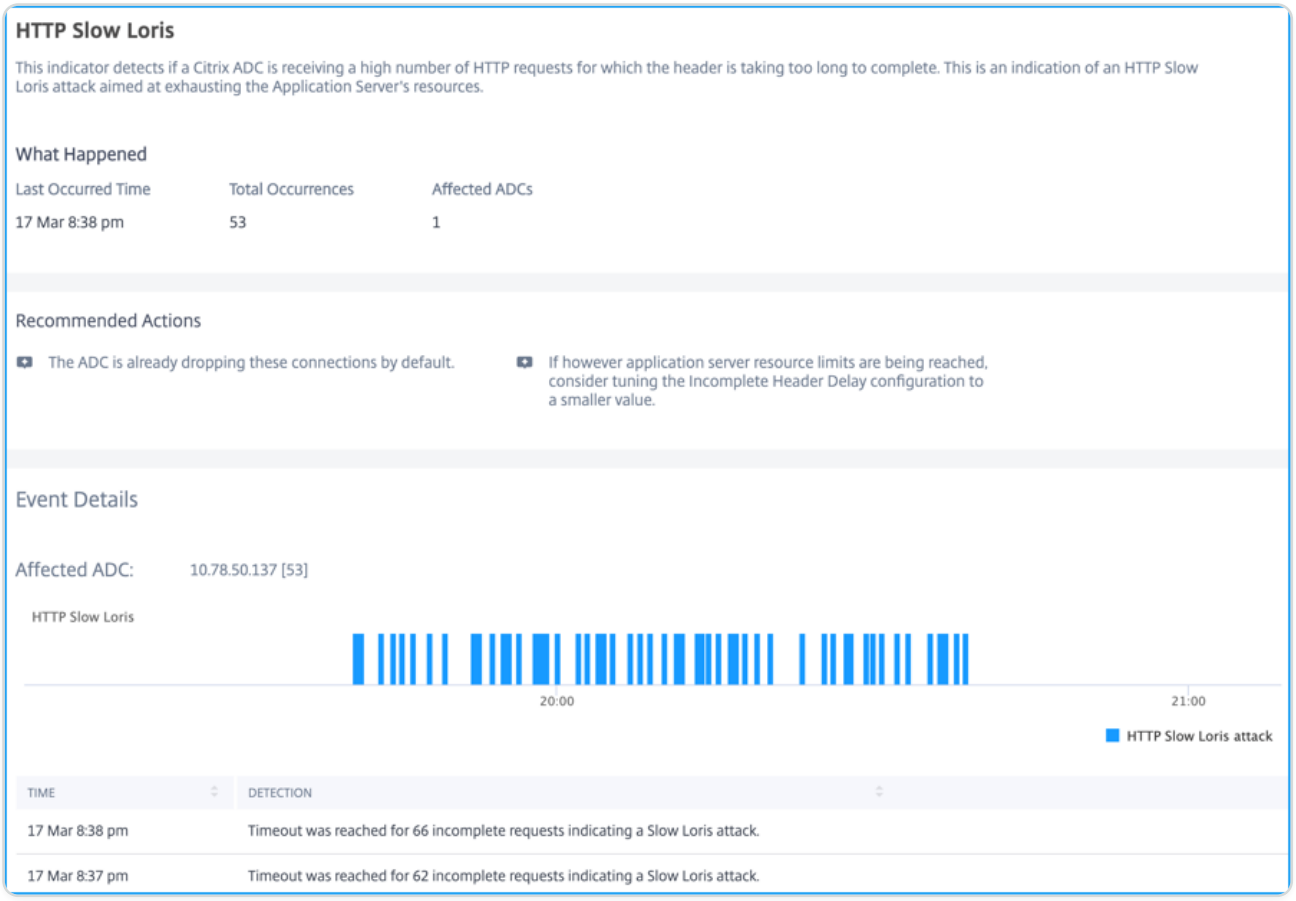
Network violation details

HTTP Slow Loris

Slow loris is a denial-of-service attack that can send HTTP headers to the target application as slow as possible. The target application is forced to wait for headers arrival and can also quickly become unavailable to handle requests if multiple similar connections get opened. When a NetScaler instance receives a high volume of HTTP requests, the HTTP header increases and takes a long time to complete the requests. This process can exhaust application server resources and result in **HTTP Slow Loris** attack.

Using the **HTTP Slow Loris** indicator, you can analyze the requests that are resulted in **HTTP Slow Loris** attack.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **Recommended Actions** to troubleshoot the issue:

- Consider tuning the incomplete Header Delay (incompHdrDelay) configuration to a smaller value.
- By default, the NetScaler instance drops these incomplete requests.

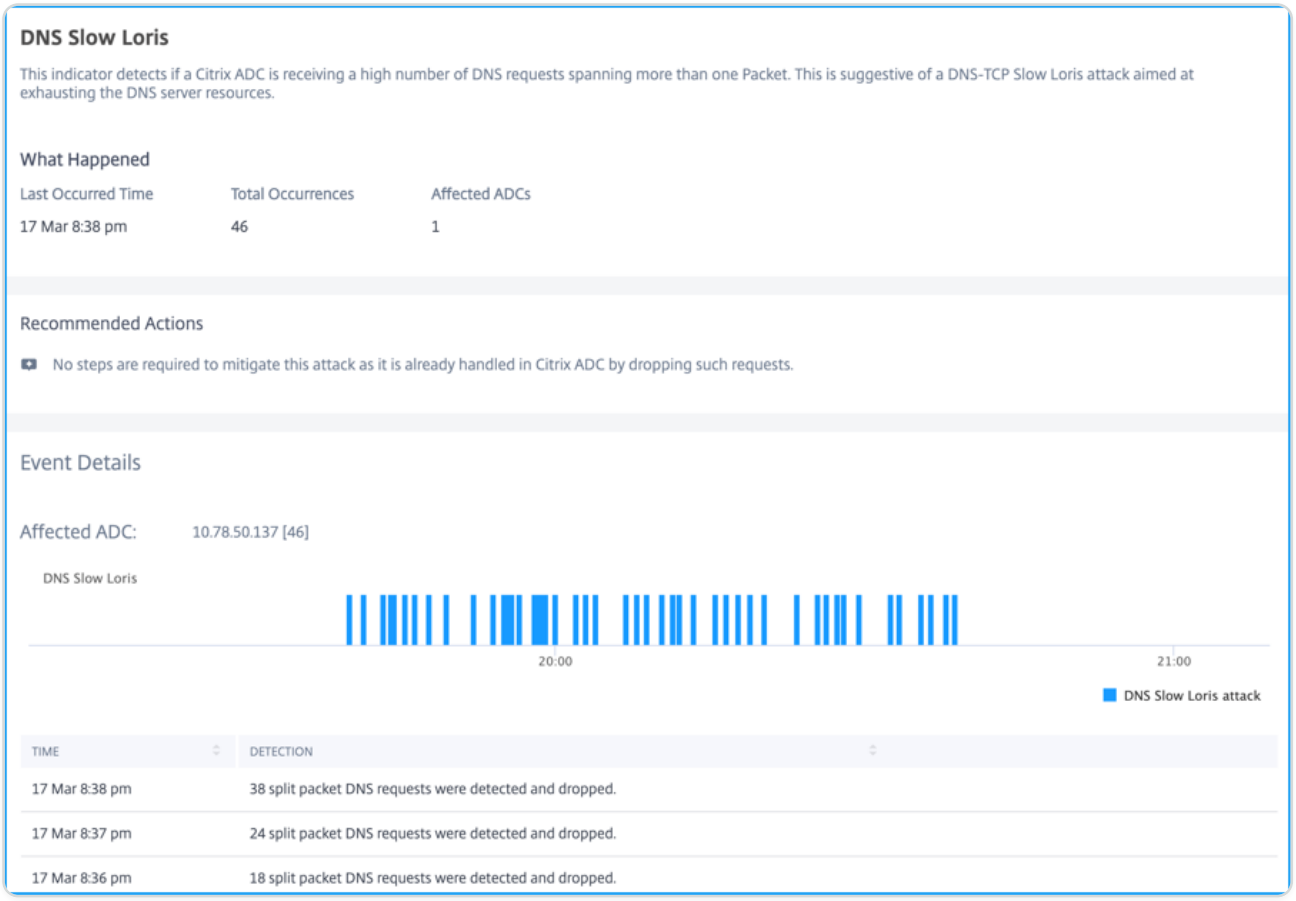
Under **Event Details**, you can view:

- The affected application. You can also select the application from the list if two or more applications are affected with violations.
- The graph indicating all violations
- The violation occurrence time
- The detection message indicating the total incomplete requests as **slow loris** attack

DNS Slow Loris

The **DNS Slow Loris** indicator detects when a NetScaler receives a high number of DNS requests spanning more than one packet. This process can exhaust DNS server resources and result in **DNS Slow Loris** attack. By default, NetScaler instance drops these **DNS slow loris** requests and no further action is required to troubleshoot this issue.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Under **Event Details**, you can view:

- The affected application. You can also select the application from the list if two or more applications are affected with violations.
- The graph indicating all violations
- The violation occurrence time
- The detection message indicating the total DNS requests as **slow loris** attack

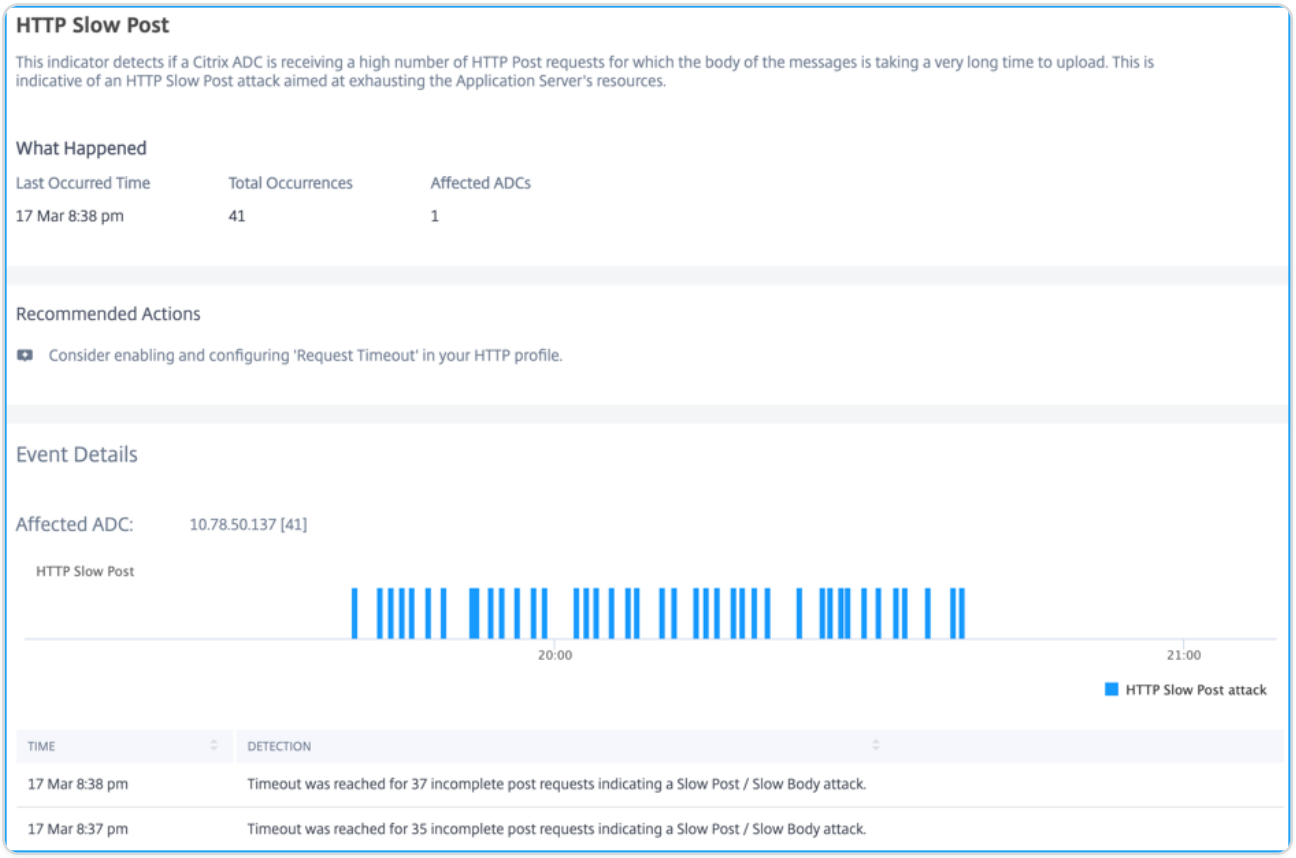
HTTP Slow Post

The **Slow Post** is a Denial-of-Service attack that can send HTTP POST headers to a target application. In the headers, the body message sizes are specified correct, but the message body is sent at a low speed. The target application is forced to wait and can also quickly become unavailable to handle requests if multiple similar connections get opened.

This process can exhaust application server resources and result in **HTTP Slow Post** attack.

Using the **HTTP Slow Post** indicator, you can analyze the requests that are resulted in slow post attack.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **Recommended Action** to troubleshoot this issue to enable and configure Request Timeout in NetScaler HTTP profile. For more information, see HTTP Configurations.

Under **Event Details**, you can view:

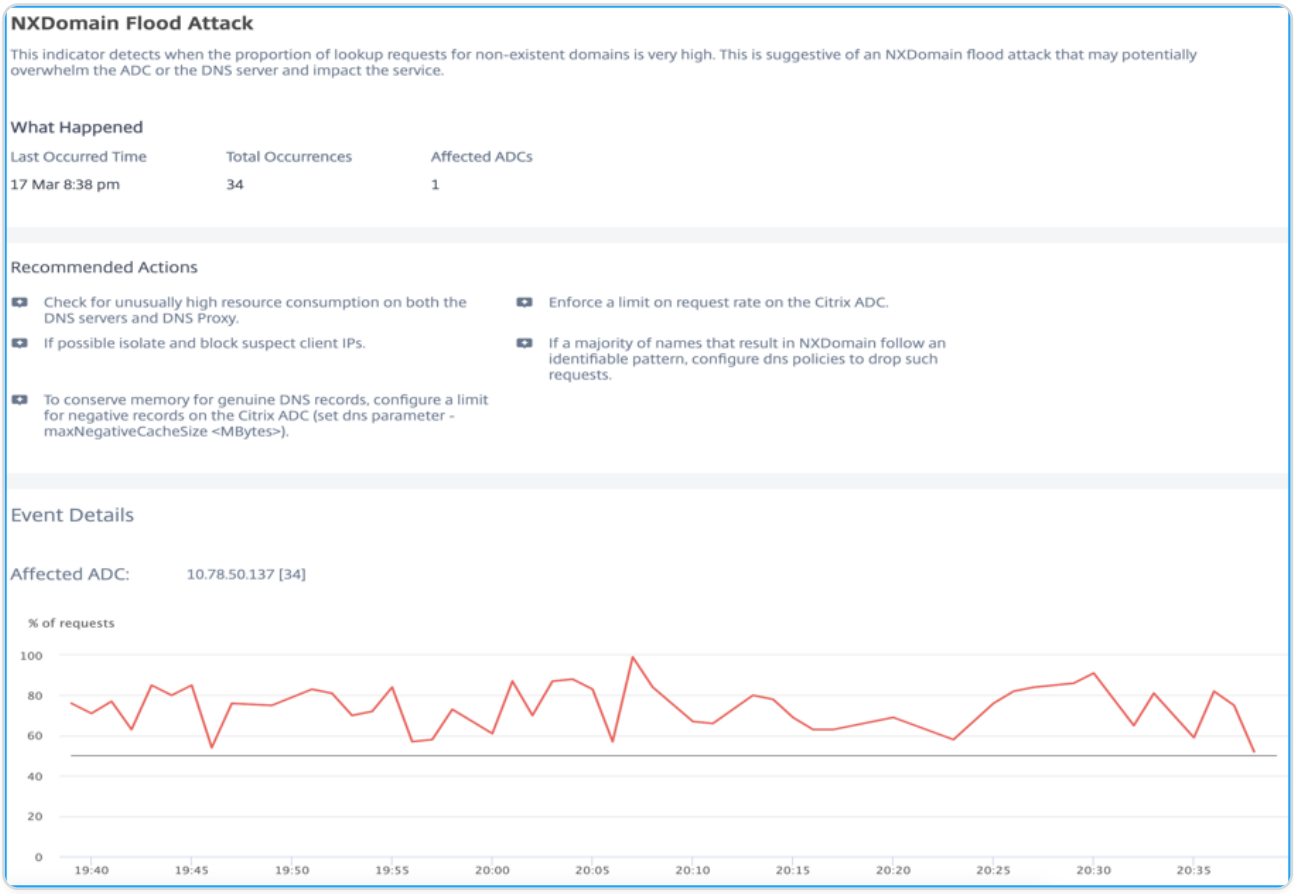
- The affected application. You can also select the application from the list if two or more applications are affected with violations.
- The graph indicating all violations
- The violation occurrence time
- The detection message indicating the total POST requests as **slow loris** attack

NXDOMAIN Flood Attack

The **NXDOMAIN Flood Attack** is a distributed denial-of-service (DDoS) attack that can target a DNS server or a NetScaler instance (that is configured as a DNS proxy server) and send a high volume of non-existence or invalid requests. This attack can impact the DNS server or NetScaler instance resulting in slowdown or requests not getting a response.

Using the **NXDOMAIN Flood Attack** indicator, you can analyze if the requests are resulted in NXDOMAIN attack.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **Recommended Actions** to troubleshoot the issue:

- Check for unusually high resource consumption on both DNS server and DNS proxy server.
- Enforce a limit for request rate on NetScaler instance
- Isolate and block suspect client IP addresses
- If most names result in NXDOMAIN, follow an identifiable pattern and configure DNS policies to drop such requests
- To conserve memory for genuine DNS records, configure a limit for negative records on NetScaler instance. For more information, see Mitigate DNS DDoS attacks.

Under **Event Details**, you can view:

- The affected application. You can also select the application from the list if two or more applications are affected with violations.
- The graph indicating all violations

HTTP Desync Attack

In an HTTP desync attack, a single HTTP request is interpreted as:

- A single request to the front-end server (virtual server)

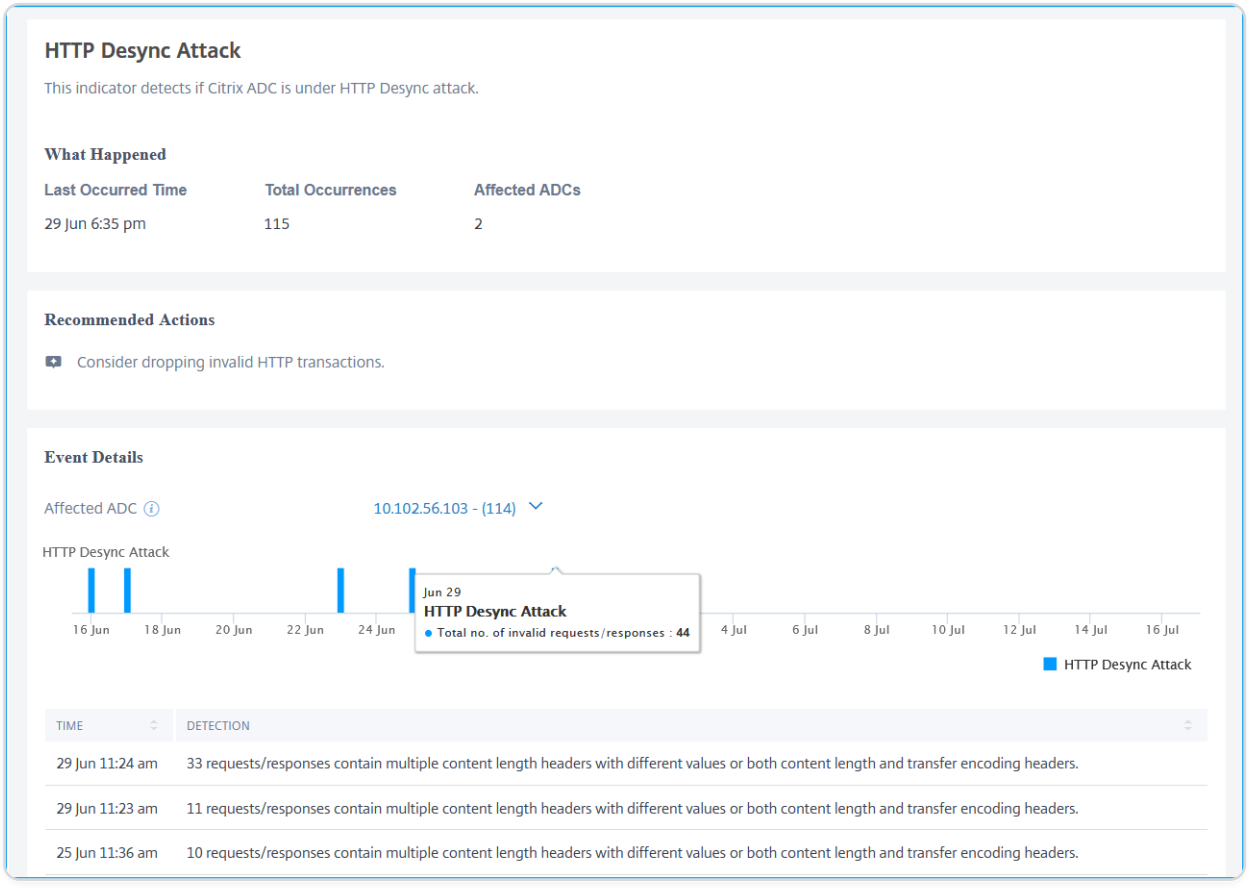
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 2 requests to the back-end server

In this scenario, the back-end server interprets the second request is from a different client. The connection between the virtual server and back-end server is reused for different requests. If the first client request is processed from a malicious client with some malicious data, the next client request can have a customized request. This activity can cause an attack by misusing the combination of two headers; content length and transfer encoding.

Using the **HTTP Desync Attack** indicator, you can analyze if the NetScaler instance might be under HTTP desync attack that has occurred due to the presence of:

- Content length and transfer encoding headers in a single HTTP transaction
- Multiple content-length headers with different values in a single HTTP transaction



The **Recommended Action** suggests you to consider dropping invalid HTTP transactions.

Under **Event Details**, you can view:

- The affected application. You can also select the application from the list if two or more applications are affected with this violation.
- The graph indicating the violation details. Hover the mouse pointer on the bar graph to view the total invalid requests/reponses.

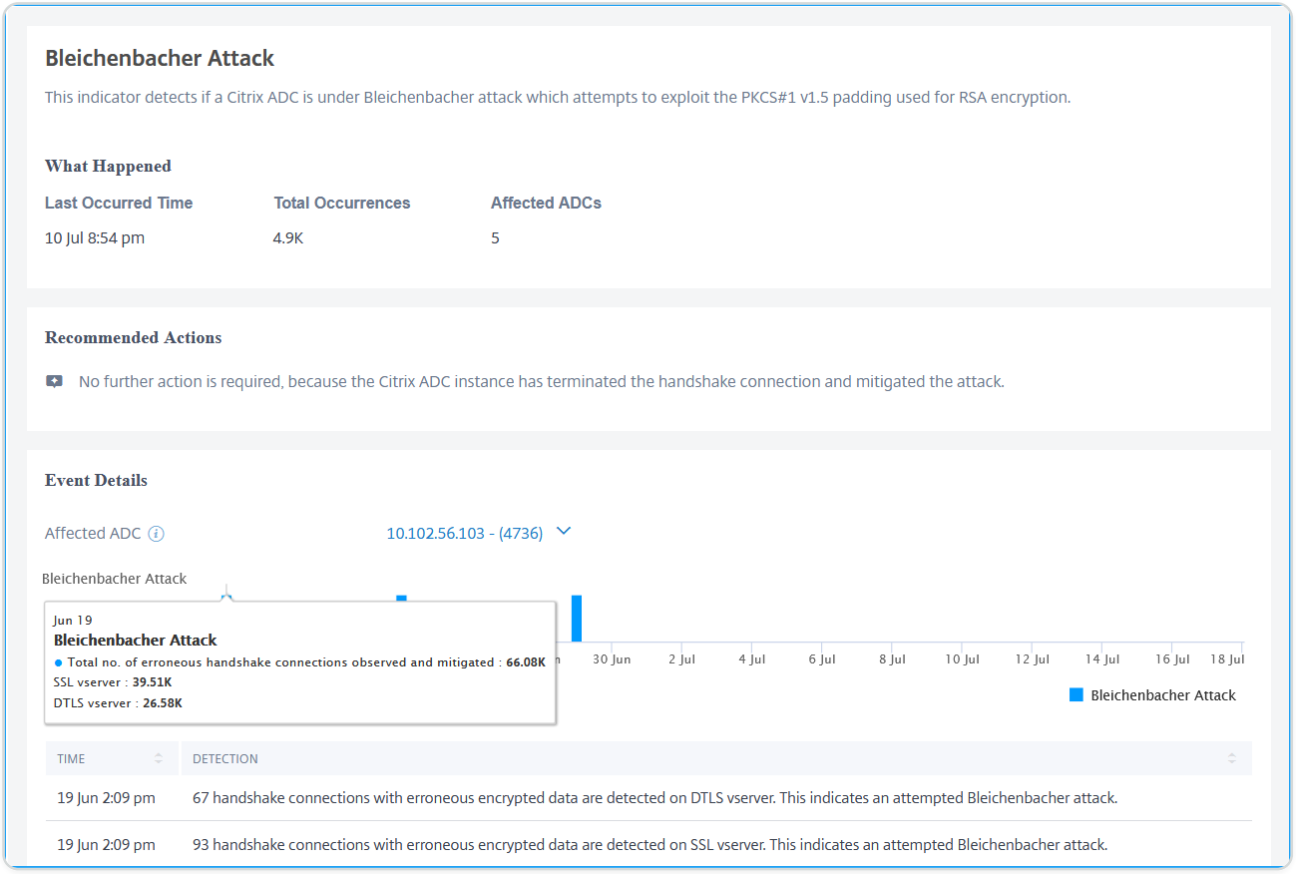
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The detection message for the violation, indicating the total requests/responses:
  - Containing multiple content-length headers with different values
  - Containing both content length and transfer encoding headers

Bleichenbacher Attack

NetScaler instance detects if a given sequence of bytes of an encrypted message has the correct padding format upon decryption.

Using the **Bleichenbacher Attack** indicator, you can analyze if the NetScaler instance receives any SSL/TLS handshake connections with erroneous encrypted data.



The **Recommended Action** indicates no further action is required because the NetScaler instance terminates the handshake connections and mitigates this attack.

Under **Event Details**, you can view:

- The affected application. You can also select the application from the list if two or more applications are affected with this violation.
- The graph indicating the violation details. Hover the mouse point on the bar graph to view the total erroneous handshake connections detected.

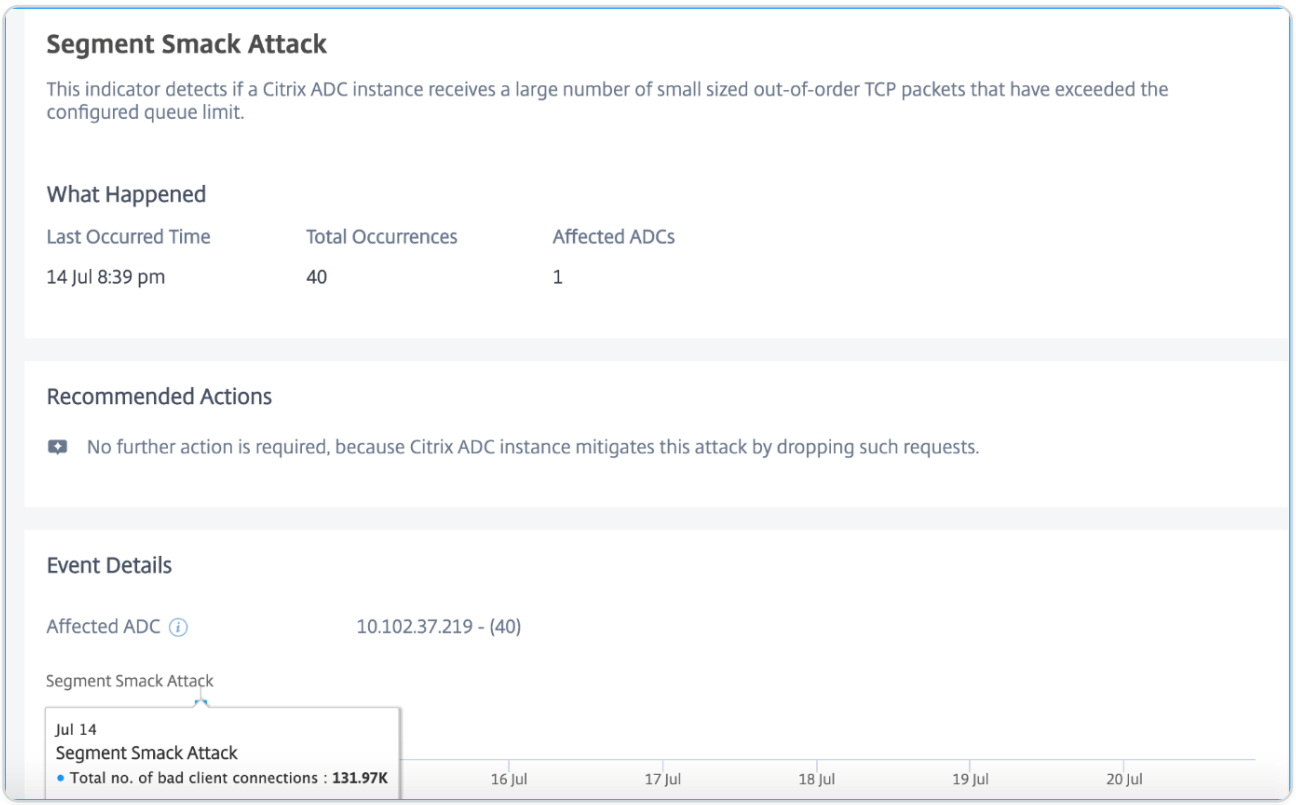
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The detection message for the violation, indicating the total handshake connections on the virtual server with erroneous encrypted data.

Segment Smack Attack

A **Segment Smack Attack** is a Denial of Service (DoS) attack, in which the attacker can send unordered small-sized packets during a TCP session. These customized TCP packets can affect the CPU and Memory, and result in a denial of service on the NetScaler instance.

Using the **Segment Smack Attack** indicator, you can analyze if a NetScaler instance has received a large number of TCP packets than the configured queue limit. For more information, see TCP configuration.

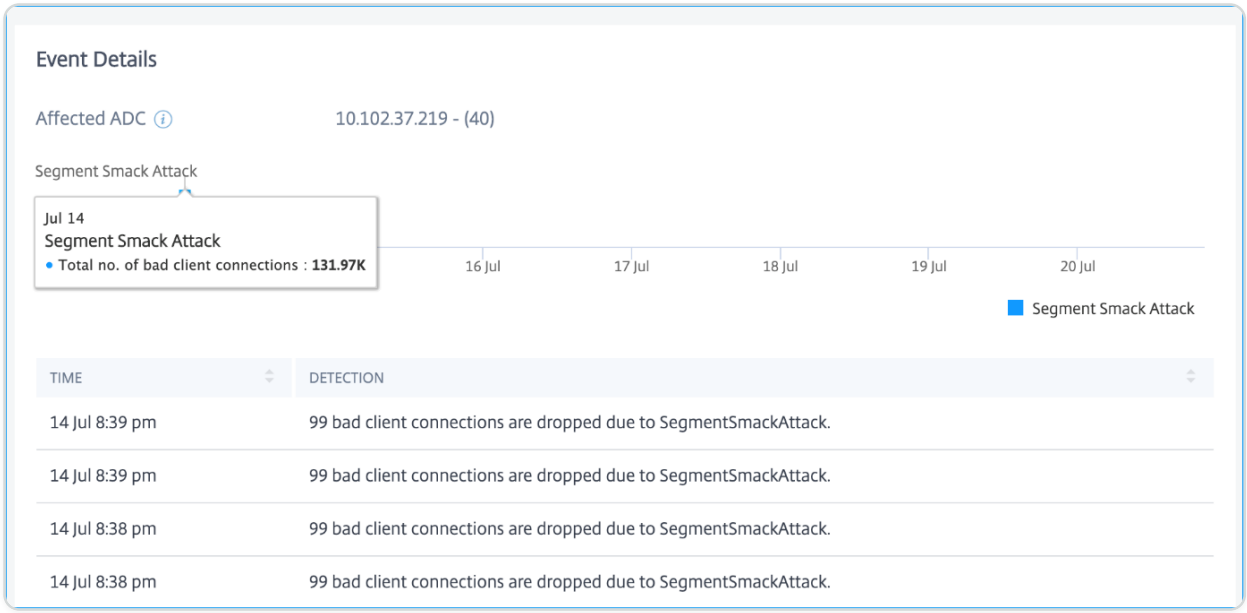


As an administrator, no further action is required because the NetScaler instance mitigates this attack by dropping all those excess TCP packets.

Under **Event Details**, you can view:

- The affected NetScaler instance
- The graph indicating the violation details. Hover the mouse point on the bar graph to view the total number of bad client connections detected.
- The detection message for the violation, indicating the total client connections dropped.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



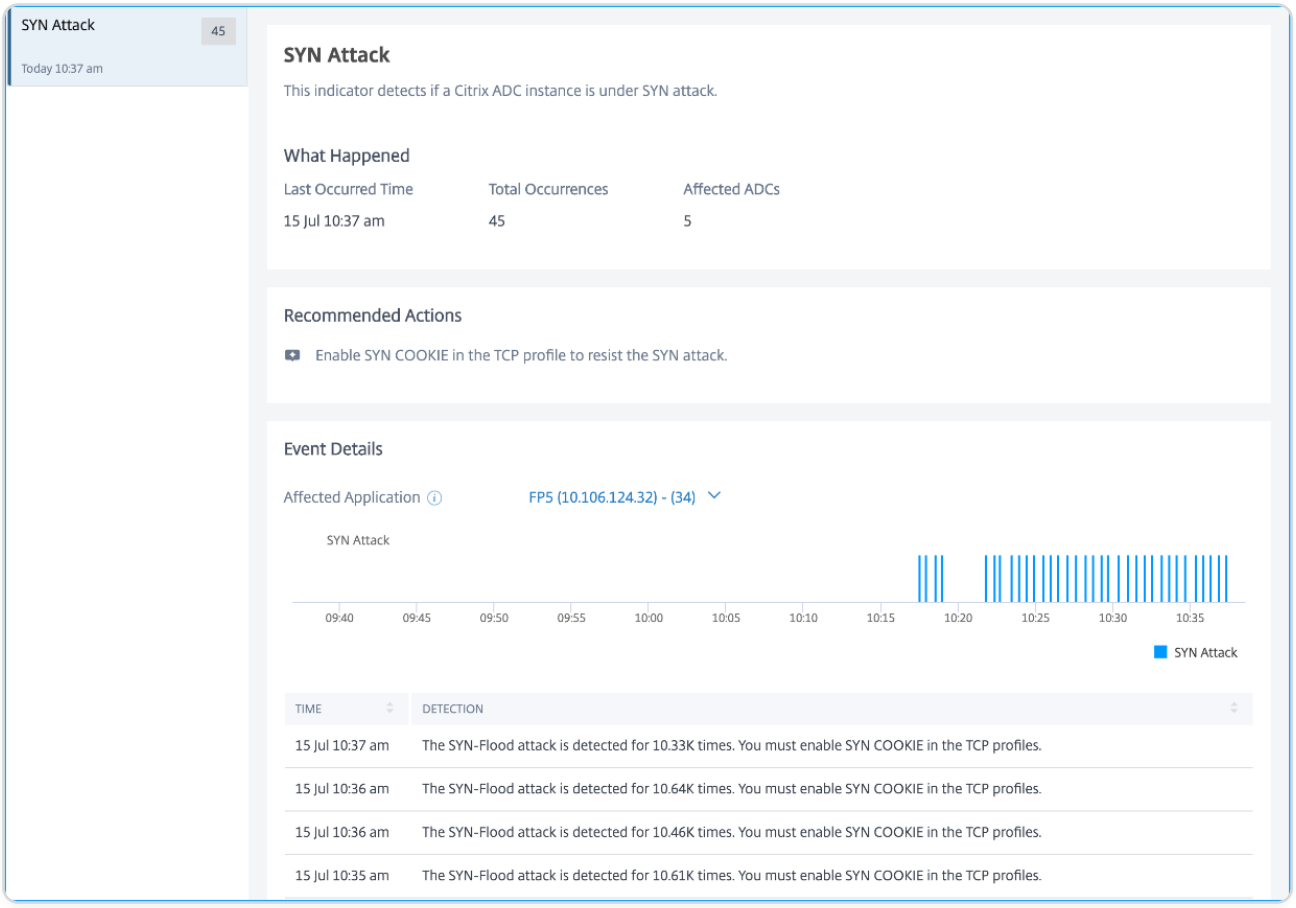
SYN Flood Attack

A SYN Flood Attack is a Denial of Service (DoS) attack that can affect the target machine, by sending thousands of connection requests using spoofed IP addresses. When a NetScaler instance is under a **SYN Flood** attack, the instance attempts to open a connection for each malicious request and then wait for an acknowledgment packet that never arrives.

The **SYNCOOKIE** in the TCP profile prevents SYN attacks on the NetScaler appliance. By default, the **SYNCOOKIE** on the NetScaler instance is enabled. The possibility for the NetScaler instance under a SYN flood attack is high only when `SYNCOOKIE` is disabled. For more information, see Layer 3–4 SYN Denial-of-Service protection.

Using the **SYN Flood Attack** indicator, you can analyze if the NetScaler instance is under SYN attack.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



As an administrator, the **Recommended Action** suggests you to enable `SYN COOKIE` in the TCP profile.

Under **Event Details**, you can view:

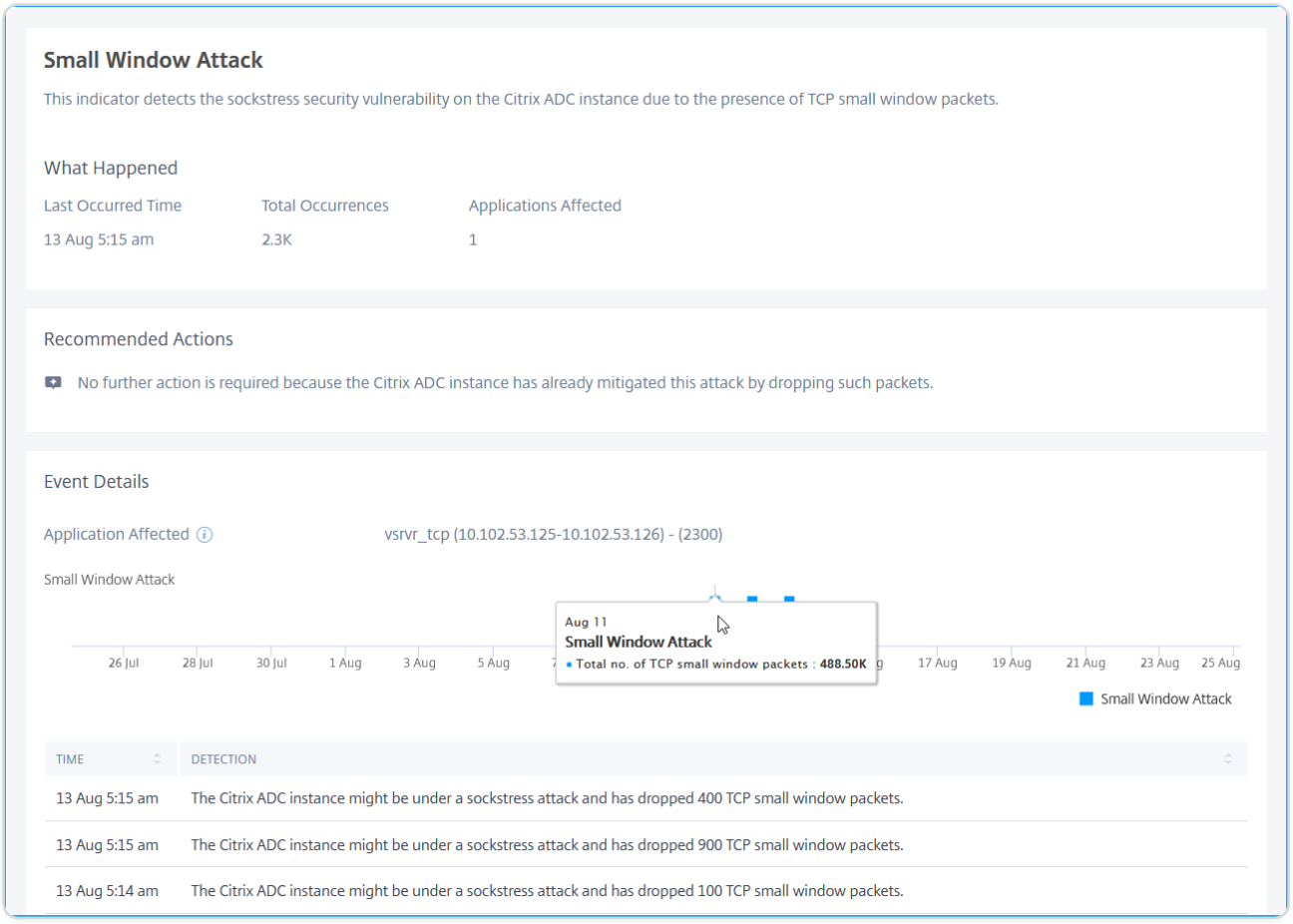
- The affected application. You can also select the application from the list if two or more applications are affected with this violation
- The graph indicating the SYN attack details
- The detection message, indicating the total number of times the application is detected with the SYN attack

Small Window Attack

A **Small Window Attack** is a Denial of Service (DoS) attack that can affect the target machine, by sending thousands of TCP packets with either smaller size window or window size 0. The window size 0 indicates that the target machine has to stop sending any more data until further notice. By sending as much as similar connections to the target machine, the target machine memory gets utilized to the maximum and becomes unresponsive.

Using the **Small Window Attack** indicator, you can analyze if the NetScaler instance is under the sockstress attack.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



By default, NetScaler instance mitigates this attack by dropping all such TCP small window packets. Hence, as an administrator, no further action is required.

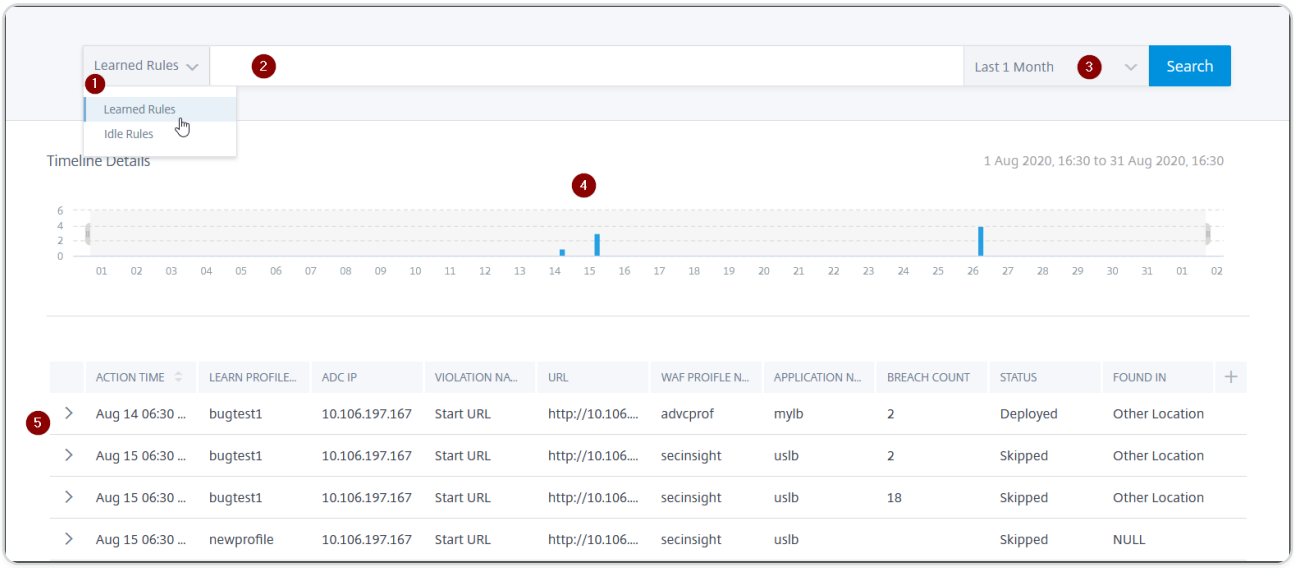
Under **Event Details**, you can view:

- The affected application. You can also select the application from the list if two or more applications are affected with this violation.
- The graph indicating the attack details. Hover the mouse point on the bar graph to view the total number of TCP small window packets detected.
- The detection message indicating the total TCP small window packets dropped.

View WAF learning Actions Summary

The WAF Learning **Actions Summary** page enables you to view all the deployed rules.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1 – Select **Learned Rules** or **Idle Rules** from the list to view details in the dashboard.

2 – An advanced search bar that enables you to show the result based on the suggestions and operators.

3 – Time duration list for which you want to view the result

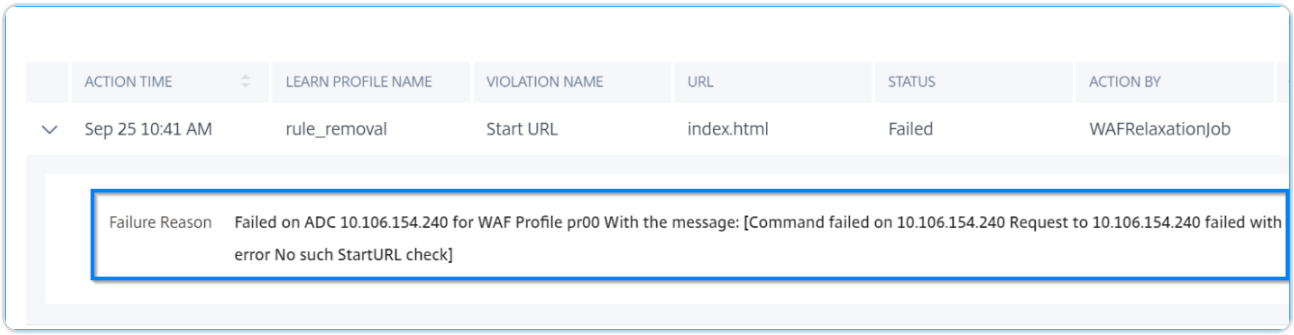
4 – A graph format result that enables you to drag and select the graph to filter the results

5 – The deployed or removed rules details

Click **>** to view the details.

View failed rules

If a deployed learn rule has failed, you can view the failure reason.

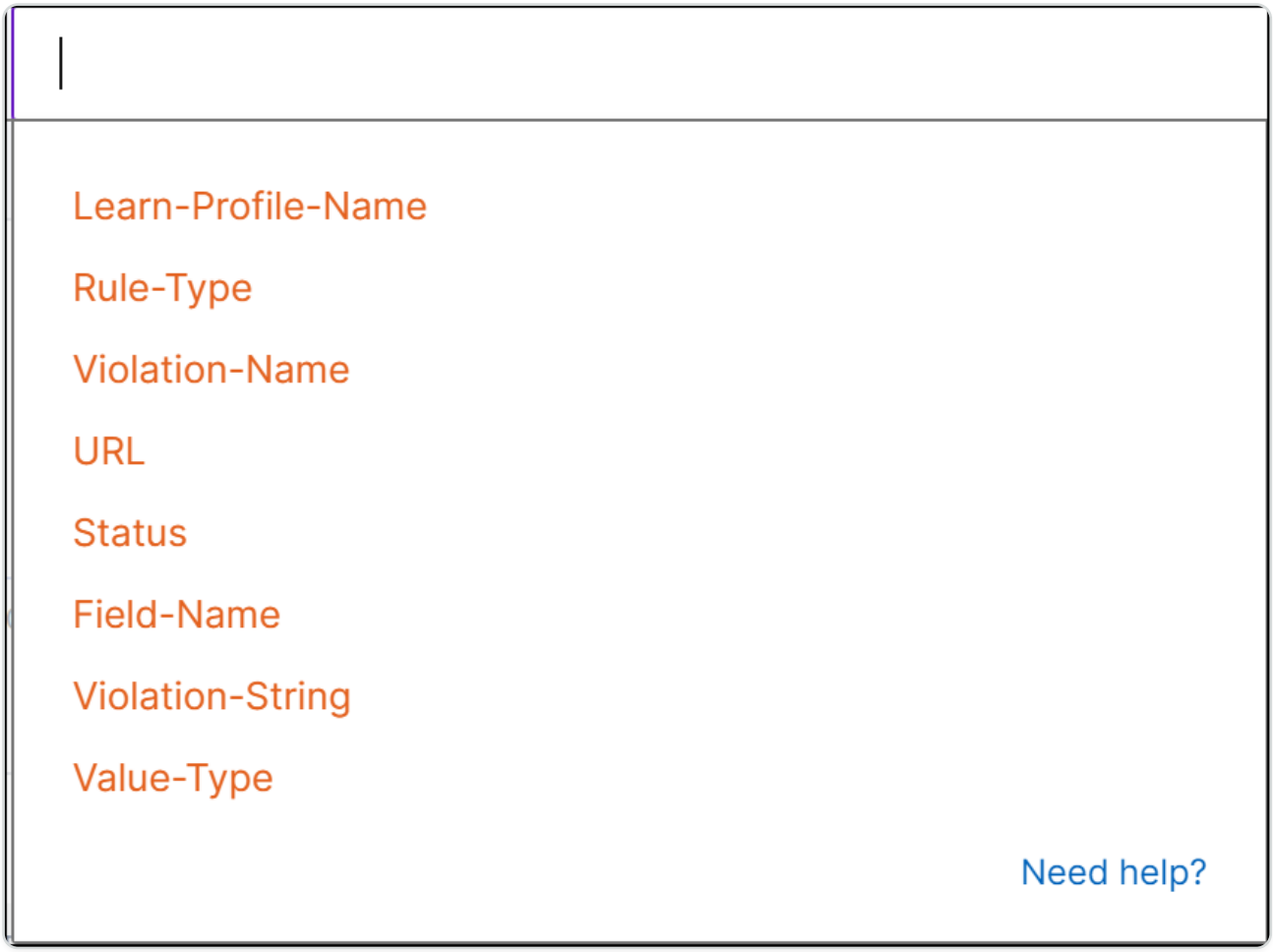


Advanced search

The advanced search bar enables you to view the results as per your requirement. When you click the search box, the search box gives you a list of search suggestions. You can also use operators in your search queries to narrow the focus of your search.

The following suggestions are displayed when you place the mouse pointer on the search box:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Learn-Profile-Name** – Indicates the learning profile name that you configured.
- **Rule-Type** – Indicates the rule type (Deny or Allow).
- **Violation-Name** – Indicates the violation name such as Start URL, Cross-Site script, and so on.
- **URL** – Indicates the web application URL.
- **Status** – Indicates the deployed rule status.
- **Field-Name** – Indicates the field name updated in the web forms for form field security check.
- **Violation-String** – Indicates the possible string from where the violation has originated.
- **Value-Type** – Indicates the data types used in the security checks. For example, keyword.

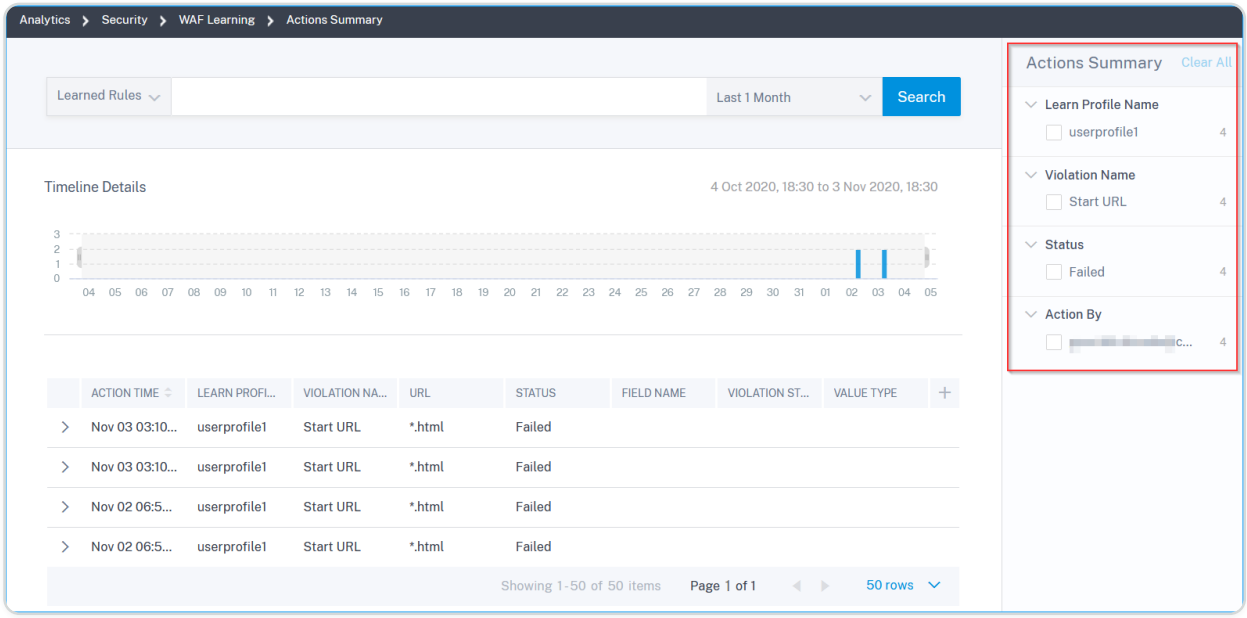
Filter results

From the **Actions Summary**, you can filter the results by selecting the following options:

- **Learn Profile Name** - Filter based on the learn profile name.
- **Violation Name** - Filter based on the violation name such as Start URL, HTML Cross-Site Scripting, Content Type, and so on.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Status** - Filter based on the status of the deployed or idle rules.
- **Action By** - Filter based on the user.



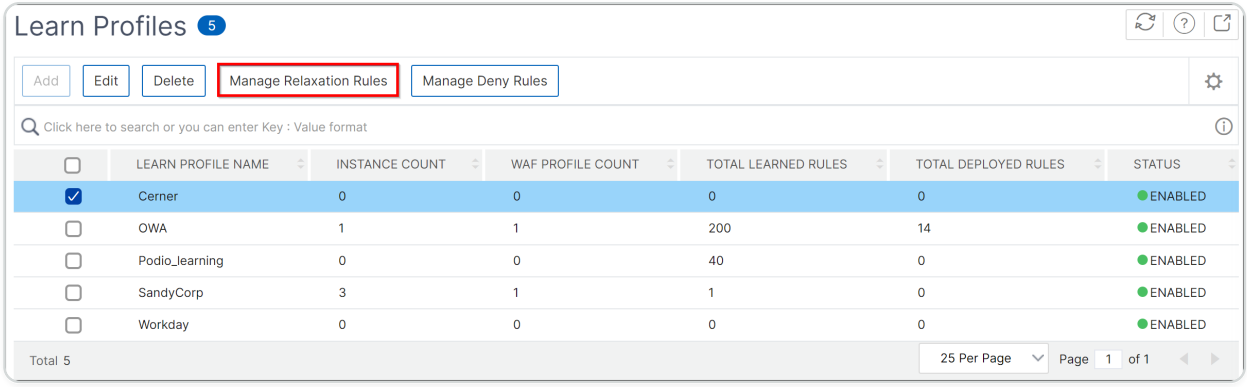
View relaxation rules, idle, and deny rules

After you configure the learning profile, NetScaler Console starts to get a list of relaxation, idle, and deny rules.

1. Navigate to **Security** > **WAF Learning** > **Learn Profiles**.

   The **Learn Profiles** page indicates the WAF learning profile name, total NetScaler instance associated, total WAF profile created on the instance, total learned rules, total deployed rules, and the status.

2. Select the profile name and click **Manage Relaxation Rules**.



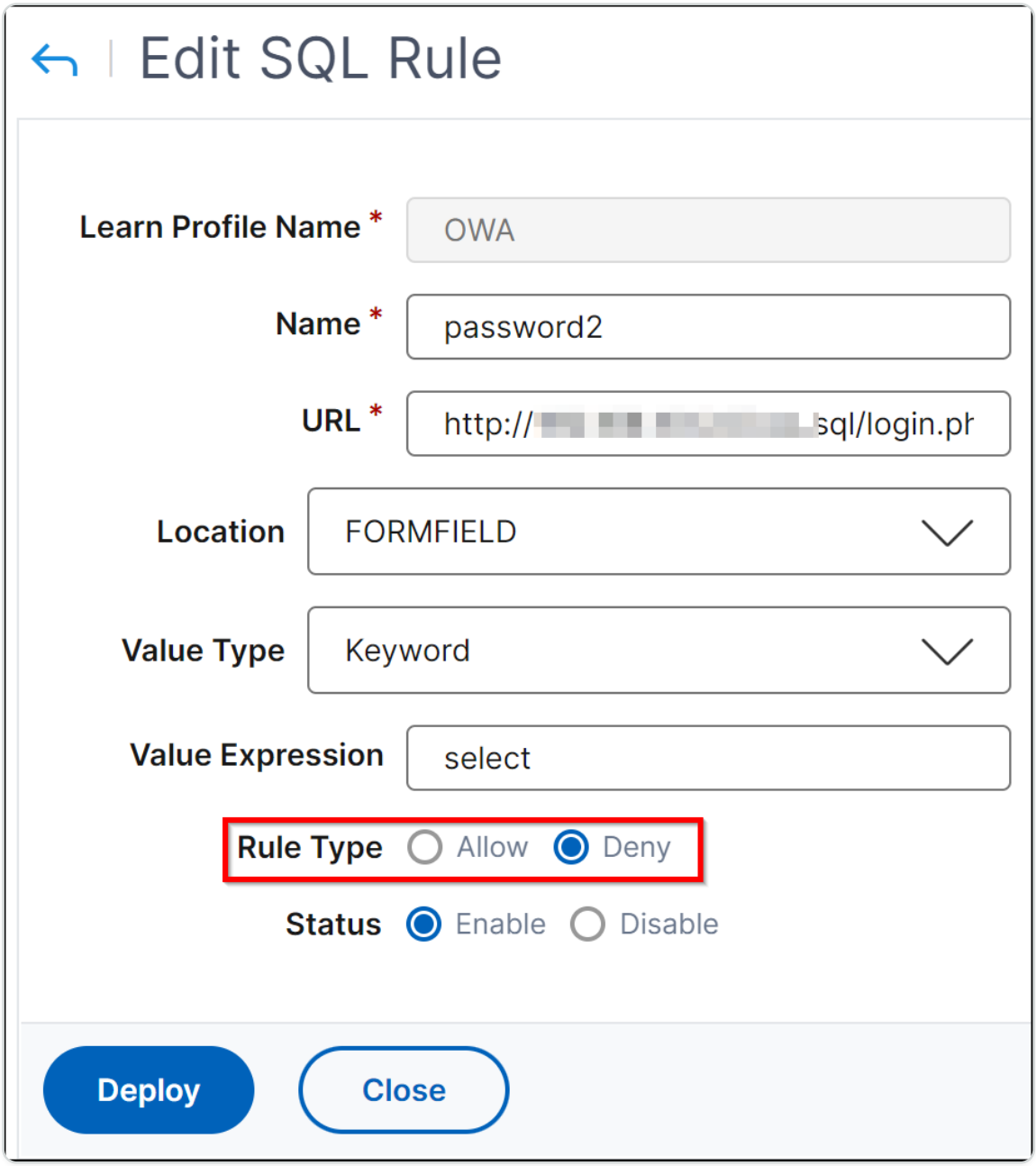
You can view the total rules, total learned rules, total deployed rules, and total idle rules for the selected profile.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- In the **Learned Rules** tab, you can view the relaxed rules. Select the rule, validate, and click **Add & Deploy**, **Deploy**, **Edit & Deploy**, **Delete**, or **Deploy as Deny**.
    - **Add & Deploy** - Enables you to create a new rule with the security check options. After you create the rule, click **Deploy**.
    - **Deploy** - Enables you to deploy the relaxed rule.
    - **Edit & Deploy** - Enables you to edit the rule before you want to deploy. For SQL security check, you can edit the rule and change the **Rule Type** to **Deny** and then deploy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For more information, see Relaxation and deny rules for handling HTML SQL injection attacks.

- **Delete** - Enables you to delete the rule without any action.
- **Deploy as Deny** - For the SQL security check, you can use this option to deny requests.

- Click the **Deployed Rules** tab to view the deployed rules. Select a rule and choose to delete, enable, or disable the rule.
- Click the **Idle Rules** tab to view the idle rules that have no traffic. Click **Delete** if you want to delete the rule.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

The violation list is available until the configured grace duration. After the grace period, NetScaler Console deploys the available violations automatically.

For each configured learned profile, you can view up to 1 million learned rules.

Manage deny rules

In addition to relaxation (allow) mode, you can also configure and use the deny rules for handling HTML SQL injection attack security check. If you configure the HTML SQL Injection security check in deny mode, the detected violations are blocked.

In the **Manage Deny Rules** tab, you can view the denied rules for HTML SQL injection checks. Select the rule, validate, and click **Add & Deploy**, **Deploy**, **Edit & Deploy**, **Delete**, or **Deploy as Relaxation**.

- **Add & Deploy** - Enables you to create a new rule with the security check options. After you create the rule, click **Deploy**.
- **Deploy** - Enables you to deploy the denied rule.
- **Edit & Deploy** - Enables you to edit the rule before you want to deploy.
- **Delete** - Enables you to delete the rule without any action.
- **Deploy as Relaxation** - Allows the traffic.

SSL Insight

SSL Insight provides visibility into secure web transactions (HTTPS) and allows IT administrators to monitor all the secure web applications being served by the NetScaler by providing integrated and real-time and historic monitoring of secure web transactions. With this visibility the administrator can assess following:

- **Determine Configuration Change Impact on Customer Usage**. The administrator can understand the impact on clients for making a configuration change like turning off SSLv3 or removing a cipher like RC4-MD5. This can be done by assessing the historic transaction data on this protocol and cipher.
- **Quantify client performance**. Administrator can understand the impact on Application Response Time based on the SSL ciphers/protocol used or the certificates negotiated.
- **Application Security**. Assess if any of the applications have transactions running on low security protocols, ciphers, or weak key strength.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When SSL Analytics is enabled on a NetScaler instance, SSL statistics are recorded and logged for every SSL transaction. The statistics show the details of the SSL flow. Also, every successful connection is logged and displayed by NetScaler Console.

SSL Insight provides the following critical information, which is displayed by NetScaler Console Analytics:

- SSL Protocol version negotiated
- Cipher negotiated, and the cipher strength
- Signature Hash algorithm of the certificate used
- Certificate Type & Size
- SSL Front end and Back end errors

NOTE

For successful SSL connections, SSL AppFlow® logging happens at the end of every transaction.

Prerequisites

- The NetScaler instance on which you intend to configure SSL Insight must be running NetScaler software release 11.1 51.21 and higher. Run the following commands on the NetScaler instance running 11.1 51.21 to enable **Logstream** as a transport type for SSL Insight.

1. `enable ns mode ulfd`
2. `add ulfd server <IP Address of the NetScaler Console>`

   For NetScaler instances running version 12.0 and above, select **Logstream** as the transport type while enabling AppFlow from NetScaler Console.

- The NetScaler Console version and build must be equal to or higher than the NetScaler version and build. For example, if you have installed NetScaler Console 11.1 build 61.7, then ensure you have installed NetScaler 11.1 build 60.14 or earlier.

Configure SSL Insight

SSL Insight Metrics are included in Web Insight reports if you enable the following elements:

- Enable AppFlow for Web Insight on each NetScaler instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Enable ULFD mode on each NetScaler instance.
- Enable required AppFlow parameters on each NetScaler instance.

Enable the insight

NOTE

You can enable the AppFlow feature either from NetScaler Console or from each NetScaler instance.

Enable the AppFlow feature from NetScaler Console

1. Navigate to **Infrastructure > Instances**, and select the NetScaler instance on which you want to enable analytics.
2. From the **Select Action** list, select **Configure Analytics**.
3. On the **Configure Analytics on Virtual Servers** page:

   a. Select the virtual servers that you want to enable Web Insight and click **Enable Security & Analytics**

   The **Enable Security & Analytics** window is displayed.

   b. Select **Web Insight**

   c. Under **Advanced Options**, select **Logstream** or **IPFIX** as Transport Mode

   NOTE

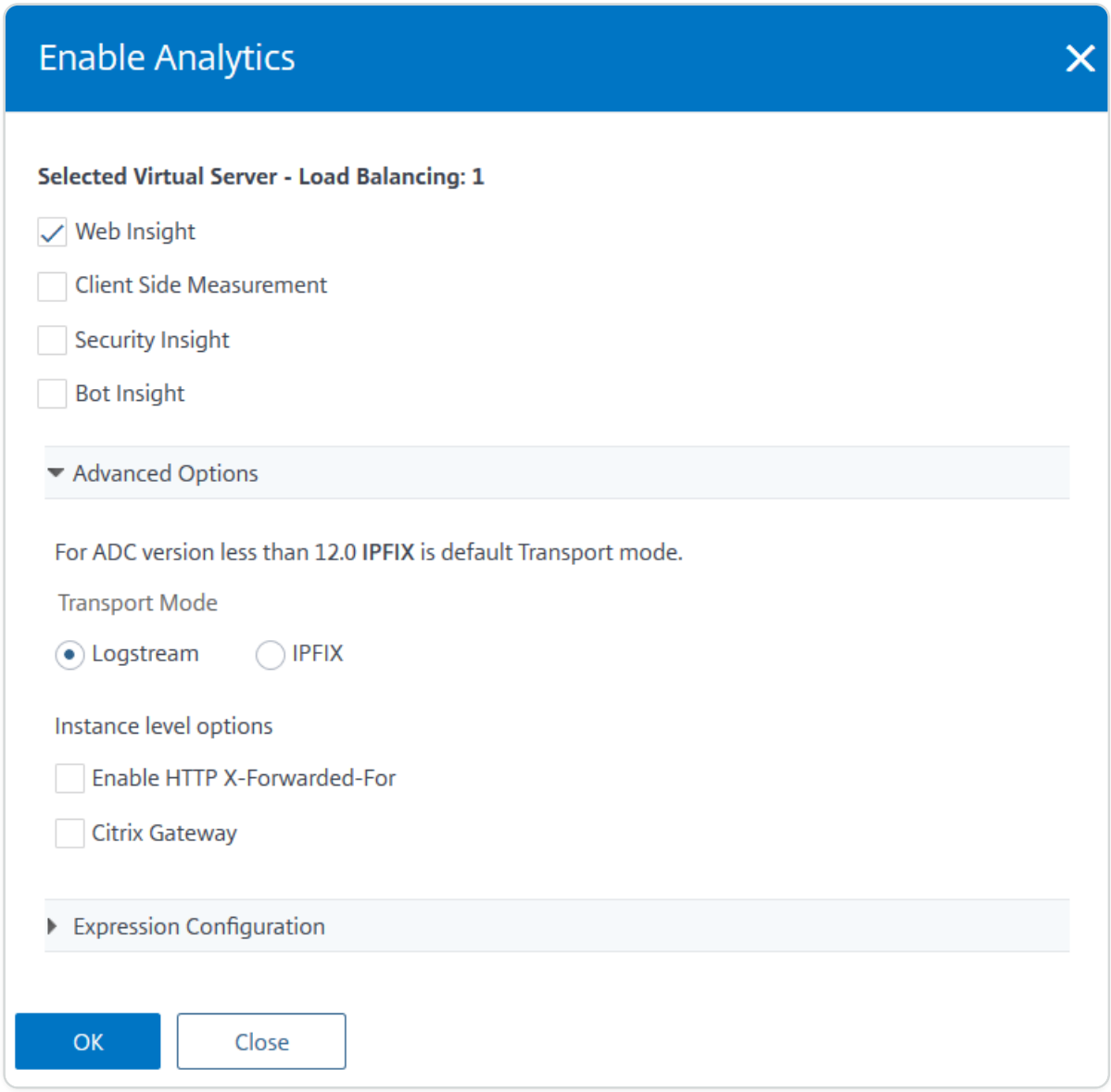
   For NetScaler 12.0 or earlier, **IPFIX** is the default option for Transport Mode. For NetScaler 12.0 or later, you can either select **Logstream** or **IPFIX** as Transport Mode.

   For more information about **IPFIX** and **Logstream**, see **Logstream overview**.

   d. The Expression is true by default

   e. Click **OK**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE

You cannot enable data collection on a virtual server if the operational state of the virtual server is other than UP.

Enable the AppFlow feature by using the NetScaler GUI

In a NetScaler instance's GUI, navigate to **Configuration** > **System** > **Settings**, click **Configure Advanced Features**, and select **AppFlow**.

Enable ULFD mode

After you enable ULFD mode on the NetScaler instances on which the virtual servers are configured, the ULFD server streams the analytics data from the NetScaler instances to NetScaler Console.

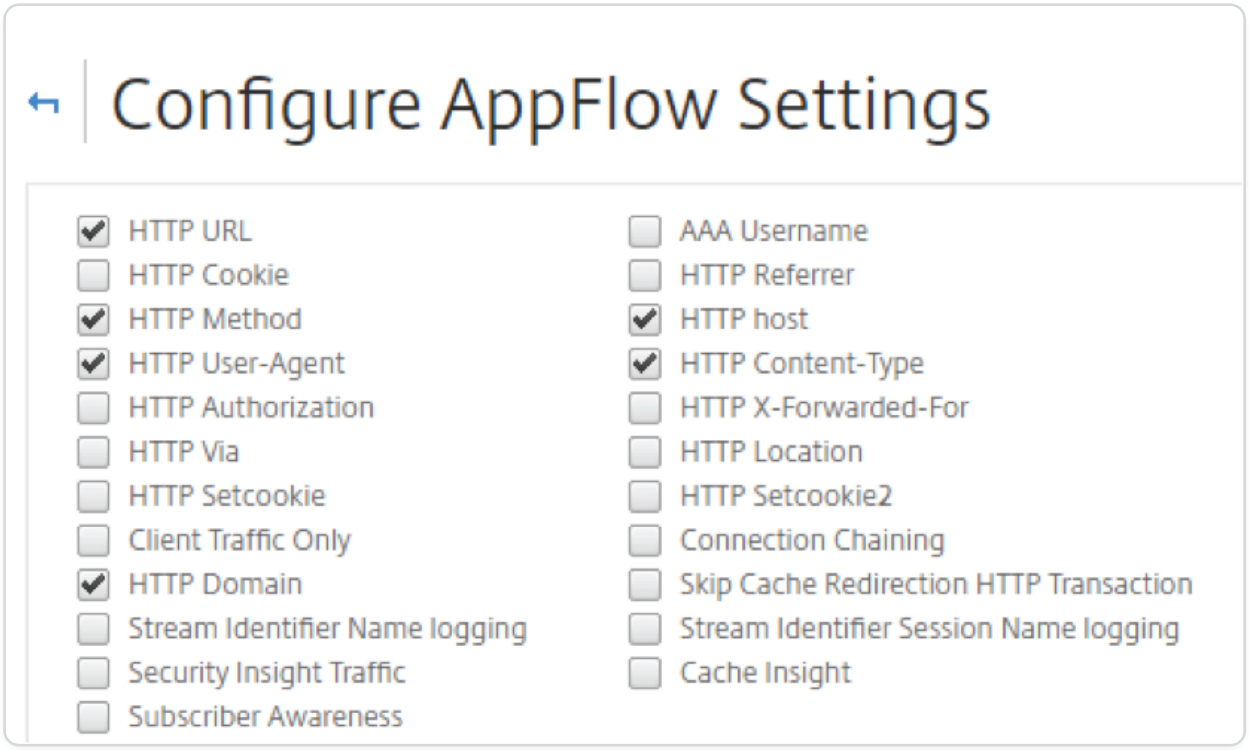
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enable SSL Insight parameters

On each NetScaler instance, you have to enable some HTTP parameters to display SSL Insight records in NetScaler Console.

Enable SSL Insight parameters from the NetScaler configuration utility

1. Navigate to **Configuration** > **System** > **AppFlow**, and click **Change AppFlowSettings**.
2. Select the following check boxes: **HTTP Domain**, **HTTP Host**, **HTTP Method**, **HTTP URL**, **HTTP User-Agent**, **HTTP Content-Type**.
3. Click **OK**.



View the SSL Insight metrics

SSL Insight metrics in NetScaler Console provide a detailed view of the performance of the SSL transactions served by the NetScaler instances. You can view the SSL Insight metrics at the client, server, or application level, and the SSL success and failure transactions' metrics. With the help of these metrics, you can analyze and optimize your NetScaler HTTPS settings and SSL-certificate settings, and track performance issues.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTE

When you create a group, you can assign roles to the group, provide application-level access to the group, and assign users to the group. NetScaler Console analytics now supports virtual IP address based authorization. Your users can now see reports for all Insights for only the applications (virtual servers) that they are authorized to. For more information on groups and assigning users to the group, see Configuring Groups on NetScaler Console.

Monitor SSL Insight metrics in NetScaler Console

As an administrator, you can view SSL metrics for:

- An application. Navigate to **Applications > Dashboard**, click an application, and select **Web Insight** tab to view the detailed metrics. For more information, see Application Usage Analytics.
- All applications. Navigate to **Applications > Web Insight** and click **Applications** and **Clients** tabs to view the SSL metrics.

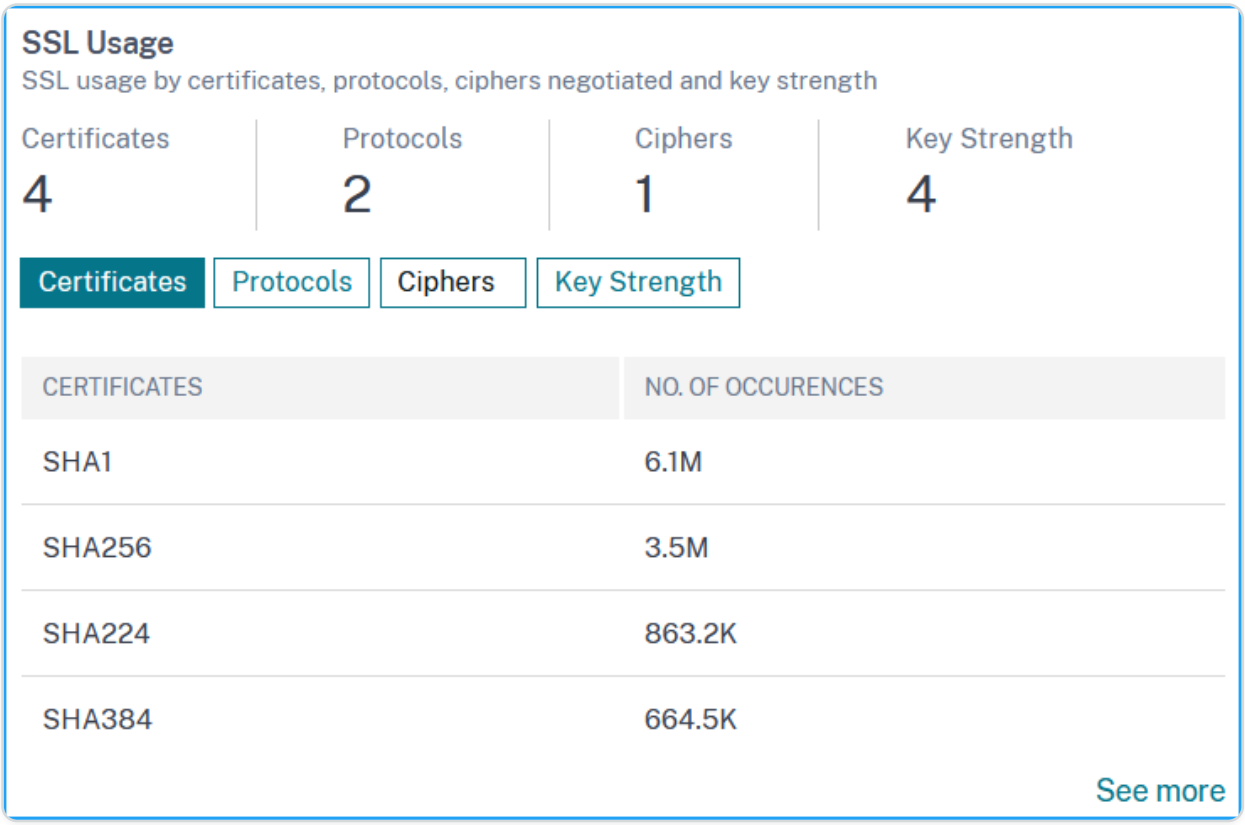
Use case: Obtain an overview of the SSL transactions

The following use case describes how you can use SSL Insight to assess the usage of various SSL Parameters and improve security measures.

Consider that you have a set of applications that are using SSL transactions (HTTPS) for communication, and you have configured NetScaler Console to monitor the SSL components. You might need to frequently review the applications so that you can focus first on the applications that need the most attention. The **Web Insight** dashboard for an application or all applications provides a summary of following SSL parameters under **SSL Errors** and **SSL Usage**:

- SSL Certificates
- SSL Protocols
- SSL Cipher
- SSL Key Strength
- SSL Failure – Front end
- SSL Failure – Back end

© 1997–2026 Citrix Systems, Inc. All rights reserved.



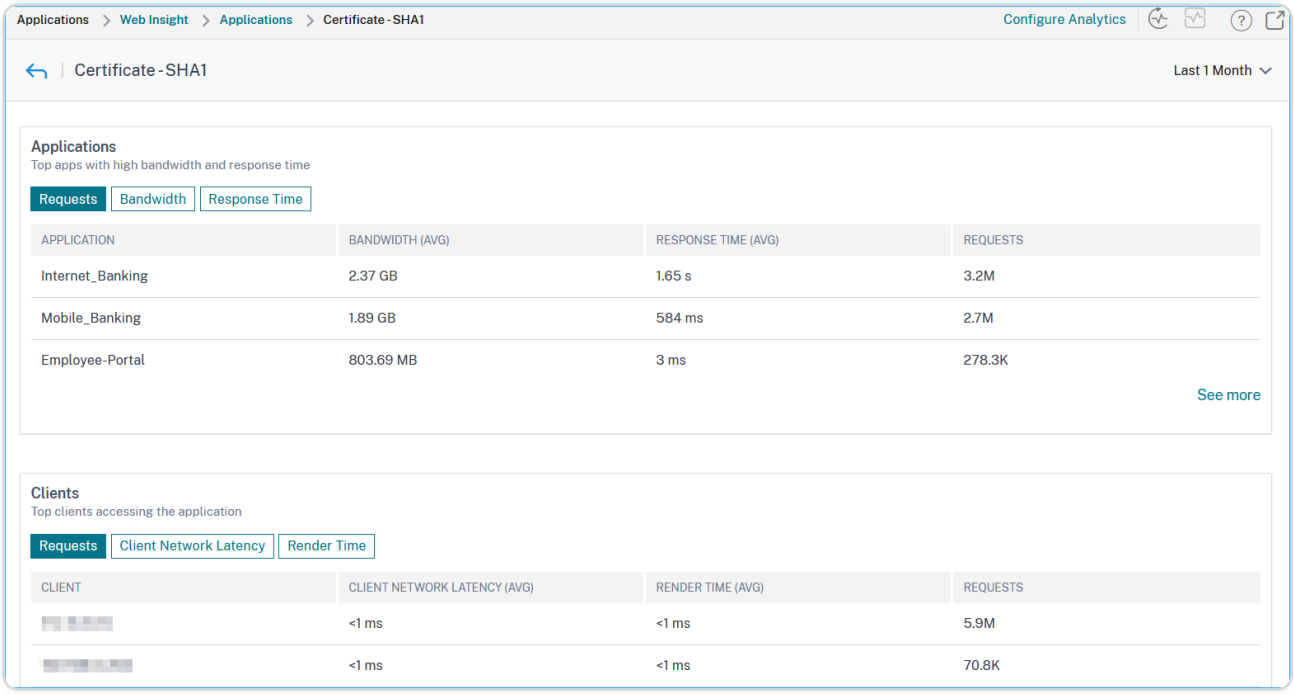
You can click each tab to view details.

Use case: SSL metrics for clients

You can see list of clients (identified by their IP addresses) and the total occurences per client. Navigate to **Applications > Web Insight** and select the **Clients** tab to view the details under **SSL Usage**.

Click a metric to view details and under **Clients**, click any client IP address to view the SSL metrics for the selected client.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



View analytics for Web transactions

Web transaction analytics enables view detailed transactions for:

- Response time > 500 ms
- 5xx errors

NOTE:

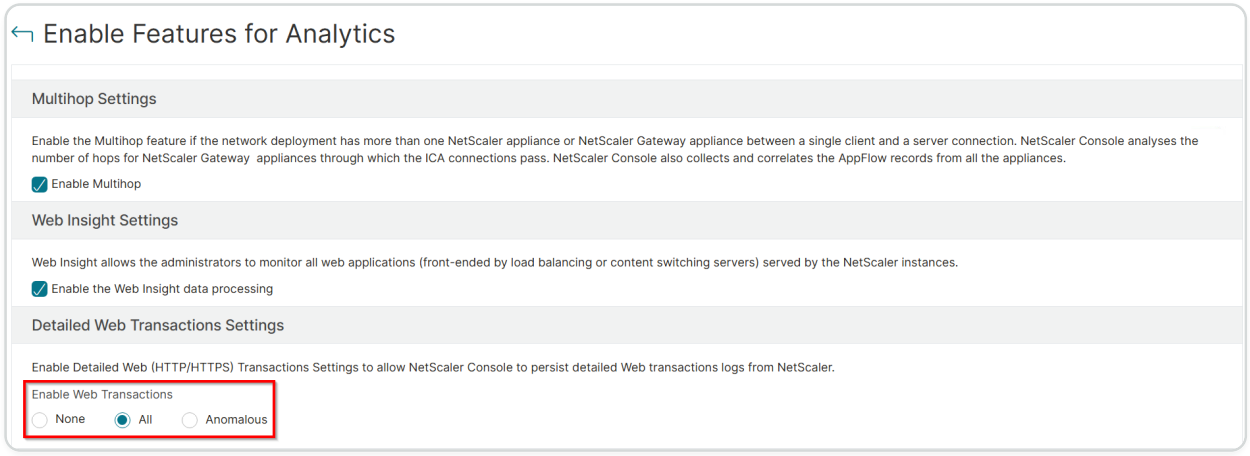
You can view only a few sample 2xx transactions for the selected application.

Prerequisites

To view the Web transaction analytics, you must:

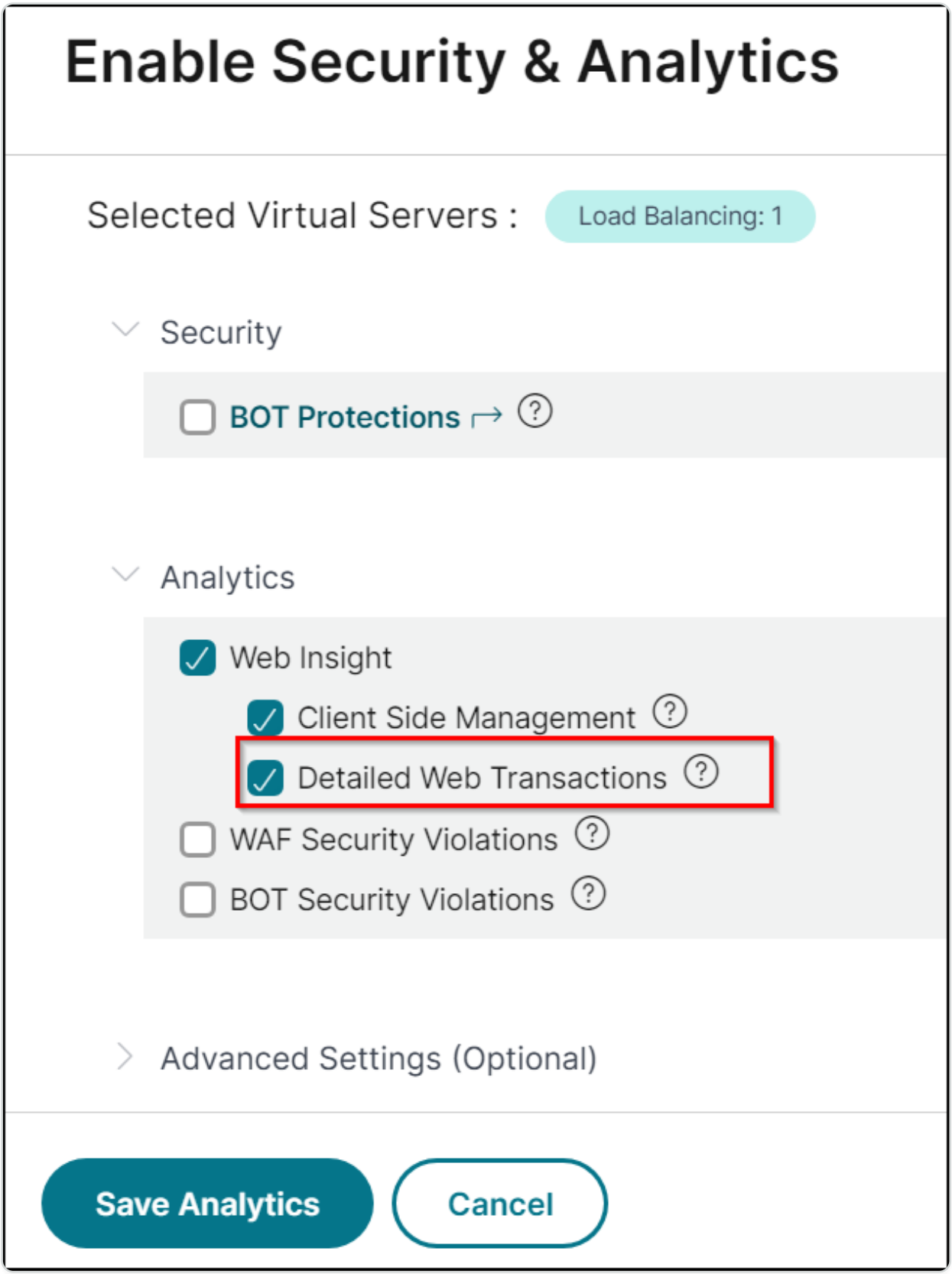
1. Navigate to **Settings > Analytics Settings > Enable Features for Analytics**, and select any one of the following:
    - **None** - No data is displayed.
    - **All** - Displays all HTTP transactions. If you select this option, NetScaler Console consumes more storage. Ensure that you use this option only for critical applications.
    - **Anomalous** - Displays transactions with 5xx error and response time > 500 ms.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Select **Detailed Web Transactions** under **Web Insight** when you enable analytics for the virtual servers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NOTE:

Starting from 14.1-44.x build, **Web Transaction Analytics** is available at the virtual server level.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Detailed Web transactions

This feature not only enables you to look into the detailed transactions, but also understand the metrics (such as Client RTT, server response time, and SSL metrics) split across the client, NetScaler, and server visually.

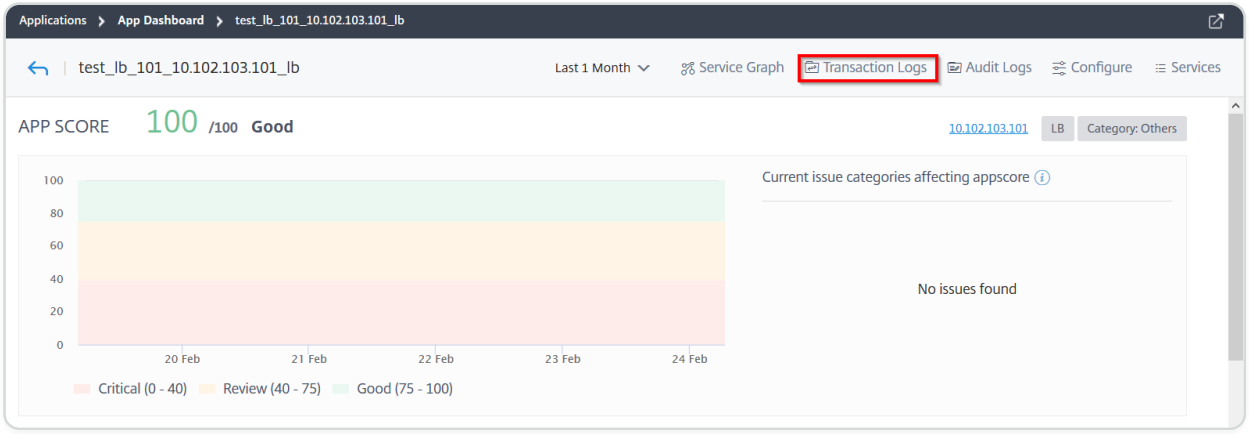
NOTE:

In some scenarios, NetScaler might not be able to calculate the RTT values for some transactions. For such transactions, NetScaler Console displays the RTT values as:

- **NA** – Displays when the NetScaler instance cannot calculate the RTT.
- **< 1ms** – Displays when the NetScaler instance calculates the RTT in decimals between 0 ms and 1 ms. For example, 0.22 ms.

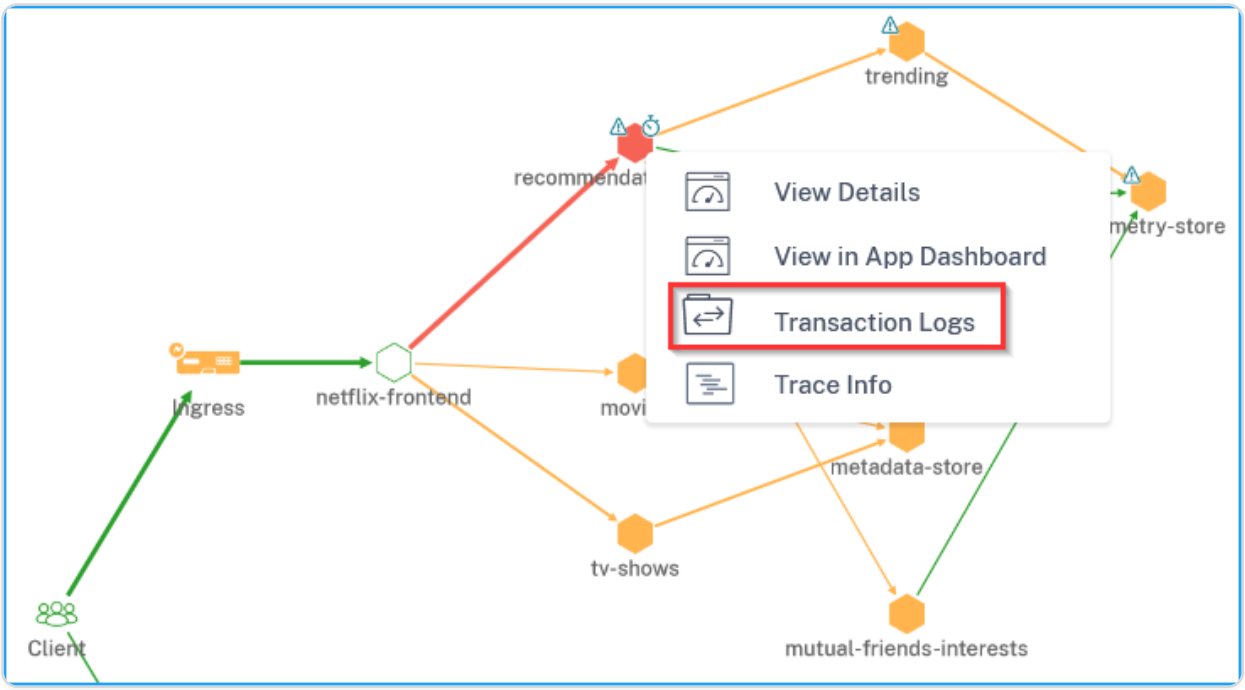
You can view the detailed transactions for:

- **Applications** – Navigate to **Applications > Dashboard**, select an application, and click **Transaction Log**.



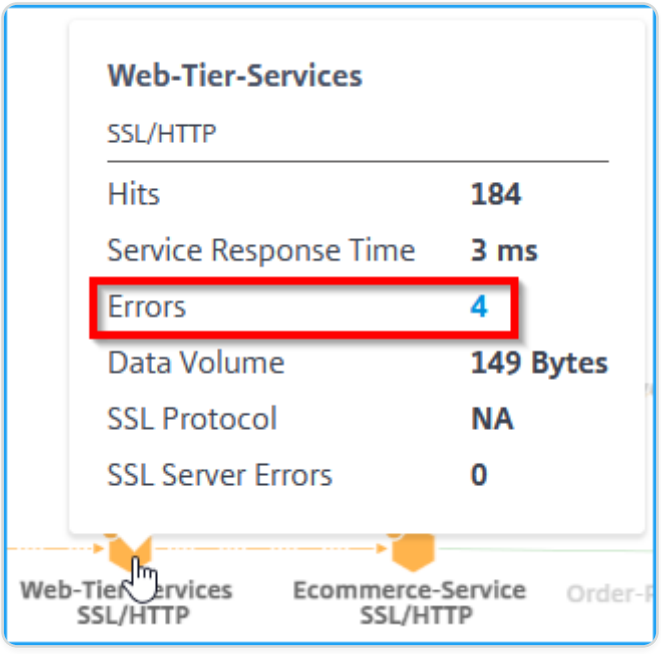
- **Kubernetes applications** – Navigate to **Applications** > **Service Graph**. Click a service and then select **Transaction Logs**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



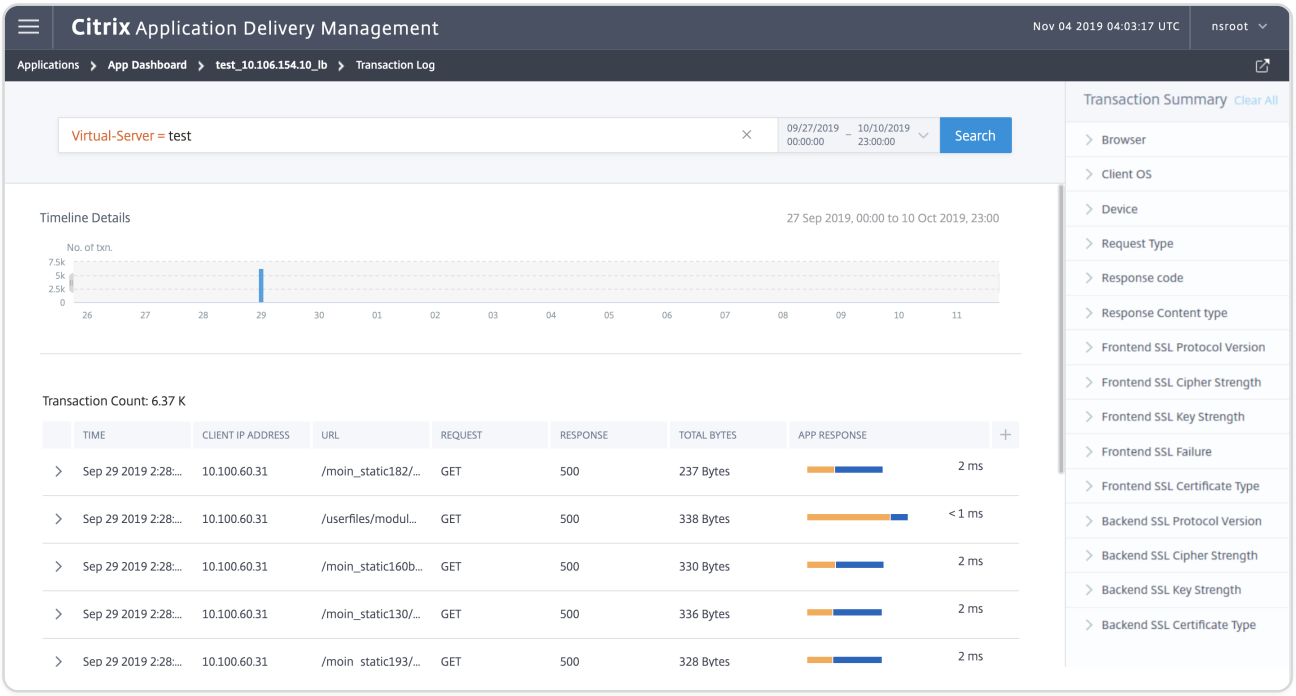
NOTE:

You can view the errors by hovering the mouse pointer on an erroneous service and click the issue count.



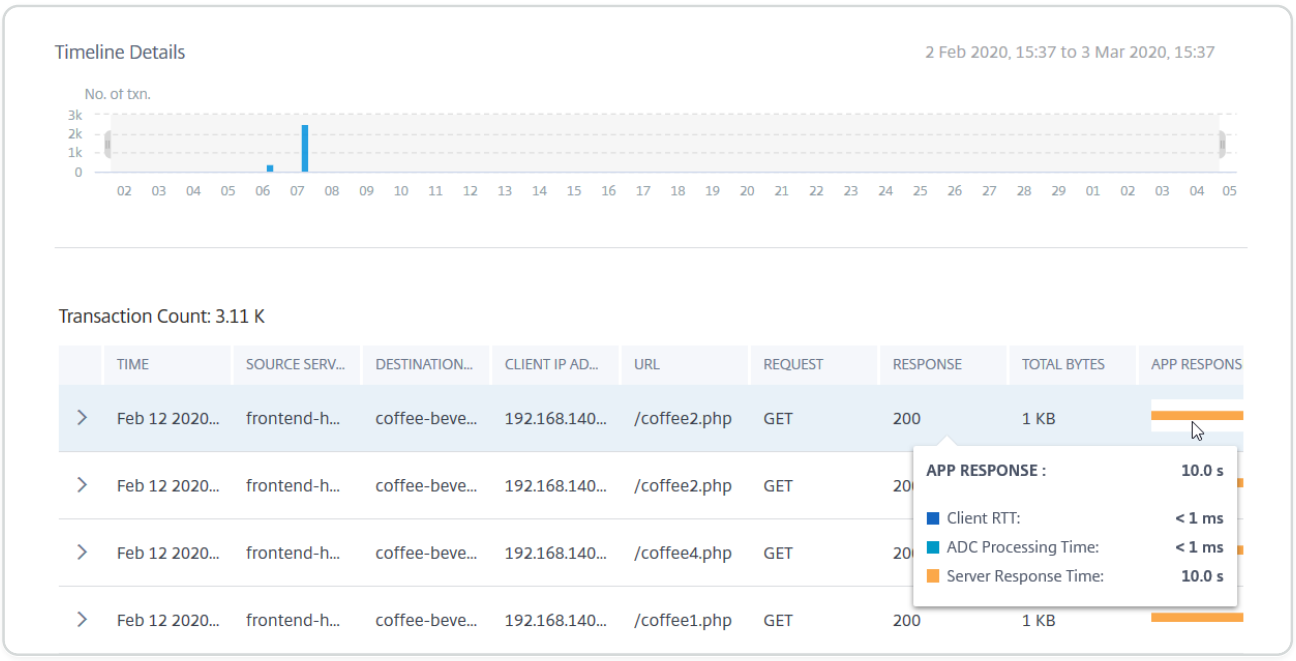
The detailed transaction with **Transaction Summary** for the selected application is displayed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



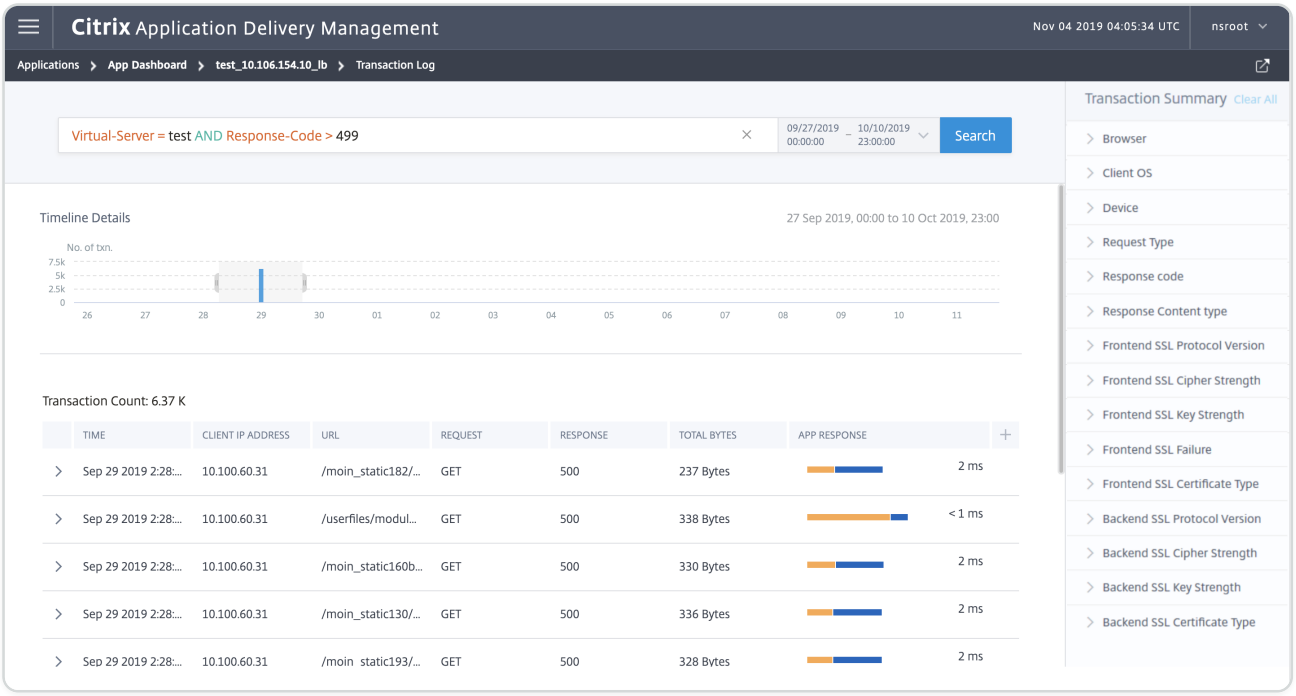
Hover the mouse pointer in **App Response** to view details such as RTT and processing time from NetScaler instance and the server.

The following example helps you analyze that the issue is from the server. The server response time indicates 10 seconds.



You can also drag and select to view the transactions for a specific duration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

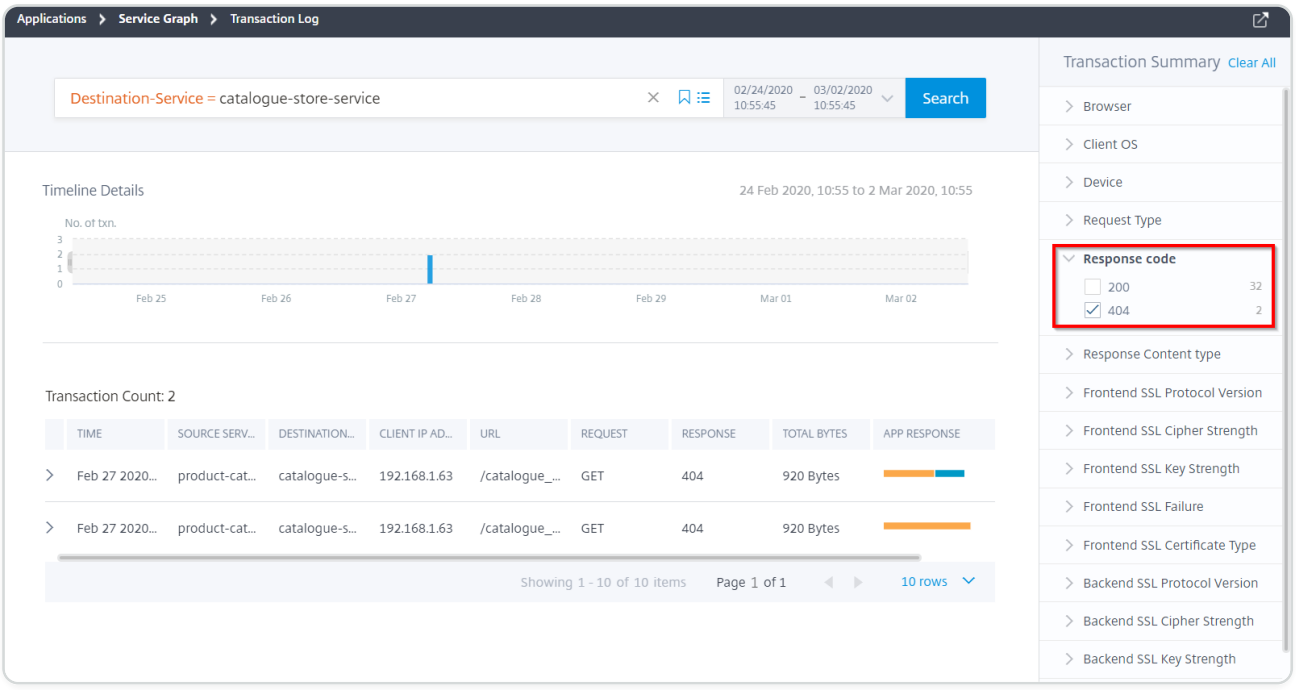


View events

You can view the detailed information about a particular event. On the **Transaction Summary** panel, you can filter results by selecting the options from each metric.

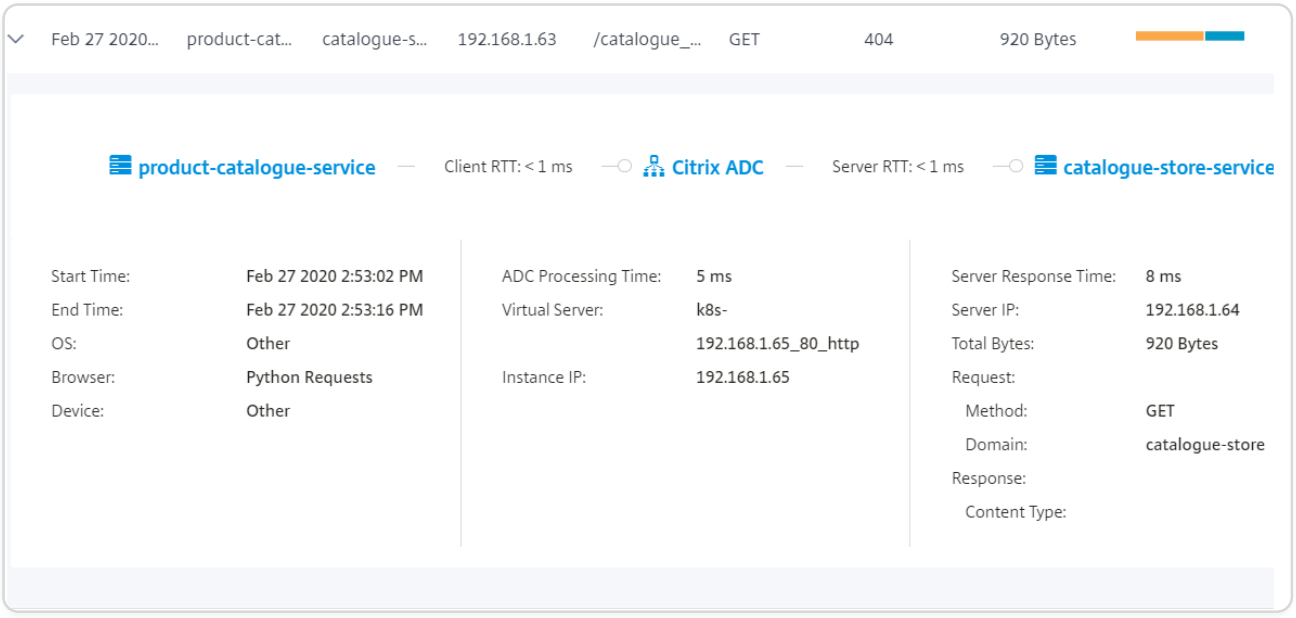
For example, consider that you want to view 4xx transactions.

On the **Transaction Summary** panel, click **Response code**, and select **404** to view the result.



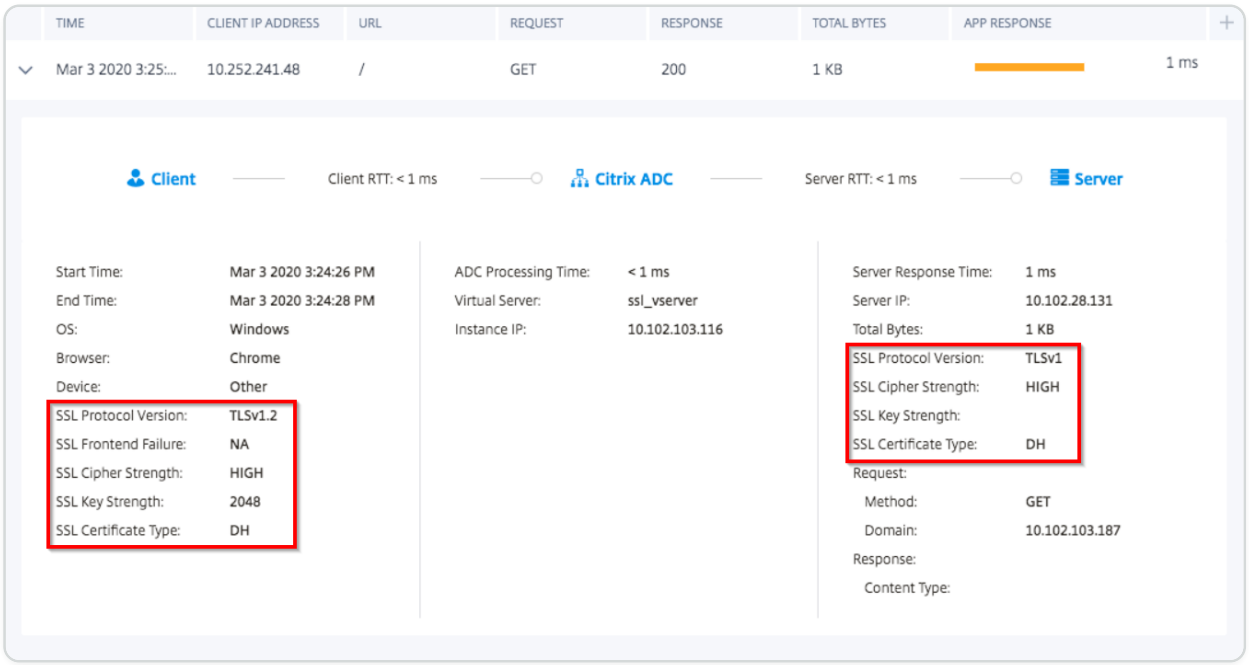
Click a transaction to view the details that display the metrics information from client to server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For transactions that have SSL errors, the details are displayed for both client and server. The following SSL metrics are displayed:

- SSL Protocol Version
- SSL Front end Failure
- SSL Cipher Strength
- SSL Key Strength
- SSL Certificate Type



You can also click the SSL Front end and SSL Back end metrics from the **Transaction Summary** panel to filter the results.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To filter the results, select the options available under **Transaction Summary**.



- **Browser**: The browsers types used by the clients. For example: Chrome, Firefox.
- **Client OS**: The client OS based on the User Agent details from the browser. For example: Windows
- **Device**: The devices based on the User Agent details from the browser. For example: Tablet, Mobile.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Request Type**: The transaction request type. For example: GET.
- **Response code**: The response code received from the server. For example: 501, 404, 200.
- **Response content type**: The transaction content type. If the client request is for text/html, then the response from the server must be text/html.
- **Frontend SSL Protocol Version**: The SSL protocol version used by the clients. For example: SSLv3.
- **Frontend SSL Cipher Strength**: The cipher strength based on the SSL certificate key size such as high, medium, and low.
- **Frontend SSL Key Strength**: The SSL cipher strength is calculated from the SSL certificate key size. The key length defines the SSL algorithm security. For example: 2048
- **Frontend SSL Failure**: The front end SSL handshake error message. For example: SSL CLIENTAUTH FAILURE
- **Frontend SSL Certificate Type**: The certificate type used by the client. For example: RSA, DSA, ECDSA, DH.
- **Backend SSL Protocol Version**: The SSL protocols used by the server. For example: SSLv3
- **Backend SSL Cipher Strength**: The cipher strength based on the SSL certificate key size such as high, medium, and low.
- **Backend SSL Key Strength**: The SSL cipher strength is calculated from the SSL certificate key size. The key length defines the SSL algorithm security. For example: 2048
- **Backend SSL Certificate Type**: The certificate type used by the server. For example: RSA, DSA, ECDSA, DH.

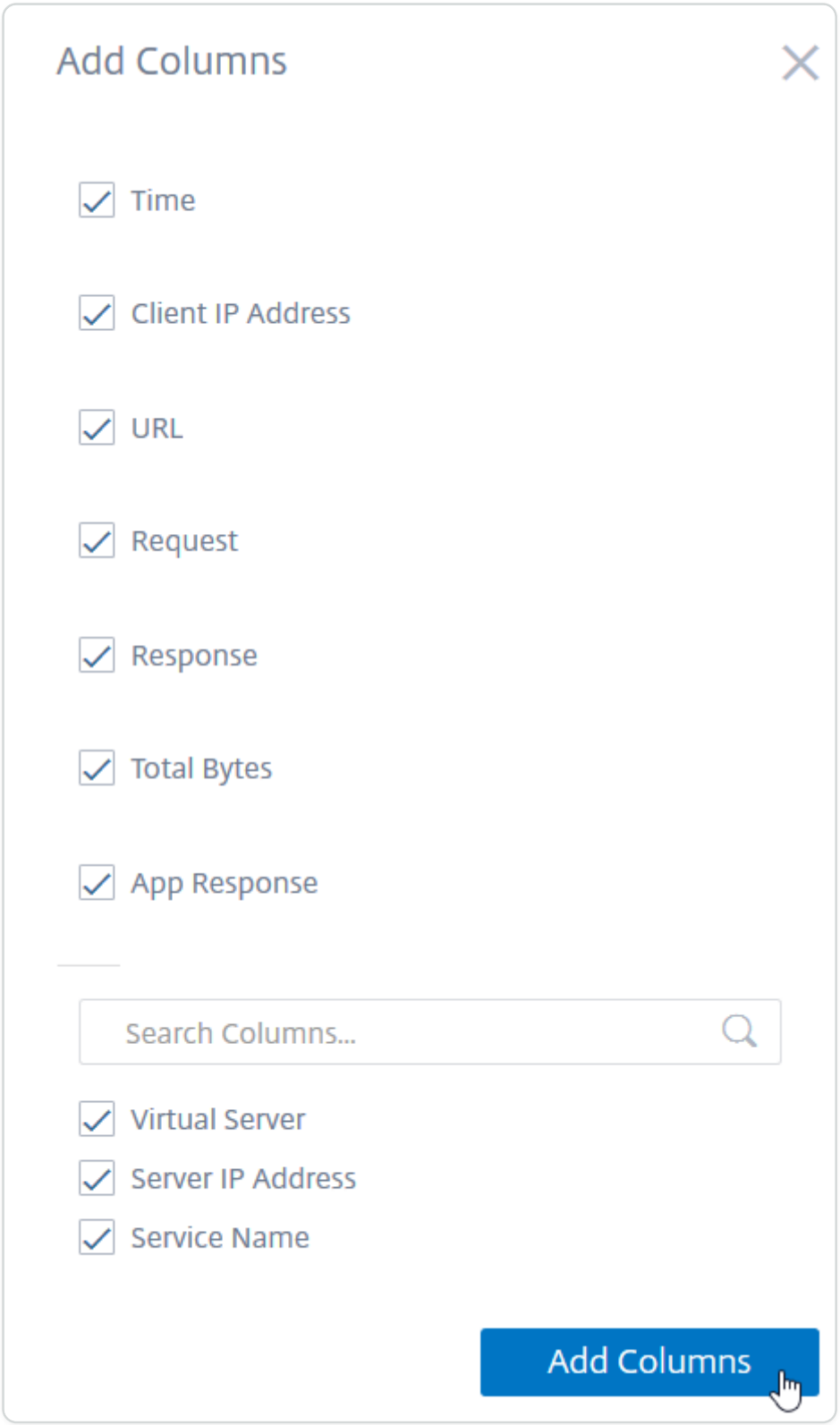
Add columns in the event list

You can click the



button to choose the list of options and click **Add Columns** to get the details displayed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Advanced search

The **Transaction Summary** also has a search text box and time duration list, where you can view the events as per your requirement. When you place the cursor in the search box, the search box gives you a list of search suggestions. You can also use operators in your search queries to narrow the focus of your search.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

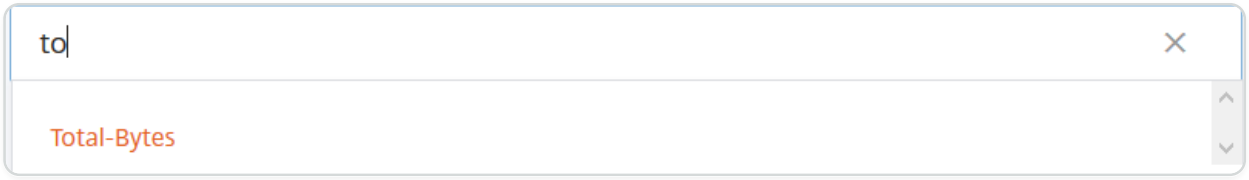
The following are the operators you can use for your search queries:

OPERATORS	DESCRIPTION	EXAMPLE	OUTPUT
=	Equals to some value	Virtual-Server = test	Displays the event for the virtual server with the name "test"
>	Greater than some value	App-Response-Time > 500	Displays the events for the applications that have the app response with more than 500 ms
<	Lesser than some value	App-Response-Time < 300	Displays the events for the applications that have the app response time with less than 300 ms
>=	Greater or equal to some value	Total-Bytes >= 1024	Displays the events for the transactions with greater or equal to 1 kb
<=	Less or equal to some value	Total-Bytes <= 1024	Displays the events for the transactions with lesser or equal to 1 kb
!=	Not equal to some value	Response-code != 200	Displays the events with all transactions, except the failed transactions.
~	Contains some value	Virtual-Server ~ mas	Displays the events for the virtual servers that have the name mas.

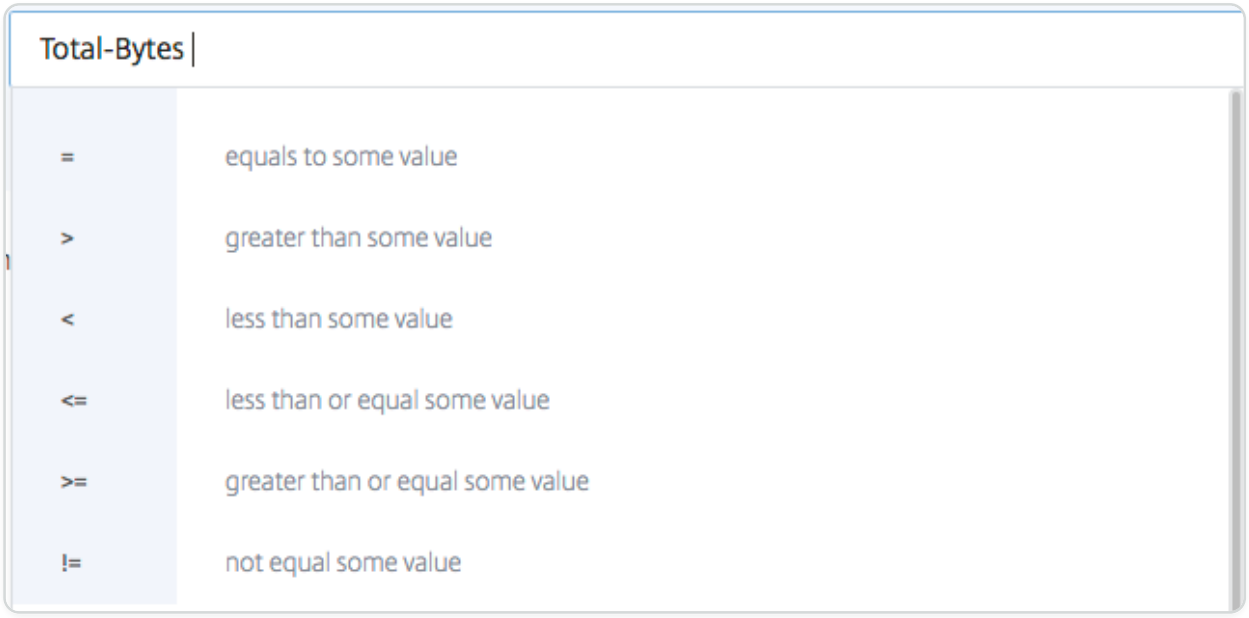
For example, consider a scenario that you want to generate events for total bytes that are lesser than 300 bytes. Specify the search queries as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Specify the required word in the search box to get the related suggestions.



2. Select **Total-Bytes** and click again on the search text box, and select **\<**.

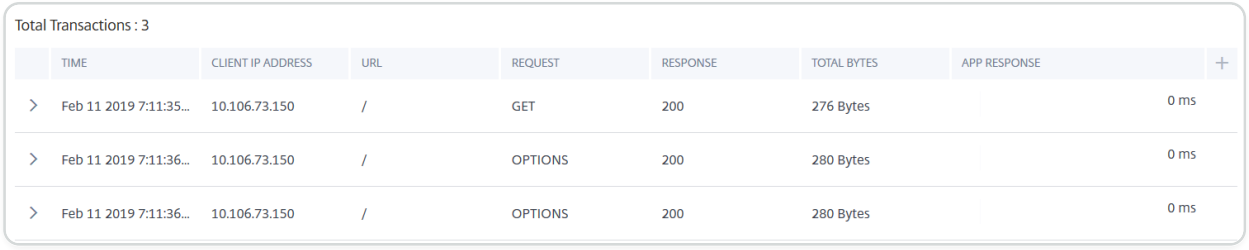


3. Type the value 300.



4. Select the time period and click **Search** to view the events based on your search query.

   The search result is displayed.

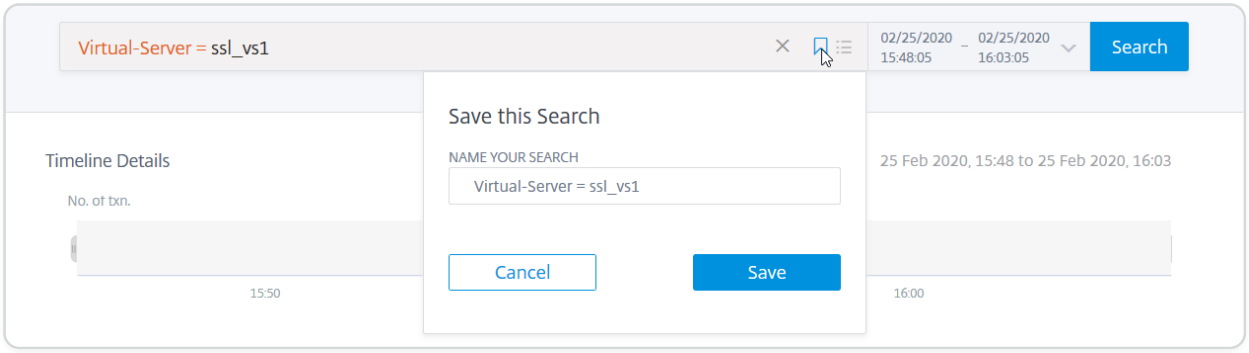


Save search

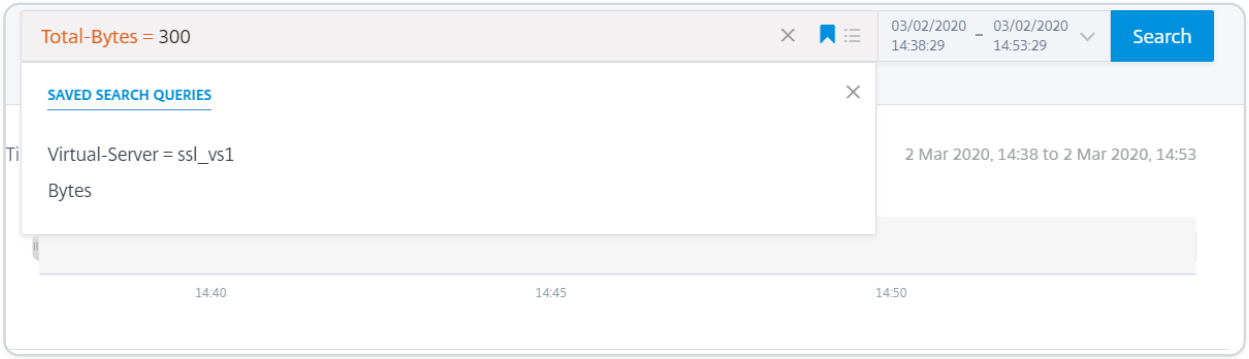
After you use the suggestions and operators, you can save the search query. You can then use it later from the list, instead of using the suggestions and operators again.

- To save a search query, click the bookmark icon, specify a name of your choice, and then click **Save**.

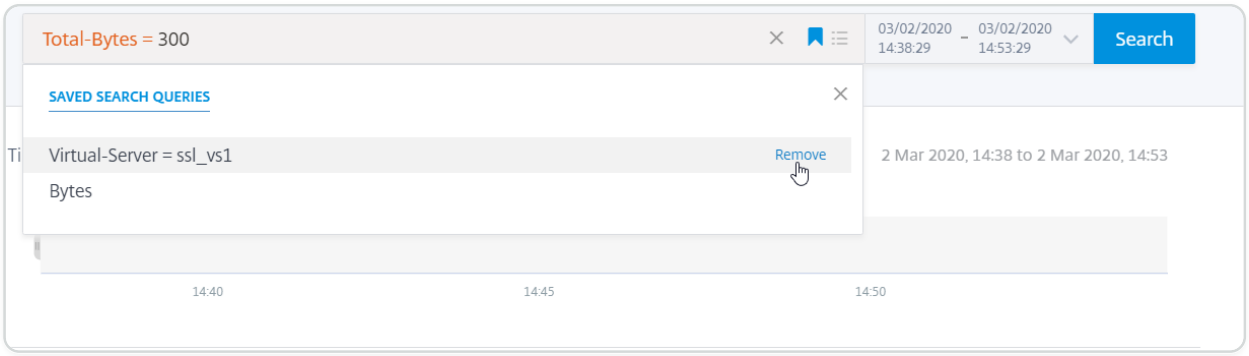
© 1997–2026 Citrix Systems, Inc. All rights reserved.



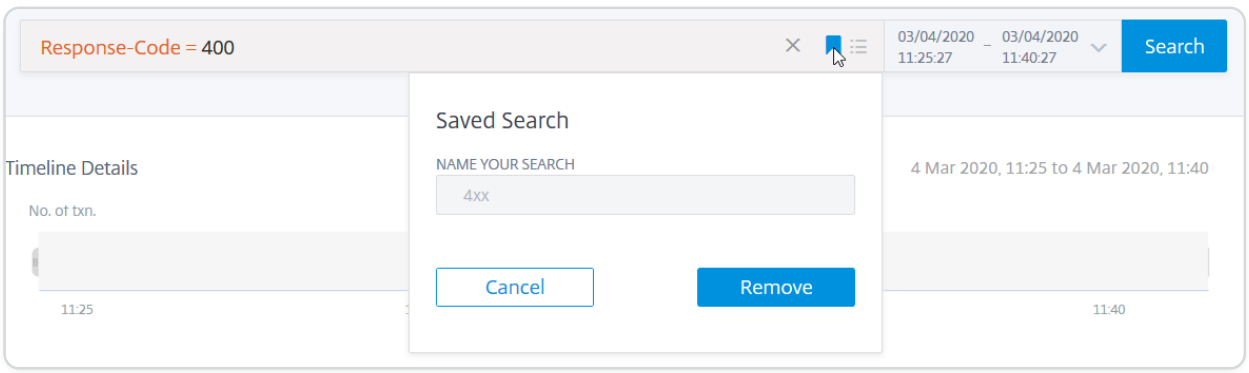
- To use the search query from the list, click the icon and select the search query from the list to display the results.



- To remove the search query, click the icon, hover the mouse pointer on the saved search query, click **Remove**.



You can also click the bookmark icon and click **Remove**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Export data

You can export the web transaction analytics data for the selected duration by clicking the **Export** icon. You can export in PDF, PNG, JPEG, and CSV formats. The **Export** option enables you to do one of the following:

- Select **Export Now** to view and export the report in PDF, JPEG, PNG, or CSV format.
- Select **Schedule Export** tab to schedule the report daily, weekly, or monthly and send the report over an email or a Slack message.

Detailed procedures to setup dual tier or service mesh lite topology

The prerequisites to deploy the dual tier or service mesh lite topology is available at Setting up service graph.

Configure a NetScaler agent

To enable communication between Kubernetes cluster and NetScaler Console, you must install and configure an agent. You can configure an agent using a hypervisor, public cloud services (such as Microsoft Azure, AWS), or built-in agent available on NetScaler instances (ideal for HA deployments).

Follow the procedure to configure an agent.

NOTE

- You can also use an existing agent.
- The agents are, by default, automatically upgraded to NetScaler Console latest build. You can view the agent details on the **Infrastructure > Instances > Agents** page. You can also specify the time when you want the agent upgrades to happen. For more information, see Configuring Agent Upgrade Settings.

Configure static routes in the agent

Inside the Kubernetes cluster, all containerized pods use an overlay network. Establishing the communication using those private IP addresses directly is not possible. To enable communication from NetScaler Console to Kubernetes cluster, you must configure static routing in the agent.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

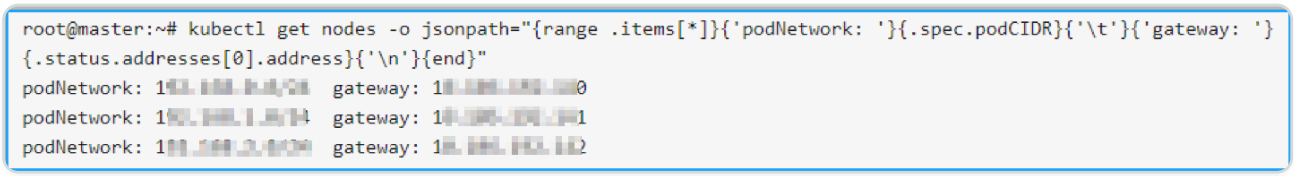
Consider that you have the following IP addresses for your Kubernetes cluster:

- Kubernetes master – 101.xx.xx.112
- Kubernetes worker 1 – 101.xx.xx.111
- Kubernetes worker 2 – 101.xx.xx.110

On the Kubernetes master, run the following command to identify the pod network to do the static routing:

```
kubectl get nodes -o jsonpath="{range .items[*]}{'podNetwork: '}{.spec.podCIDR}{'\t'}{'gateway: '}{.status.addresses[0].address}{'\n'}{end}"
```

The following is an example output after you run the command:



After successfully configuring an agent:

1. Using an SSH client, log on to the agent
2. Type `shell` and press **Enter** to switch to `bash`
3. Configure the static routing using the command `route add -net <public IP address range> <Kubernetes IP address>`

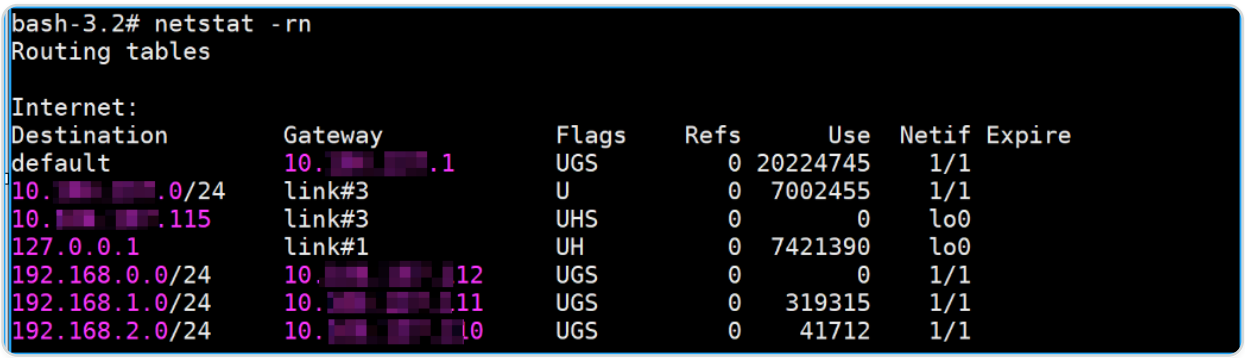
   For example:

   ```
   route add -net 192.168.0.0/24 101.xx.xx.112
   ```

   ```
   route add -net 192.168.1.0/24 101.xx.xx.111
   ```

   ```
   route add -net 192.168.2.0/24 101.xx.xx.110
   ```

4. Verify the configuration by using `netstat -rn`



© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Append these route commands in `/mpsconfig/svm.conf` file.

    a. In NetScaler agent, access the **svm.conf** file using the following command:

    `vim /mpsconfig/svm.conf`

    b. Add the static routes in **svm.conf** file.

    For example, `route add -net 192.168.0.0/24 101.xx.xx.112`.

Download the sample deployment files from GitHub

1. Use the command **git clone** `https://github.com/citrix/citrix-k8s-ingress-controller.git` to clone the git hub repository in the master node.
2. To access the YAMLs:

    `cd citrix-k8s-ingress-controller/example/servicegraph-demo/`

Add parameters in CPX YAML file

NOTE

If you are using CPX 58.x or later, you must use the non-nsroot password while registering to the agent. To ensure security, NetScaler agent 61.x or later releases need mandatory password change. If your NetScaler agent is upgraded to 61.x or latest version, you must ensure to use **CPX 58.x or later** build.

You must include the following parameters in the `cpx.yaml` file to ensure CPX registration with NetScaler Console:

```
- name: "NS_MGMT_SERVER"

  value: "xx.xx.xx.xx"

- name: "NS_MGMT_FINGER_PRINT"

  value: "xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx"

- name: "NS_HTTP_PORT"

  value: "9080"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
- name: "NS_HTTPS_PORT"

  value: 9443"

- name: "NS_MGMT_USER"

  value: "nsroot"

- name: "NS_MGMT_PASS"

  value: <your password>

- name: "LOGSTREAM_COLLECTOR_IP"

  value: "xx.xx.xx.xx"
```

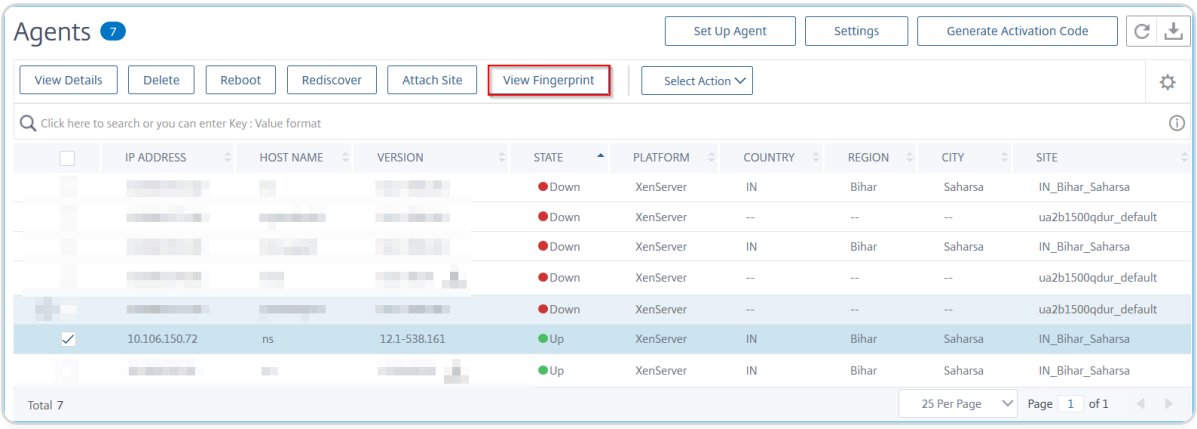
```
- name: "EULA"
  value: "yes"
- name: "KUBERNETES_TASK_ID"
  value: ""
- name: "NS_MGMT_SERVER"
  value: "10.104.146.232"
- name: "NS_MGMT_FINGERPRINT"
  value: "EA:E3:15:6C:E8:B3:73:99:CB:62:56:6E:69:EB:AD:95:B8:E1:86:F4"
- name: "NS_HTTP_PORT"
  value: "9080"
- name: "NS_HTTPS_PORT"
  value: "9443"
- name: "NS_MGMT_USER"
  value: "nsroot"
- name: "NS_MGMT_PASS"
  value: "TTls123$%^"
- name: "LOGSTREAM_COLLECTOR_IP"
  value: "10.104.146.232"
```

- **NS_MGMT_SERVER** – Indicates the agent IP address
- **NS_MGMT_FINGER_PRINT** – Indicates the authentication for CPX in the agent. To get the fingerprint:

  a. In NetScaler Console, navigate to **Infrastructure > Instances > Agents**

  b. Select the agent and then click **View Fingerprint**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **NS_HTTP_PORT** – Indicates the HTTP port for communication
- **NS_HTTPS_PORT** – Indicates the HTTPS port for communication
- **NS_MGMT_USER** - Indicates the user name
- **NS_MGMT_PASS** - Indicates the password. Specify a password of your choice
- **LOGSTREAM_COLLECTOR_IP** – Indicates the agent IP address, where **Logstream** protocol must be enabled to transfer log data from CPX to NetScaler Console

Add VPX or SDX or MPX or BLX instance in NetScaler Console

To get the tier-1 NetScaler instance analytics in service graph, you must add the VPX/SDX/MPX/BLX instance in NetScaler Console and enable **Web Insight**. You must enable **Web Insight** for NetScaler Console to display the web transaction details from the VPX/SDX/MPX/BLX instance.

1. Navigate to **Infrastructure > Instances > NetScaler**
2. Click the **Add** option to add the instance. For more information, see Add instances in NetScaler Console
3. After adding the instance, select the virtual server and enable **Web Insight**. For more information, see Manage licensing and enable analytics on virtual servers

Add Kubernetes cluster in NetScaler Console

To add the Kubernetes cluster:

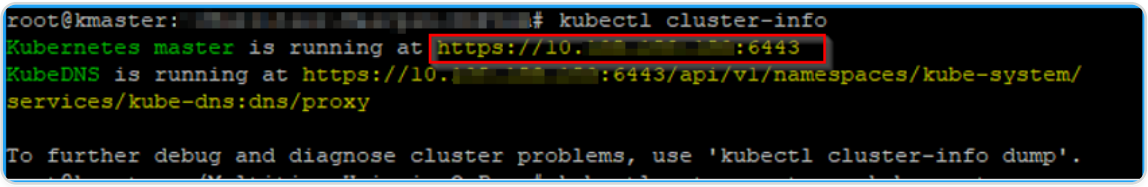
1. Log on to NetScaler Console with administrator credentials.
2. Navigate to **Infrastructure > Orchestration> Kubernetes > Cluster**. The Clusters page is displayed.
3. Click **Add**.
4. In the **Add Cluster** page, specify the following parameters:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. **Name** - Specify a name of your choice.

b. **API Server URL** - You can get the API Server URL details from the Kubernetes Master node.

   i. On the Kubernetes master node, run the command `kubectl cluster-info`.



   ii. Enter the URL that displays for **“Kubernetes master is running at.”**

c. **Authentication Token** - Specify the authentication token. The authentication token is required to validate access for communication between Kubernetes cluster and NetScaler Console. To generate an authentication token:

   On the Kubernetes master node:

   i. Use the following YAML to create a service account:

```
apiVersion: v1

kind: ServiceAccount

metadata:

  name: <name>

  namespace: <namespace>
```

   ii. Run `kubectl create -f <yaml file>`.

   The service account is created.

   iii. Run `kubectl create clusterrolebinding <name> --clusterrole=cluster-admin --serviceaccount=<namespace>:<name>` to bind the cluster role to service account.

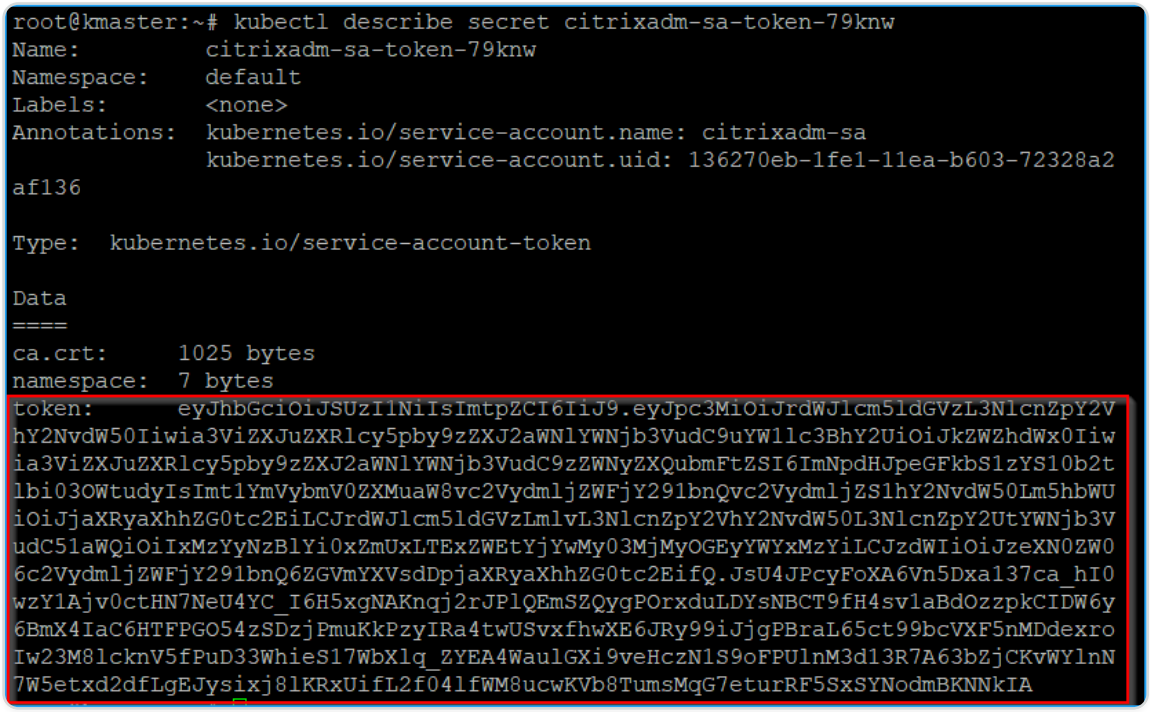
   The service account now has the cluster-wide access.

   A token is automatically generated while creating the service account.

   iv. Run `kubectl describe sa <name>` to view the token.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

v. To get the secret string, run `kubectl describe secret <token-name>`.



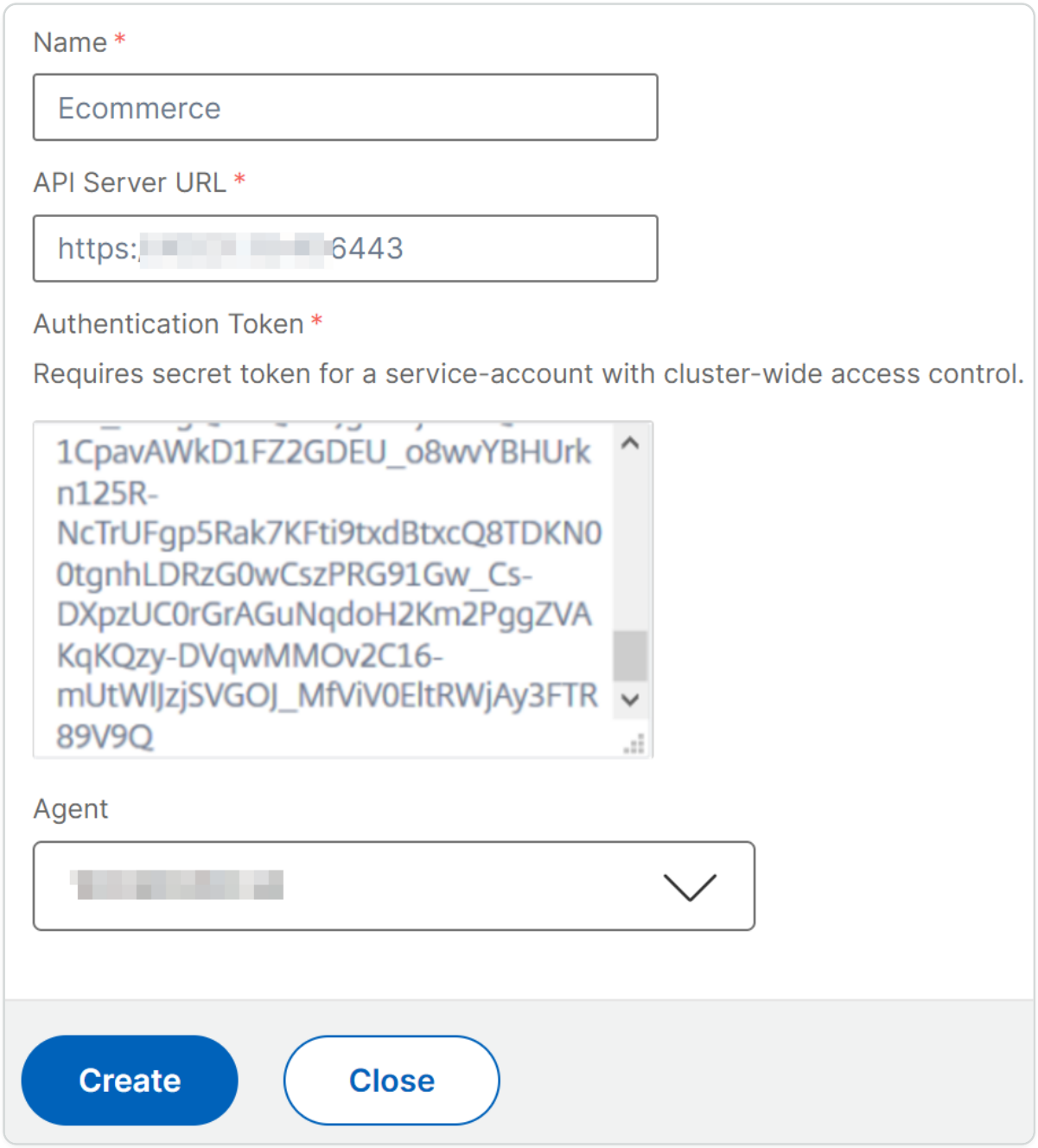
d. Select the agent from the list.

Note

Ensure to select the same agent that you have added in the CPX YAML.

e. Click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Deploy a sample microservice application

On the master node:

1. Run `kubectl create -f namespace.yaml` to create a namespace.
2. Deploy `hotdrink` microservices, ingress, and secrets using following commands:

   ```
   kubectl create -f team_hotdrink.yaml -n sg-demo
   ```

   ```
   kubectl create -f hotdrink-secret.yaml -n sg-demo
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Deploy CPX and register CPX in NetScaler Console

1. Run `kubectl create -f rbac.yaml` to deploy cluster role and cluster binding.
2. Run `kubectl create -f cpx.yaml -n sg-demo` to deploy CPX.

After the deployment, the CPX registration is automatically done.

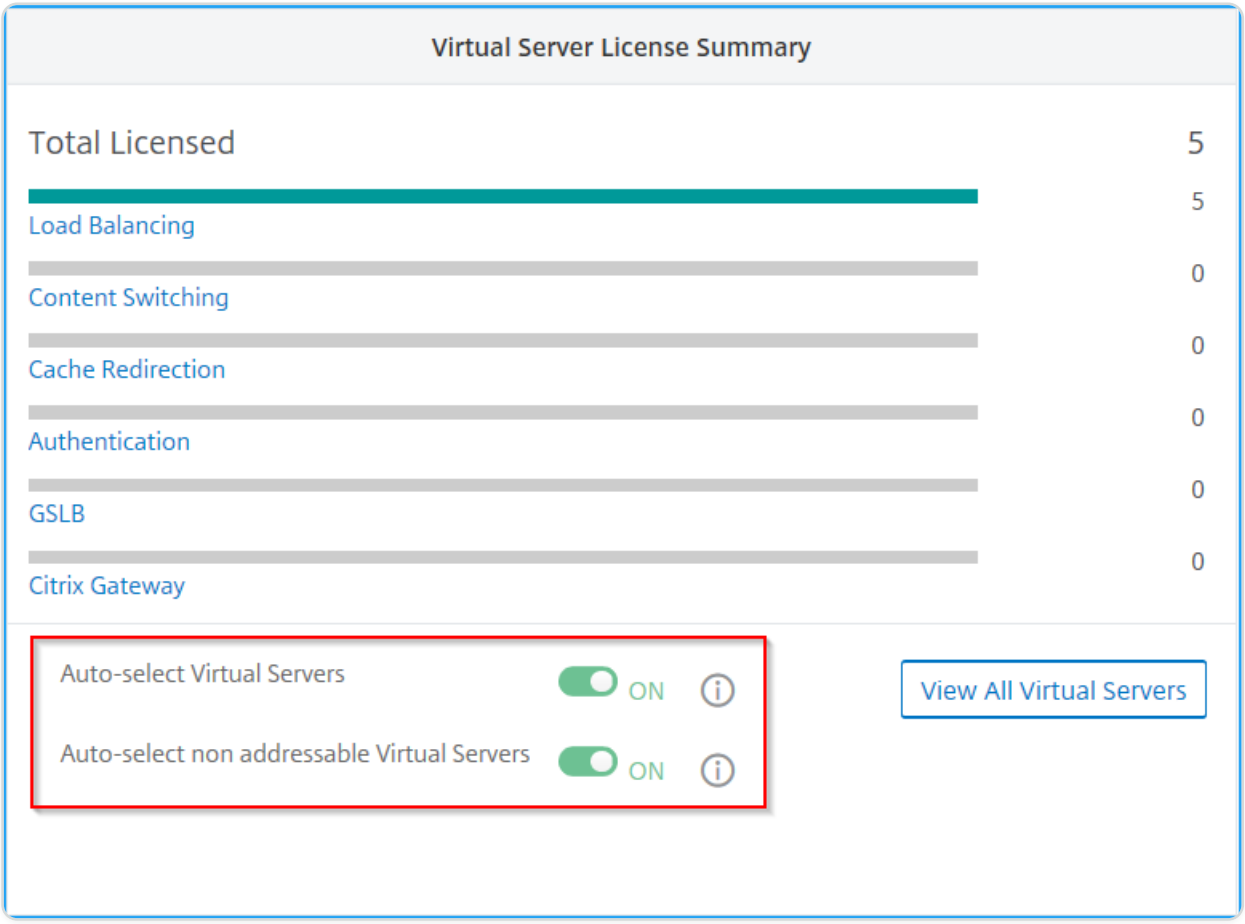
Enable auto select virtual servers for licensing

Note

> Ensure you have sufficient virtual server licenses. For more information, see Licensing

After you add Kubernetes cluster in NetScaler Console, you must ensure to auto-select virtual servers for licensing. CPX virtual servers must be licensed to display data in service graph. To auto-select virtual servers:

1. Navigate to **Settings > NetScaler Console Licensing & Analytics Config**.
2. Under **Virtual Server License Summary**, enable **Auto-select Virtual Servers** and **Auto-select non addressable Virtual Servers**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

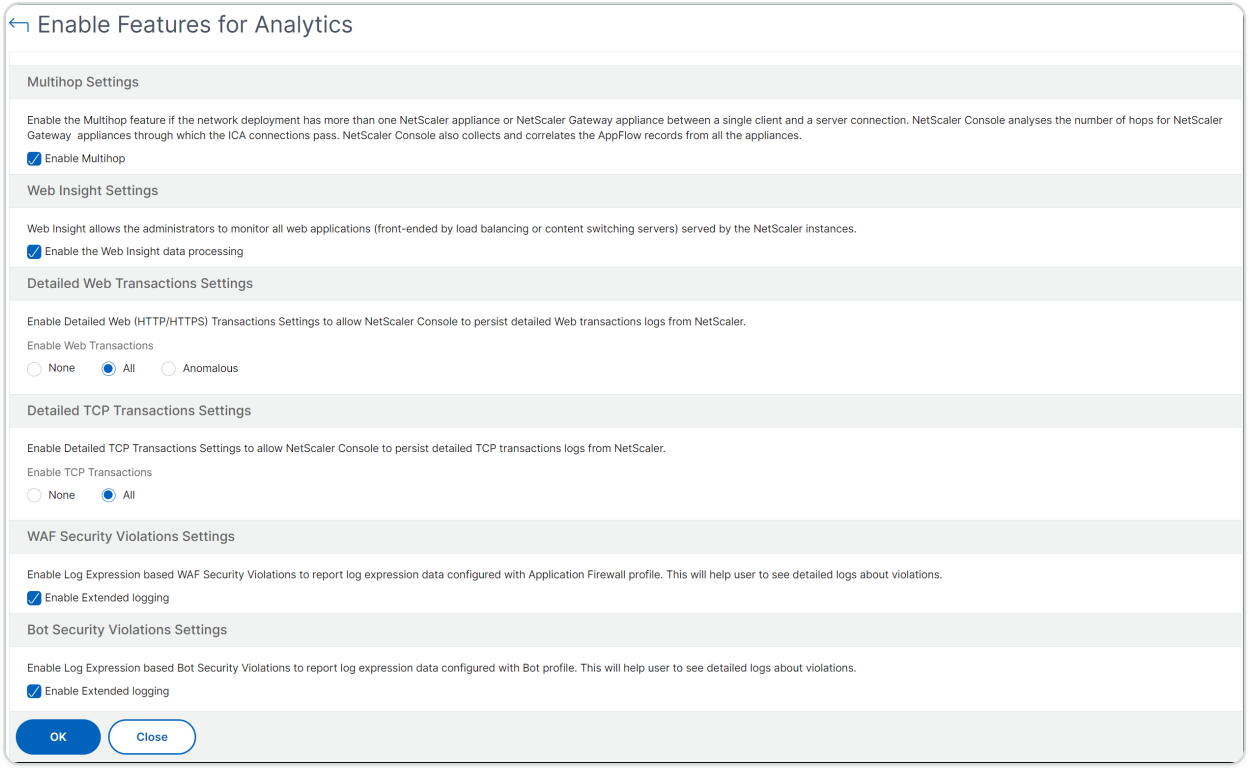
Enable Web Transaction and TCP Transaction settings

After you add the Kubernetes cluster and enable the auto-select virtual servers, change the **Web Transaction Settings** and **TCP Transactions Settings** to **All**.

1. Navigate to **Settings > Analytics Settings**.

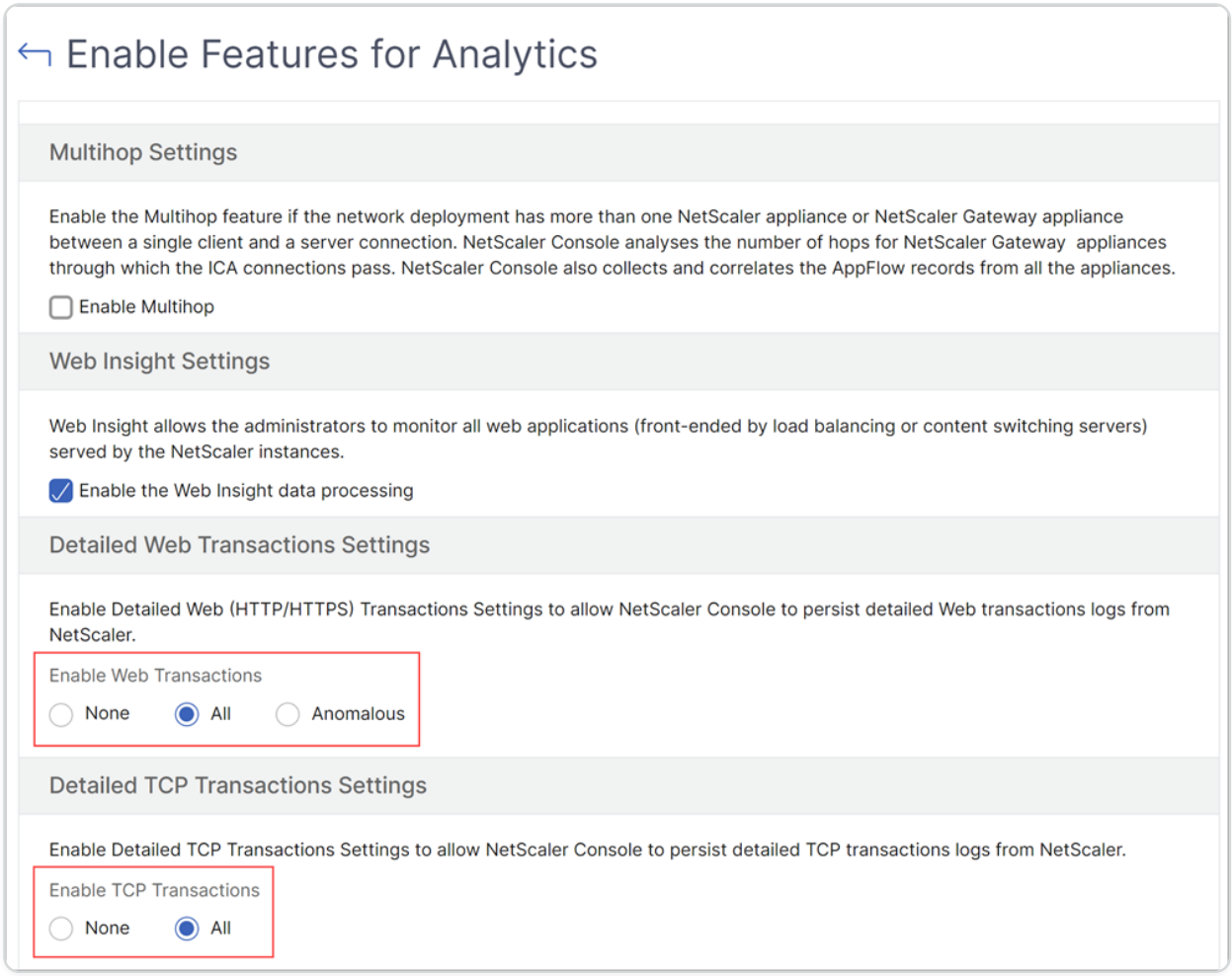
   The **Settings** page is displayed.

2. Click **Enable Features for Analytics**.
3. Under **Web Transaction Settings**, select **All**.



4. Under **TCP Transactions Settings**, select **All**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Click **OK**.

Send traffic to microservices

Next, you must send traffic to microservices to get the service graph populated in NetScaler Console.

1. Run `kubectl get svc -n sg-demo` to expose CPX through NodePort.

```
root@adm-cic-master:~/adm# kubectl get svc -n sg-demo
NAME                  TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)
 AGE
coffee                ClusterIP   10.102.13.37    <none>        80/TCP,443/TCP
 83s
coffee-beverage       ClusterIP   None            <none>        80/TCP,443/TCP
 83s
cpx-service           NodePort    10.98.190.208   <none>        80:30402/TCP,443:32042/TCP
 34s
frontend-hotdrinks    ClusterIP   None            <none>        80/TCP,443/TCP
 83s
lb-service-hotdrinks  ClusterIP   None            <none>        80/TCP,443/TCP
 33s
tea                   ClusterIP   10.103.233.53   <none>        80/TCP,443/TCP
 83s
tea-beverage          ClusterIP   None            <none>        80/TCP,443/TCP
 83s
```

2. Edit the **etc/host** file and create a domain IP entry for `hotdrink.beverages.com`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can now access the microservice using `https://hotdrink.beverages.com`

Detailed procedures to setup service mesh topology

The prerequisites to deploy the service mesh topology is available at Setting up service graph.

Configure NetScaler agent

To enable communication between Kubernetes cluster and NetScaler Console, you must install and configure an agent. You can configure an agent using a hypervisor, public cloud services (such as Microsoft Azure, AWS), or built-in agent available on NetScaler instances (ideal for HA deployments).

Follow the procedure to configure an agent.

NOTE

- You can also use an existing agent.
- The agents are, by default, automatically upgraded to NetScaler Console latest build. You can view the agent details on the **Infrastructure > Instances > Agents** page. You can also specify the time when you want the agent upgrades to happen. For more information, see Configuring Agent Upgrade Settings.

Configure static routes in the agent

Inside the Kubernetes cluster, all containerized pods use an overlay network. Establishing the communication using those private IP addresses directly is not possible. To enable communication from NetScaler Console to Kubernetes cluster, you must configure static routing in the agent.

Consider that you have the following IP addresses for your Kubernetes cluster:

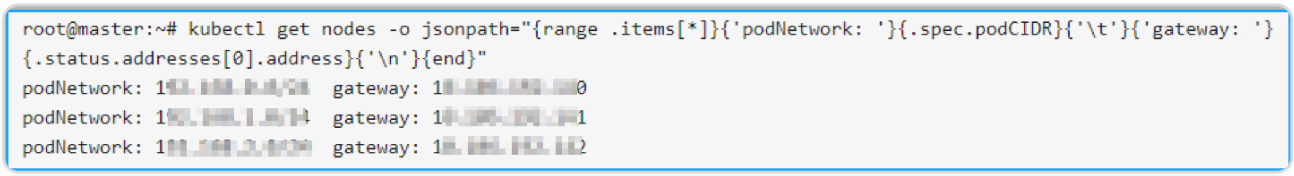
- Kubernetes master – 101.xx.xx.112
- Kubernetes worker 1 – 101.xx.xx.111
- Kubernetes worker 2 – 101.xx.xx.110

On the Kubernetes master, run the following command to identify the pod network to do the static routing:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
kubectl get nodes -o jsonpath="{range .items[*]}{'podNetwork: '}{.spec.podCIDR}{'\t'}{'gateway: '}{.status.addresses[0].address}{'\n'}{end}"
```

The following is an example output after you run the command:



After successfully configuring an agent:

1. Using an SSH client, log on to the agent
2. Type `shell` and press **Enter** to switch to `bash`
3. Configure the static routing using the command `route add -net <public IP address range> <Kubernetes IP address>`

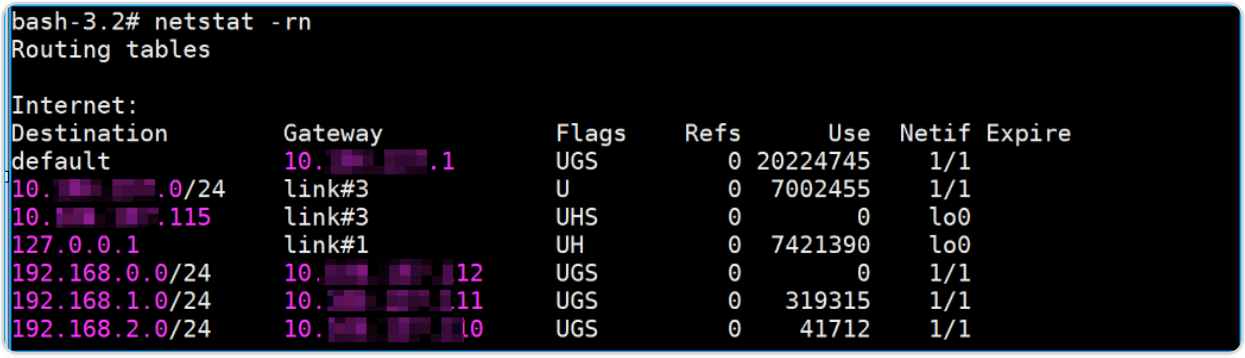
   For example:

   ```
   route add -net 192.168.0.0/24 101.xx.xx.112
   ```

   ```
   route add -net 192.168.1.0/24 101.xx.xx.111
   ```

   ```
   route add -net 192.168.2.0/24 101.xx.xx.110
   ```

4. Verify the configuration by using `netstat -rn`

5. Append these route commands in `/mpsconfig/svm.conf` file.

   a. In the agent, access the **svm.conf** file using the following command:

      ```
      vim /mpsconfig/svm.conf
      ```

   b. Add the static routes in **svm.conf** file.

      For example, `route add -net 192.168.0.0/24 101.xx.xx.112`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure the required parameters

In the Kubernetes master:

1. Create secret with the agent credentials in every namespace where CPX as an ingress gateway / sidecar is deployed.

   ```
   kubectl create secret generic admlogin --from-literal=username=<username> --from-literal=password=<password> -n <namespace>
   ```

2. ```
   helm repo add citrix https://citrix.github.io/citrix-helm-charts/
   ```

3. Deploy the NetScaler CPX as an Ingress Gateway

   ```
   helm install citrix-adc-istio-ingress-gateway citrix/citrix-adc-istio-ingress-gateway --version 1.2.1 --namespace <namespace> --set ingressGateway.EULA=YES,citrixCPX=true,ADMSettings.ADMFingerPrint=XX:00:X1:00:XX:0X:X0,A
   ingressGateway.image=quay.io/citrix/citrix-k8s-cpx-ingress,ingressGateway.tag=13.0-58.30
   ```

   The following table lists the configurable parameters in the Helm chart and its default values:

PARAMETER	DESCRIPTION	DEFAULT	OPTIONAL/ MANDATORY (HELM)
citrixCPX	NetScaler CPX	FALSE	Mandatory for NetScaler CPX
xDSAdaptor.image	Image of the Citrix xDS adaptor container	quay.io/citrix/citrix-istio-adaptor:1.2.1	Mandatory
ADMSettings.ADMIP	NetScaler Console IP address	null	Mandatory for NetScaler CPX
ADMSettings.ADMFingerPrint	The NetScaler Console Fingerprint. Navigate to **Infrastructure > Instances > Agents**, select the agent, and click **View Fingerprint**	null	Optional

© 1997–2026 Citrix Systems, Inc. All rights reserved.
   ```

PARAMETER	DESCRIPTION	DEFAULT	OPTIONAL/ MANDATORY (HELM)
ingressGateway.EULA	End User License Agreement(EULA) terms and conditions. If yes, then user agrees to EULA terms and conditions.	NO	Mandatory for NetScaler CPX
ingressGateway.image	Image of NetScaler CPX designated to run as Ingress Gateway	quay.io/citrix/citrix-k8s-cpx-ingress:13.0–58.30	Mandatory for NetScaler CPX

4. Deploy the Citrix SideCar Injector.

```
helm install cpx-sidecar-injector citrix/citrix-cpx-istio-sidecar-injector --version 1.2.1 --namespace <namespace> set cpxProxy.EULA=YES,ADMSettings.ADMFingerPrint=xx:xx:xx:xx,ADMSettings.ADMIP=<xx.xx.xx.xx> citrix/citrix-k8s-cpx-ingress,cpxProxy.tag=13.0-58.30
```

The following table lists the configurable parameters in the Helm chart and its default values:

PARAMETER	DESCRIPTION	DEFAULT VALUE
ADMSettings.ADMIP	The NetScaler Console IP address	NIL
cpxProxy.image	NetScaler CPX image used as sidecar proxy	quay.io/citrix/citrix-k8s-cpx-ingress:13.0–58.30
cpxProxy.imagePullPolicy	Image pull policy for NetScaler	IfNotPresent
cpxProxy.EULA	End User License Agreement(EULA) terms and conditions. If yes, then user agrees to EULA terms and conditions.	NO

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	DESCRIPTION	DEFAULT VALUE
cpxProxy.cpxSidecarMode	Environment variable for NetScaler CPX. It indicates that NetScaler CPX is running as sidecar mode or not.	YES

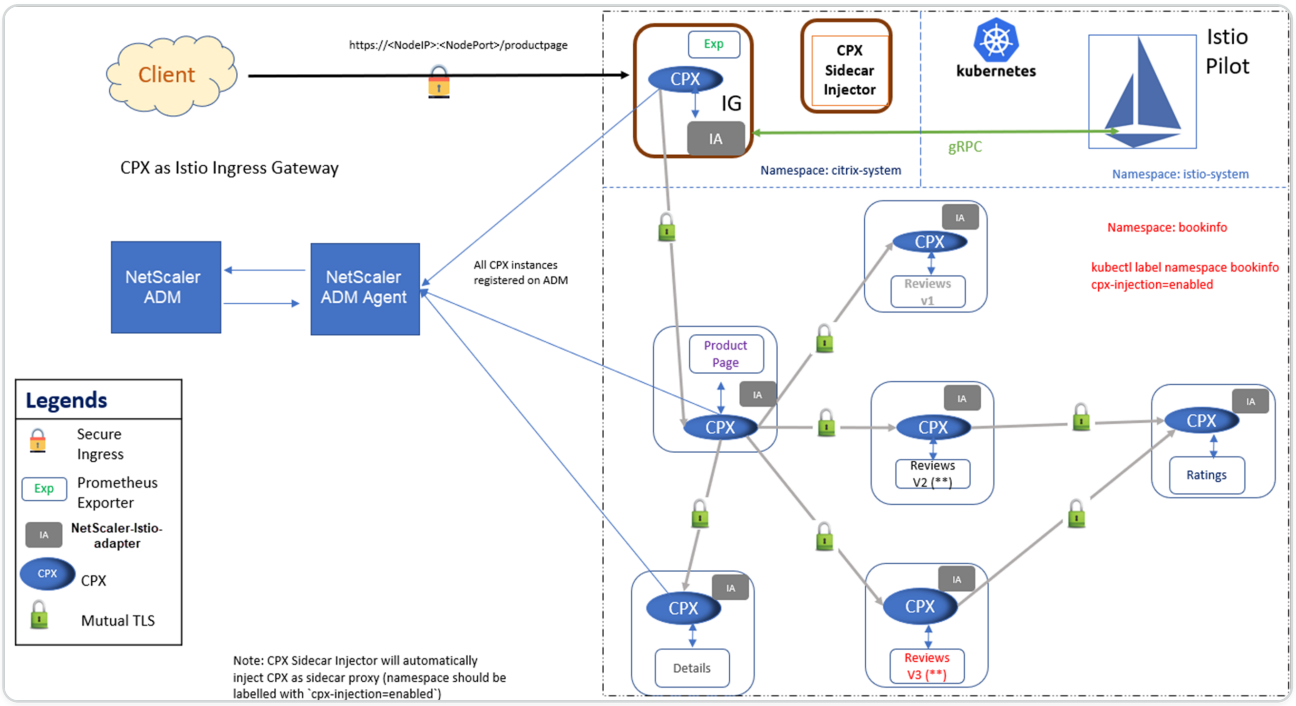
5. Set the label on any Namespace that needs CPX Sidecar Injection.

   ```
   kubectl label namespace <app-namespace> cpx-injection=enabled
   ```

   After performing step 3 and 5, you can see the NetScaler CPX is registered in NetScaler Console.

Deploy a sample application

Consider that you want to deploy the following applications:



Perform the following procedure to deploy a sample application:

1. `kubectl create namespace citrix-system`
2. `kubectl create namespace bookinfo`
3. `kubectl label namespace bookinfo cpx-injection=enabled`
4. `kubectl create secret generic admlogin --from-literal=username=<uername> --from-literal=password=<password> -n citrix-system`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Note

You can give a user name and a password of your choice.

5. `kubectl create secret generic admlogin --from-literal=username=<username> --from-literal=password=<password> -n bookinfo`

   Note

   You can give a user name and a password of your choice.

6. `helm install citrix-adc-istio-ingress-gateway citrix/citrix-adc-istio-ingress-gateway --version 1.2.1 --namespace citrix-system --set ingressGateway.EULA=YES,citrixCPX=true,ADMSettings.ADMFingerPrint=xx:xx:xx:xx,ADMSetting agent IP address>,ingressGateway.image=quay.io/citrix/citrix-k8s-cpx-ingress,ingressGateway.tag=13.0-58.30`

   Note

   You must give your NetScaler Console fingerprint and agent IP address

7. `helm install cpx-sidecar-injector citrix/citrix-cpx-istio-sidecar-injector --namespace citrix-system --set cpxProxy.EULA=YES,ADMSettings.ADMFingerPrint=xx:xx:xx:xx,ADMSettings.ADMIP=<ADM agent IP address>,cpxProxy.image=quay.io/citrix/citrix-k8s-cpx-ingress,cpxProxy.tag=13.0-58.30`

   Note

   You must give your NetScaler Console fingerprint and agent IP address

8. `helm install bookinfo bookinfo/ --namespace bookinfo --set citrixIngressGateway.namespace=citrix-system`

Add Kubernetes cluster in NetScaler Console

To add the Kubernetes cluster:

1. Log on to NetScaler Console with administrator credentials.

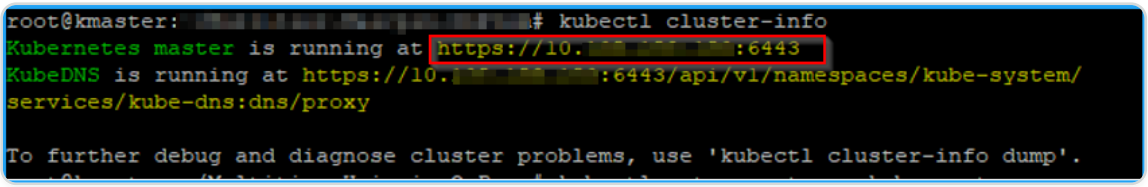
© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Navigate to **Infrastructure > Orchestration > Kubernetes > Cluster**. The Clusters page is displayed.
3. Click **Add**.
4. In the **Add Cluster** page, specify the following parameters:

    a. **Name** - Specify a name of your choice.

    b. **API Server URL** - You can get the API Server URL details from the Kubernetes Master node.

        i. On the Kubernetes master node, run the command `kubectl cluster-info`.

        ii. Enter the URL that displays for **"Kubernetes master is running at."**

    c. **Authentication Token** - Specify the authentication token. The authentication token is required to validate access for communication between Kubernetes cluster and NetScaler Console. To generate an authentication token:

    On the Kubernetes master node:

        i. Use the following YAML to create a service account:

        ```
        apiVersion: v1

        kind: ServiceAccount

        metadata:

          name: <name>

          namespace: <namespace>
        ```

        ii. Run `kubectl create -f <yaml file>`.

        The service account is created.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

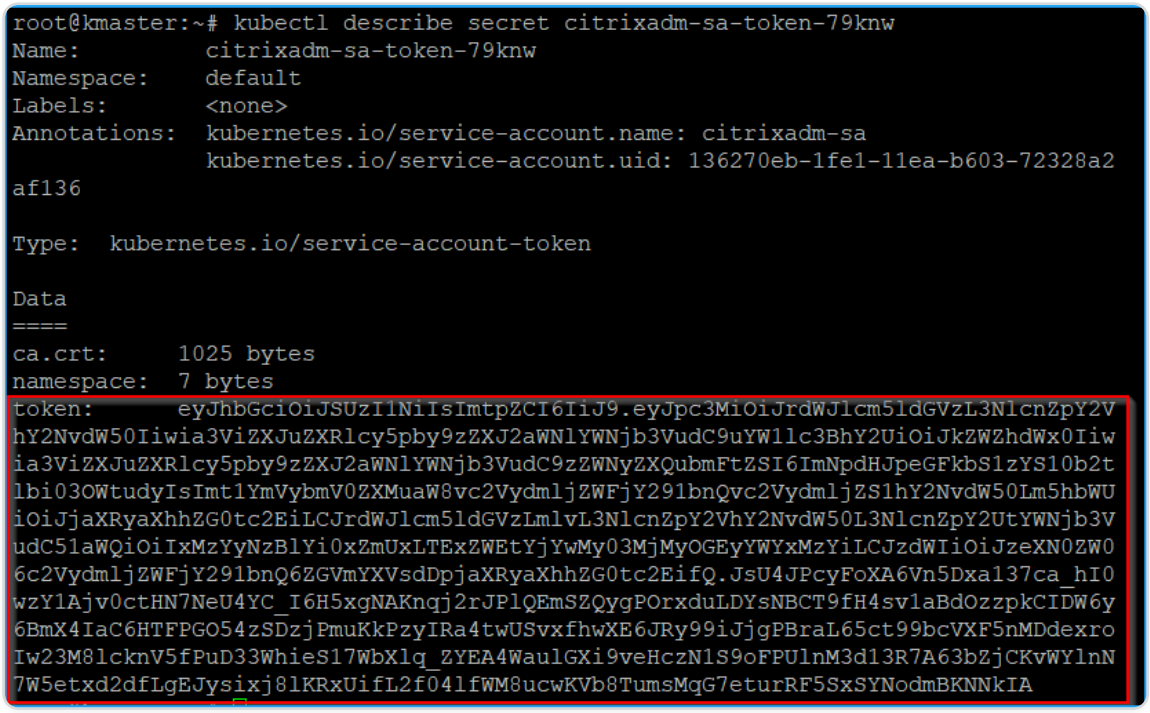
iii. Run `kubectl create clusterrolebinding <name> --clusterrole=cluster-admin --serviceaccount=<namespace>:<name>` to bind the cluster role to service account.

The service account now has the cluster-wide access.

A token is automatically generated while creating the service account.

iv. Run `kubectl describe sa <name>` to view the token.

v. To get the secret string, run `kubectl describe secret <token-name>`.



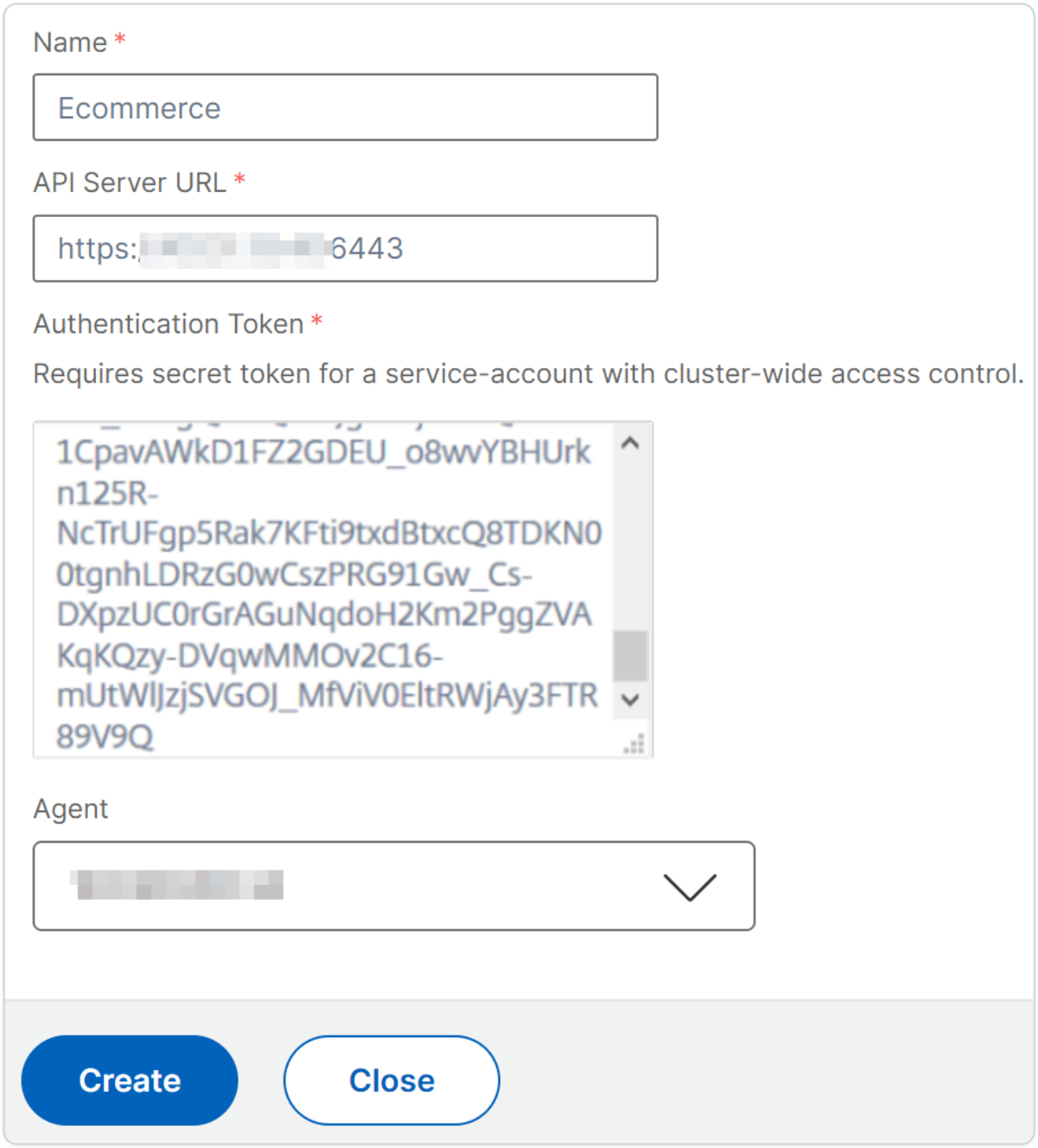
d. Select the agent from the list.

Note

> Ensure to select the same agent that you have added in the CPX YAML.

e. Click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Enable auto select virtual servers for licensing

Note

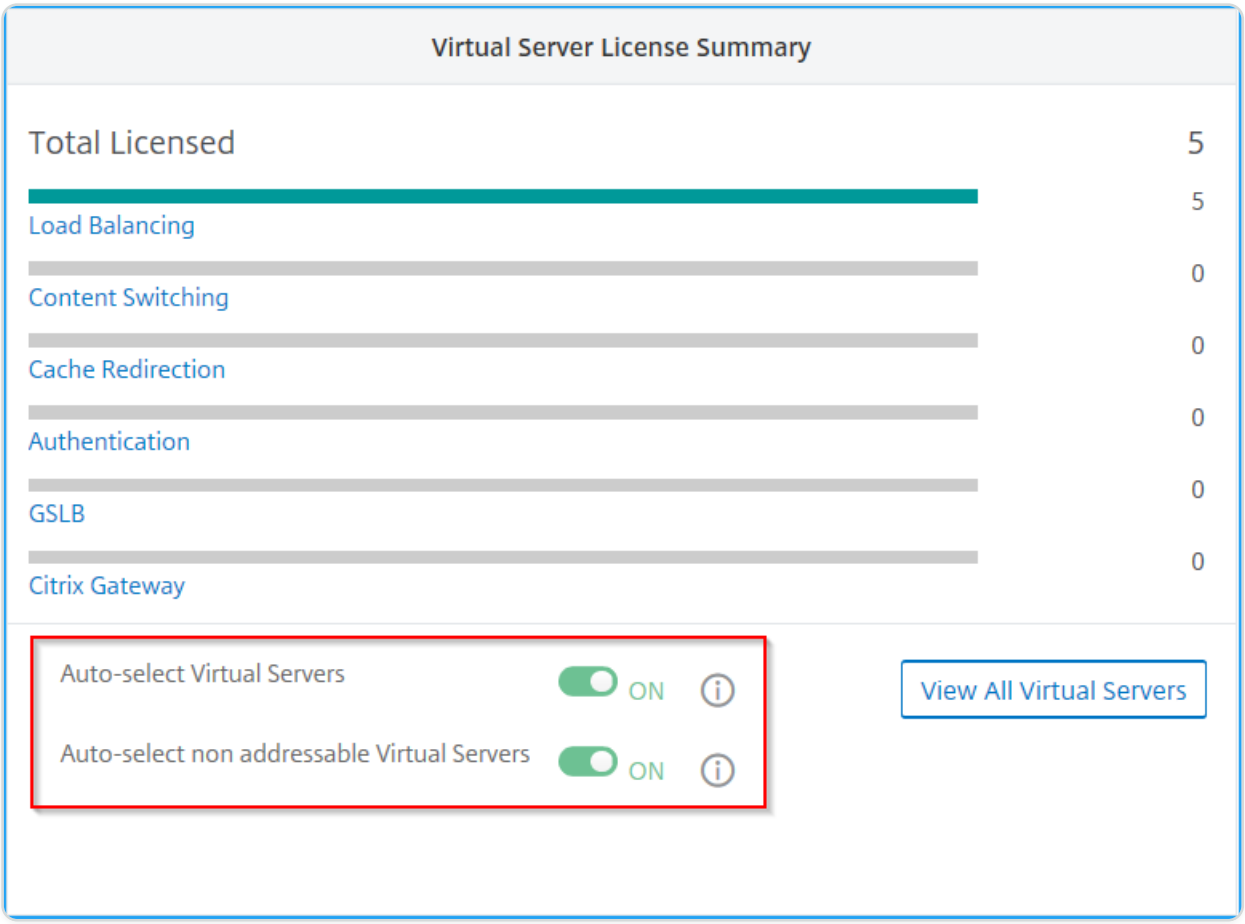
> Ensure you have sufficient virtual server licenses. For more information, see Licensing

After you add Kubernetes cluster in NetScaler Console, you must ensure to auto-select virtual servers for licensing. Virtual servers must be licensed to display data in Service Graph. To auto-select virtual servers:

1. Navigate to **Settings > NetScaler Console Licensing & Analytics Config**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Under **Virtual Server License Summary**, enable **Auto-select Virtual Servers** and **Auto-select non addressable Virtual Servers**.



Enable Web Transaction and TCP Transaction settings

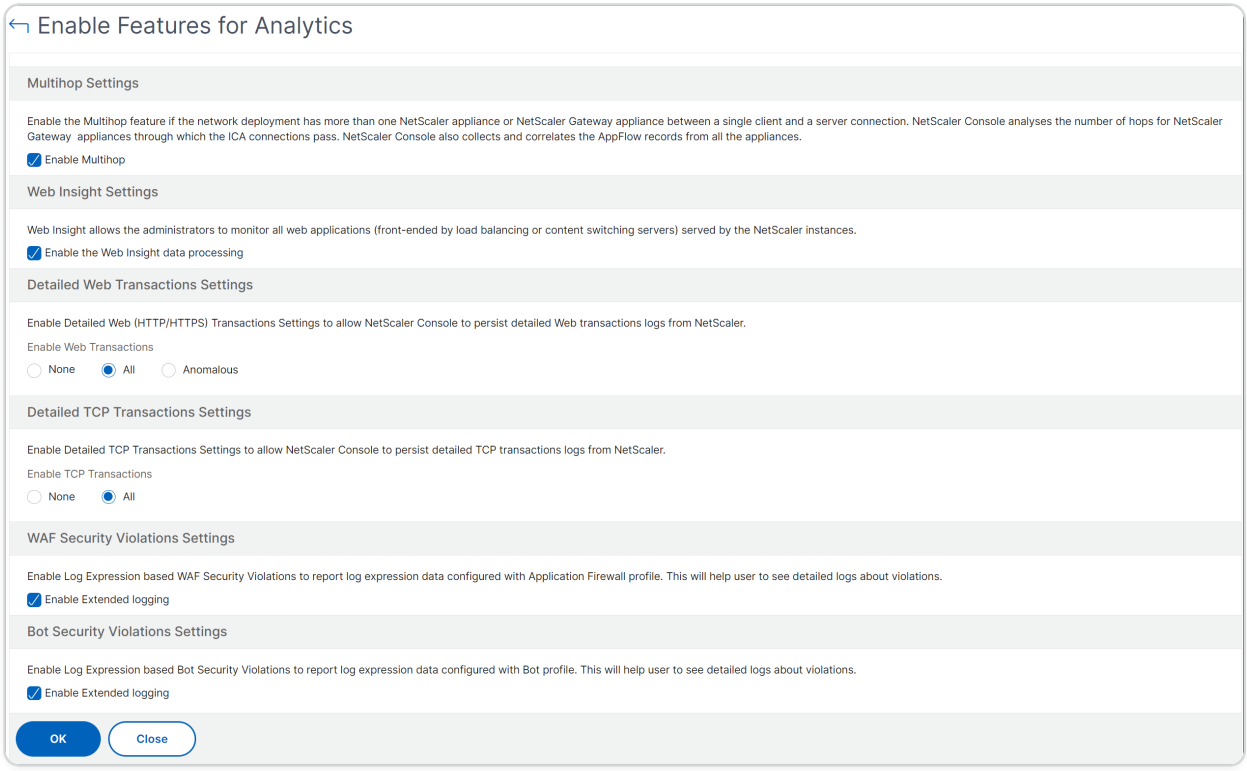
After you add the Kubernetes cluster and enable the auto-select virtual servers, change the **Web Transaction Settings** and **TCP Transactions Settings** to **All**.

1. Navigate to **Settings** > **Analytics Settings**.

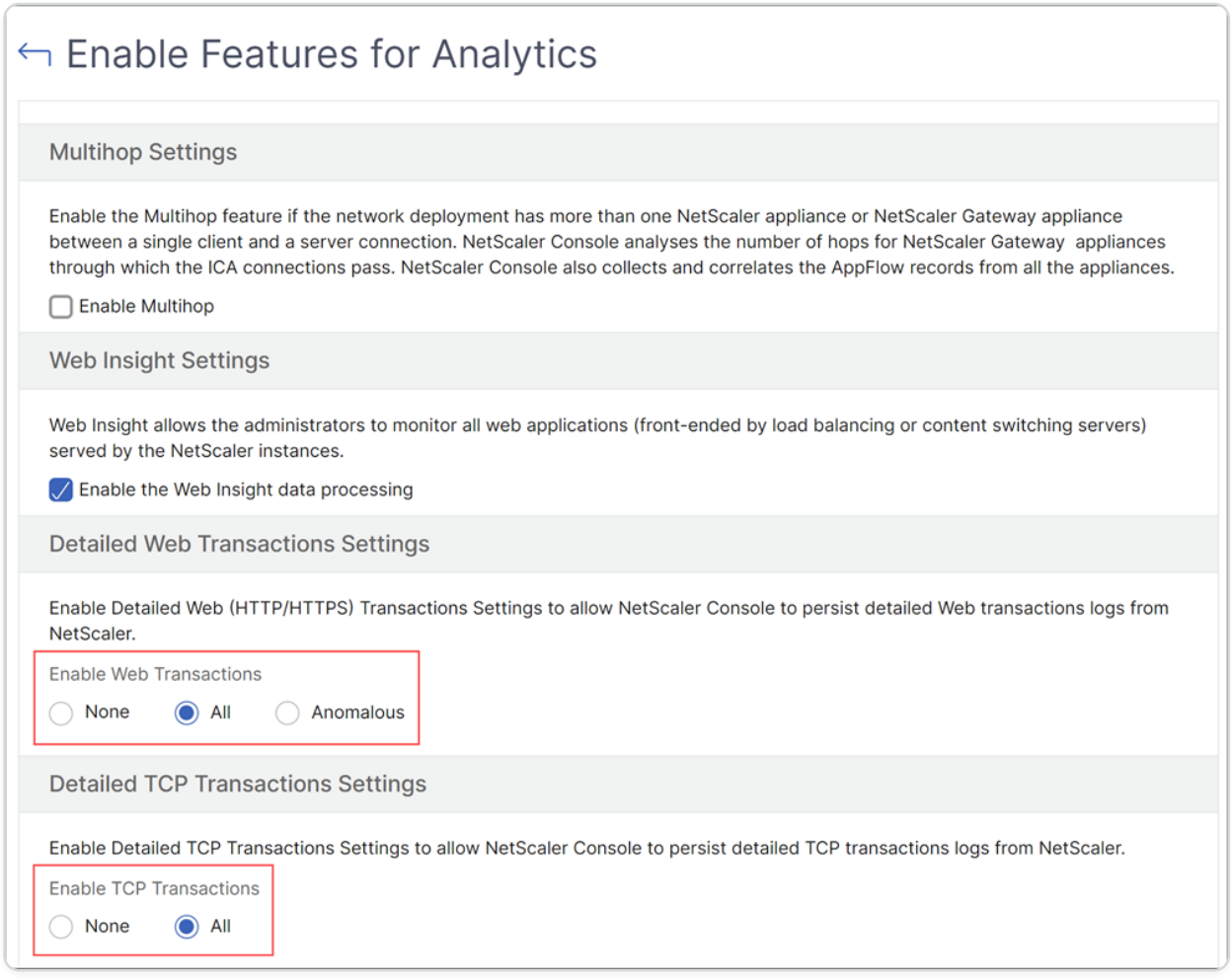
   The **Settings** page is displayed.

2. Click **Enable Features for Analytics**.
3. Under **Web Transaction Settings**, select **All**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Under **TCP Transactions Settings**, select **All**.



5. Click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Send traffic to microservices

Next, you must send traffic to microservices to get the service graph populated in NetScaler Console.

1. Determine the Ingress IP and port

   ```
   export INGRESS_HOST=$(kubectl get pods -l app=citrix-ingressgateway -n citrix-system -o 'jsonpath={.items[0].status.hostIP}')
   ```

   ```
   export INGRESS_PORT=$(kubectl -n citrix-system get service citrix-ingressgateway -o jsonpath='{.spec.ports[?(@.name=="http2")].nodePort}')
   ```

   ```
   export SECURE_INGRESS_PORT=$(kubectl -n citrix-system get service citrix-ingressgateway -o jsonpath='{.spec.ports[?(@.name=="https")].nodePort}')
   ```

2. Access the Bookinfo front end application using curl. The `productpage` service must return 200 OK response.

   ```
   curl -kv https://$INGRESS_HOST:$SECURE_INGRESS_PORT/productpage
   ```

   ```
   curl -v http://$INGRESS_HOST:$INGRESS_PORT/productpage
   ```

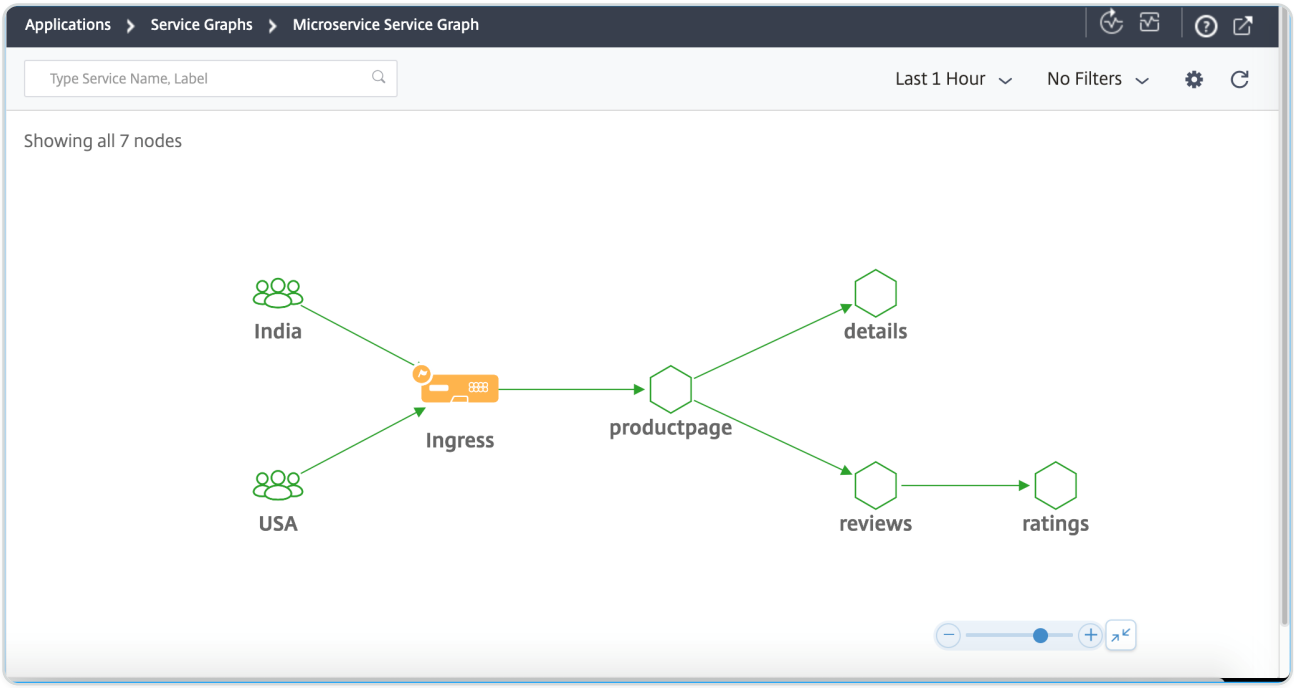
3. Visit `https://$INGRESS_HOST:$SECURE_INGRESS_PORT/productpage` from a browser.

   The **Bookinfo** page is displayed.

4. Ensure that $INGRESS_HOST and $SECURE_INGRESS_PORT is replaced by an IP address and a port value.

After you send traffic to microservices, the service graph is populated approximately in 10 minutes duration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Using the service graph, you can analyze various service details such as metrics, errors, and so on. For more information, see Service graph.

Detailed procedures to setup single tier or unified ingress topology

The prerequisites to deploy the single tier or unified ingress topology is available at Setting up service graph.

Add VPX or SDX or MPX or BLX instance in NetScaler Console

To get the tier-1 NetScaler instance analytics in service graph, you must add the VPX/SDX/MPX/BLX instance in NetScaler Console and enable **Web Insight**. You must enable **Web Insight** for NetScaler Console to display the web transaction details from the VPX/SDX/MPX/BLX instance.

1. Navigate to **Infrastructure > Instances > NetScaler**
2. Click the **Add** option to add the instance. For more information, see Add instances in NetScaler Console
3. After adding the instance, select the virtual server and enable **Web Insight** to view the web transaction details. For more information, see Manage licensing and enable analytics on virtual servers

Add Kubernetes cluster in NetScaler Console

To add the Kubernetes cluster:

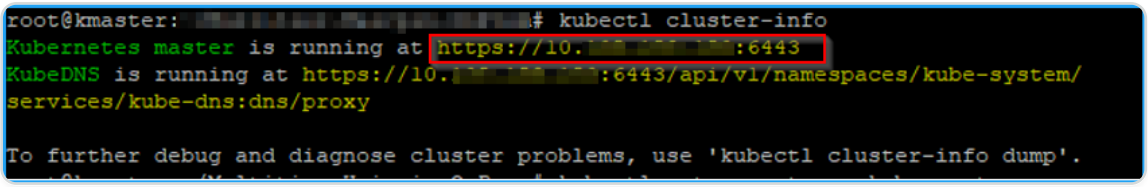
© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Log on to NetScaler Console with administrator credentials.
2. Navigate to **Infrastructure > Orchestration > Kubernetes > Cluster**. The Clusters page is displayed.
3. Click **Add**.
4. In the **Add Cluster** page, specify the following parameters:

    a. **Name** - Specify a name of your choice.

    b. **API Server URL** - You can get the API Server URL details from the Kubernetes Master node.

        i. On the Kubernetes master node, run the command `kubectl cluster-info`.

        ii. Enter the URL that displays for **“Kubernetes master is running at.”**

    c. **Authentication Token** - Specify the authentication token. The authentication token is required to validate access for communication between Kubernetes cluster and NetScaler Console. To generate an authentication token:

    On the Kubernetes master node:

        i. Create a service account by using the YAML.

        `kubectl create -f adm_svc_account.yaml`

        The service account is created.

        ii. Run `kubectl create clusterrolebinding citrixadm-sa-admin --clusterrole=cluster-admin --serviceaccount=default:citrixadm-sa` to bind the cluster role to service account.

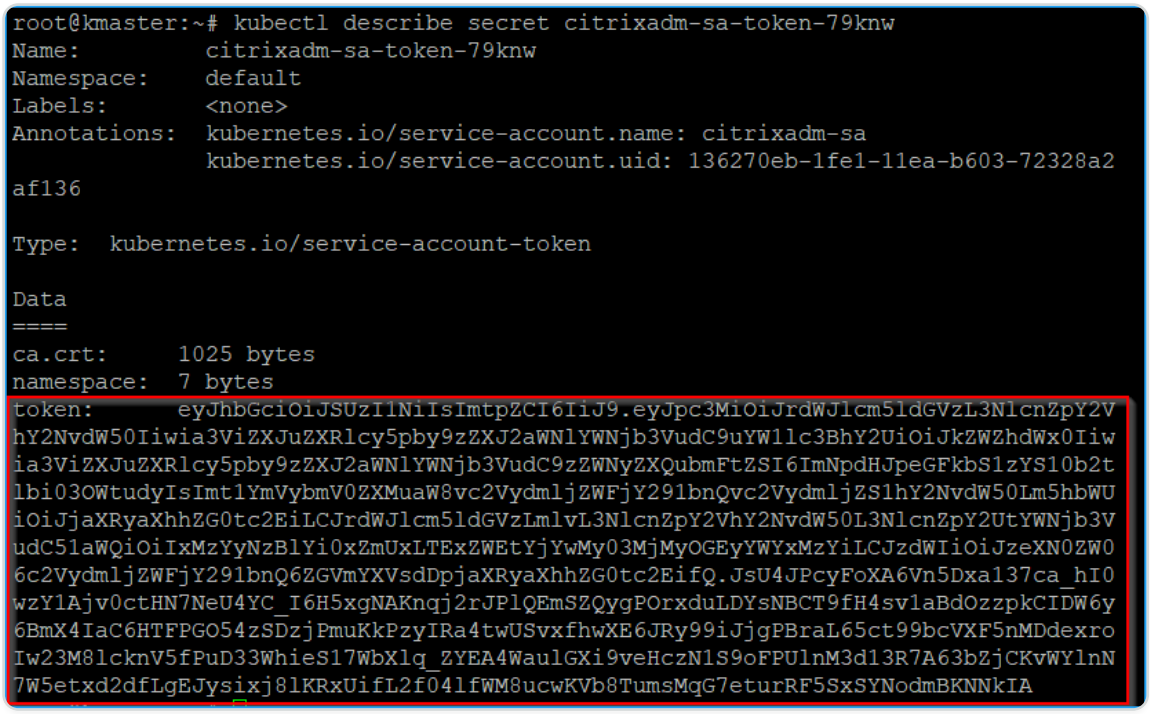
        The service account now has the cluster-wide access.

        A token is automatically generated while creating the service account.

        iii. Run `kubectl describe sa citrixadm-sa` to view the token.

        iv. To get the secret string, run `kubectl describe secret <token-name>`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



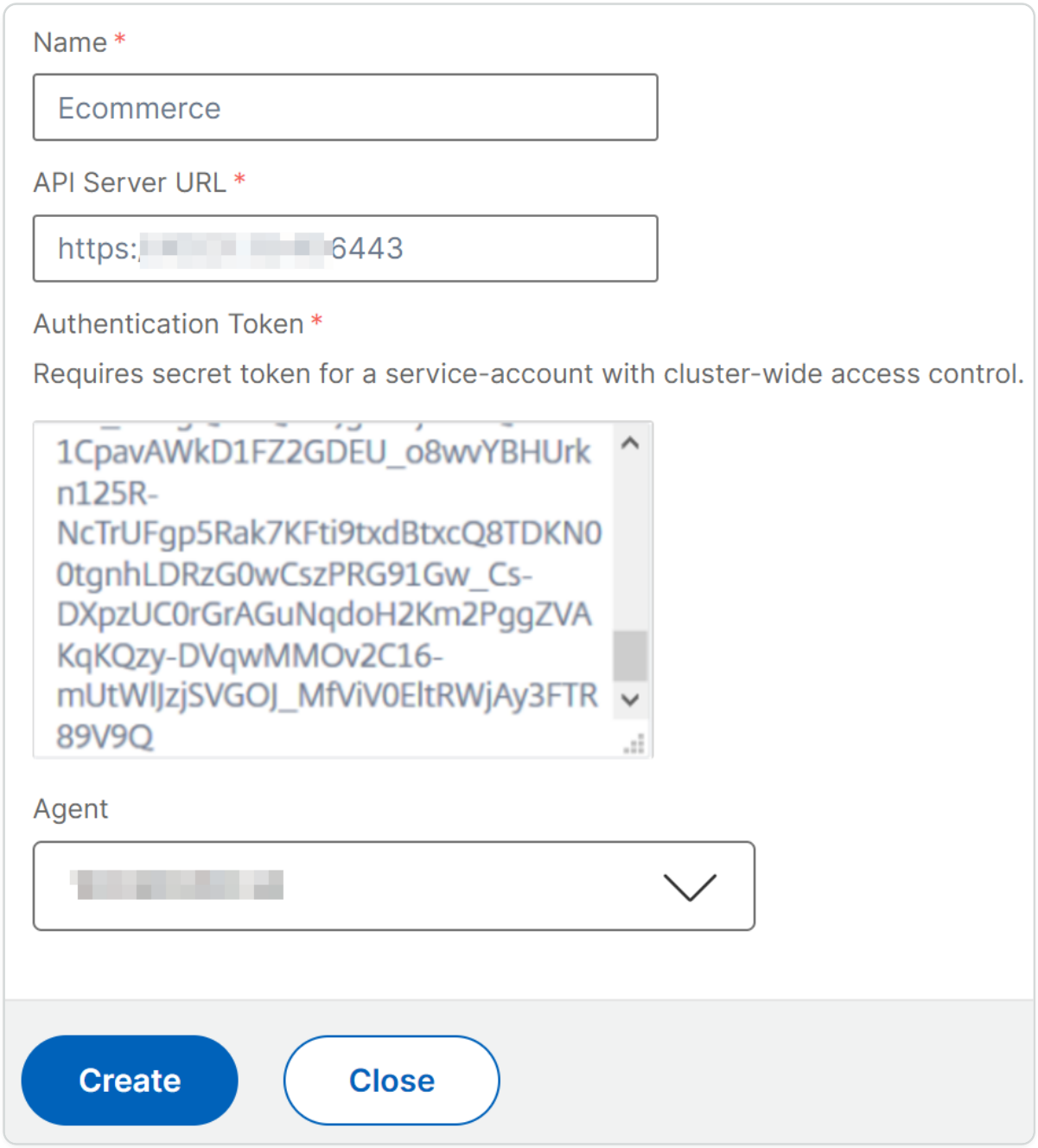
d. Select the agent from the list.

Note

Ensure to select the same agent that you have added in the CPX YAML.

e. Click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Data governance for NetScaler® telemetry program

All existing NetScaler Console customers must be compliant with the NetScaler telemetry program by uploading the required telemetry data. The NetScaler telemetry program is enabled starting from **14.1-28.x** build and the telemetry data is automatically uploaded. For more information, see the NetScaler telemetry program. Citrix collects basic license telemetry data and NetScaler deployment and feature usage telemetry data for its legitimate interests, including license compliance. NetScaler Console configuration and feature usage data is also collected to manage, measure and improve Citrix products and services.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTES:

- The telemetry upload happens every 24 hours automatically.
- To collect and store the telemetry metrics in your NetScaler instances, the following configuration was pushed to your NetScaler instances through NetScaler Console as part of the NetScaler telemetry program released on 18th June 2024.

```
enable ns feature AppFlow

add analytics profile telemetry_metrics_profile -type timeseries
-outputMode prometheus -metrics ENABLED -serveMode Pull -schemaFile "./
telemetry_collect_ns_metrics_schema.json" -metricsExportFrequency 300
```

- The `/nsconfig/.telemetry.conf` file is updated with the following command for the Gateway telemetry. NetScaler Console checks for this command every hour and adds it, if this command is missing. This command is pushed only to the NetScaler instances that have VPN virtual server configuration:

```
ns_telemetry_server,&lt;Console IP>,5140
```

- Some telemetry parameters are collected through scripts that are pushed from NetScaler Console to NetScaler instances. These scripts are read-only and do not change anything in NetScaler.

The following table provides the required parameter details that are collected as part of NetScaler telemetry program:

CATEGORIES	DESCRIPTION	WHAT DO WE USE IT FOR?
License, and NetScaler deployment and usage telemetry	Information about license entitlement, usage, and high-level NetScaler deployment data, and NetScaler feature usage.	License compliance and to manage, measure, and improve the service.
NetScaler Console deployment and feature usage telemetry	Information about Console deployment and feature usage.	To manage, measure, and improve the service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Required telemetry data

The data collected as part of the NetScaler telemetry program is listed in the Telemetry data governance document.

*The information collected through telemetry, such as email addresses, user names, and IP addresses, is securely pseudonymised by hashing the information at the source using one-way hashing algorithms. As a result, Citrix cannot access or read these values. This telemetry data is used solely for logical asset-matching purposes.

How to change the NetScaler MPX and VPX root password

Occasionally, you must change the root password of the NetScaler appliance occasionally, for security reasons or compliance of password rotation policy.

This document describes the steps required to change the root password of the NetScaler MPX and VPX appliances managed through NetScaler Console cloud.

If you change the NetScaler password, you must modify the NetScaler Console admin profile that is associated with the NetScaler. An NetScaler Console admin profile maintains the NetScaler credentials for REST API, SSH, SCP, or SNMP based communication with the NetScaler appliance. Through admin profiles, NetScaler Console manages NetScaler MPX and VPX appliances.

For more information about how to change the NetScaler `nsroot` password on an individual appliance, see article CTX224027.

Change password using the Configuration Jobs feature

By using the NetScaler Console Configuration Jobs feature, you can simplify the repetitive password change process and apply the changes to the NetScaler appliances, without accessing the individual instances.

Follow these steps to change the password:

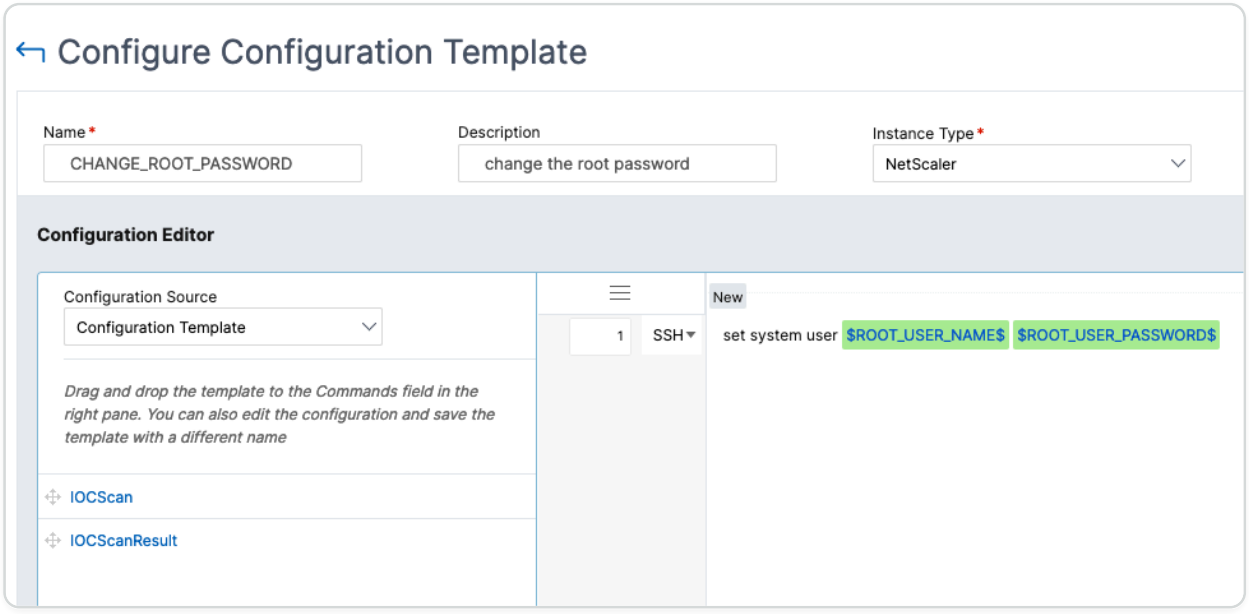
Step 1. Create a Configuration Template. Step 2. Create a Configuration Job. Step 3. Create an admin profile and modify it.

Note: If the NetScaler appliances are managed by other tools as well, you must change the credentials on those tools as well.

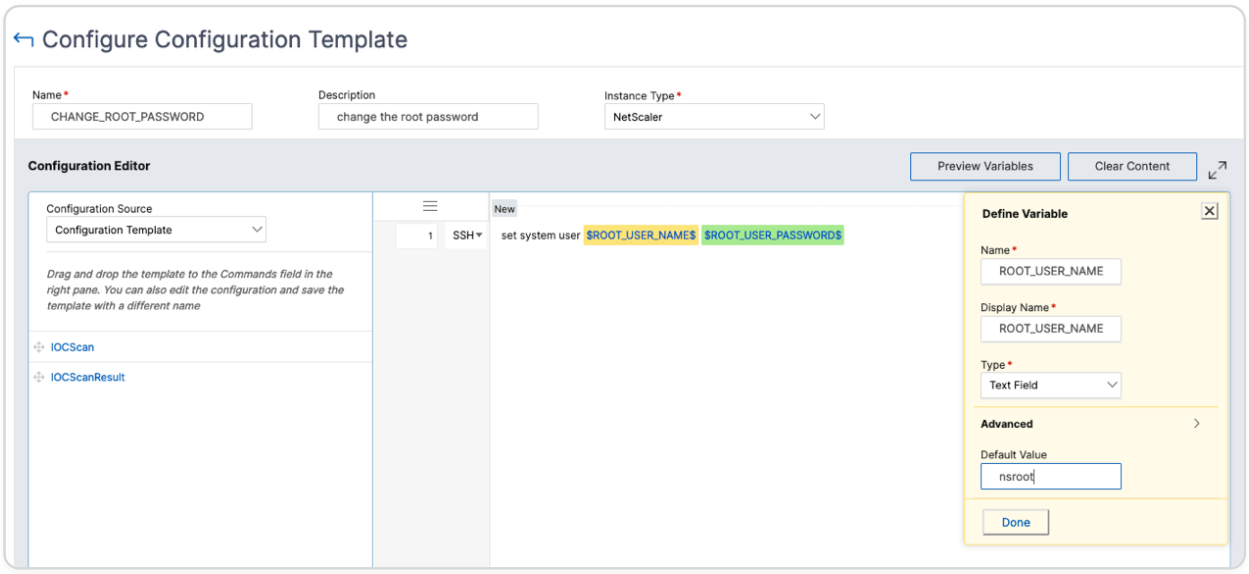
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 1. Create a Configuration Template

1. From the NetScaler Console GUI, navigate to **Infrastructure > Configuration Jobs > Configuration Templates**.
2. Select **Add**. Create a Configuration Template with by typing the SSH command `set system user $ROOT_USER_NAME$ $ROOT_USER_PASSWORD$`.



3. Select the `$ROOT_USER_NAME$` variable, and select **Text Field as Type**.
4. Optionally, provide the default value for the root user name. Select **Done** to save the variable settings.



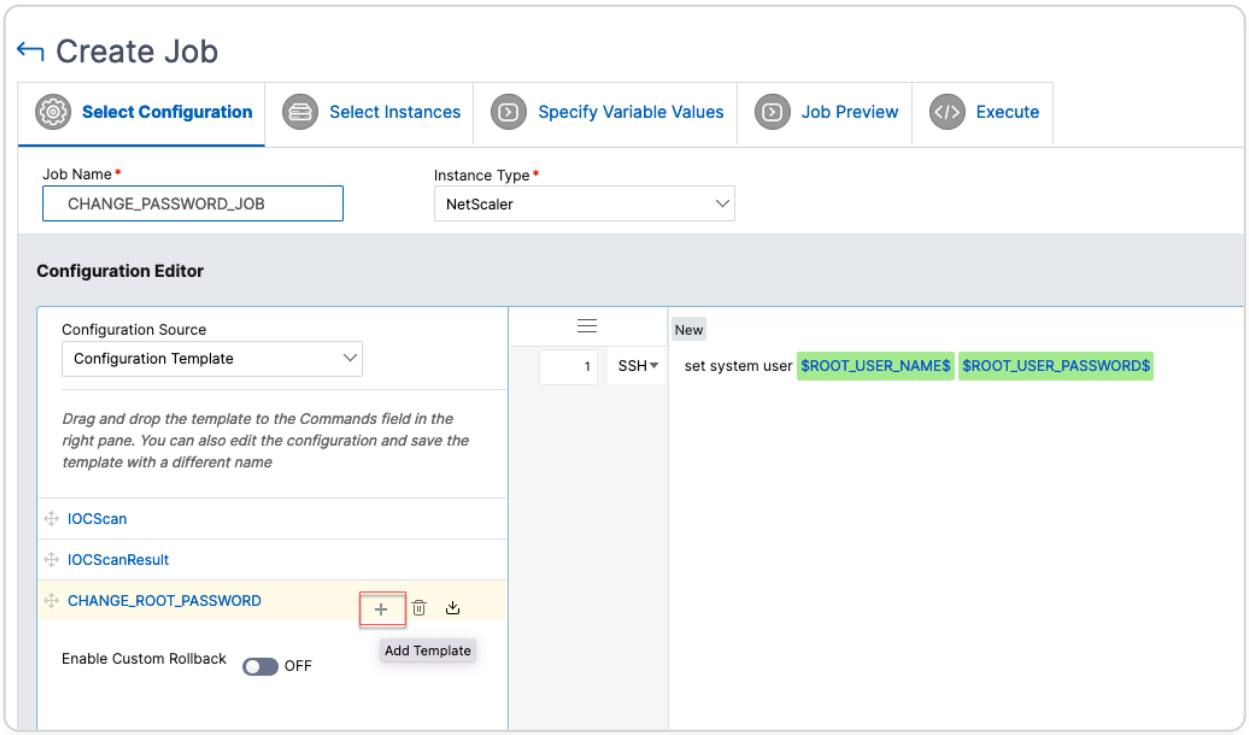
5. Select the `$ROOT_USER_PASSWORD$` variable, and select **Password Field as Type**. Select **Done** to save the variable settings.
6. Select **OK** to save the Configuration Template.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

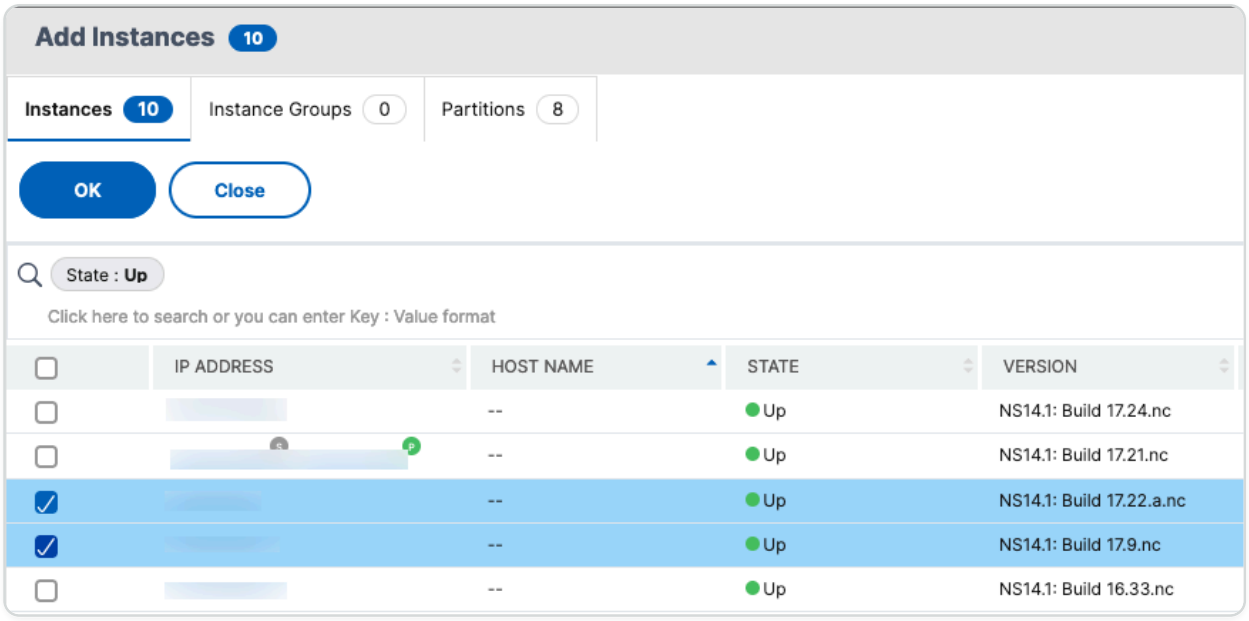
7. The new Configuration Template appears under **Configuration Templates**.

Create a Configuration Job

1. From the NetScaler Console GUI, navigate to **Infrastructure > Configuration Jobs**.
2. Select **Create Job** and click the "+" icon of the new configuration template. Select **Next**.



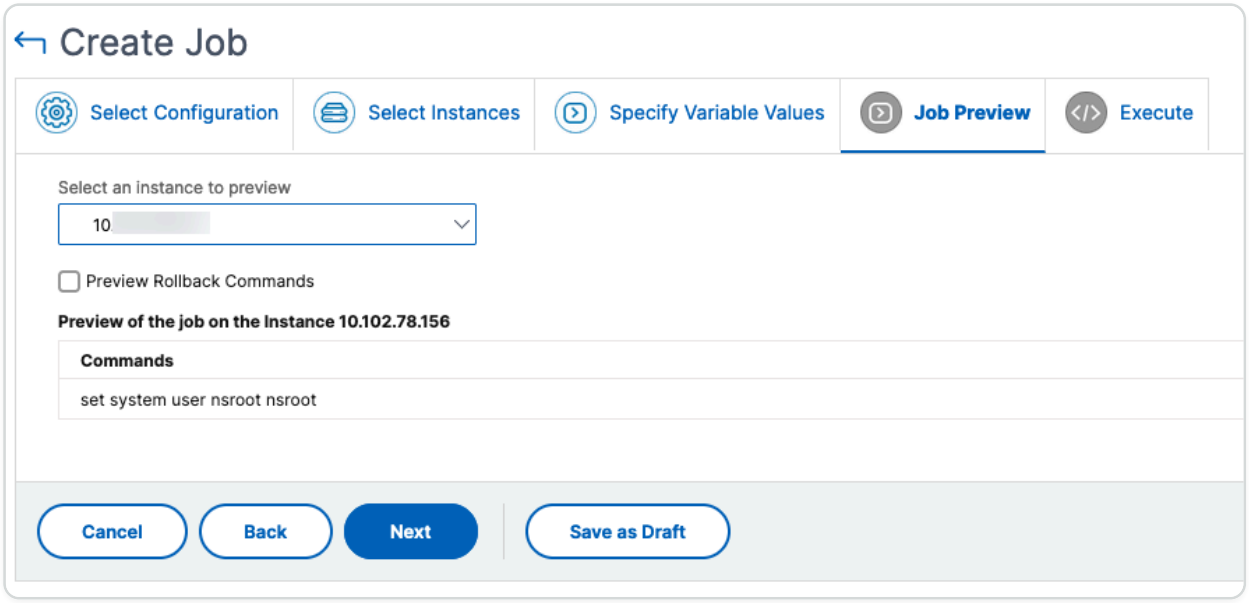
3. Select the NetScaler instance or instances for which the password must be modified.



4. In the **Select Instances** pane, select the instances, and click **Next**.
5. In the **Specify Variable Values** pane provide values for user name and password, and click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Under **Job Preview**, check the actual CLI commands that the NetScaler Console will run on the NetScaler instances. If the preview looks fine, click **Next**.

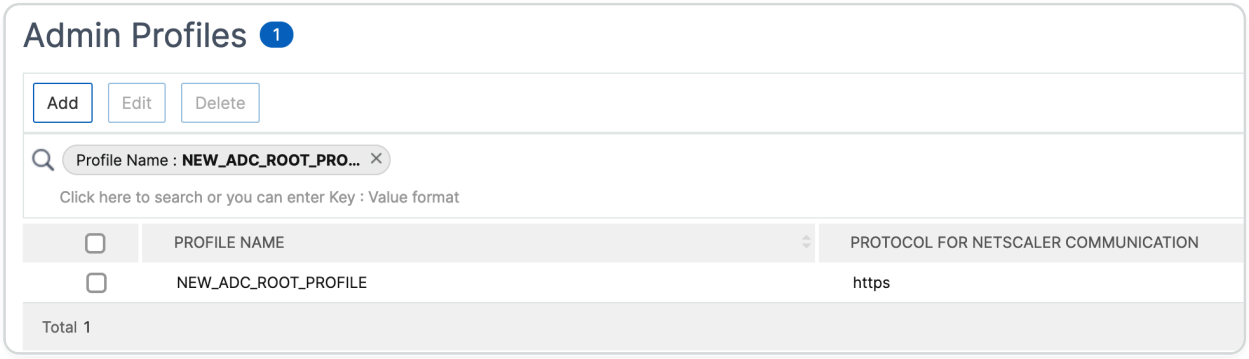


7. In the **Execute** pane, you have the choice to run the job immediately or schedule it for later. You can also choose to run the job in parallel on all the selected instances or do it sequentially. Select **Finish** after you've provided the execution details.
8. The **Jobs** page shows if the execution succeeded or failed.
9. Select the **Job** and click **Details**. The execution details show the status at individual instance level.

Modify the admin profile

After you've modified the NetScaler passwords, you must add and modify the admin profiles of the instances. Follow these steps:

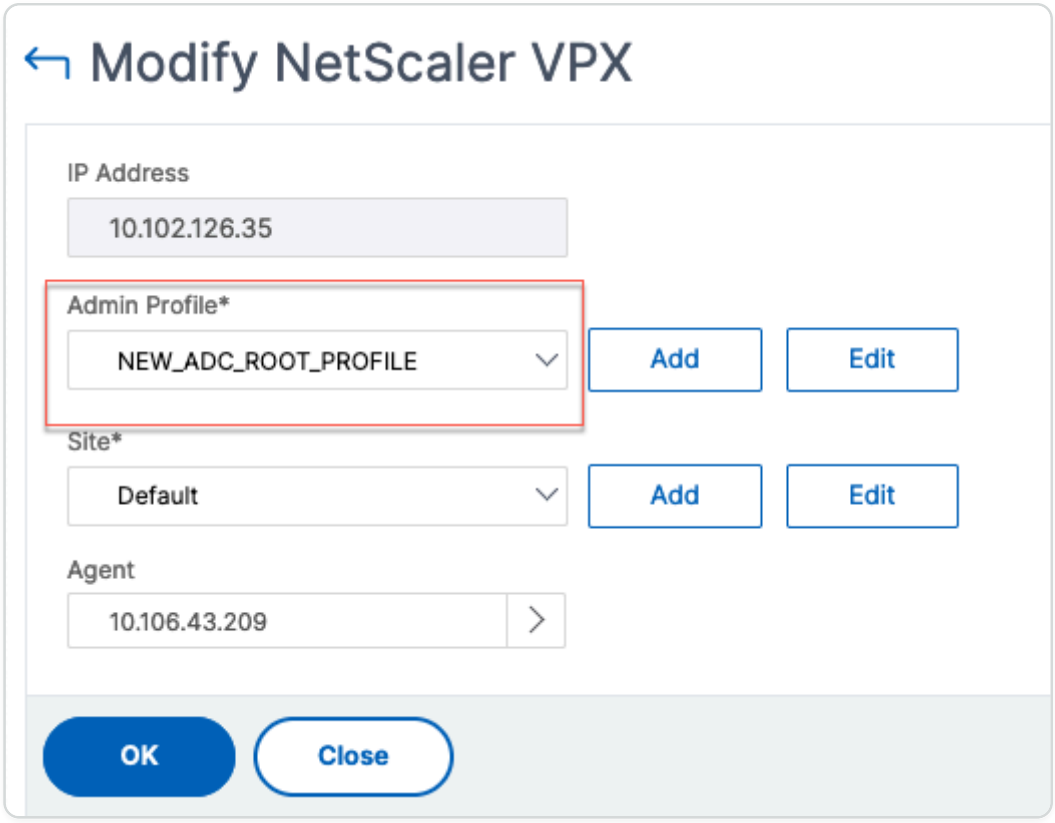
1. Navigate to **Infrastructure > Instances > NetScaler**.
2. Click **Select Action > Profiles** to see all the admin profiles.
3. Select **Add** to create an admin profile and provide new NetScaler credentials.



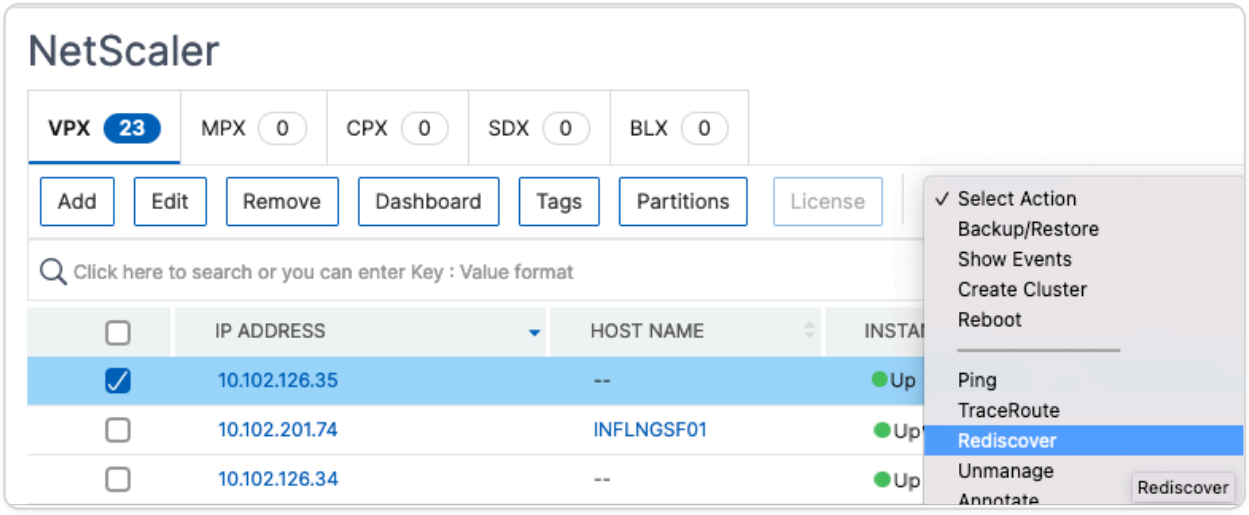
4. The newly created profile appears under **Admin Profiles**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Go to **Network > Instances > NetScaler**. Select the NetScaler instance for which the password has been modified, and the select **Edit**.
6. Select the newly created Profile Name and click **OK**.



7. Select the instance again, right-click, select **Rediscover**.



These steps complete the password reset process in NetScaler Console.

Previous releases

This topic is the list of previous releases for NetScaler Application Delivery Management (NetScaler Console).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

December 13, 2023

Infrastructure

NetScaler® ADM service rebranding

NetScaler Application Delivery Management service (ADM Service) is now rebranded to NetScaler Console service.

Other terminologies that have been rebranded are as follows:

- ADM agent is now rebranded to NetScaler agent
- ADM Service Connect is now rebranded to Console Advisory Connect

NOTE:

Our NetScaler Console service product UI and documentation are currently undergoing updates to reflect these changes. During this time, you may come across the earlier and rebranded names being referenced interchangeably. We thank you for your understanding during this transition.

Licensing

NetScaler Flexed licensing

NetScaler Flexed licensing is the new licensing framework aimed at simplifying the license management process. Your Flexed license includes software instance licenses (VPX/CPX/BLX, SDX, MPX, and VPX FIPS) and bandwidth capacity licenses. You must apply the Flexed licenses on NetScaler Console service or NetScaler ADM on-prem. You must also apply the MPX Z-Cap and SDX Z-Cap license on NetScaler MPX hardware and NetScaler SDX hardware, respectively. You can then allocate them across all NetScaler form factors deployed in cloud or on-prem.

NOTE:

Ensure that your NetScaler agents are running version 16.x or later.

For more information, see Flexed license.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Analytics

Flexed license - Metrics Collector disabled by default for the new NetScaler instances added in NetScaler Console

If you are using the Flexed license, the Metrics Collector is now disabled by default for the new NetScaler instances added in NetScaler Console. You must manually enable this option to push the NetScaler metrics and counters data to the Console. The metrics collector configuration for the existing managed instances remain unchanged.

NOTE:

The Metrics Collector must be enabled for the data to appear in the Application Dashboard and its related tabs such as Performance, SSL, and Key Metrics for all the licensed virtual servers on that instance.

For more information, see Configure Intelligent App Analytics.

Deprecation of Video and TCP insight features

With the latest release, **Video Insight** and **TCP Insight** reporting data are no longer available for visualization in the NetScaler Console.

Infrastructure

Download files for batch configuration jobs

The configuration jobs now allow you to download files from a directory on a NetScaler instance to a directory on your local machine using the NetScaler ADM GUI.

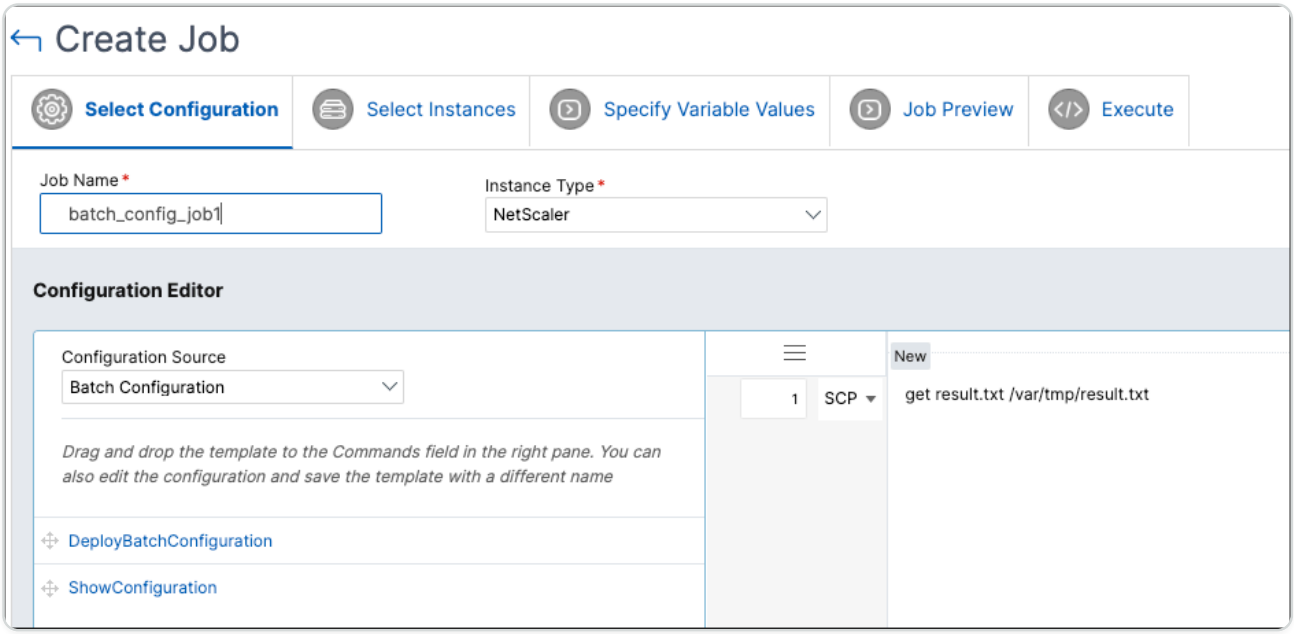
To use this feature, navigate to **Infrastructure > Configuration > Configuration Jobs**, select a job and click **Download Result Files**.

The **Download Result Files** button is available only if the following conditions are met:

- The configuration job that is created is a batch configuration job. To create a batch configuration job, go to **Create Job > Select Configuration** and in the **Configuration Editor**, select **Configuration Source > Batch Configuration**
- A `scp get` command is used in the **Configuration Editor**

For multiple NetScaler instances, the downloaded result files are available in separate folders, each corresponding to an individual instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Pause and resume a scheduled upgrade job

NetScaler ADM now offers the option to pause your scheduled upgrade job. To use this feature, navigate to **Infrastructure > Upgrade Jobs**, select an existing scheduled upgrade job, and click **Stop** to pause the job. To resume the scheduled upgrade job, click **Resume**.

NOTE:

If the scheduled time for the upgrade job has passed after you decided to resume it, you need to create the upgrade job again.

For more information, see Upgrade Jobs

Fixed Issues

The issues that are addressed in Build December 13, 2023.

Analytics

- In **Applications > Dashboard**, the export of transaction log data to the tabular or CSV format does not display any data. This issue is noticed when NetScaler ADM is configured with non UTC time zones.
- In **Security > Security Violations > Violation Details**, the search filter does not recognise the "Client-IP !=" query.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Scheduled snapshot reports exported from **Security > Security Violations > Export Reports > Schedule Export** with the file format selected as JPEG display the following error:

  "Please provide query parameters in the report context or csv_export_arr."

Infrastructure

- Certain users see "For development purposes only" watermark on the maps in the **Infrastructure > Instances** page.

Management and Monitoring

- NetScaler ADM agent generates "netScalerLoginFailure" SNMP traps. This issue occurs because the credentials that the ADM agent uses to log into NetScaler gets truncated due to a newline character.

Security

- After configuring protections in the Unified security dashboard (**Security > Security Dashboard > Manage Application**), the protections are not getting deployed in the content switching virtual server.

November 29, 2023

Infrastructure

Use tags to authorize instances for user groups

As an administrator, you can now authorize users to specific instances based on associated tags. When creating user groups, navigate to **Settings > Users & Roles > Add > Authorization Settings > Select Tags** and then authorize users to instances by tags.

For more information, see Configuring role-based access control.

Fixed Issues

The issues that are addressed in Build November 29, 2023.

- When you provision a VPX instance on SDX in **Infrastructure > Instances > NetScaler > SDX > Select Action > Provision VPX**, the **Manage through network** option does not appear.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

November 09, 2023

Analytics

Configure Gateway session timeout

In **Settings > Analytics Settings > Configure ICA/Gateway Session Timeout**, you can now configure timeout session for Gateway Insight. By default, the value is 30 minutes. With this configuration, if NetScaler ADM does not receive session terminate record within the configured duration, then the session is recorded as terminated.

Update in NetScaler backup process and firewall access

NetScaler instance backups are now uploaded from the NetScaler agent to NetScaler ADM Service directly and then to Amazon S3. So, you no longer need to allow access to S3 URLs in your firewall for the NetScaler backup service.

Unified Security dashboard

In NetScaler ADM, you can now use a single-pane dashboard to configure protections, enable analytics, and deploy them on your applications. Navigate to **Security > Security Dashboard** and then click **Manage Application** to:

- View all secured and unsecured applications.
- Select a unsecured application, configure protections from various template options, enable analytics for the protections, and deploy them on your application to secure the application.

Earlier, you had to configure all protections in the NetScaler instances and you were able to view only analytics for the configured protections in NetScaler ADM. As an administrator, this single-pane dashboard enables you to configure protections for the application in a single workflow.

For more information, see Unified Security dashboard.

Fixed Issues

The issues that are addressed in Build Nov 09, 2023.

Infrastructure

- When setting up the NetScaler built-in agent to manage instances, the configuration gets stuck at the **Add Instances** page, even though the registration is successful, and the agent can be viewed in the **Instance Dashboard** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBooks

- When config packs with special characters in their parameters are updated or deleted, NetScaler ADM displays a success message despite incomplete update or delete operations on NetScaler. With this fix, NetScaler ADM now accurately displays errors for any incomplete configurations resulting because of special characters in the configpack definition.

October 25, 2023

Analytics

Create custom dashboards to view instance key metric details

Similar to the unified dashboard (**Overview > Dashboard**), you can now view instance metric details based on your choice by creating custom dashboards. For example, if you want to monitor the key metrics for applications and application security, you can create a custom dashboard by selecting only those two categories. You can create up to 20 dashboards by using a unique name for each dashboard. As an administrator, this enhancement enables you to create multiple dashboards and monitor only the required instance insights.

To get started, navigate to **Overview > Custom Dashboard**.

For more information, see Create custom dashboards to view instance key metric details.

Actionable tasks and recommendations

The following enhancements are now added to the **Tasks** feature:

- A new **Tasks** tab is introduced where you can view actionable tasks that need your immediate attention. These tasks are displayed based on your current utilization. As an administrator, completion of these actionable tasks ensure that your NetScaler deployment is secured, compliant, and efficient. You can also view these actionable tasks based on the severity of the issues (Critical and Medium).
- The **To Do** tab is renamed as **Recommendations**. In **Recommendations**, you can continue to review the existing tasks and click **Guide Me** to complete the task.
- The **Archive** tab is no longer available. Instead, you can choose to **Dismiss** a recommendation from the list.

For more information, see Actionable tasks and recommendations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infrastructure

Use certificate store to update SSL certificates

When you update an SSL certificate in **Infrastructure > SSL Dashboard > Update,** you can now select the certificate from the certificate store. Earlier, you had to upload the certificate file and key file to update an SSL certificate.

Updated list of SNMP traps

The list of SNMP traps is now updated with new traps as well as some previously missing traps. To view the complete list, navigate to **Infrastructure > Events > Event Settings > NetScaler**.

Fixed issues

The issues that are addressed in Build Oct 25, 2023.

- When you provision a VPX instance on SDX in **Infrastructure > Instances > NetScaler > SDX > Select Action > Provision VPX**, the **Manage through network** option does not appear.

October 10, 2023

Management and Monitoring

Support for identification and remediation of CVE-2023-4966 and CVE-2023-4967

NetScaler Console Security Advisory now supports the identification and remediation of CVE-2023-4966 and CVE-2023-4967.

- Identification requires a combination of version and configuration scan.
- Remediation requires an upgrade of the vulnerable NetScaler instances to a recommended build that has the fix.

NOTE:

Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

For more information on how to use NetScaler ADM to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.

For more information, see Security Bulletin.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

September 26, 2023

Analytics

Export data to Splunk and New Relic only from selected instances

When you create a subscription to export data to Splunk and New Relic, you can now select the NetScaler instances. If you create a subscription with specific instances, the data is exported to Splunk and New Relic only from the selected NetScaler instances.

For more information, see Integration with Splunk and Integration with New Relic.

Infrastructure

ADM on-prem instances connected with ADM Service using Cloud Connector

In **Settings**, you can now view a new option called **ADM On-Prem**. In this page, you can view details of the ADM on-prem instances that are connected with the ADM service tenant through ADM On-Prem Cloud Connector.

For more information, see ADM on-prem instances connected with ADM Service using Cloud Connector.

Fixed Issues

The issues that are addressed in Build Sep 26, 2023.

Analytics

- The periodic pruning of the App Dashboard data did not function as expected. As a result, NetScaler Console consumed more disk space.

September 13, 2023

Infrastructure

Authentication token to upload technical support bundle

You now need an authentication token to upload the technical support bundle generated on your NetScaler to the Citrix technical support server. Previously, you uploaded the technical support bundle using Citrix user name and password. For more information, see How to generate a technical support bundle for a NetScaler instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed Issues

The issues that are addressed in Build Sep 13, 2023.

Analytics

- When NetScaler Console loses the virtual server licenses, the analytics status for the virtual servers using those licenses is expected to be disabled. This scenario was not working as expected for the VPN virtual servers.

Infrastructure

- In **Gateway > HDX™ Insight** and **Gateway > Gateway Insight**, the X-axis of the graph displays dates instead of time.

Management and Monitoring

- Reports exported from **Infrastructure > Network Reporting > Export** appear truncated or incomplete.

- Azure Active Directory (AD) users who belong to many Azure groups cannot access NetScaler Console even if the AD groups are mapped to ADM groups.

August 31, 2023

Infrastructure

View the Certificate Store page under SSL Dashboard

You can now navigate to **Infrastructure > SSL Dashboard > Certificate Store** to view the **Certificate Store** page.

Support for SNMP functionality for the agents

In **Infrastructure > Agents > Actions > Manage SNMP**, you can now create SNMP managers, SNMP users and SNMP views for agents.

For more information on SNMP managers and users, see Create SNMP managers and users for NetScaler ADM agent.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

User experience and functionality improvements for the Data Storage Management dashboard

To improve the user experience and make the data storage management more efficient, the following improvements are now available for the **Data Storage Management** dashboard:

- New UI design for the dashboard:
  - Added **Data Ingestion**, **Storage Consumption**, **Data Pruning**, and **Actions** tiles
  - **Actions** tile provides options to add more storage, review data retention policy, perform data pruning, and review your system notifications
- Search functionality in **Storage Consumption Trends** section:

  In addition to viewing the storage trends, you can now search for specific features and trends.
- Perform data pruning:
  - You can now select one or more features and prune their data to free up your storage
  - You are entitled to 10 data prunes each month

For more information on the Data Storage Management dashboard, see Data Storage Management.

Security

API Gateway renamed to API Security

API Gateway is now renamed to **API Security**. You can view the changes in the following pages:

- **Security > API Security**
- **Security > API Security > API Analytics > Get help > API Security docs**
- **Settings > Users & Roles > Groups > Authorization Settings > API Security**
- **Settings > Users & Roles > Access Policies > Permissions > Security > API Security**

Fixed Issues

The issues that are addressed in Build August 31, 2023.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Management and Monitoring

- In **Infrastructure > Network Reporting,** the Network Reporting dashboard does not display any historical data in the virtual server reports. This issue is seen when you select a NetScaler HA pair in **Select Entities** while creating the dashboard.

August 11, 2023

Management and Monitoring

Security Advisory - File integrity monitoring

The NetScaler Console Security Advisory now enables you to scan the NetScaler build files and view results of any alterations or additions to the original NetScaler build files.

In Security Advisory (**Infrastructure > Instance Advisory > Security Advisory**), the **Scan Now** option enables you to select **Scan CVEs**, **Scan Files**, or **Scan Both**. After you select **Scan Files** or **Scan both**, NetScaler Console compares the binary hash for managed NetScaler build files with the original binary hash values and highlights if there are any file alterations or file additions under the **File Integrity Monitoring** tab.

The scan results showcase the NetScaler instances that have any potential changes to the original files and/or any other file additions. For further investigations on the scan results, you can contact your organization's digital forensics.

For more information, see Security Advisory.

August 09, 2023

Infrastructure

View virtualization platform details for NetScaler VPX™

In **Infrastructure > Instances > NetScaler > VPX**, you can now view the platform on which NetScaler VPX is hosted by selecting **Settings > Cloud Platform**.

Retry failed upgrade jobs

In **Infrastructure > Upgrade Jobs**, you can now select the failed upgrade job and do either of the following actions:

- Click **Retry** next to the failed upgrade job

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Go to **Select Action > Retry Upgrade Job**

For more information, see Retry failed upgrade jobs.

Security

Update an existing API definition

In **Security > API Gateway > API Discovery**, you can now update an existing API definition with selected API resources.

For more information, see Update an existing API definition with discovered API endpoints.

Fixed Issues

The issues that are addressed in Build August 09, 2023.

Provisioning

- The NetScaler VPX provision on VMware vCenter (**Infrastructure > Instance > Citrix ADC > VPX > Provision**) fails because of the same name that was used in the previously deleted VPX instance.

StyleBooks

- When you try to migrate an ADC configuration from a source ADC instance to a target instance in **Applications > Configuration > Config Packs > Migrate ADC > Get Started > Specify Configuration**, and click **Next**, the following error message is displayed intermittently:

  No Job found.

- If you create a configpack from a StyleBook definition that has an authentication virtual server and built-in cache policy bindings, and then you delete the configpack, the deletion is successful. However, if you try to create the configpack again with the same parameters, the following error message appears:

  Resource already exists.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

July 26, 2023

Analytics

Support to configure the export of metrics from NetScaler to Prometheus through StyleBook

To export metrics from NetScaler to Prometheus, you must create an analytics profile in NetScaler and specify the schema file. For more information, see Monitoring NetScaler Console, applications, and application security using Prometheus.

In **Applications > Configuration > Stylebooks > Default Stylebook**, you can now use the **Prometheus TimeSeries Analytics Configuration** StyleBook and run the configuration to all managed instances.

For more information, see Prometheus analytics StyleBook.

Assign a Net Profile for the managed NetScaler instances from NetScaler Console

When you enable analytics for the virtual servers in NetScaler Console, the AppFlow data from the NetScaler is exported to NetScaler Console through the NetScaler subnet IP address (SNIP). In some scenarios, the SNIP might be blocked because of the firewall in the network. In such scenarios, you might have to use a different IP address than the SNIP. For more information about net profile, see Use a specified source IP for back-end communication.

You can now assign net profiles to a NetScaler instance through NetScaler Console. Navigate to **Infrastructure > Instances > Citrix ADC**, select the instance, and from the **Select Action** list, click **Configure Net Profiles** to assign a net profile for the instance.

NOTE:

Ensure that you have disabled analytics in all virtual servers before you assign a net profile for the instance.

With this enhancement, you can assign a net profile for exporting AppFlow data from NetScaler to NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infrastructure

Improved user experience when using CLI to configure NetScaler agent as a proxy

When you try to register a NetScaler agent to the NetScaler Console service, the CLI now prompts you with (y/n) questions regarding the proxy usage.

You also have an option to configure the proxy in the same script, if needed.

CLI support to view endpoint URLs while registering a NetScaler agent

After you enter a service URL in CLI while registering a NetScaler agent with the NetScaler Console service, you can view the list of all the endpoint URLs that must be allowed access.

StyleBooks

Support for additional attributes in StyleBooks analytics

The StyleBooks analytics section is now enhanced to:

- Accept parameters to configure Transport Mode (`transport-mode`)
- Configure HDX Insight for different types of traffic(`enable-hdxinsight-for`)
  - Enable HTTP X-Forwarded-For option (`http-x-forwarded-for`)
  - Enable Client side Measurements (`client-side-measurements`)

For more information, see StyleBooks Analytics.

July 18, 2023

Management and Monitoring

Support for identification and remediation of CVE-2023-3519, CVE-2023-3466, and CVE-2023-3467

NetScaler Console Security Advisory now supports the identification and remediation of CVE-2023-3519, CVE-2023-3466, and CVE-2023-3467.

Identification of:

- CVE-2023-3519 requires a combination of version and config scan.
- CVE-2023-3466 and CVE-2023-3467 requires a version scan.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The remediation for CVE-2023-3519, CVE-2023-3466, and CVE-2023-3467 requires an upgrade of the vulnerable NetScaler instance to a release and build that has the fix.

NOTE:

Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.

For more information on how to use NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.

For more information on how to remediate CVE-2023-3519, CVE-2023-3466, and CVE-2023-3467, see Security Bulletin.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2023-3519, CVE-2023-3466, and CVE-2023-3467 in the security advisory module. To see the impact sooner, you can start an on-demand scan by clicking **Scan Now**.

July 12, 2023

Fixed issues

The issues that are addressed in Build July 12, 2023.

- When you back up or restore a NetScaler instance, the `/var/metrics_conf` directory is not backed up.
- The deployment of config packs might fail when the StyleBook definition includes the `operations` section.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

July 03, 2023

Analytics

Configuration Job - Support to create a job for configuring export of metrics from NetScaler to Prometheus

To export metrics from NetScaler to Prometheus, you must create an analytics profile in NetScaler and specify the schema file. For more information, see Monitoring NetScaler, applications, and application security using Prometheus.

In **Configuration Job**, you can now create a job using the `NSConfigurePrometheusAnalyticsProfile` template from the **Inbuilt Template**, specify the required parameters, and run the job to all managed instances.

For more information, see Schedule a job for configuring export of metrics from NetScaler to Prometheus.

Infrastructure

NetScaler agent caches NetScaler images

The time taken for the NetScaler upgrade is now considerably reduced as the NetScaler images are cached in the NetScaler agent after they are downloaded. Hence, the images are not required to be downloaded for subsequent upgrade jobs.

NOTE:

This is applicable only for NetScalers that are added using the NetScaler agent.

For more information, see Create an ADC upgrade job.

Fixed issues

- In Web Insight, when you drill down any metric to view details and then further drill down any metric, the graph remains in the previous view, but all other details appear as expected.

  As a result, this creates an assumption that the further drill down is not working as expected.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When you try to migrate an ADC configuration from a source ADC instance to a target instance in **Applications > Configuration > Config Packs > Migrate ADC > Get Started > Specify Configuration**, and click **Next**, the following error message is displayed intermittently:

  "No Job found".

- In the **App dashboard**, when you select an application and navigate to the **SSL** tab to bind a certificate, an error message "**Certificate not found in database**" is displayed.

June 14, 2023

Security

Support to create API definition without selecting endpoints

In the **Security > API Gateway > API Discovery** > **Vserver** page, you can now create an API definition without selecting an endpoint. When you click **Create API Definition**, a pop-up window appears for you to confirm if an API definition must be created for all the discovered endpoints. Click **Yes** to create the API definition with all the endpoints, else click **No**.

For more information, see Discover API endpoints.

StyleBooks

Support for additional argument types in replace() function

The `replace()` built-in function can also accept a list of the following built-in types:

- `string`
- `ipaddress`
- `tcp-port`
- `number`
- `boolean`

For more information, see replace().

Fixed Issues

The issues that are addressed in Build June 14, 2023.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- In Upgrade Jobs (**Infrastructure > Upgrade Jobs**), when you select the pre-upgrade validation failed instance and click **Revalidate**, an error message is displayed.
- MPX instances are missing from the **Infrastructure > Citrix ADC Inventory > Citrix ADC (MPX/VPX/CPX/BLX)** page.
- When you export the SSL expiry reports for weekly, 30 days or 90 days from **Infrastructure > SSL Dashboard > SSL Certificates > Export Reports** and select **Tabular**, the resulting report displays an empty Domain column.
- In **Infrastructure > SSL Dashboard > SSL Certificates**, the NetScaler high-availability pair does not display the superscript of 'P' and 'S' for the primary and the secondary devices.
- In NetScaler release 13.1 and above, the ISSU commands do not get executed during the NetScaler upgrade.
- For multiple Cluster IP addresses (CLIPs) in a cluster, when you add a CLIP in brackets in **Infrastructure > Instances > Citrix ADC > Add**, the configuration fails and the CLIP does not get added to NetScaler Console.

May 31, 2023

Analytics

Pooled licensing recommendations in the Tasks feature

In **Tasks**, you can now view recommendations and Guide Me workflows for pooled licensing entitlements. As an administrator, these pooled licensing recommendations ensure that you are making use of all capabilities of NetScaler Console.

For more information, see View recommendations and manage your ADCs and applications efficiently.

Export SSL insights data to Splunk and New Relic

When you create a new subscription in **Settings > Ecosystem Integration** for the integration of Citrix ADM with Splunk and New Relic, you can now select the **SSL Certificate Insights** option. After you configure the subscription with the **SSL Certificate Insights** option, you can view the SSL data (SSL vserver and SSL certificate related data) in the Splunk and New Relic dashboard.

For more information, see Integration with Splunk and Integration with New Relic.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed Issues

The issues that are addressed in Build May 31, 2023.

- In **Gateway > HDX Insight > Instances**, when you select an instance and export the data, the user name information for Desktop Users was not available. With this fix, the user name information is also available in the report.

- When you select **Configure SNMP** for an SDX instance in **Infrastructure > Instances> Citrix ADC > SDX**, an error message is displayed. This issue occurs if the SDX profile is configured with SNMP v3 and **NoAuthNoPriv** as the security level.

- In **Infrastructure > Configuration > Configuration Jobs > Create Job > Select Configuration**, when you enter a password variable ($password$) and retain the **Type** as **Text Field** instead of **Password Field**, and click **Next**, the page does not load.

- In Web Insight, when you export data using the snapshot option, the graphs in the report appear blank.

- Analytics is not visible in HDX Insight. Even if Citrix ADM is rebooted, the analytics is visible only for a short duration and becomes invisible later.

- For an SDX instance in **Infrastructure > Instances > Citrix ADC > SDX > Dasboard**, when the used and free values for a resource are zero, the **System Resource Utilization** chart displays a blank space and blank value fields.

  With this fix, the number zero is displayed next to the resource name if the used and free values are zero.

May 18, 2023

Analytics

Support to export from each widget in Web Insight

In **Web Insight**, the export option is now introduced in all widgets and it enables you to export data in tabular format. Using this enhancement, you can:

- Export the required data individually from any widget.
- Drill down any metric and also export the required data from any widget.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Earlier, the export data provided only the consolidated report.

Note

> You can also continue to use the existing Export option to generate the consolidated report.

Infrastructure

View the complete certificate chain

You can now view the complete chain of links for a certificate including the intermediate certificates up to the root CA certificate.

To view the certificate chain, navigate to **Infrastructure > SSL Dashboard**, choose an SSL certificate and click **Details**.

Support to log events irrespective of event age

NetScaler Console now allows you to record all events irrespective of the event age you set in the event rules.

To set this option, navigate to **Infrastructure > Rules > Add > Configure Event Age** and select the **Log events instantly irrespective of event age duration** checkbox.

Fixed Issues

The issues that are addressed in Build May 18, 2023.

- In **Infrastructure > Upgrade Jobs> Add > Schedule Task**, if you select **Perform two stage upgrade for nodes in HA** and select the same time in the two **Start Time** fields, the following error message appears when you proceed:

  "common.date_diff_error:There should be atleast 1 hour difference between upgrade time"

  Even if you change the start time in the fields, the **Create Job** tab displays an empty page.

- In **Infrastructure > Instance Advisory > Upgrade Advisory**, the End of Maintenance (EOM) and End of Life (EOL) details for Release 13.0 is incorrect.

- The email alert for any event was showing the region incorrectly. With this fix, the region is not shown in the email alerts for events.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

May 09, 2023

Management and Monitoring

Support for identification and remediation of CVE-2023-24488 and CVE-2023-24487

NetScaler Console Security Advisory now supports the identification and remediation of CVE-2023-24488 and CVE-2023-24487.

Identification of:

- CVE-2023-24488 requires a combination of version and config scan.
- CVE-2023-24487 requires a version scan.

The remediation for CVE-2023-24487 and CVE-2023-24488 requires an upgrade of the vulnerable ADC instance to a release and build that has the fix.

For more information on the fixed build version details for CVE-2023-24487 and CVE-2023-24488, see Security Bulletin.

NOTE:

ADC build 13.1–45.63 replaces build 13.1–45.61.

For more information on how to use NetScaler Console to upgrade ADC instances, see Create an ADC upgrade job.

NOTE:

It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2023-24488 and CVE-2023-24487 in the security advisory module. To see the impact sooner, you can start an on-demand scan by clicking **Scan Now**.

April 25, 2023

The enhancements and changes that are available in Build April 25, 2023.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Analytics

Web Insight - Support to view nil values in graphs

In **Web Insight**, when you drill down any metric under Applications, Clients, URLs, or Instances, the analytics view now provides the visibility of nil values (for example, 0 ms and 0 request) in the graph for the selected duration.

Earlier, if there is no traffic or transactions received for the selected duration, Web Insight displayed the graphs by skipping those nil values. As an administrator, you can now view the complete graph with these nil values.

StyleBooks

Specify user group access to config packs

As an administrator, you can now restrict user groups from accessing config packs created by other user groups. To select this option, navigate to **Settings > Users & Roles > Groups > Authorization Settings > Config Packs > All Configurations created by the user group**.

Fixed Issues

The issues that are addressed in Build April 25, 2023.

- In **Applications > Configuration > Config Packs**, when you enter a search query using the search criteria of **Properties > Display Key**, the search result is displayed but the search bar displays the index number of the result.

  With this fix, the search bar displays the search query in text instead of a number.

Analytics

- The bandwidth data in **HDX Insight** and **Gateway Insight** is displayed incorrectly in bytes per second instead of bits per second.

April 13, 2023

The enhancements and changes that are available in Build April 13, 2023.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Analytics

Integrated Cache notification in Web Insight

After you enable Integrated Cache in the NetScaler instance, the eligible requests are processed without requiring a round trip to an origin server. In **Web Insight**, these Integrated Cache requests are currently visible under **Servers** with virtual server IP address instead of the actual server IP address.

For a better visibility of these Integrated Cache requests, you can now view an IC notification next to the ADC virtual server IP address under **Servers**.

For the requests that are not processed with Integrated Cache, the actual origin server IP address is visible.

As an administrator, this notification enables you to quickly identify that the ADC instance has processed the Integrated Cache requests.

Integrated Cache hits and misses graph in Web Insight

In **Web Insight**, when you drill down a server, the **Server Metrics** now display **Integrated Cache Hits** and **Integrated Cache Misses** tabs.

As an administrator, the graph view in:

- The **Integrated Cache Hits** tab enables you to view the total responses that the NetScaler appliance serves from the cache.
- The **Integrated Cache Misses** tab enables you to view the total responses that the NetScaler appliance serves from the origin server.

Web Insight - View both average and maximum values in graphs

Starting from 13.1 45.47 or later versions, the **Web Insight** in NetScaler Console is supported with the visibility of maximum latency values under **Servers** and **Clients**.

In addition to this support, when you drill down a server or a client, you can now view both average and maximum values in the summary panel, and also by hovering the mouse pointer on the time series analytics graph in **Server Network Latency**, **Server Response Time**, and **Client Network Latency**.

As an administrator, this enhancement enables you to visualize the maximum latency in graphs for the selected duration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infrastructure

View data storage trends in NetScaler Console GUI

In **Settings > Data Storage**, you can now view the data storage information across the different features in your current deployment. The **Data Storage Management** dashboard helps you visualize how the data is stored and if the features are operating within their storage entitlement.

NOTE

The data storage policies are expected to change in the upcoming releases. With these changes, you will not be able to store historical data after it exceeds the storage limit.

For more information, see Manage data storage.

Fixed Issues

The issues that are addressed in Build April 12, 2023.

Infrastructure

- In high-availability deployments, there is no option to upload build image files only to the secondary node.

  As part of the fix, you can now upload build image files to the secondary node from **Infrastructure > Upgrade Jobs** > **Create Job** tab > **Upload to secondary node only**.

- The reports exported from **Infrastructure > Instances > NetScaler** do not display the serial number of secondary nodes.

  The reports now display the serial numbers of both primary and secondary nodes of the NetScaler instances. You can also view the reports from **Infrastructure > NetScaler Inventory**.

April 05, 2023

The enhancements and changes that are available in Build April 05, 2023.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Security

Create API definitions from discovered API endpoints in NetScaler Console GUI

You can now create API definitions from discovered API endpoints in **Security > API Gateway > API Discovery**.

Unified dashboard - View API analytics key metrics

In the unified dashboard (**Overview > Dashboard**), you now view key metrics for the API endpoints configured through NetScaler Console.

For more information, see A unified dashboard to view instance key metric details.

Fixed Issues

The issues that are addressed in Build April 05, 2023.

- The **Choose Appliance** option for **Certificate File** and **Key File** fields appears for the following pages:
  - **Infrastructure > SSL Dashboard > Manage Certificate Store > Add**
  - **Infrastructure > SSL Dashboard > SSL Certificates > Update**

  As a fix, the **Choose Appliance** option is now removed.

- If NetScaler has an on-premises NetScaler Console as a licensing server and an agent is modified in **Infrastructure > Instances > Agents**, the following issue occurs:

  `The IP address of the license server on NetScaler changes from the IP address of the on-premises NetScaler Console to the IP address of one of the NetScaler agents`.

- When you edit the password for an SDX admin profile configured with SNMPv3 from **Infrastructure > Instances> NetScaler > SDX tab > Profile**, the following error message appears:

  `Please provide valid authentication protocol. The possible values are MD5, SHA`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

March 14, 2023

Fixed issues

The following issue is addressed in Build March 14, 2023:

In **Infrastructure > SSL Dashboard > Install Certificates**, when you upload a certificate chain that has the same root certificate as an existing certificate chain, the certificate installation fails. The following text is displayed in **Infrastructure > SSL Dashboard > SSL Audit Logs > Device Log > Command Log**:

```
Resource Already Exists
```

When you delete an email distribution list from **Settings > Notifications > Email**, the following error is seen:

```
Error: Bad Gateway
```

This issue occurs because the name of the email distribution list has a white space.

As part of the fix, NetScaler Console now allows you to delete email distribution lists with white spaces.

March 02, 2023

Analytics

Improvements to Web Insight

In Web Insight, you can now view the following enhancements under **Application Metrics**:

- A new **Summary** tab is introduced that enables you to visualize an overview of the application performance such as Response Time, Requests, and Bandwidth. As an administrator, this enables you to get an insight of the application performance for the selected duration. You can use the toggle option and customize the view.
- In the **Requests** tab, apart from the existing total requests, you can also view requests from the top 5 clients based on the total requests. As an administrator, this enables you to get an insight on the clients accessing the application for the selected duration.
- In the **Bandwidth** tab, you can view the bandwidth consumption from the top 5 servers based on the total bandwidth consumption. As an administrator, this enables you to get an insight on the servers consuming more bandwidth for the selected duration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- In the **Response Time** tab, you can also view Client Network Latency, Server Network Latency, and Server Processing Time on the same graph. As an administrator, this enables you to get an insight on the latency that occurs from client, server, and application for the selected duration. You can use the toggle option and customize the view.

Infrastructure

Deletion of inactive NetScaler Console Express accounts

If your NetScaler Console Express account remains inactive for 45 days, the account will be deleted. Citrix sends a reminder after 30 days of inactivity.

Management and Monitoring

Change in execution summary for NetScaler high availability upgrade

In NetScaler Console GUI, the execution summary in **Infrastructure > Upgrade Jobs > Execution Summary** no longer displays the high availability synchronization related commands.

This is because, during the NetScaler high availability upgrade, if the NetScaler primary and secondary nodes are in different versions, NetScaler performs the disabling of the high availability synchronization between the nodes. NetScaler Console does not perform this operation.

Set threshold for individual entities in Network Reports

In **Infrastructure > Network Reporting > Thresholds**, you can now set the threshold value for specific entities while configuring the threshold.

For more information, see Network Reporting.

Support for scheduling individual agent upgrade

In **Infrastructure > Instances > Agents > Settings**, you can now schedule the upgrade of each NetScaler agent. You can choose to either automatically upgrade an agent to the next build or specify a time and time zone to schedule an upgrade.

For more information, see Agent upgrade settings.

Improvements in NetScaler instance upgrade

The following changes are now available in the **Pre-upgrade validation** tab:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Instances blocked from upgrade** section - This new section lists the instances that are blocked from upgrade because of pre-upgrade validation errors.
- **Quick Cleanup** button - This button is available in the **Disk Space Details** pane and allows you to quickly free up the disk space from multiple folders.

For more information, see How to upgrade an ADC instance.

NetScaler BLX images now available in the image library

While upgrading NetScaler BLX from **Infrastructure > Upgrade jobs > Upgrade NetScaler BLX > Select Image**, you can now select the **NetScaler BLX images** from the image library.

Security

View the versions of NetScaler Web App Firewall and bot signatures for a NetScaler instance

You can now view the versions of NetScaler Web App Firewall and bot signatures for a NetScaler instance. The latest signature versions protect your instance from the CVEs. For more information, see Signature Alert Articles and Bot signature alert articles.

Application Performance Analytics

Improvements to Web Insight

In **Web Insight**, you can now view the maximum network latency values in both **Server** and **Client**. As an administrator, this enhancement enables you to identify the exact server or client that is performing with maximum latency.

Earlier, Web Insight provided the maximum value only based on the average latency values across all servers and clients.

Miscellaneous

Create and apply filters in the unified dashboard

In the unified dashboard (**Overview > Dashboard**), you can now create and apply filters in:

- Applications
- ADC Infrastructure
- Application Security

© 1997–2026 Citrix Systems, Inc. All rights reserved.

As an administrator, you can apply filters and view insights only for the selected instances or applications.

For more information, see A unified dashboard to view instance key metric details.

Fixed Issues

The issues that are addressed in Build Mar 02, 2023.

- In **Infrastructure > Upgrade Jobs**, when you select a completed job that has the pre-upgrade or post-upgrade script file name with special characters and then download the output scripts from the **Select Action** list, the **File not found** error message is displayed.

February 07, 2023

Analytics

Security violations display OWASP tags

In the NetScaler Console GUI, the security violations now display OWASP tags. It supports the OWASP 2017 and OWASP 2021 lists. These tags help you determine whether the violation belongs to the OWASP top 10 list.

Select a violation to view more details. The details now include the OWASP 2017 and OWASP 2021 columns. These columns display the OWASP codes and you can use them to learn more about the violation from the OWASP website.

Management and Monitoring

Support for changing agent password without current password

As a super administrator, you can now allow agent passwords to be changed without their current passwords.

Navigate to **Settings** > **Global Settings** > **System Configurations** > **Agent and Time Zone > Agent** and select the **Remove current password prerequisite for agent password change** checkbox. The **Change Agent Password** page will no longer have the **Current password** field.

To display the **Current password** field again, clear the **Remove current password prerequisite for agent password change** checkbox.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Time series data visualization interval for NetScaler Console Express accounts is revised

For virtual servers managed with the Express account, the time series data visualization in analytics graphs and Network Reporting graphs for the **Last 1 Hour** duration is now revised.

FEATURE	EXISTING DATA VISUALIZATION INTERVAL	NEW DATA VISUALIZATION INTERVAL
Application dashboard	1 minute	5 minutes
Network Reporting	5 minutes	10 minutes
Web Insight, HDX Insight, Gateway Insight, Security Insights, BOT Insights, Detailed Transactions	1 minute	5 minutes

Fixed issues

The following issues are addressed in Build February 07, 2023.

When you enable or disable syslog settings for the ADC instance, ADM does not save configuration in the ADC instance. As a result, configuration changes events are not saved in NetScaler Console.

In **Infrastructure > Instances > Agent**, after you install the SSL certificate with a password encrypted key, the connection to agent on Port 443 fails.

January 24, 2023

Fixed issues

The following issues are addressed in Build January 24, 2023.

An error message appears when you enable SNMP v3 on a NetScaler SDX instance from the NetScaler Console GUI by navigating to **Infrastructure > Instances > NetScaler > SDX > Select Action > Configure SNMP**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

January 10, 2023

Management and Monitoring

View recommendations and manage your ADCs and apps efficiently as actionable Tasks with Guide Me workflows

In the NetScaler Console GUI, a new **Task** option is introduced, where you can now view recommendations based on your subscription and current utilization. As an administrator, you can:

- View **To-Do** tasks as actionable recommendations for licensing, analytics, events, SSL certificates, and many more
- Complete the task using the **Guide Me** option that provides guidance tool tips to successfully complete the task
- Acknowledge the tasks and move them to archive
- Go to **Archived tasks** and use the guided tool tips for recurring needs

These recommendations ensure that you are utilizing all the capabilities of NetScaler Console, enable product discovery and functionalities recommended by the product for efficient administration of the deployment.

For more information, see View recommendations and manage your ADCs and applications efficiently.

StyleBooks

Enable or disable netmask length in StyleBook configuration GUI

When you create a configuration pack from StyleBooks with the `type: ipnetwork` attribute, the StyleBook configuration GUI now displays the **Netmask Length** button next to the **IP address** field.

You can do one of the following actions:

- Enable to input netmask length
- Disable to input netmask IP address

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler® Console service documentation history

The following table describes important changes to the NetScaler Console service. To receive notifications about these updates, subscribe to the RSS feed.

DATE	CHANGE	TOPIC
03 Oct 2026	Refreshed the release notes by adding the information related to CVE-2026-88779.	Release notes
27 Sep 2026	Refreshed the release notes by adding the information related to CVE-2026-88771, CVE-2026-88772, CVE-2026-88773, CVE-2026-88774, CVE-2026-88775, CVE-2026-88776, CVE-2026-88777, CVE-2026-88778.	Release notes
15 Sep 2026	Added the latest release notes.	To view the list of new features and fixed issues, see What's new and Known issues.
01 Sep 2026	Added the latest release notes.	To view the list of new features and fixed issues, see What's new and Known issues.
19 Aug 2026	Refreshed the release notes by adding the CVE-2026-19489 and CVE-2026-19490 related information.	Release notes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TOPIC
04 Aug 2026	Added the latest release notes.	To view the list of new features and fixed issues, see What's new and Known issues.
14 Jul 2026	Added the latest release notes.	To view the list of new features and fixed issues, see What's new and Known issues.
30 Jun 2026	Refreshed the release notes by adding the CVE-2026-8451, CVE-2026-8452, CVE-2026-8655, CVE-2026-10816, and CVE-2026-10817 related information.	Release notes
17 Jun 2026	Added the latest release notes.	To view the list of new features and fixed issues, see What's new and Known issues.
03 Jun 2026	Added the latest release notes.	To view the list of new features and fixed issues, see What's new and Known issues.
19 May 2026	Added the latest release notes.	To view the list of new features and fixed issues, see What's new and Known issues.
31 Mar 2026	Added the latest release notes.	To view the list of new features and fixed issues, see What's new and Known issues.
23 Mar 2026	Refreshed the release notes by adding the	Release notes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TOPIC
	CVE-2026-4368 and CVE-2026-3055 related information.	
09 Mar 2026	Added the latest release notes.	To view the list of new features and fixed issues, see What's new and Known issues.
20 Feb 2026	Refreshed release notes to include an enhancement: CTXENG-72150.	To view the list of new features and fixed issues, see What's new and Known issues.
17 Feb 2026	Added the latest release notes.	To view the list of new features and fixed issues, see What's new and Known issues.
04 Feb 2026	Added the latest release notes.	To view the list of new features and fixed issues, see What's new and Known issues.
09 Dec 2025	Refreshed the release notes to include fixed issue NSHELP-41292.	Release notes
11 Nov 2025	Refreshed the release notes by adding the CVE-2025-12101 related information.	Release notes
06 Nov 2025	Added the latest release notes.	To view the list of new features and fixed issues, see What's new and Known issues.
15 Oct 2025	Added the latest release notes.	To view the list of new features and fixed issues, see

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TOPIC
		What's new and Known issues.
17 Sep 2025	Added the latest release notes.	To view the list of new features and fixed issues, see What's new and Known issues.
08 Sep 2025	Refreshed release notes to include new feature support for License Activation Service (LAS) licensing mechanism.	To view the list of new features and fixed issues, see What's new.
03 Sep 2025	Added the latest release notes.	To view the list of new features and fixed issues, see What's new and Known issues.
29 Aug 2025	Refreshed release notes to include known issue: NSADM-123777.	To view the list of known issues, see Known issues.
26 Aug 2025	Refreshed the release notes by adding the CVE-2025-7775, CVE-2025-7776, and CVE-2025-8424 related information.	Release notes
20 Aug 2025	Added the latest release notes.	To view the list of new features and fixed issues, see What's new and Known issues.
17 Jul 2025	Added the latest release notes.	To view the list of new features and fixed issues, see What's new and Known issues.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TOPIC
15 Jul 2025	Refreshed release notes to include an enhancement: CTXENG-66078.	To view the list of new features and fixed issues, see What's new and Known issues.
04 Jul 2025	Refreshed release notes to include fixed issues NSHELP-40244, NSHELP-39868, and NSADM-121464.	To view the list of new features and fixed issues, see What's new and Known issues.
02 Jul 2025	Added the latest release notes.	To view the list of new features and fixed issues, see What's new and Known issues.
25 Jun 2025	Refreshed the release notes by adding the CVE-2025-6543 related information.	Release notes
17 Jun 2025	Refreshed the release notes by adding the CVE-2025-5349 and CVE-2025-5777 related information.	Release notes
03 Jun 2025	Added the latest release notes.	To view the list of new features and fixed issues, see What's new and Known issues.
30 May 2025	Refreshed the release notes by adding an enhancement: CTXENG-66229	Release notes
26 May 2025	Added the latest release notes.	To view the list of new features and fixed issues, see What's new and Known issues.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE	CHANGE	TOPIC
06 May 2025	Added the latest release notes.	To view the list of new features and fixed issues, see What's new and Known issues.
15 Apr 2025	Added the latest release notes.	To view the list of new features and fixed issues, see What's new and Known issues.
19 Feb 2025	Added the latest release notes.	To view the list of new features and fixed issues, see What's new and Known issues.
10 Feb 2025	Refreshed the release notes by adding an enhancement [NSADM-108789].	Release notes
06 Feb 2025	Added the latest release notes.	To view the list of new features and fixed issues, see What's new and Known issues.
15 Jan 2025	Added the latest release notes.	To view the list of new features and fixed issues, see What's new and Known issues.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

fix

This is the content for the sample heading topic. It is hidden from the main table of contents but remains accessible via links.

© 1997–2026 Citrix Systems, Inc. All rights reserved.