NetScaler® Console service

Copyright © 1997–2025. Citrix Systems, Inc. All Rights Reserved.

Contents

Overview 10

Features and solutions 12

Release notes 15

What's new 16

Known issues 64

Data compliance 65

NetScaler telemetry program 66

Data governance 68

Getting started 74

Configure the built-in agent to manage instances 88

Install a NetScaler agent on-premises 93

Install a NetScaler agent on Microsoft Azure cloud 95

Install a NetScaler agent on Amazon Web Services (AWS) 106

Install a NetScaler agent on GCP 120

Install NetScaler agent in Kubernetes cluster using YAML 124

Install a NetScaler agent operator using the OpenShift console 125

Install a container-based agent using helm chart 132

How to Get Help and Support 133

Enhanced Graphical User Interface 141

Low-touch onboarding of NetScaler instances using Console Advisory Connect 149

Onboard NetScaler instances using Console Advisory Connect 152

Test onboarding readiness of NetScaler instances 171

Email Settings 172

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Troubleshoot issues using the diagnostic tool or the NetScaler Console GUI 176

Transition from a built-in agent to an external agent 184

Connect SAML as an identity provider to NetScaler Console 185

System requirements 198

Licenses 207

Upgrade Advisory 210

Security Advisory 217

Secure configuration recommendations 225

CVE Detection 231

File integrity monitoring 237

Identify and remediate vulnerabilities for CVE-2025-8424 239

Identify and remediate vulnerabilities for CVE-2025-7776 241

Identify and remediate vulnerabilities for CVE-2025-7775 242

Identify and remediate vulnerabilities for CVE-2025-6543 243

Identify and remediate vulnerabilities for CVE-2025-5349 245

Remediate vulnerabilities for CVE-2025-5777 247

Remediate vulnerabilities for CVE-2024-8535 251

Remediate vulnerabilities for CVE-2020-8300 256

Remediate vulnerabilities for CVE-2021-22927 and CVE-2021-22920 268

Identify and remediate vulnerabilities for CVE-2021-22956 280

Identify and remediate vulnerabilities for CVE-2022-27509 287

Unsupported CVEs in Security Advisory 289

Setting up 290

Adding multiple agents 290

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Configure agents for multisite deployment 292

Configuring agent upgrade settings 294

Dual NIC support on NetScaler Console 297

Adding instances 300

Configuring syslog on instances 310

Logstream overview 312

How to assign more permissions to delegated admin users 314

Integration with the ServiceNow instance 320

Actionable tasks and recommendations 322

A unified dashboard to view instance key metric details 333

Create custom dashboards to view instance key metric details 344

API Security 348

Create or upload an API definition 351

Deploy an API instance 353

Add policies to an API deployment 357

View API analytics 364

Discover API endpoints 374

Undeploy an API instance 379

Use APIs to manage API Security 380

Create WAF and BOT profiles using StyleBooks 390

Applications 391

Web Insight dashboard 393

Analyze the root cause for application slowness 400

Service Graph 404

© 1997–2025 Citrix Systems, Inc. All rights reserved.

StyleBooks 407

Application Security Dashboard 409

Unified Security dashboard 413

View application security violation details 422

Application overview 424

All Violations 435

API Security 438

WAF learning 441

WAF recommendations 443

Gateway Insight 451

HDX Insight 470

Enable HDX Insight data collection 481

Enable data collection for NetScaler Gateway appliances deployed in single-hop mode 481

Enable data collection to monitor NetScalers deployed in transparent mode 483

Enable data collection for NetScaler Gateway appliances deployed in double-hop mode 485

Enable data collection to monitor NetScalers deployed in LAN user mode 490

Create thresholds and configure alerts for HDX Insight 493

View HDX Insight reports and metrics 498

Troubleshoot HDX Insight issues 498

Metrics information for thresholds 511

Infrastructure Analytics 514

View instance details in Infrastructure Analytics 539

View the capacity issues in an NetScaler instance 547

Enhanced Infrastructure Analytics with new indicators 549

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Instance management **553**

How to monitor globally distributed sites **554**

How to create tags and assign to instances **563**

How to search instances using values of tags and properties **566**

Centralized GeoIP DB Updates through NetScaler Console **569**

Manage admin partitions of NetScaler instances **573**

Back up and restore NetScaler instances **578**

Force a failover to the secondary NetScaler instance **584**

Force a secondary NetScaler instance to stay secondary **585**

Create instance groups **585**

Global Server Load Balancing site groups **586**

Create SNMP managers and users for NetScaler agent **587**

Provision NetScaler VPX instances on SDX **593**

Rediscover multiple NetScaler instances **602**

Polling overview **602**

Unmanage an instance **609**

Trace the route to an instance **610**

View NetScaler-owned IP addresses **610**

How to change the NetScaler MPX or VPX root password **615**

How to change a NetScaler SDX nsroot password **620**

How to generate a technical support bundle for a NetScaler instance **624**

Events **625**

Use events dashboard **626**

Create event rules **628**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Schedule an event filter **644**

Modify the reported severity of events that occur on NetScaler instances **645**

View events summary **646**

Display event severities and SNMP trap details **648**

View and Export syslog messages **651**

Suppress syslog messages **656**

SSL dashboard **659**

Zero-touch certificate management **660**

Use the SSL dashboard **663**

Set up notifications for SSL certificate expiry **672**

Update an installed certificate **673**

Install SSL certificates on a NetScaler instance **676**

Create a Certificate Signing Request (CSR) **678**

Link and unlink SSL certificates **680**

Configure an enterprise policy **681**

Poll SSL certificates from NetScaler instances **682**

Use the NetScaler Console certificate store to manage SSL certificates **682**

Configuration jobs **684**

Create a configuration job **687**

Configuration audit **691**

Upgrade jobs **691**

Use jobs to upgrade NetScaler instances **701**

Network functions **719**

Generate reports for load balancing entities **719**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Export or schedule export of network functions reports **722**

Network reporting **724**

Provisioning NetScaler VPX Instances on AWS **733**

Manage the Kubernetes cluster for Service Graph **744**

License Activation Service **747**

License management **756**

Minimum and maximum capacity for checkout **767**

NetScaler agent behavior **774**

Flexed license **778**

Configure license **782**

License dashboard **793**

License reporting **796**

Transition to Flexed licensing **800**

Scenarios for Flexed or Pooled license expiry and connectivity issues behavior **805**

Configure NetScaler Console server only as the Flexed or Pooled license server **810**

Pooled capacity **813**

Upgrade a perpetual license in NetScaler MPX to NetScaler Pooled capacity **814**

Upgrade a perpetual license in a NetScaler SDX to NetScaler Pooled capacity **826**

NetScaler VPX check-in and check-out licensing **829**

NetScaler virtual CPU licensing **833**

FAQs and other resources **835**

Troubleshoot Pooled capacity license issues **838**

Console on-prem instances connected with Console service using Cloud Connect **844**

Console on-prem upload **845**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Configure analytics on virtual servers 848

Configure role-based access control 856

Assign a net profile for the managed NetScaler instance 877

Data storage management 878

Understand your data storage 879

Manage your storage space 885

Data retention policy 888

Configure and view system alarms 890

Observability Integration 895

Integration with Splunk 895

Integration with New Relic 907

Integration with Microsoft Sentinel 911

Configure NetScaler instances for the export of insights to Prometheus using the default schema 930

Configure the export of NetScaler metrics and audit logs to Splunk 932

Configuring Analytics settings 934

Configure notifications 936

Export or schedule export reports 940

Instance settings 943

Instance settings 945

System configurations 948

Email subscriptions 949

Enable or disable features 951

Configure an action policy to receive application event notifications 952

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Use audit logs for managing and monitoring your infrastructure **964**

Configure IP address management (IPAM) **966**

How-to articles **970**

FAQs **973**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Overview

January 8, 2024

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 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

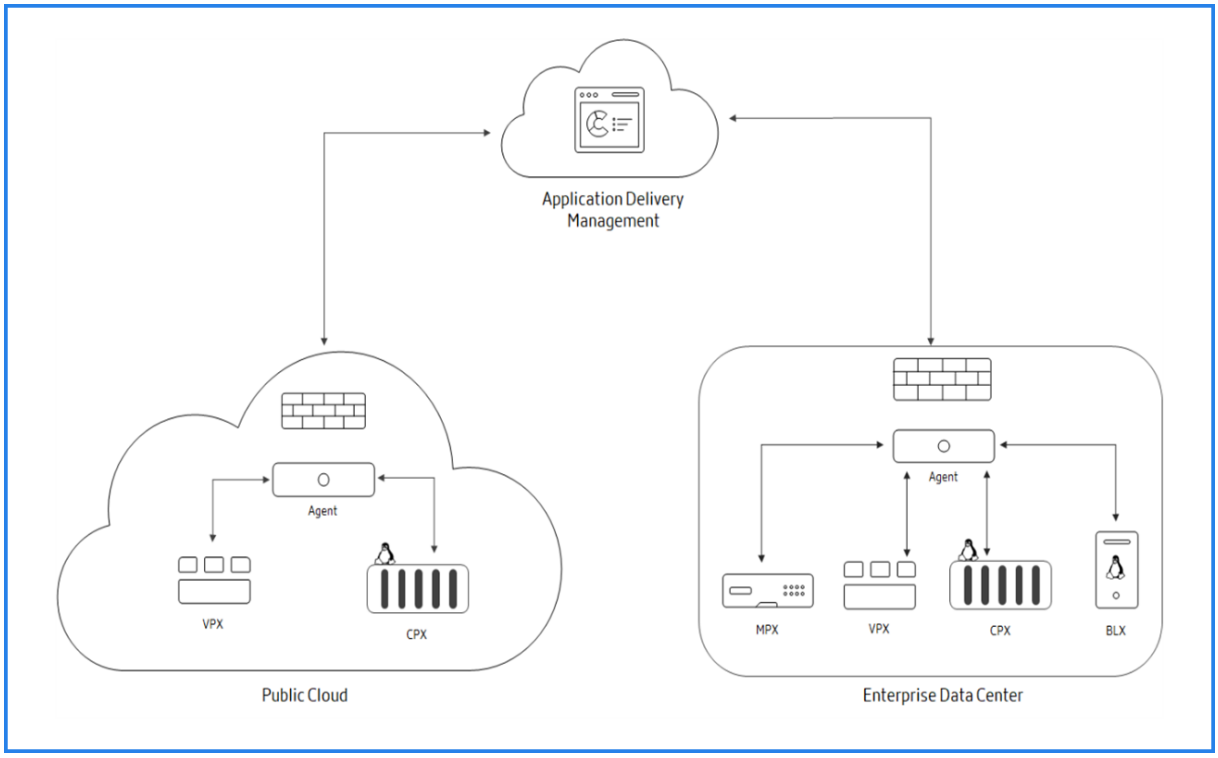
The service collects instance details such as:

- 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):

© 1997–2025 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

January 8, 2024

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 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

© 1997–2025 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.
- Security Insight: Provides a single-pane solution to help you assess your application security status and take corrective actions to secure your applications.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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

Release notes

January 8, 2024

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

September 8, 2025

September 08, 2025

Licensing

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 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..

[CTXENG-65614]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

[NSHELP-40538]

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 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.

[CTXENG-69636]

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:**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 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.

[CTXENG-69636]

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

- 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.

[CTXENG-69636]

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**.

[CTXENG-68123]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

[CTXENG-67372]

Fixed issues

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

[NSHELP-40497]

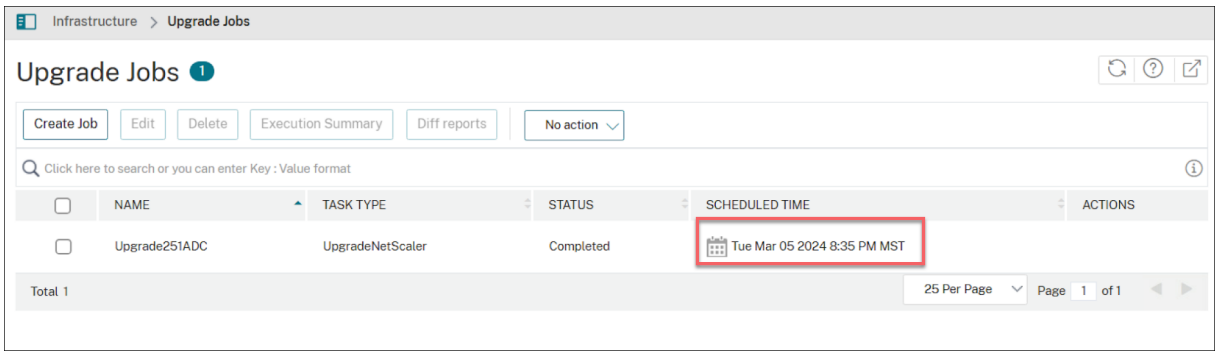
July 17, 2025

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.



[CTXENG-67854]

© 1997–2025 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.

[NSADM-122828]

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

[NSADM-122827]

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.

[CTXENG-67426]

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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

`rm analytics profile telemetry_metrics_profile`

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

[CTXENG-67328]

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

[CTXENG-66078]

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.

[NSHELP-40028]

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.

[NSHELP-39868]

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

[NSHELP-40244]

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

[NSADM-121464]

© 1997–2025 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.

[CTXENG-68572]

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:

  1. Upgrade the vulnerable NetScaler instance to a release and build that has the fix.
  2. Apply configuration jobs.

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

© 1997–2025 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**.

[CTXENG-67354]

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.

[NSHELP-39910]

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

[NSHELP-40070]

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

[NSHELP-40002]

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 vir-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

tual 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.

[CTXENG-66309]

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.

[CTXENG-66308]

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.
- 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.

[CTXENG-66229]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Fixed issues

Analytics

- Some processes in NetScaler agent crash and generate core files. As a result, the disk space is full.

[NSHELP-40082]

- Export of more than 1 MB data from NetScaler Console to Microsoft Sentinel fails.

[NSHELP-39935]

- 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.

[NSHELP-39702]

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

[NSHELP-39508]

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

[NSHELP-39484]

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.

[NSHELP-39701]

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

[NSHELP-39101]

© 1997–2025 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

[CTXENG-66758]

Deprecation of autoscaling of NetScaler instances in public clouds

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

[CTXENG-66472]

Improvements to Configuration Jobs

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

[CTXENG-66227]

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.

[CTXENG-66224]

© 1997–2025 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.

[NSHELP-39571]

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

[NSHELP-39425]

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

[NSHELP-39392]

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.

[NSADM-116346]

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.

© 1997–2025 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**.

[NSHELP-39415]

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.

[NSADM-117800]

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.

[NSADM-108789]

© 1997–2025 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
```

[NSHELP-39259]

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.

[NSADM-112194]

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:

- Compatibility with diverse network proxies that use various headers.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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.

  [NSADM-114167]

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.

[NSADM-107153]

Infrastructure

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

[NSADM-113715]

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

[NSADM-114530]

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.

[NSADM-112540]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

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

[NSADM-111339]

Fixed issues

Analytics

- In **Settings > Observability Integrations**, editing or deleting a subscription might fail if a NetScaler command failure occurs.

  [NSHELP-39094]

- In **HDX Insight** and **Web Insight**, the Geolocation report does not resolve the client IP location for the defined IP block.

  [NSHELP-39036]

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**.

  [NSHELP-39046]

- 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.

  [NSHELP-39077]

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.

  [NSHELP-39196]

- 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.

  [NSHELP-39035]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- When you edit config packs in **Applications > Configurations > Config Packs**, the order of added items is not retained.

  [NSHELP-38893]

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

For more information, see: Simplified migration using StyleBook

[NSADM-115574]

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.

[NSADM-117532]

Fixed Issues

Analytics

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

  [NSHELP-38356]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Infrastructure

- NetScaler Console fails to generate a Certificate Signing Request (CSR) from the SSL dashboard.

  [NSHELP-39085]

- When you update the permissions in Identity and Access Management (IAM) for an Azure group, the changes are not reflected in NetScaler Console.

  [NSHELP-39020]

- DeviceAPIProxy calls fail to get the results for the ‘‘systemfiles’’NITRO call from NetScaler.

  [NSHELP-38971]

- The **PINNED** menu list is visible only when the first level of the menu is expanded in the enhanced GUI of NetScaler Console.

  [NSADM-117694]

StyleBooks

- Attempting to configure a Link Aggregation Control Protocol (LACP) channel using a StyleBook config pack fails.

  [NSHELP-38914]

- Force deleting a configpack fails if it is missing mandatory parameters.

  [NSHELP-38906]

- When you update a StyleBook definition, draft and scheduled configpacks are inadvertently deployed .

  [NSHELP-38905]

- 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.

  [NSHELP-38894]

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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.

[NSADM-114172]

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.

[NSADM-104780]

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.

  [NSHELP-38869]

- 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.

    [NSHELP-38849]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- When a read-only user logs in to NetScaler Console, the following error message appears:

  No or invalid session found.

  [NSHELP-38833]

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.

[NSHELP-38656]

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.

- 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:

  1. Upgrade the vulnerable NetScaler instance to a release and build that has the fix.
  2. 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 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**.

[NSADM-116109]

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.

[NSADM-114637]

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.

[NSADM-113728]

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.

[NSADM-109893]

Fixed issues

Infrastructure

- In the **Infrastructure > SSL Dashboard**, the root and intermediate certificates in the SSL certificate chain are not displayed.

  [NSHELP-38428, NSADM-116525]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- In the **Infrastructure > SSL Dashboard**, the issuer of the publicly available certificates is incorrectly displayed as **Not Recommended**.

  [NSHELP-38408]

- In NetScaler Console, event messages containing between "**<**" and "**>**" are not displayed in the email body.

  [NSHELP-38257]

- 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
  "
  ```

  [NSHELP-38763]

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 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.

[NSADM-111746]

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.

[NSADM-115574]

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:

  1. Select an application from the **Top Applications** reported under WAF to view more details.
  2. Click **See more** under **Violation details**.
  3. Under **Timeline Details**, click **+** and select all columns.

  [NSHELP-38591]

Infrastructure

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

  [NSHELP-38058]

StyleBooks

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

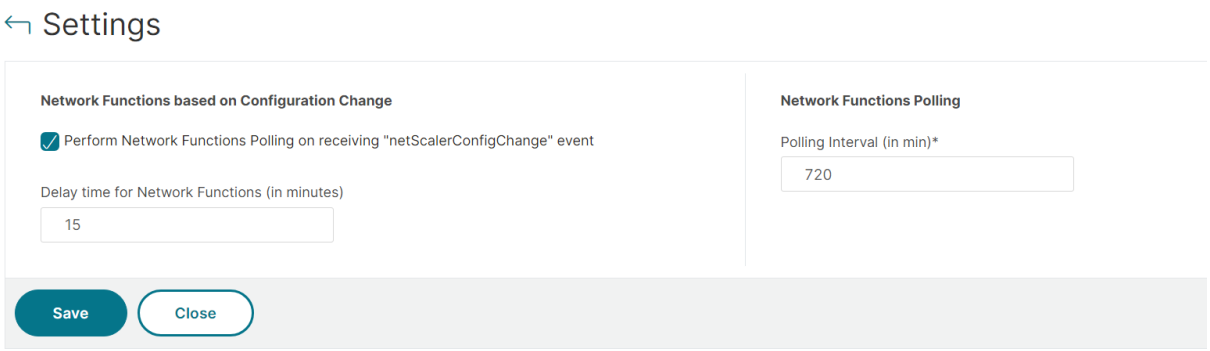
  [NSHELP-38535]

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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.

[NSADM-115408]

Fixed issues

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

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

[NSHELP-38490]

StyleBooks

- Creating a configpack from a StyleBook definition that has `snmptrap_snmpuser_binding` fails with an error message list index out of range.

  [NSHELP-38538]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- When configuring a StyleBook, the GUID of the selected datasource is shown instead of its readable name in the input summary view.

  [NSADM-115644]

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

[NSADM-114776]

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.

  [NSHELP-38370]

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

  [NSHELP-38356]

August 27, 2024

Analytics

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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.

[NSADM-97377]

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.

[NSADM-111546]

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.

[NSADM-91862]

StyleBooks

Reuse configurations created outside of StyleBooks and share configurations between Config-Packs 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.

[NSADM-112547]

Fixed Issues

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

[NSHELP-38292]

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.

  [NSHELP-38443, NSHELP-38448]

- When provisioning the NetScaler agent or NetScaler VPX on Microsoft Azure, the NetScaler Console Provisioning service API fails to retrieve Azure subnet details.

[NSHELP-38349]

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.

[NSADM-113851]

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

[NSADM-114375]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

[NSADM-109528]

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.

[NSADM-88798, NSADM-91769]

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.

[NSADM-105358]

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.

[NSADM-100327]

Fixed issues

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

  [NSHELP-38083]

- 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.

  [NSHELP-37831]

- 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.

  [NSADM-113332]

- The SNMP traps are not received in NetScaler Console service when it is configured by using the built-in agent.

  [NSHELP-38191]

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

[NSADM-110351]

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.

© 1997–2025 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.

[NSADM-113300]

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.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

[NSADM-111609]

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.

[NSADM-111138]

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

[NSADM-109022]

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.

[NSADM-109019]

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

data centers, enabling efficient application delivery from these environments.

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

[NSADM-108491]

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.

  [NSHELP-38032]

- 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.

  [NSHELP-37713]

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 ”

  [NSHELP-37977]

- 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**).

  [NSHELP-37902]

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.

  [NSHELP-37656]

© 1997–2025 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

[NSADM-108930]

Platform

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

[NSPLAT-29640]

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.

[NSADM-110734]

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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

[NSADM-110728]

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**.

  [NSHELP-37720]

- If more than 25000 virtual servers are managed through NetScaler Console, App Dashboard might take more time to load details.

  [NSADM-111705]

Infrastructure

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

  [NSHELP-37616]

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.

  [NSHELP-37826]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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.

  [NSHELP-37824]

- 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.

  [NSHELP-37793]

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.

[NSADM-108164]

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Bandwidth is renamed to throughput capacity.

For more information, see Flexed license reporting

[NSADM-97093]

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.

[NSADM-12651]

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.

[NSHELP-37831]

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.

[NSHELP-37786]

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.

[NSADM-109020]

© 1997–2025 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.

[NSADM-97285]

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.

  [NSHELP-37689]

- 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.

  [NSHELP-37749]

Licensing

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

  [NSHELP-37733]

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**.

  [NSHELP-37562]

© 1997–2025 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.

[NSADM-108858]

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.

[NSADM-108790]

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 .

[NSADM-103826]

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.

  [NSHELP-37551]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- The count of used and unused certificates displayed in **Infrastructure > SSL Dashboard > Usage** is incorrect when the SSL certificates have certificate chains.

  [NSHELP-37469, NSADM-106867]

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.

  [NSADM-110461]

Security

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

  "**HTTP Error 500 ([object Object]) while accessing the data endpoint: "apps"**"

  [NSHELP-37598]

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.

  [NSADM-110118]

- 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
  ```

  [NSHELP-37313]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

  [NSHELP-37368]

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.

[NSADM-105168]

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**.

  [NSHELP-37400]

- In **Gateway > Gateway Insight**, the **Authentication** tab does not display user details for the failed authentications.

  [NSHELP-37465]

Infrastructure

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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"

  [NSHELP-37331]

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 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.

[NSADM-108300]

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.

[NSADM-108803]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

[NSADM-104833]

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

[NSADM-104702]

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.

[NSADM-101426]

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.

[NSADM-96821]

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.

[NSADM-105513]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

[NSADM-92376]

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.

  [NSHELP-37006]

- Users are unable to access NetScaler Console if they belong to multiple Azure Active Directory groups.

  [NSHELP-37005]

- In **Web Insight** and **Security Violations**, the Schedule Export workflow in the GUI is enhanced for better user experience.

  [NSADM-106624]

- In **Infrastructure > Network Reporting**, the tabular export report does not include details such as service, service group, virtual server, and interface name.

  [NSHELP-37224]

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

  [NSADM-106497]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

[NSADM-105343]

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.
- 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.

[NSADM-100803]

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.png).

© 1997–2025 Citrix Systems, Inc. All rights reserved.

For more information, see Automate radar object deployment.

[NSADM-104691]

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**).

  [NSHELP-37159]

Licensing

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

  [NSADM-106497]

Management and Monitoring

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

  [NSHELP-37176]

- 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**).

  [NSHELP-36943]

- 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.

  [NSHELP-36438]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

[NSADM-104715]

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**)

[NSADM-104710]

Fixed Issues

The issues that are addressed in Build Jan 24, 2024.

- The built-in agent registration in NetScaler SDX displays a success message but the SDX instance does not appear in **Infrastructure > Instances Dashboard**.

  [NSHELP-37137, NSHELP-37128]

- 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.

  [NSHELP-36964]

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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**.

[NSADM-104763]

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.

[NSADM-100879]

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.png), 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.

[NSADM-91686]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

[NSADM-101036]

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.

[NSADM-101035]

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.

[NSADM-104715]

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.

[NSADM-101273]

Fixed Issues

The issues that are addressed in Build Jan 09, 2024.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Licensing

- After the Flexed or Pooled license is applied, the **Analytics Configuration** page (**Settings > Analytics Configuration**) is not updated with the correct details.

  [NSADM-106665]

- The Flexed license dashboard in **NetScaler Licensing > Flexed Licensing > Dashboard** appears blank.

  [NSADM-106561]

- In **NetScaler Licensing > License Management**, the configuration for the threshold breach through email notification is not working as expected.

  [NSHELP-36895]

Known issues

September 1, 2025

NetScaler Application Delivery Management (NetScaler Console) has the following known issues:

Management and monitoring

- 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.

  [NSADM-123777]

- In **Infrastructure > SSL Dashboard > Manage Certificate Store**, when you click **Import NetScaler Certificates**, NetScaler Console fails to import NetScaler certificates of PFX format.

  [NSHELP-34803]

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.

  [NSADM-119768]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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>_.`

  [NSADM-102202]

- 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.

  [NSADM-110553]

- 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:

  1. Log on to NetScaler Console using an SSH client.
  2. Check the output for the following command:

     ```
     ls -l /etc/sshd_config
     ```

  3. In `/etc/sshd_config`, update it to add the following:

     ```
     HostKey /nsconfig/ssh/ssh_host_ecdsa_key
     ```

  4. Apply the changes:

     ```
     ps -aux | grep /usr/sbin/sshd | grep -v grep | tr -s ''| cut
     -d ''-f 2 | xargs kill -9
     ```

[NSADM-114072]

Data compliance

January 8, 2024

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

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.

NetScaler telemetry program

January 3, 2025

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

```
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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
ns_telemetry_server,<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:

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.

Data governance

June 14, 2024

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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).

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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).
- **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **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 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

> **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:
  - Google Maps, 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)

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

Getting started

September 8, 2025

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`.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Important**
>
> - You cannot change the region later.
> - This step is not applicable if you login from Citrix Cloud Japan (`citrix.citrixcloud.jp`). You must ensure that the endpoint URLs applicable for Japan are in 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

Select one of the following deployment options that suits your business requirement:

- **Smart deployment** - This option is an automated environment setup to deploy new NetScaler instances. It automatically installs an agent to enable communication between the NetScaler Console and the managed instances.

  This option supports AWS, Microsoft Azure, and Google Cloud environments. In three steps, you can deliver an application that is present in the cloud using NetScaler instances.

- **Custom deployment** - This option is a multi-stage deployment. You can select each environment option and deploy or discover NetScaler instances.

Select smart deployment for AWS

This deployment option creates the following infrastructure in AWS:

- A CloudFormation stack in AWS to create the required infrastructure that includes subnets, security groups, NAT gateways, and so on.
- An agent in the VPC to manage NetScaler instances.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

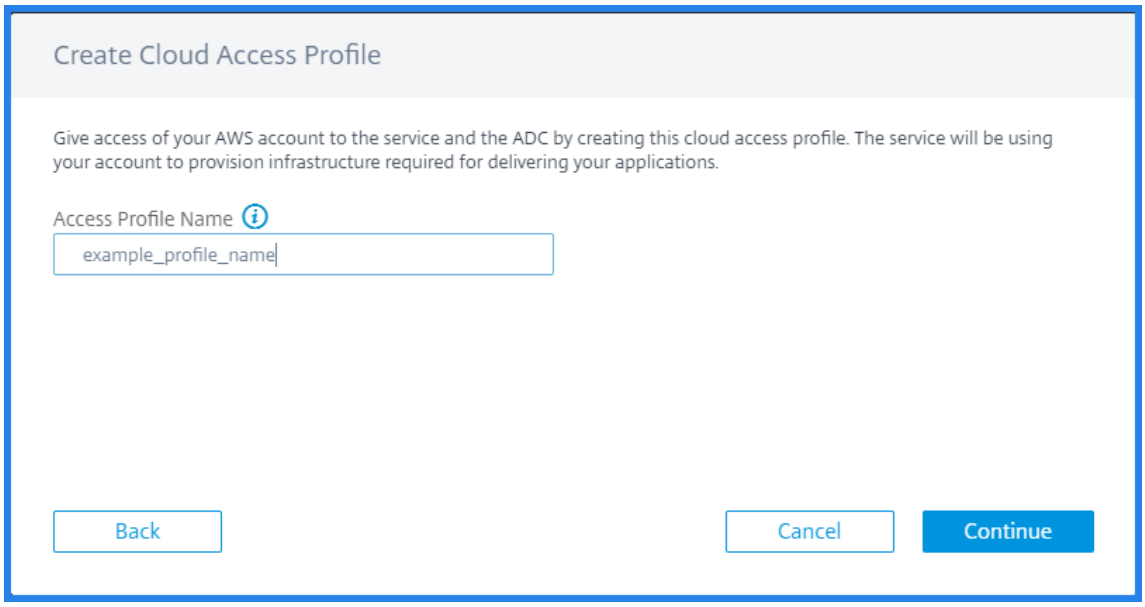
- A NetScaler Autoscale group. You can customize this group later in the **Infrastructure > Public Cloud > Autoscale Groups** page.

Before deploying NetScaler instances, ensure the following:

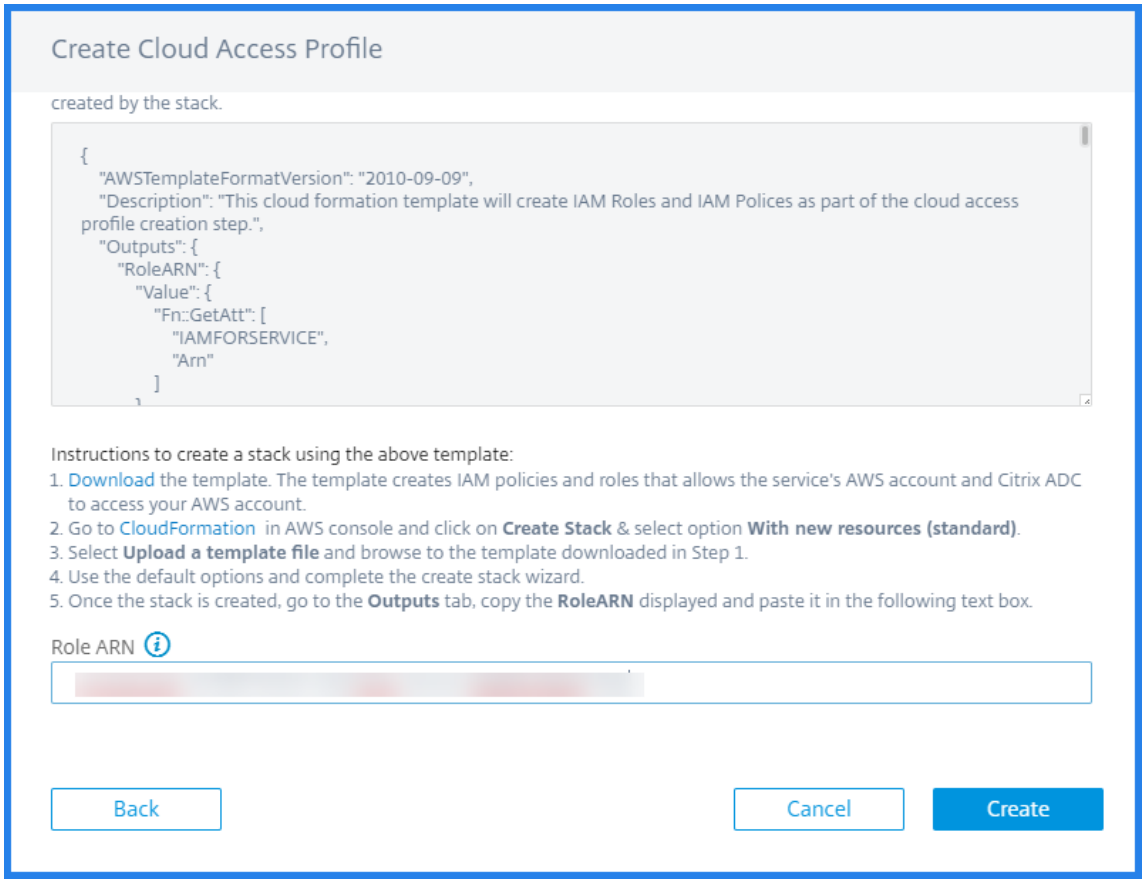
1. You already possess an AWS account.
2. You have created an IAM user with all administrative permissions.

To deploy NetScaler instances, perform the following steps:

1. In **Create Cloud Access profile**, select **AWS** as a deployment environment. Specify **Access Profile Name** and **Role ARN** to create a Cloud Access Profile.



© 1997–2025 Citrix Systems, Inc. All rights reserved.



The NetScaler Console uses the Cloud Access Profile to access an AWS account.

2. Specify the following details to prepare the AWS environment:

   a) In **Data Center Details**, select **AWS Region** and **AWS VPC** where you want to deploy NetScaler instances.

      AWS VPC lists the VPCs present in the selected **AWS Region**.

   b) In **NetScaler AutoScale Group Details**, specify the following to Autoscale NetScaler instances in the AWS cloud:

      - **AutoScale Group Name** - A name to identify an Autoscale group.
      - **Availability Zones** - Select the zones in which you want to create the Autoscale groups.

        You can select multiple zones from the list.
      - **Deployment Type** - Select either **Evaluation** or **Production** option.

        If you want to evaluate the NetScaler Console Autoscale solution before purchasing the production license, select the **Evaluation** option.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Important**
>
> – The evaluation option supports only one availability zone.
> – With the evaluation option, you can select only NetScaler VPX Express. And, the NetScaler Console Autoscale solution can scale up to three NetScaler instances.

- **NetScaler VPX product** - Select licenses to provision NetScaler instances.

  Subscribe to the selected license in the AWS marketplace and return to this page.

  Review and select the user consent message.

- **Instance type** - Select the required instance type.

c) Click **Next**.

After successful validation, click **Create** to deploy NetScaler instances in AWS and create an Autoscale group.

3. After the successful NetScaler deployment, click **Deploy Application**.

   In **Configure Application**, specify the necessary details and click **Submit**.

   For more information, see Configure an application for the Autoscale group.

Select smart deployment for Microsoft Azure

This deployment option creates the following infrastructure in Azure:

- An Azure Resource Manager (ARM) template to create the required infrastructure that includes subnets, security groups, NAT gateways, and so on.
- An agent in the VPC to manage NetScaler instances.
- A NetScaler Autoscale group. You can customize this group later in the **Infrastructure > Public Cloud > Autoscale Groups** page.

Before deploying NetScaler instances, ensure 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.

To deploy NetScaler instances, perform the following steps:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

1. In **Create Cloud Access profile**, select **Microsoft Azure** as a deployment environment. Specify NetScaler Console and NetScaler cloud access profile details.

   The NetScaler Console uses the NetScaler Console Cloud Access Profile to access a Microsoft Azure account. And, a NetScaler Cloud Access Profile is used to provision NetScaler VPX instances.

2. Specify the following details to prepare the Azure environment:

   a) In **Application Environment Details**, specify a name for your deployment. And, ensure that the correct Cloud Access Profile is selected.

   b) In **Data Center Details**, specify the region, resource group, and virtual network details where you want to deploy NetScaler instances.

   c) In **NetScaler AutoScale Group Details**, specify the following:

   - **Availability** - Select the availability zone or set in which you want to create the Autoscale groups. Depending on the cloud access profile that you have selected, availability zones appear on the list.
   - **Deployment Type** - Select either **Evaluation** or **Production** option.

     If you want to evaluate the NetScaler Console Autoscale solution before purchasing the production license, select the **Evaluation** option.

     > **Important**
     >
     > - The evaluation option supports only one availability zone or set.
     > - With the evaluation option, you can select only NetScaler VPX Express. And, the NetScaler Console Autoscale solution can scale up to three NetScaler instances.

   - **Select NetScaler VPX product** - Select licenses to provision NetScaler instances.

     Subscribe to this Azure Marketplace license and return to the page.

     Review and select the user consent message.

   - **Select VM size** - Select the required virtual machine size.

   d) Click **Next**.

   After successful validation, click **Create** to deploy NetScaler instances in Microsoft Azure and create an Autoscale group.

3. After the successful NetScaler deployment, click **Deploy Application**.

   In **Configure Application**, specify the necessary details and click **Submit**.

   For more information, see Configure an application for the Autoscale group.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Select smart deployment for Google Cloud

This deployment option creates the following infrastructure in Google Cloud:

- A Google Cloud Deployment Manager to create the required infrastructure that includes VPC networks, subnets, Cloud NAT, Cloud Router gateways, and firewall rules.
- An agent in the VPC to manage NetScaler instances.
- A NetScaler Autoscale group. You can customize this group later in the **Infrastructure > Public Cloud > Autoscale Groups** page.

Before deploying NetScaler instances, ensure that you already possess a Google Cloud account. For more information on how to create an account, see Google Cloud Documentation.

To deploy NetScaler instances, perform the following steps:

1. In **Create Cloud Access profile**, select **Google Cloud** as a deployment environment.

   Specify **Cloud Access Profile Name** and **Service Account Key**.

   The NetScaler Console uses the Cloud Access Profile to access a Google Cloud account.

2. Specify the following details to prepare the Google Cloud environment:

   a) In **Application Environment Details**, specify a name for your deployment. And, ensure that the correct Cloud Access Profile is selected.

   b) In **Data Center Details**, select **Google Cloud Region** where you want to deploy NetScaler instances.

   c) In **NetScaler AutoScale Group Details**, specify the following to Autoscale NetScaler instances in Google Cloud:

      - **VPC Network's Subnet CIDR** - Specify a VPC network created for management, client, and server traffic. However, you can select the existing network for server.
      - **Zones** - Select the zones in which you want to create the Autoscale groups.

        You can select multiple zones from the list.
      - **Deployment Type** - Select either **Evaluation** or **Production** option.

        If you want to evaluate the NetScaler Console Autoscale solution before purchasing the production license, select the **Evaluation** option.

        > **Important**
        >
        > - The evaluation option supports only one availability zone.
        > - With the evaluation option, you can select only NetScaler VPX Express. And, the NetScaler Console Autoscale solution can scale up to three NetScaler in-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> stances.

- **NetScaler VPX product** - Select licenses to provision NetScaler instances.
- **Machine type** - Select the required instance type.

d) Click **Next**.

After successful validation, click **Create** to deploy NetScaler instances in Google Cloud and create an Autoscale group.

3. After the successful NetScaler deployment, click **Deploy Application**.

In **Configure Application**, specify the necessary details and click **Submit**.

For more information, see Configure an application for the Autoscale group.

Select custom deployment

This option provides a multi-stage deployment. Select this option to discover NetScaler instances from various environments. With this option, you can also deploy new instances by specifying custom environment options.

Perform the following steps to deploy or discover NetScaler instances:

1. Select any of the following environments:

   - **AWS**
   - **Microsoft Azure**
   - **Google Cloud Platform**
   - **On-premises**

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.

   - **On-premises** - If you select **On-premises**, you can install an agent on the following hypervisors:
     - Citrix Hypervisor
     - VMware ESXi
     - Microsoft Hyper-V
     - Linux KVM Server

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Public clouds** - If you select **AWS**, **Microsoft Azure**, or **Google Cloud Platform**, you can externally install an agent on the selected cloud.

  The following is an example image for the AWS environment.

- **As a microservice** - To deploy an agent as a Kubernetes application.
- **Built-in agent** - To discover built-in agents available with NetScaler version 12.0 or later.

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.

> **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Install an agent on a 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.

   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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

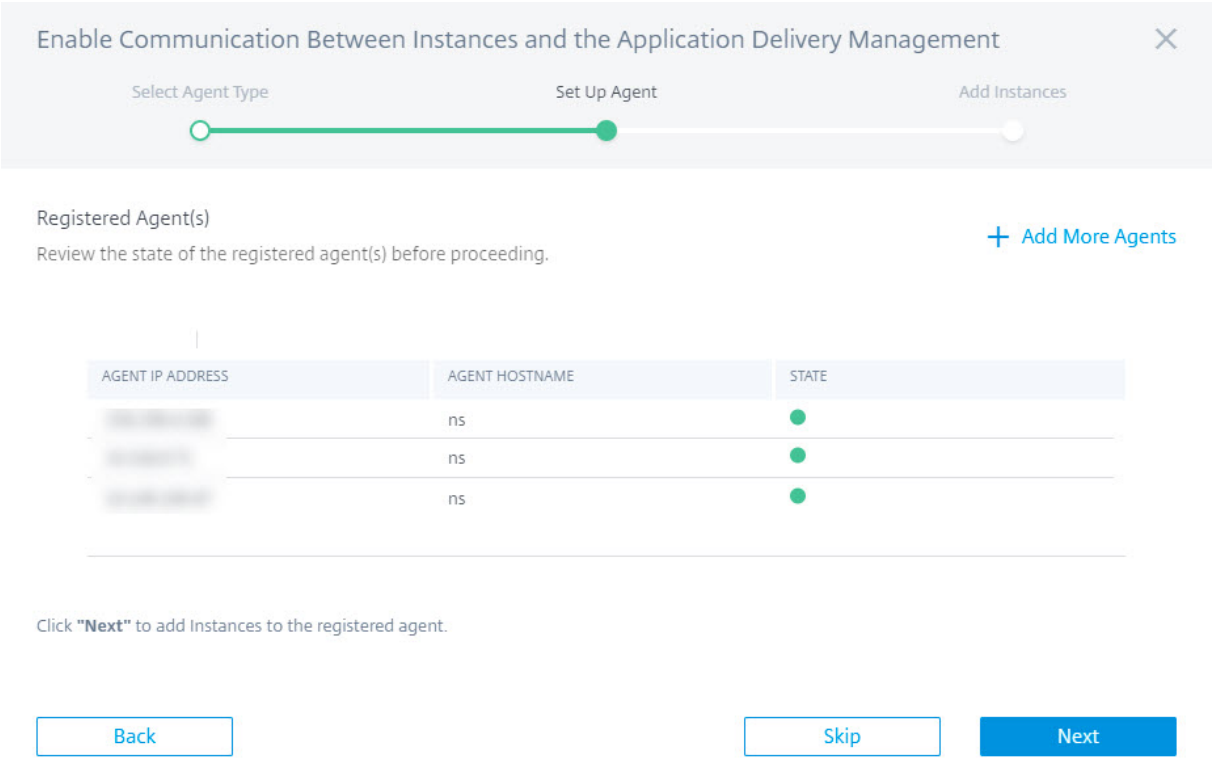
2. After the built-in agent is initiated, return to the **Set Up Agent** page and click **Register Instance**.

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.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

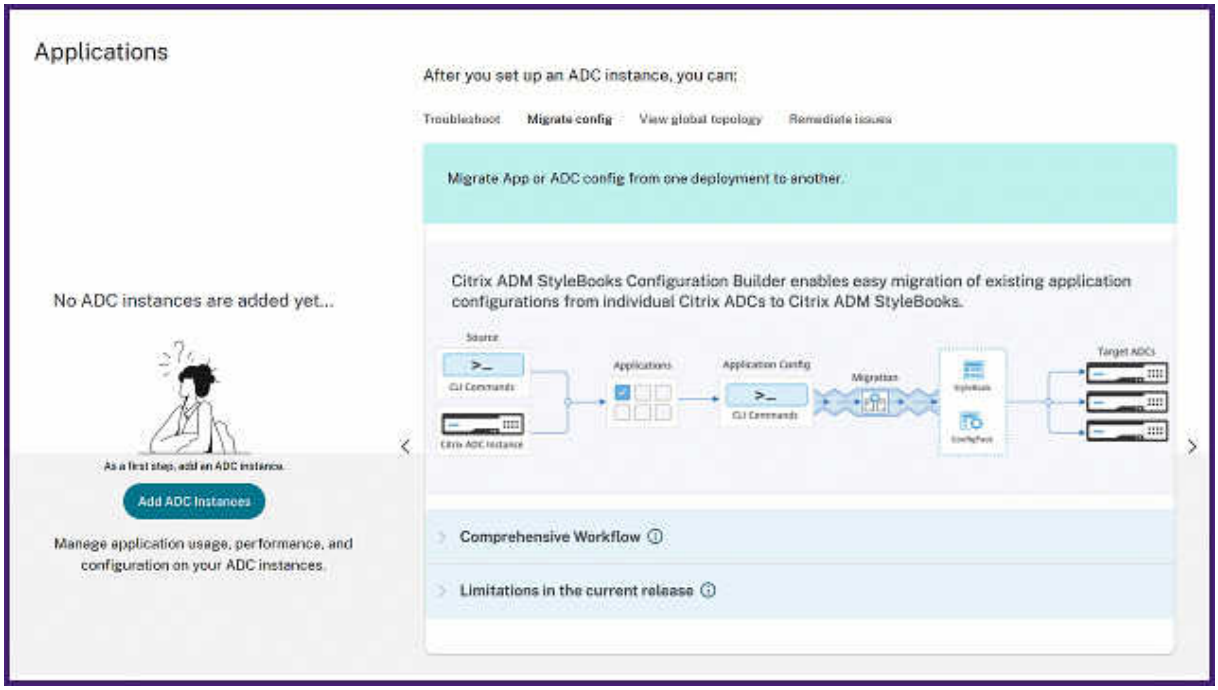
1. In the **Add Instances** page, view the NetScaler instances that are connected to the registered agent. Ensure that the instance is in the **Up** status and click **Next**.
2. Click **Done** to complete your initial setup and start managing your deployment.

> **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.



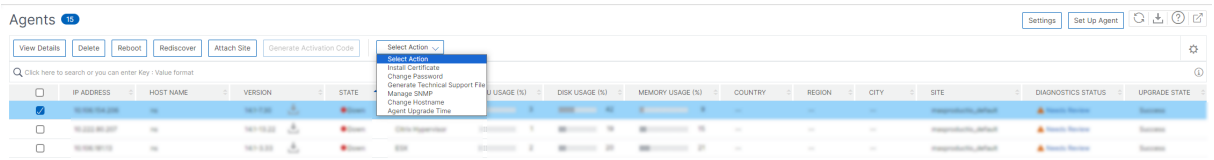
Click **Add NetScaler instances** to onboard the instances. The **Get Started** workflow restarts. Follow the steps from Step 3: Select an NetScaler deployment type onwards, given in this document, to onboard the instances.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:

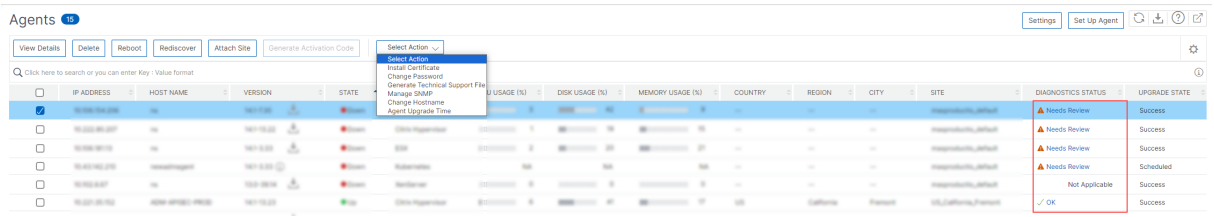
- **Install a new certificate**: if you need a different agent certificate to meet your security requirement, you can add one.
- **Change the agent password**: to ensure security of your infrastructure, change the default password of an agent.
- **Generate a technical support file**: generate a technical support file for a selected agent. You can download this file and send it to Citrix technical support for investigation and troubleshooting.

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:

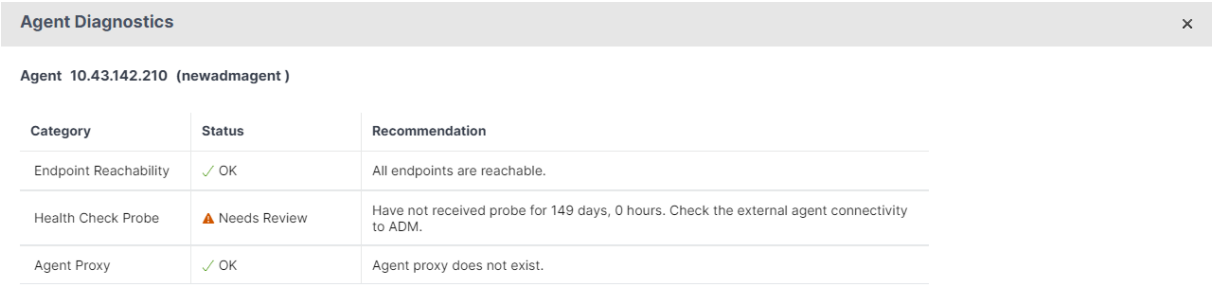
- **Endpoint reachability** –Checks if all endpoints are reachable. The agent uses various endpoints for the communication between NetScaler Console and NetScaler instances. For more information, see Software Requirements.
- **Health check probe** –Provides the time stamp of the latest health check.
- **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**.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Click to view the diagnostic information of an agent.

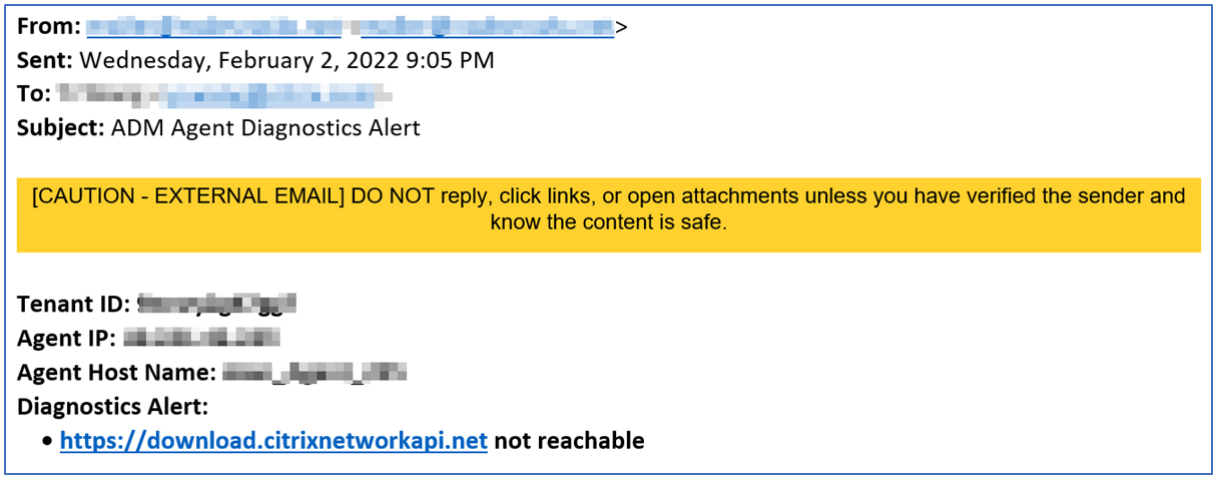


- **Category**. Provides the issue category.
- **Status**. Provides the issue status such as **Needs Review** or **OK**.
- **Recommendation**. Provides the required recommendation to troubleshoot the issue.

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.

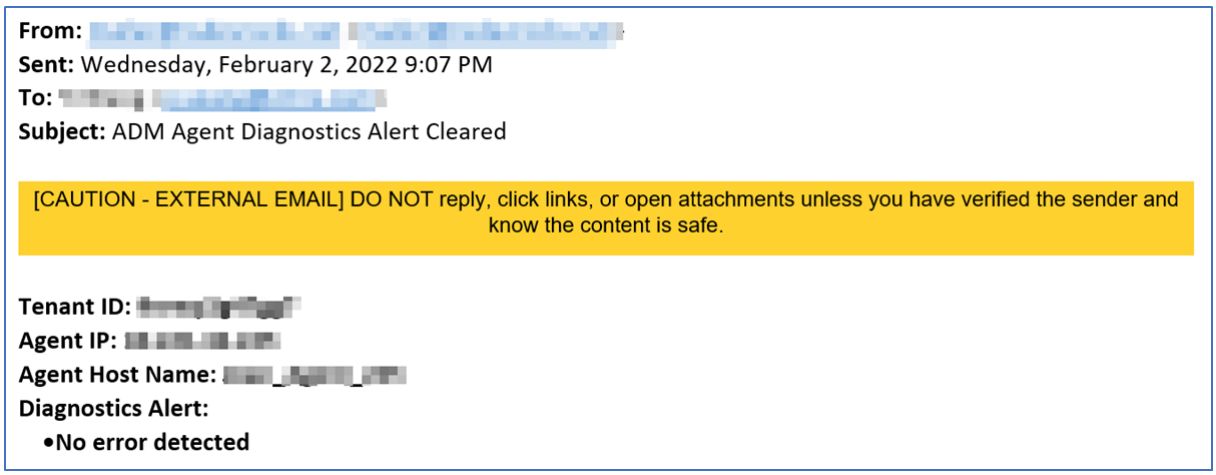
Email notification

The following example is an email notification after the endpoint reachability status has changed from **OK** to **Needs Review**:



The following example is an email notification after the endpoint reachability status has changed from **Needs Review** to **OK**:

© 1997–2025 Citrix Systems, Inc. All rights reserved.


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

May 26, 2025

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.

> **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 supports management and monitoring of NetScaler instances using built-in agents. However, the following features are not supported in the built-in agent:

- Application dashboard
- Web Insight

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- SSL insight
- HDX insight
- Gateway insight
- Security insight
- Advanced analytics
- Pooled/Flexed 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.
- 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

		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 same access privileges as nsroot.	Enter `nsroot` in <user_name>. Alternatively, you can use a user name that has the 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.

© 1997–2025 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	Yes	./mastools_init.sh <device_profile_name> <service_url> "MAS;<activation_code>"-profile	./mastools_init.sh <user_name><pwd> <service_url> "MAS;<activation_code>"
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:

© 1997–2025 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:
  - **Mastools_upgrade** logs in `/var/mastools/logs/mastools_upgrade.log`
  - **Binary logs** in `/var/log/mastoolsd.log`.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Install a NetScaler agent on-premises

September 8, 2025

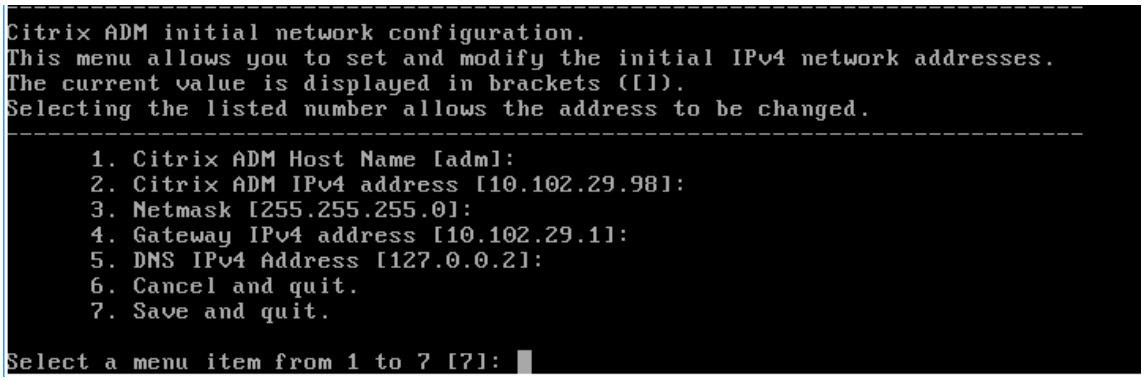
The agent works as an intermediary between the NetScaler Console and the discovered instances in the data center.

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.

   If you want to change the configured network settings on the agent, type the `networkconfig` command and follow the prompts in the CLI.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
bash-3.2#
bash-3.2# networkconfig

------------------------------------------------------------------------------
Citrix ADM Agent initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
------------------------------------------------------------------------------
      1. Citrix ADM Agent Host Name [ns]:
      2. Citrix ADM Agent IPv4 address [10.106.100.143]:
      3. Netmask [255.255.255.0]:
      4. Gateway IPv4 address [10.106.100.1]:
      5. DNS IPv4 Address [10.140.50.5]:
      6. Cancel and quit.
      7. Save and quit.

Select a menu item from 1 to 7 [7]:
```

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:

```
1 deployment_type.py
```

```
1 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.

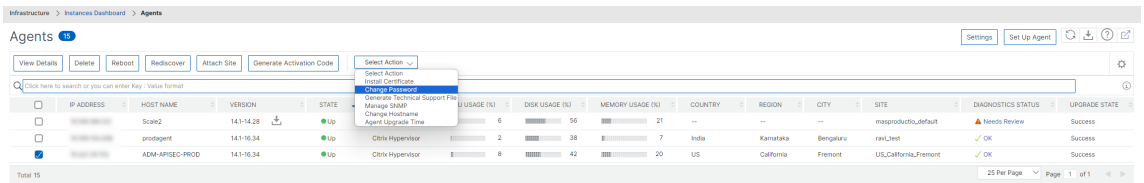
```
Citrix ADM Agent Registration with Citrix ADM Service. This menu allows you to s
pecify a cloud url and obtain an instance ID for your device.
------------------------------------------------------------------------------

   Enter Service URL:
   Enter Activation Code :
```

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**.



© 1997–2025 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

September 8, 2025

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.

Prerequisites

Make sure that you have the following:

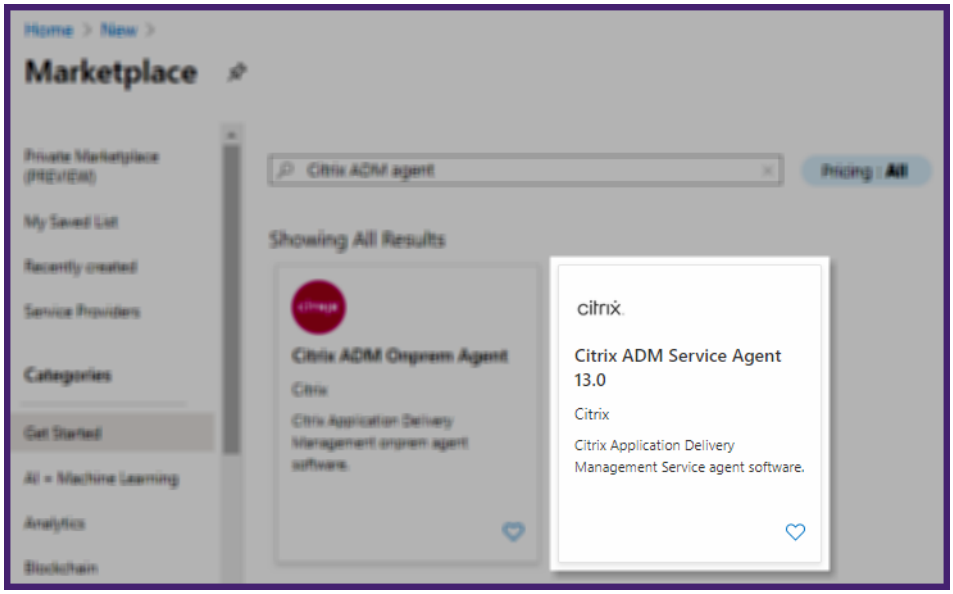
- A Microsoft Azure user account
- Access to Microsoft Azure Resource Manager

© 1997–2025 Citrix Systems, Inc. All rights reserved.

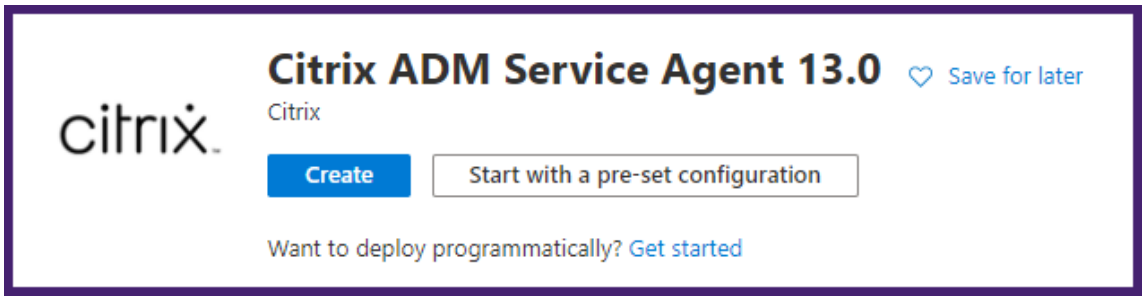
> **Note**
>
> - We recommend that you create resource group, network security group, virtual network, and other entities before you provision the NetScaler agent virtual machine, so that the network information is available during provisioning.
> - For the NetScaler agent to communicate with NetScaler 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**.



4. Click **Create**.



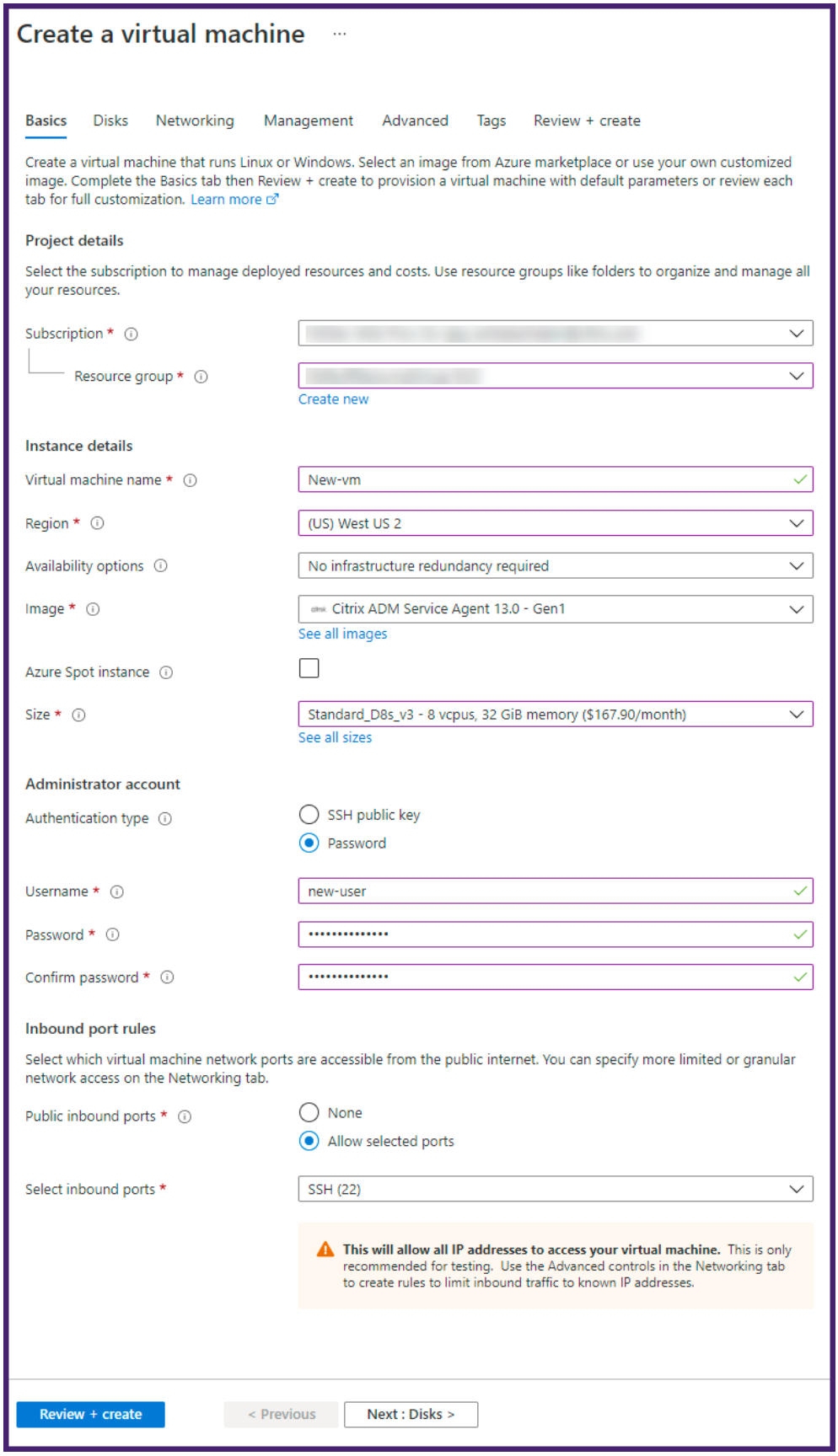
5. In the **Create virtual machine** pane, specify the required values in each section to create a virtual machine.

   Basics:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

In this tab, specify **Project details**, **Instance details**, and **Administrator account**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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.

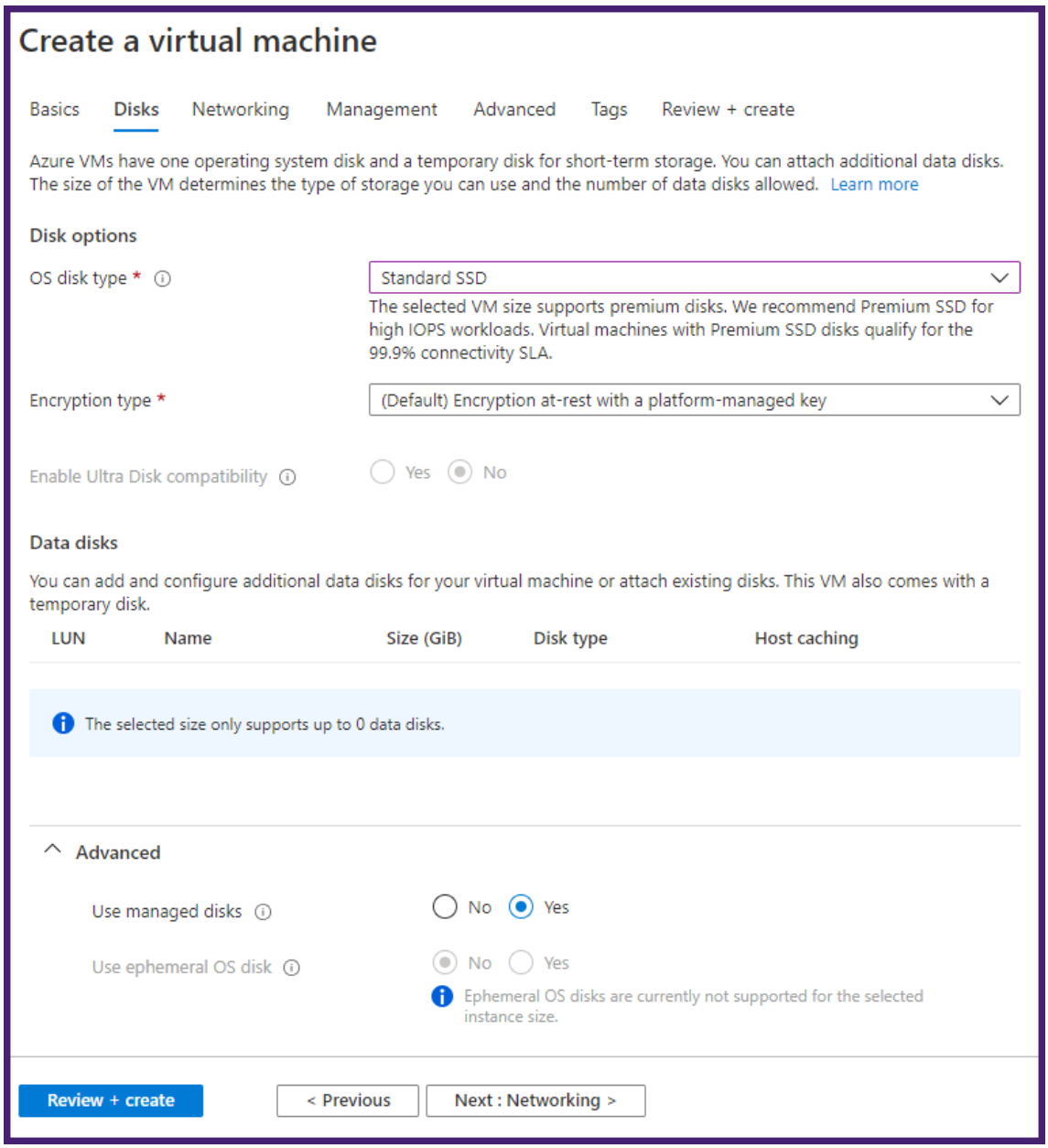
- **Authentication Type** –Select Password.
- **User name and Password** –Specify a user name and password to access the resources in the resource group that you have created.

  > **Important**
  >
  > We recommend you specify your own user name and password for your agent. Do not use `nsrecover` or `nsroot` as the user name because they are reserved for agent users.

Disks:

In this tab, specify **Disk options** and **Data disks**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

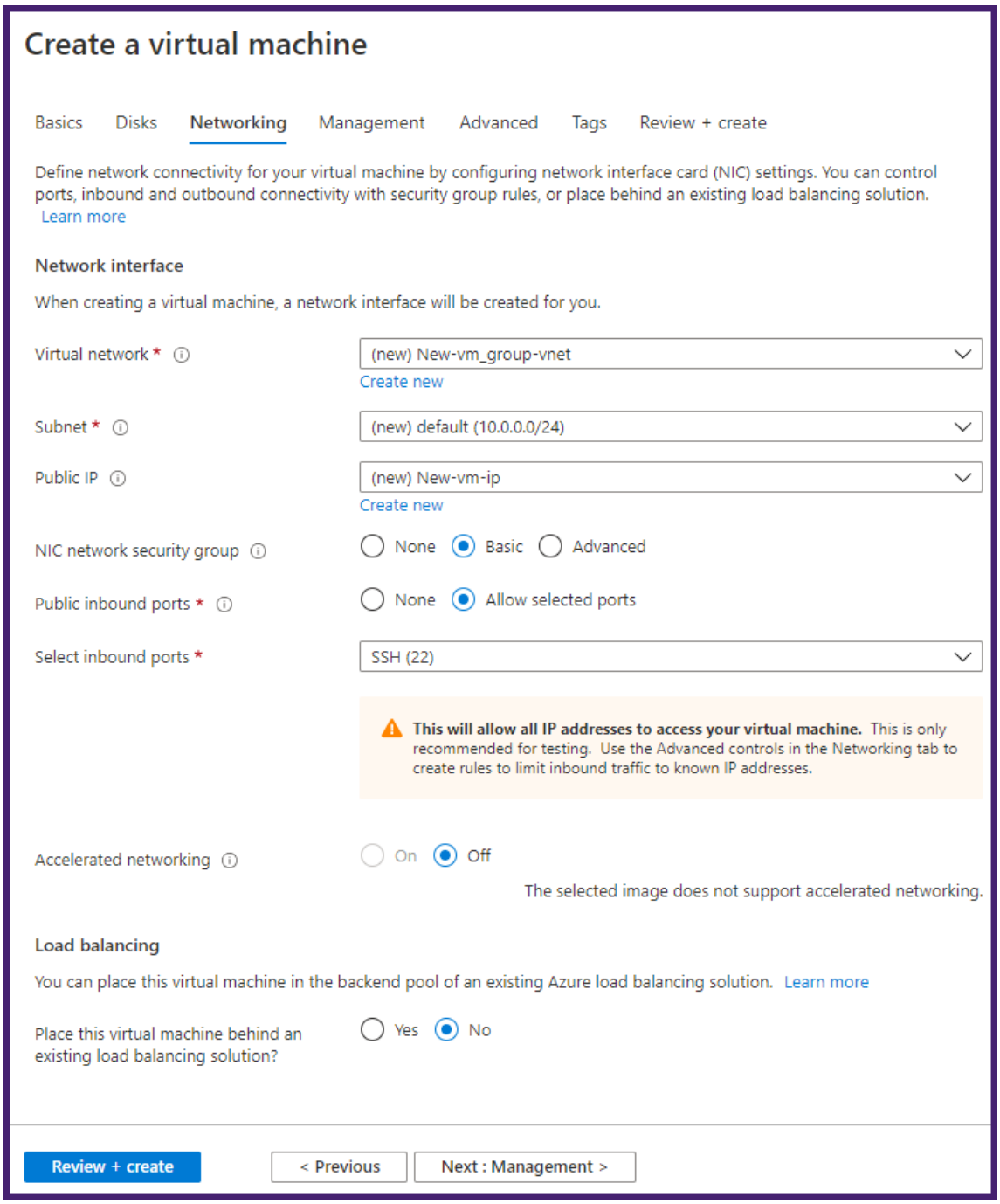


- **OS disk type** - Select the virtual disk type (HDD or SSD).

Networking:

Specify the required networking details:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



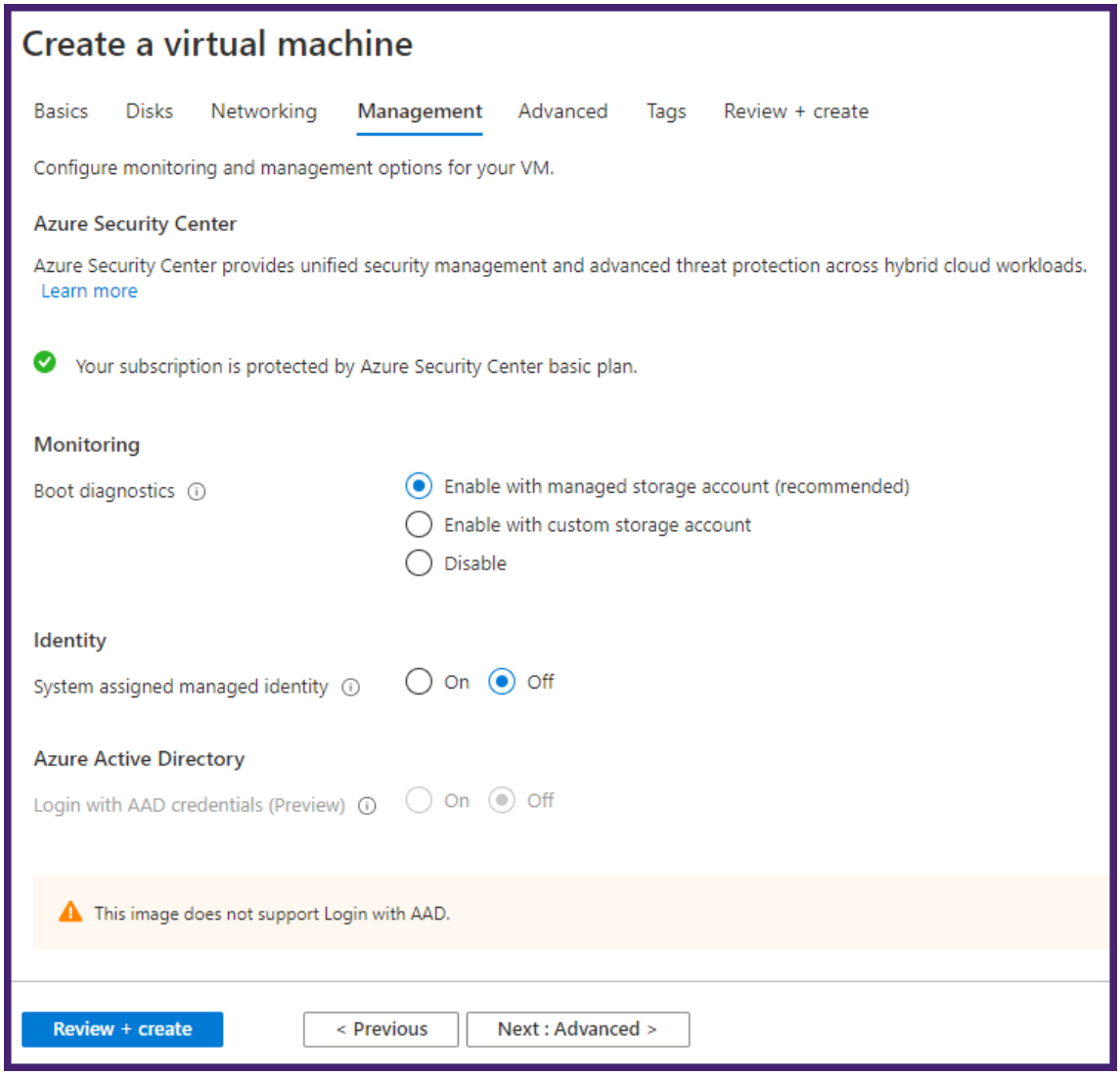
- **Virtual network** –Select the virtual network.
- **Subnet** –Set the subnet address.
- **Public IP address** - Optional, select the IP address.
- **Network security group** –Optional, select the security group that you have created.
- **Select inbound ports** - If you allow public inbound ports, 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Note**
>
> Ensure that agent has Internet access.

Management:

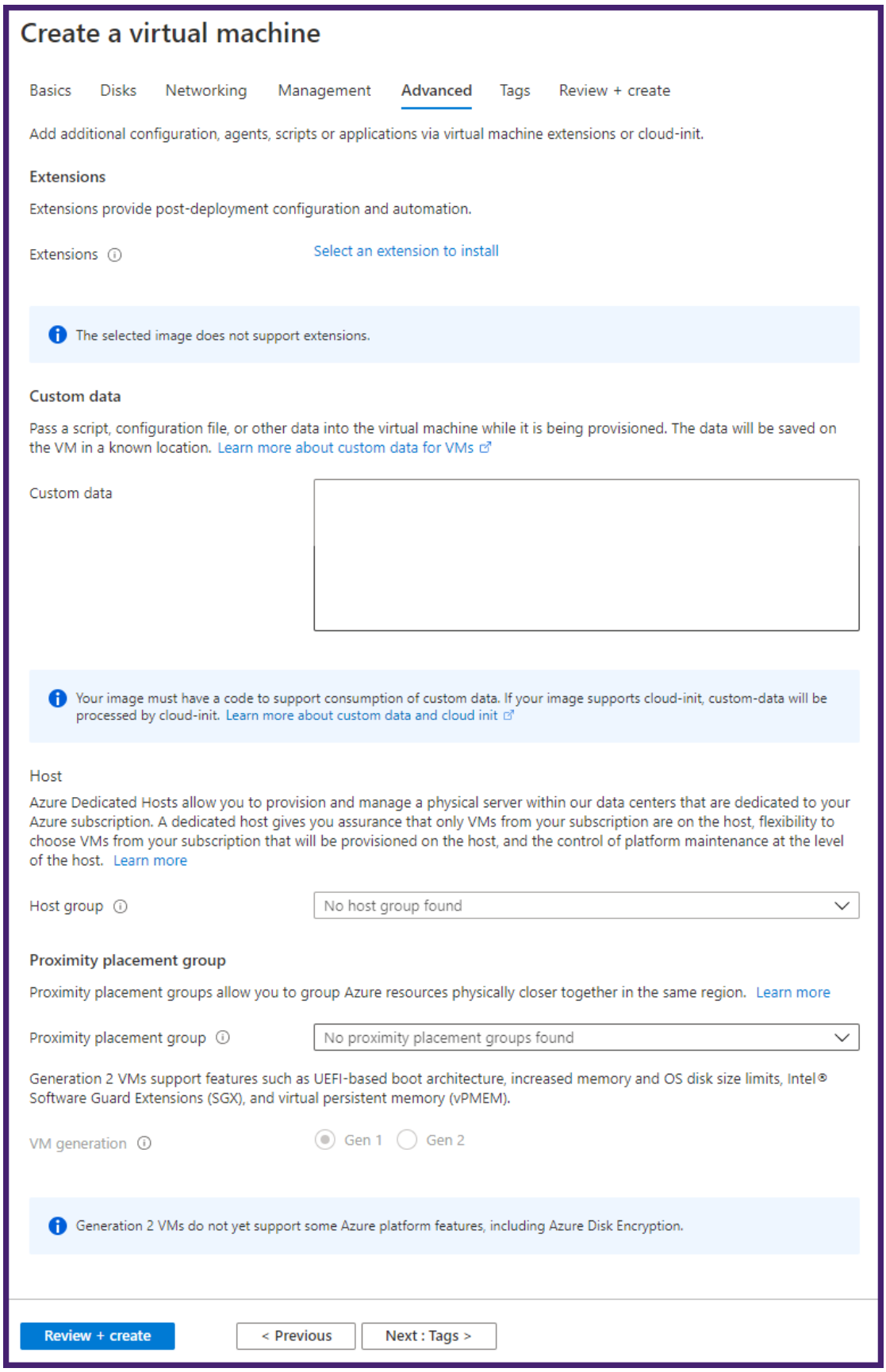
Specify **Azure Security Center**, **Monitoring**, and **Identity**.



Advanced:

Optional, specify **Extensions**, **Custom Data**, and **Proximity placement group**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



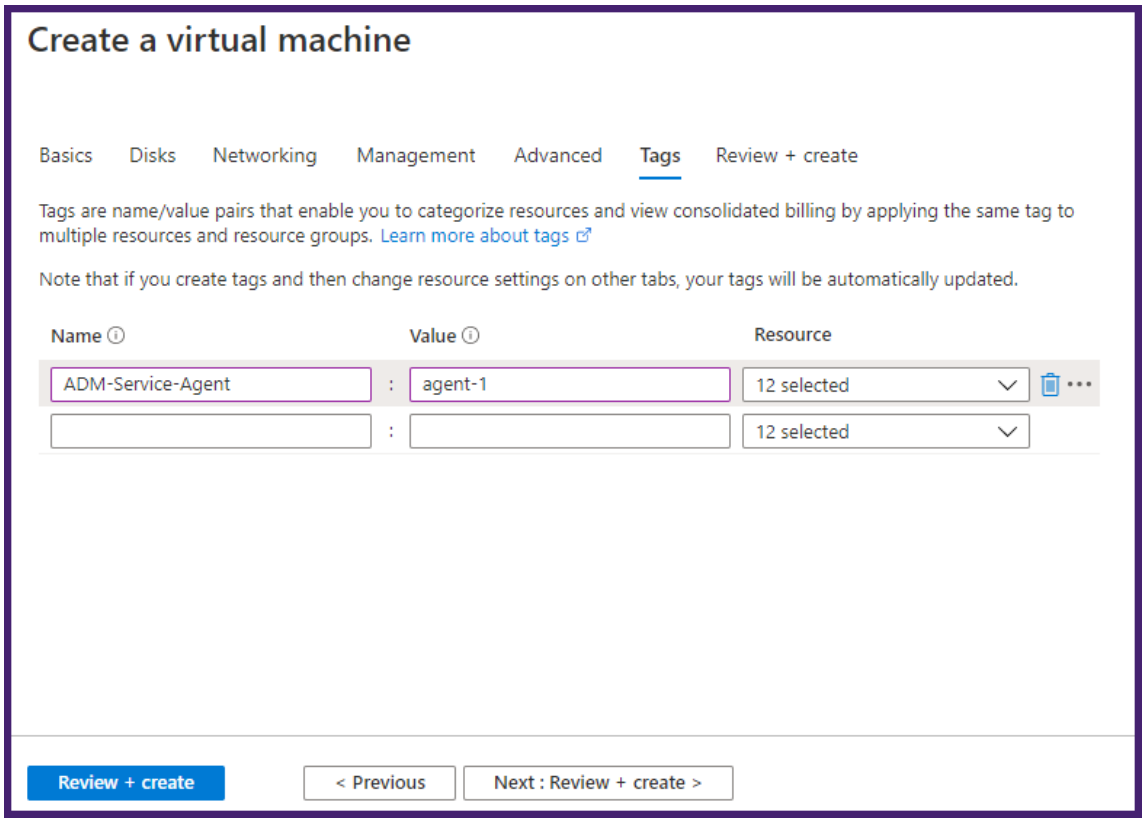
© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **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 <apigatewayurl> -activationcode <
>    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.

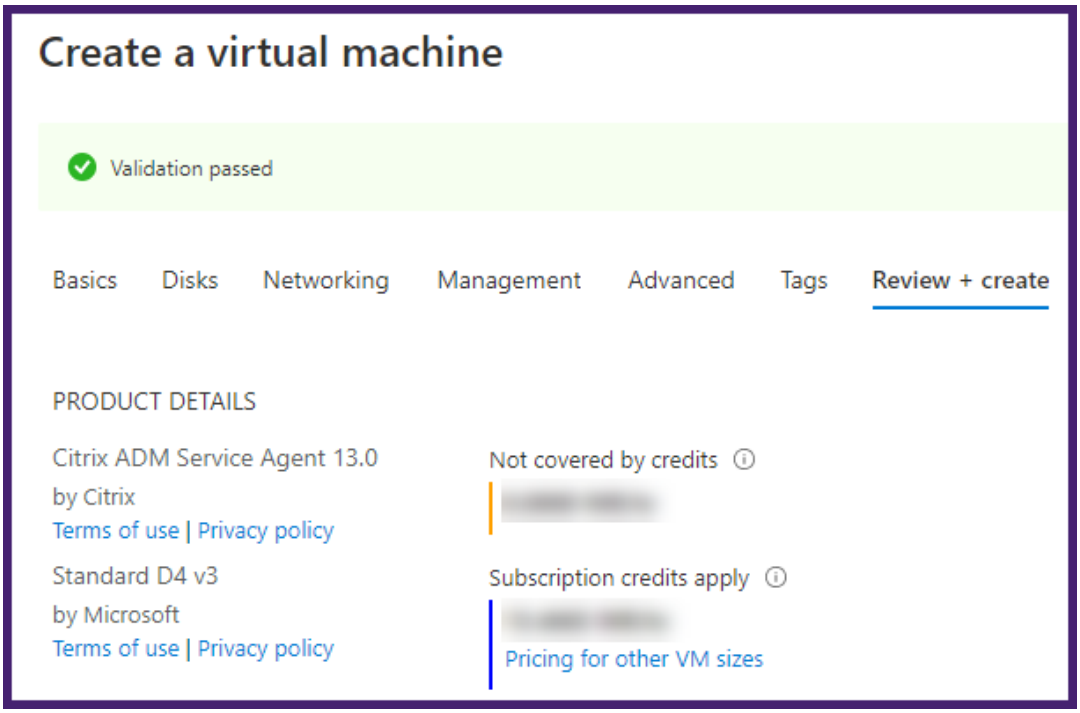


The configuration settings are validated and the **Review and create** tab displays the result of the validation.

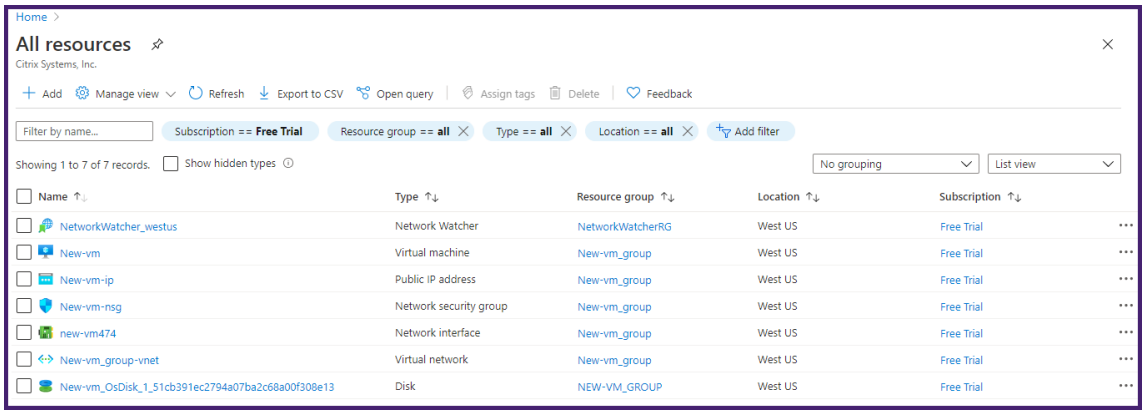
- If the validation fails, this tab displays the reason for the failure. Go back to the particular section and make changes as required.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- If the validation passes, click **Create**. The agent deployment process begins.

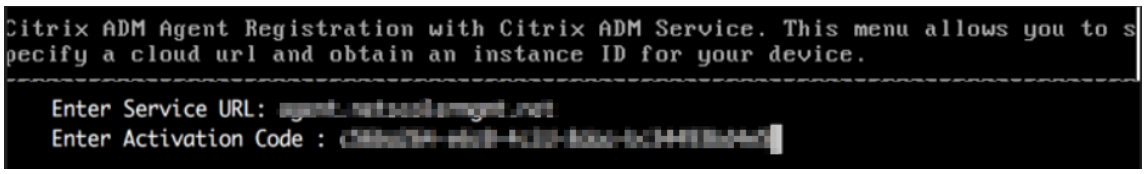


The deployment process might take approximately 10–15 minutes. Once the deployment is successfully completed, you can view your NetScaler agent virtual machine in your Microsoft Azure account.



6. Once the agent is up and running, use an SSH client to log on to your NetScaler agent. Use the user name 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**.
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.

© 1997–2025 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 a NetScaler agent on Amazon Web Services (AWS)

September 4, 2024

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:

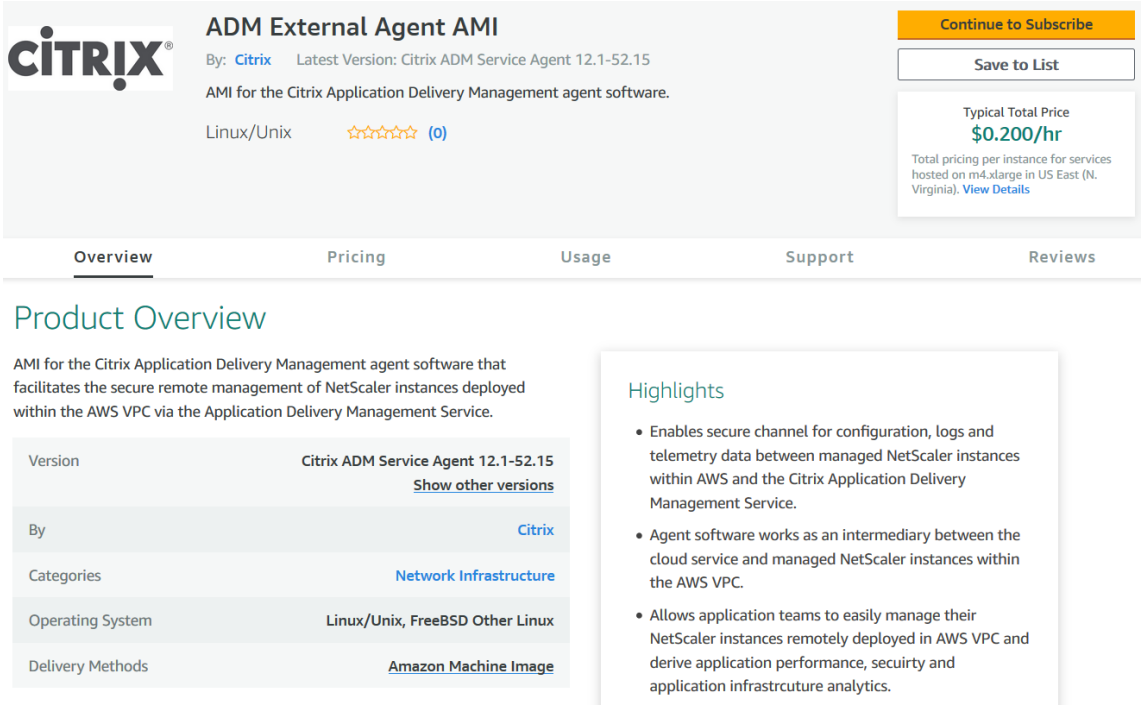
- An AWS account
- An AWS virtual private cloud (VPC)
- An IAM account
- A Service URL and Activation code for the agent to connect to NetScaler Console service. In NetScaler Console service GUI, navigate to **Infrastructure > Instances > Agents** and click **Generate Activation Code** to generate your Service URL and Activation code.

> **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.

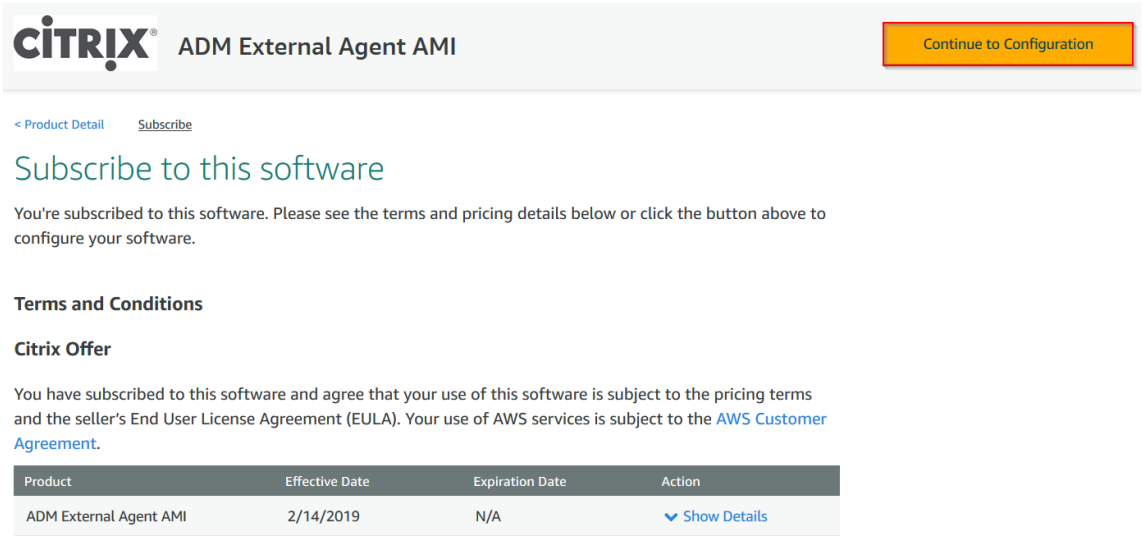
To install the NetScaler agent on AWS:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.



6. On the **Configure this software** page:

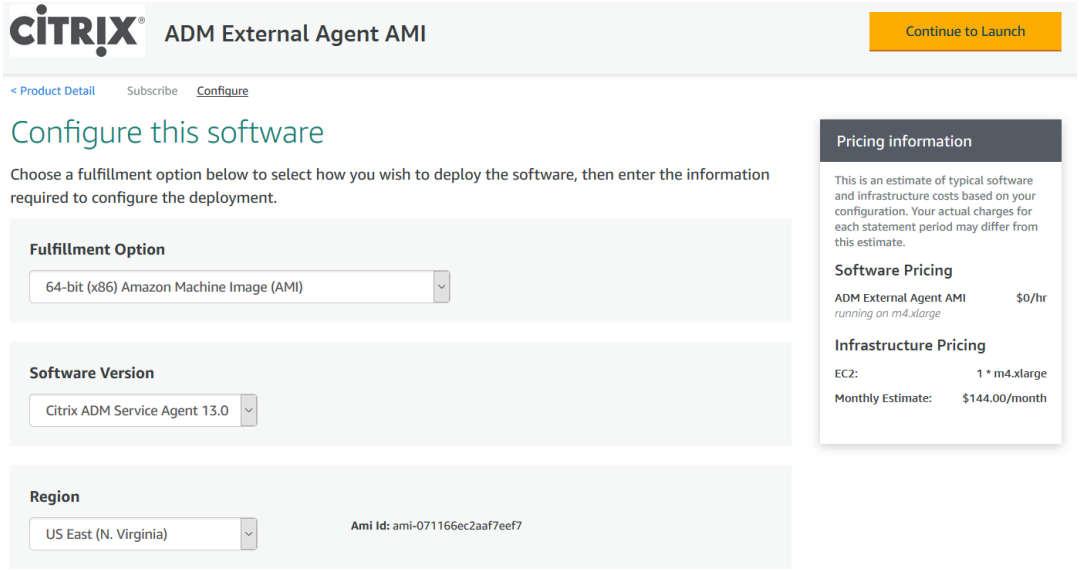
   a) Select the AMI from the **Fulfillment option** list.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**

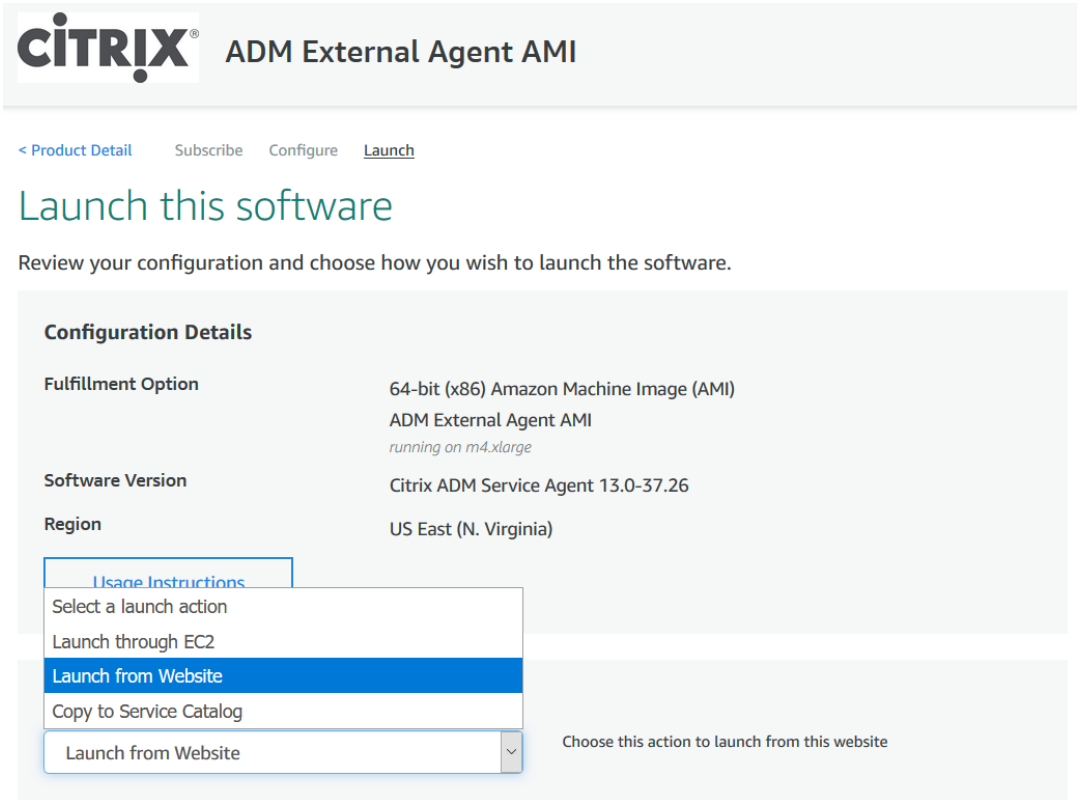


7. On the **Launch this software** page, you have two options to register the NetScaler agent:

a) **Launch from Website**

b) **Launch with EC2**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

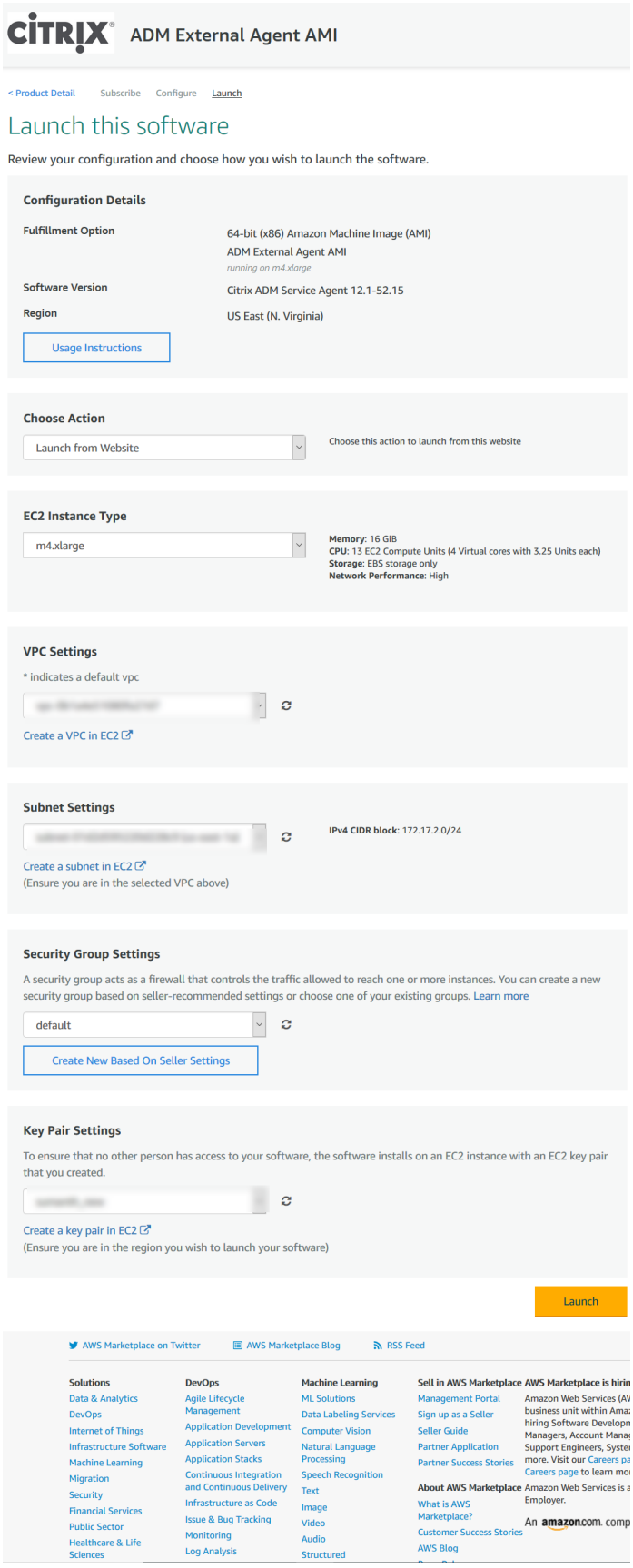


Launch from a Website

To launch from a Website, select:

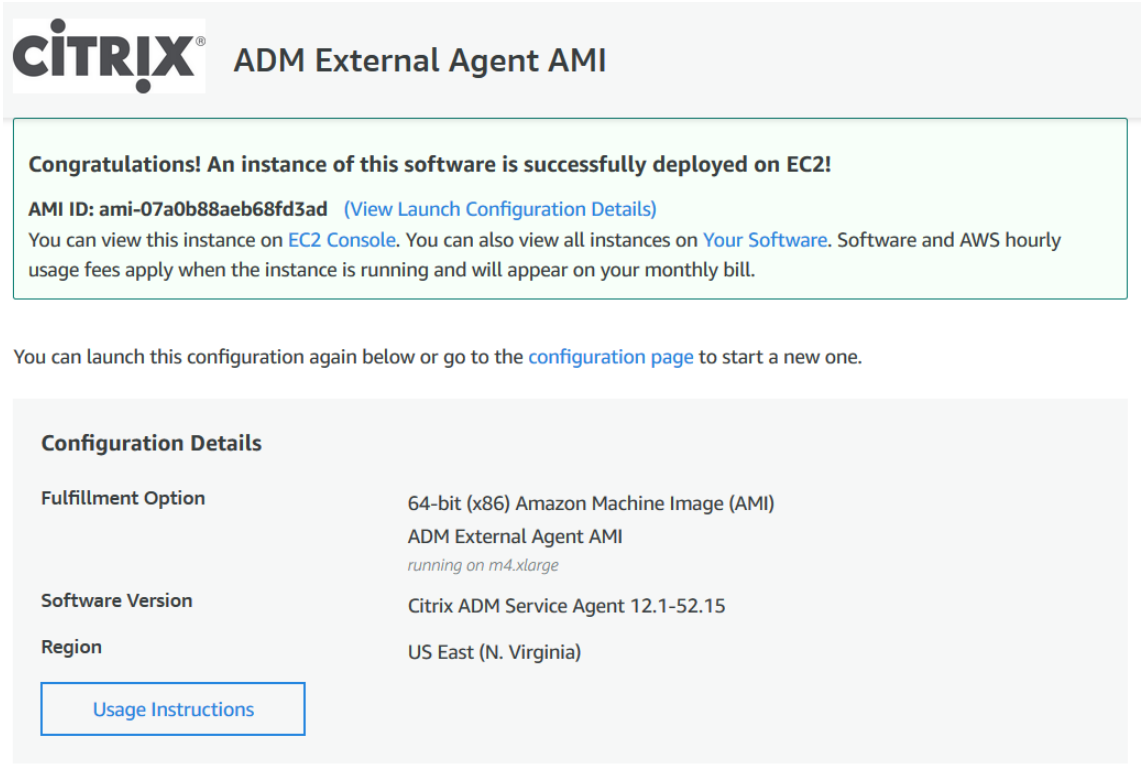
1. An EC2 instance type from the **EC2 Instance Type** list
2. A VPC from the **VPC Settings** list. Click **Create a VPC in EC2** to create a VPC for your software.
3. A Subnet from the **Subnet Settings** list. Click **Create a subnet in EC2** to create a subnet after you selected the VPC.
4. A security 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**

© 1997–2025 Citrix Systems, Inc. All rights reserved.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

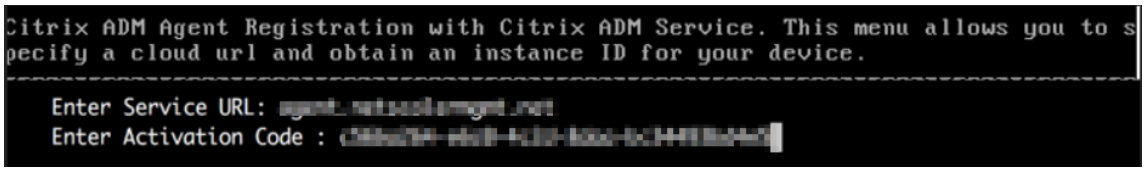
> **Note**
>
> Elastic IP address enables NetScaler agent to communicate with NetScaler Console. But, an elastic IP address might not be required if you have configured NAT Gateway to route the traffic to the Internet.

10. Using an SSH client, log on to your NetScaler agent.

> **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.



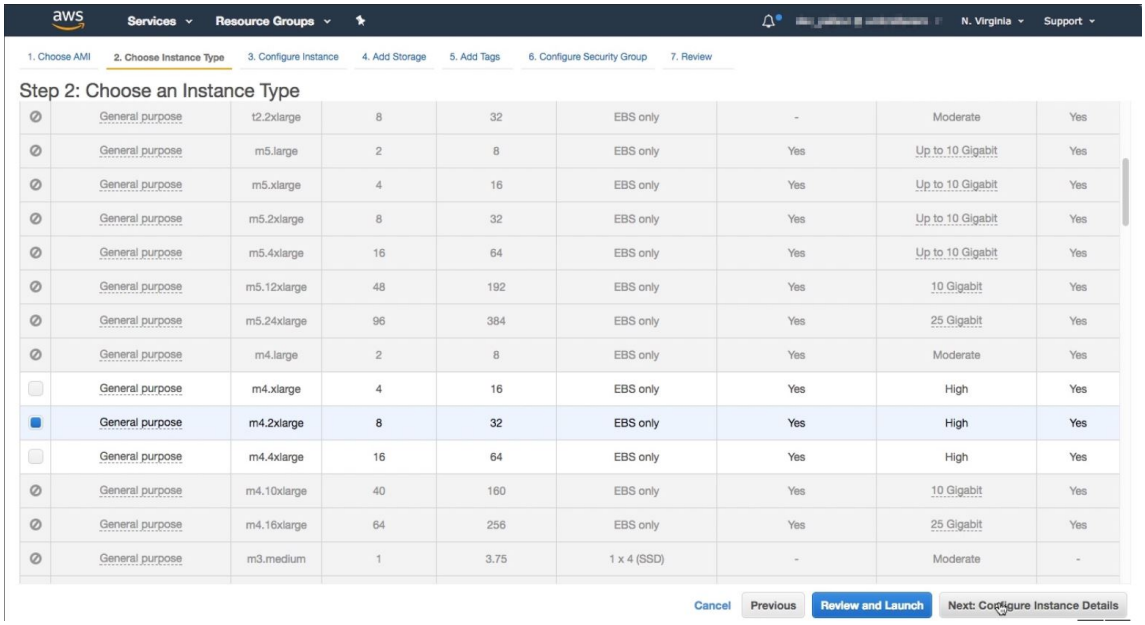
After agent registration is successful, the agent restarts to complete the installation process.

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**.



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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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
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
{
 "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"
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
31
32  '''
33  Set up a specific logger with your desired output level and
        log file name
34  '''
35  log_file_name_local = os.path.basename(__file__)
36  LOG_FILENAME = '/var/log/' + 'bootstrap' + '.log'
37  LOG_MAX_BYTE = 50*1024*1024
38  LOG_BACKUP_COUNT = 20
39
40  logger = logging.getLogger(__name__)
41  logger.setLevel(logging.DEBUG)
42  logger_handler = logging.handlers.RotatingFileHandler(
        LOG_FILENAME, maxBytes=LOG_MAX_BYTE, backupCount=
        LOG_BACKUP_COUNT)
43  logger_fortmater = logging.Formatter(fmt='%(asctime)-2s:%(
        funcName)30s:%(lineno)4d: [%(levelname)s] %(message)s',
        datefmt="%Y-%m-%d %H:%M:%S")
44  logger_handler.setFormatter(logger_fortmater)
45  logger.addHandler(logger_handler)
46
47  class APIHandlerException(Exception):
48      def __init__(self, error_code, message):
49          self.error_code = error_code
50          self.message = message
51
52      def __str__(self):
53          return self.message + ". Error code '" + str(self.
                error_code) + "'"
54
55  def parse_response(response, url, print_response=True):
56      if not response.ok:
57          if "reboot" in url:
58              logger.debug('No response for url: reboot')
59              resp = {
60  "errorcode": "500", "message": "Error while reading response.
        " }
61
62              return resp
63
64          if print_response:
65              logger.debug('Response text for %s is %s' % (url,
                    response.text))
66
67          response = json.loads(response.text)
68          logger.debug("ErrorCode - " + str(response['errorcode
                '']) + ". Message -" + str(response['message']))
69          raise APIHandlerException(response['errorcode'], str(
                response['message']))
70      elif response.text:
71          if print_response:
72              logger.debug('Response text for %s is %s' % (url,
                    response.text))
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
73
74          result = json.loads(response.text)
75          if 'errorcode' in result and result['errorcode'] > 0:
76              raise APIHandlerException(result['errorcode'],
                    str(result['message']))
77          return result
78
79  def _request(method, url, data=None, headers=None, retry=3,
        print_response=True):
80      try:
81          response = requests.request(method, url, data=data,
                headers=headers)
82          result = parse_response(response, url, print_response
                =print_response)
83          return result
84      except [requests.exceptions.ConnectionError, requests.
            exceptions.ConnectTimeout]:
85          if retry > 0:
86              return _request(method, url, data, headers, retry
                    -1, print_response=print_response)
87          else:
88              raise APIHandlerException(503, 'ConnectionError')
89      except requests.exceptions.RequestException as e:
90          logger.debug(str(e))
91          raise APIHandlerException(500, str(e))
92      except APIHandlerException as e:
93          logger.debug("URL: %s, Error: %s, Message: %s" % (url
                , e.error_code, e.message))
94          raise e
95      except Exception as e:
96          raise APIHandlerException(500, str(e))
97
98  try:
99      '''Get the AWS Region'''
100     client = boto3.client('s3')
101     my_region = client.meta.region_name
102     logger.debug("The rgion is %s" % (my_region))
103
104     '''Creating a Boto cleint session'''
105     session = boto3.session.Session()
106     client = session.client(
107         service_name='secretsmanager',
108         region_name=my_region
109     )
110
111     '''Getting the values stored in the secret with id: <
            aws_secret_id>'''
112     get_id_value_response = client.get_secret_value(
113         SecretId = aws_secret_id
114     )
115     adm_user_id = json.loads(get_id_value_response["
            SecretString"])["adm_user_id_key"]
116     adm_user_secret = json.loads(get_id_value_response["
```

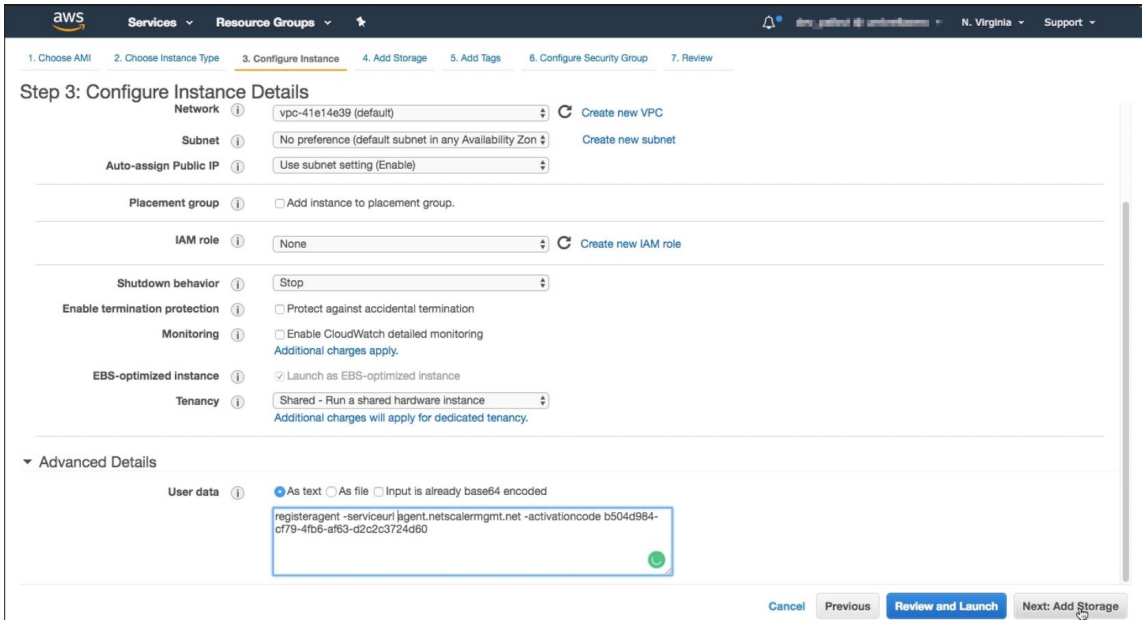
© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
            SecretString"])["adm_user_secret_key"]
117
118     except Exception as e:
119         logger.debug("Fetching of NetScaler Console credentials
               from AWS secret failed with error: %s" % (str(e)))
120         raise e
121
122     '''
123     Initializing common NetScaler Console API handlers
124     '''
125     mas_common_headers = {
126
127         'Content-Type': "application/json",
128         'Accept-type': "application/json",
129         'Connection': "keep-alive",
130         'isCloud': "true"
131      }
132
133
134     '''
135     API to login to the NetScaler Console and fetch the Session
           ID and Tenant ID
136     '''
137     url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/
           config/login"
138     payload = 'object={
139     "login":{
140     "ID":"' + adm_user_id + '","Secret":"' + adm_user_secret + '"
            }
141      }
142     '
143     try:
144         response = _request("POST", url, data=payload, headers=
               mas_common_headers)
145         sessionid = response["login"][0]["sessionid"]
146         tenant_id = response["login"][0]["tenant_name"]
147     except Exception as e:
148         logger.debug("Login call to the NetScaler Console failed
               with error: %s" % (str(e)))
149         raise e
150
151     '''
152     API to fetch the service URL and Token to be used for
           registering the agent with the NetScaler Console
153     '''
154     mas_common_headers['Cookie'] = 'SESSID=' + str(sessionid)
155     url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/
           config/trust_preauthtoken/" + tenant_id +"?customer="+
           tenant_id
156     logger.debug("Fetching Service URL and Token.")
157     try:
158         response = _request("GET", url, data=None, headers=
               mas_common_headers)
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
159         service_name  = response["trust_preauthtoken"][0]["
                service_name"]
160         token = response["trust_preauthtoken"][0]["token"]
161         api_gateway_url = response["trust_preauthtoken"][0]["
                api_gateway_url"]
162     except Exception as e:
163         logger.debug("Fetching of the Service URL Passed with
                error. %s" % (str(e)))
164         raise e
165
166     '''
167     Running the register agent command using the values we
            retrieved earlier
168     '''
169     try:
170         registeragent_command = "registeragent -serviceurl "+
                api_gateway_url+" -activationcode "+service_name+"\;"+
                token
171         file_run_command = "/var/python/bin/python2.7 /mps/
                register_agent_cloud.py "+registeragent_command
172         logger.debug("Executing registeragent command: %s" % (
                file_run_command))
173         os.system(file_run_command)
174     except Exception as e:
175         logger.debug("Agent Registeration failed with error: %s"
                % (str(e)))
176          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.

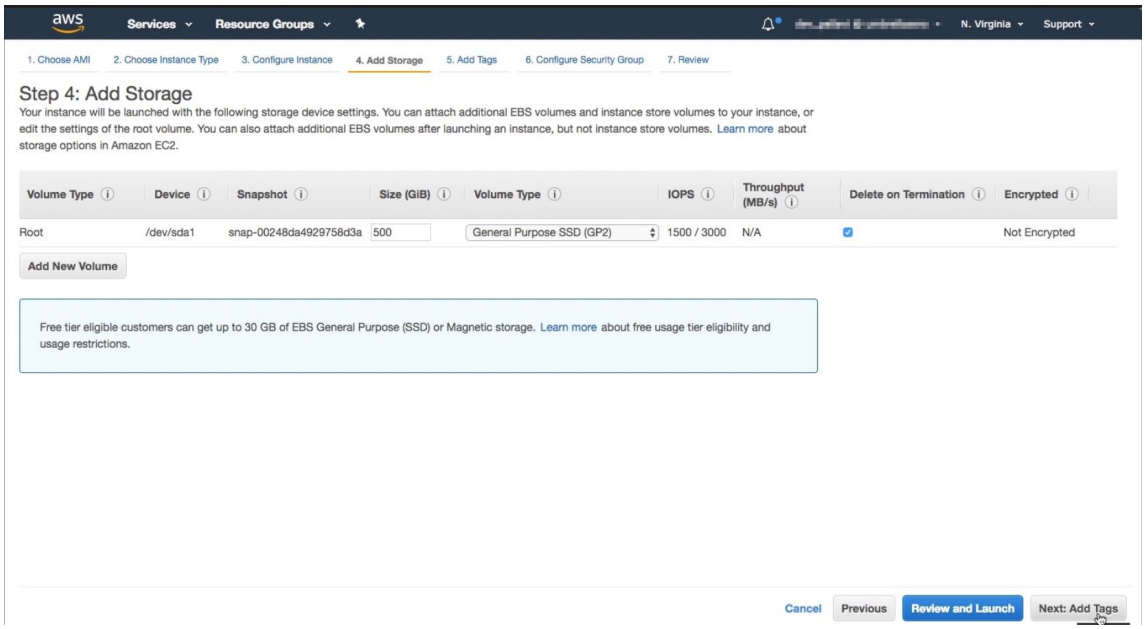


© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **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.

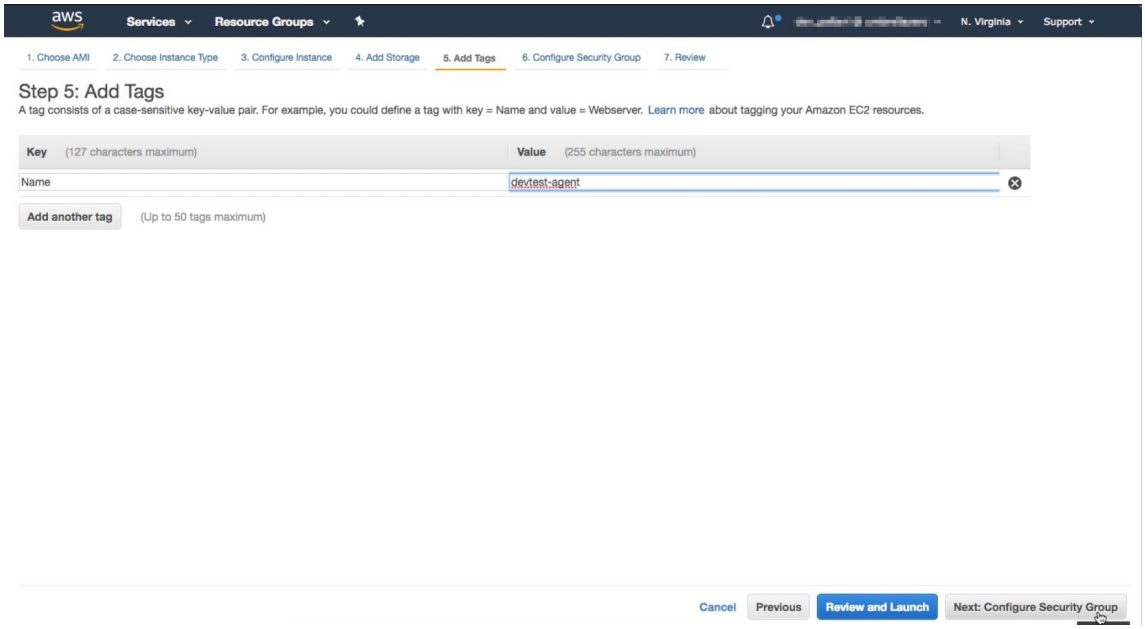
Click **Add Storage**.

3. On the **Add Storage** page, configure the storage device settings for the instance, and click **Next: Add Tags**.

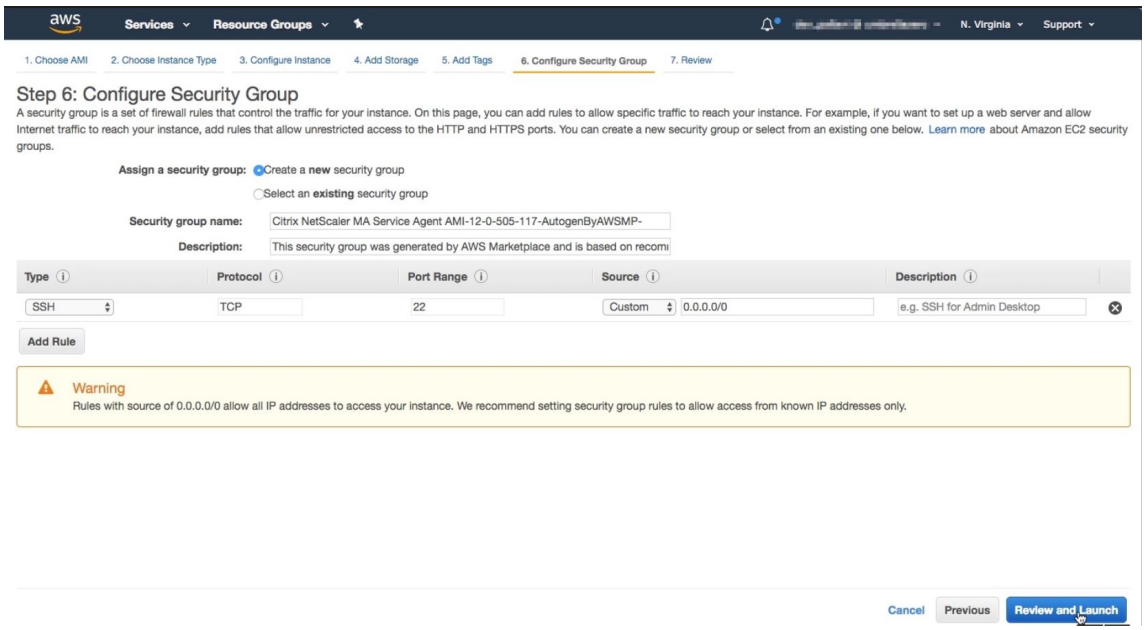


4. On the **Add Tags** page, define the tag for the instance, and click **Next: Configure Security Group**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



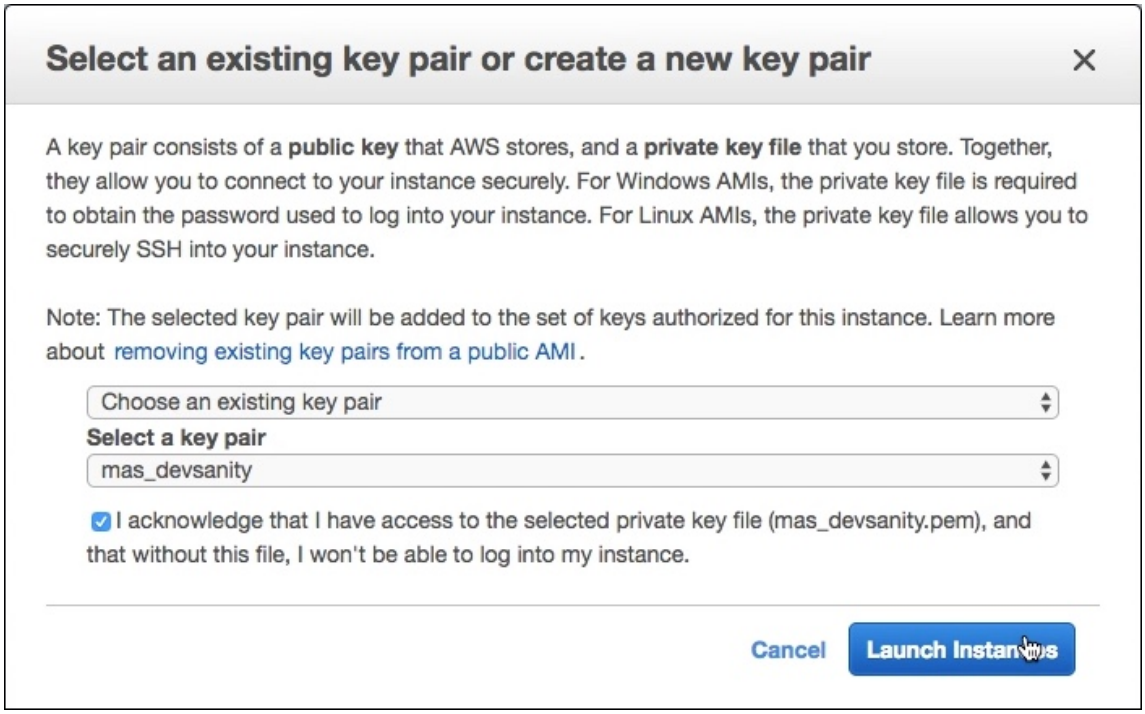
5. On the **Configure Security Group** page, add rules to allow specific traffic to your instance and click **Review and Launch**.



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**.

© 1997–2025 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

January 8, 2024

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

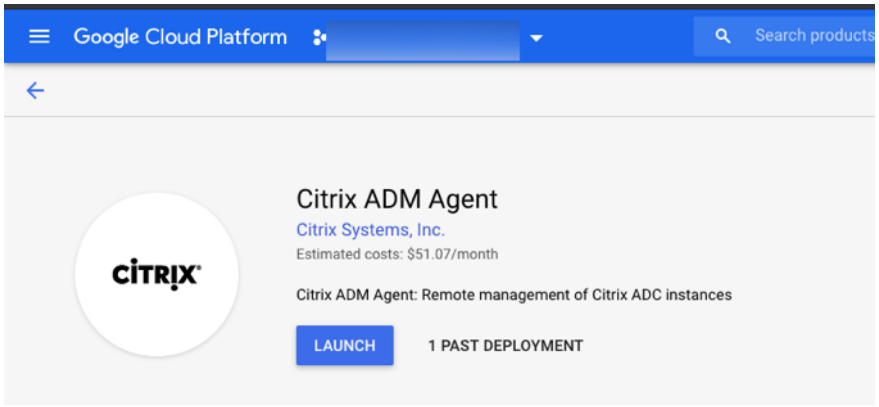
To install a NetScaler agent on GCP, you need a GCP account.

Install the NetScaler agent on GCP

Follow these steps to install a NetScaler agent on GCP.

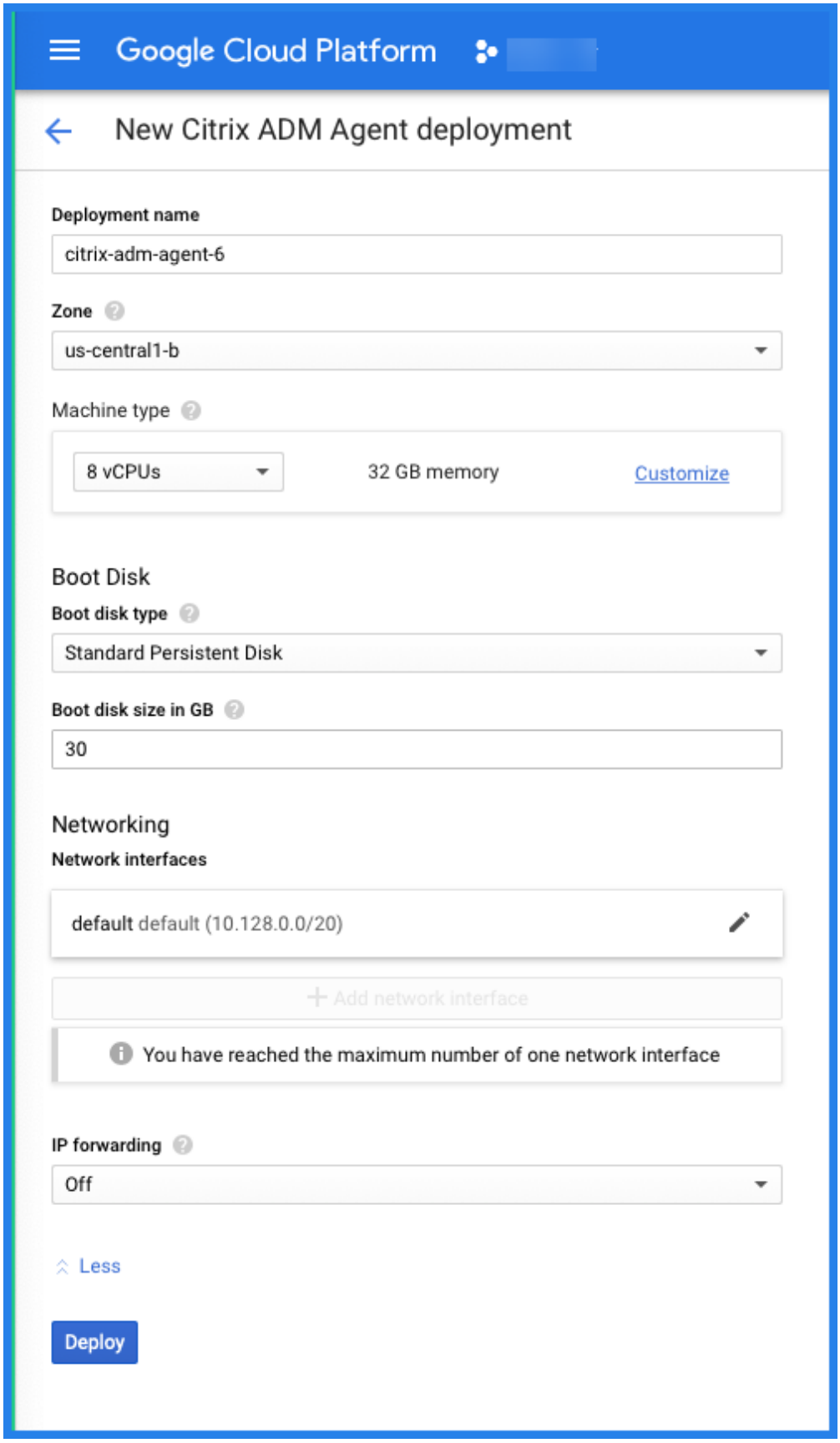
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.



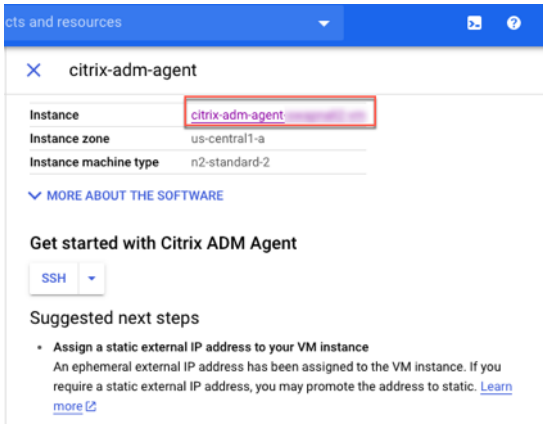
4. In the **New NetScaler agent deployment** page, most of the options are set by default. You can change the default configurations as required and click **Deploy**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



© 1997–2025 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**.

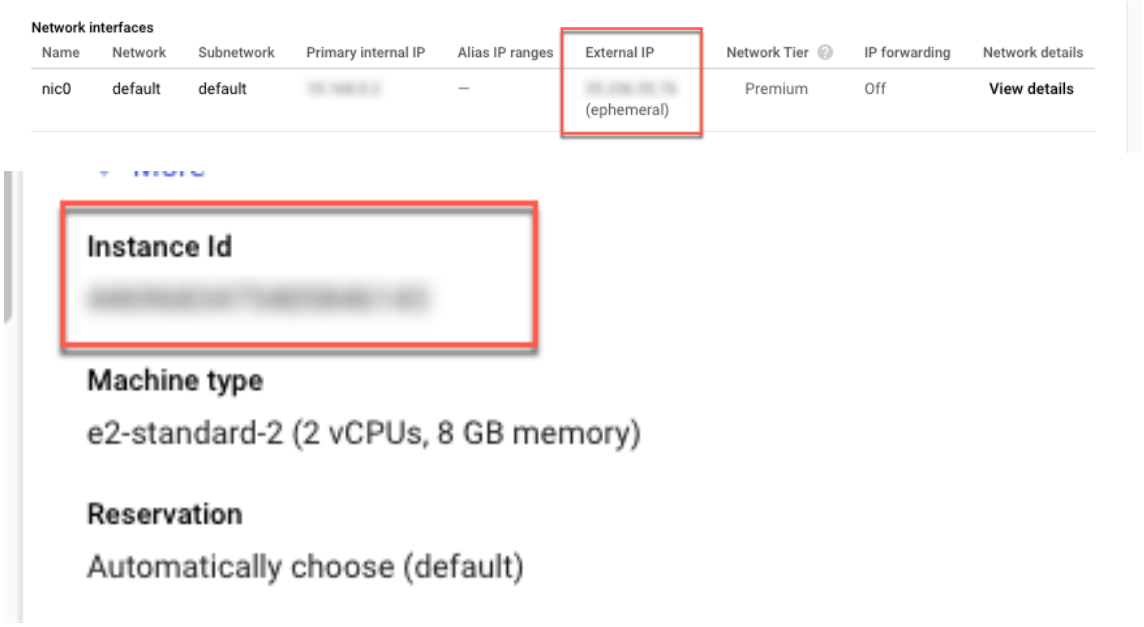


6. Log on to the agent through an SSH client using the agent external IP address. Use the following commands:

   ```
   ssh nsrecover@<external IP address of the agent>
   ```

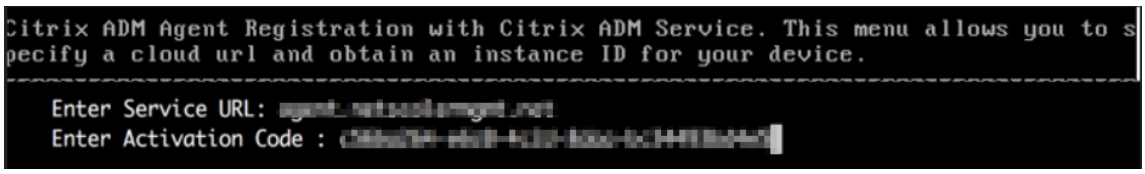
   Password: Instance ID

   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.

© 1997–2025 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

January 8, 2024

> **Note**
>
> The procedure to install an agent as a microservice is available in the Getting Started section.

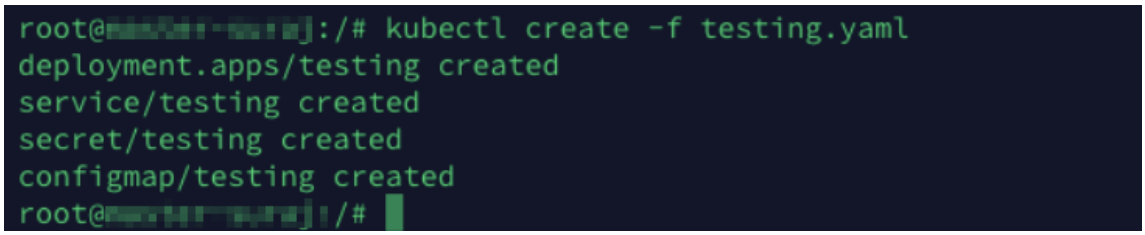
In the Kubernetes master node:

1. Save the downloaded YAML file
2. Run the following command:

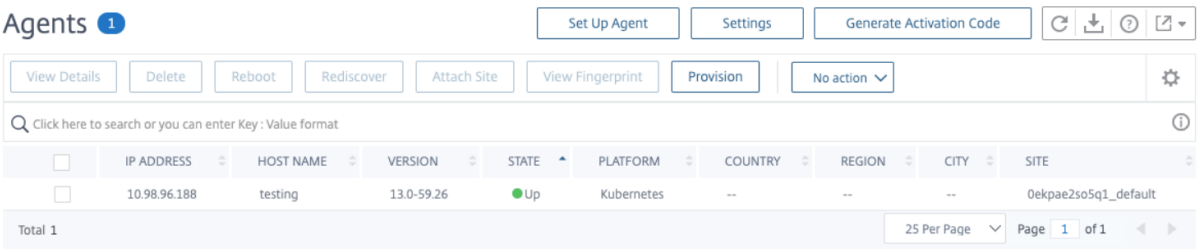
   `kubectl create -f <yaml file>`

   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.



© 1997–2025 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

September 27, 2024

> **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
  >
  ```

  > **Note:**
  >
  > - <adm-agent-password> is an example password. You must set a password for

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 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.

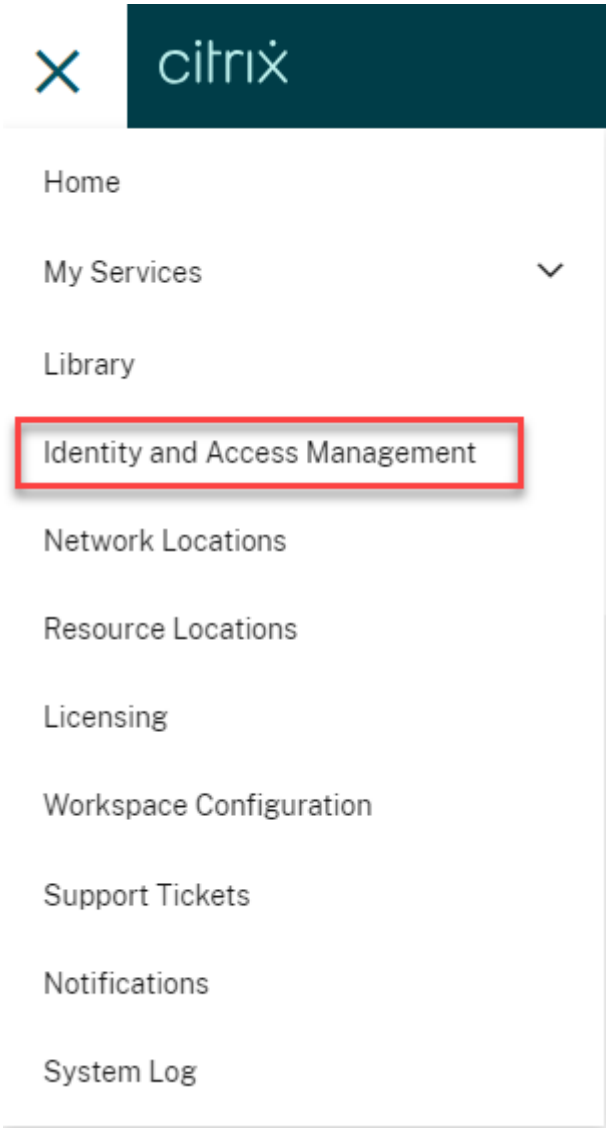
  ```
  kubectl create secret generic <secretname> --from-literal=accessid
  =<ID> --from-literal=accesssecret=<Secret> -n namespace
  ```

  > **Note:**
  >
  > Provide a secret name for accessSecret in agent YAML while creating the instance.

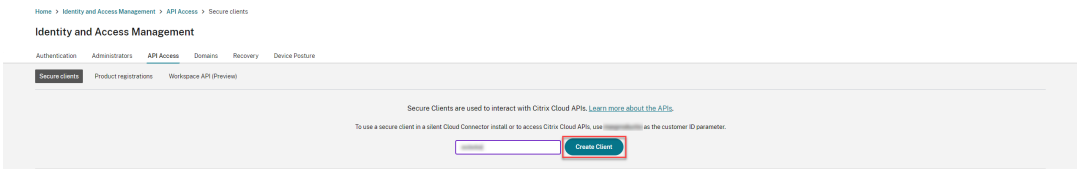
  You can get access ID and secret for accessing the NetScaler Console from the following procedure:

  1. Log on to the Citrix Cloud management console.
  2. From the Citrix Cloud menu, select **Identity and Access Management**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

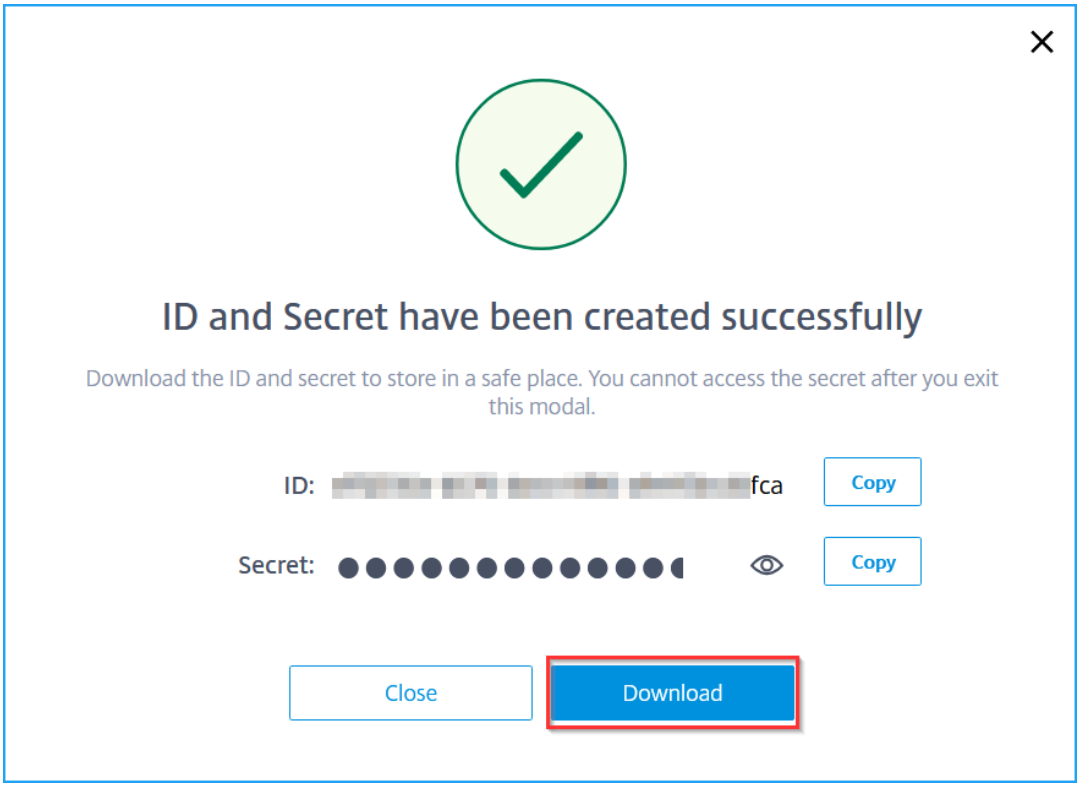


3. From the **API Access** tab, enter a secure client name and click **Create Client**.



4. ID and Secret are generated. Click **Download** and save the CSV file.

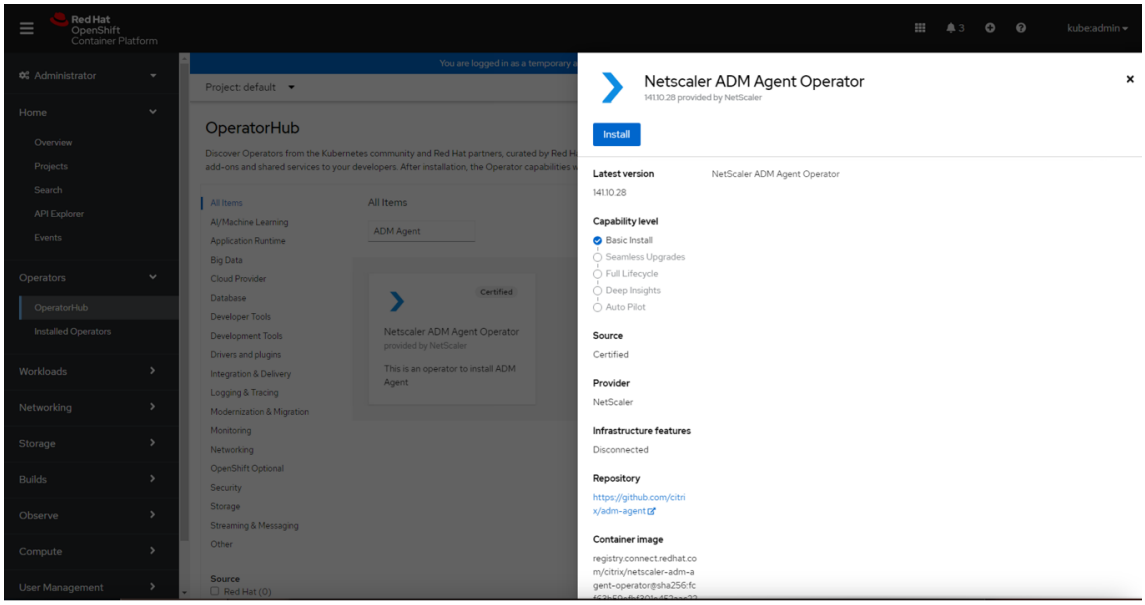
© 1997–2025 Citrix Systems, Inc. All rights reserved.



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**.

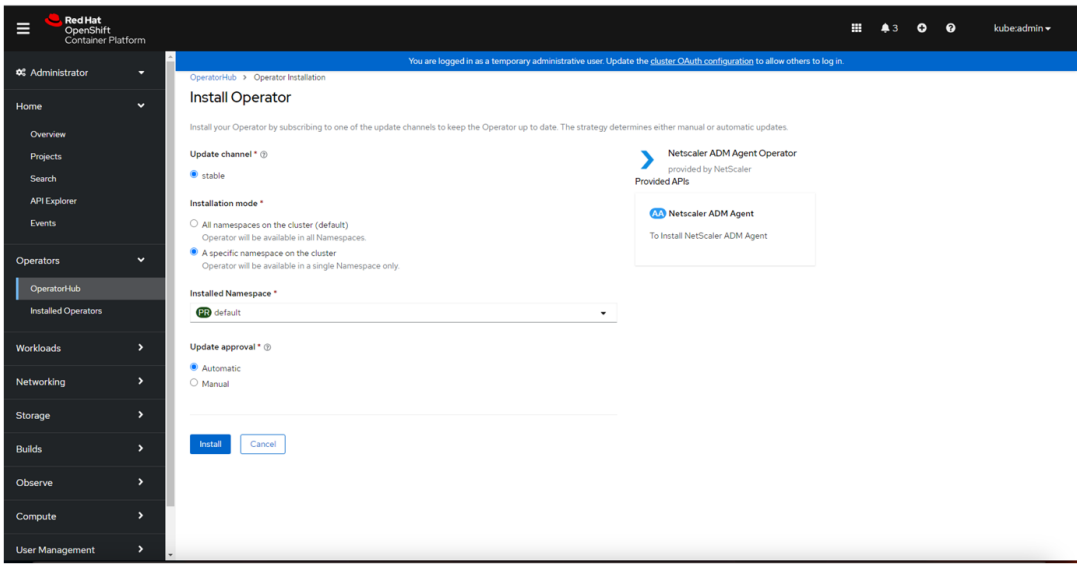
© 1997–2025 Citrix Systems, Inc. All rights reserved.



4. In the **Install Operator** page, you have two options:

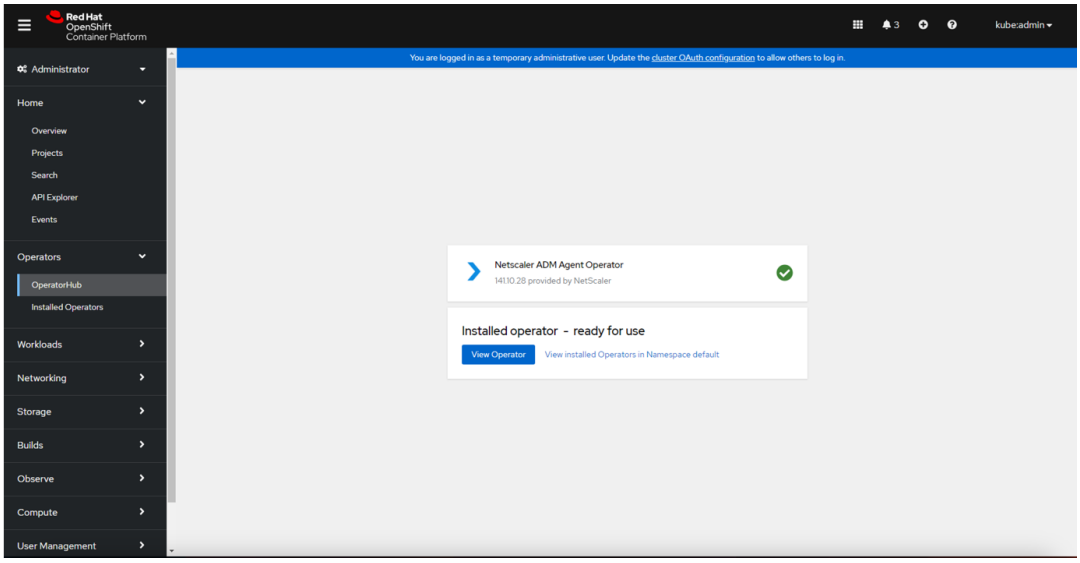
   - **All namespaces on the cluster (default)** - Enables the Agent operator to subscribe to all namespaces available in the cluster and allows you to initiate the instance of agent operator from any namespace on the cluster.
   - **A specific namespace on the cluster** - Enables the Agent operator to 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**.

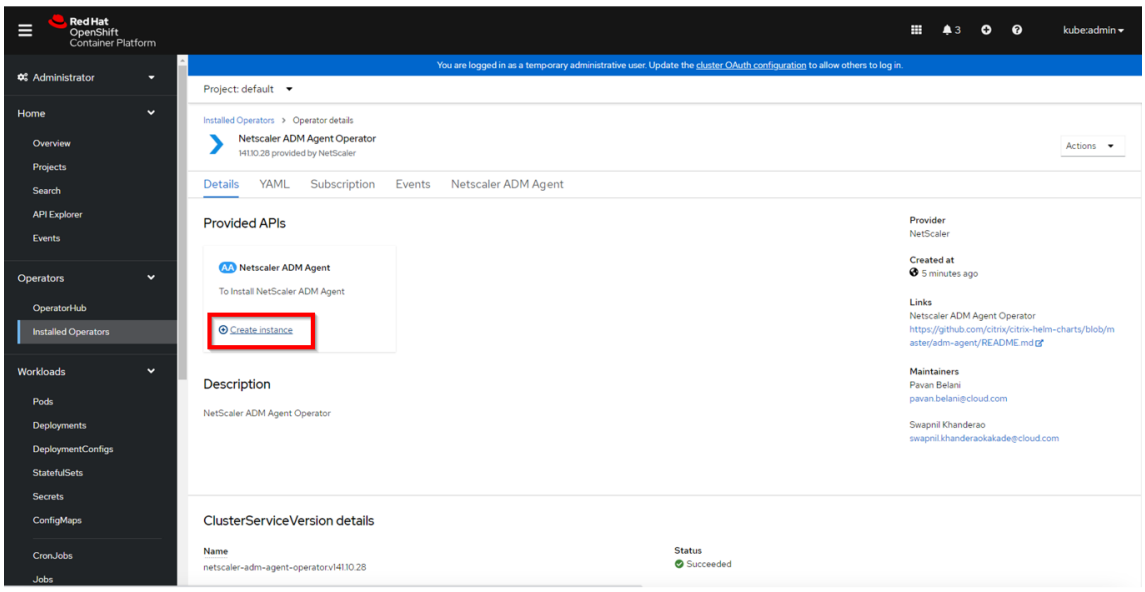
     

     Wait until the Agent operator is successfully subscribed.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



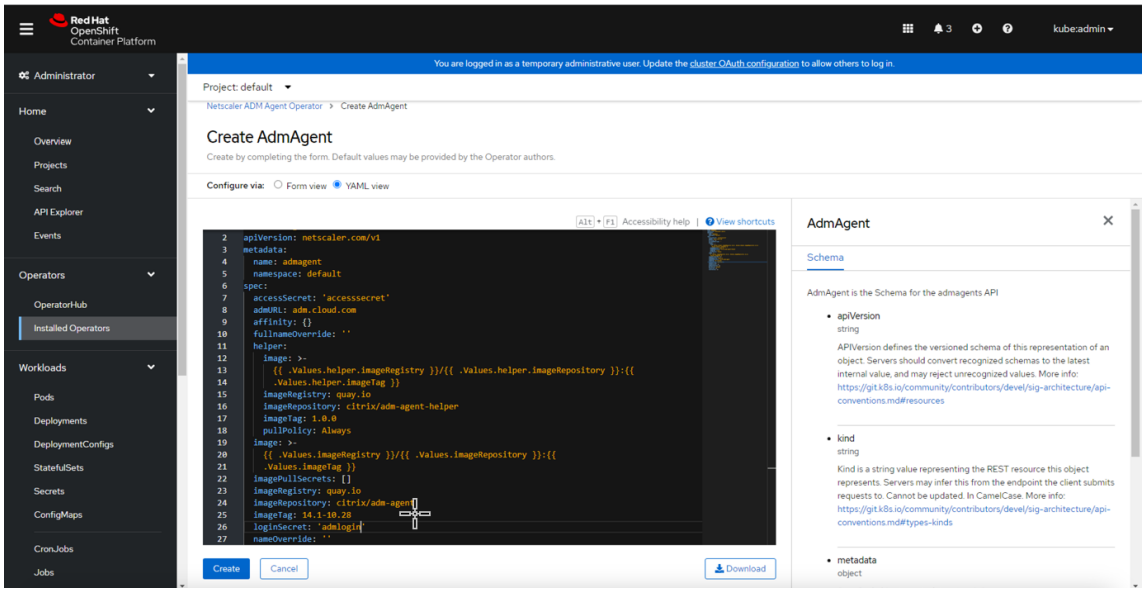
5. Navigate to **Workloads > Pods** and verify that the `netscaler-adm-agent-operator-controller` pod is up and running.
6. After the pod is up and running, click **Create Instance**.



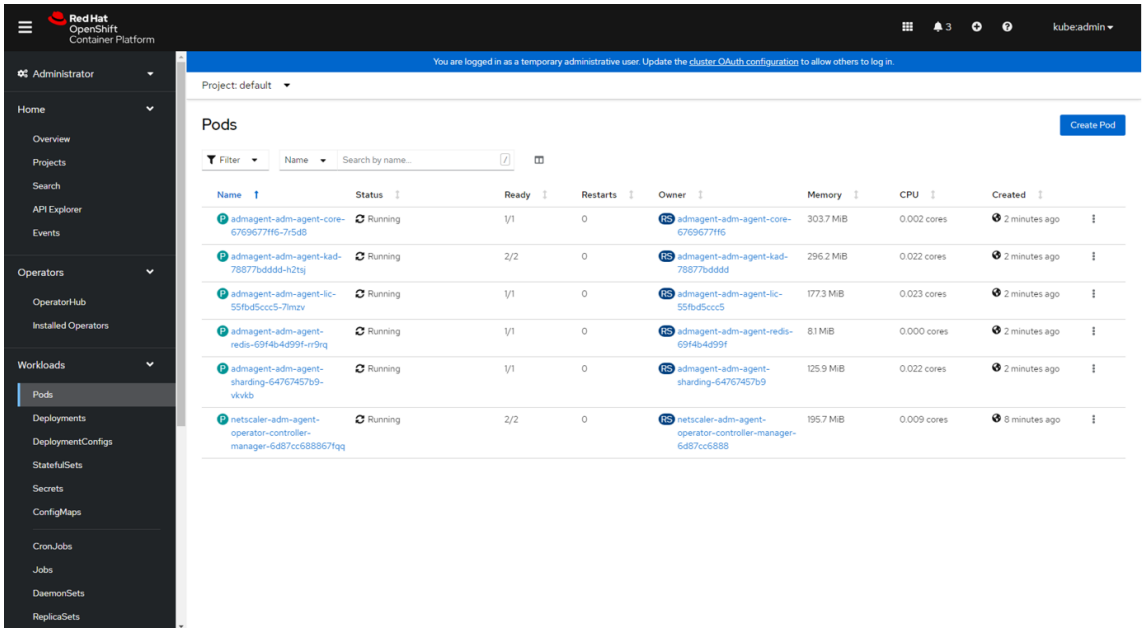
7. Select the **YAML view** to update any parameters and then click **Create**.

> **Note:**
>
> Ensure that there must be only one instance of agent per OpenShift cluster.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



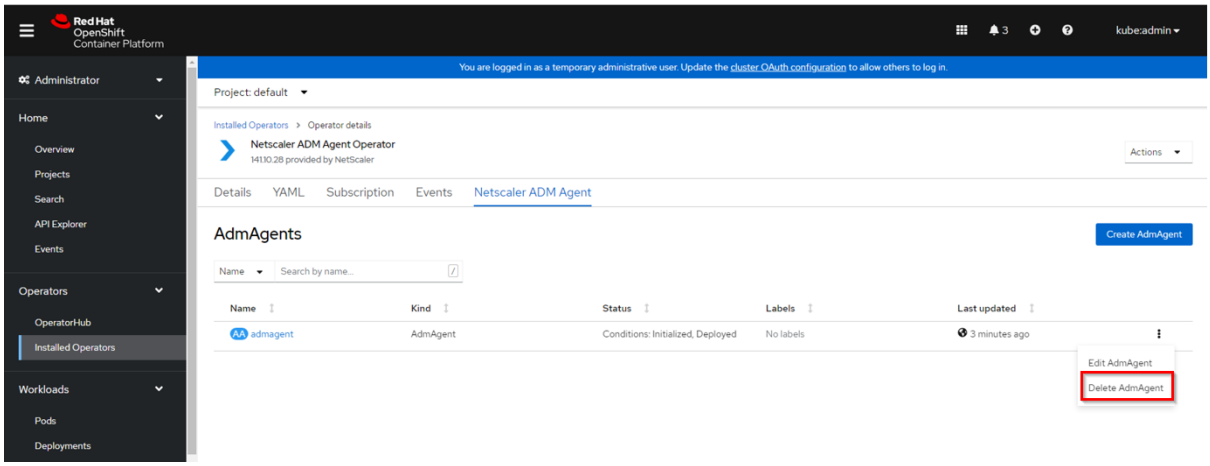
8. Navigate to **Workloads > Pods** and ensure that the agent pods are up and running.



Delete an agent instance

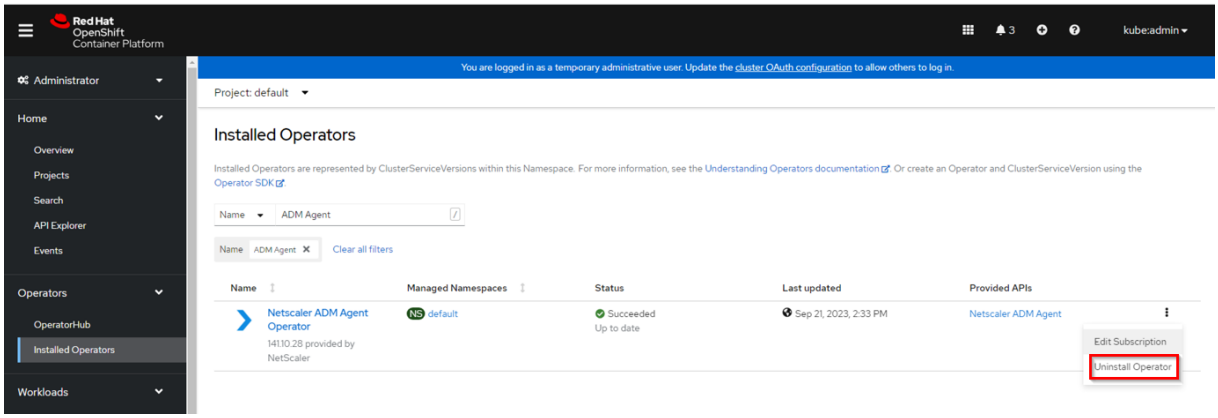
You can delete the instance of agent from the cluster by navigating to **Operators > Installed Operators**. In the **NetScaler ADM Agent Operator** tab, select the instance, and select **Delete AdmAgent** from the list.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.



Install a container-based agent using helm chart

January 8, 2024

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

How to Get Help and Support

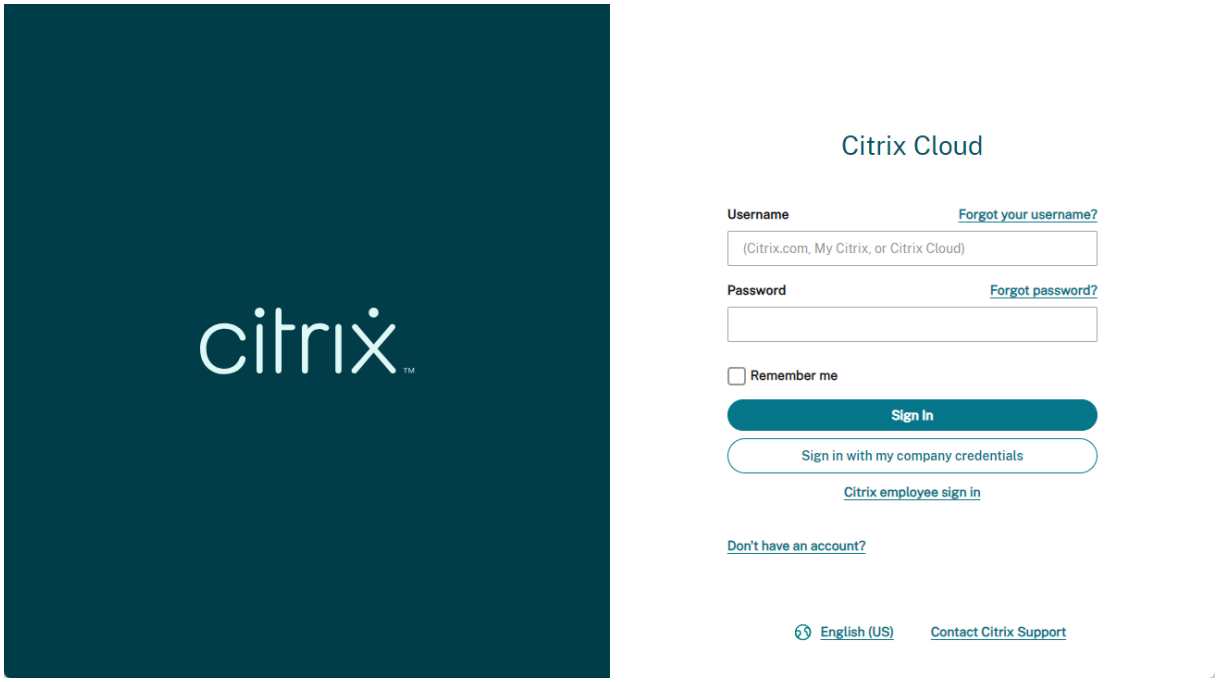
September 8, 2025

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.

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

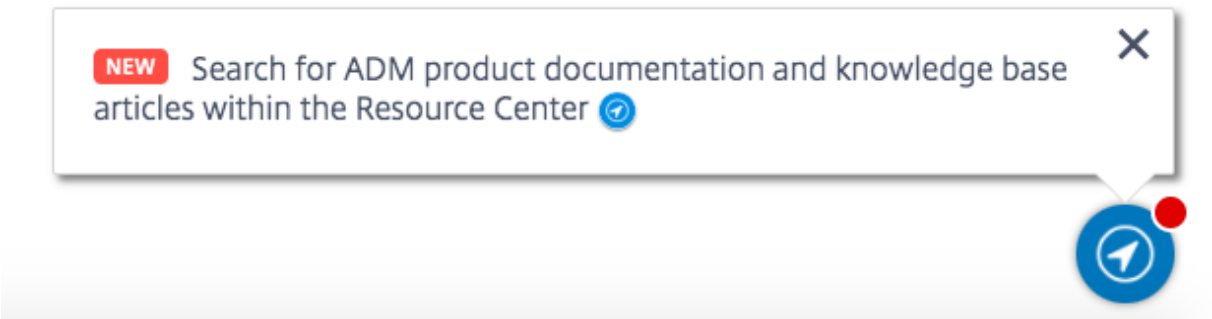
Support articles and documentation

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.

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.

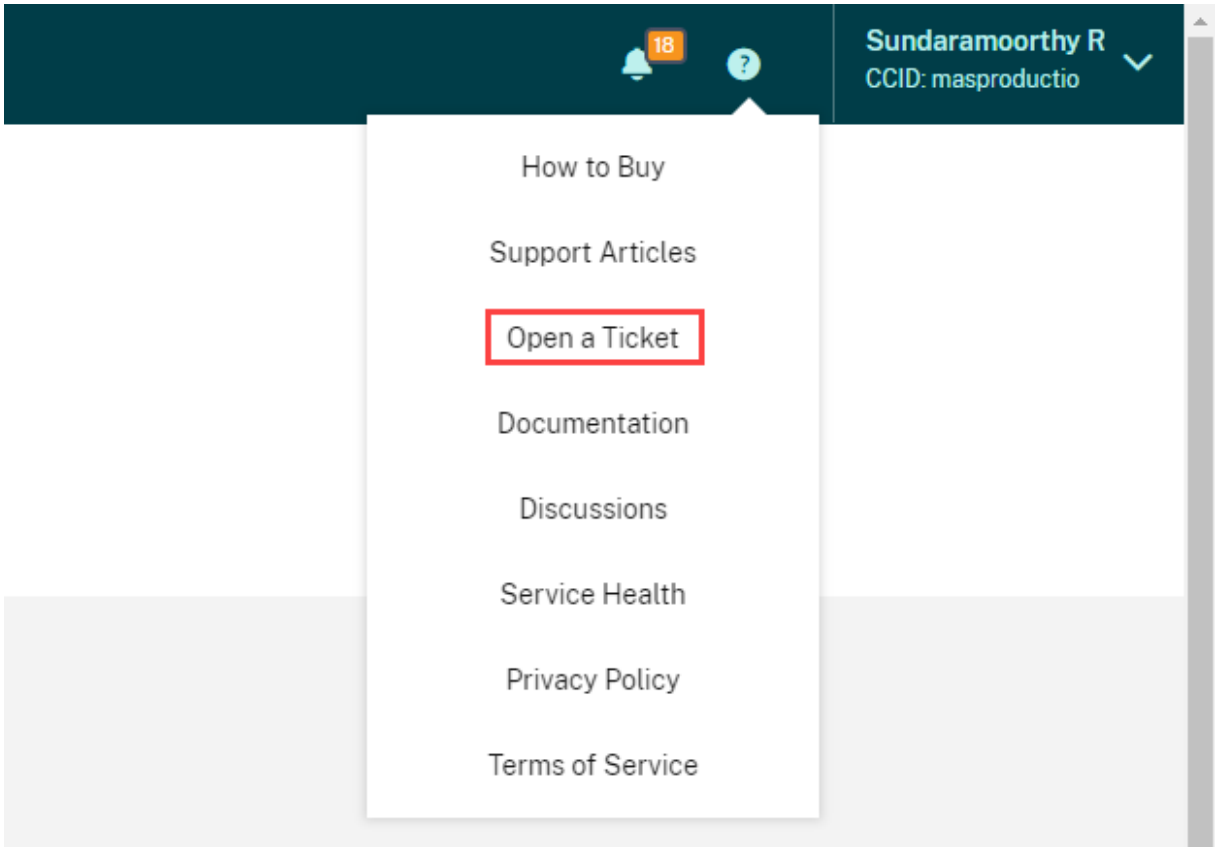
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.**



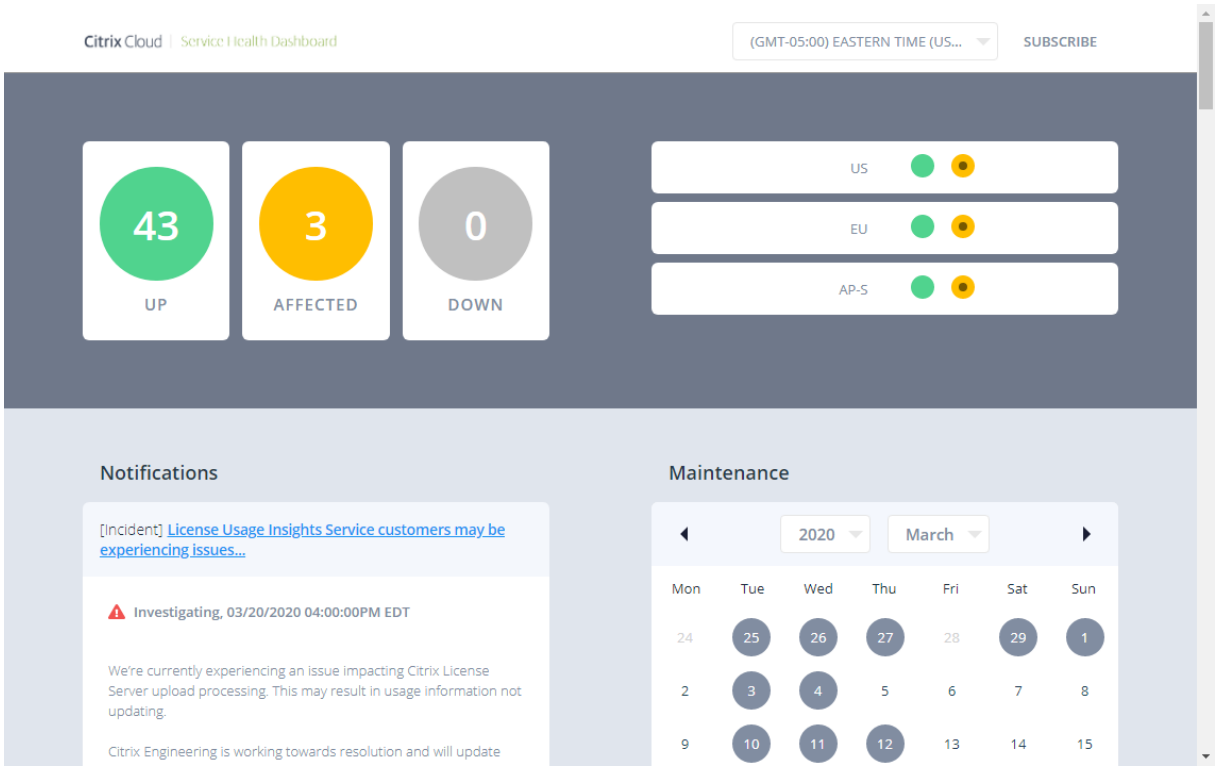
Click **Go to My Support** and then **My Support** to open a ticket through the My Support portal. You can also use the My Support portal to track your existing tickets and view your current product entitlements.

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Cloud, check the Service Health Dashboard to verify that Citrix Cloud or specific services are operating normally.

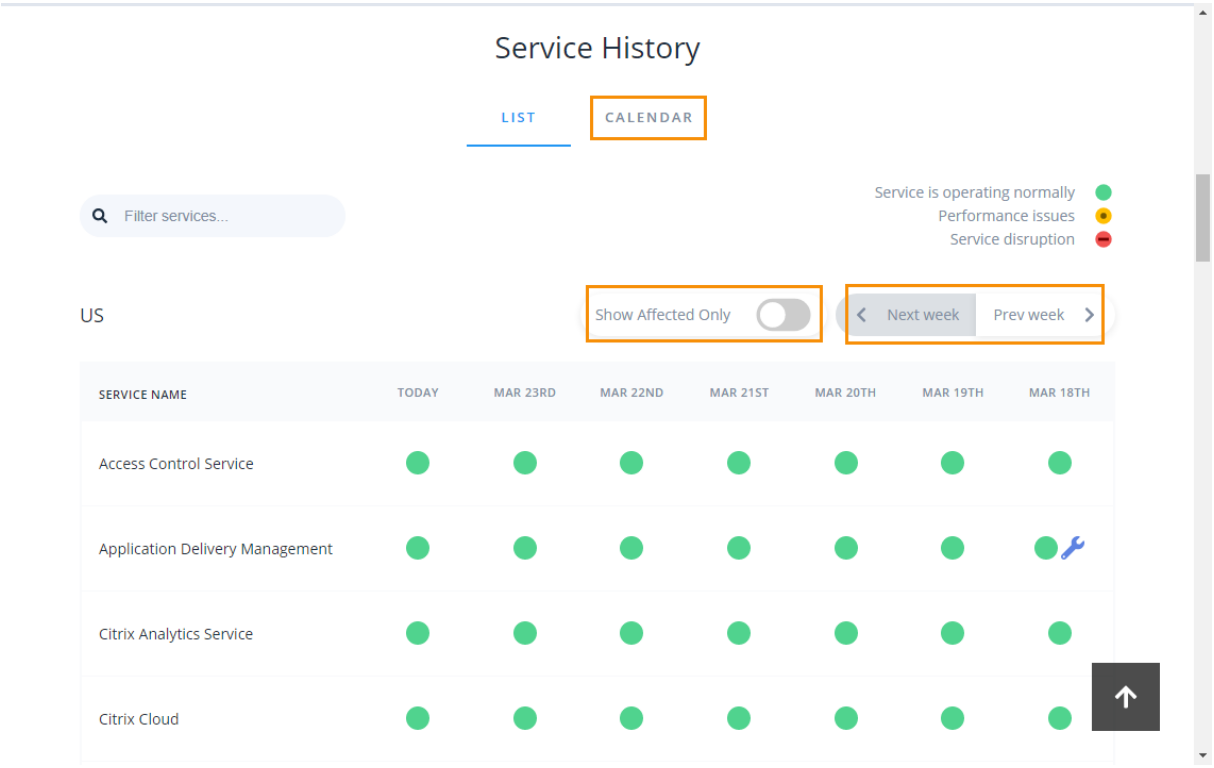


Use the dashboard to learn more about the following conditions:

- 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

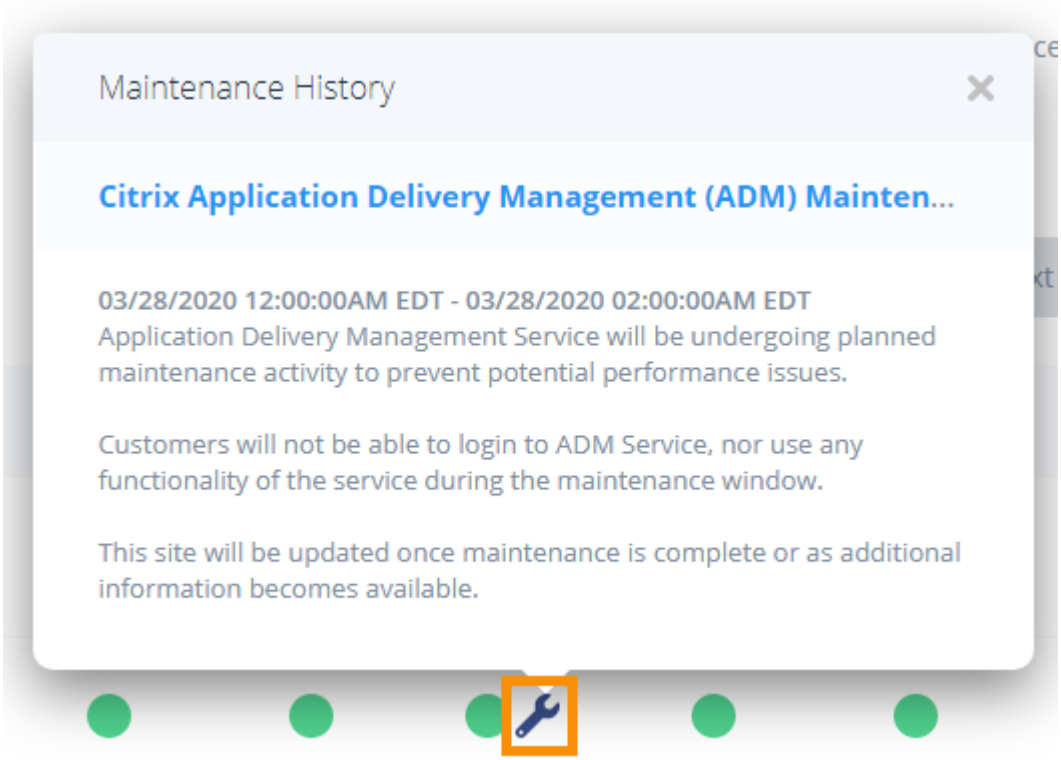
By default, service health status is displayed as a list, but you can also display the status in a calendar view. Select **Next** or **Previous** to scroll through the service health history in seven-day increments. You can also filter the list to display affected services only.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



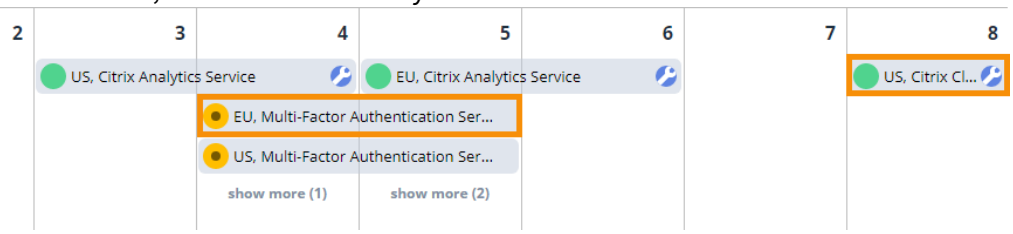
To view more detailed information about the service health incident for an affected service:

- From the list view, click the icon next to the service indicator to view more detailed information about the service health incident.



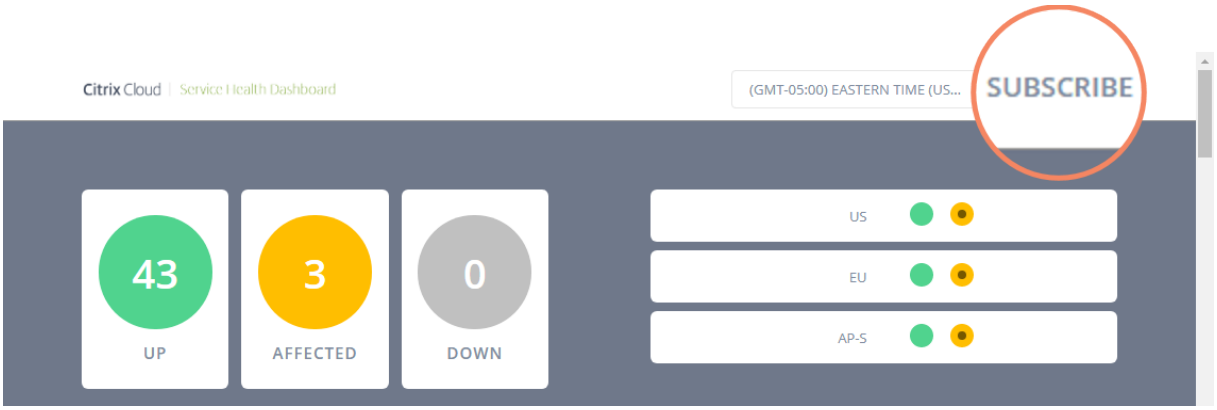
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- From the calendar view, click the service entry to view the status for the service health incident.



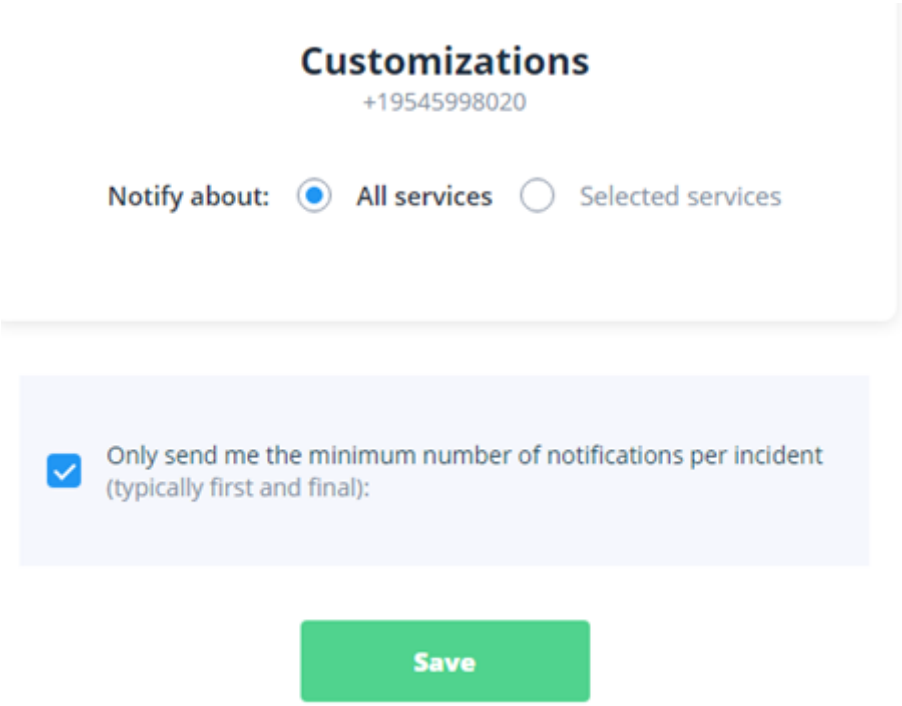
Service health subscriptions

To receive service health notifications, click **Subscribe** in the upper-right of the dashboard and select the notification method you want to use.

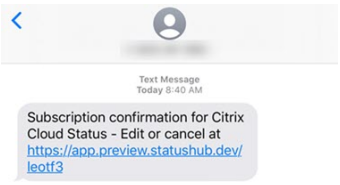


You can subscribe to notifications for all services or only the services you select. By default, you receive all notifications for a service health incident. To limit the frequency of notifications during an incident, you can choose to receive only the first and final notifications.

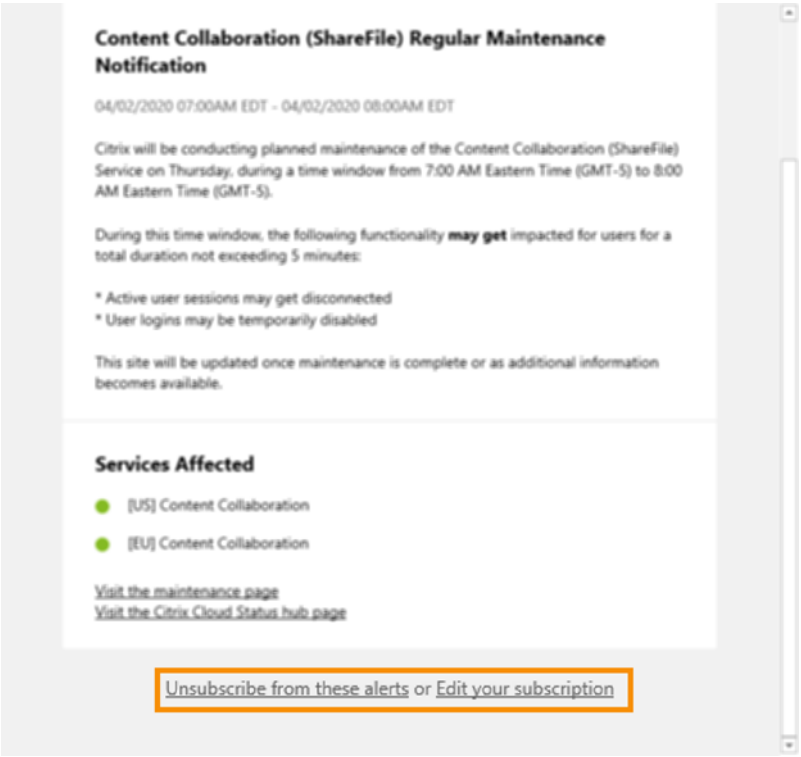
© 1997–2025 Citrix Systems, Inc. All rights reserved.



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).



© 1997–2025 Citrix Systems, Inc. All rights reserved.



To unsubscribe or change your subscription preferences:

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**.

Enhanced Graphical User Interface

November 20, 2024

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.

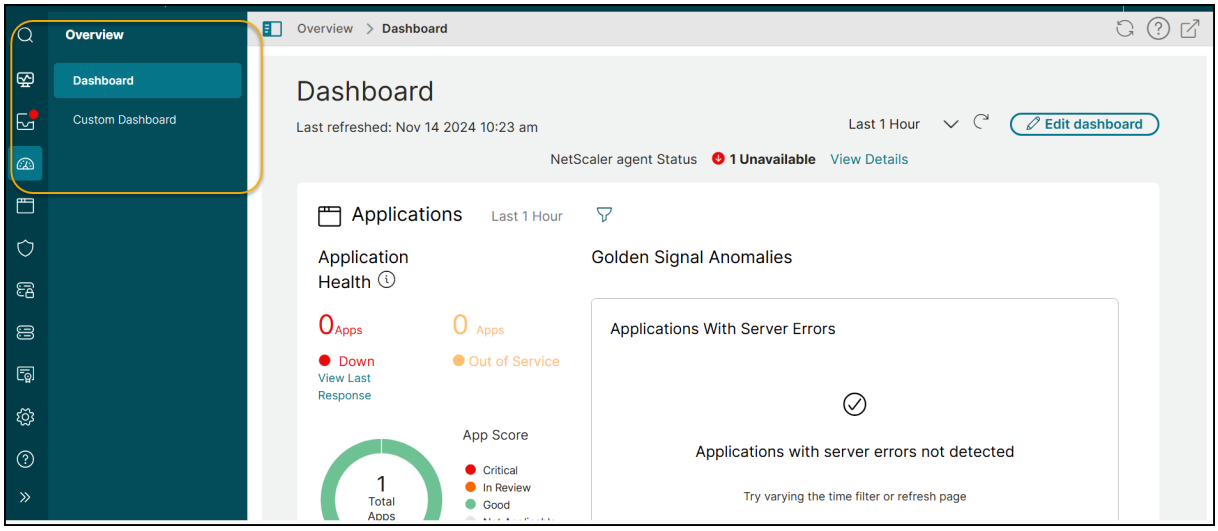
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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.



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:

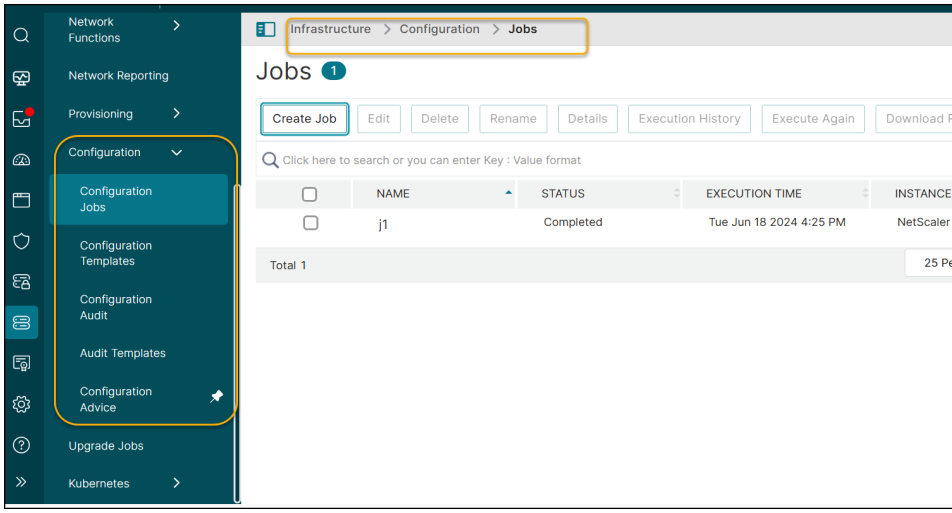
- **Infrastructure > Configuration**
- **NetScaler Licensing > Pooled Licensing**
- **Gateway > HDX Insight**

Updated submenu labels

The names of some submenus are changed to align with this navigation approach. Screen navigation changes and submenu label updates are:

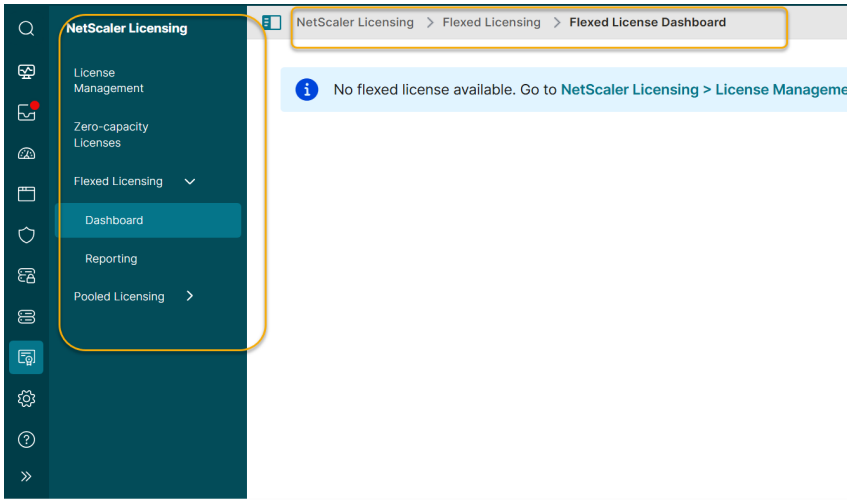
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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
Configuration > Configuration Audit > Audit Templates	**Configuration > Audit Templates**	No
Configuration > Configuration Audit > Configuration Advice	**Configuration > Configuration Advice**	No

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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
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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Previous screen navigation	Changed screen navigation	Is there a change in the submenu label?
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**

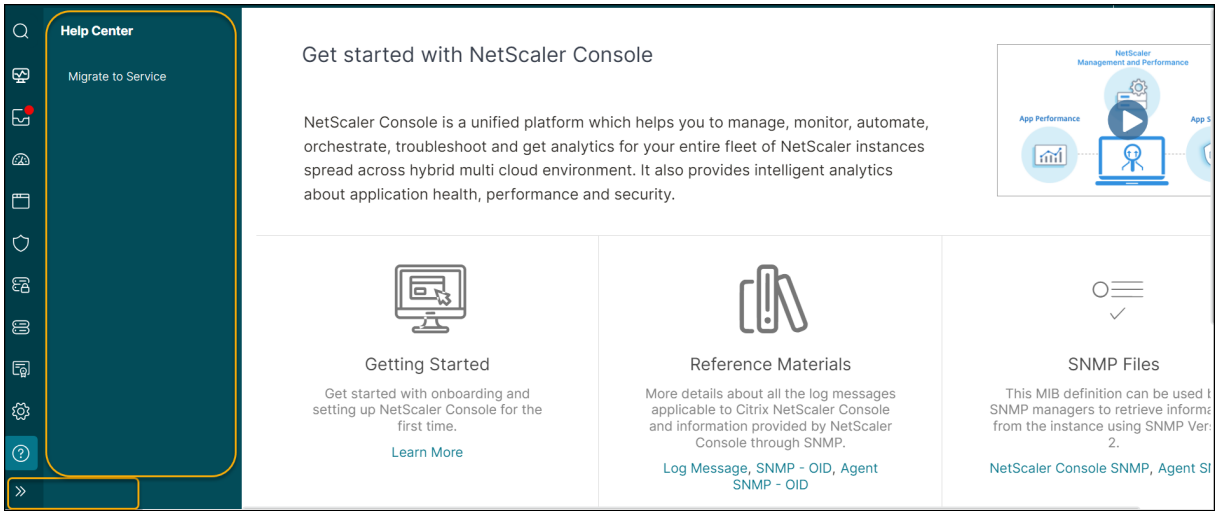
Collapsible menu

You can collapse or expand the entire menu by clicking an icon.

Expanded menu

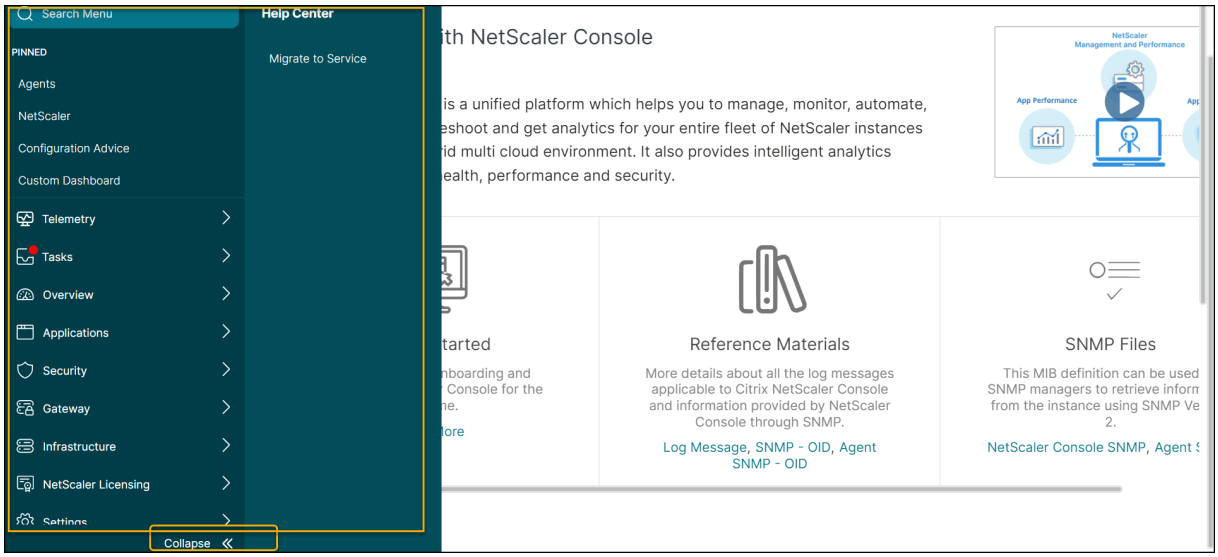
Click the icon » in the pane to expand the entire menu.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Collapsed menu

Click **Collapse** « in the pane to collapse the entire menu.

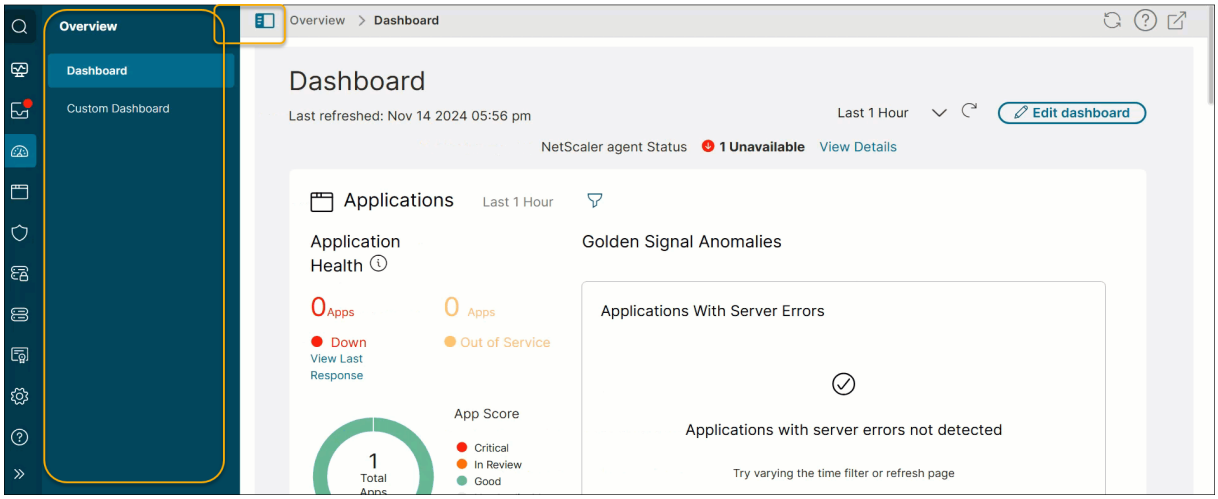


Sidebar Toggle

You can optimize screen space by toggling the sidebar visibility. Click the toggle button in the bread-crumb to hide or show the sidebar.

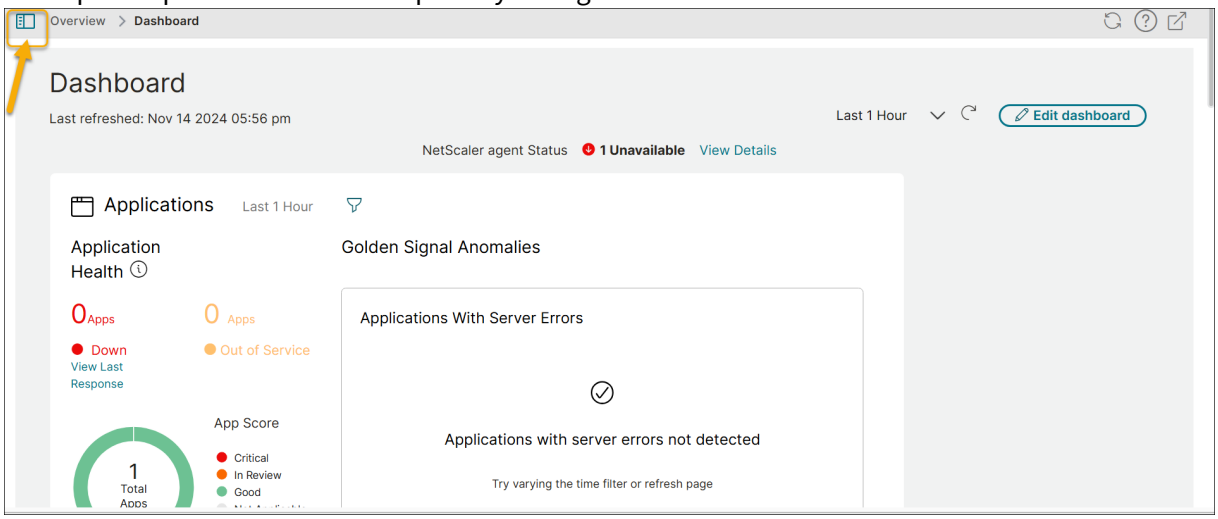
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Show sidebar



Hide sidebar

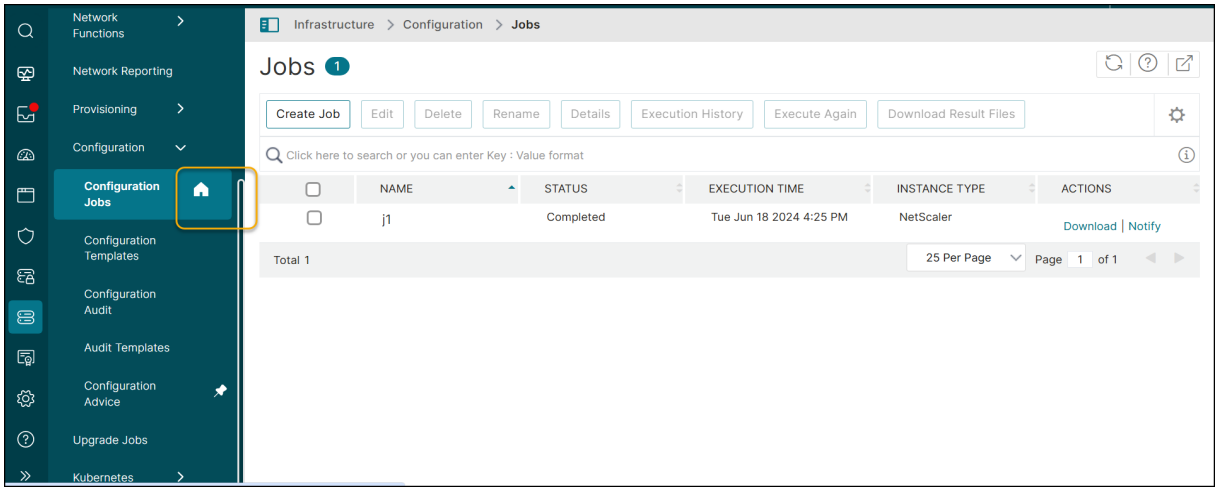
This option optimizes the screen space by hiding the sidebar.



Set as home screen

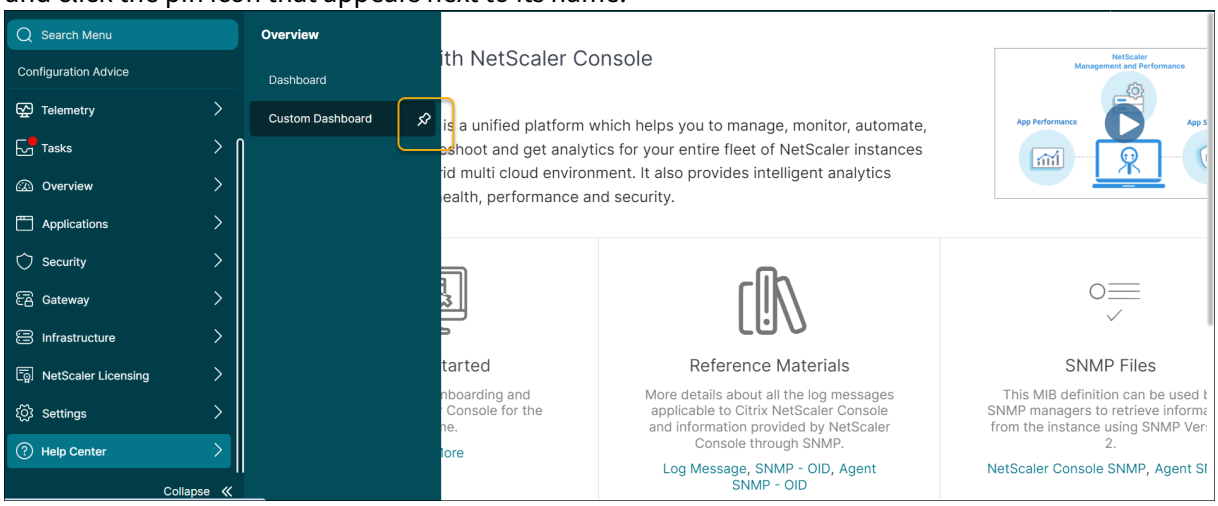
NetScaler Console GUI features an icon next to the name of a submenu that is displayed as a page.The home screen icon allows you to set your landing page. It only appears when you are on that specific page. To remove the page from the home page, simply click the icon again.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



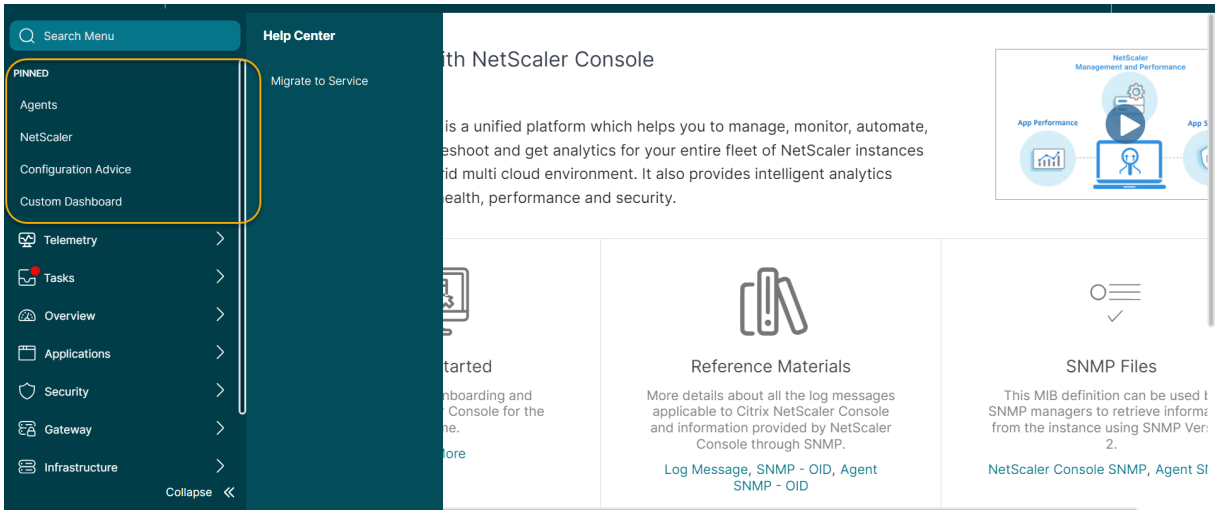
Pin favorite items

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Low-touch onboarding of NetScaler instances using Console Advisory Connect

March 7, 2025

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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - 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 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> sent directly from NetScalerto the NetScaler Console service endpoint and are not routed through through the external agent.

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.
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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

March 7, 2025

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.

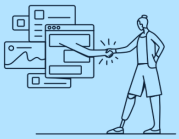
Step 1: Get started

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

citrix

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.

2 ADC instances are on older builds and releases.

Recent events

4 ADC instances encountered SSL card failure.
2 ADC instances encountered hard disk failure.

Resource utilization

2 ADC instances CPU usage exceeded 50%
3 ADC instances memory usage exceeded 50%

ADC deployment

5 ADC instances are not deployed as High Availability (HA) pair. Citrix ADM recommends HA pair for production ADC instances.

To get more details and recommendations on these insights, **onboard your ADC instances to Citrix ADM service, today.**

As a first step, you will need to create Citrix Cloud account by clicking on the button below.

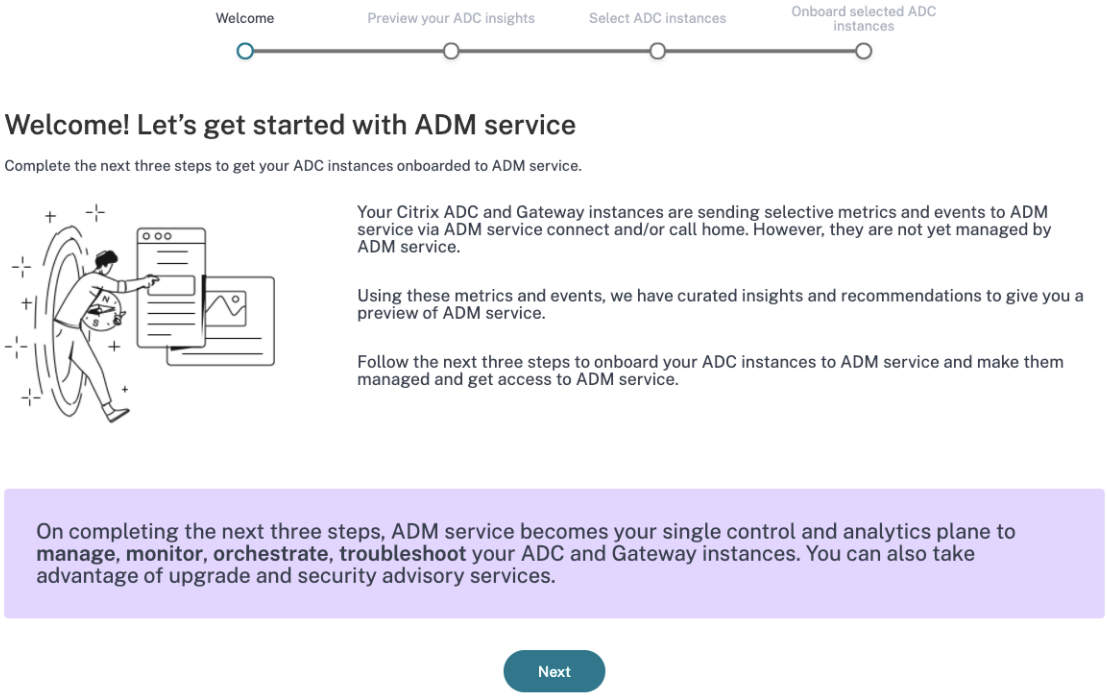
Onboard to ADM Service

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.



> **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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 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.
- **NetScaler deployment guidance**: onboard NetScaler instances to NetScaler Console and configure them as HA pair, using configuration jobs on NetScaler Console.

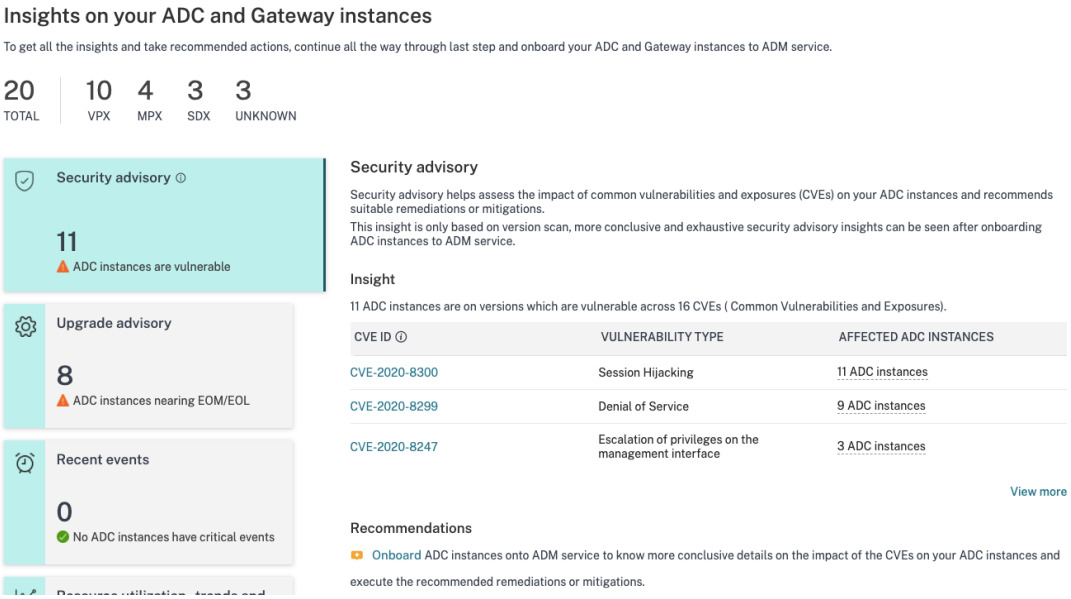
1. **Security advisory**: NetScaler Console Security Advisory alerts you about vulnerabilities putting your NetScaler instances at risk and recommends mitigations and remediations.

   > **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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

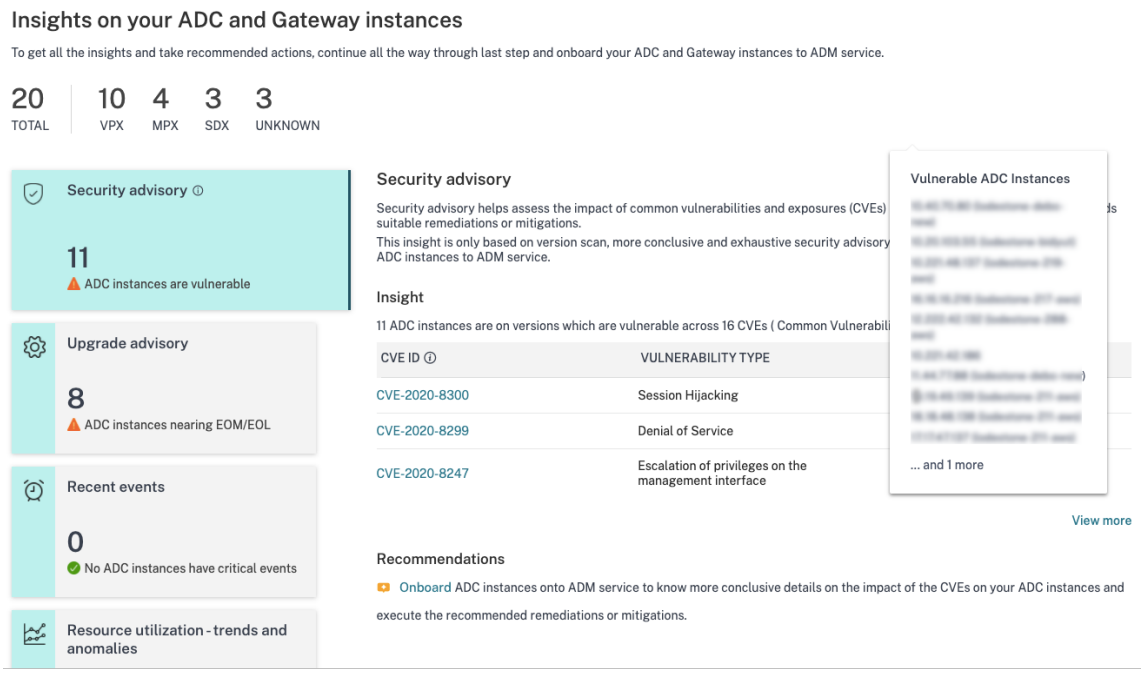
> CVE needs both version scan and config scan for vulnerability assessment, the onboarding email and guided workflow shows the results based on version scan. So, there might be false positives. To know a more conclusive and accurate assessment of the impact, onboard NetScaler to NetScaler Console. After 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.

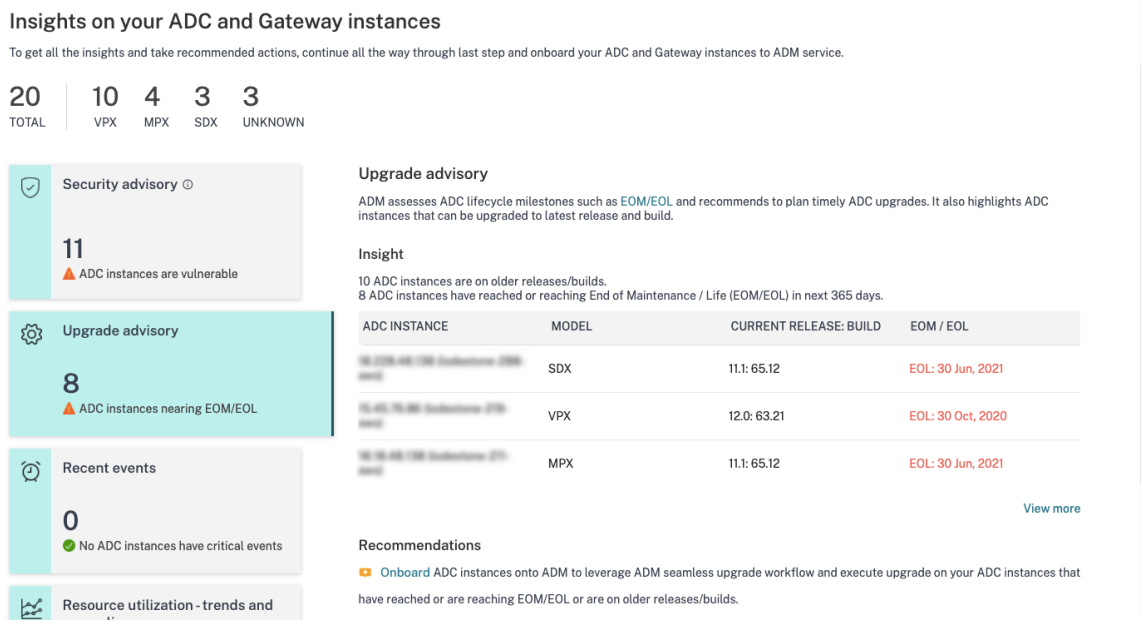
© 1997–2025 Citrix Systems, Inc. All rights reserved.



2. **Upgrade advisory**: Use this advisory to check which NetScaler instances are nearing EOM/EOL or are on older builds.

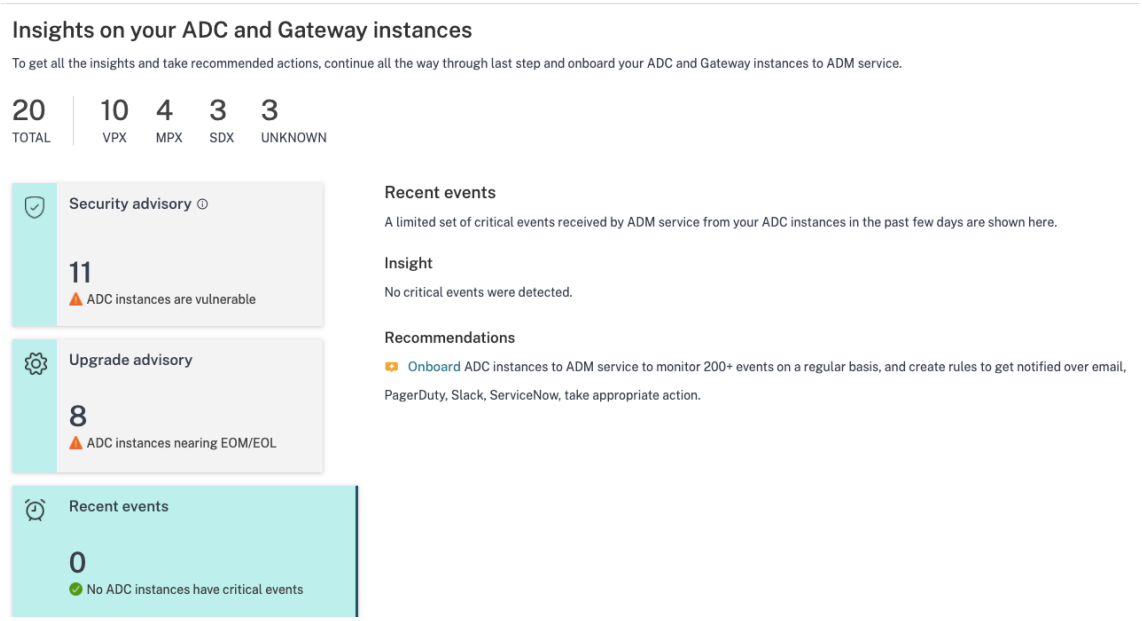
   Based on these insights, NetScaler Console recommends you to plan a timely upgrade before EOM/EOL or to benefit from the latest features and fixes.

   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.

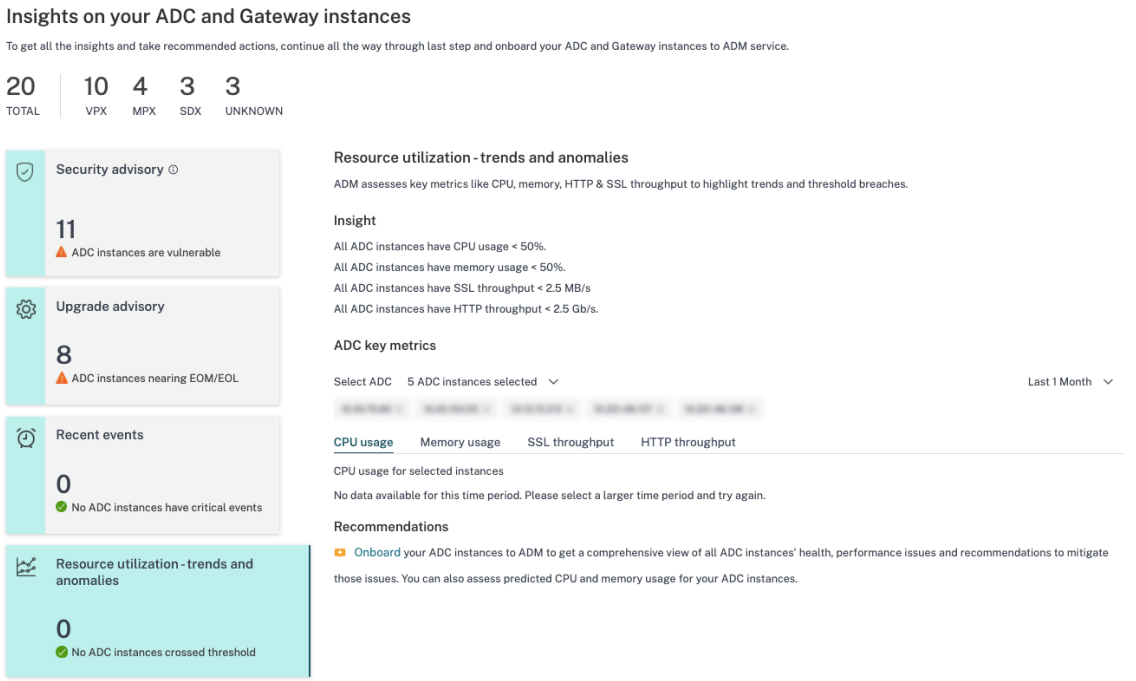
© 1997–2025 Citrix Systems, Inc. All rights reserved.



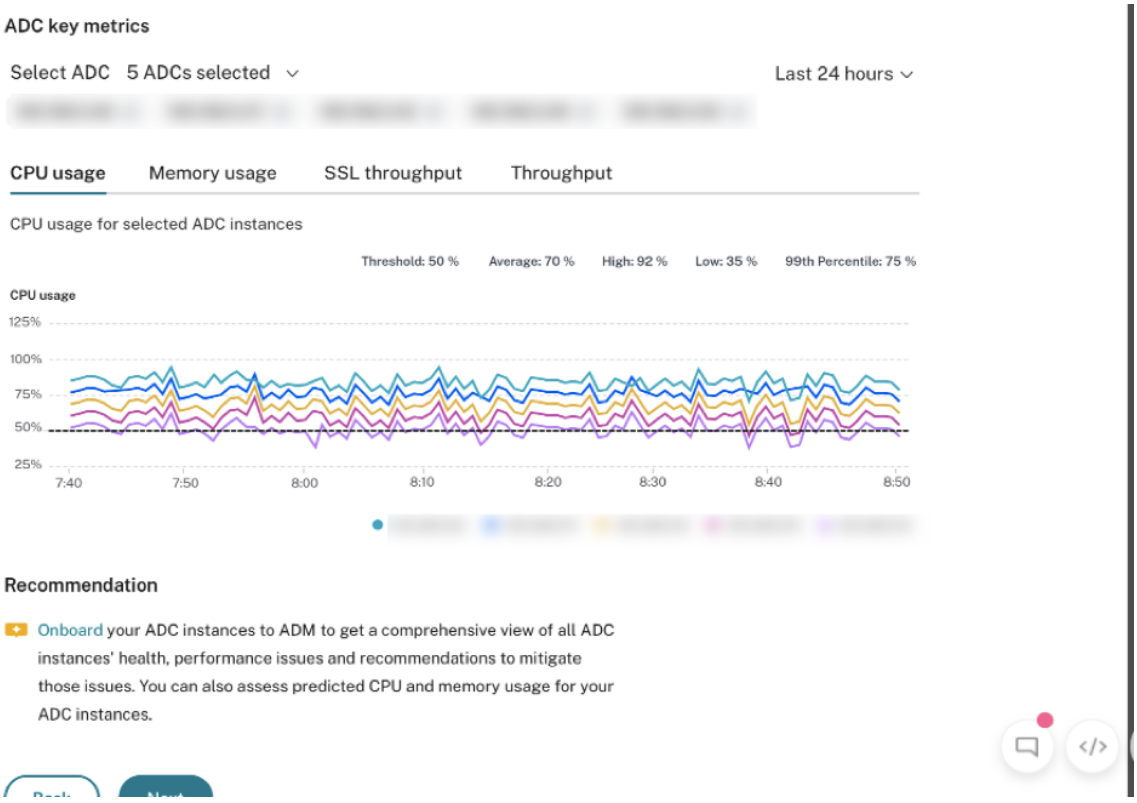
4. **Resource utilization - trends and anomalies**: Find insights about high resource utilization for CPU, memory, HTTP throughput, and SSL throughput. For each insight, NetScaler Console suggests recommended action. To have more visibility into these insights and recommendations, you must onboard your 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



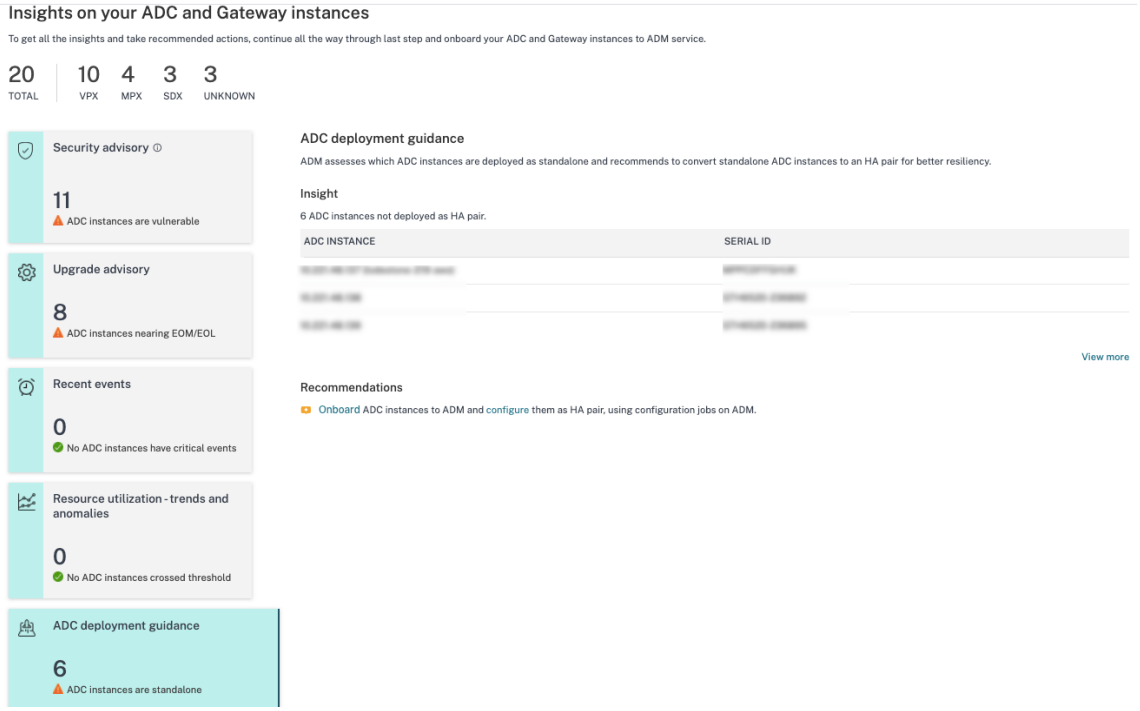
- **Key Metrics**: Get details of key metrics related to CPU, memory, HTTP throughput, SSL throughput, and uncover anomalous trends in metrics.



5. **Deployment guidance**: Have visibility into NetScaler instances that are deployed as a standalone NetScaler. NetScaler Console gives the recommendation to configure these NetScaler

© 1997–2025 Citrix Systems, Inc. All rights reserved.

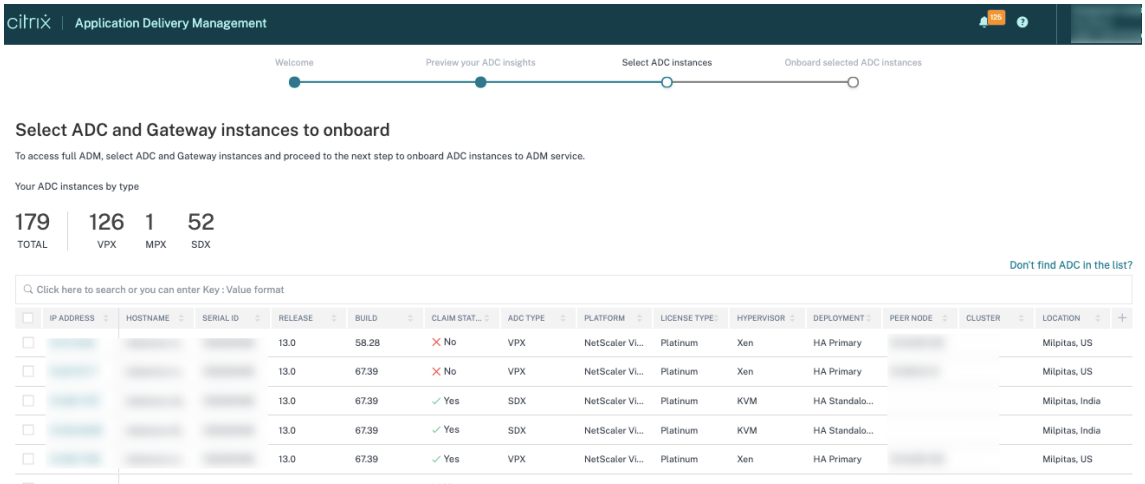
instances as an HA pair for better resiliency. This requires you to onboard your NetScaler instances to NetScaler Console and then use maintenance jobs to configure the instances as an HA pair.



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.

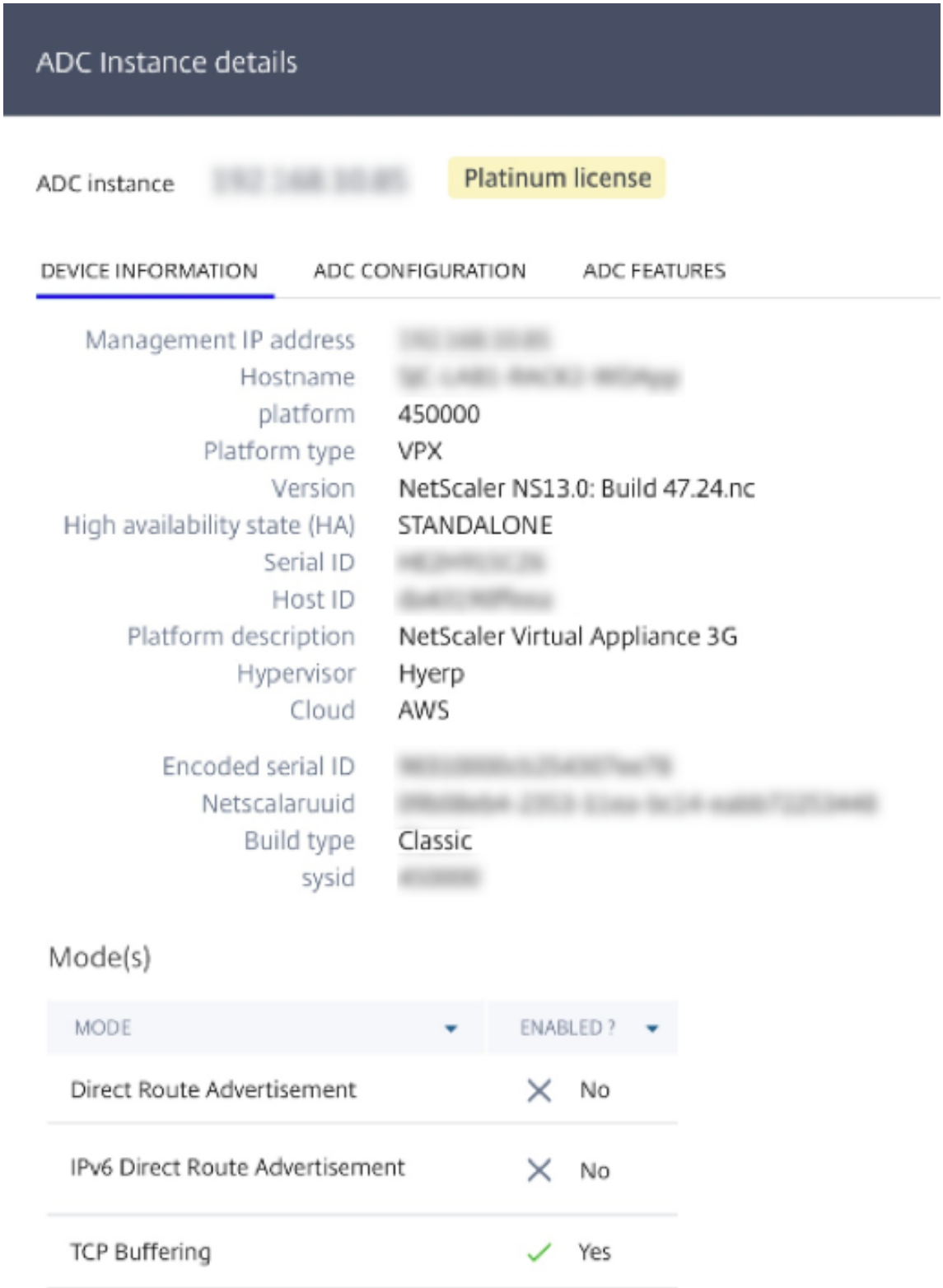


If you need details about any instance such as device information, NetScaler configuration,

© 1997–2025 Citrix Systems, Inc. All rights reserved.

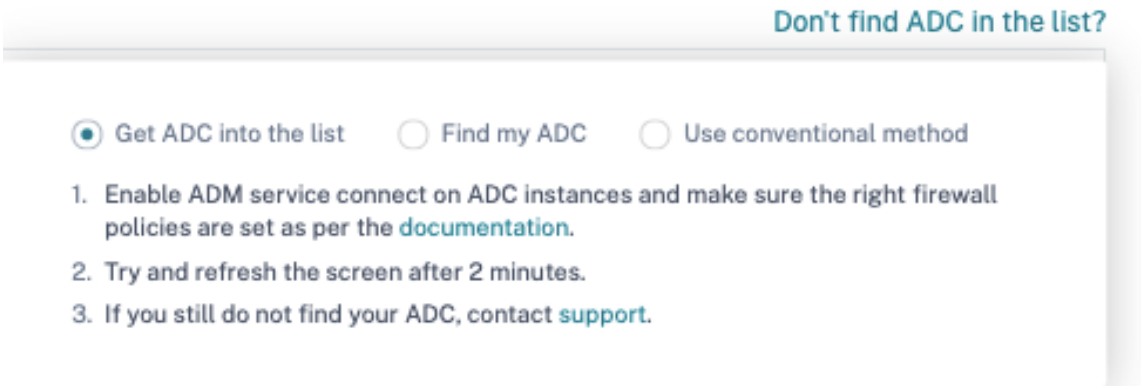
NetScaler features available, or license information, click the instance IP address under the NetScaler instance.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



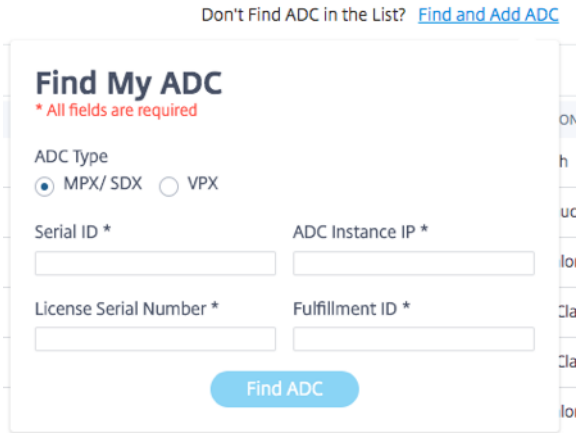
© 1997–2025 Citrix Systems, Inc. All rights reserved.

If your instance is not listed, use the **Don't find NetScaler in the list** on the upper-right corner.



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.

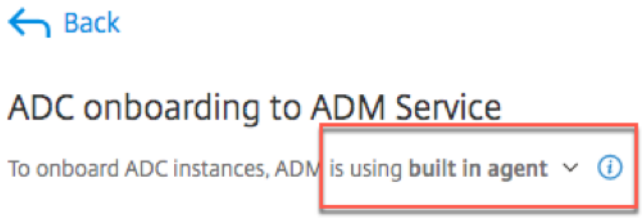
For the **Find my NetScaler option**, enter the details in the mandatory fields (serial ID, NetScaler instance IP address, license serial number, and fulfillment ID) and search.



Step 4: Onboard NetScaler instances to NetScaler Console

You can onboard your instances using the built-agent (default option) or an external agent.

© 1997–2025 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

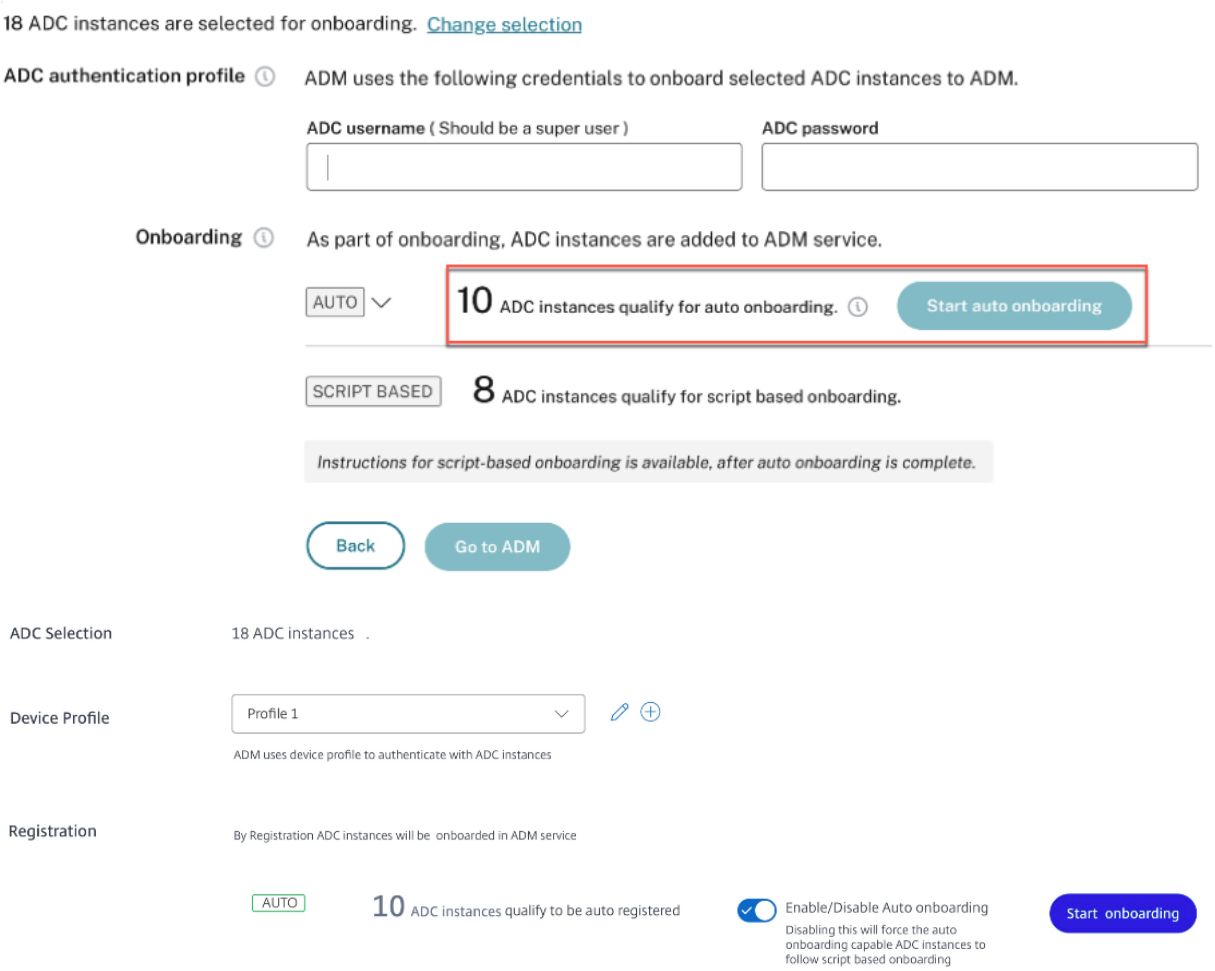
To select a different NetScaler instance, click **Change selection**.

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.

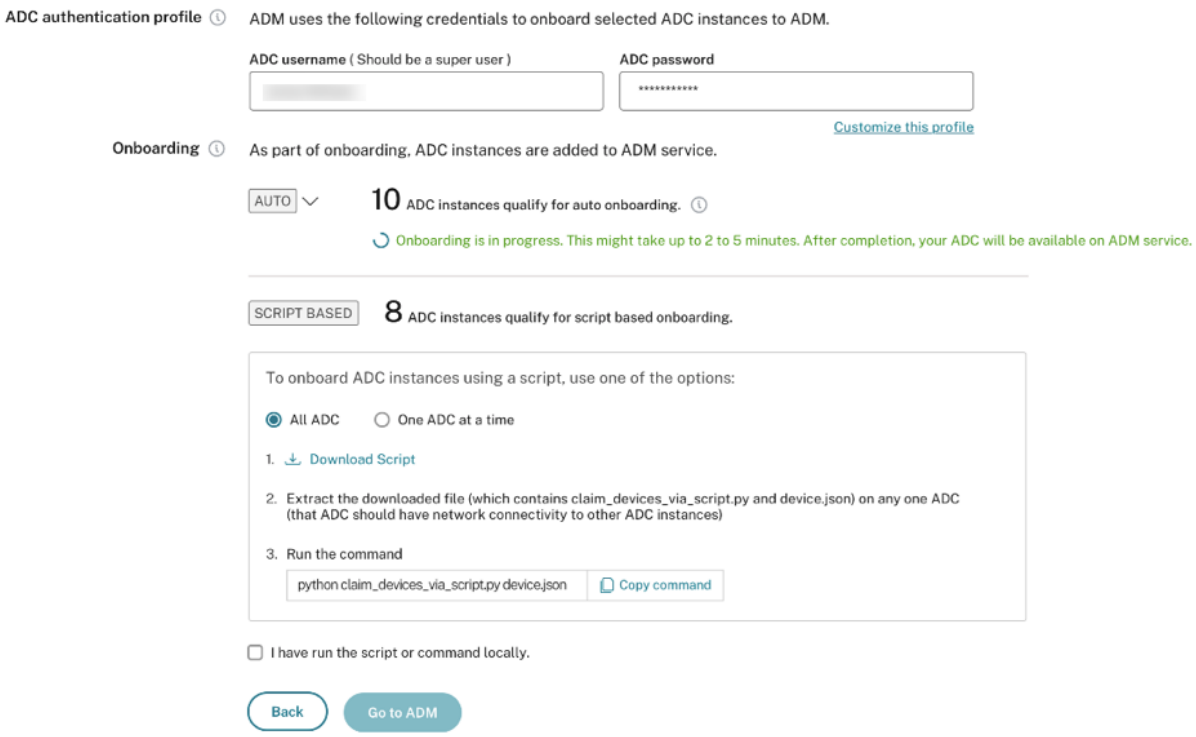
© 1997–2025 Citrix Systems, Inc. All rights reserved.



> **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

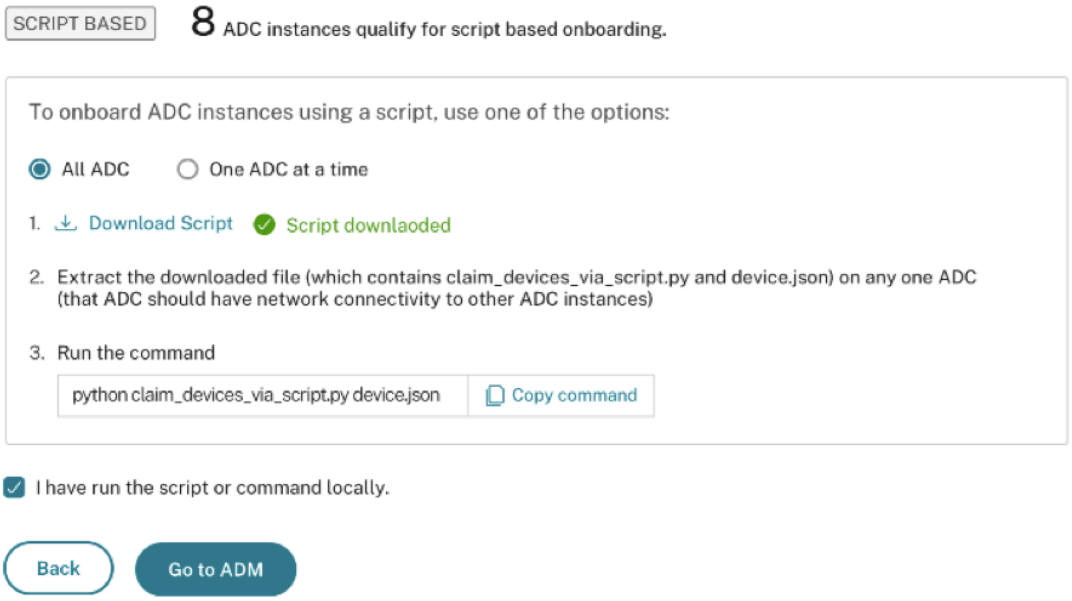


> **Note:**
>
> If you don't want the NetScaler instances to auto-onboard to NetScaler Console, you can disable auto-onboarding and you use the script-based option for on onboarding.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

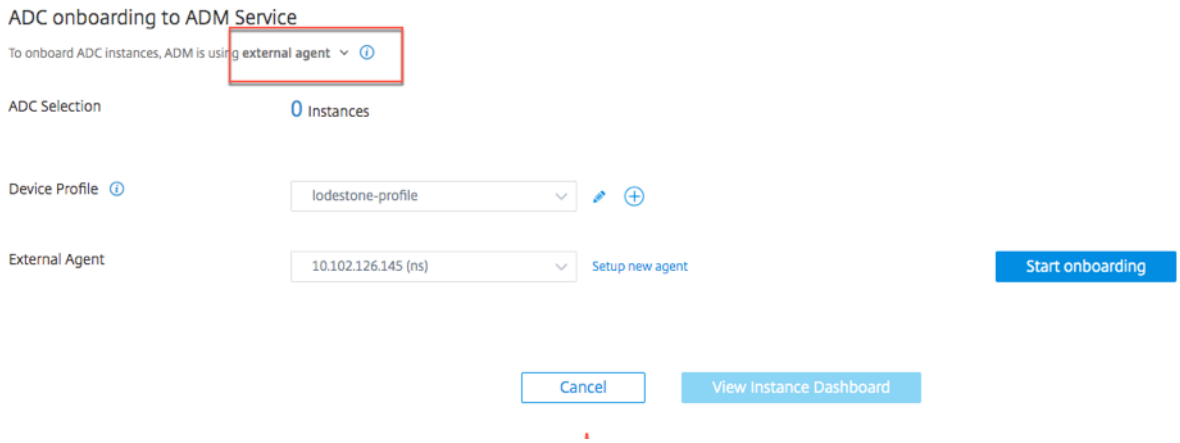


After you've onboarded all your instances, click **Go to NetScaler Console** to go to the NetScaler Console instance management UI dashboard and explore the different features.

> **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.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Complete the following steps:

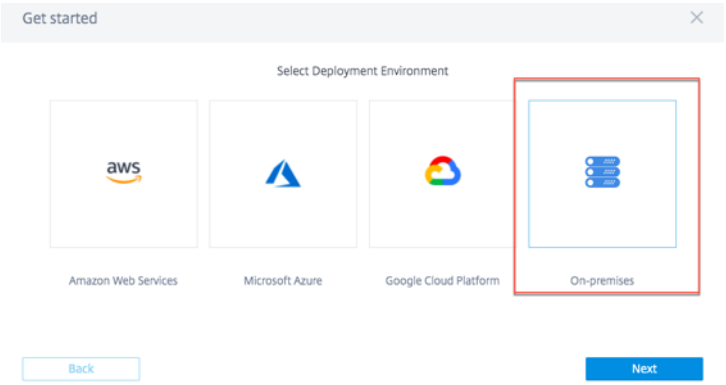
1. Select a device profile.

   > **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:

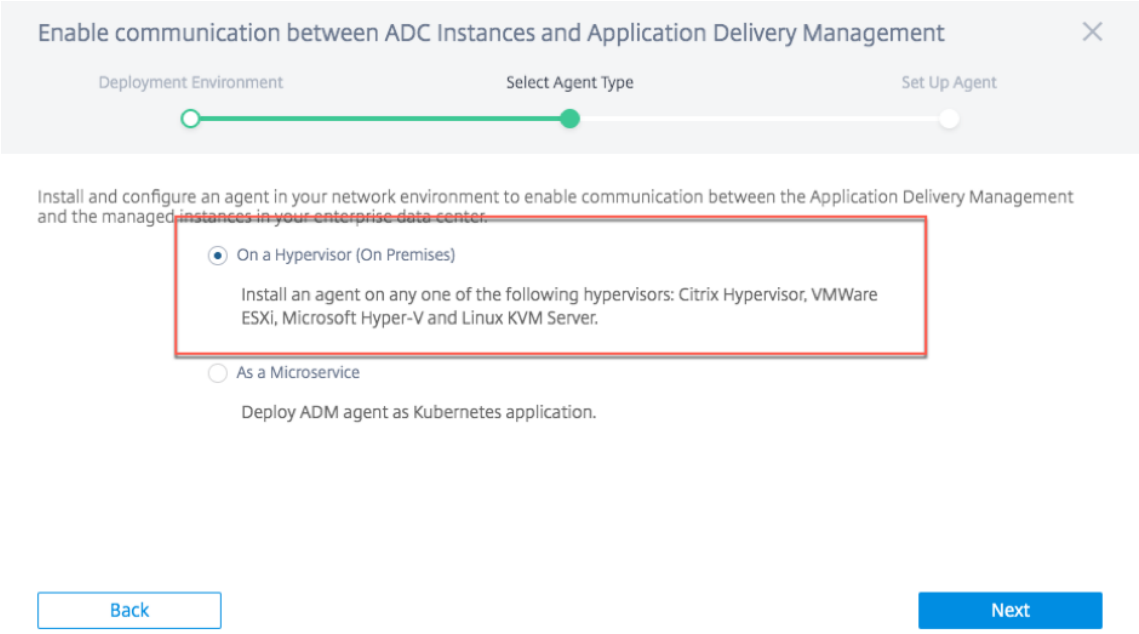
   - Amazon Web Services
   - Microsoft Azure
   - Google Cloud Platform
   - On-premises

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.

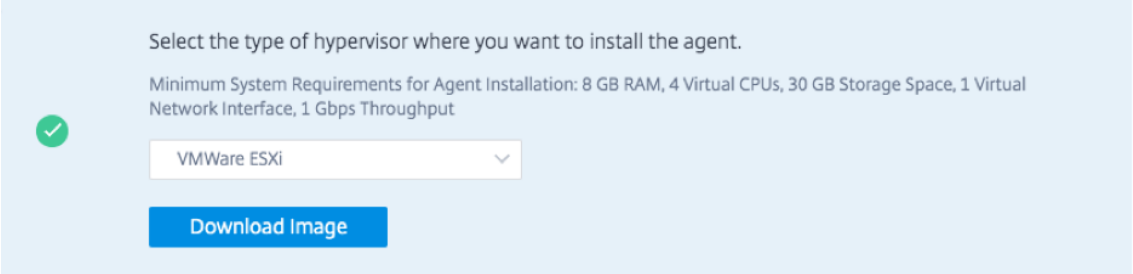


1. Select **On a Hypervisor (On Premises)** and click **Next**.

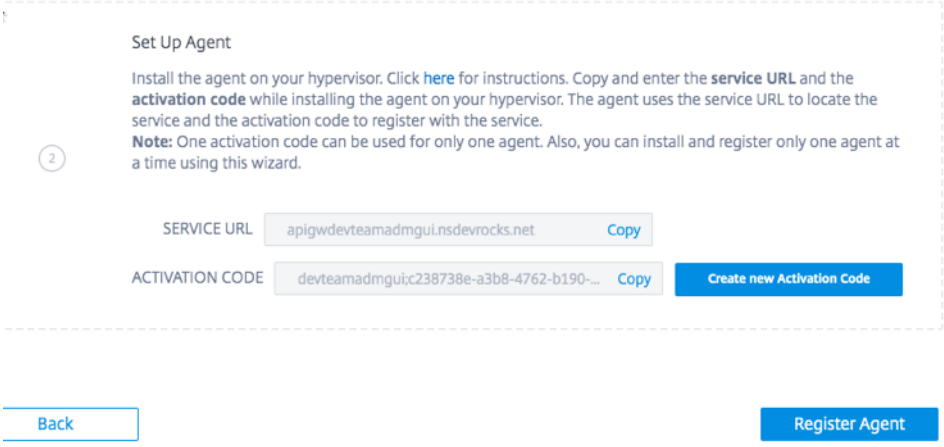
© 1997–2025 Citrix Systems, Inc. All rights reserved.



2. Select the hypervisor type and download the image, for example, VMware ESXi.



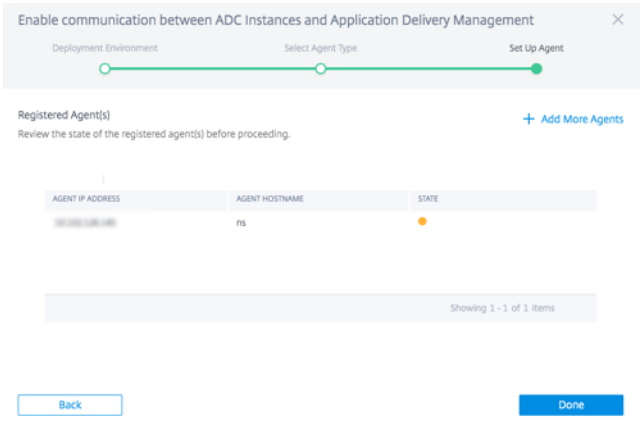
3. Use the service URL and activation code to configure the agent.



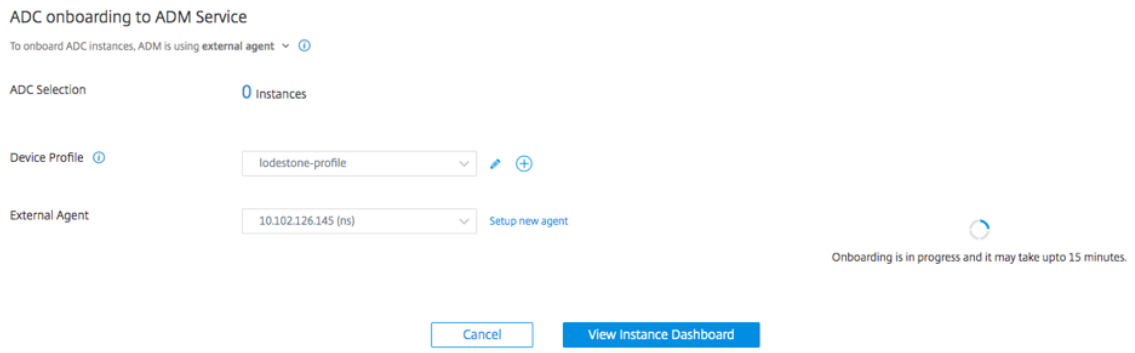
The agent uses the service URL to locate the service and the activation code to register with the service. For detailed instructions about installing an agent on your on-premises hypervisor, see Install a NetScaler agent on-premises

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.



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:

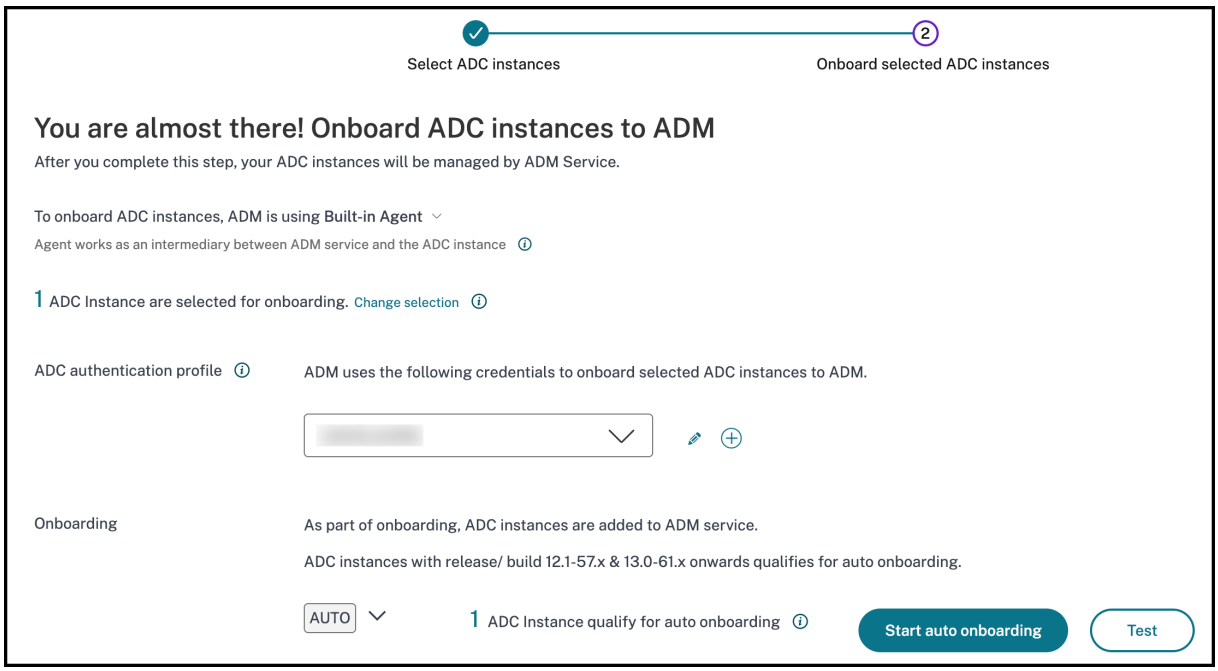
- Install an agent on Microsoft Azure cloud
- Install an agent on AWS
- Install an agent on GCP

© 1997–2025 Citrix Systems, Inc. All rights reserved.

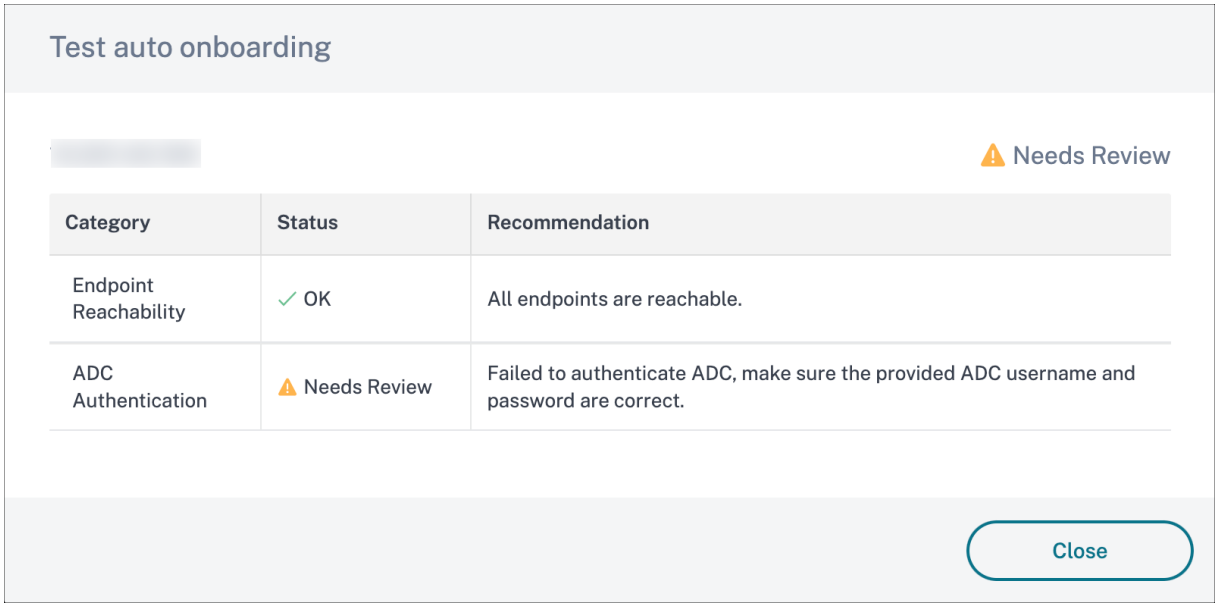
Test onboarding readiness of NetScaler instances

July 31, 2024

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.



Click **Test** to start the diagnostic dry run. The **Test auto onboarding** page displays the issue category, status, and recommendation.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

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`
  - `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

March 7, 2025

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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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.

> **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.

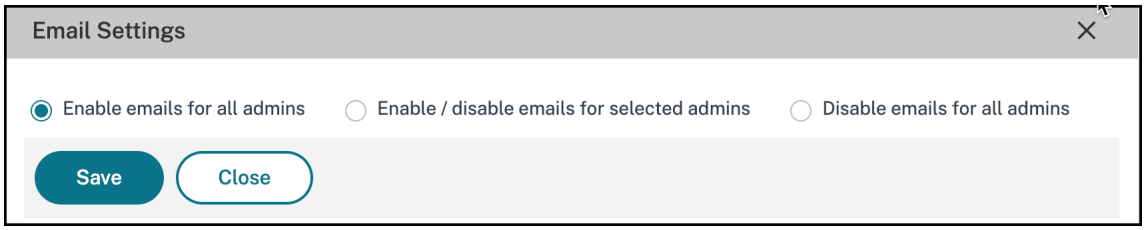
3. In the NetScaler Console landing page, click **Next**.

   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.

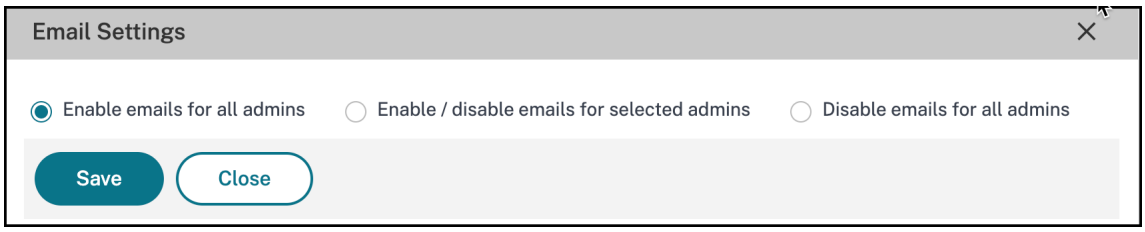
If you are already on the NetScaler Console GUI and you want to configure the email settings:

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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

3. Click **Email Settings**. The **Email Settings** pane appears.



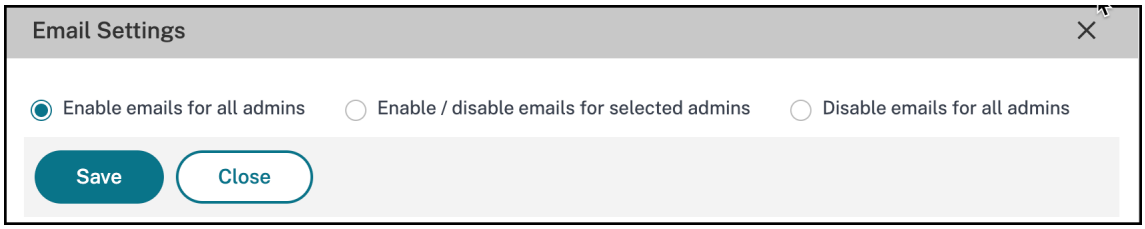
You can now configure the email settings to enable or disable emails.

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.

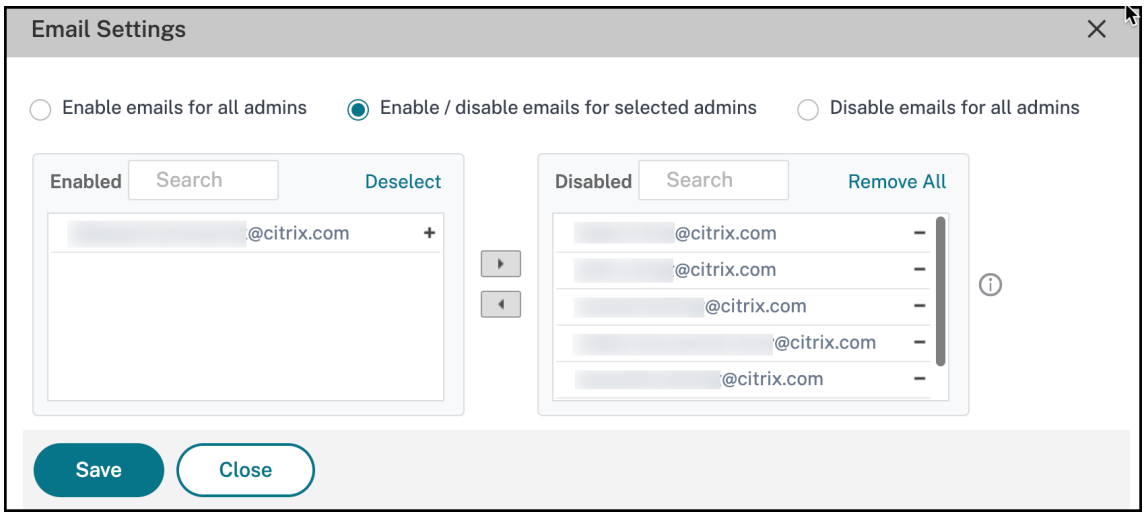
Enable / disable emails for specific admins in the org

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 (**+**).

© 1997–2025 Citrix Systems, Inc. All rights reserved.



You will see the admin email address added to the **Disabled** list.

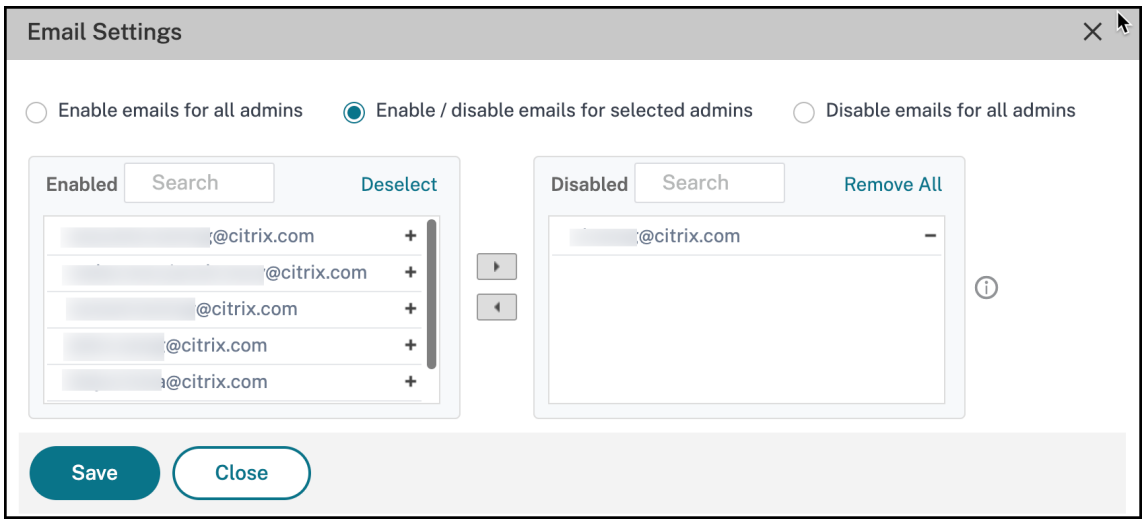
3. Click **Save** and **Close**.

   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.



© 1997–2025 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.

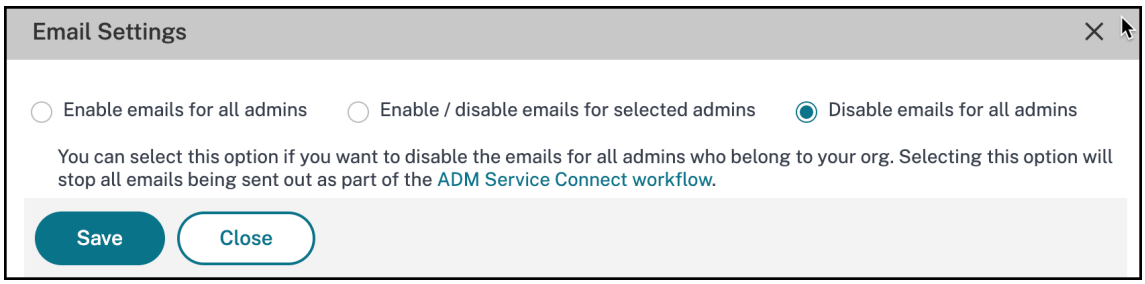
   > **Note:**
   >
   > If you want to enable emails for multiple admins, select all their email IDs in the **Disabled** email list, and click the remove button (-) to add the email IDs to the **Enabled** list. Click **Save** and **Close**.

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.

Troubleshoot issues using the diagnostic tool or the NetScaler Console GUI

January 8, 2024

> 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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`.

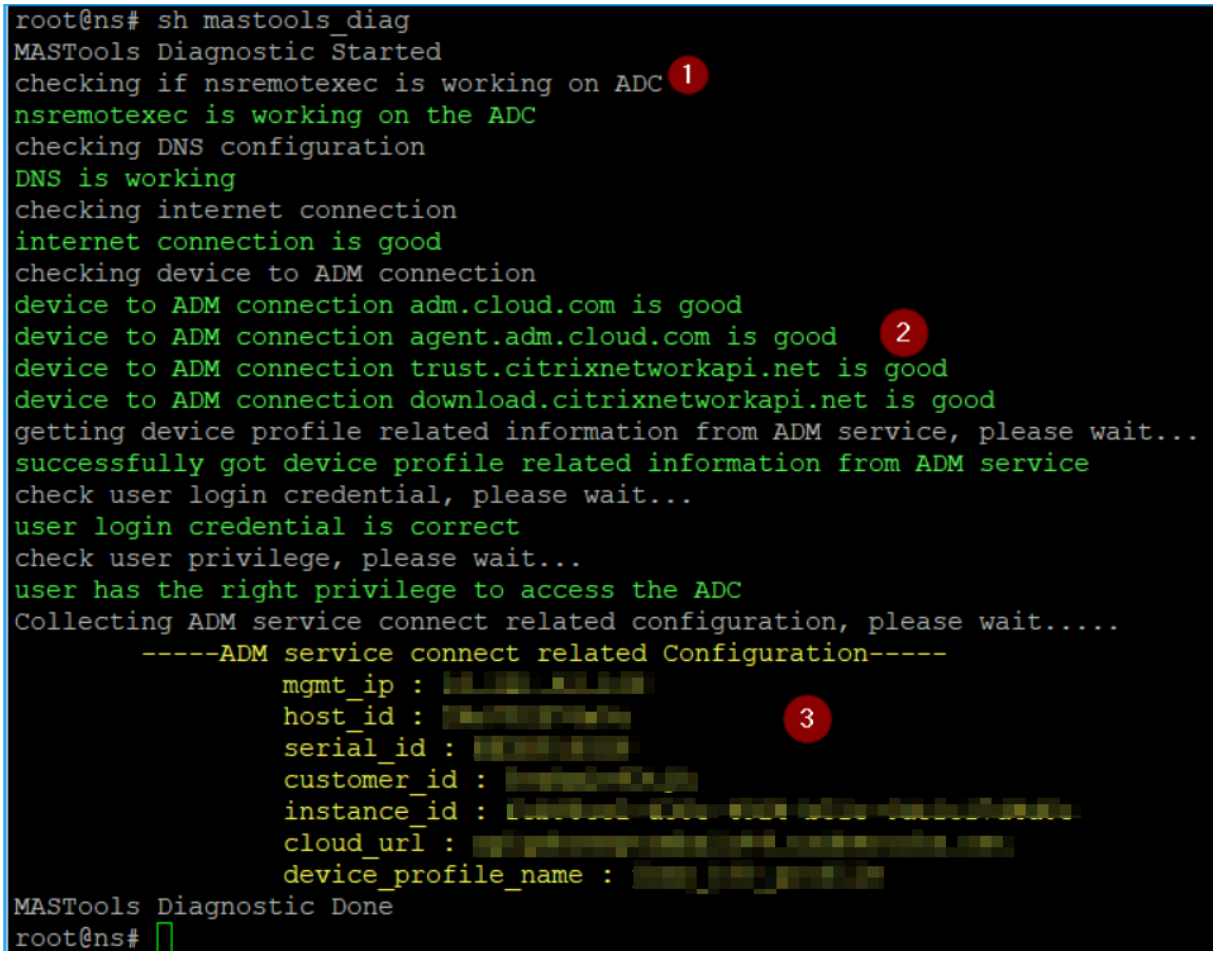
The tool starts and displays the results for the following diagnostic checks:

- **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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

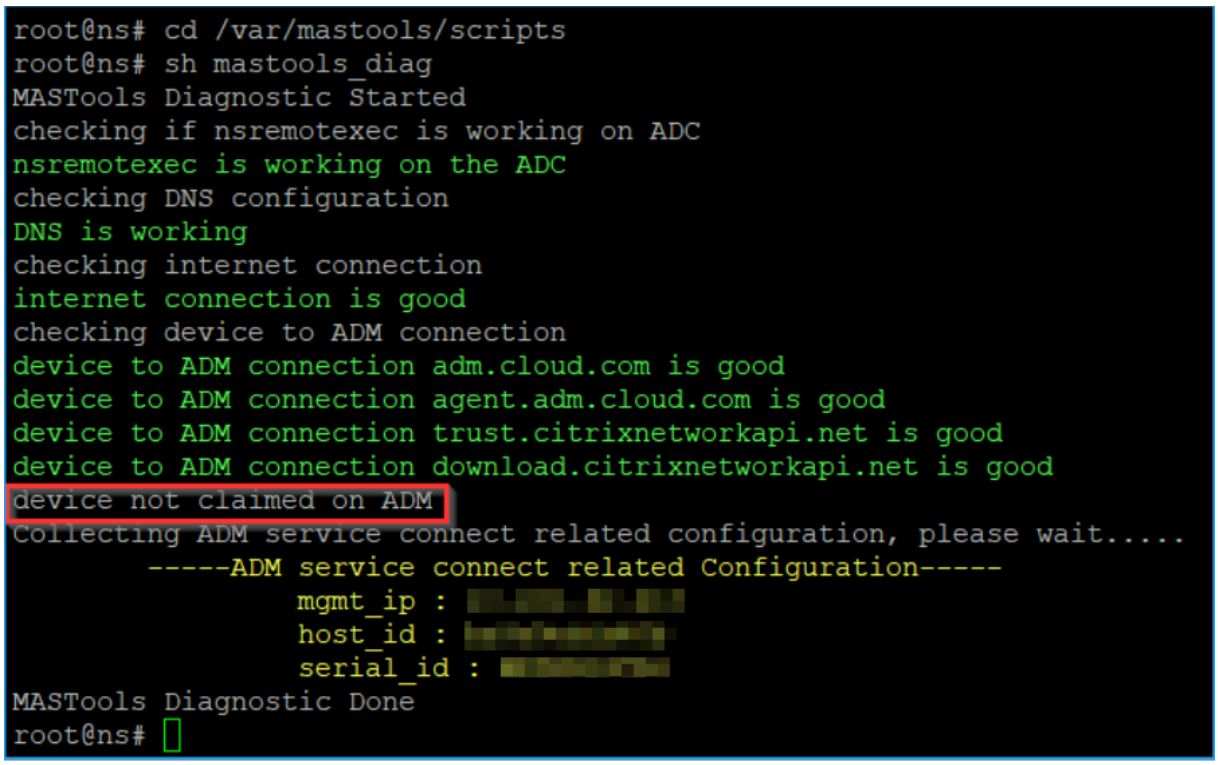


- **1** –Displays the type of diagnostic check
- **2** –Displays the diagnostic check results either in green or in red. Green indicates the result is successful and red indicates the result is not successful.
- **3** –Displays the NetScaler Console configuration information in yellow each time you run the diagnostic tool. If you want to contact NetScaler support, you must provide this information.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



View NetScaler diagnostic information in NetScaler Console GUI

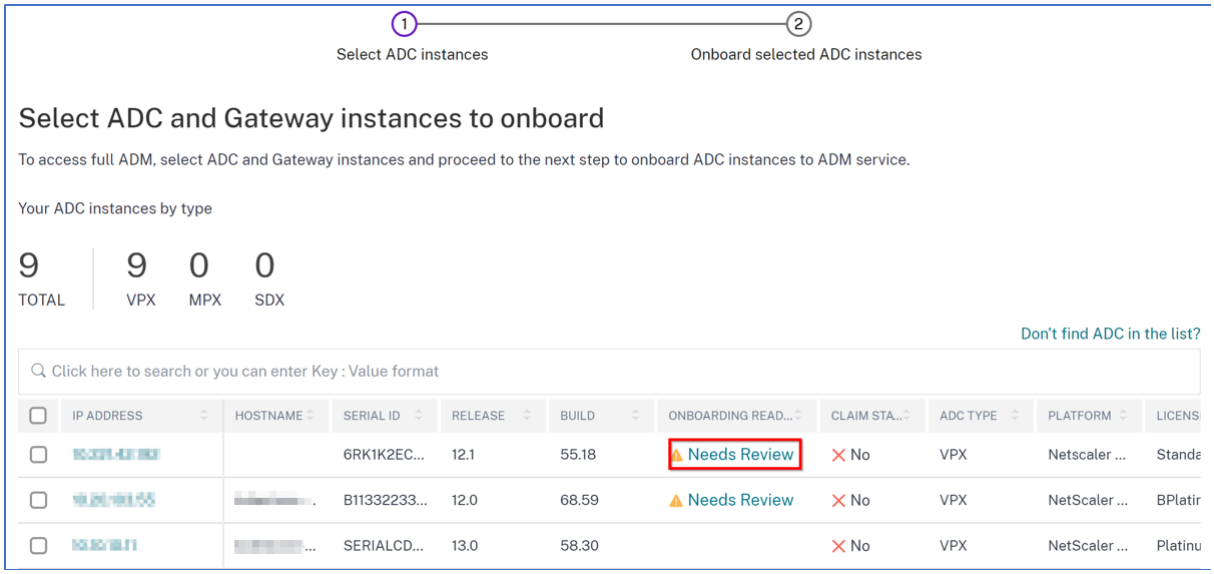
Navigate to **Infrastructure > Instances > NetScaler** and click **Asset Inventory** to see the newly added **Onboarding Readiness** option that provides the NetScaler instance onboarding readiness status such as **Needs Review** or **OK**.

- **Needs Review**. The NetScaler instance has issues that need to be fixed.
- **OK**. The NetScaler instance is ready to onboard.

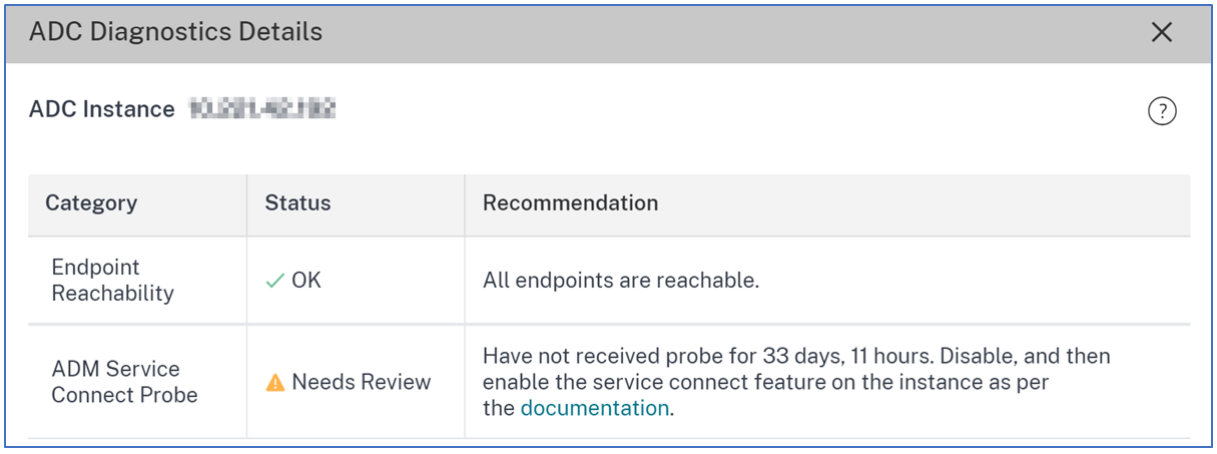
> **Note:**
>
> If the **Onboarding Readiness** appears blank, it means the NetScaler instance is not running with the latest image that has diagnostic support.

If the NetScaler instance has any issues, the **Needs Review** option appears, and you can click to view more details.

© 1997–2025 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.

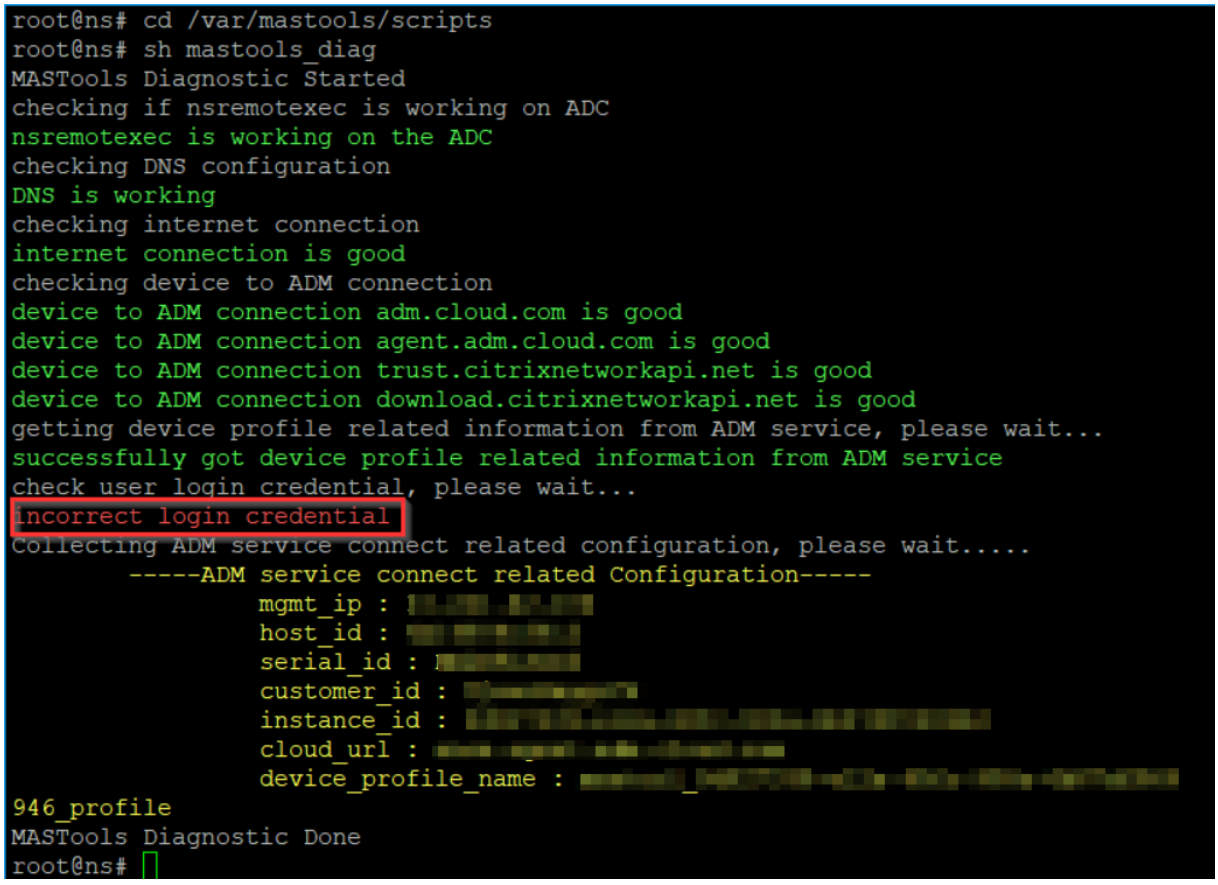
After you fix the issue, the status in the Onboarding Readiness gets changed to **OK**.

Troubleshoot

The following are some of the NetScaler instance issues and their troubleshooting steps:

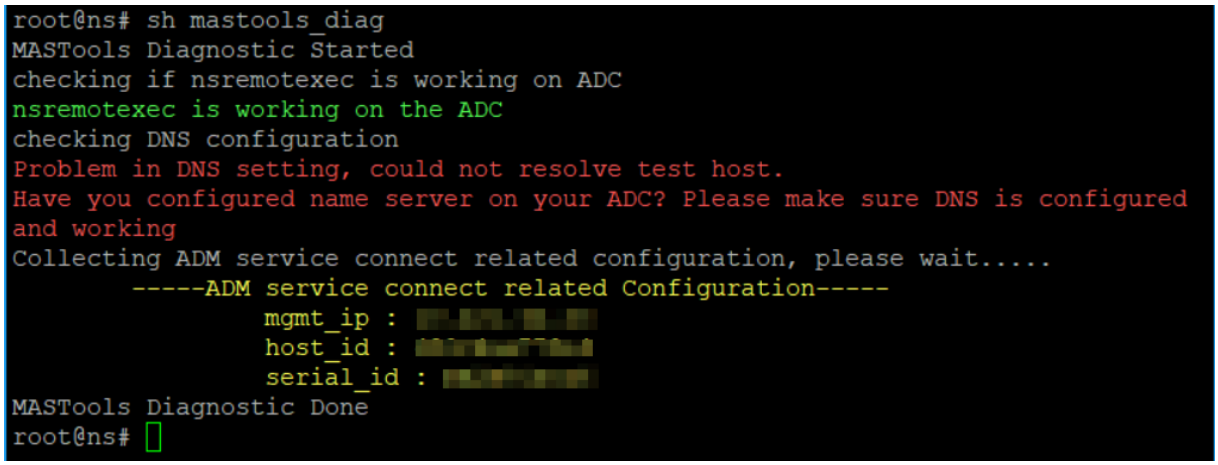
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Workaround: Ensure the DNS is configured or the DNS IP address is valid. For more information, see DNS configuration.

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"
```

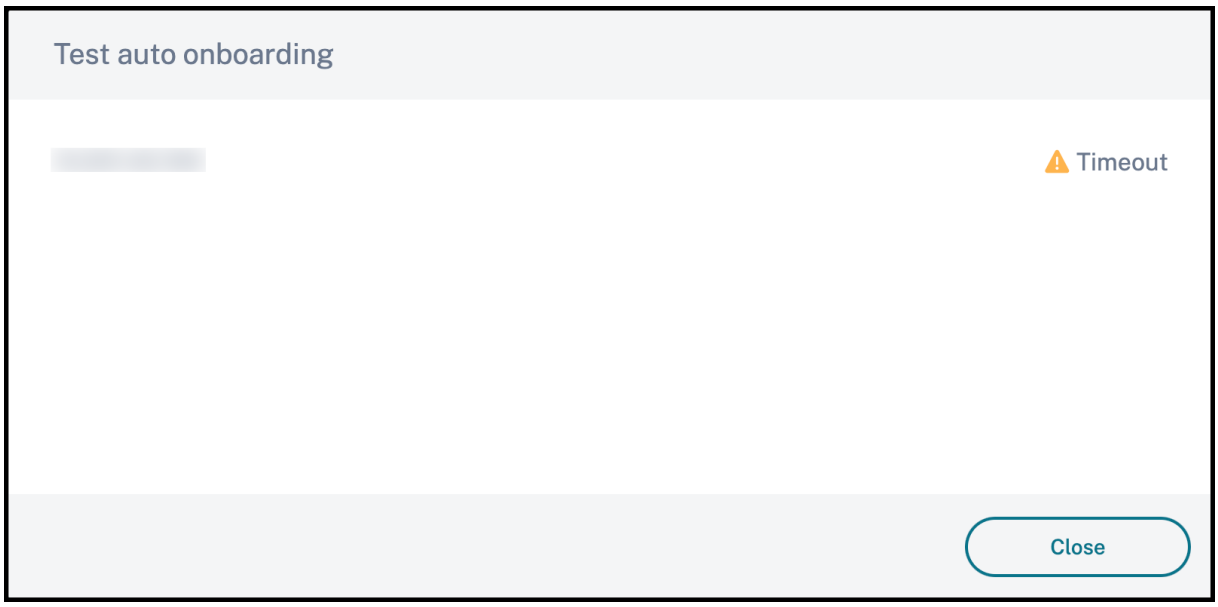
If no issue found in the diagnostic checks and the no connection issue still persists, make a note of the NetScaler Console configuration information (available in yellow) and contact NetScaler support.

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.

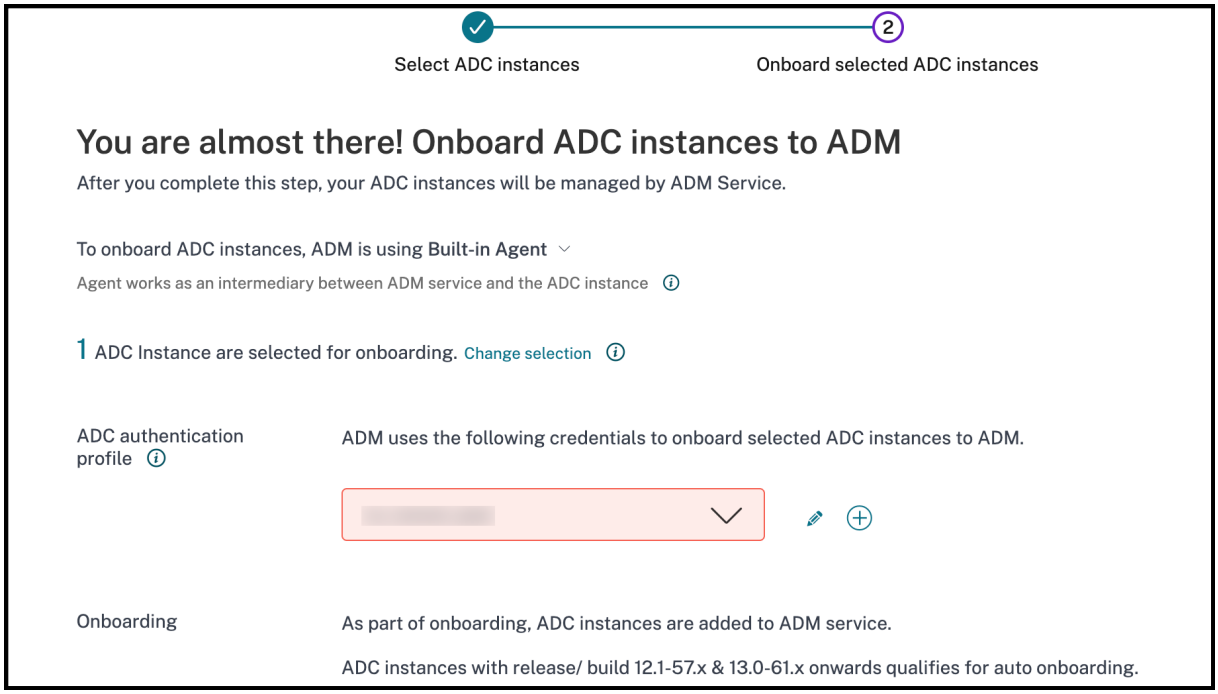
© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Recommendation: Re-enter the NetScaler user admin credentials again, create the device profile and click Test to run the dry run again.

Transition from a built-in agent to an external agent

January 8, 2024

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.

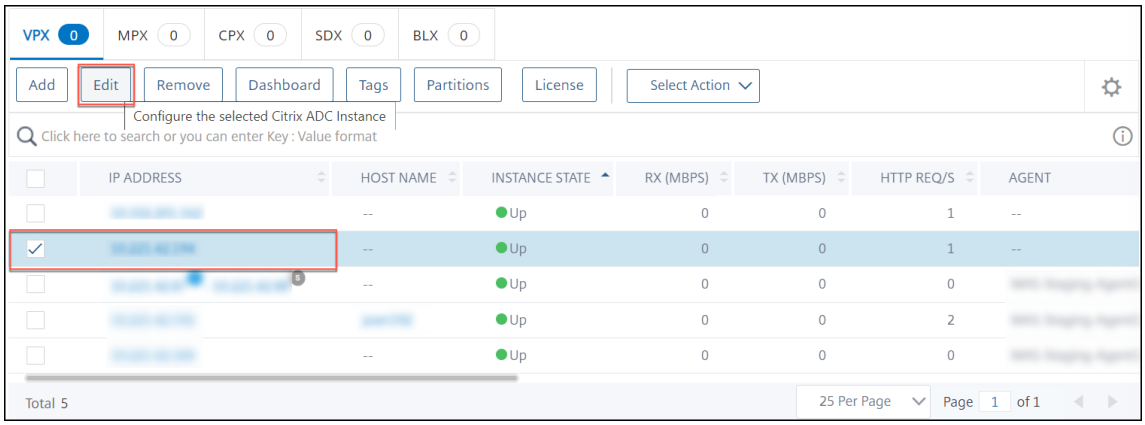
Before you start

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

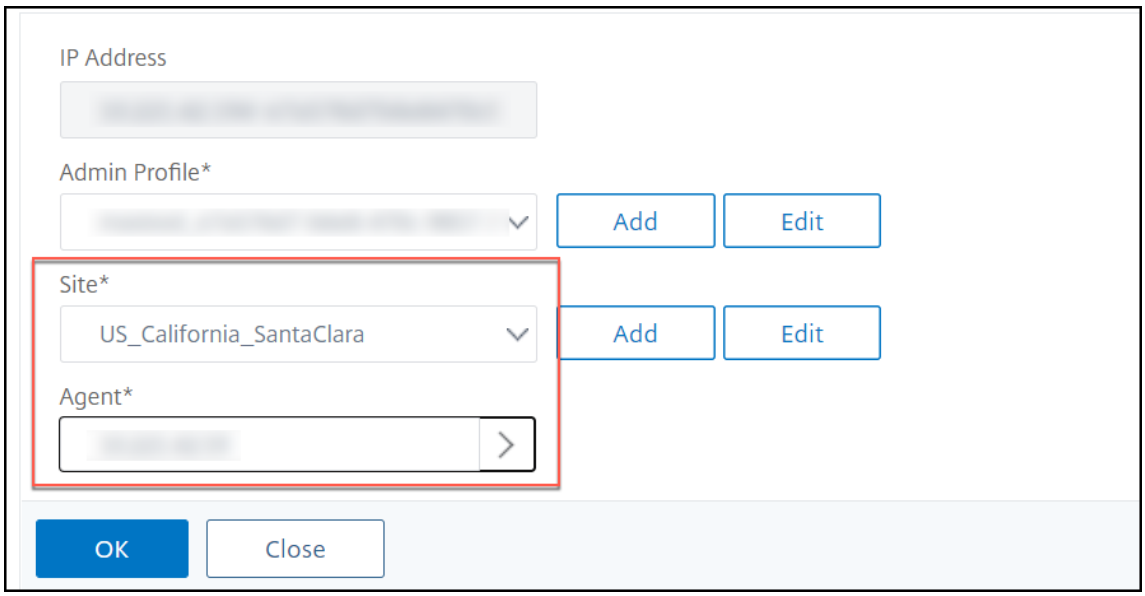
Follow these steps to transition from a built-in agent to an external agent:

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**.

© 1997–2025 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

Connect SAML as an identity provider to NetScaler Console

January 8, 2024

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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.
- 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

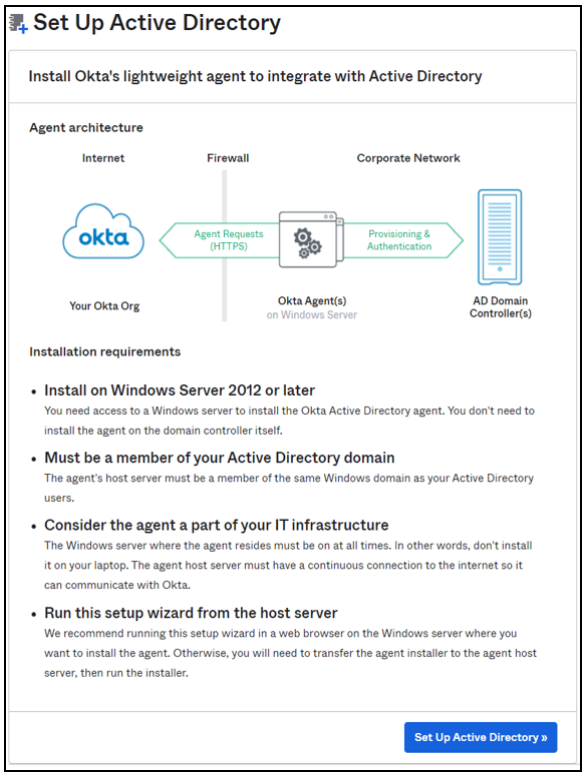
© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - 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**.



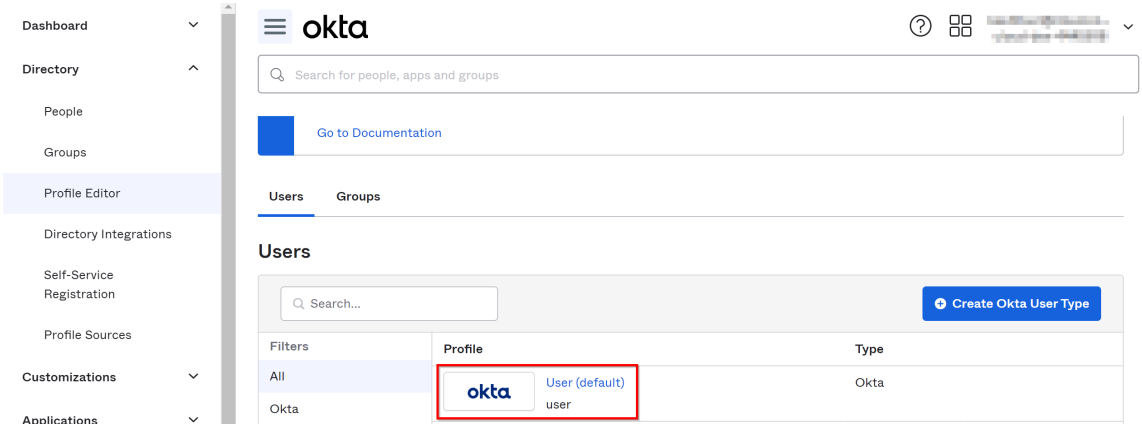
For a successful integration, the SAML identity provider must pass Citrix Cloud certain Active Directory attributes of the user in the SAML assertion. Specifically,

- Security Identifier (SID)
- objectGUID (OID)
- user Principal Name (UPN)
- Mail (Email)

1. Log on to Okta with administrator credentials.

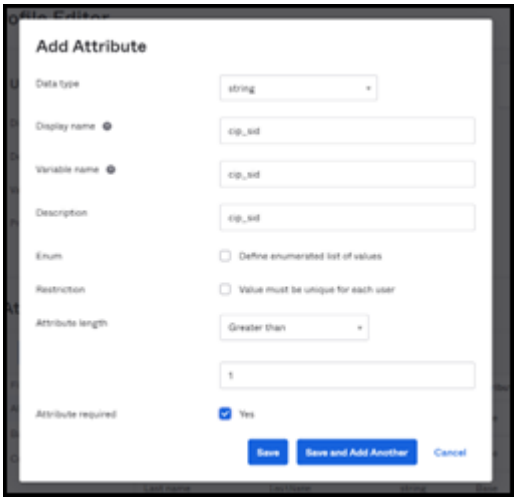
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

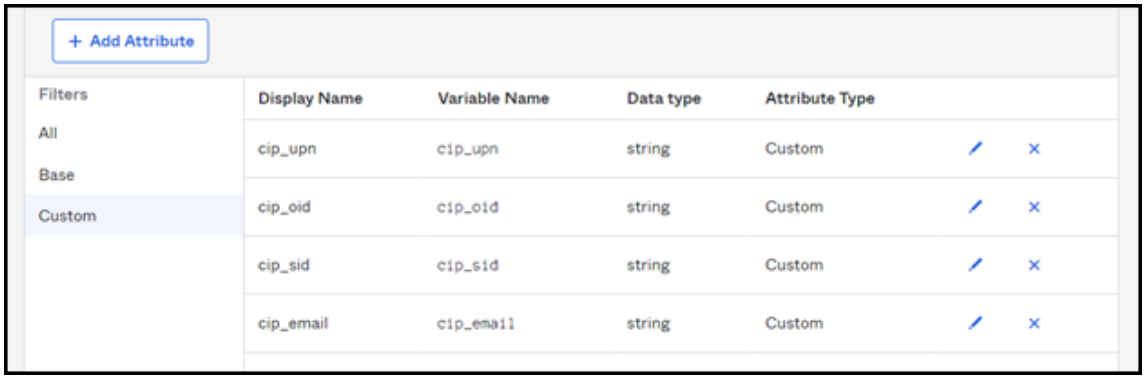
   - `cip_sid`
   - `cip_upn`
   - `cip_oid`
   - `cip_email`



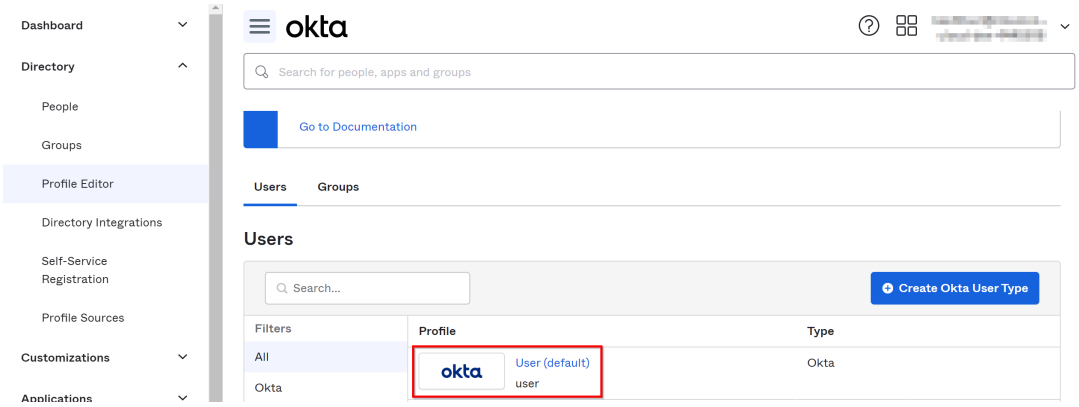
   Click **Save and Add Another** and repeat the process to create 4 custom attributes.

   You can view the following details after creating 4 custom attributes:

© 1997–2025 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.



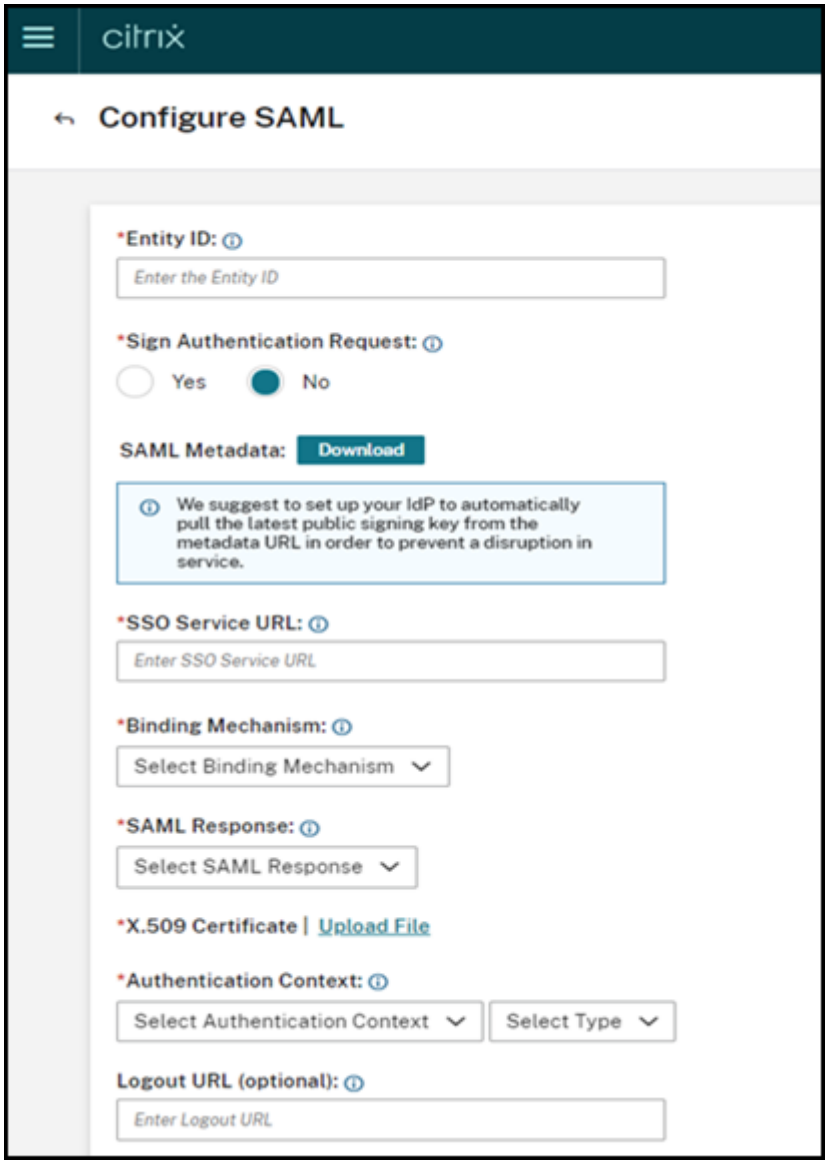
   d) In the **Okta User User Profile** column, map the Active Directory attributes to the custom attributes you have created:
      i. For `cip_email`, select email from the User Profile column for your domain. When selected, the mapping appears as `appuser.email`.
      ii. For `cip_sid`, select **objectSid** 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`.
      iv. For `cip_oid`, select `externalId` from the **User Profile** column for your domain. When selected, the mapping appears as `appuser.externalId`.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.



   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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:

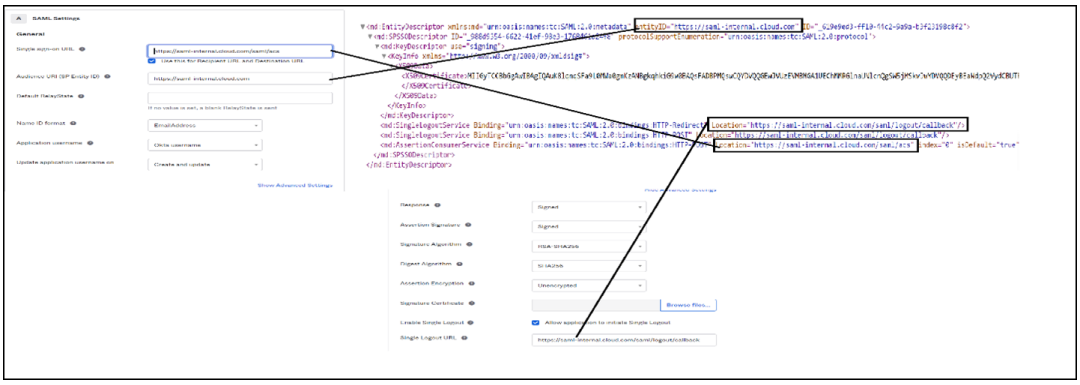
    a) Provide the URL details for **Single sign-on URL** as `https://saml-internal.cloud.com/saml/acs` and **Audience URI (SP Entity ID)** as `https://saml-internal.cloud.com`.

    > **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**.

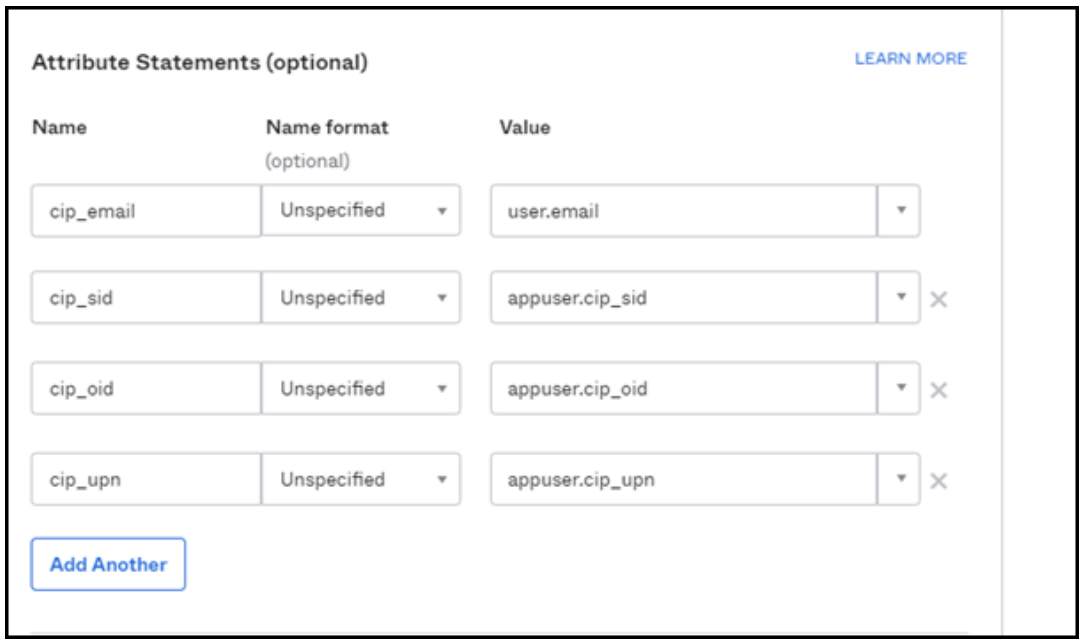
    c) Select **Okta Username** for **Application Username**.

    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.

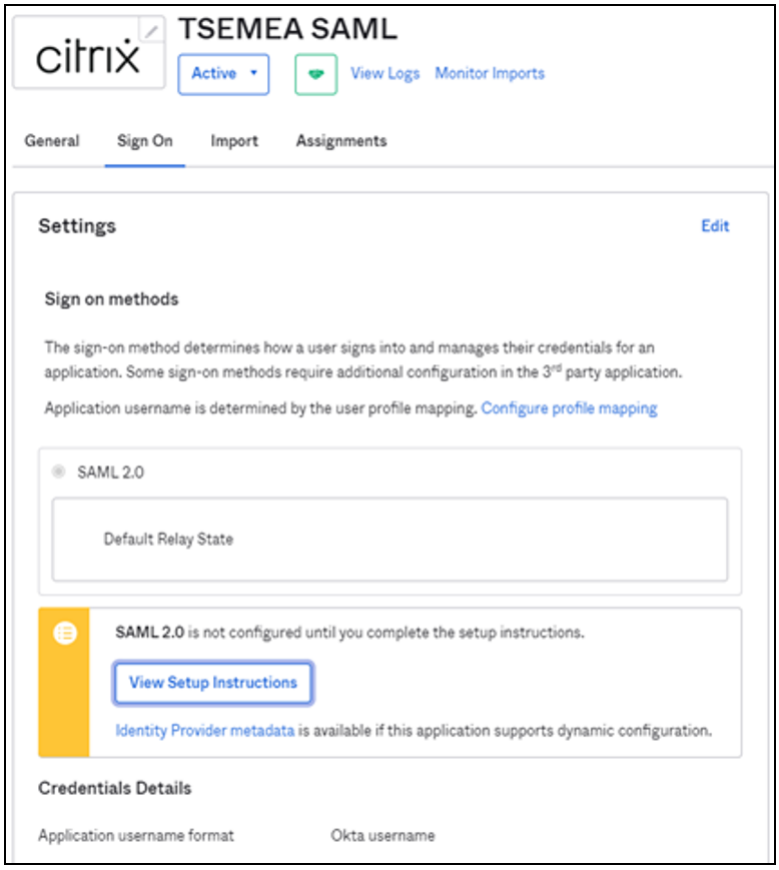
© 1997–2025 Citrix Systems, Inc. All rights reserved.



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**.

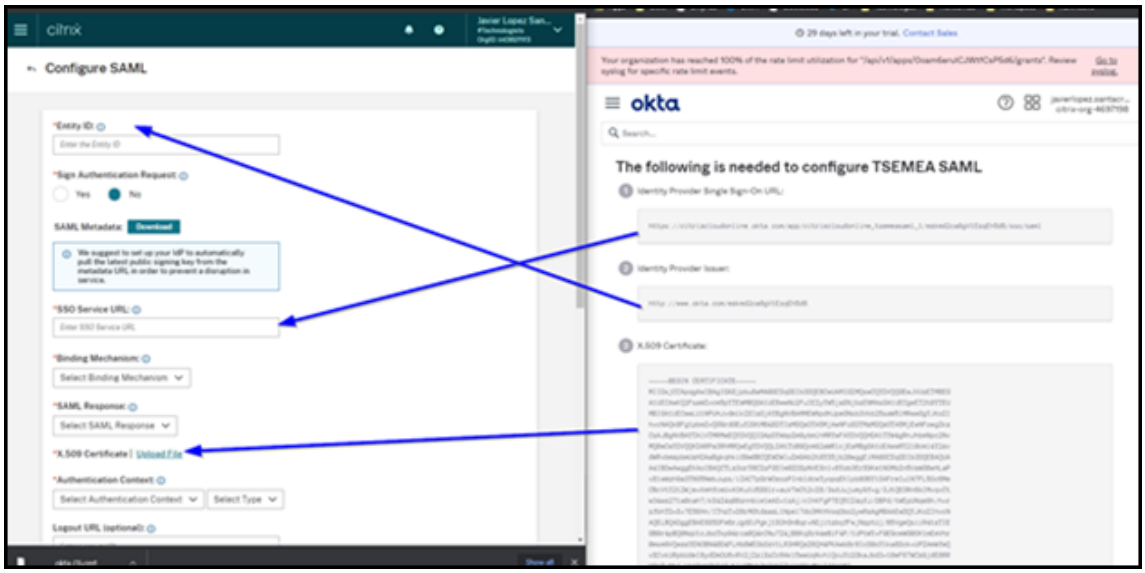


© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

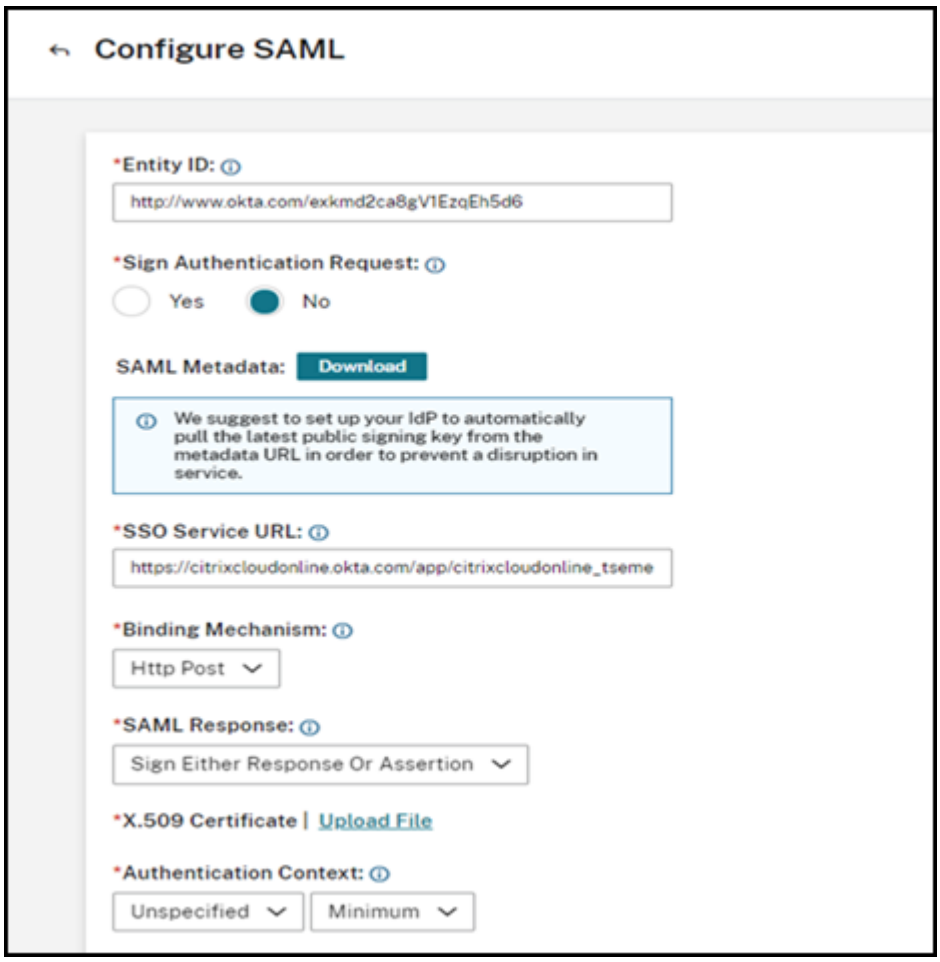
15. You must now return to the **Configure SAML** page in Citrix Cloud and complete the remaining configuration as mentioned in the following:



Use the downloaded certificate and rename the file name extension from `.cert` to `.crt` to upload it to Citrix Cloud.

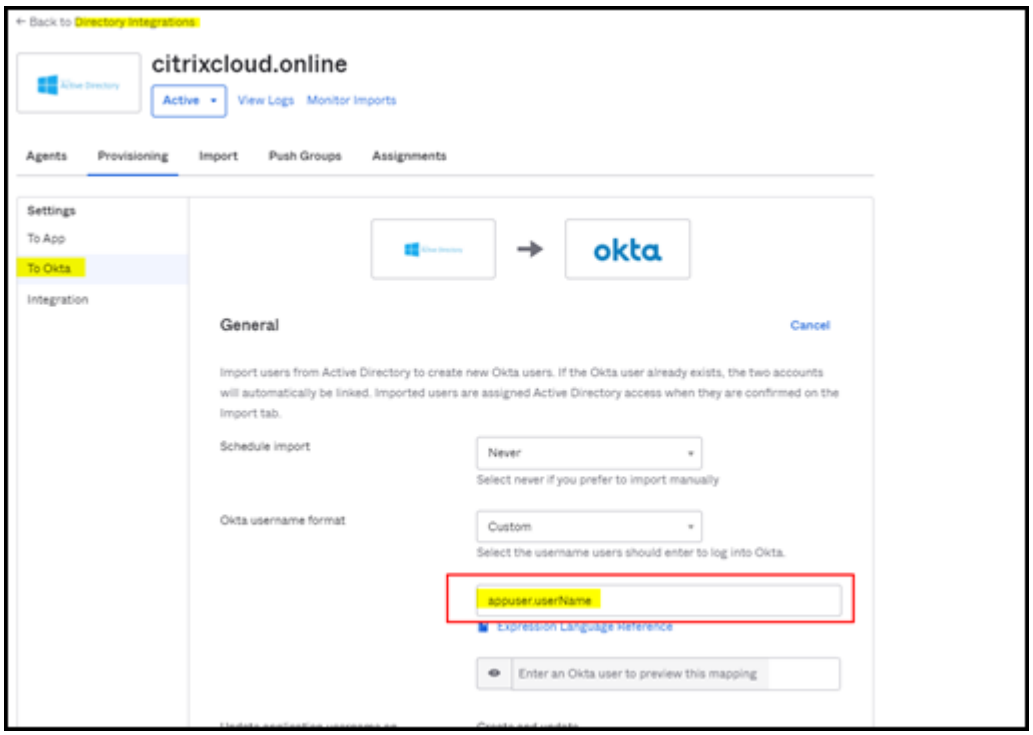
16. After you upload the certificate, use all other options that are by default:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



17. Next, you must ensure `appuser.userName` is defined at **Directory-integrations > Active Directory -> Provisiong > To okta**.

© 1997–2025 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:

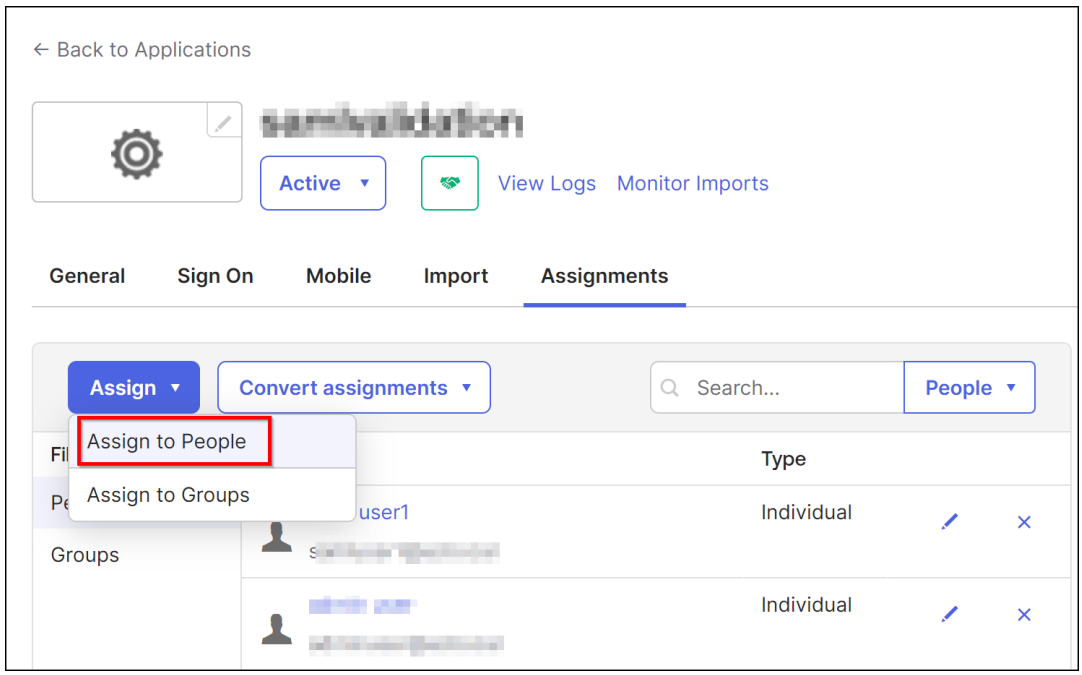
    a) Log on to Okta with administrator credentials

    b) Navigate to **Applications > Applications**

    c) Select the SAML application that you created

    d) Click **Assign > Assign to People**

© 1997–2025 Citrix Systems, Inc. All rights reserved.



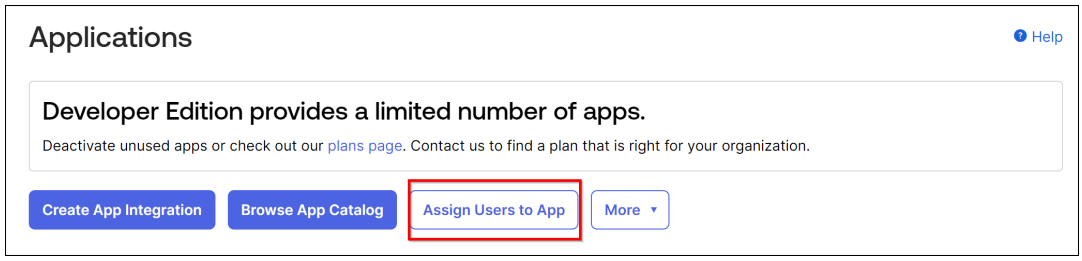
e) Click **Assign** and then select **Save and Go back**.

f) Click **Done**.

Method 2:

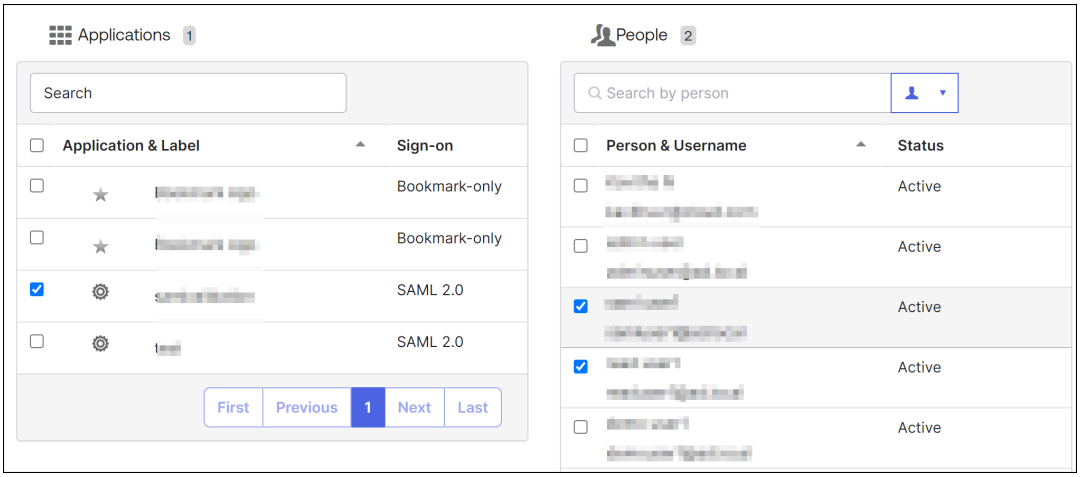
a) Navigate to **Applications > Applications**.

b) Click **Assign Users to App**.



c) Select the application and users, and then click **Next**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



d) Click **Confirm Assignments**.

Method 3:

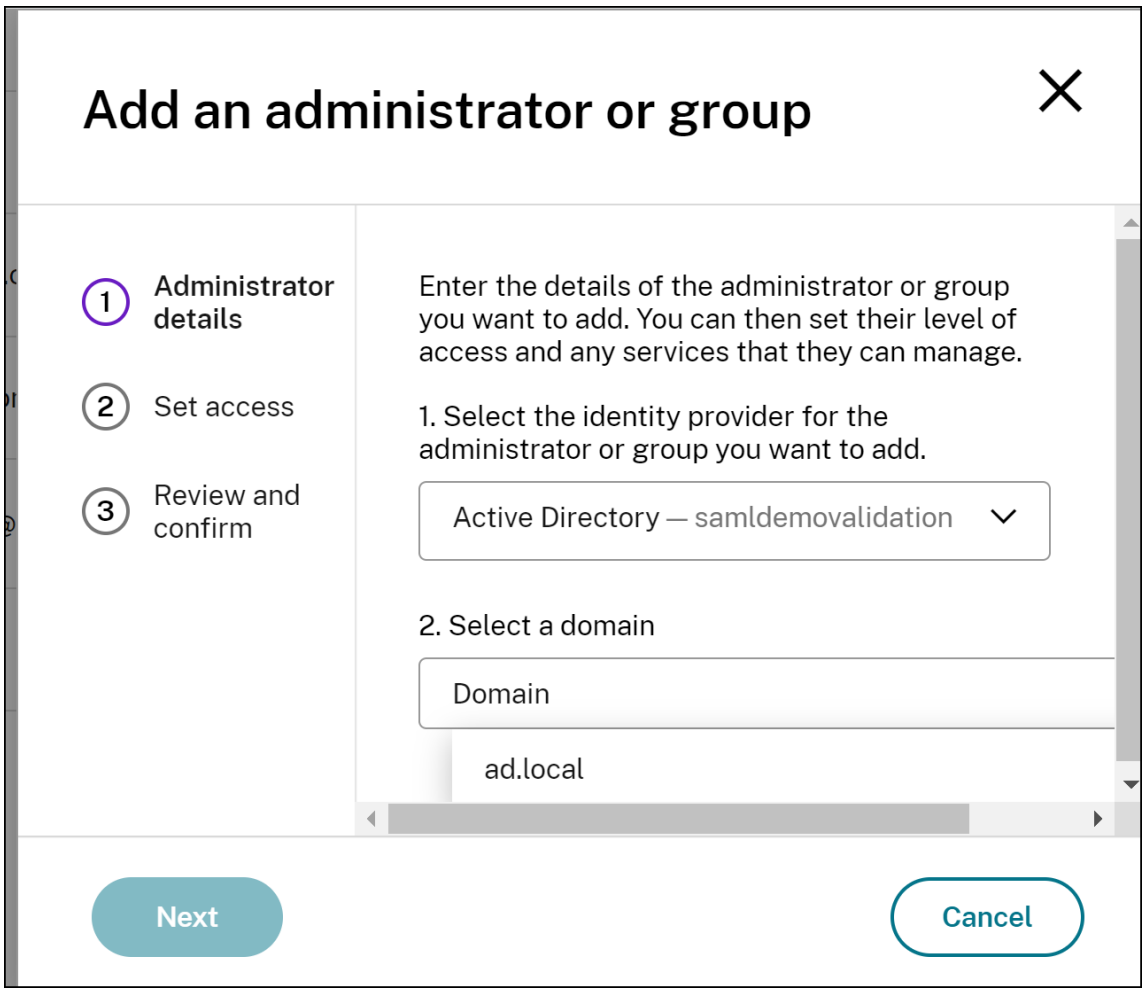
a) Navigate to **Directory > People**.

b) Select any user.

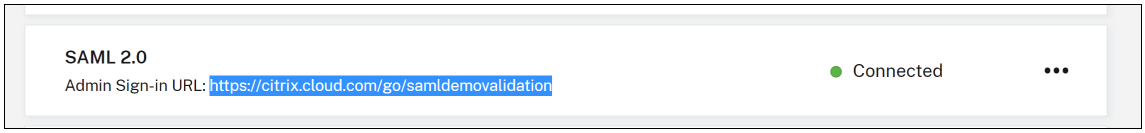
c) Click **Assign Applications** and assign the SAML application to the user.

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 - [your SAML app name]** from the list, select the domain, and then click **Next**.

© 1997–2025 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:



System requirements

September 8, 2025

Before you begin using NetScaler Console, you must review the software requirements, browser requirements, port information, license information, and limitations.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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
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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.
> - 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Component	Requirement
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:

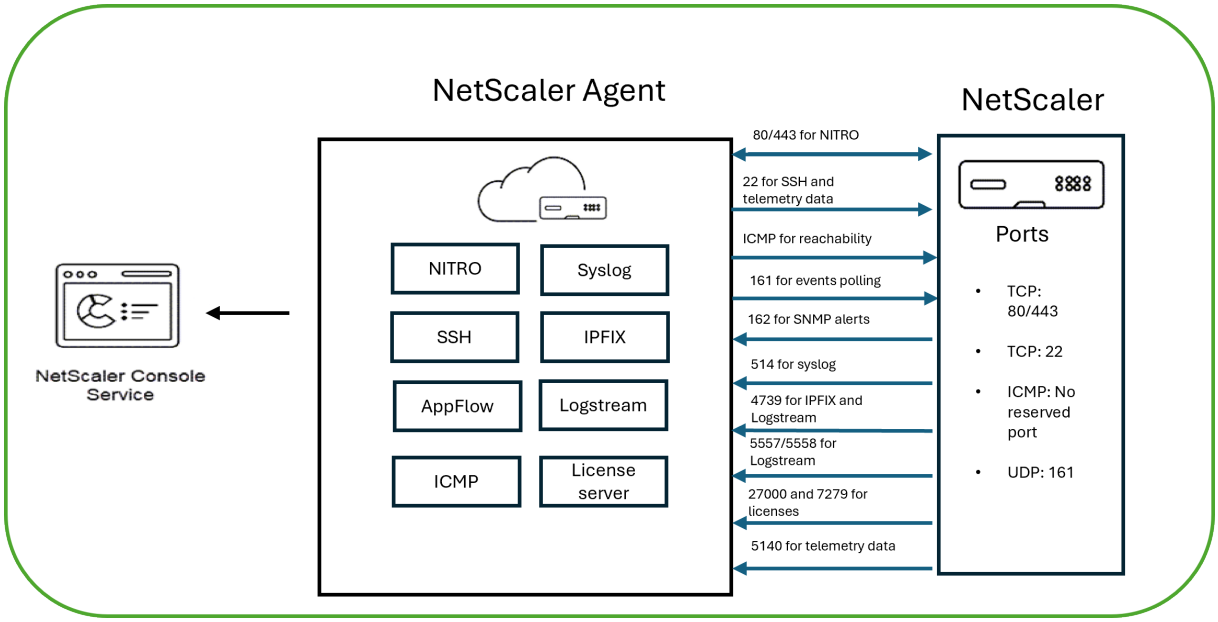
Cloud	Agent requirements	Preferred virtual machine type
AWS	4 virtual CPU, 8 GB RAM, and 30 GB storage space	`m4.xlarge`. This instance type provides 4 virtual CPU, 16 GB RAM, and 30 GB storage space. Citrix recommends this instance type since it matches most of the agent requirements among existing instance types.
Microsoft Azure	4 virtual CPU, 8 GB RAM, and 30 GB storage space	`Standard_F4s_v2`
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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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 Console service to NetScaler.	NetScaler agent to NetScaler and 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Port	Type	Details	Direction of communication
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
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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Service	Japan	Other regions (APEC, EU, and US)
Download service	https://download.citrixnetworkapi.net	https://download.citrixnetworkapi.net
Trust service	*.citrixnetworkapi.jp	*.citrixnetworkapi.net
	trust.citrixworkspacesapi.jp	trust.citrixworkspacesapi.net
Service URLs	*.agent.adm.citrixcloud.jp	*.agent.adm.cloud.com
	*.adm.citrixcloud.jp	*.adm.cloud.com
	adm.citrixcloud.jp	adm.cloud.com
Citrix Cloud connectivity	citrix.citrixcloud.jp	citrix.cloud.com
	accounts.citrixcloud.jp	accounts.cloud.com

Minimum NetScaler versions required

> Note
>
> NetScaler versions 10.5, 11.0, and 12.0 have already reached End Of Life (EOL). For more information, see the Product Matrix. The recommended NetScaler version is 12.1.

NetScaler Console Feature	NetScaler Software Version
StyleBooks	10.5 and later
Monitoring/Reporting and Configuring using Jobs Analytics	10.5 and later
HDX Insight	10.1 and later
Gateway Insight	11.0.65.31 and later
Security Insight	11.0.65.31 and later

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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
- 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

Licenses

November 20, 2024

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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)
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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

NetScaler Console Feature Group	NetScaler Console Features	NetScaler and Gateway License Requirement
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 virtual servers, services, service groups, servers)	N/A
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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.
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.

Upgrade Advisory

January 8, 2024

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

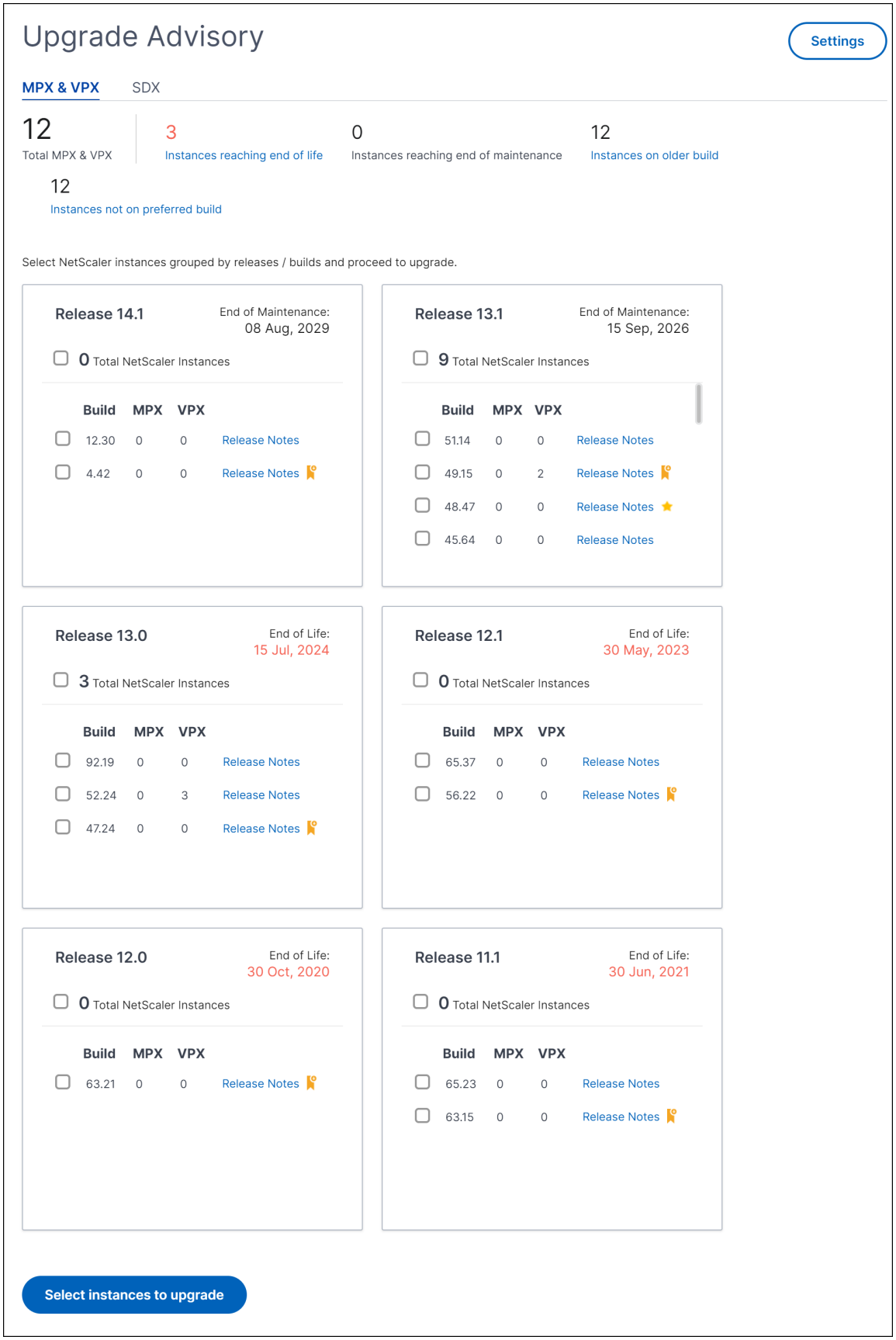
> **Important**
>
> Upgrade advisory only monitors EOL of NetScaler software releases. It doesn't check the EOL of NetScaler appliances.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



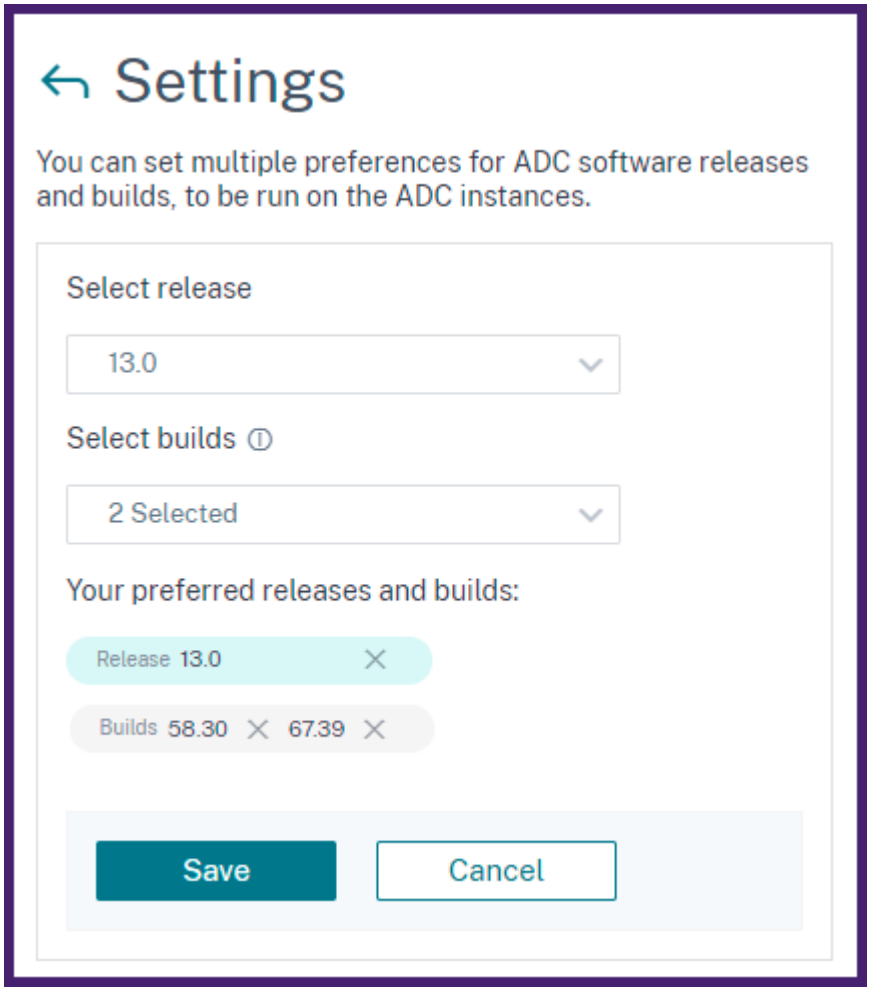
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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`.

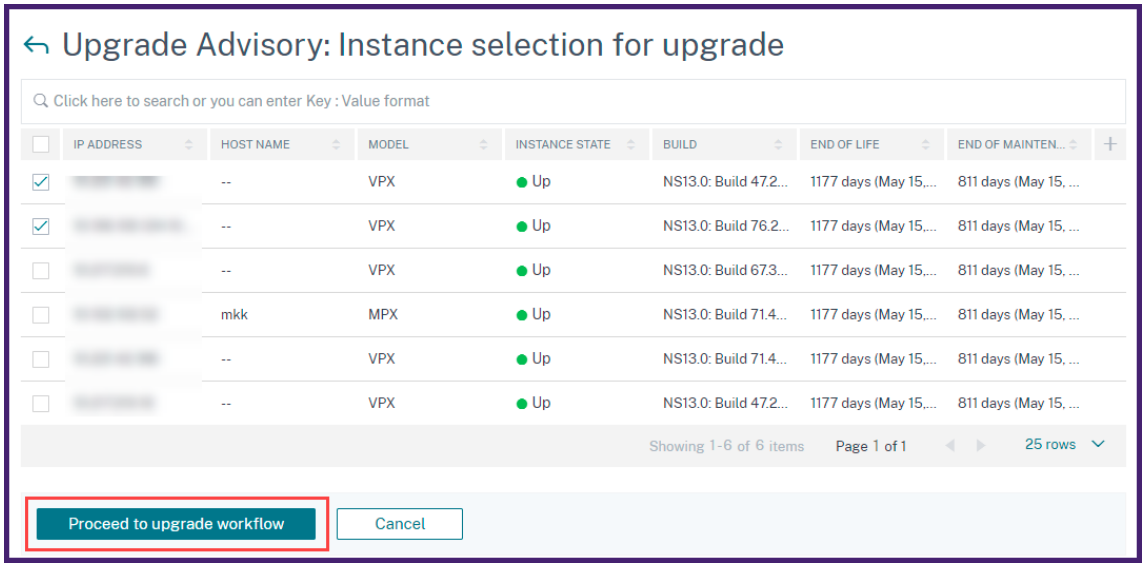
3. Click **Save**.

© 1997–2025 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:

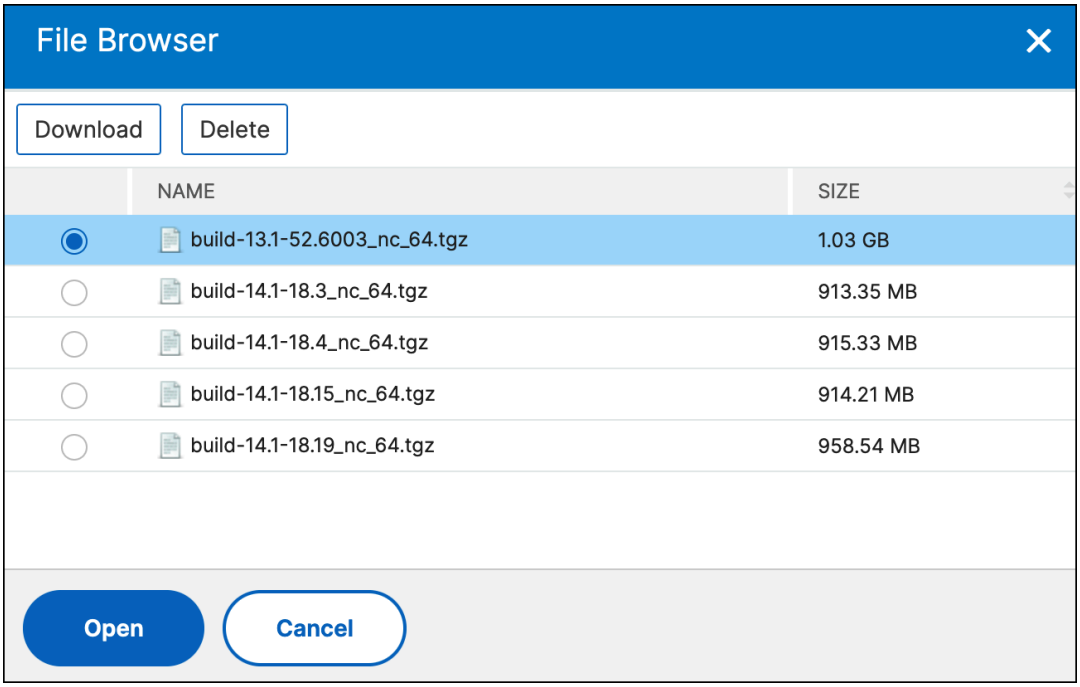
1. Select the instance builds that you want to upgrade and click **Select instances to upgrade**.
2. Select the NetScaler instance that you want to upgrade and click **Proceed to upgrade workflow**.



   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.

© 1997–2025 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.

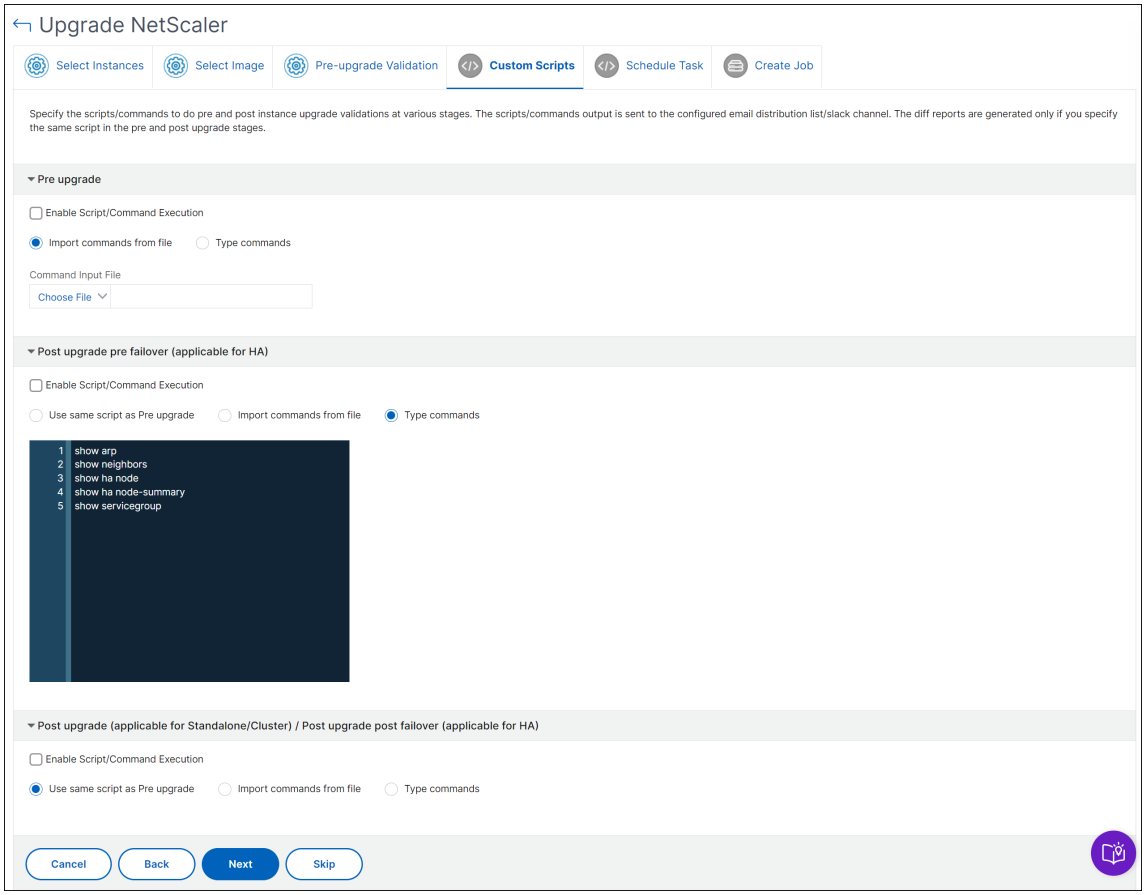
5. The **Pre-upgrade validation** tab displays the failed instances. you can remove the failed instances and click **Next**.

   - **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.

© 1997–2025 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.



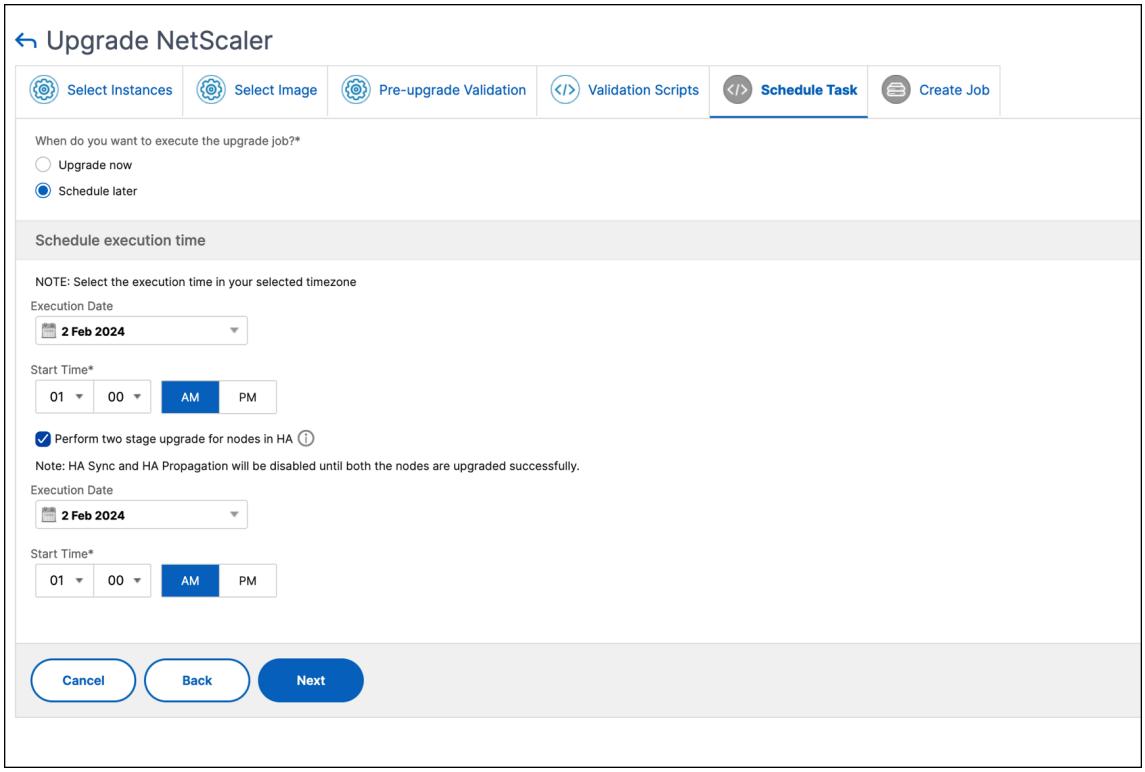
For more information, see Use custom scripts.

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.

© 1997–2025 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.

Security Advisory

August 19, 2025

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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

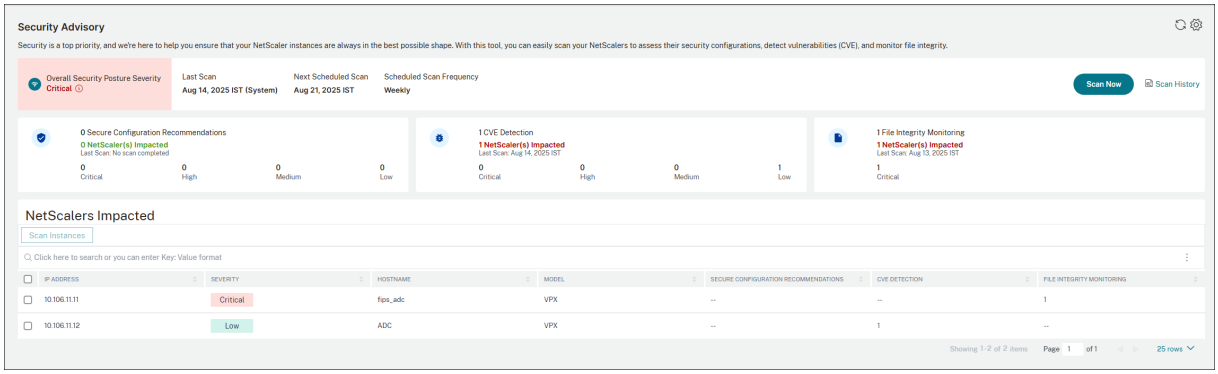
- Analyze your NetScaler configuration settings to identify any misconfigurations, weak points, or deviations from best practices that might expose your system to attacks.
- Track any new Common Vulnerabilities and Exposures (CVEs), assess the impact of CVEs, understand the remediation, and resolve the 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.



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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **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.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

CVE Detection

CVE detection primarily focuses on identifying and mitigating security vulnerabilities. For more information, see CVE Detection.

File Integrity Monitoring

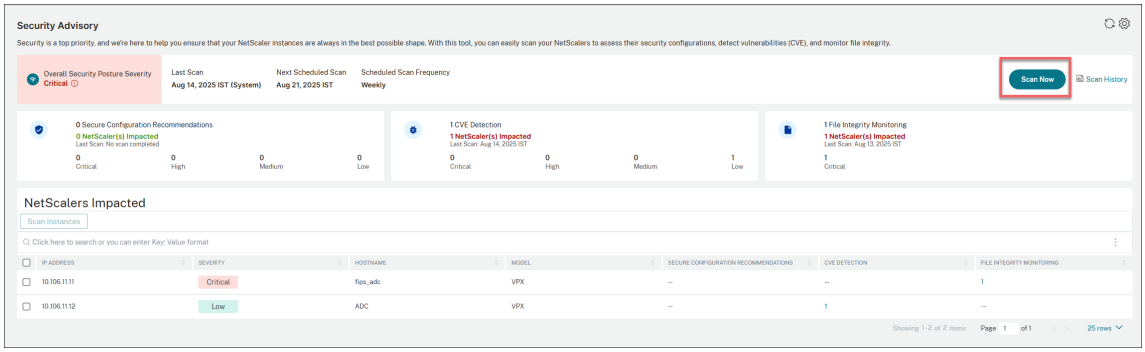
File integrity monitoring checks for unauthorized or malicious changes to the core files of a NetScaler instance. It's a key part of the security advisory. For more information, see File Integrity Monitoring.

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:

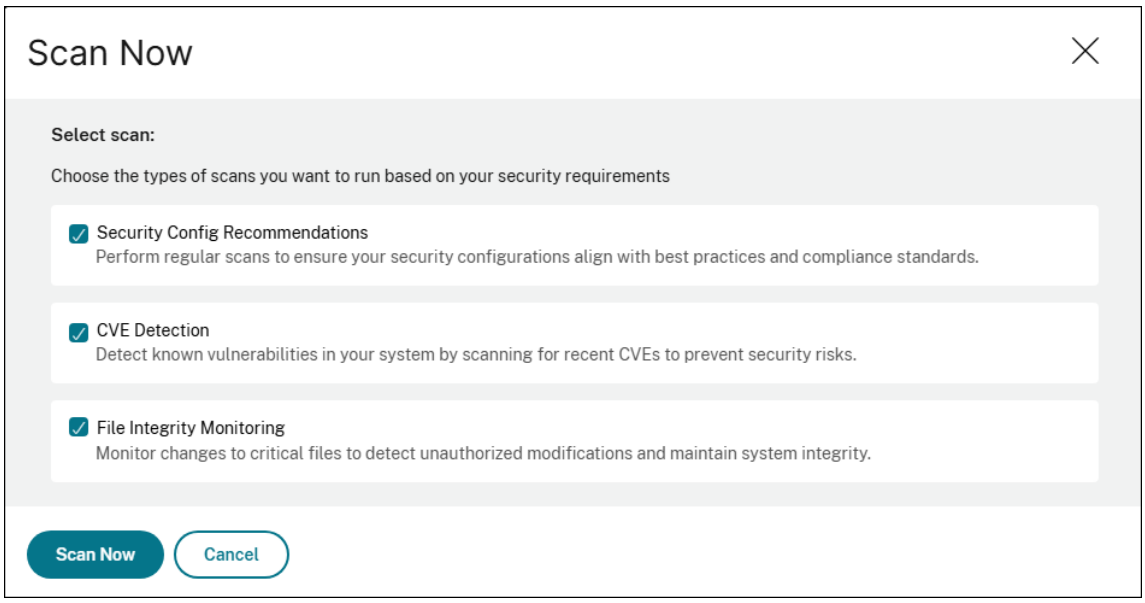
1. Click **Scan Now**.



2. Select the types of scans that you want to run.

   - Security Config Recommendations
   - CVE Detection
   - File Integrity Monitoring

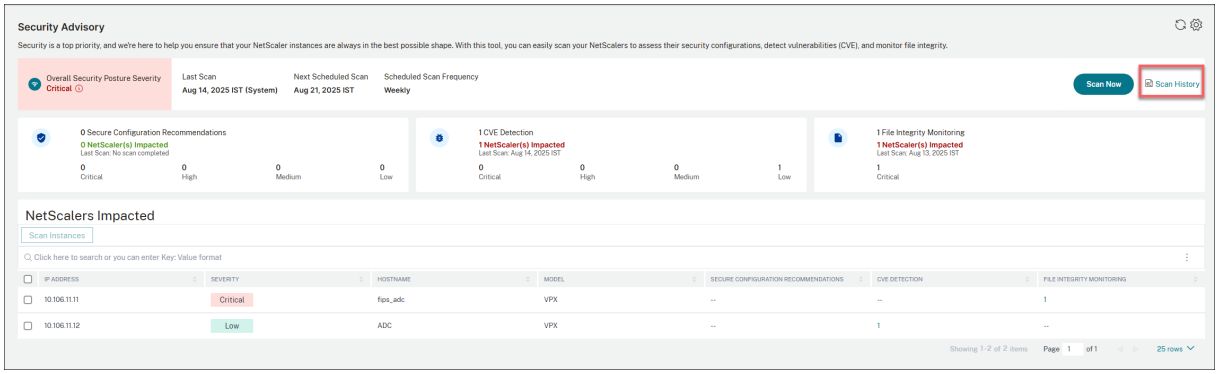
© 1997–2025 Citrix Systems, Inc. All rights reserved.



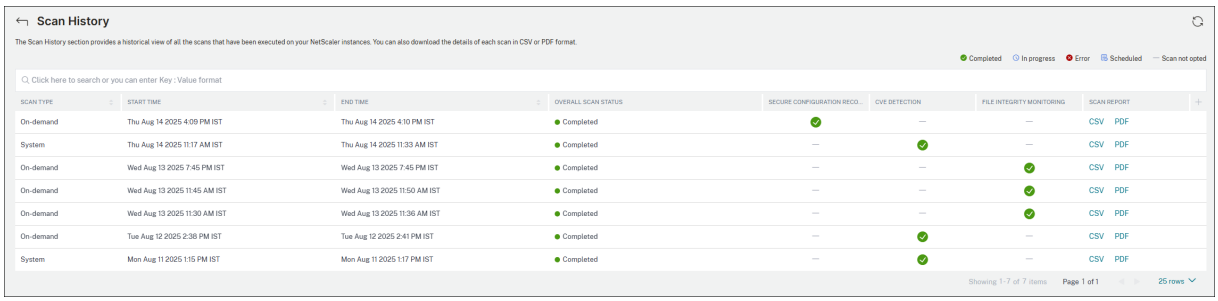
3. Click **Scan Now**. Once the scanning is completed, the revised security details appear in the security advisory dashboard.

Scan History

Click **Scan History** to view all the historical scans that have been run on your NetScaler instances.



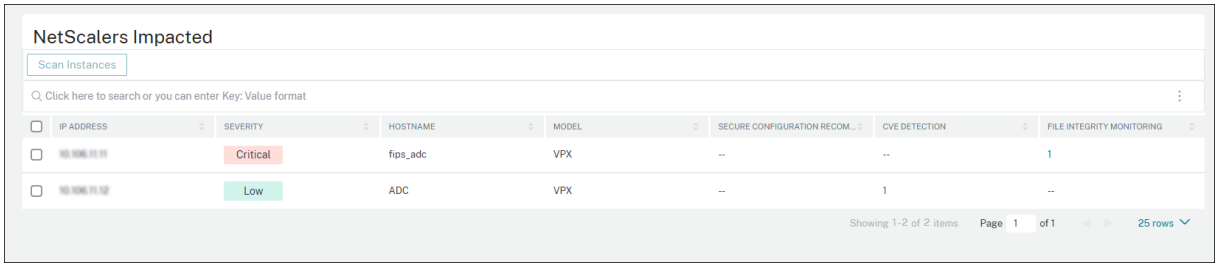
You can view the scan type (On demand scan or system scan), start and end time of the scan, overall scan status, and also download the details of each scan in CSV or PDF format.



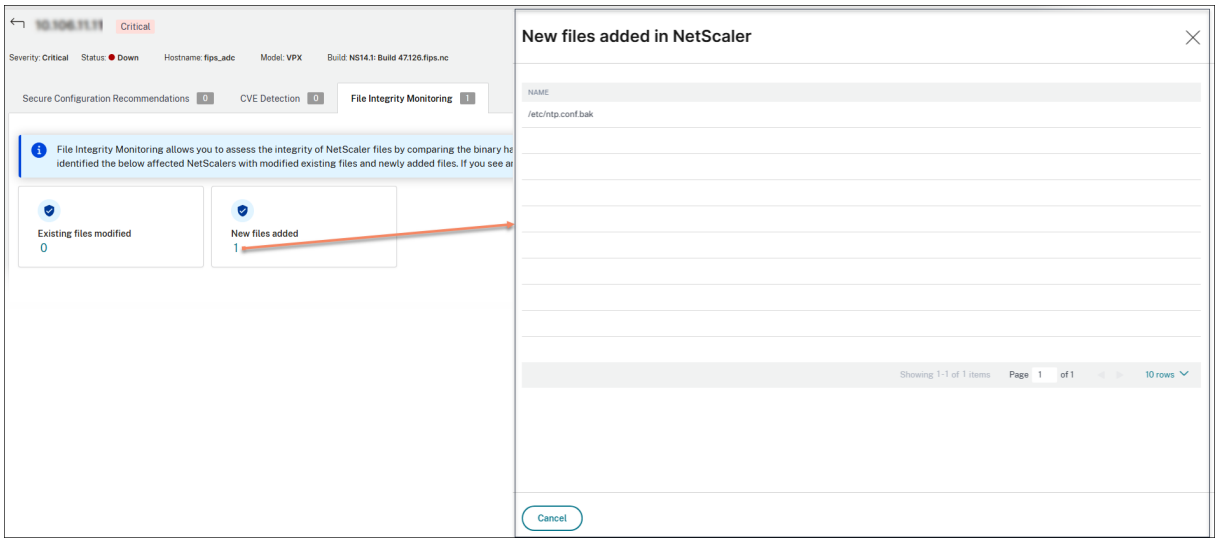
© 1997–2025 Citrix Systems, Inc. All rights reserved.

NetScalers impacted

The **NetScalers Impacted** section lists all the NetScaler instances that are impacted by the security configurations, CVEs, and monitor file integrity checks.



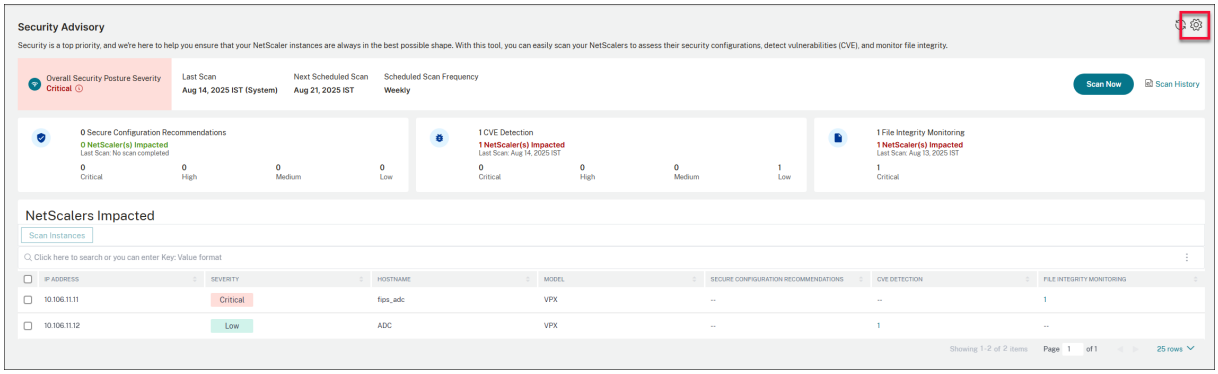
You can also click the number under the **SECURE RECOMMENDATION CONFIGURATION**, **CVE DETECTION**, or **FILE INTEGRITY MONITORING** to view further details. The following is a sample image for your reference.



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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

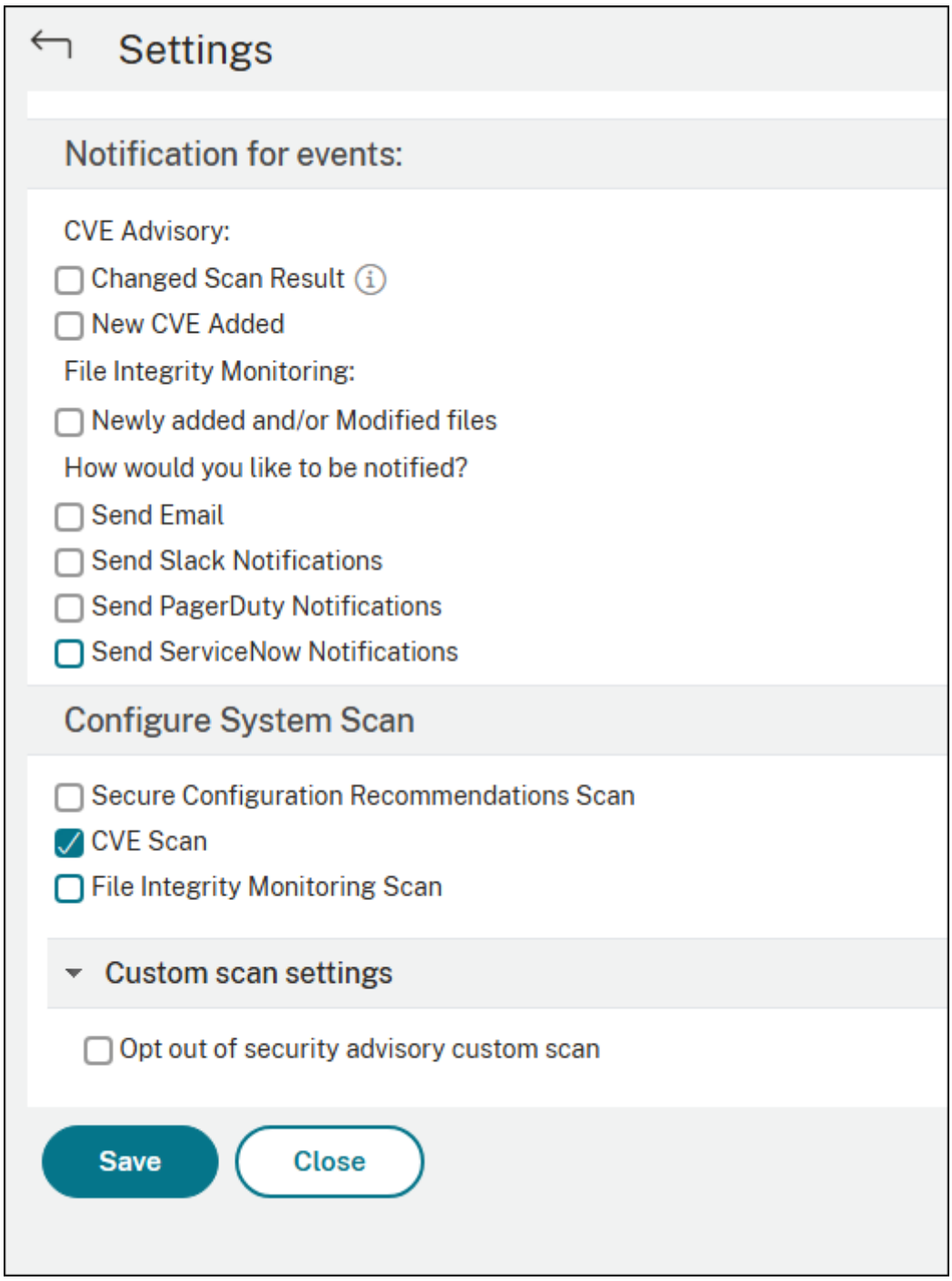


You can perform the following actions:

- 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.

© 1997–2025 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> possible threat.
>
> 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

August 19, 2025

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:

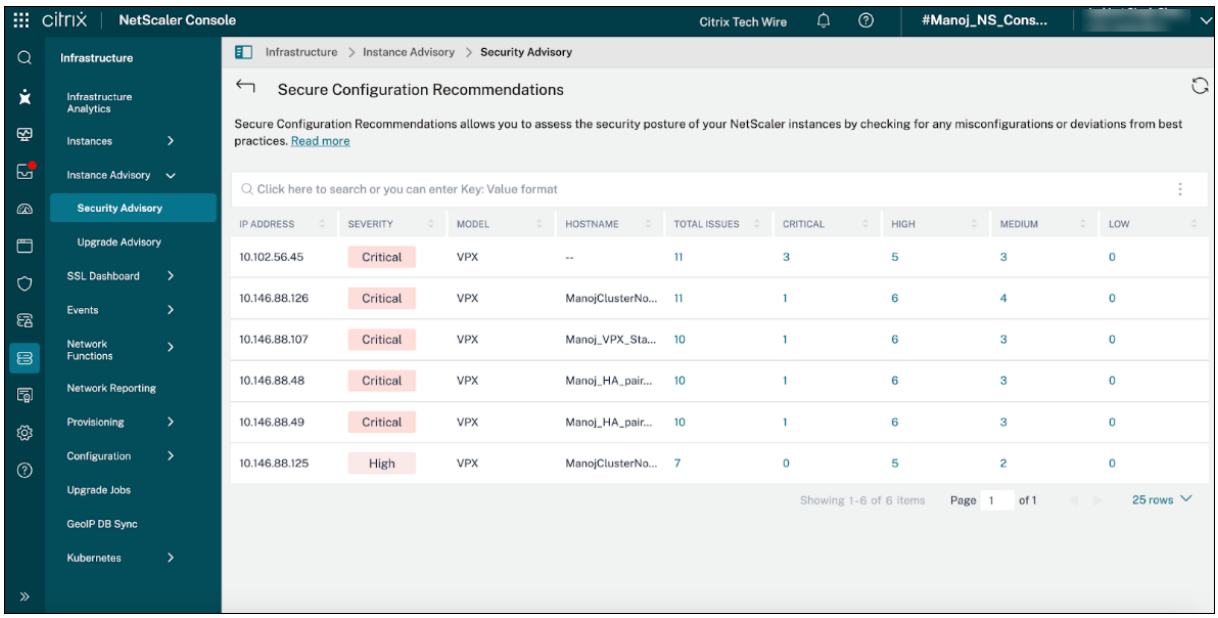
- **Critical**: Issues that pose an immediate and significant risk to the security and integrity of the NetScaler instance. These issues must be addressed with the highest urgency.
- **High**: Configurations that might lead to substantial security breaches if exploited, requiring prompt attention.
- **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.

© 1997–2025 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.

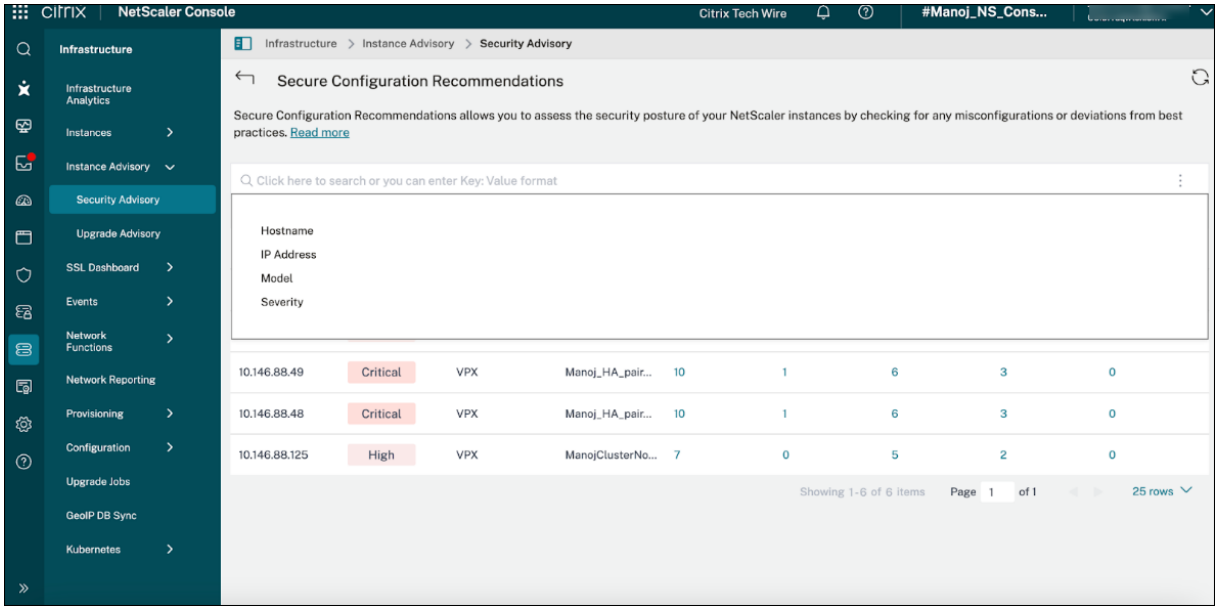
You can **pick and choose** which observations to address first, based on your priorities, risk tolerance, and available resources. This flexibility ensures that the most pressing security concerns are tackled without delay, while still providing the necessary information to achieve comprehensive configuration 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, 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

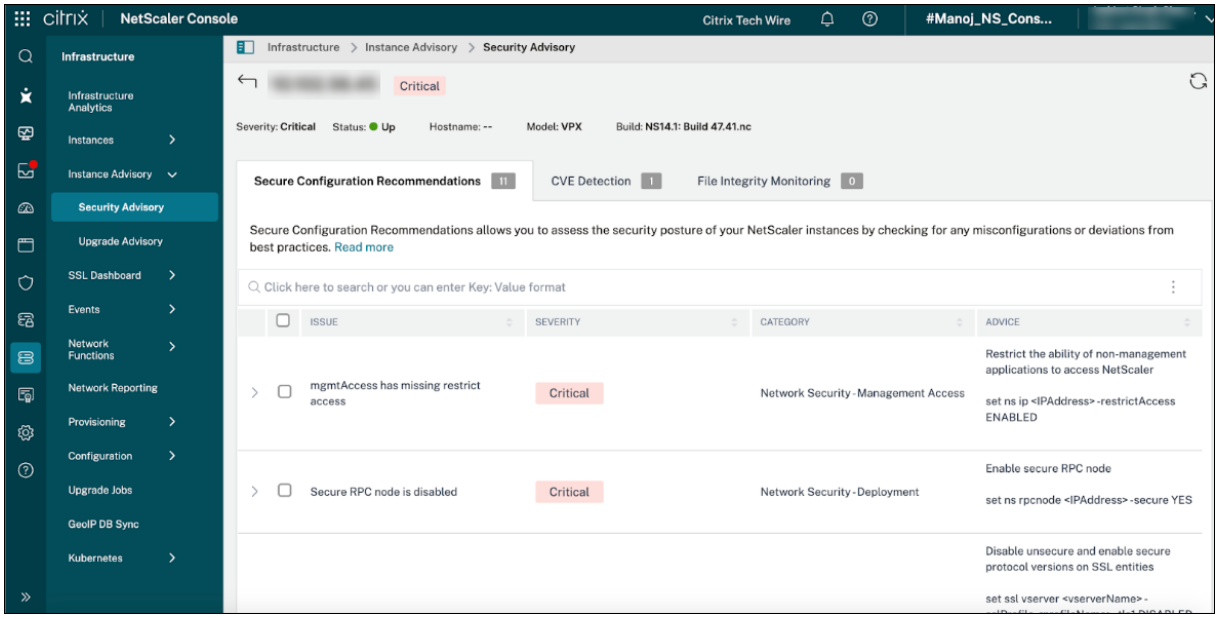
Beyond basic identification, the search also supports filtering by the NetScaler model. This means that you can specify models such as MPX, SDX, or VPX to view only instances belonging to a particular hardware or software category. You can also refine the search by Severity level, allowing you to prioritize 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.

© 1997–2025 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.

© 1997–2025 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:

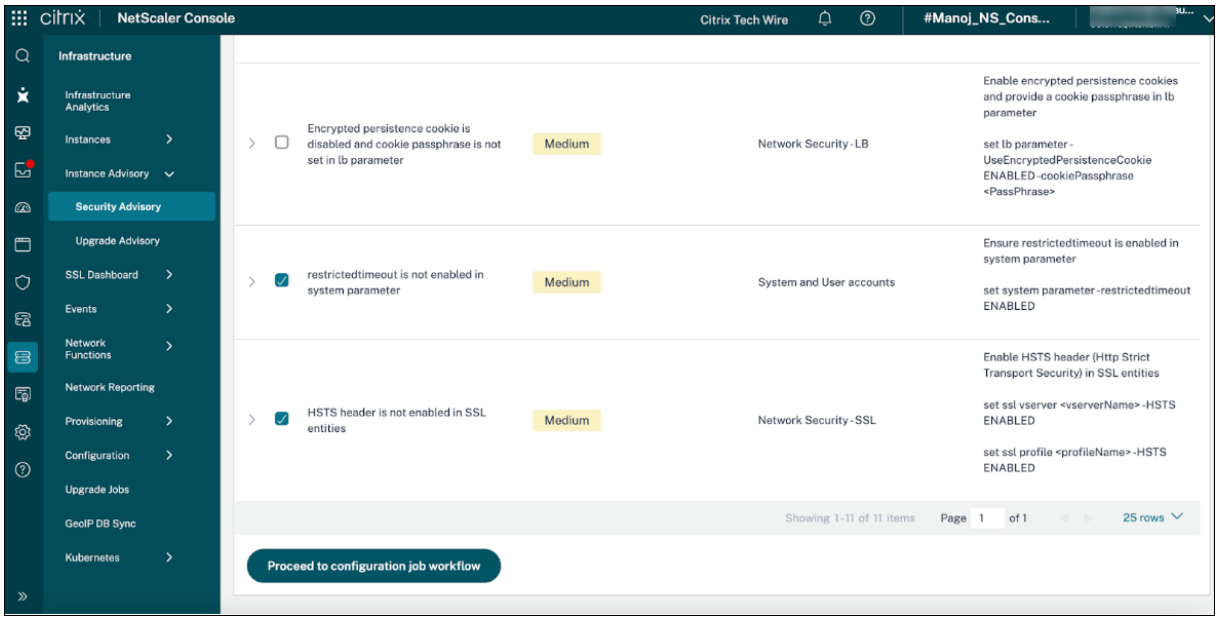
  - **Disabling weak ciphers or protocols**: Recommend that you disable SSL/TLS versions, such as SSLv3 or TLS 1.0, or specific weak cipher suites (for example, RC4, 3DES), as these are known vulnerabilities and their removal is a universal security best practice. The system does not need specific input 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.

- **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.

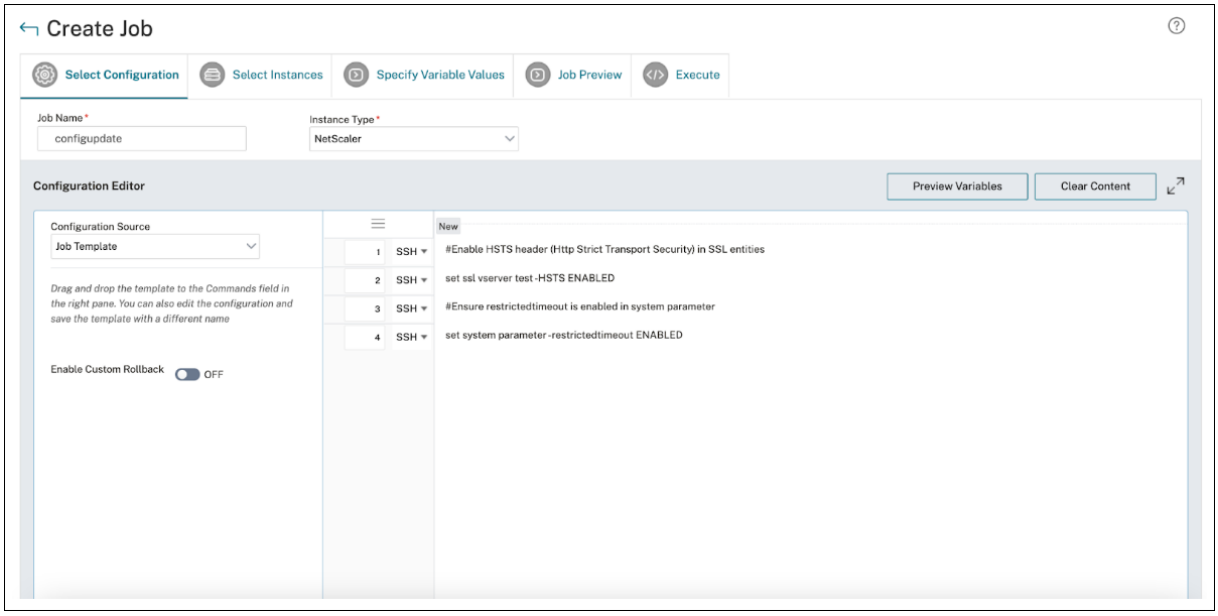
In summary, classifying configuration recommendations based on user input requirements stream-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

lines 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.

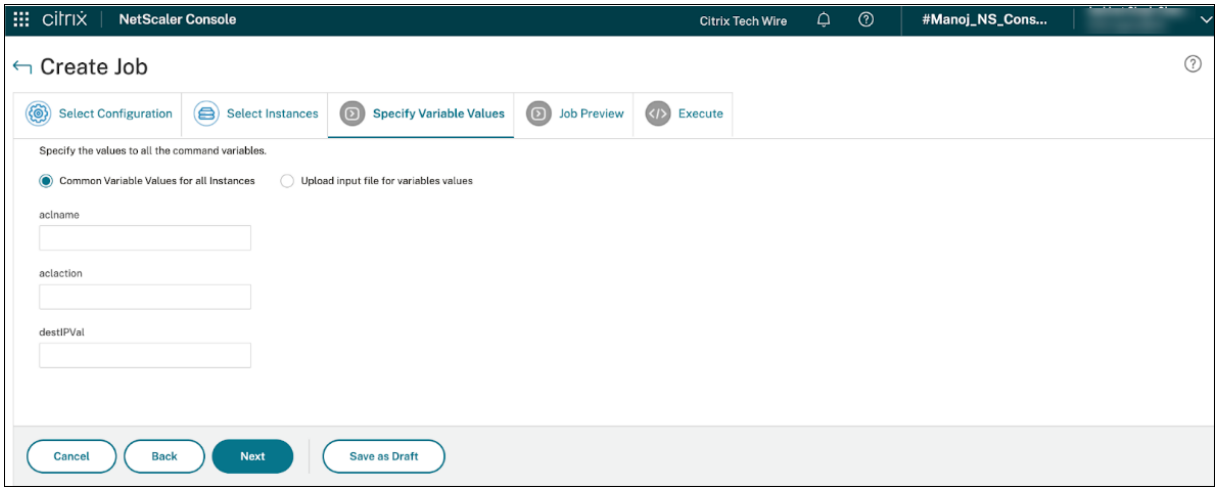


Once a user has decided which configuration to address, the existing configuration job workflow takes over to push the configuration changes.



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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



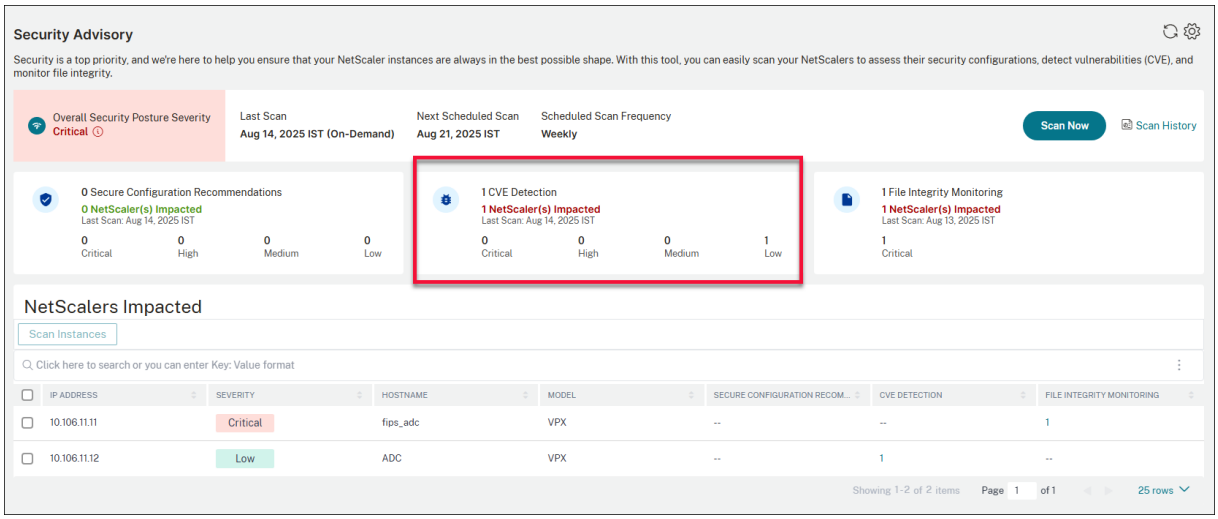
CVE Detection

August 19, 2025

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
- Impacted NetScaler instances categorized under Critical, High, Medium, and Low severity

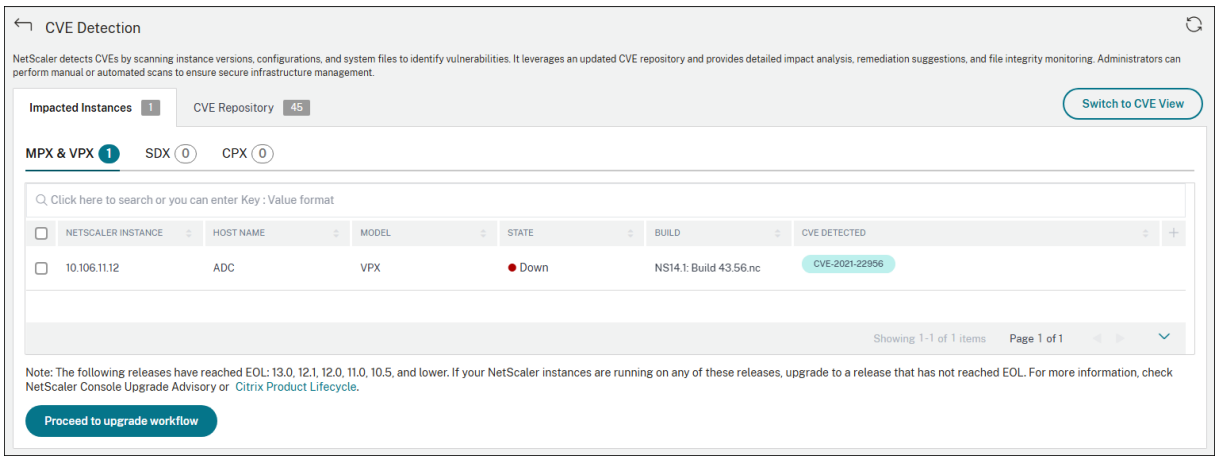


© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 secuirty advisory.

You can click the **CVE Detection** section to view detailed information.



The **CVE Detection** section has two views:

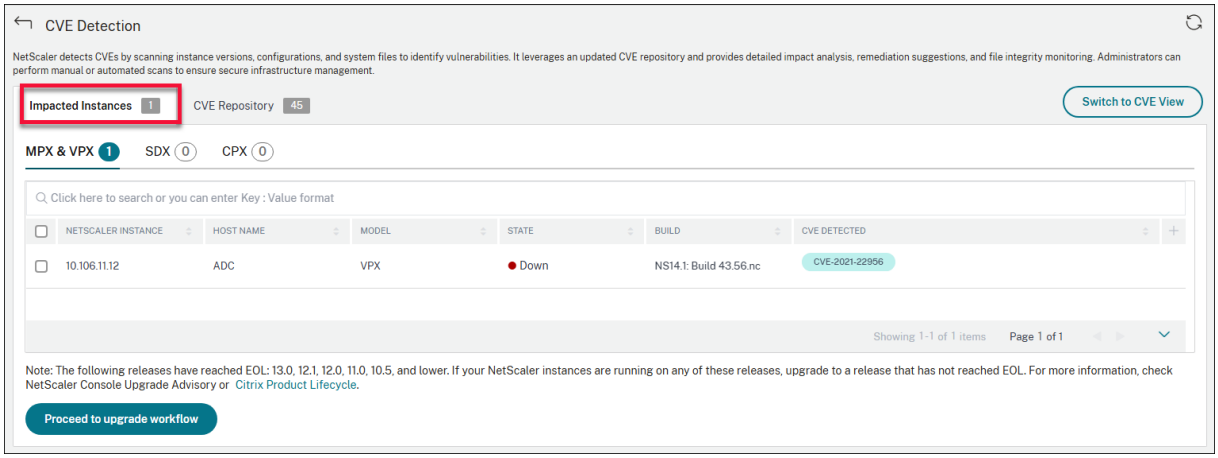
- Instance view
- CVE view

Instance view

The instance view contains **Impacted Instances** and **CVE Repository** tabs.

The **Impacted Instances** tab displays the list of impacted NetScaler instances.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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**.

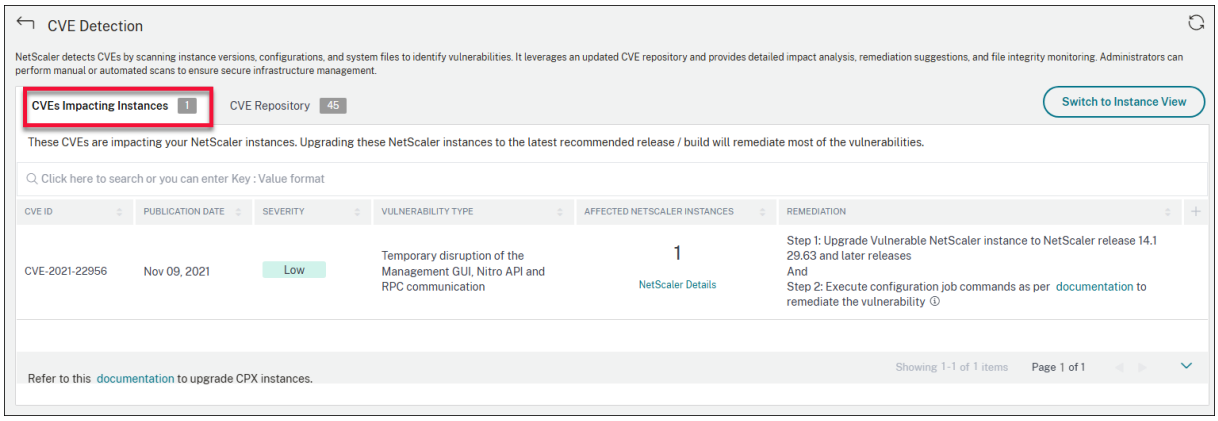
The upgrade workflow starts and the vulnerable NetScaler is auto-populated as the target NetScaler. For more information on how to use NetScaler Console to upgrade NetScaler instances, see Use jobs to upgrade NetScaler instances.

> **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**.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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.

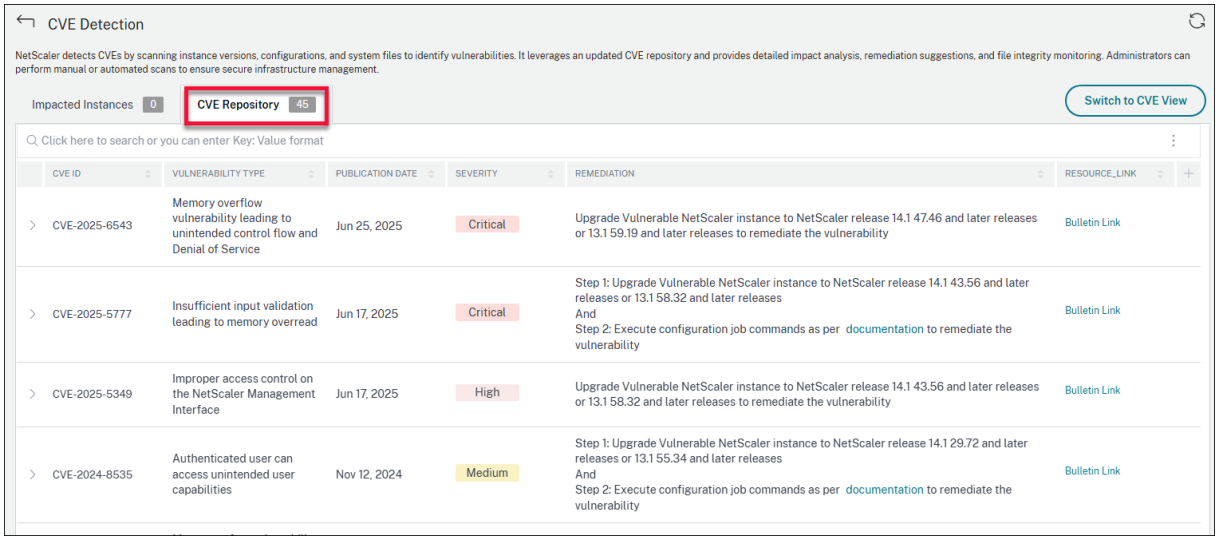
The same instance can be impacted by multiple CVEs. This table helps you see how many instances one particular CVE or multiple selected CVEs are impacting. To check the IP address of the impacted instance, hover over NetScaler Details under **Affected NetScaler Instances**. To check the details of the 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.

- CVE IDs
- Vulnerability type
- Publication date
- Severity level
- Remediation
- Links to security bulletins

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.

- 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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.

File integrity monitoring

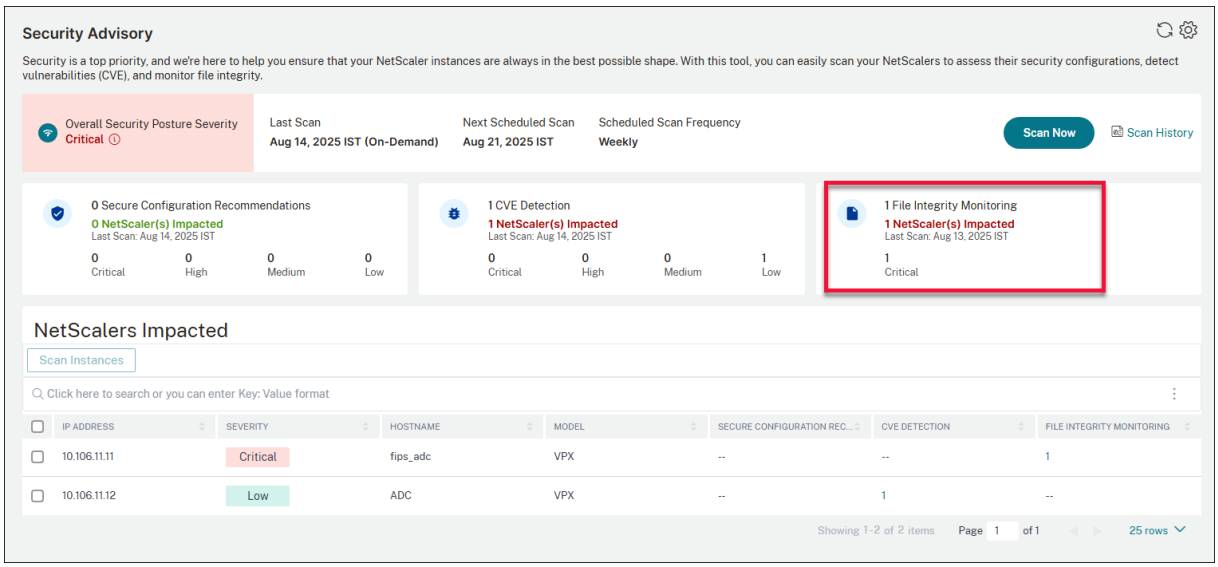
August 19, 2025

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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

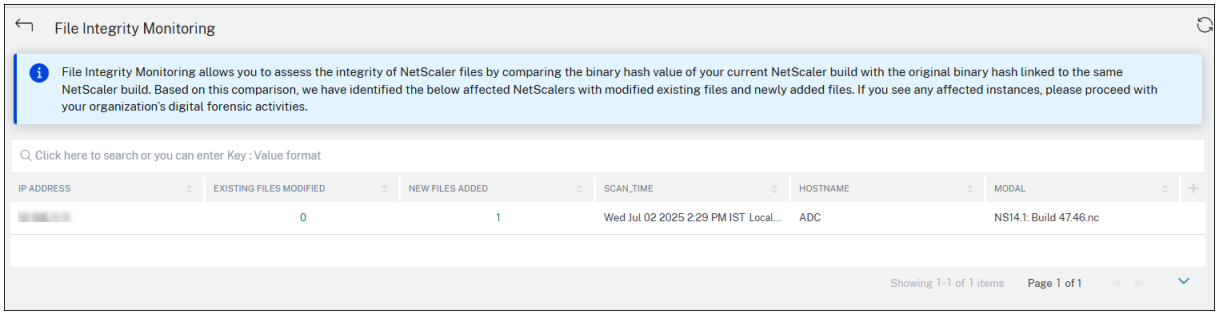
- Number of issues detected
- Number of NetScaler instances impacted
- Date when the last scan was run
- Impacted NetScaler instances categorized under Critical, High, Medium, and Low severity



As an administrator, you can allowNetScaler 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.



The table displays the following details:

- IP address - The IP address of the impacted instances.
- 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Host name - The host name of the impacted NetScaler.
- Modal - The modal name of the impacted NetScaler.

Click the numbers under **Existing files modified** and **New files added** to view details.

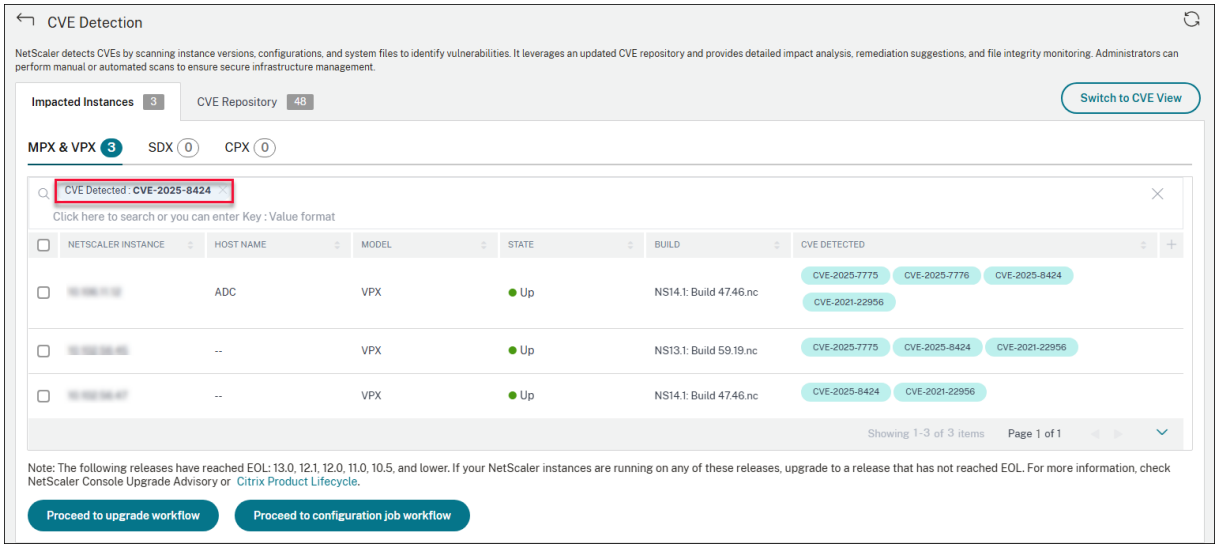
Points to note

- 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.
- The following is the list of unsupported platforms: BLX

Identify and remediate vulnerabilities for CVE-2025-8424

August 26, 2025

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.



© 1997–2025 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**.

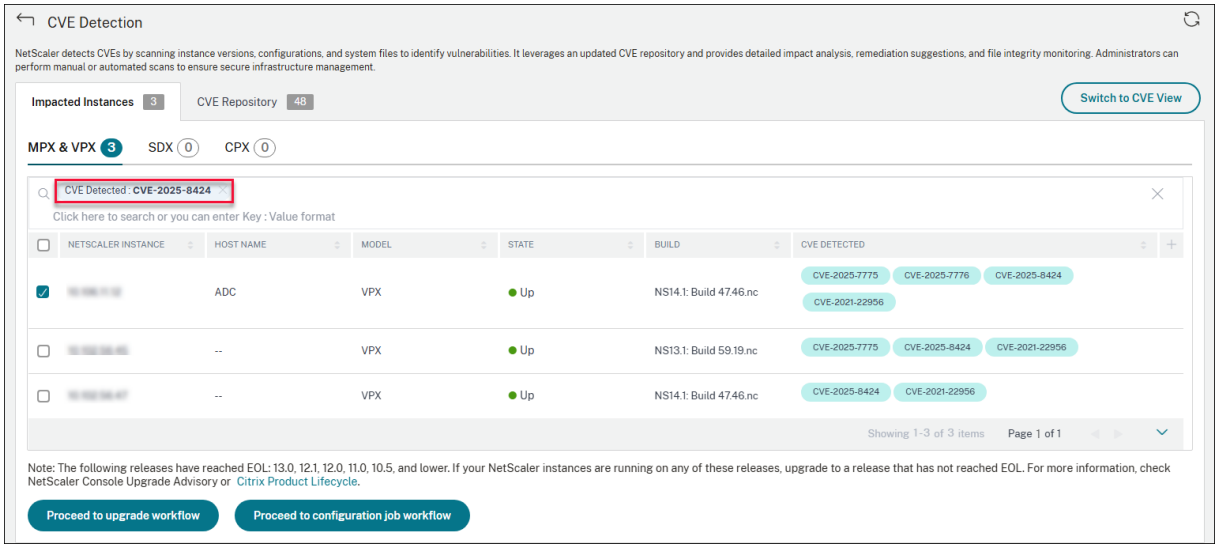
Remediate CVE-2025-8424

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.

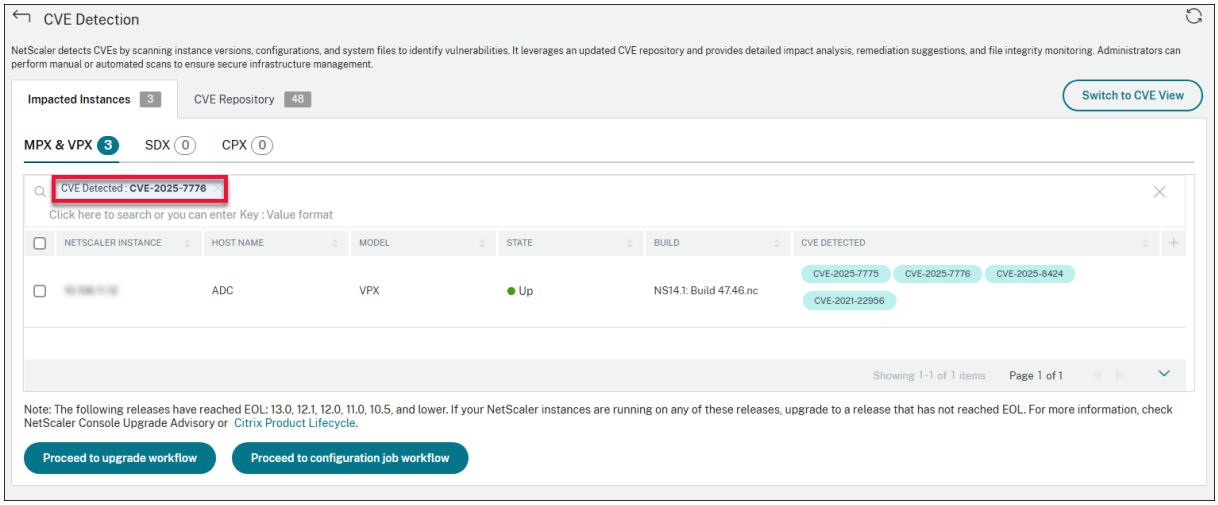


© 1997–2025 Citrix Systems, Inc. All rights reserved.

Identify and remediate vulnerabilities for CVE-2025-7776

August 26, 2025

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**.

Remediate CVE-2025-7776

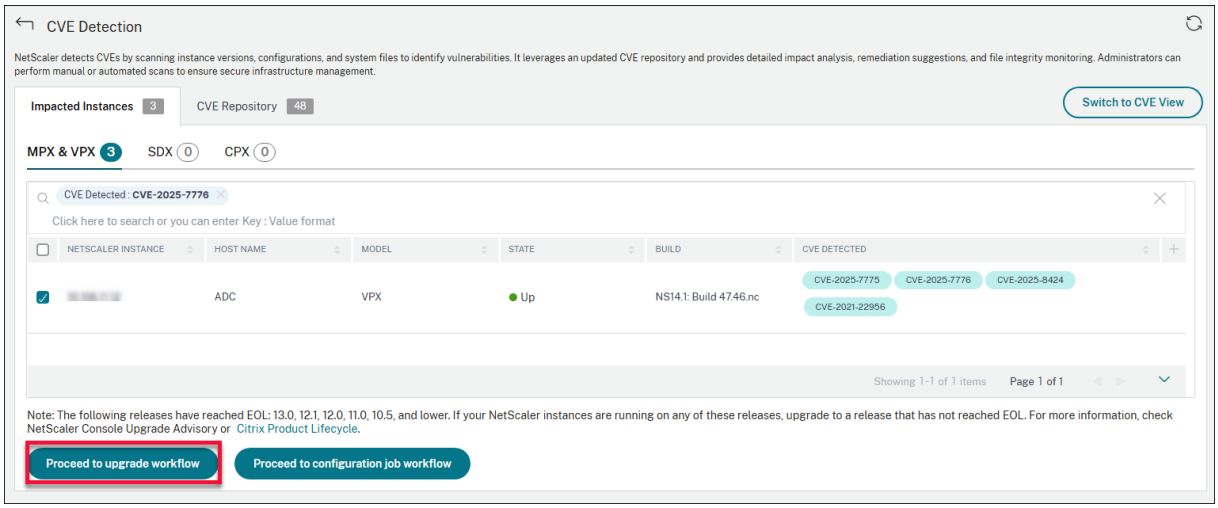
For CVE-2025-7776 impacted NetScaler instances, the remediation is a single-step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

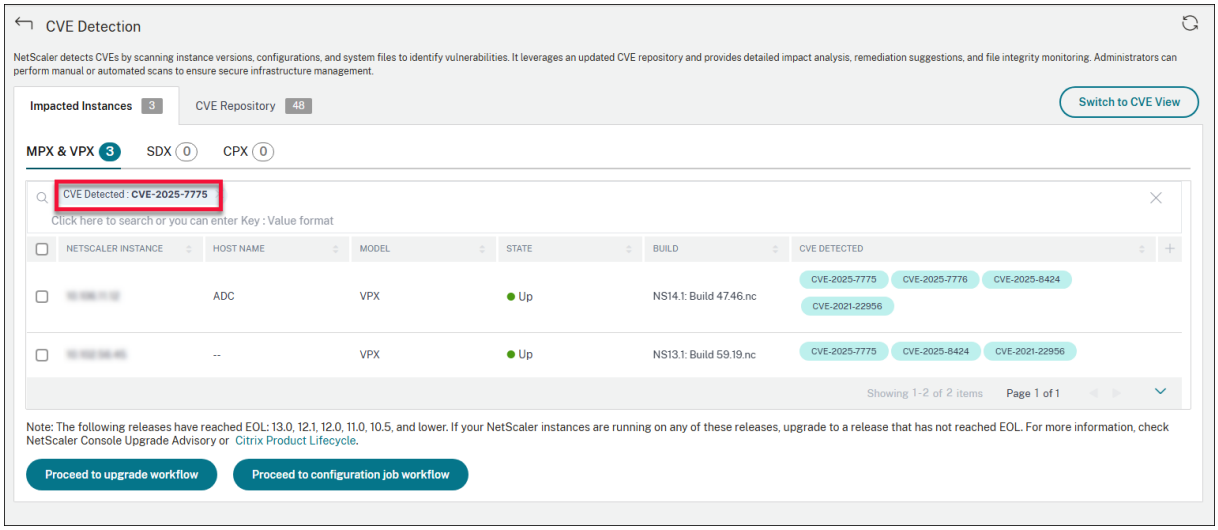
For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.



Identify and remediate vulnerabilities for CVE-2025-7775

August 26, 2025

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.



For more information about the security advisory dashboard see, Security Advisory.

© 1997–2025 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-2025-7775 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

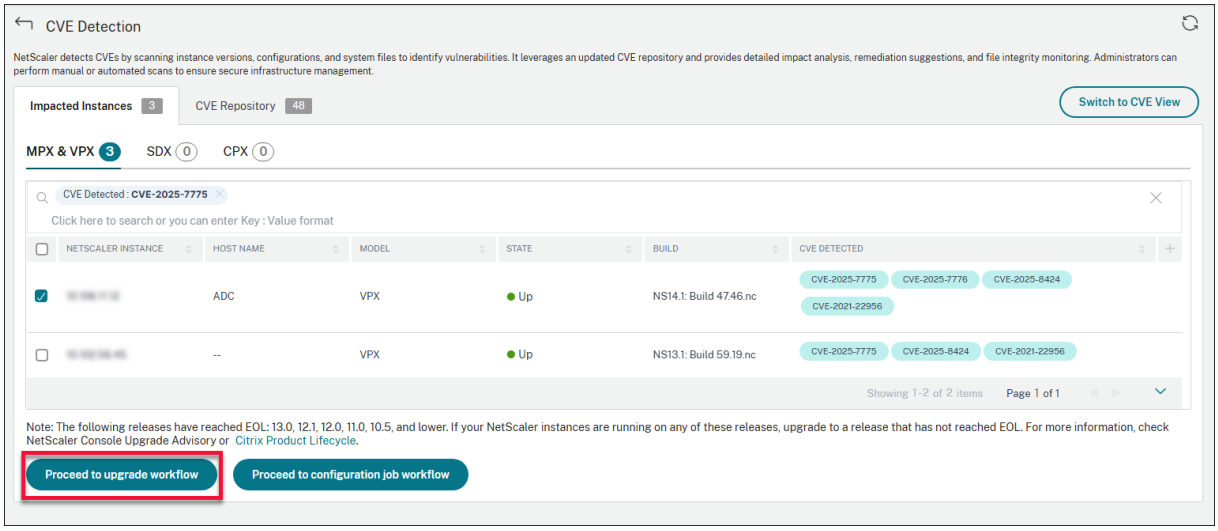
Remediate CVE-2025-7775

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.

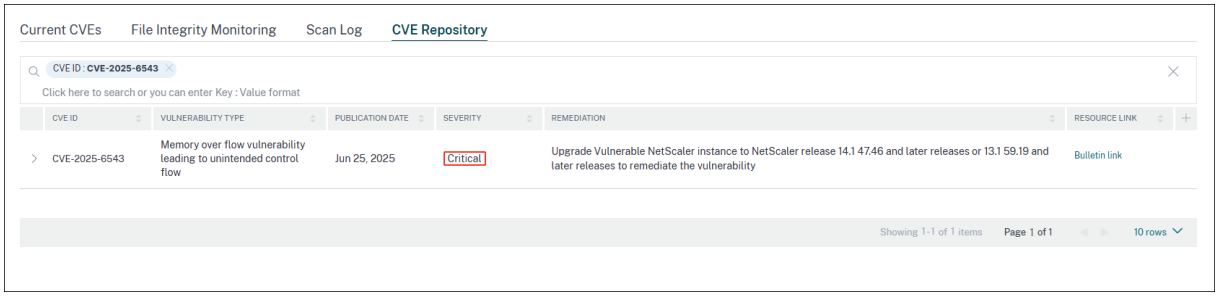


Identify and remediate vulnerabilities for CVE-2025-6543

June 25, 2025

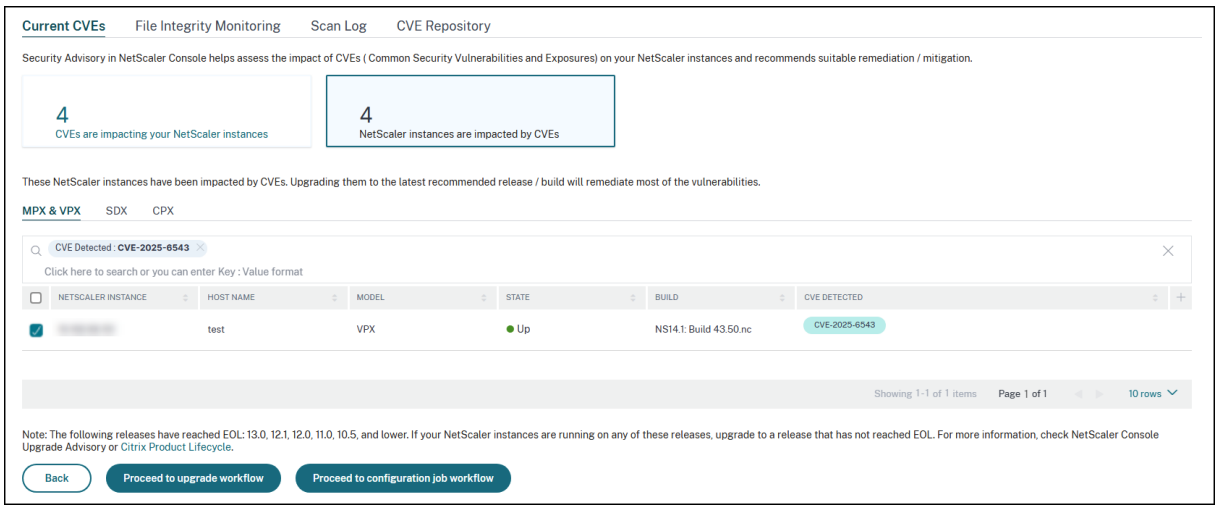
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.



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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Remediate CVE-2025-6543

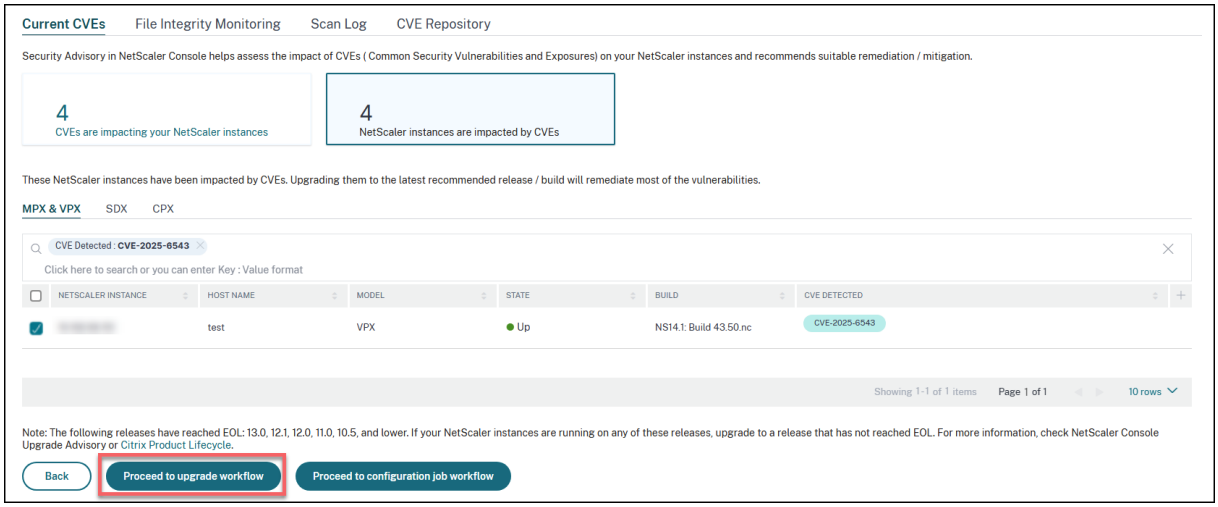
For CVE-2025-6543 impacted NetScaler instances, the remediation is a single step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix. In the GUI, under **Current CVEs > NetScaler instances are impacted by CVEs**, you can see the step to remediate.

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.

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

September 8, 2025

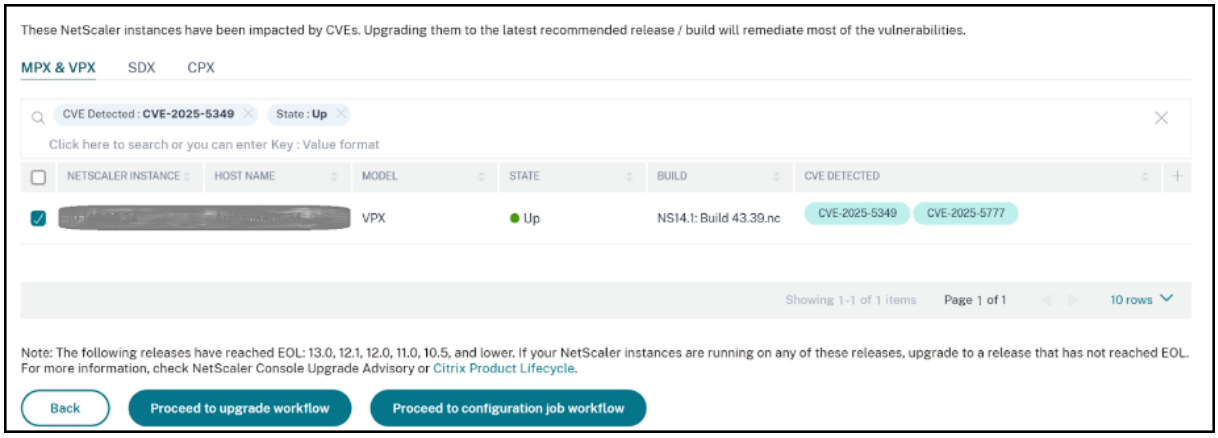
In the NetScaler Console security advisory dashboard, under **Current CVEs <number of> NetScaler instances are impacted by CVEs**, you can see all the instances vulnerable due to CVE-2025-5349. To check the details of the instances impacted by the CVEs, select CVE-2025-5349 and click **View Affected Instances**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



> **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.



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.

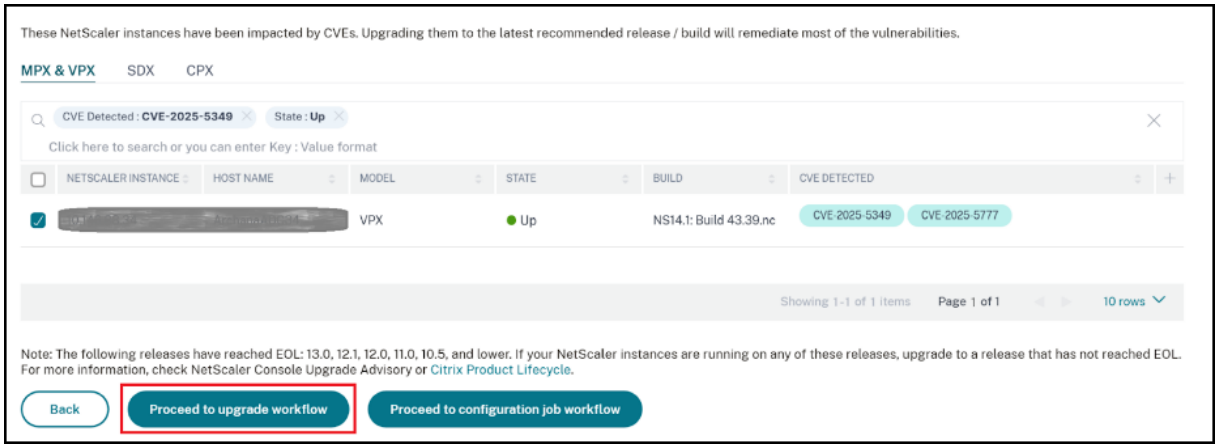
Under **Current CVEs> NetScaler instances impacted by CVEs**, you see the following workflow for this single step remediation process, which is **Proceed to upgrade workflow**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.



Remediate vulnerabilities for CVE-2025-5777

September 8, 2025

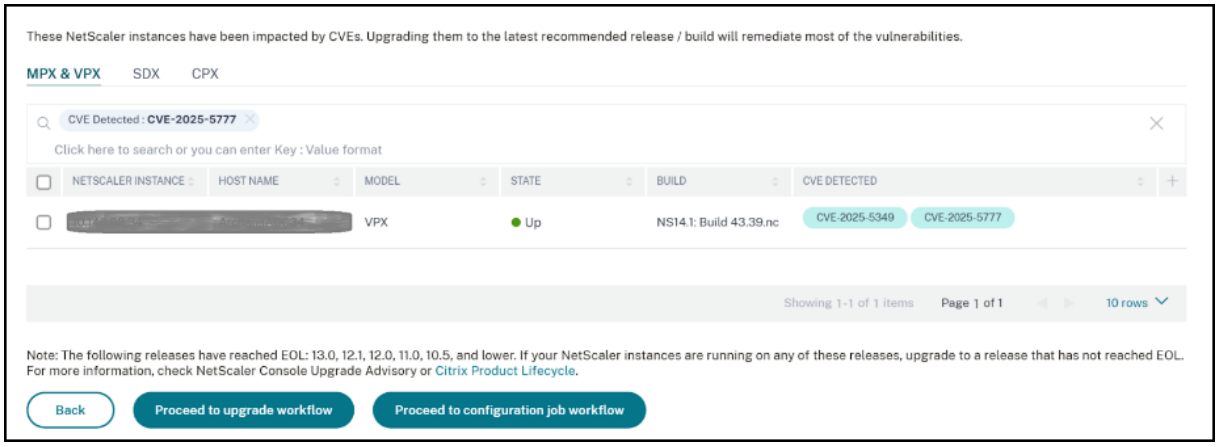
In the NetScaler Console security advisory dashboard, under **Current CVEs <number of> NetScaler instances are impacted by CVEs**, you can see all the instances vulnerable due to CVE-2025-5777. To check the details of the instances impacted by the CVEs, select CVE-2025-5777 and click **View Affected Instances**.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **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.



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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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-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.

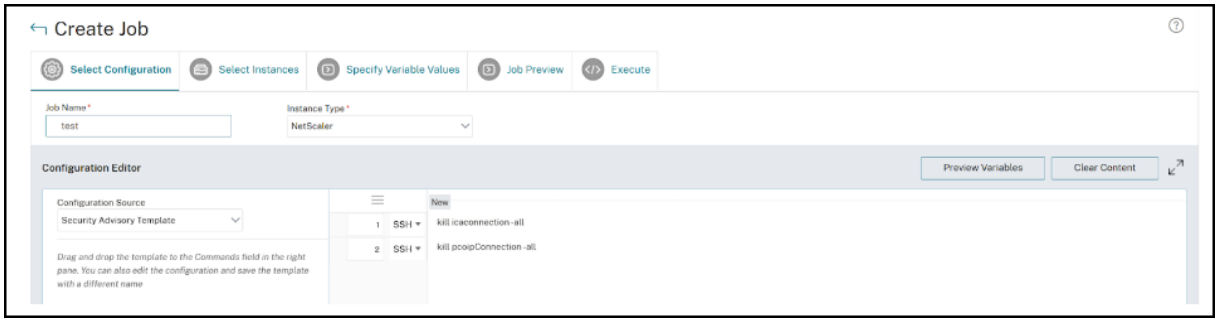
Keep the following points in mind before you select an instance and click **Proceed to configuration job workflow**:

- 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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

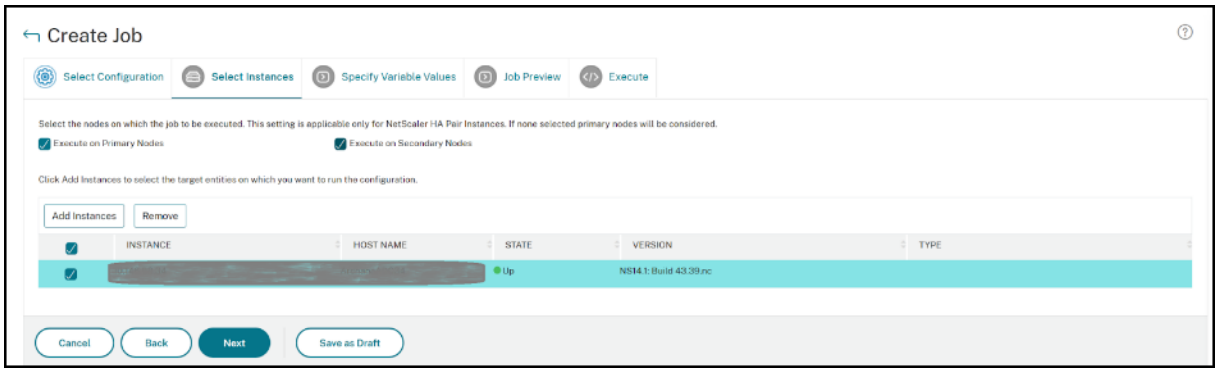
- For multiple NetScaler instances impacted by CVE-2025-5777 and one or more other CVEs (such as CVE-2020-8300, CVE-2021-22927, and CVE-2021-22920), which require remediation to be applied to each NetScaler at a time: when you select these instances and click **Proceed to configuration job workflow**, 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

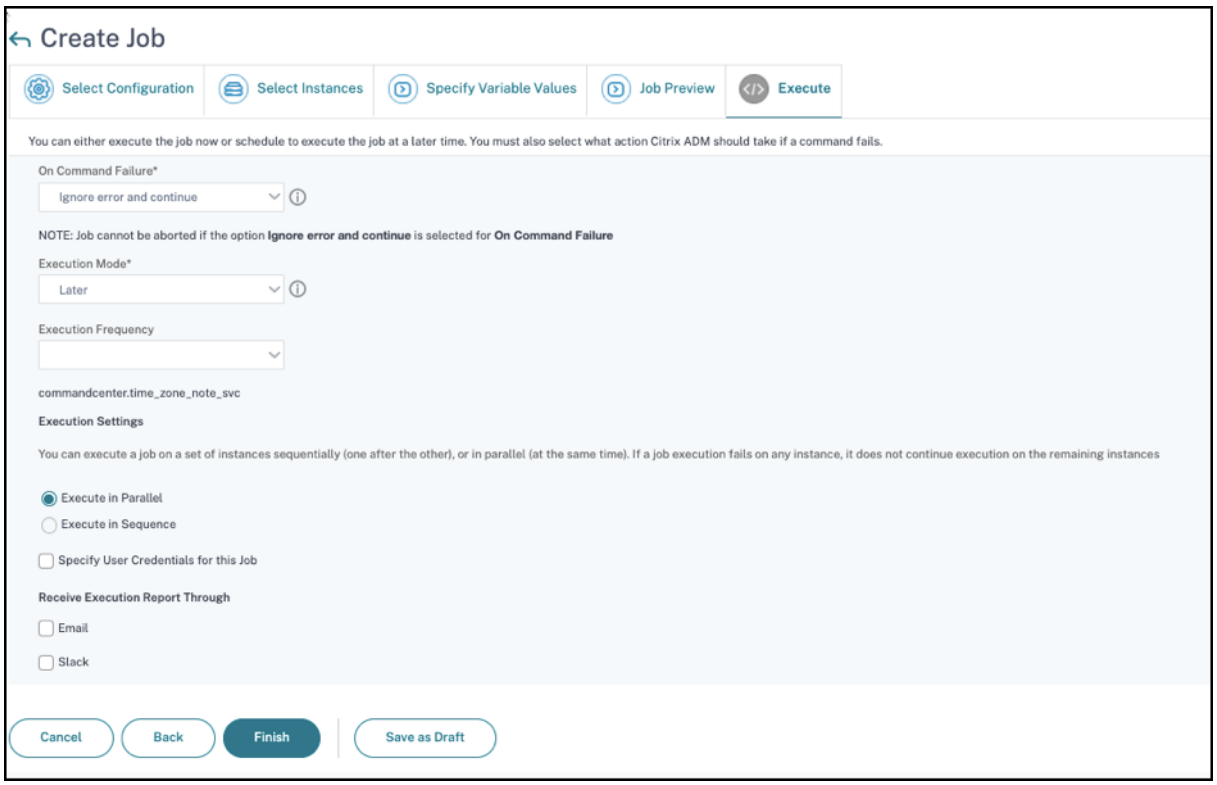
The impacted instance is auto-populated under **Select Instances**. Select the instance. If this instance is part of an HA pair, select **Execute on Secondary Nodes**. Click **Next**.



> **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



After the job is run, it appears under **Infrastructure > Configuration > Configuration Jobs**.

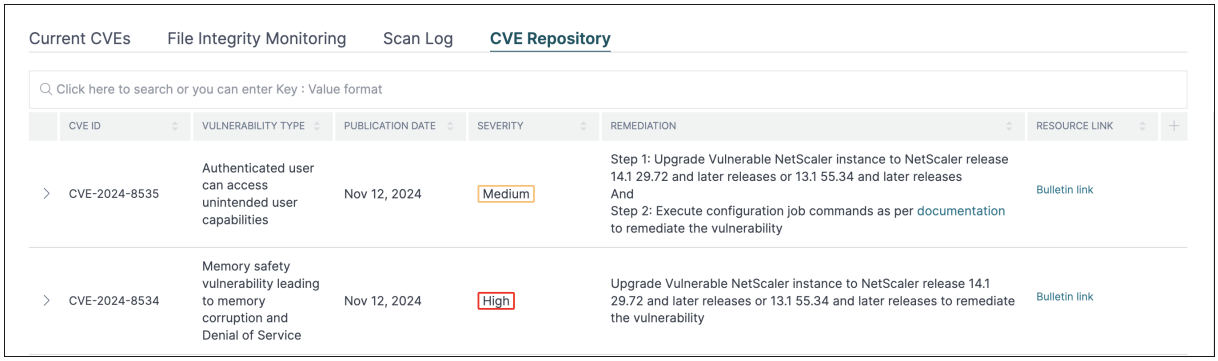
After completing the two remediation steps for all vulnerable NetScaler instances, you can run an on-demand scan to see the revised security posture.

Remediate vulnerabilities for CVE-2024-8535

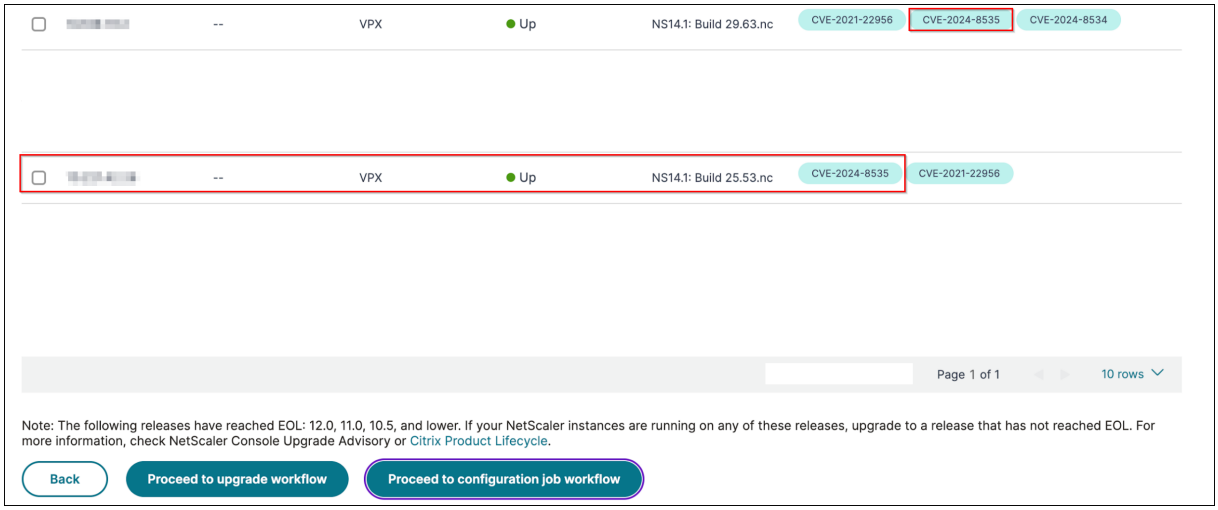
November 12, 2024

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**.

© 1997–2025 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-2024-8535.



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

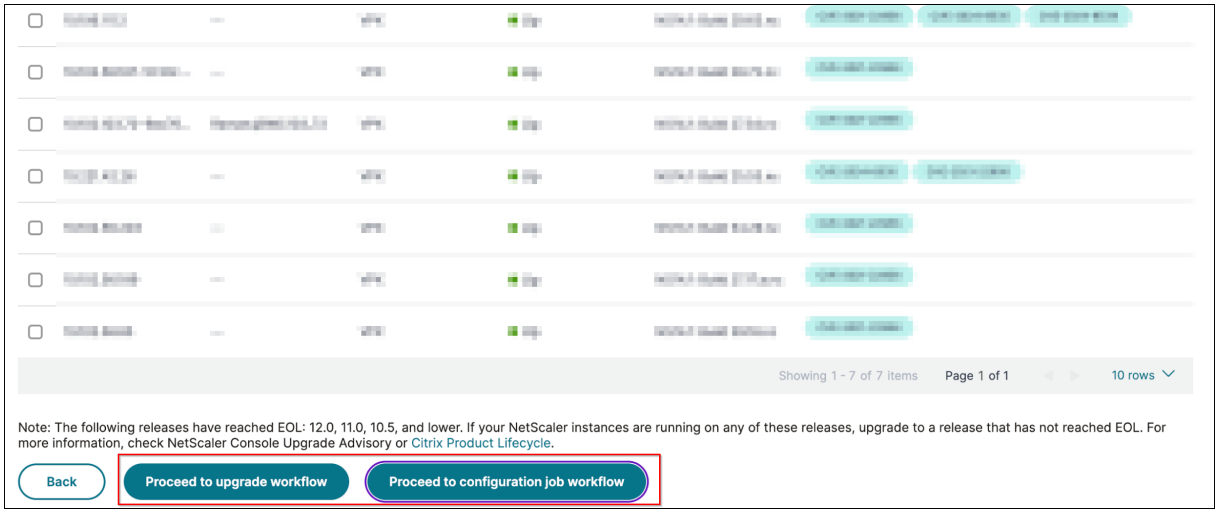
For CVE-2024-8535 -impacted NetScaler instances, the remediation is a two-step process. In the GUI, under **Current CVEs > NetScaler instances are impacted by CVEs**, you can see step 1 and 2.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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-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.

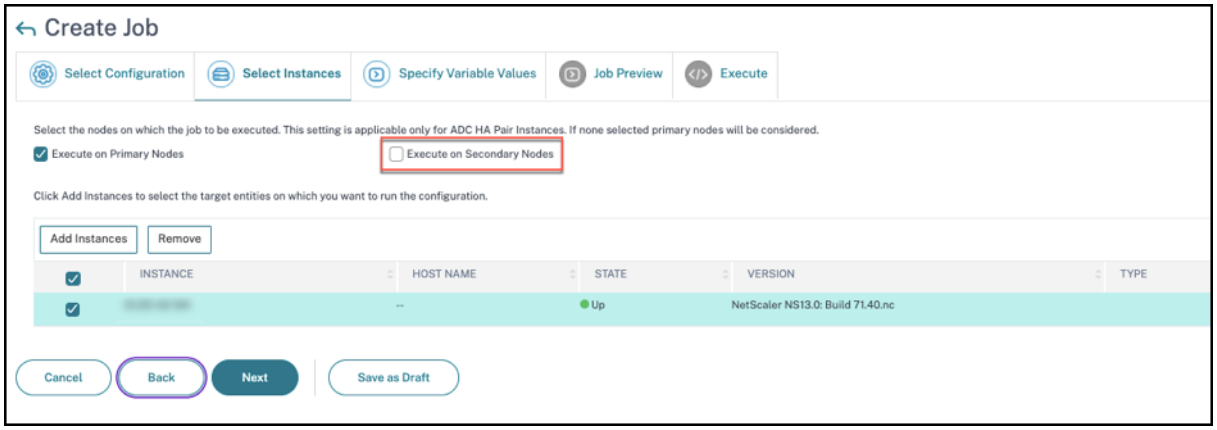
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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, 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**.

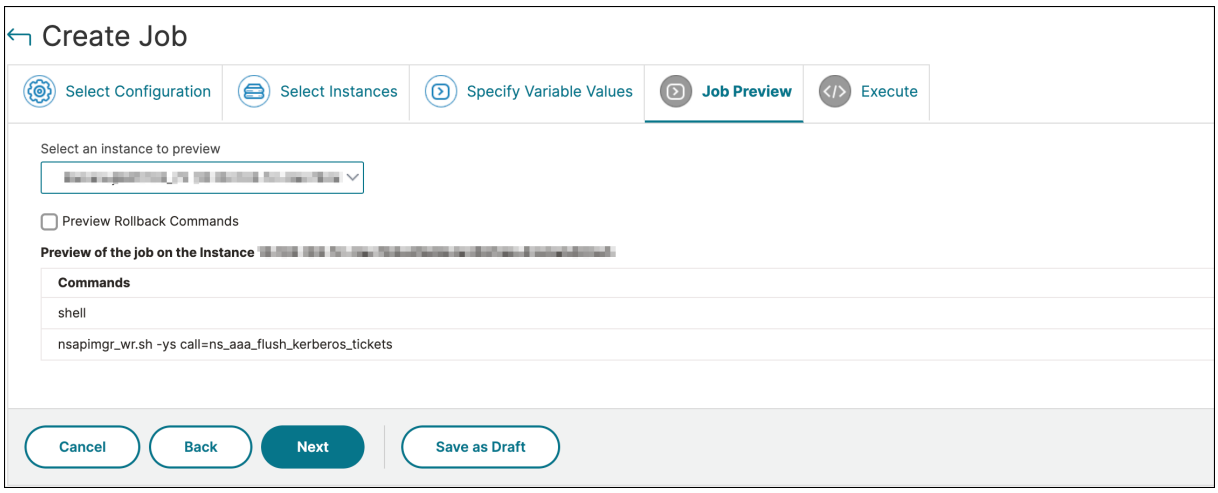


> **Note:**
>
> For NetScaler instances in cluster mode, using security advisory, the NetScaler Console supports running the config job only on the cluster configuration coordinator (CCO) node. Run the commands on non-CCO nodes separately.

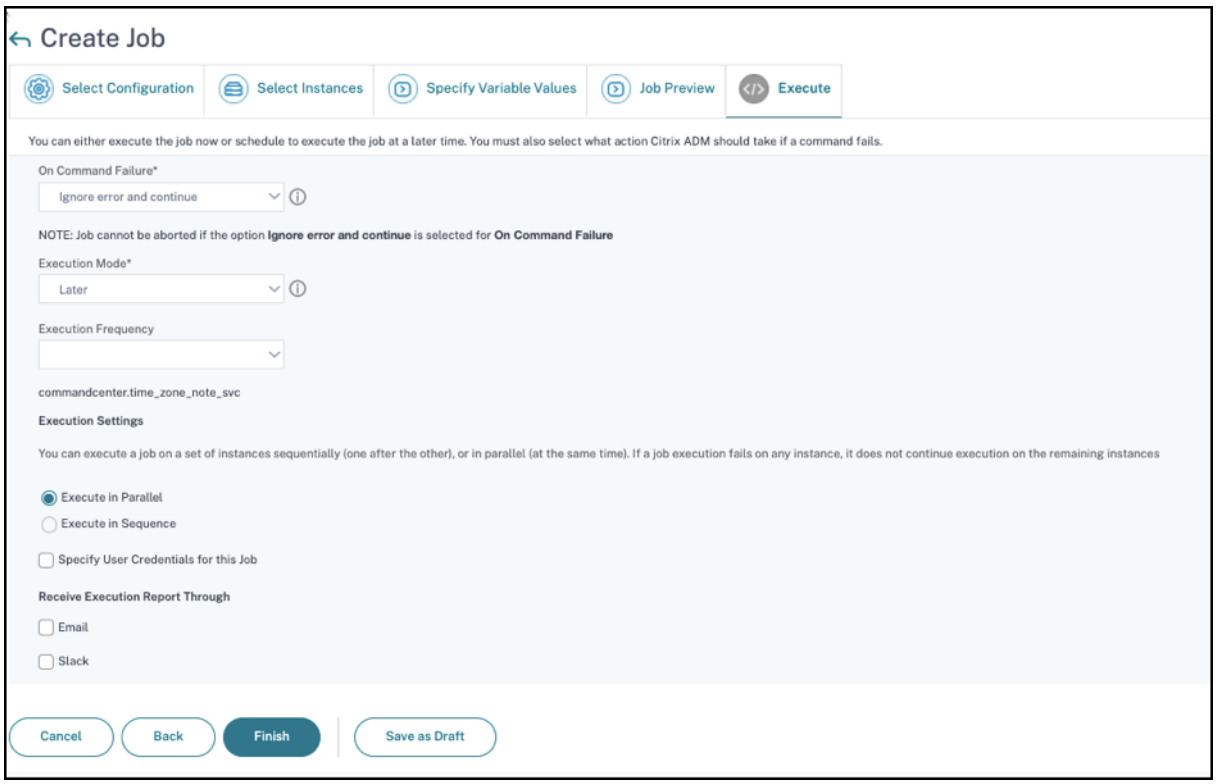
Step 3: Specify variable values No variable is required to specify in this step. Select **Common Variable Values for all instances** and click **Next**.

© 1997–2025 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**.

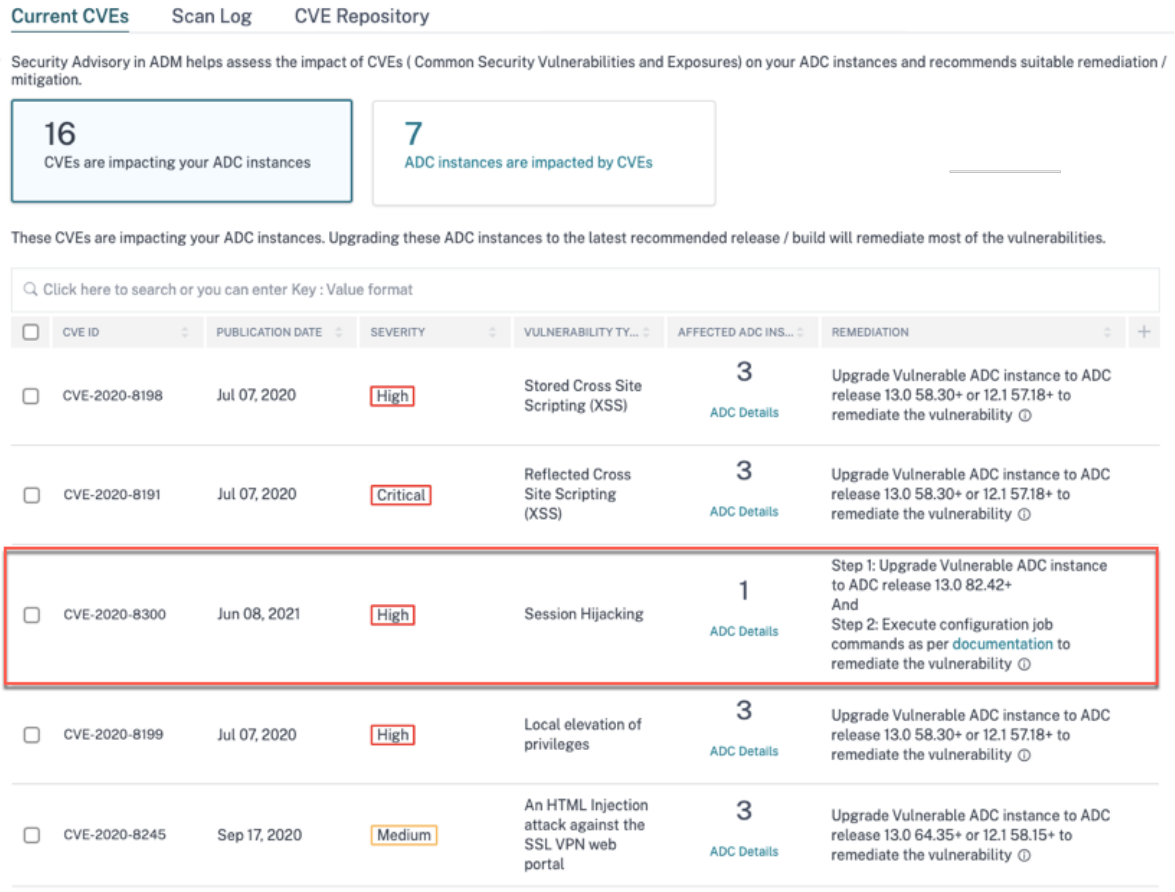
After completing the two remediation steps for all vulnerable NetScaler instances, you can run an on-demand scan to see the revised security posture.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Remediate vulnerabilities for CVE-2020-8300

January 8, 2024

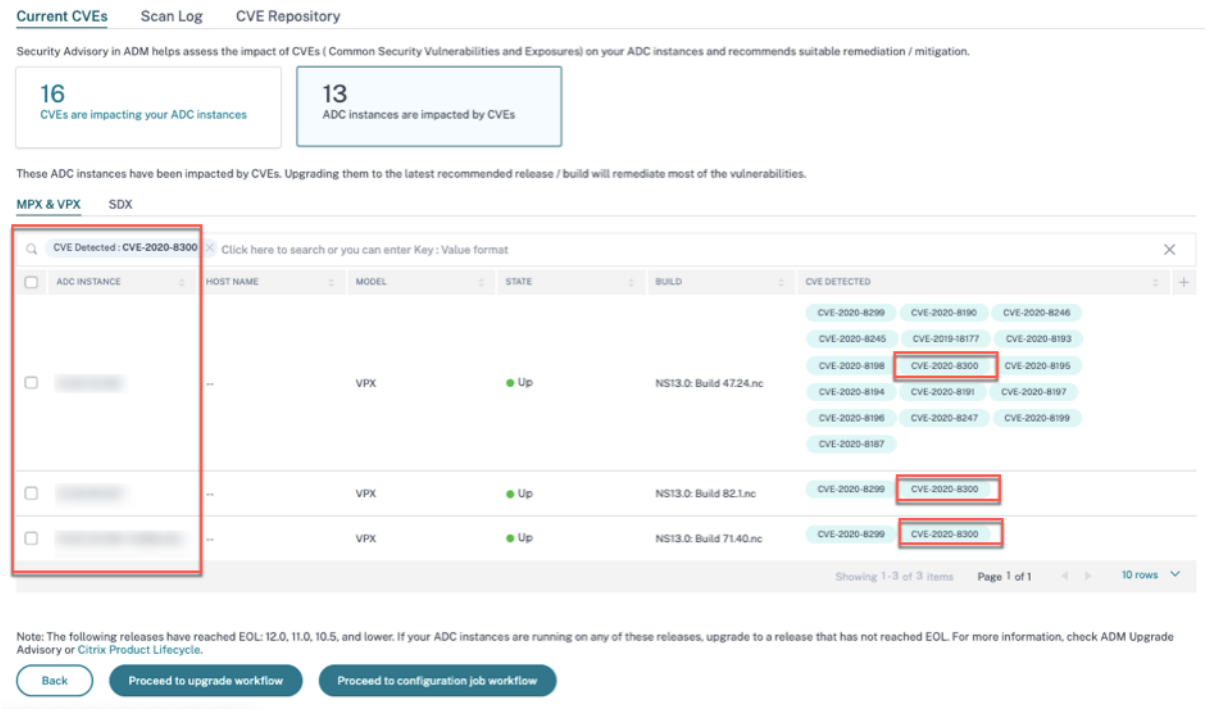
In the NetScaler Console security advisory dashboard, under **Current CVEs > <number of> NetScaler instances are impacted by CVEs**, you can see all the instances vulnerable due to this specific CVE. To check the details of the CVE-2020-8300 impacted instances, select **CVE-2020-8300** and click **View Affected Instances**.



> **Note**
>
> For more information about the security advisory dashboard see, Security Advisory.

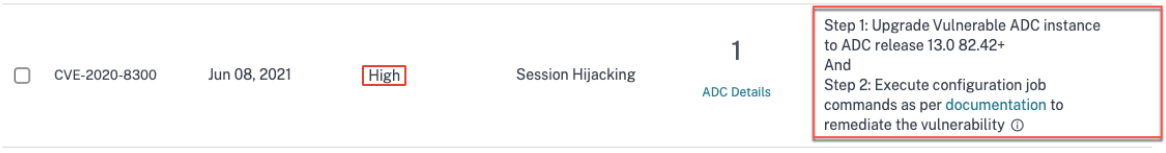
The **<number of> NetScaler instances impacted by CVEs** window appears. Here you see the count and details of the NetScaler instances impacted by CVE-2020-8300.

© 1997–2025 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.

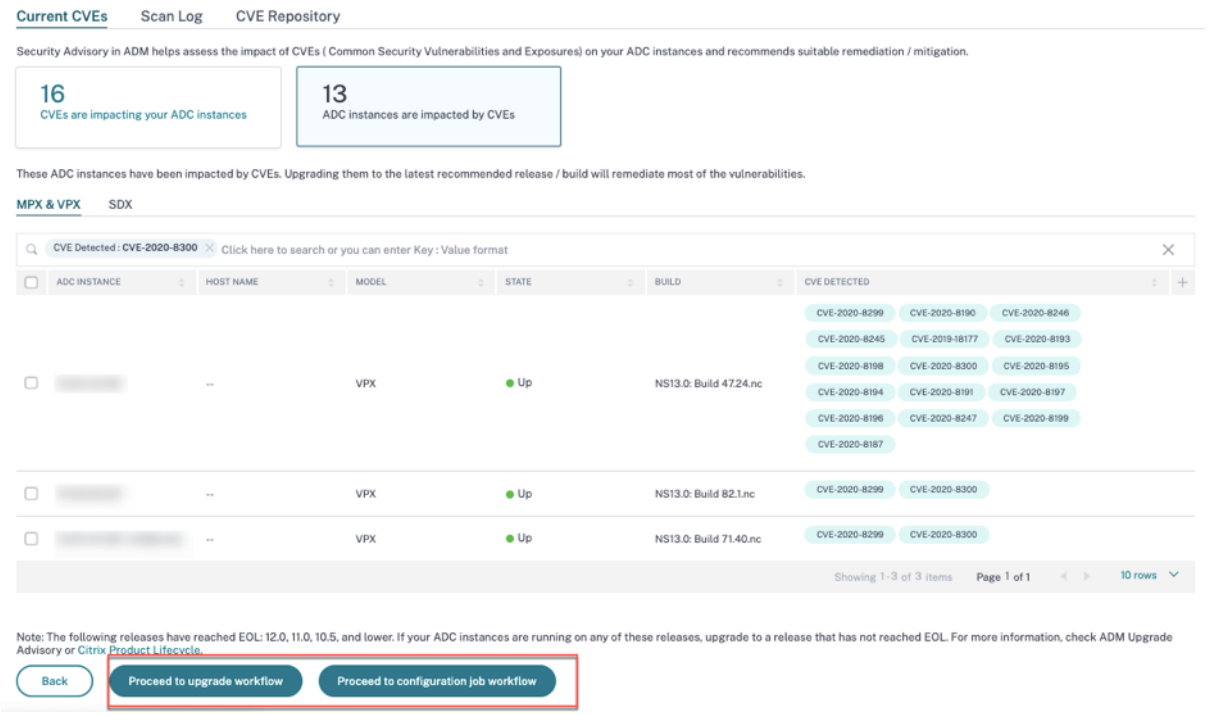


The two steps include:

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.

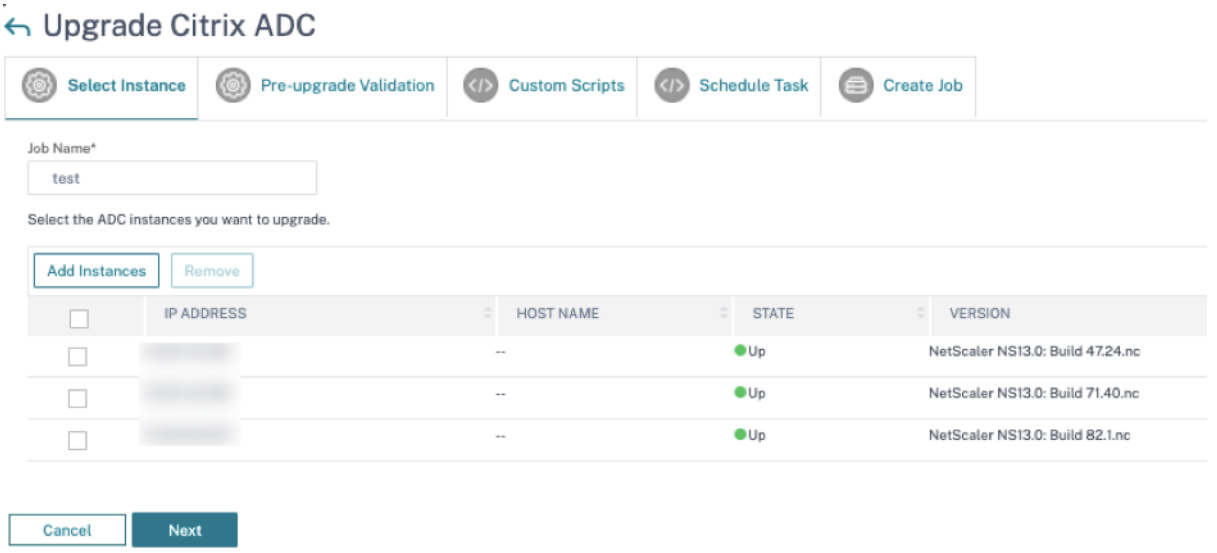
Under **Current CVEs> NetScaler instances impacted by CVEs**, you see two separate workflows for this 2-step remediation process: which are **Proceed to upgrade workflow** and **Proceed to configuration job workflow**.

© 1997–2025 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.

© 1997–2025 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.

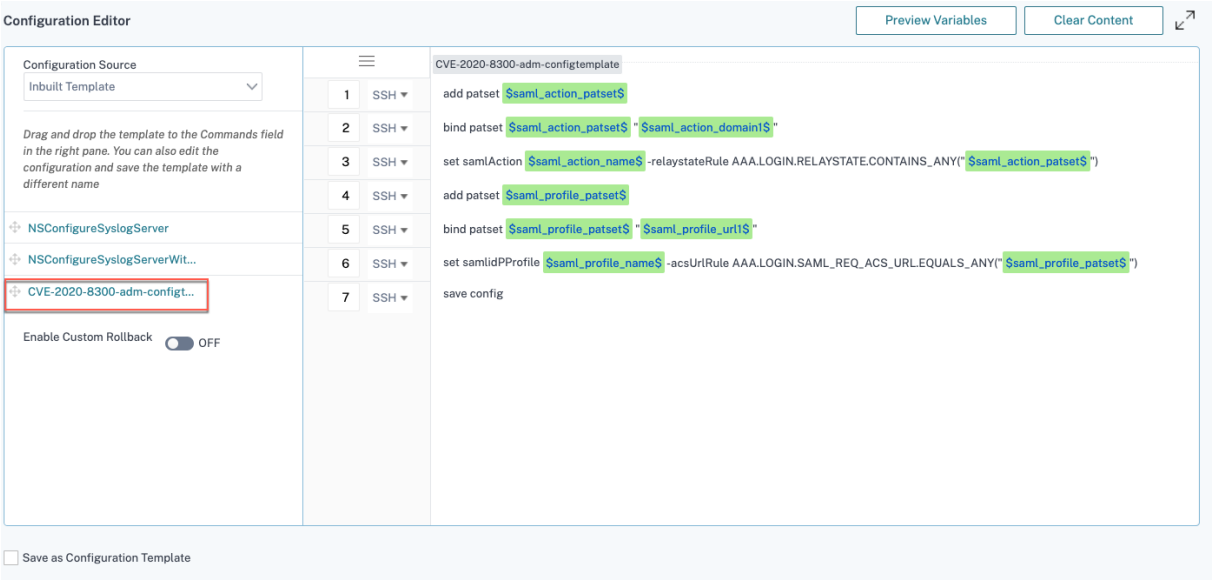
1. Customizing the configuration.
2. Reviewing the auto-populated impacted instances.
3. Specifying inputs for variables for the job.
4. Reviewing the final config with variable inputs populated.
5. Running the job.

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.

Step 1: Select configuration In the configuration job workflow, the built-in configuration template auto-populates under **Select configuration**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



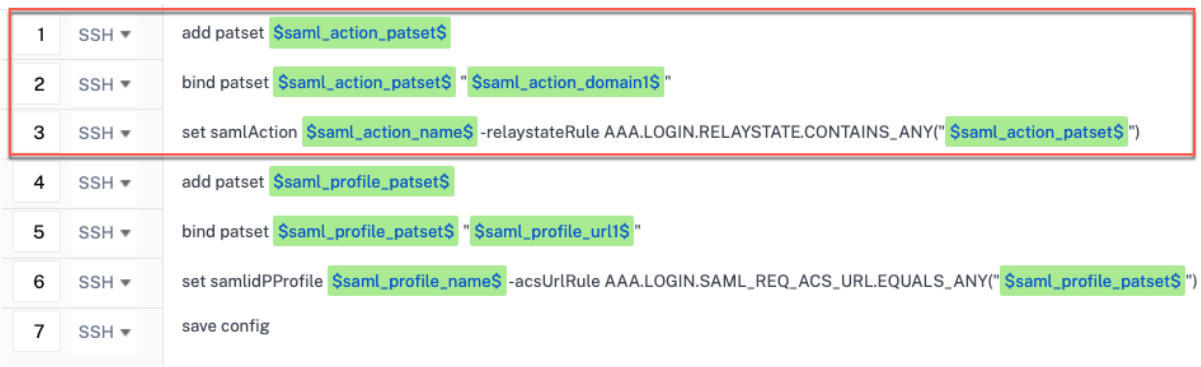
Run a separate configuration job for each impacted NetScaler instance, one at a time, and include all SAML actions and SAML profiles for that NetScaler. For example, if you have two vulnerable NetScaler instances each having two SAML actions and two SAML profiles, you must run this configuration job 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.



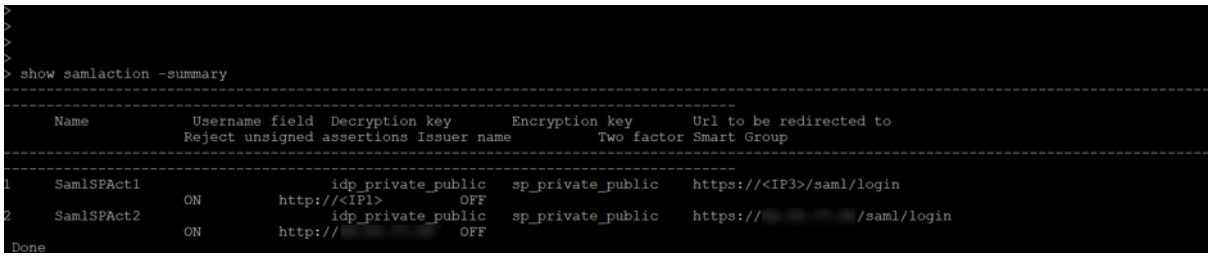
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:

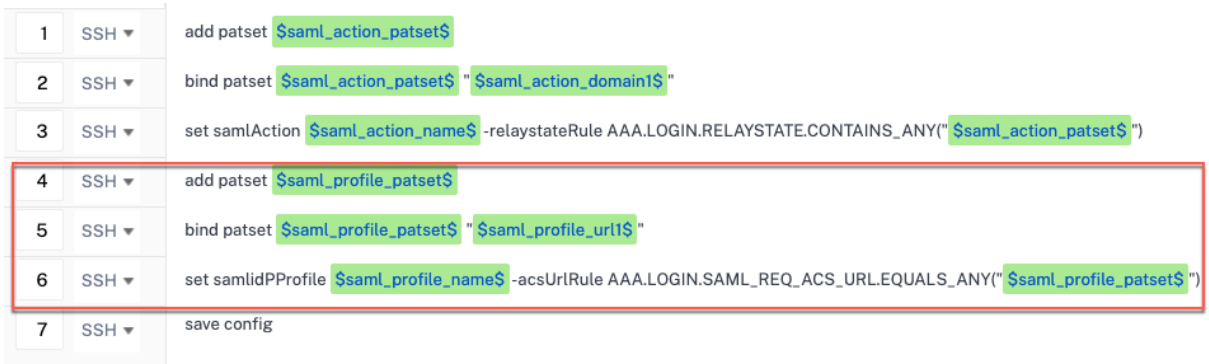
- `saml_action_patset`: is the config template variable, and it represents the value of the name of the pattern set (patset) for the SAML action. You can specify the real value in step 3 of the config job workflow. See the section Step 3: Specify variable values in this doc.
- `saml_action_domain1`: 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`.



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.



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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

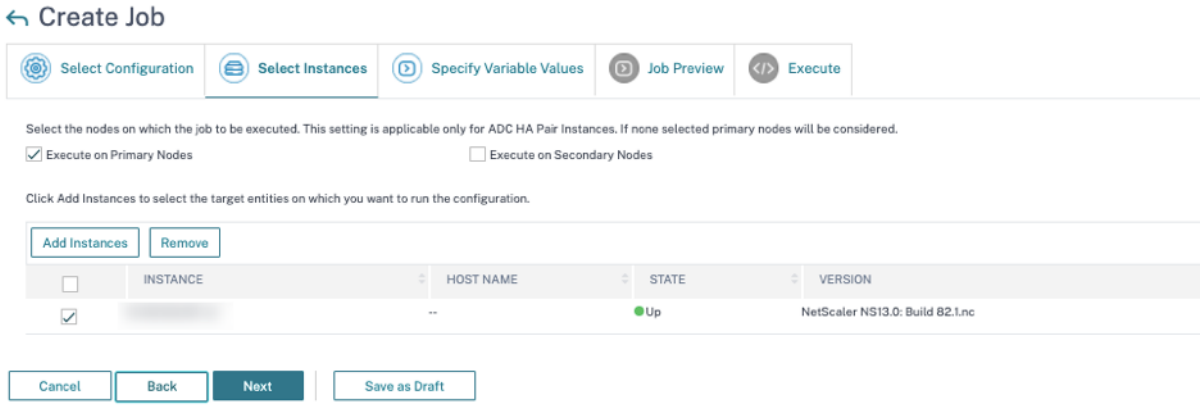
- `saml_profile_patset`: is the config template variable, and it represents the value of the name of the pattern set (patset) for the SAML profile. You can specify the real value in step 3, of the config job workflow. See the section Step 3: Specify variable values in this document.
- `saml_profile_url1`: 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**.



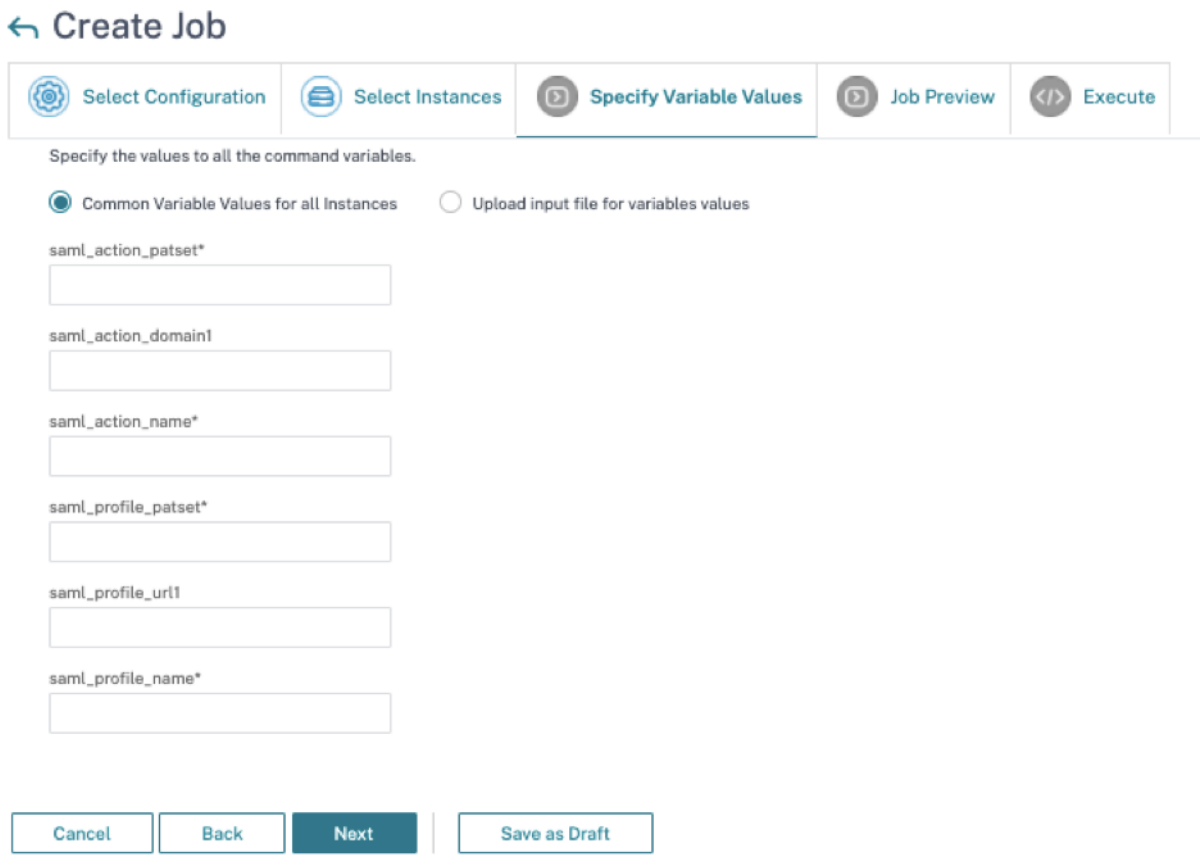
Step 3: Specify variable values Enter the variable values.

- `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`

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- `saml_profile_name`: enter the same of the SAML profile for which you are configuring the job

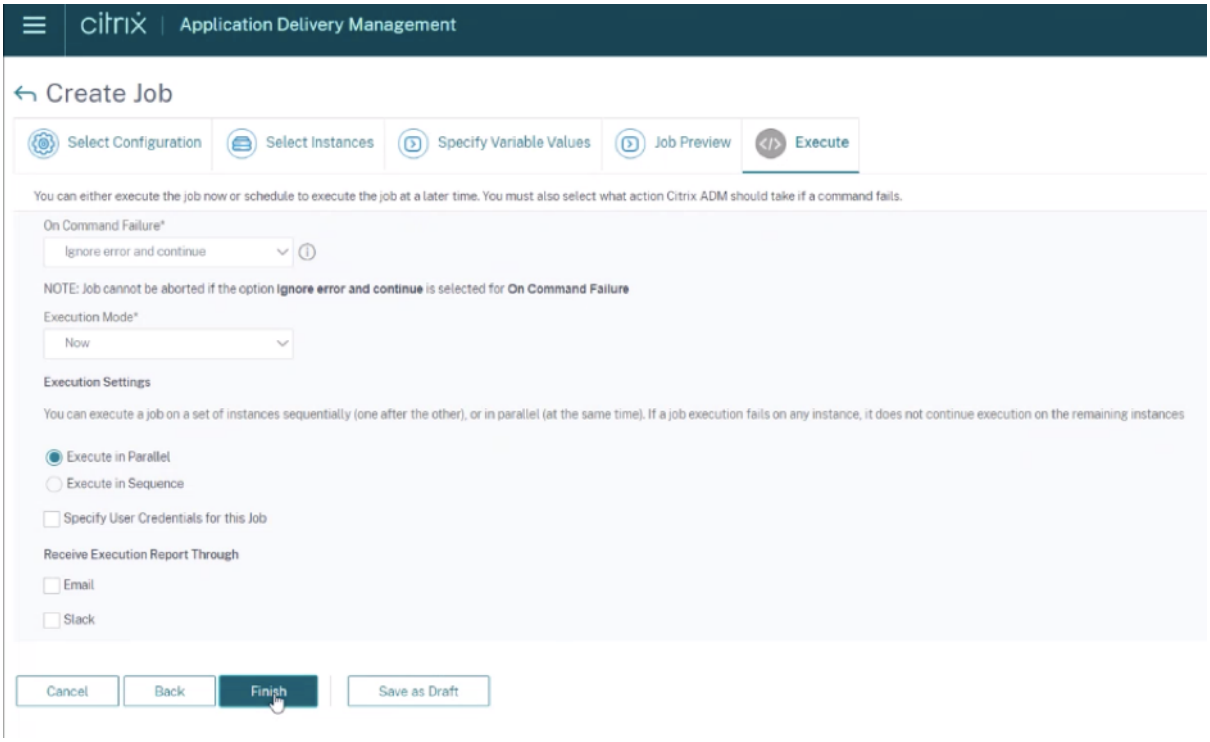
> **Note**
>
> For URLs, the extension is not always `cgi/samlauth`. It depends on what third-party authorization you have, and accordingly you must put the extension.



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.

© 1997–2025 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 respectively. In the NetScaler Console UI under **Infrastructure > Jobs**, you see only the last two configuration jobs.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

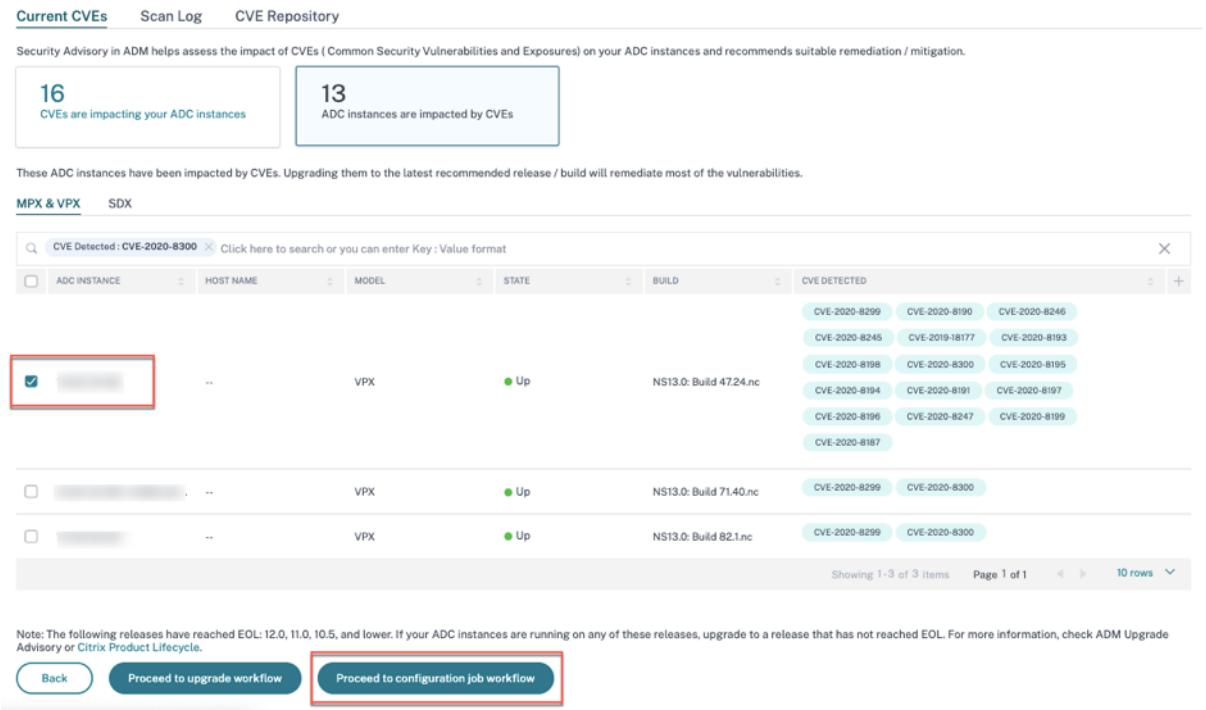
Scenario

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
SAML action 1 has one domain, and SAML action 2 has two domains	SAML profile 1 has one URL, and SAML profile 2 has two URLs



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.

© 1997–2025 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_domain1
SAML action 2 has two domains	saml_action_patset2	saml_action_name2	saml_action_domain2, saml_action_domain3

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

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



© 1997–2025 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**.

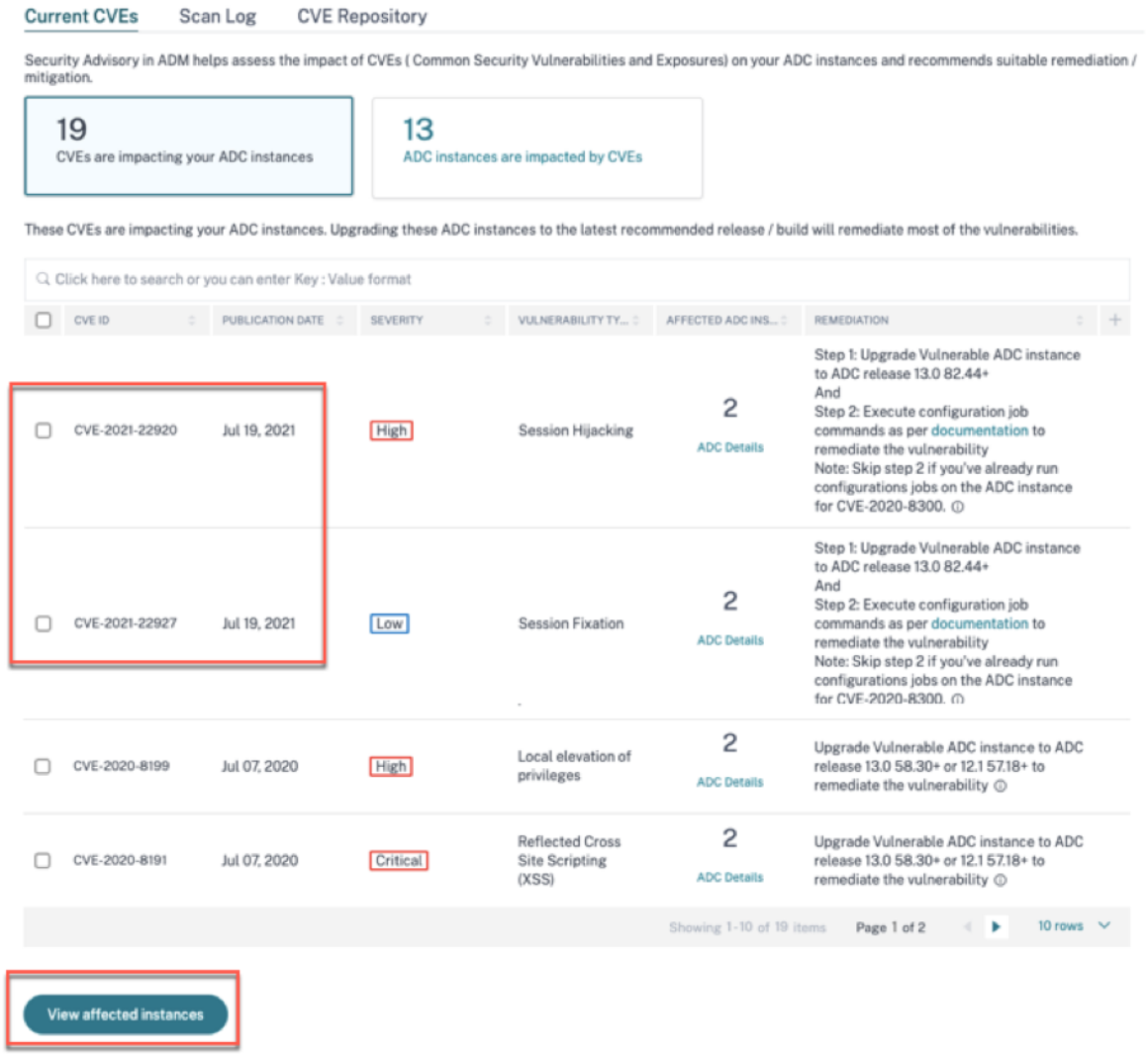
After completing the two remediation steps for NetScaler 1, follow the same steps to remediate NetScaler 2 and NetScaler 3. After remediation is complete, you can run an on-demand scan to see the revised security posture.

Remediate vulnerabilities for CVE-2021-22927 and CVE-2021-22920

January 8, 2024

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**.

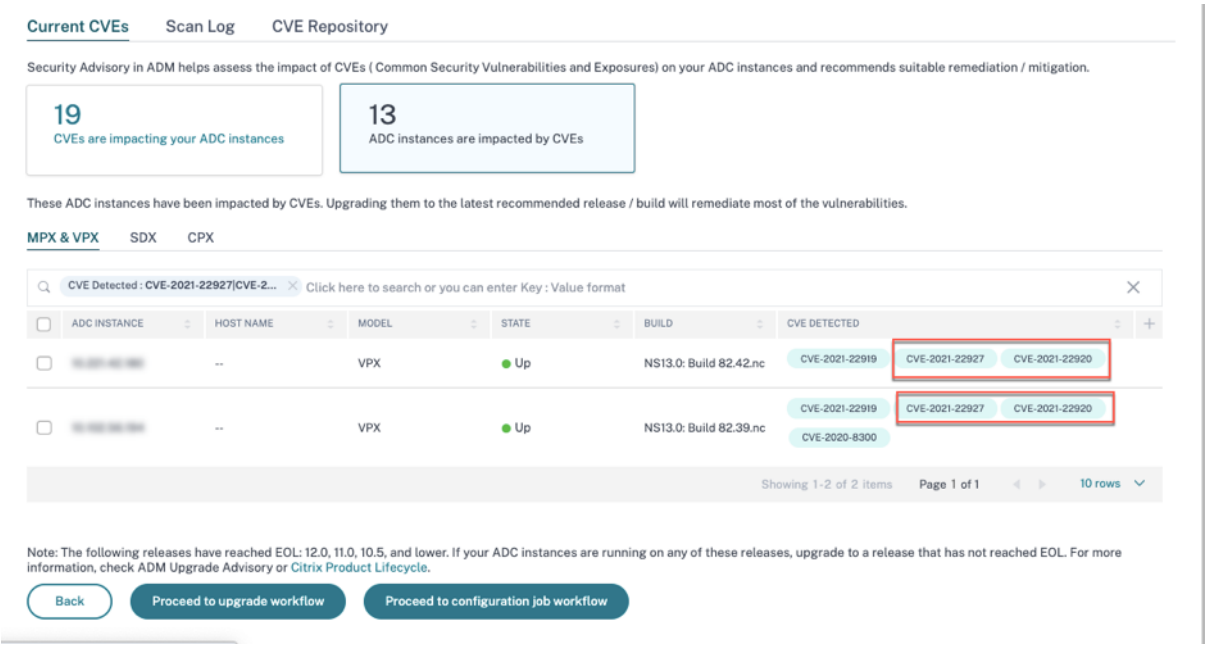
© 1997–2025 Citrix Systems, Inc. All rights reserved.



> **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.

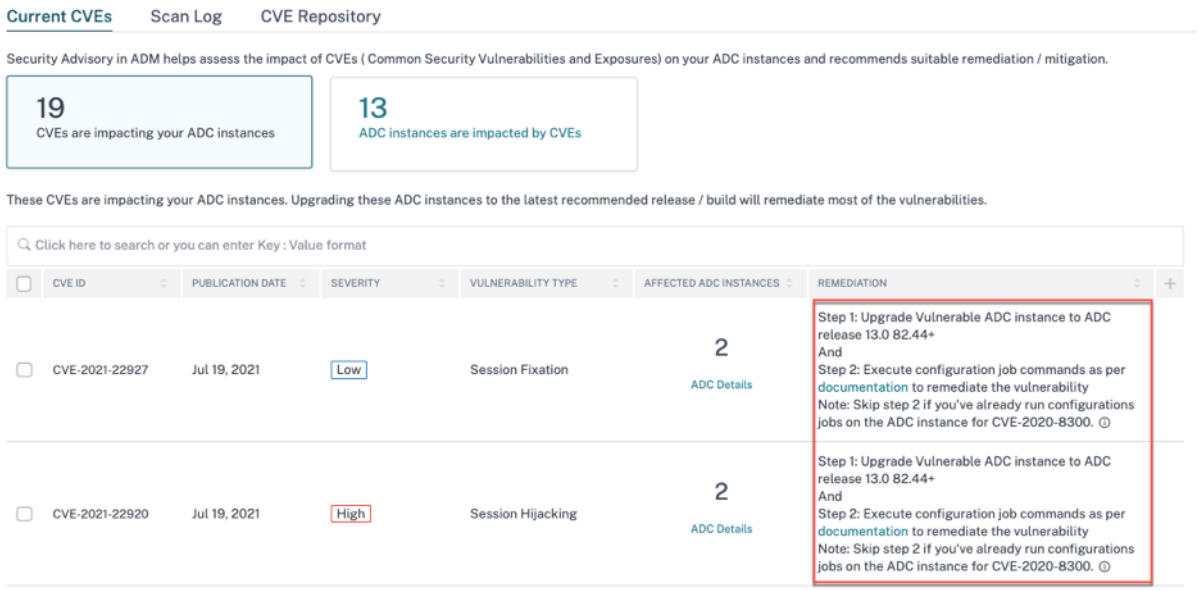
The **<number of> NetScaler instances impacted by CVEs** window appears. In the following screen capture, you can see the count and details of the NetScaler instances impacted by CVE-2021-22927 and CVE-2021-22920.

© 1997–2025 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:

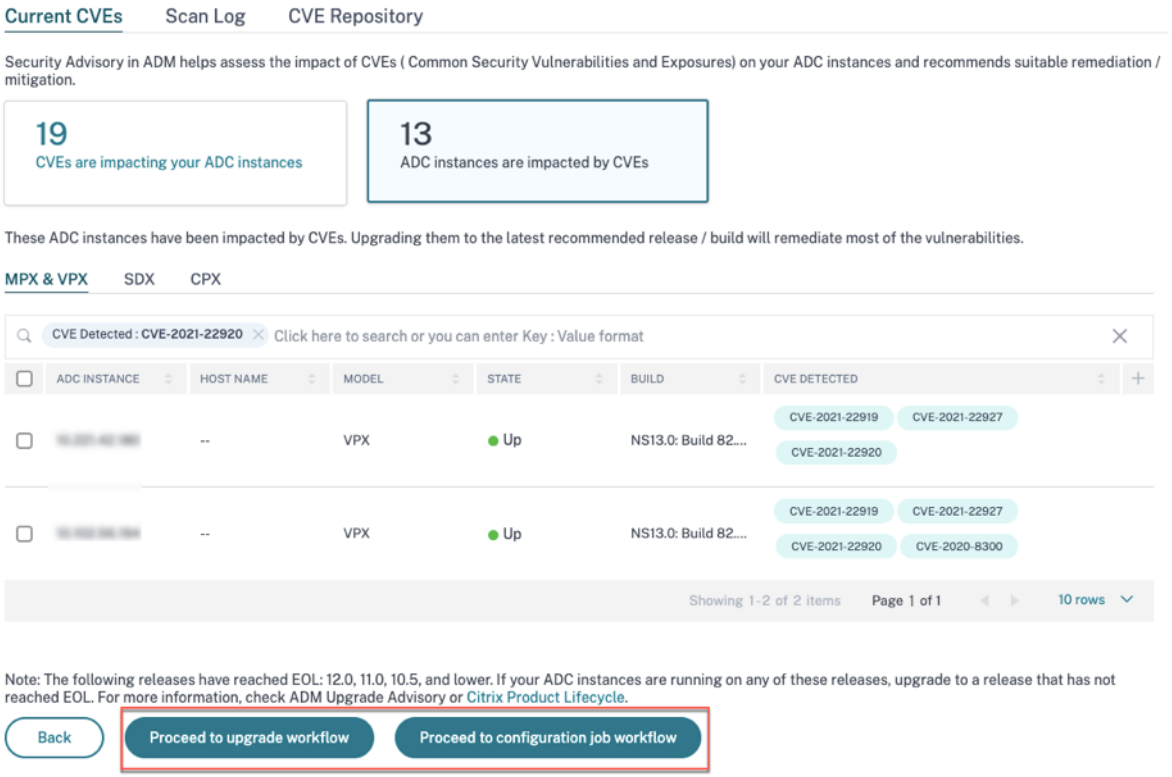
1. Upgrading the vulnerable NetScaler instances to a release and build that has the fix.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

> **Note**
>
> Skip step 2 if you've already run configuration jobs on the NetScaler instance for CVE-2020-8300.

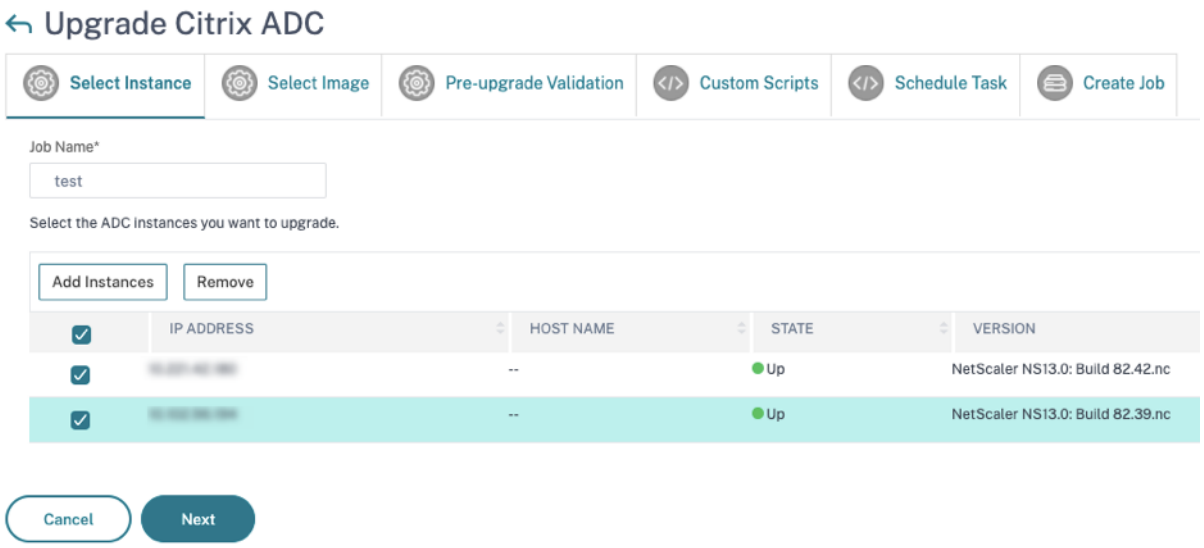
Under **Current CVEs> NetScaler instances impacted by CVEs**, you see two separate workflows for this 2-step remediation process: which are **Proceed to upgrade workflow** and **Proceed to configuration job workflow**.



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.

© 1997–2025 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.

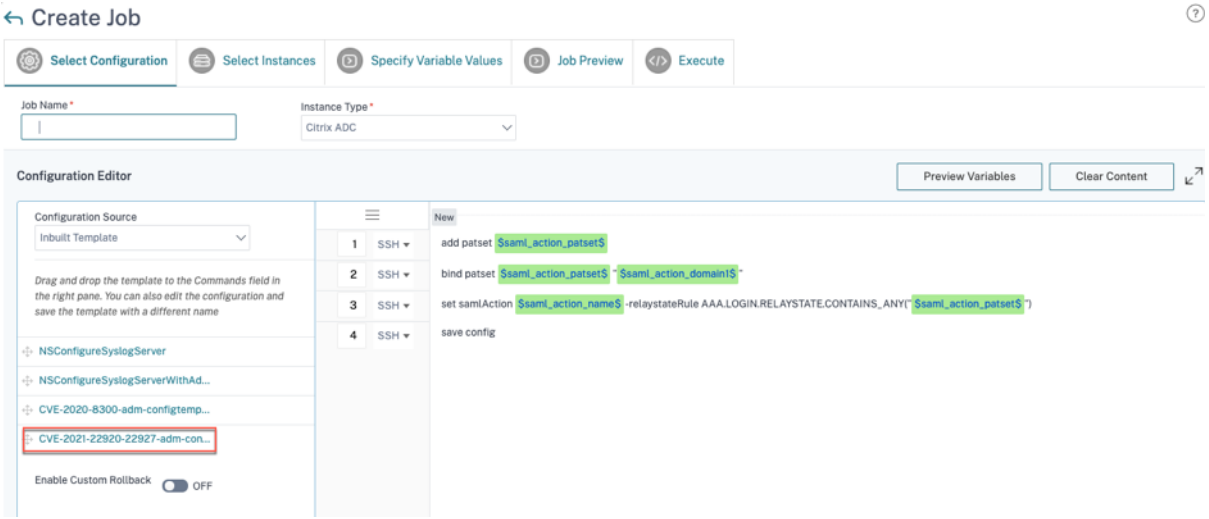
1. Customizing the configuration.
2. Reviewing the auto-populated impacted instances.
3. Specifying inputs for variables for the job.
4. Reviewing the final config with variable inputs populated.
5. Running the job.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.



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 re-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> quired for all the three CVEs. Customize this base template according to your NetScaler instance deployment and requirement.

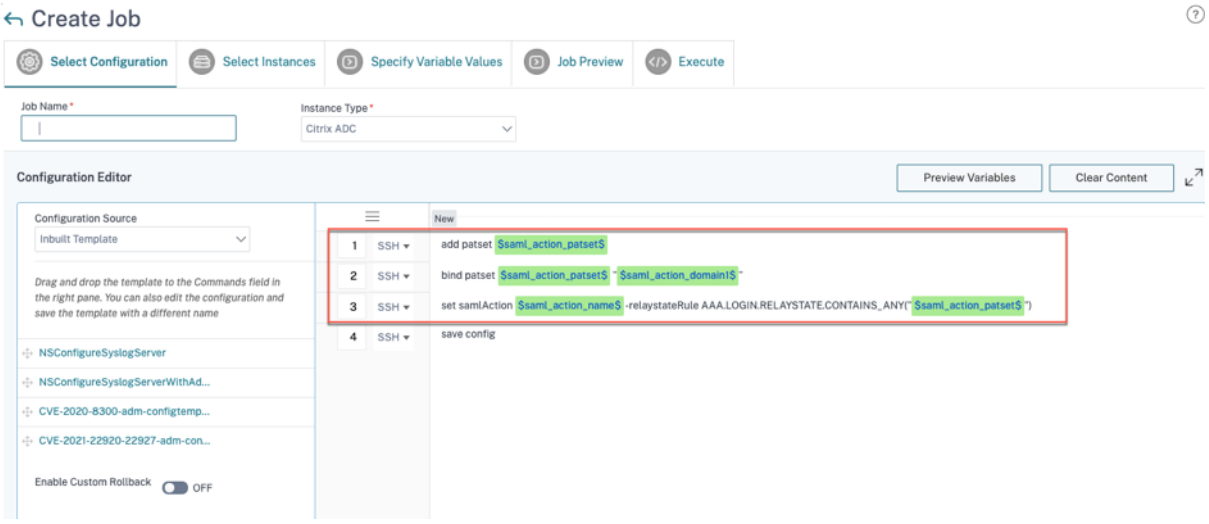
You must run a separate configuration job for each impacted NetScaler instance, one at a time, and include all SAML actions for that NetScaler. For example, if you have two vulnerable NetScaler instances each having two SAML actions, you must run this configuration job two times. One time per NetScaler 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.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

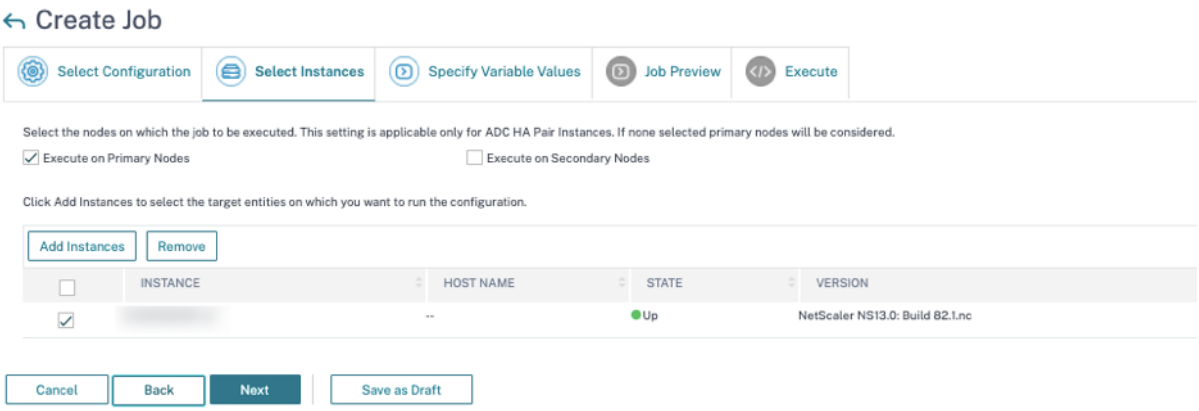
- `saml_action_domain1`: is the config template variable, and it represents the domain name for that specific SAML action. You can specify the real value in step 3, of the config job workflow. See the section Step 3: Specify variable values in this doc.

To find all the SAML actions for a device, run the command `show samlaction`.



Step 2: Select the instance

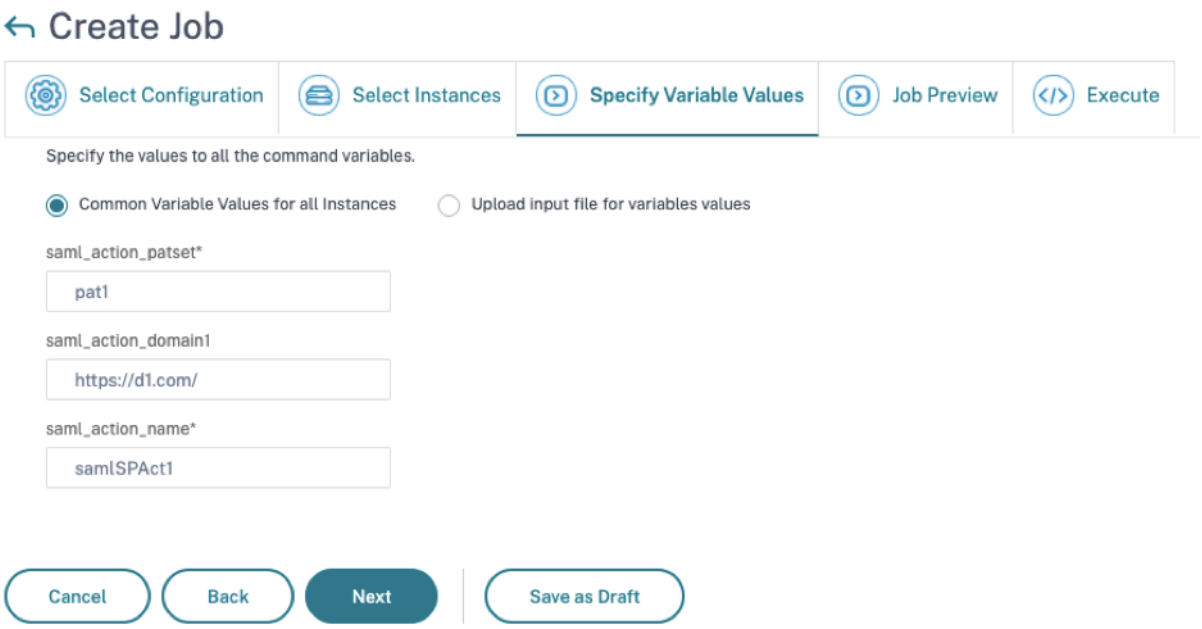
The impacted instance is auto-populated under **Select Instances**. Select the instance and click **Next**.



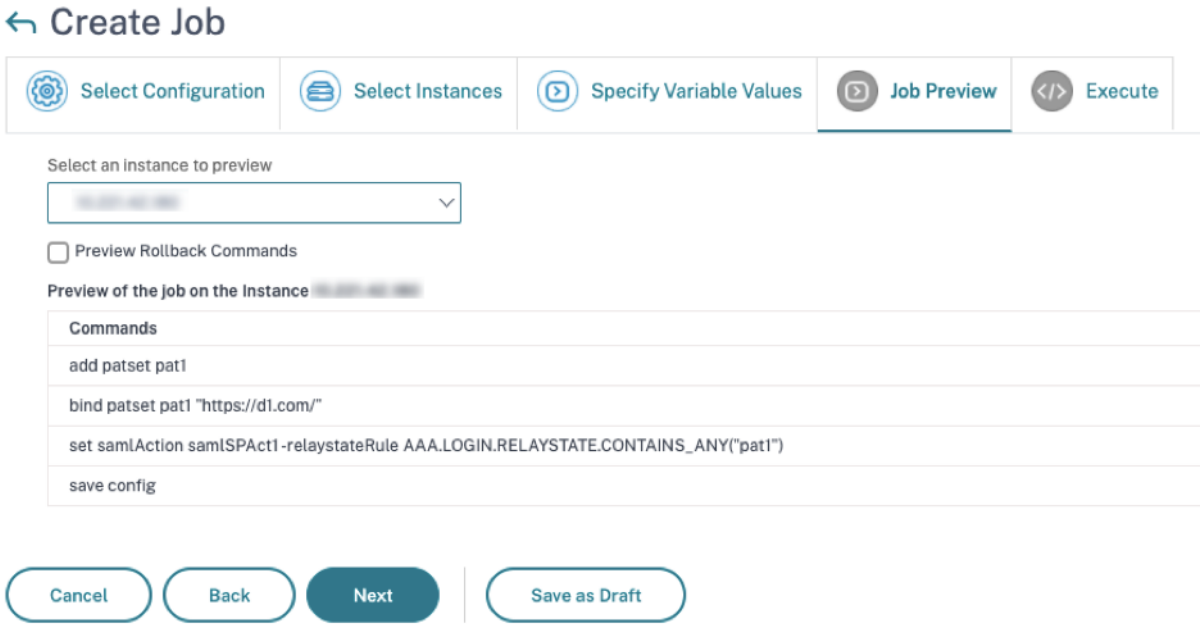
Step 3: Specify variable values Enter the variable values.

- `saml_action_patset`: add a name for the SAML action
- `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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

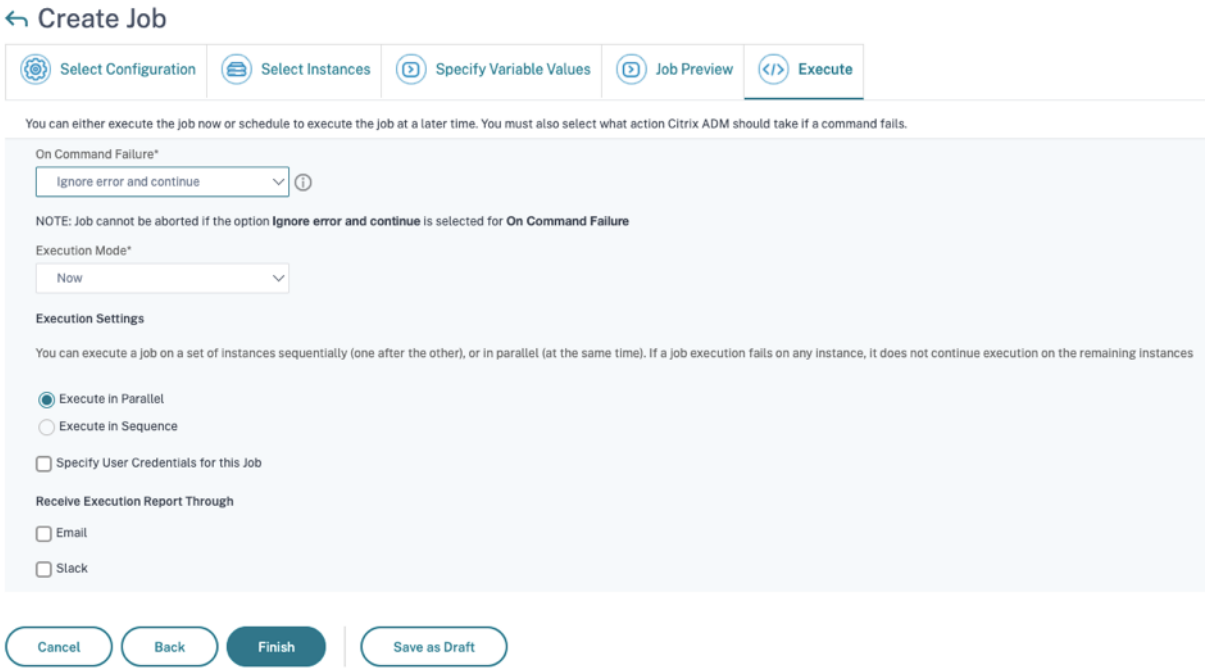


Step 4: Preview the configuration Previews the variable values having been inserted in the config and click **Next**.



Step 5: Run the job Click **Finish** to run the configuration job.

© 1997–2025 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

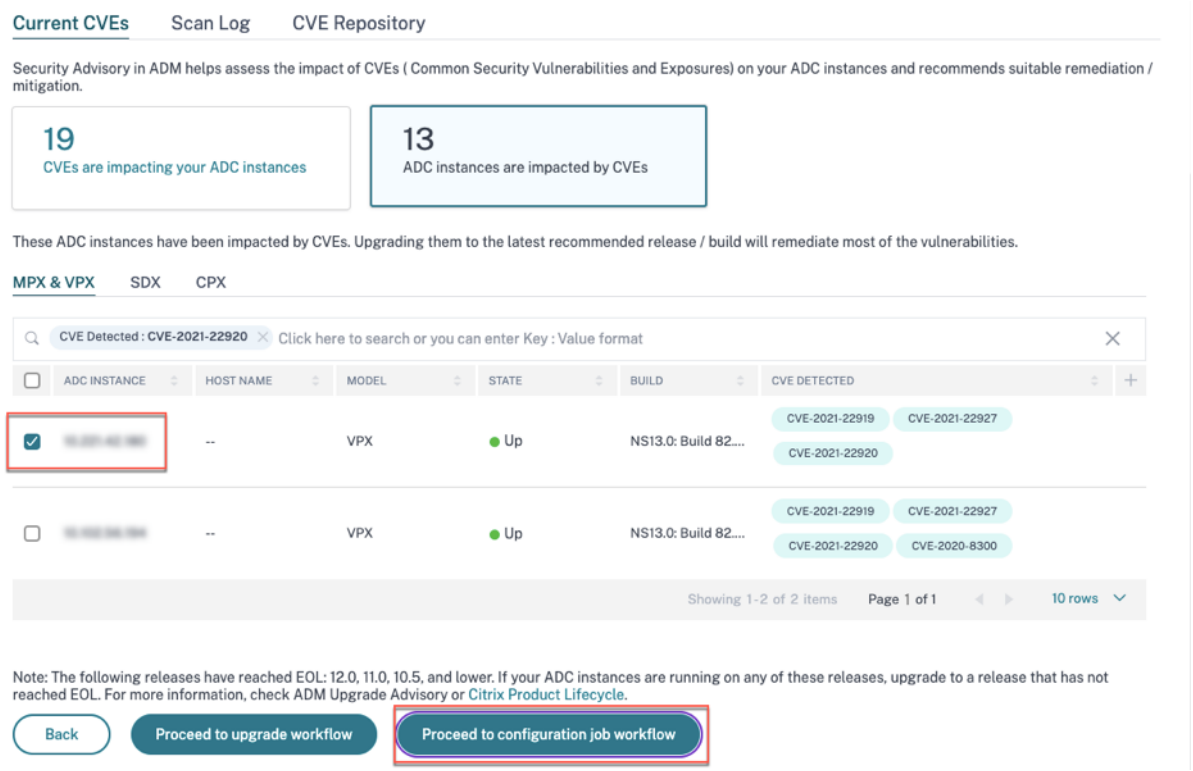
In this scenario, two NetScaler instances are vulnerable to CVE-2021-22920, and you need to remediate all the instances. Follow these steps:

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.

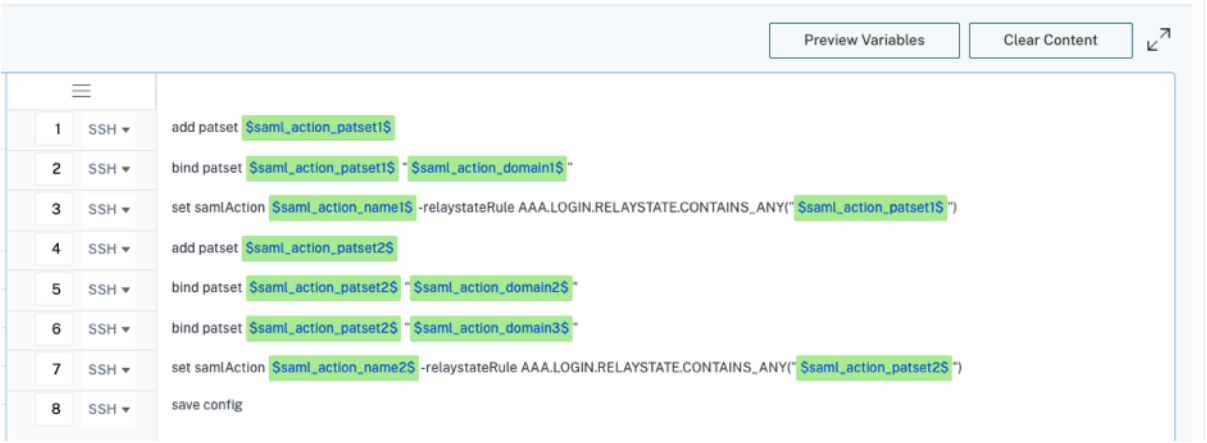
The vulnerable NetScaler 1 has two SAML actions:

- SAML action 1 has one domain
- SAML action 2 has two domains

© 1997–2025 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.

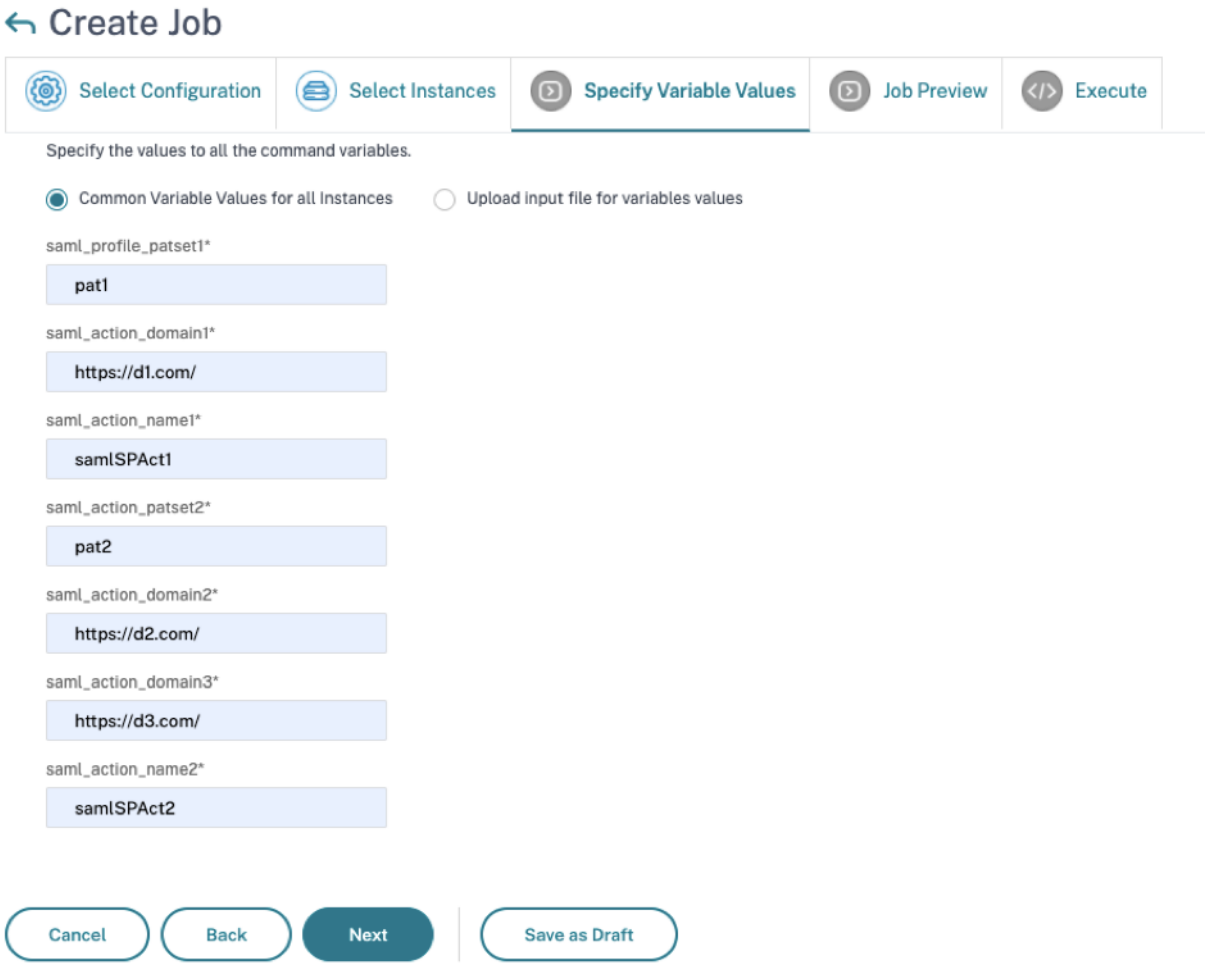
Table. Variable definitions for SAML action

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_domain1

© 1997–2025 Citrix Systems, Inc. All rights reserved.

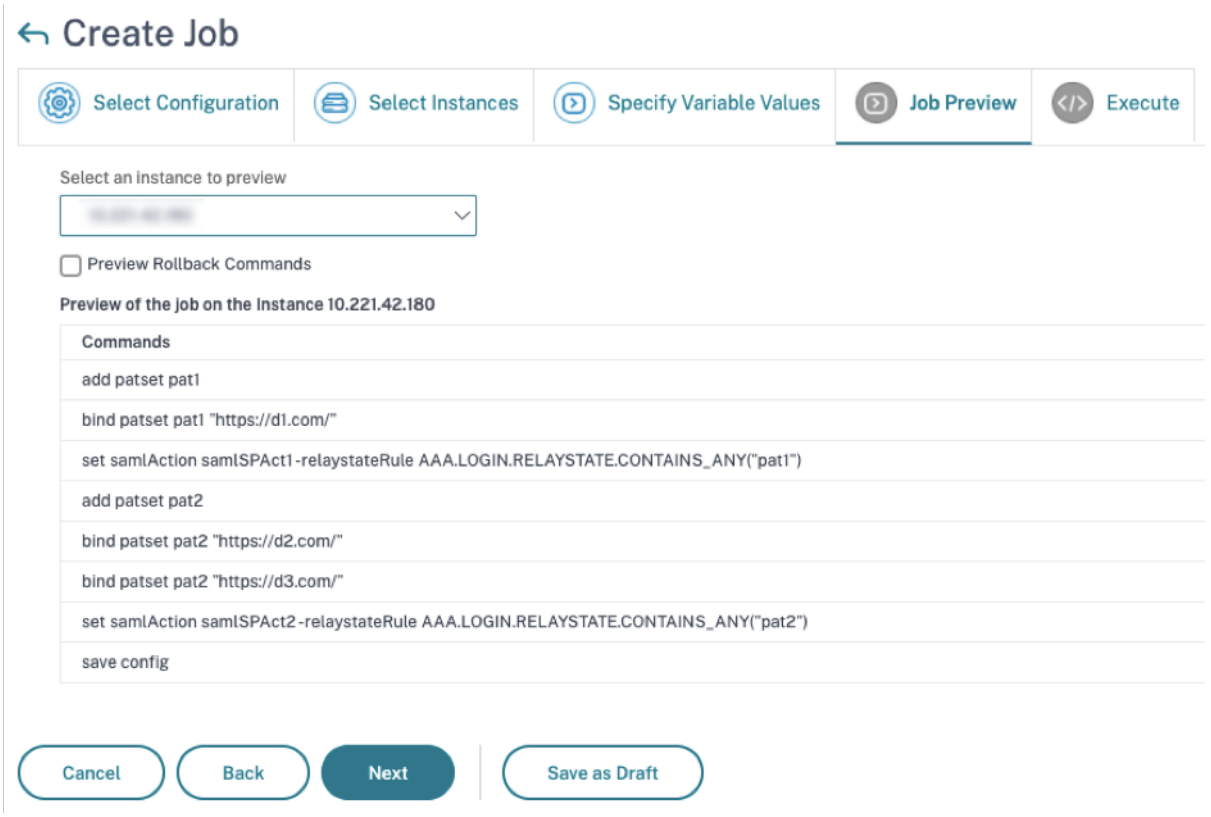
NetScaler configuration	Variable definition for patset	Variable definition for SAML action name	Variable definition for domain
SAML action 2 has two domains	saml_action_patset2	saml_action_name2	saml_action_domain2, saml_action_domain3

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.

© 1997–2025 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**.

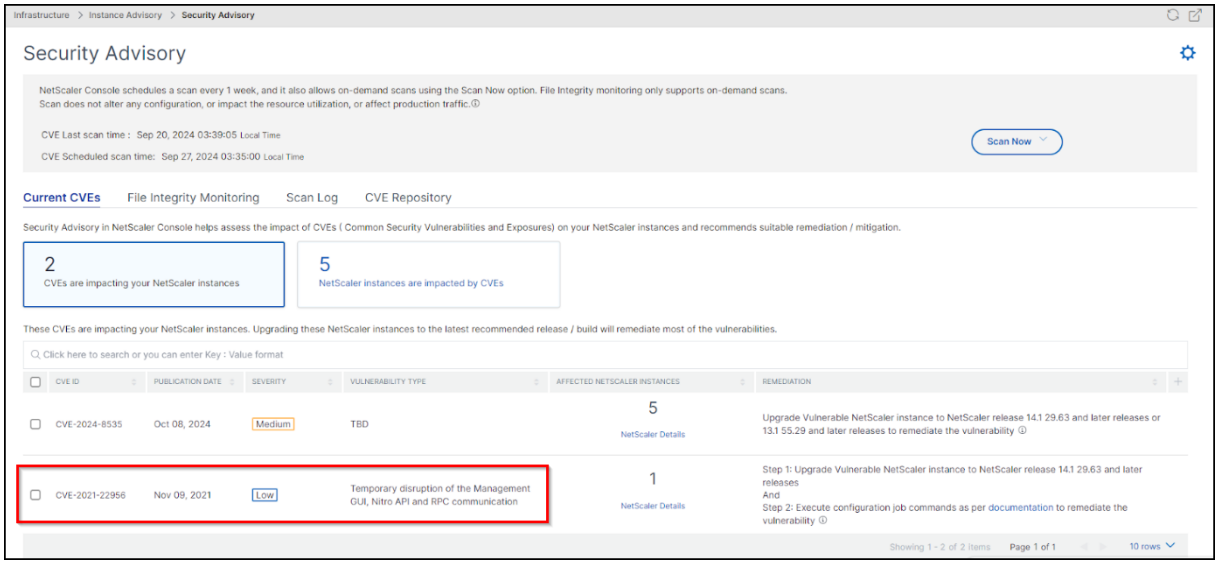
After completing the two remediation steps for NetScaler 1, follow the same steps to remediate NetScaler 2 and NetScaler 3. After remediation is complete, you can run an on-demand scan to see the revised security posture.

Identify and remediate vulnerabilities for CVE-2021-22956

September 8, 2025

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**.

© 1997–2025 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

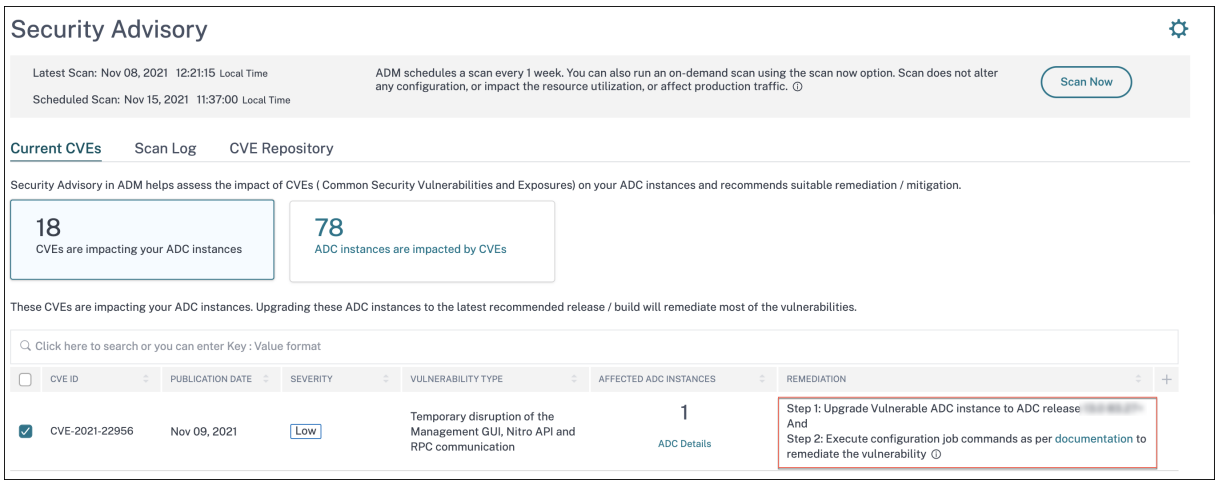
CVE-2021-22956 requires a custom scan, in which the NetScaler Console connects with the managed NetScaler instance and pushes a script to the instance. The script runs on the NetScaler instance and checks the Apache configuration file (`httpd.conf file`) and maximum client connections (`maxclient`) parameters 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 a detailed report of this list in the CSV file that you can download from the **Scan Logs** tab on **Security Advisory** page.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

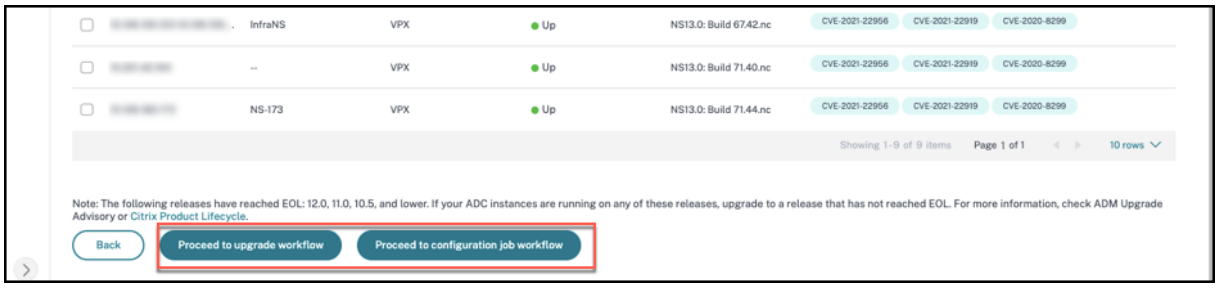
For CVE-2021-22956 -impacted NetScaler instances, the remediation is a two-step process. In the GUI, under **Current CVEs > NetScaler instances are impacted by CVEs**, you can see step 1 and 2.



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.



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.

© 1997–2025 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.

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.

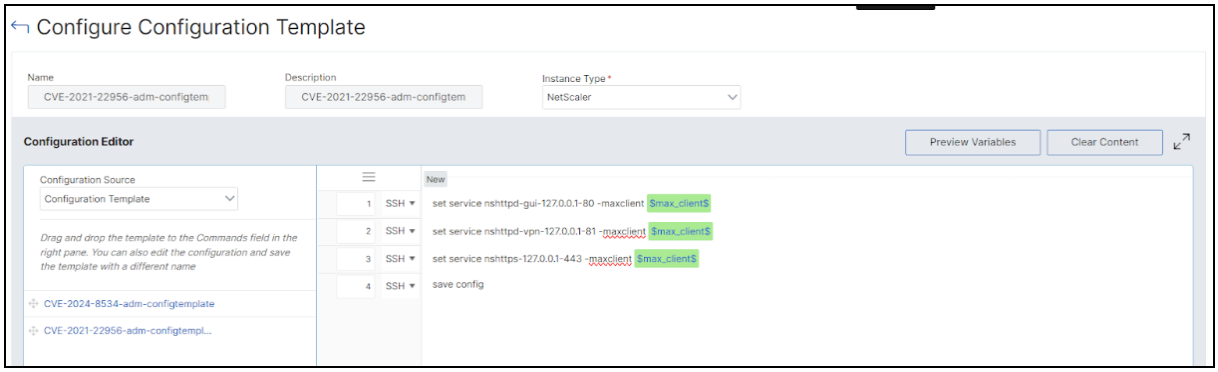
1. Customizing the configuration.
2. Reviewing the auto-populated impacted instances.
3. Specifying inputs for variables for the job.
4. Reviewing the final config with variable inputs populated.
5. Running the job.

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**.
- 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.

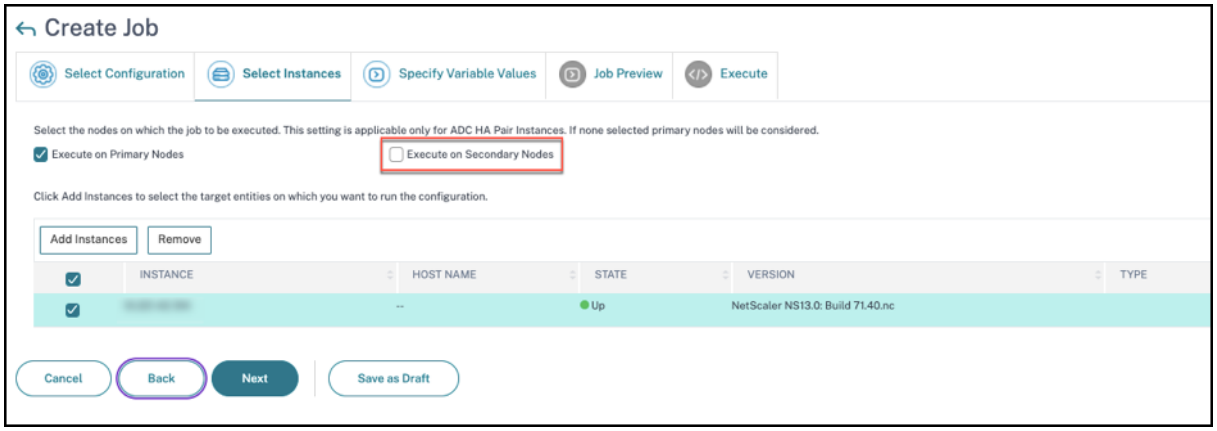
Step 1: Select configuration In the configuration job workflow, the built-in configuration base template auto-populates under **Select configuration**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Step 2: Select the instance

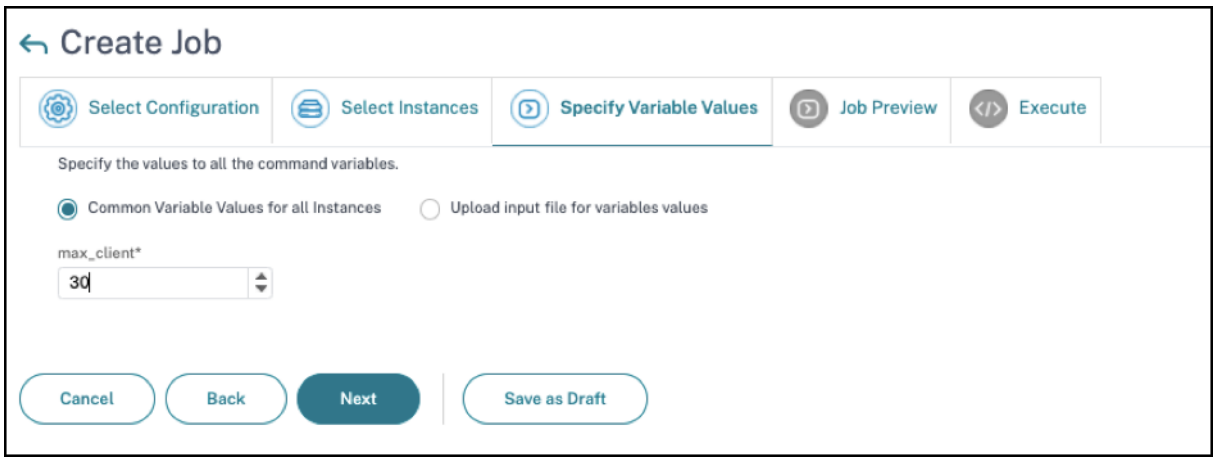
The impacted instance is auto-populated under **Select Instances**. Select the instance. If this instance is part of an HA pair, select **Execute on Secondary Nodes**. Click **Next**.



> **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 Enter the variable values.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Select one of the following options to specify variables for your instances:

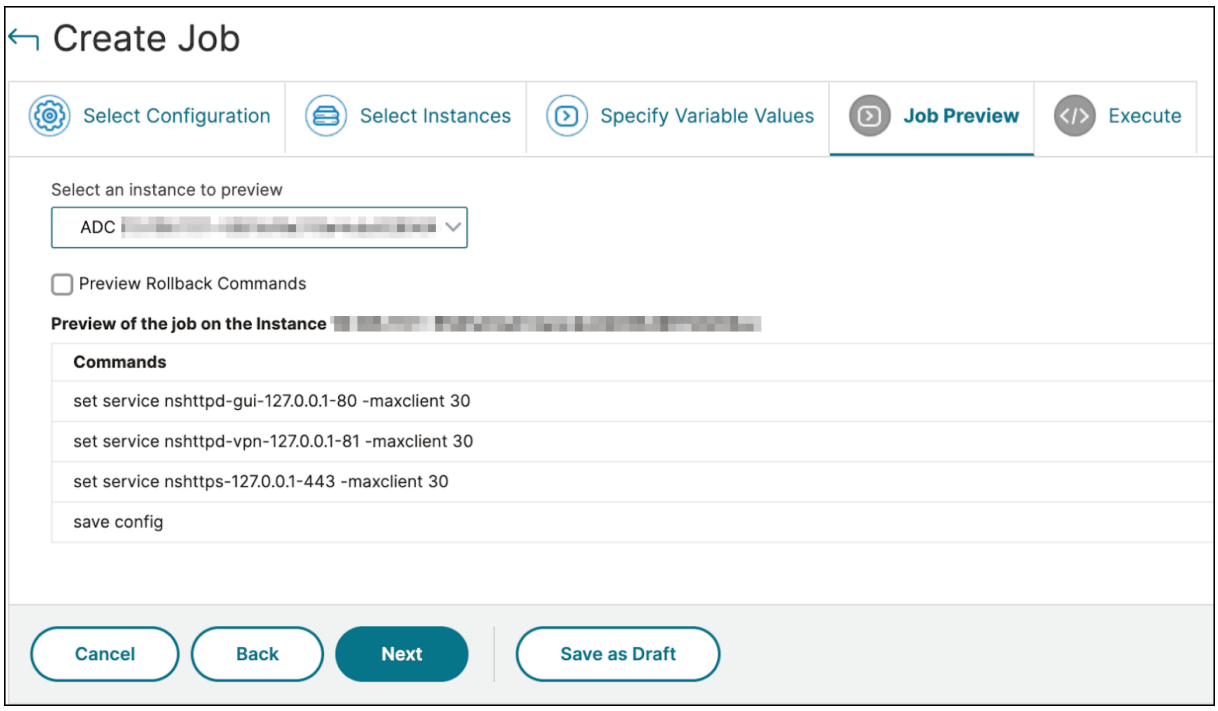
Common variable values for all instances: Enter a common value for the variable `max_client`.

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.

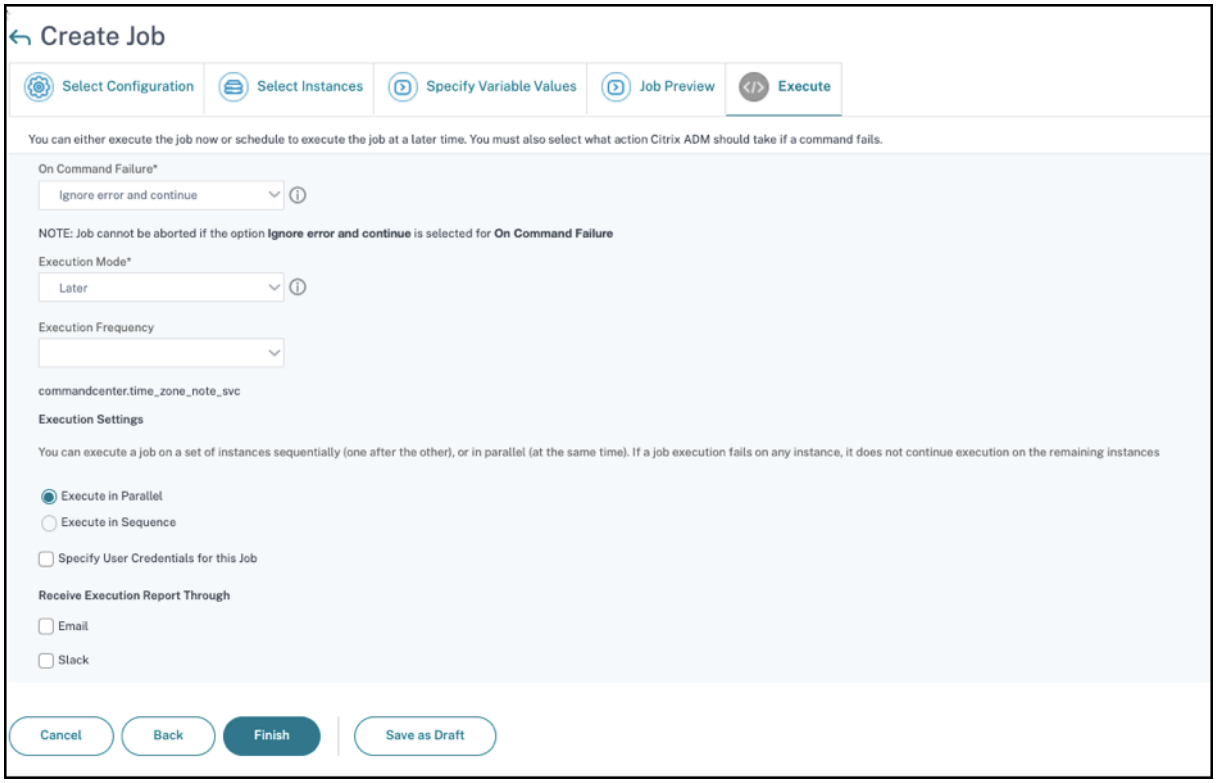
> **Note:**
>
> For both options mentioned above, the recommended `max_client` value is 30. You can set the value according to your present value. However, it should not be zero, and it should be less than or equal to the max_client set in the `/etc/httpd.conf` file. You can check the present value set 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**.

© 1997–2025 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-

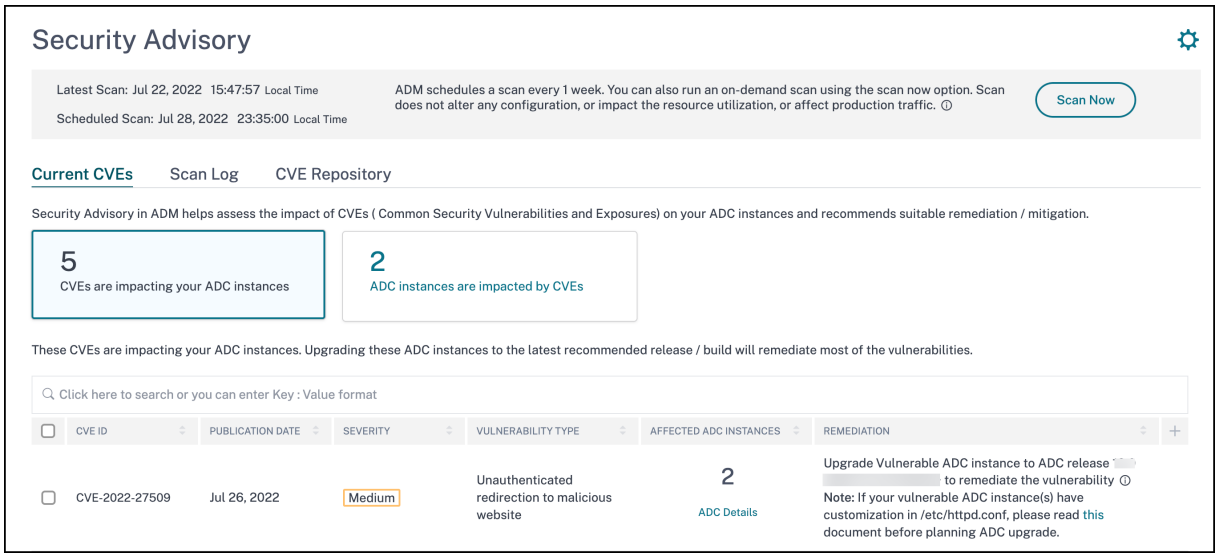
© 1997–2025 Citrix Systems, Inc. All rights reserved.

demand scan to see the revised security posture.

Identify and remediate vulnerabilities for CVE-2022-27509

January 8, 2024

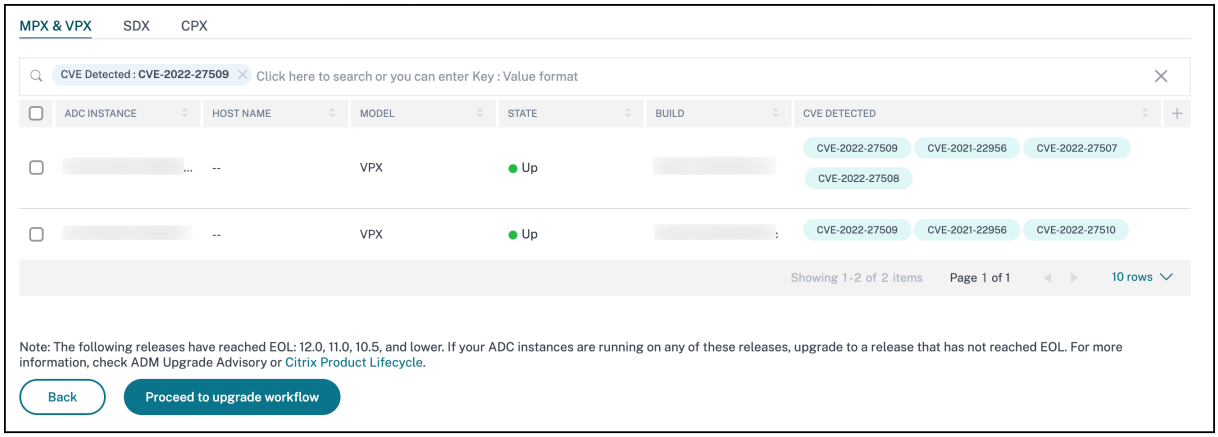
In the NetScaler Console security advisory dashboard, under **Current CVEs <number of> NetScaler instances are impacted by CVEs**, you can see all the instances vulnerable due to CVE-2022-27509. To check the details of the instances impacted by the CVEs, select CVE-2022-27509 and click **View Affected 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.

© 1997–2025 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-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.

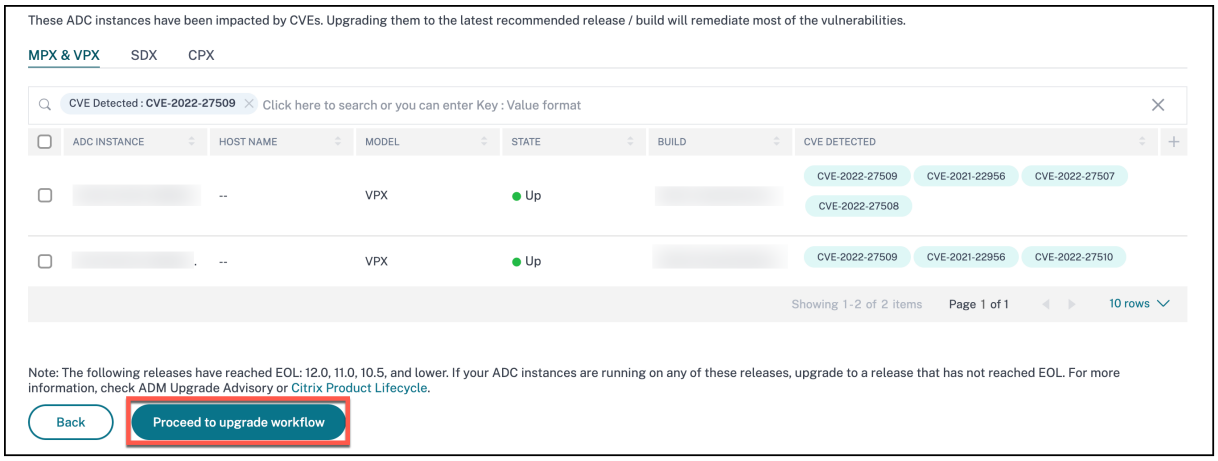
Under **Current CVEs> NetScaler instances impacted by CVEs**, you see the following workflow for this single step remediation process, which is **Proceed to upgrade workflow**.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **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.



Unsupported CVEs in Security Advisory

January 8, 2024

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

As a result, the detection and remediation of this vulnerability is out of NetScaler Console Security Advisory scope.

Setting up

January 8, 2024

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.

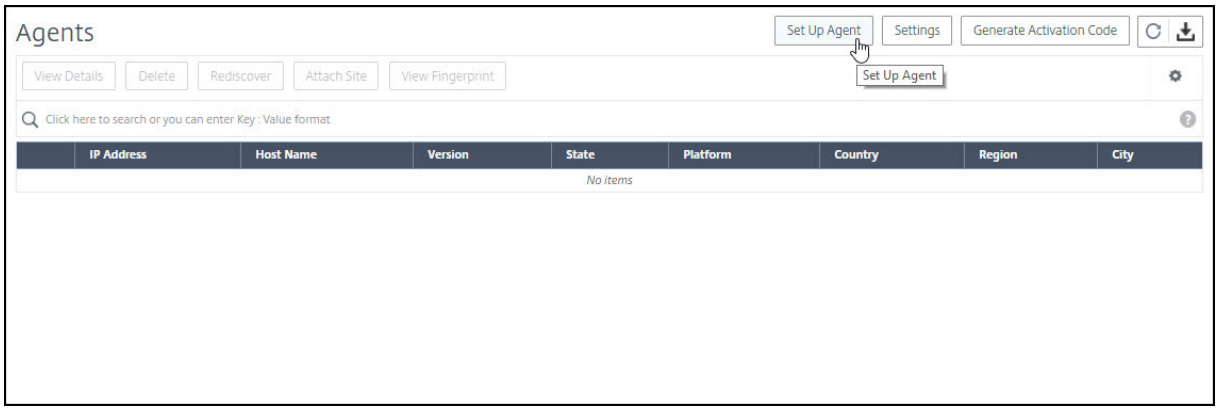
Adding multiple agents

January 8, 2024

© 1997–2025 Citrix Systems, Inc. All rights reserved.

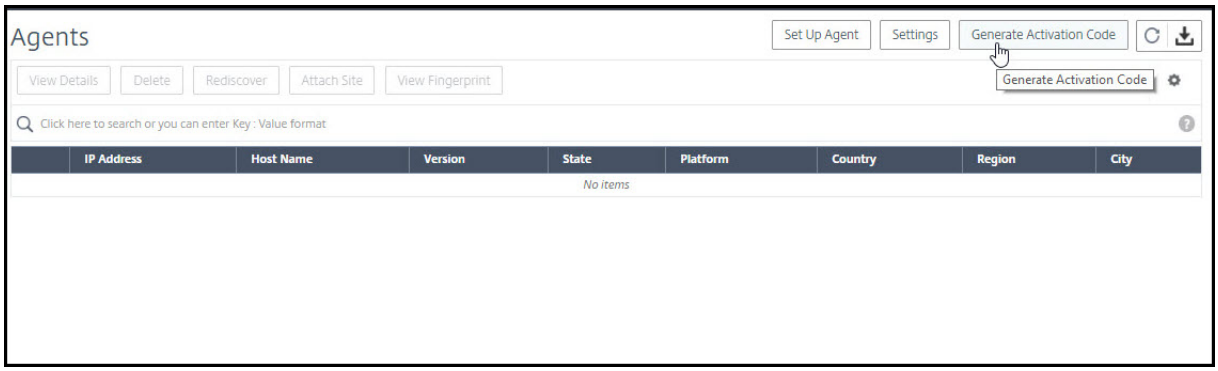
The number of agents to be installed depends on the number of managed instances in a data center and the total throughput. Citrix recommends that you install at least one agent for every data center.

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.**



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**.



After the agent is successfully installed and registered, verify the agent status on the service GUI and add instances to it.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **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

January 8, 2024

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.

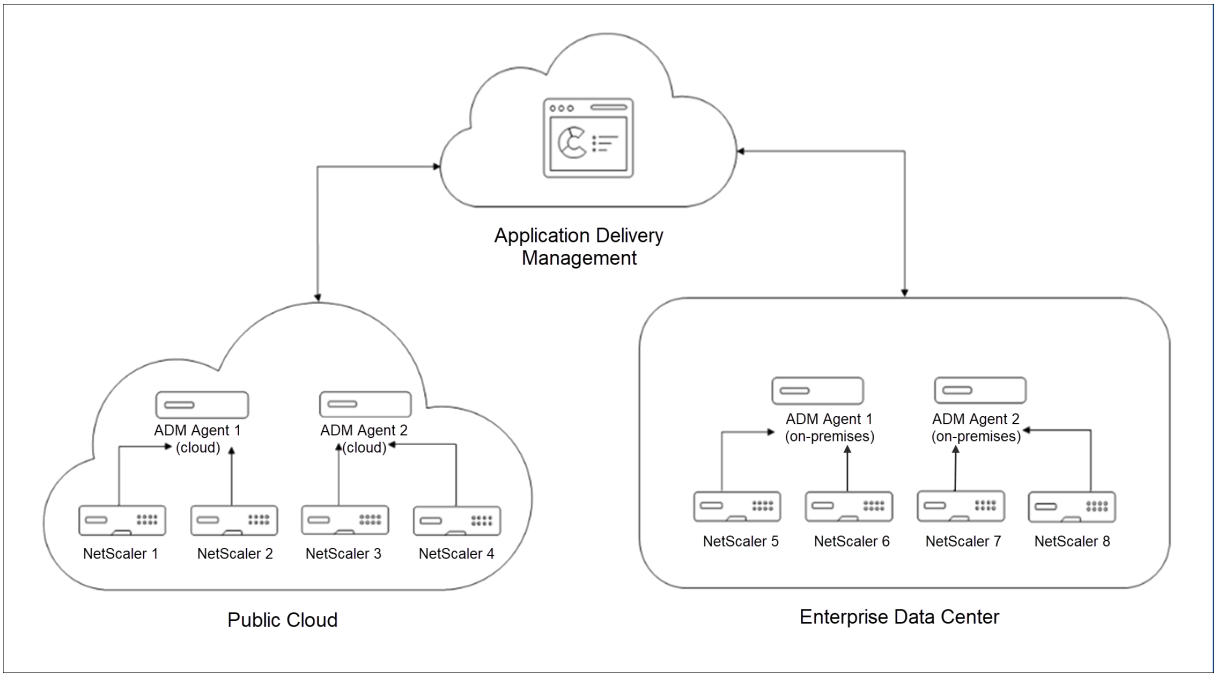
The following are the benefits of installing agents:

- 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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.

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. There-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> fore, 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.

Configuring agent upgrade settings

September 4, 2024

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**.

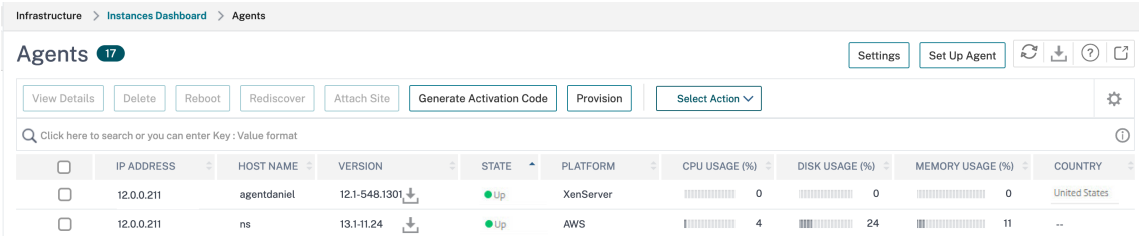
By default, an agent is upgraded automatically when a newer version is available. However, you can schedule an upgrade for each of the agents.

During the upgrade, there might be a downtime of approximately five minutes.

To configure agent upgrade settings:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

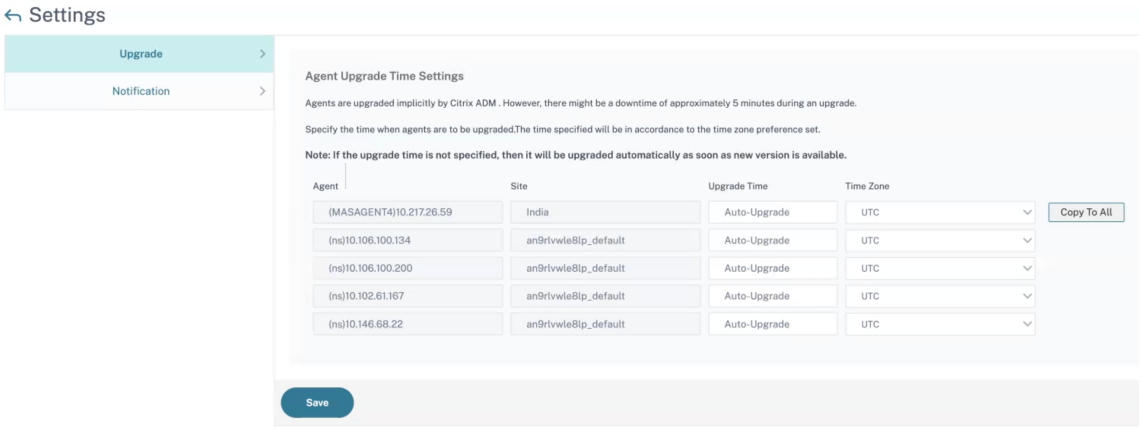
1. Navigate to **Infrastructure > Instances > Agents**, click **Settings**.



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.



   You can click **Copy to All** to apply the same upgrade time to all the agents.

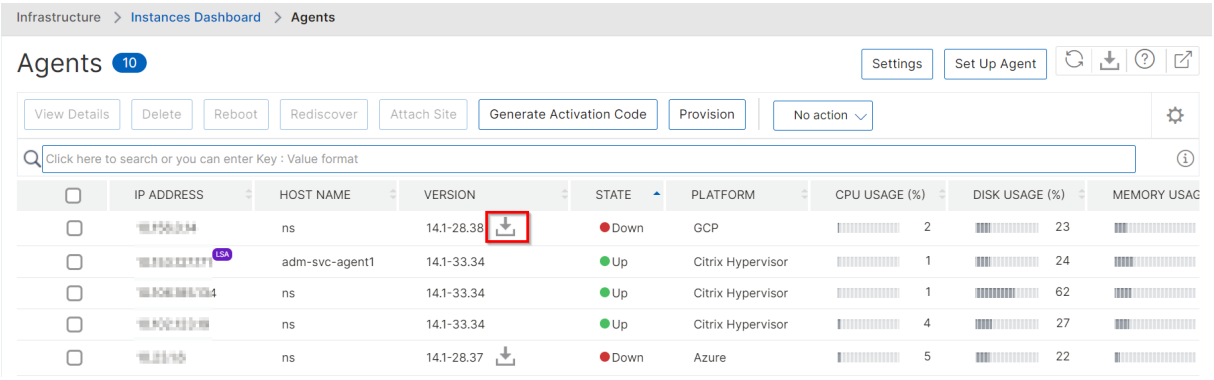
3. Click **Save**.

   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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.

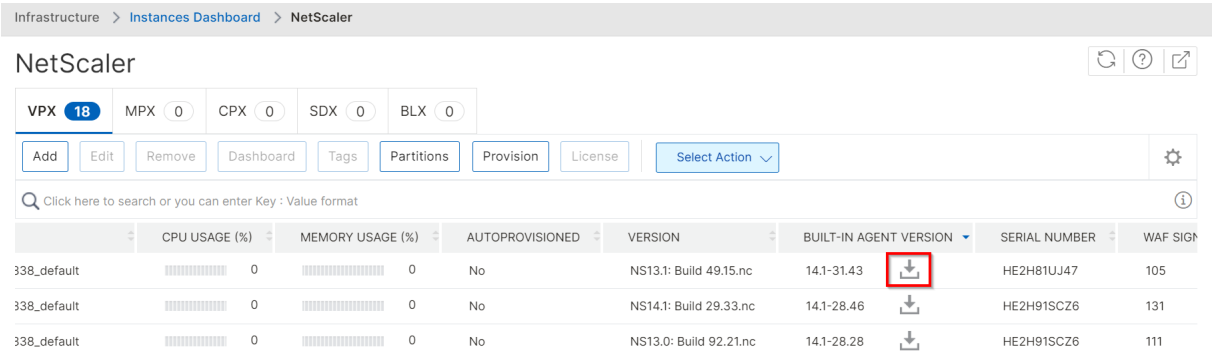
   ```
   cd /var/mps/mps_agent_images/latest
   tar -xzvf build-masagent.tgz
   ```

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.



1. In **Infrastructure > Instances > NetScaler**, download the latest build by clicking the download icon that is available in the version.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

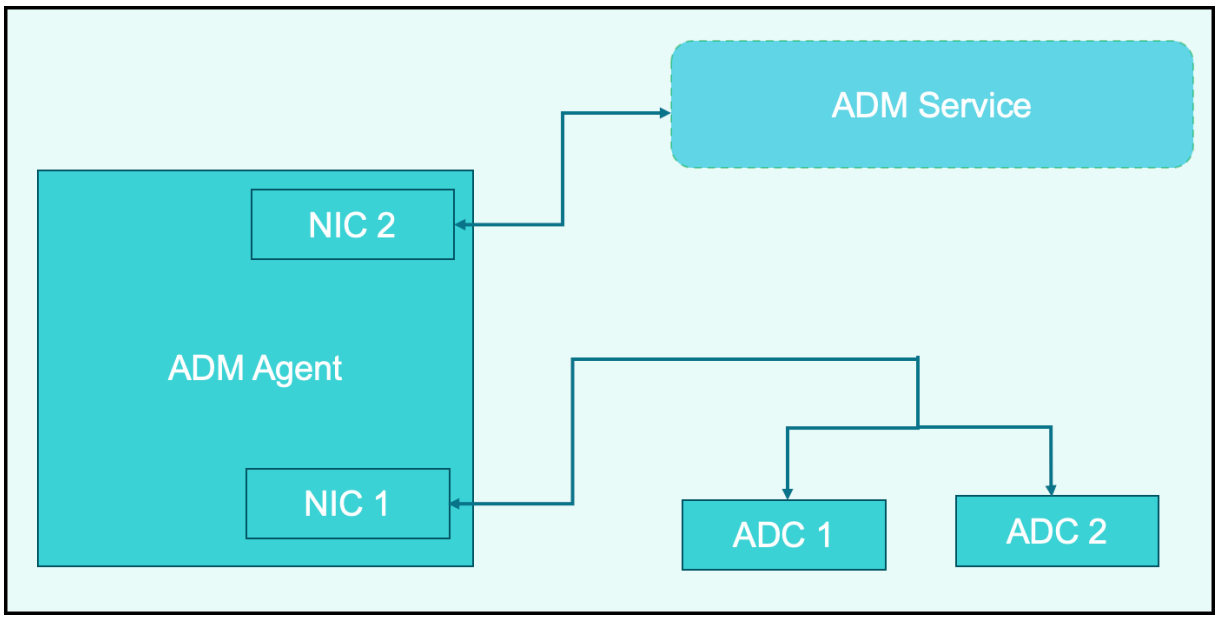
January 8, 2024

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.

> **Note**
>
> You cannot interchange the functionality and configuration of both the NICS.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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).

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 -

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- NIC 1 –For communication between agent and NetScaler Communication
- NIC 2 –For communication between agent and NetScaler Console

```
bash-3.2# ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 1500
        options=680003<RXCSUM,TXCSUM,LINKSTATE,RXCSUM_IPV6,TXCSUM_IPV6>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        groups: lo
pflog0: flags=0<> metric 0 mtu 33152
        groups: pflog
1/1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether a2:56:cd:d2:f8:8c
        hwaddr a2:56:cd:d2:f8:8c
        inet6 fe80::a056:cdff:fed2:f88c%1/1 prefixlen 64 scopeid 0x3
        inet 10.102.103.247 netmask 0xffffff00 broadcast 10.102.103.255
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet manual
        status: active
1/2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 32:89:fe:8c:8f:45
        hwaddr 32:89:fe:8c:8f:45
        inet6 fe80::3089:feff:fe8c:8f45%1/2 prefixlen 64 scopeid 0x4
        inet 10.102.103.250 netmask 0xffffff00 broadcast 10.102.103.255
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet manual
        status: active
```

4. Run the command **networkconfig**. A menu appears which allows you to set or modify the IPV4 network addresses.

```
bash-3.2# /mps/networkconfig

------------------------------------------------------------------------------
Citrix ADM Agent initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
------------------------------------------------------------------------------
     1. Citrix ADM Agent Host Name [ns]:
     2. Citrix ADM Agent IPv4 address [10.102.103.247]:
     3. Netmask [255.255.255.0]:
     4. Gateway IPv4 address [10.102.103.1]:
     5. DNS IPv4 Address [10.102.166.70]:
     6. Second NIC IPv4 address [10.102.103.250]:
     7. Second NIC Netmask [255.255.255.0]:
     8. Second NIC Network address [10.102.103.251,10.102.103.252,10.102.103.252]:
     9. Second NIC Gateway IPv4 address [10.102.103.2]:
    10. Cancel and quit.
    11. Save and quit.
```

> **Note:**
>
> Second NIC Network address can take multiple IP values.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

5. Select a menu item to modify. Save and quit the settings.

Adding instances

January 8, 2025

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.

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

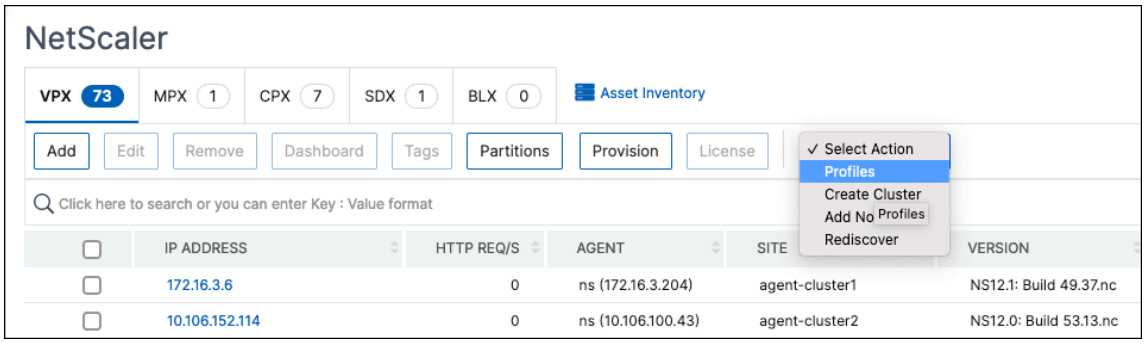
NetScaler profile contains the user name, password, communication ports, and authentication types of the instances that you want to add to NetScaler Console. For each instance type, a default profile is available. For example, the `nsroot` is the default profile for NetScaler instances. The default profile 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.

> **Note:**
>
> Ensure to use the super administrator account to create an instance profile.

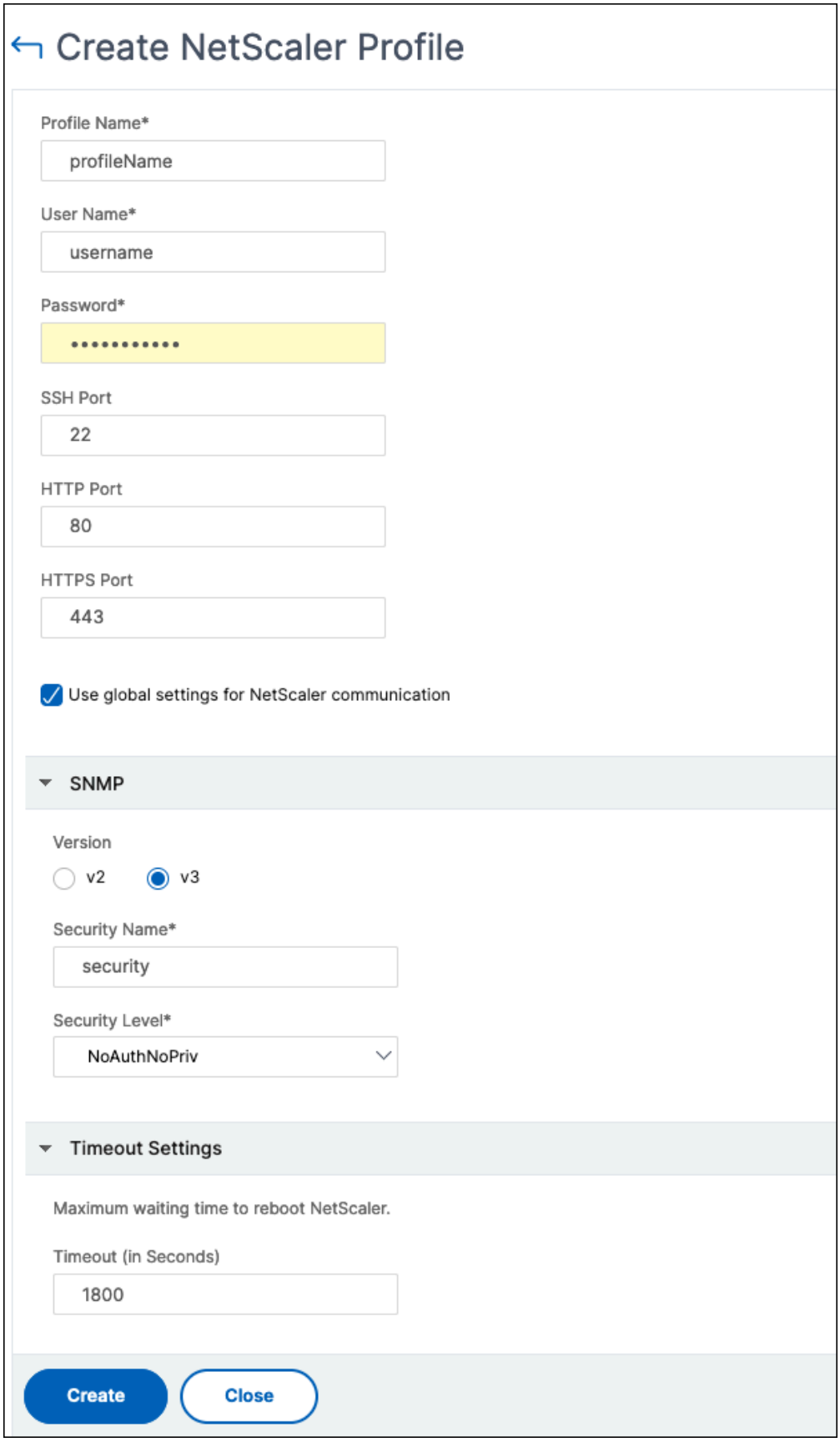
To create a NetScaler profile from the Instance page:

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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.

   > **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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

To add a NetScaler instance to NetScaler Console

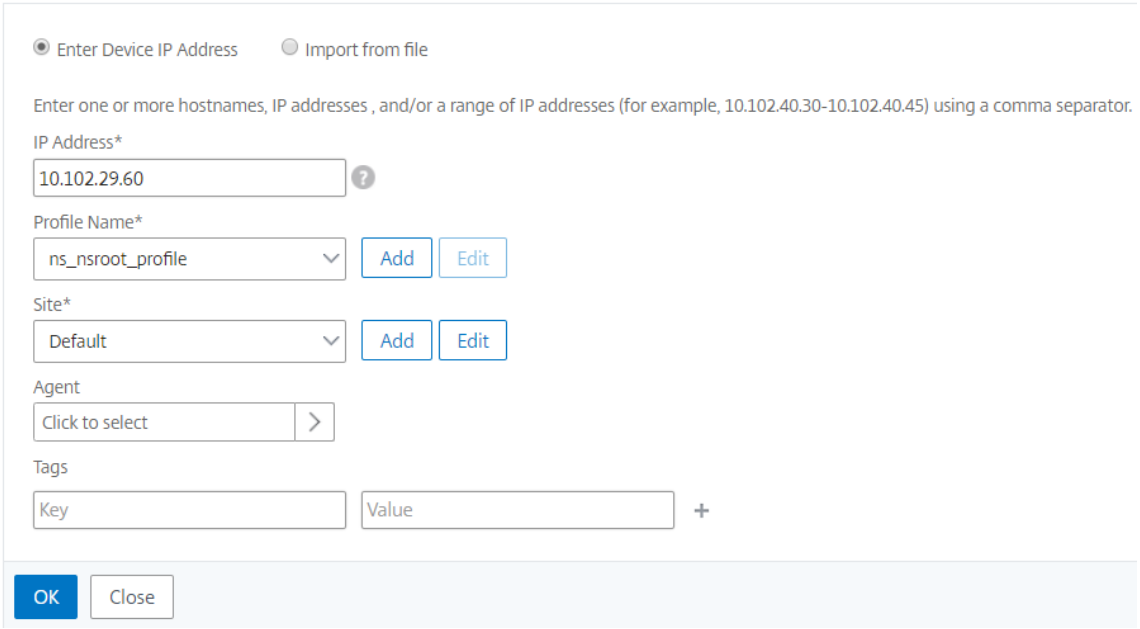
> **Note**
>
> Perform this task to add all other NetScaler instances except the NetScaler CPX instance.

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.
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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.

   > **Note**
   >
   > When you are creating a profile, ensure to specify the HTTP, HTTPS, SSH, and SNMP port

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 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**.

   > **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.

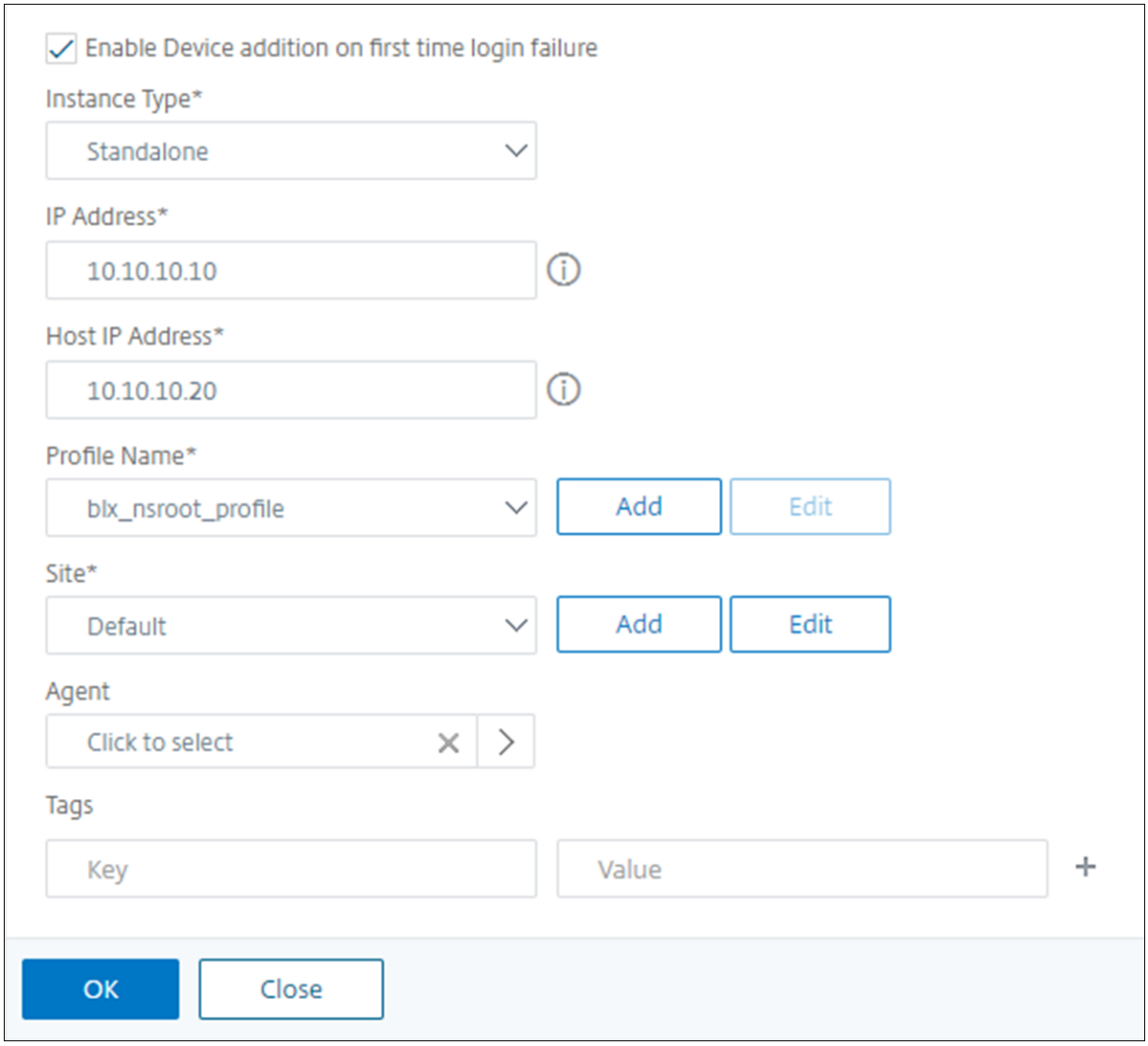
   If you want to add a site, click **Add**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.



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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.

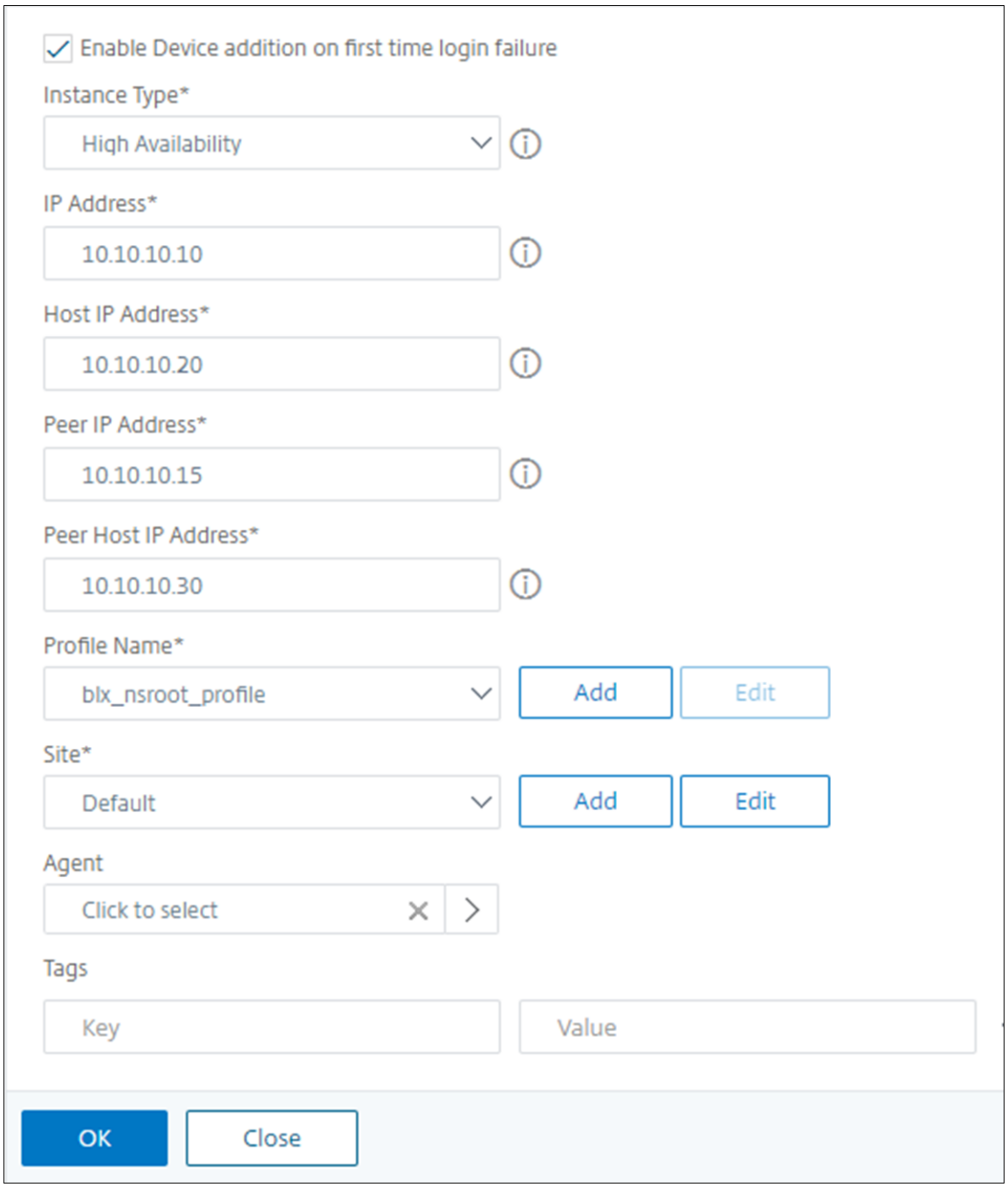
   > **Important**
   >
   > Ensure you have specified the correct host user name and password of the Linux server in the profile.

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**.

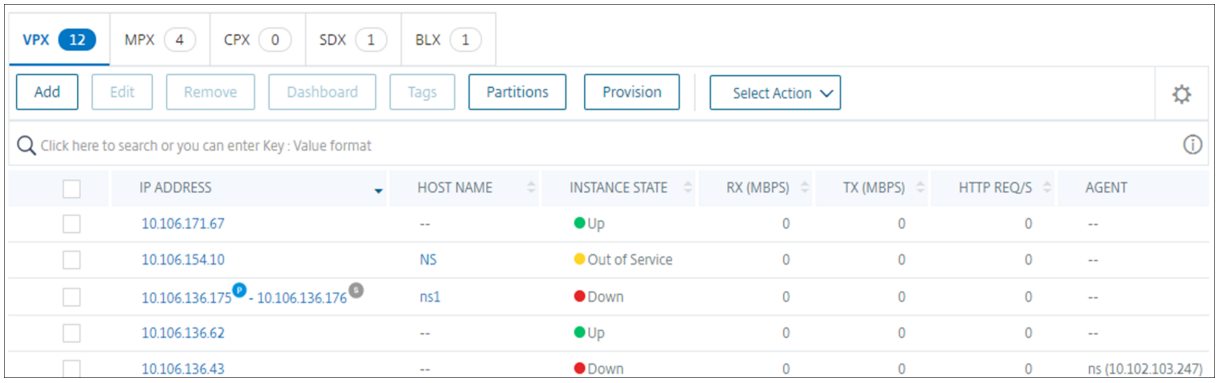
© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.

© 1997–2025 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

June 6, 2024

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 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.

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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

February 27, 2024

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. 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.

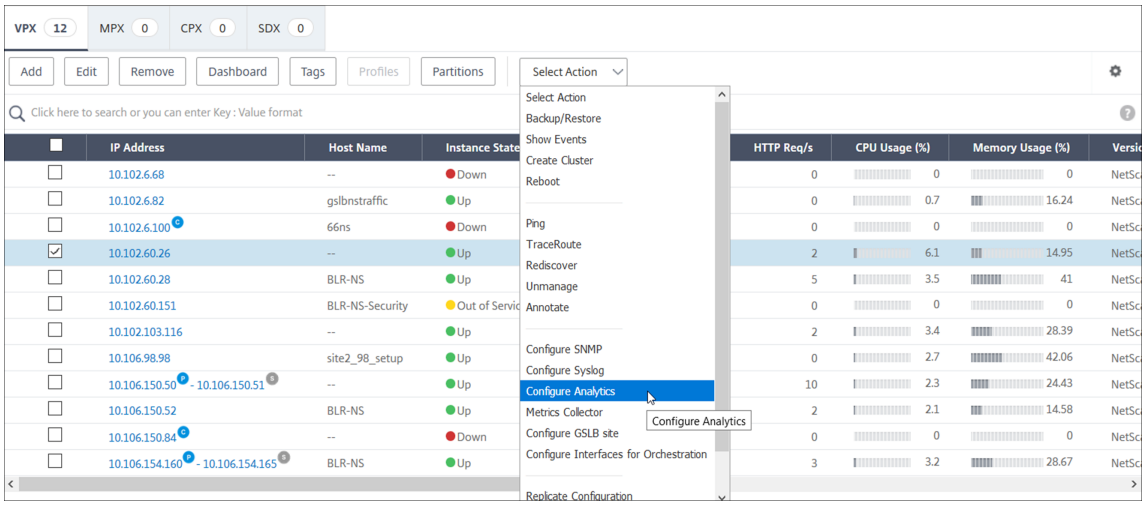
For NetScaler between **11.1 Build 47.14 and 11.1 Build 62.8**, **Logstream** is the default transport mode for enabling Web Insight (HTTP) and IPFIX is the only transport mode for enabling other insights. For NetScaler version starting from **12.0 to latest version**, you can select either **Logstream** 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.

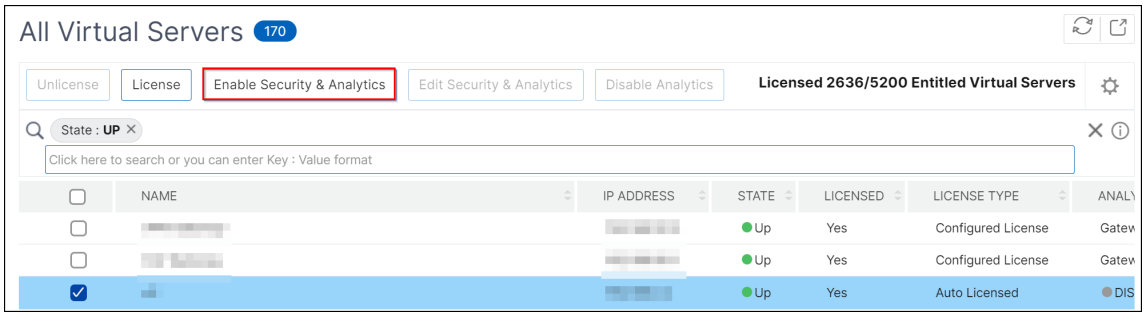
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.

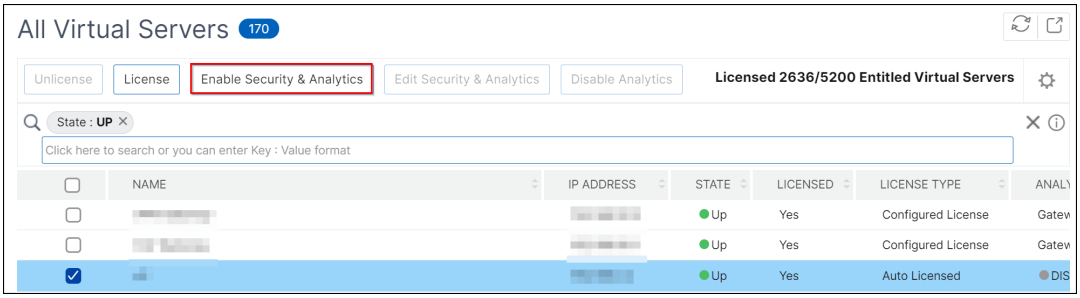


4. On the **Enable Security & Analytics** window:
   a) Select the insight types (Web Insight or WAF Security Violations or Bot Security Violations)
   b) Select **Logstream** as Transport Mode

> **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**

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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:

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

January 8, 2024

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

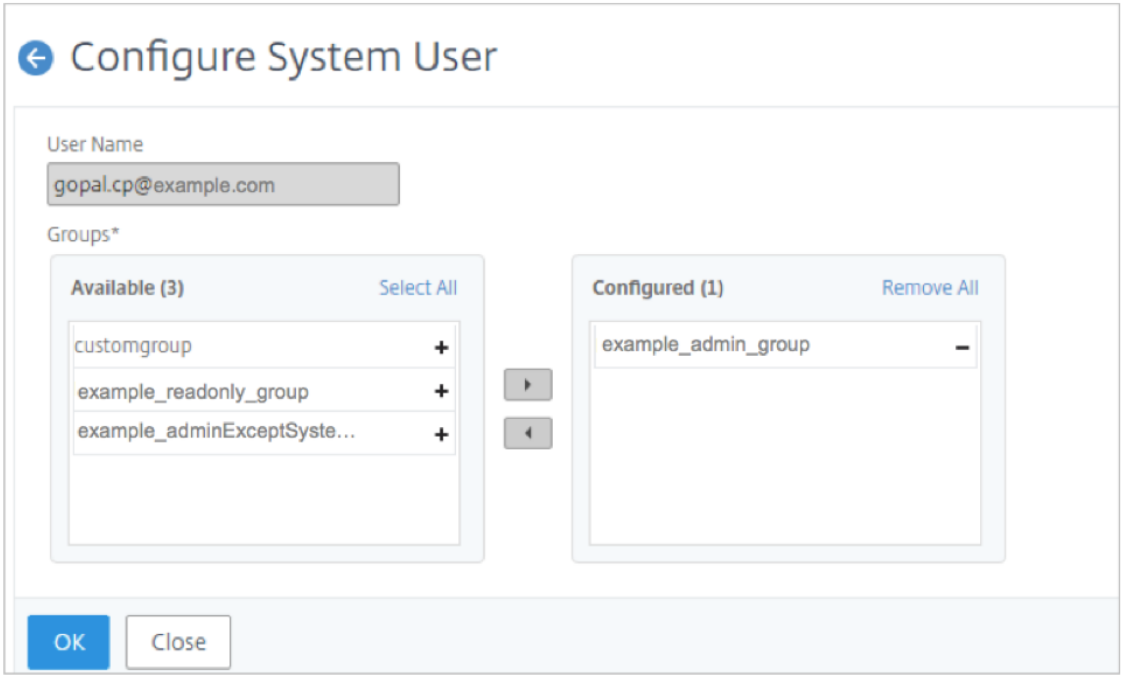
However, you can assign super admin privileges or specific non-super admin roles to a delegated admin so that the admin is able to perform tasks related to user administration.

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:

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.



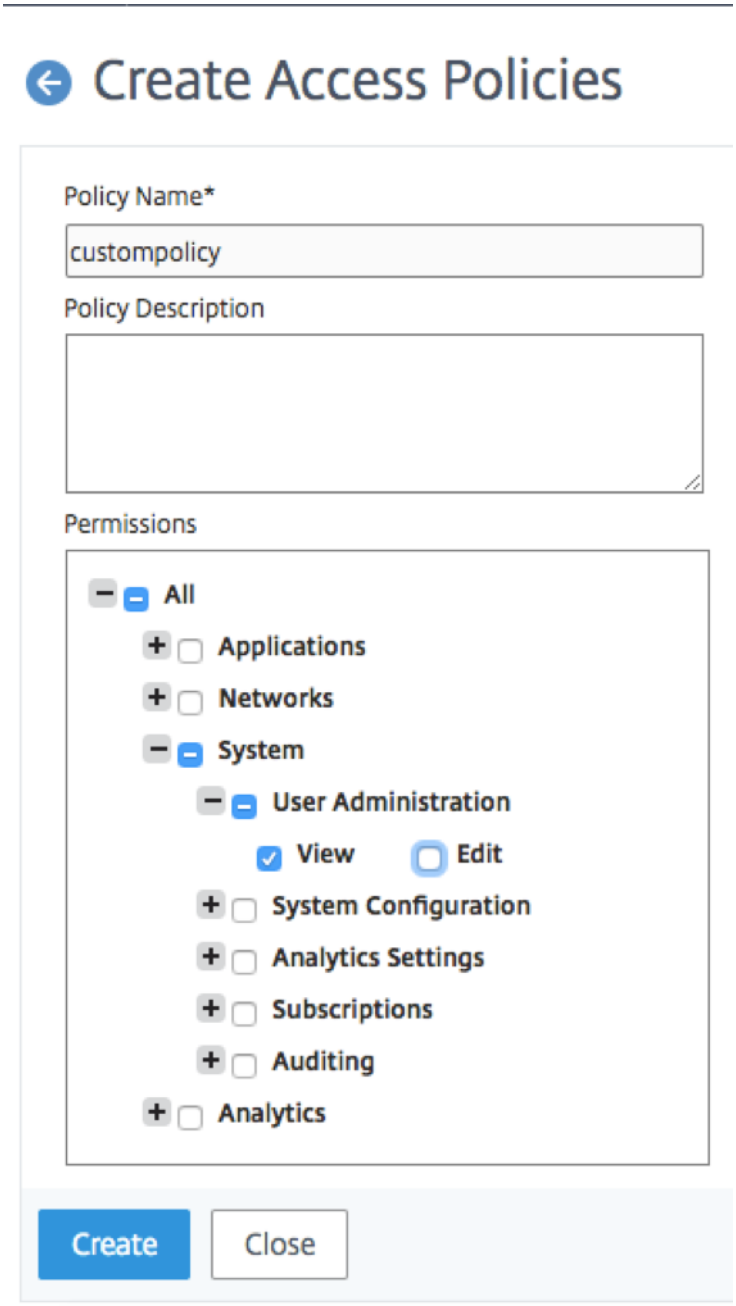
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:

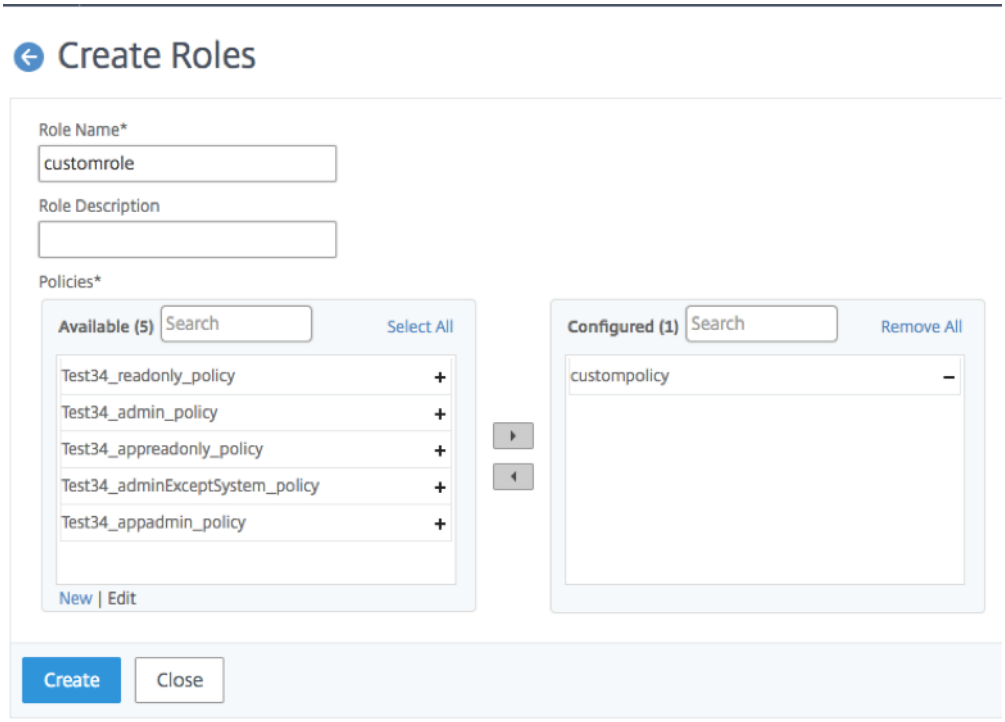
1. Log on to NetScaler Console as the super admin.
2. Navigate to **Account** > **User Administration** > **Access Policies**. Select **Add** to create an access policy with the required permissions for the delegated admin. In this example, an access policy `custompolicy` is created that allows view access to User Administration settings.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



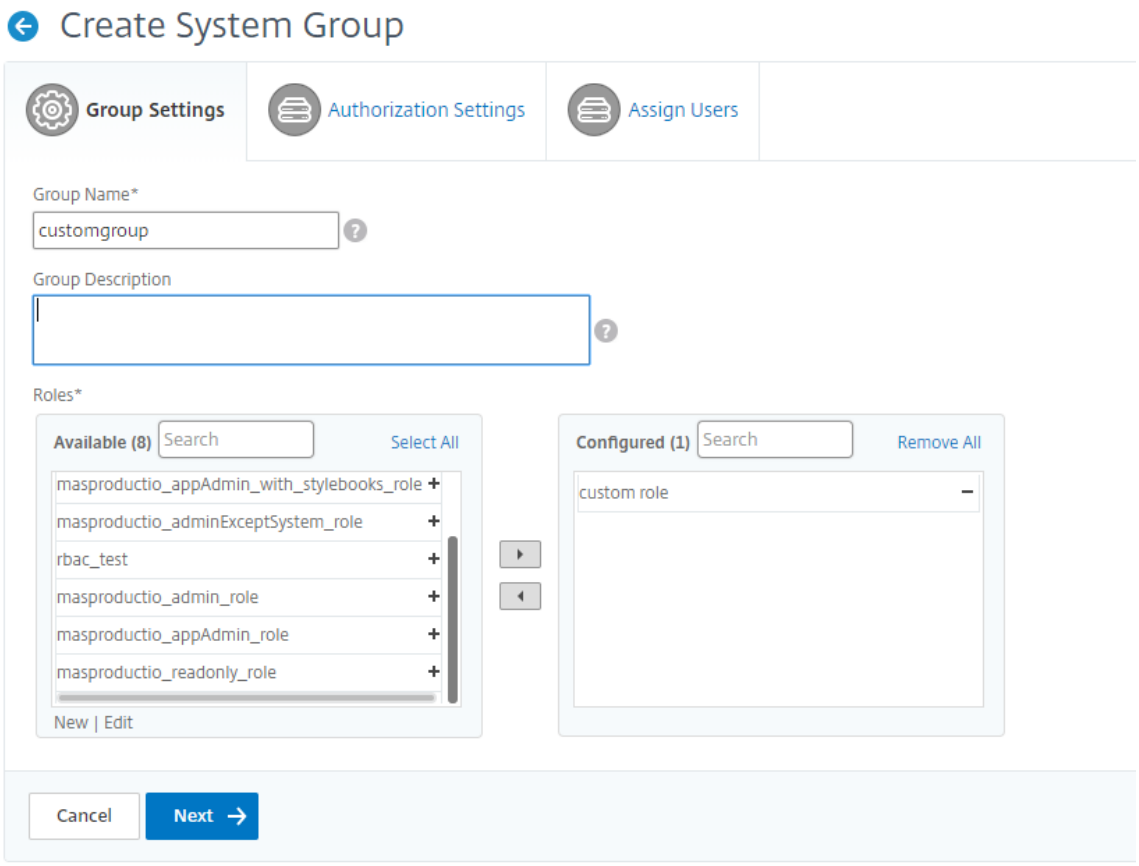
3. Navigate to **Account** > **User Administration** > **Roles**. Select **Add** to create a role and bind this role to the access policy that you created in the previous step. In this example, a role `customrole` is created and bound to the `custompolicy` access policy.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



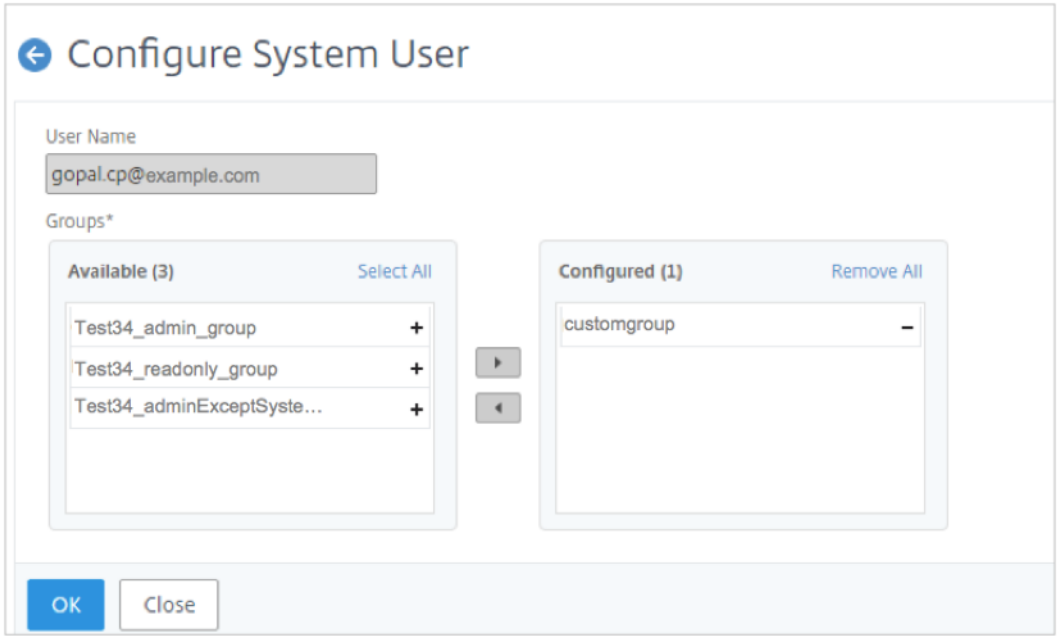
4. Navigate to **Account** > **User Administration** > **Groups**. Select **Add** to create a group and bind this group to the role you created in the previous step. In this example, the group "custom group"is created and bound to the role "custom role."

© 1997–2025 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`.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Integration with the ServiceNow instance

January 8, 2024

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.

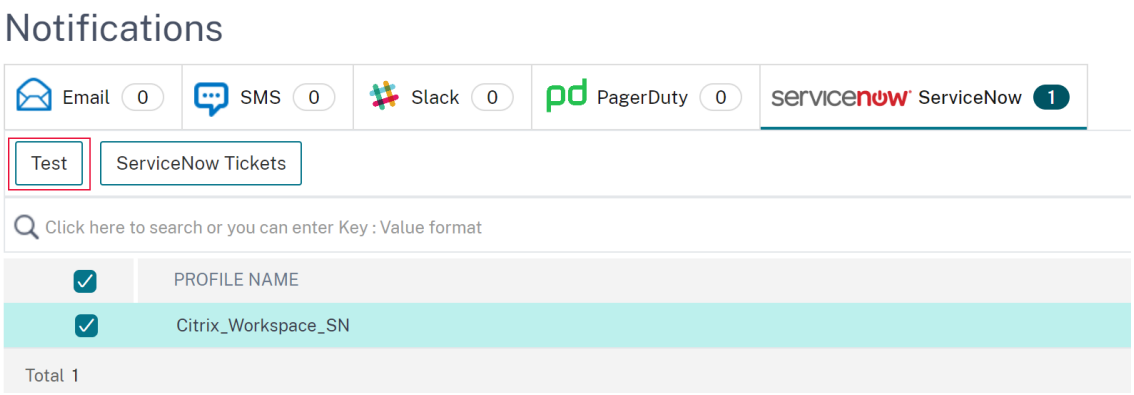
You can automate the ticket creation in ServiceNow using NetScaler Console and Citrix ITSM connector for ServiceNow. To start this automation, onboard Citrix ITSM adapter service to receive events and create relevant incidents in ServiceNow. For more information about preparation and integration steps, 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**.

© 1997–2025 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.

To send ServiceNow notifications for an SSL certificate expiry, see SSL certificate expiry.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

Actionable tasks and recommendations

November 15, 2024

> **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

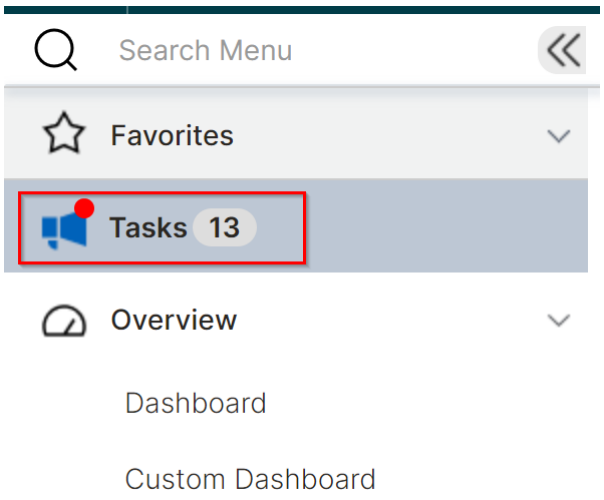
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:

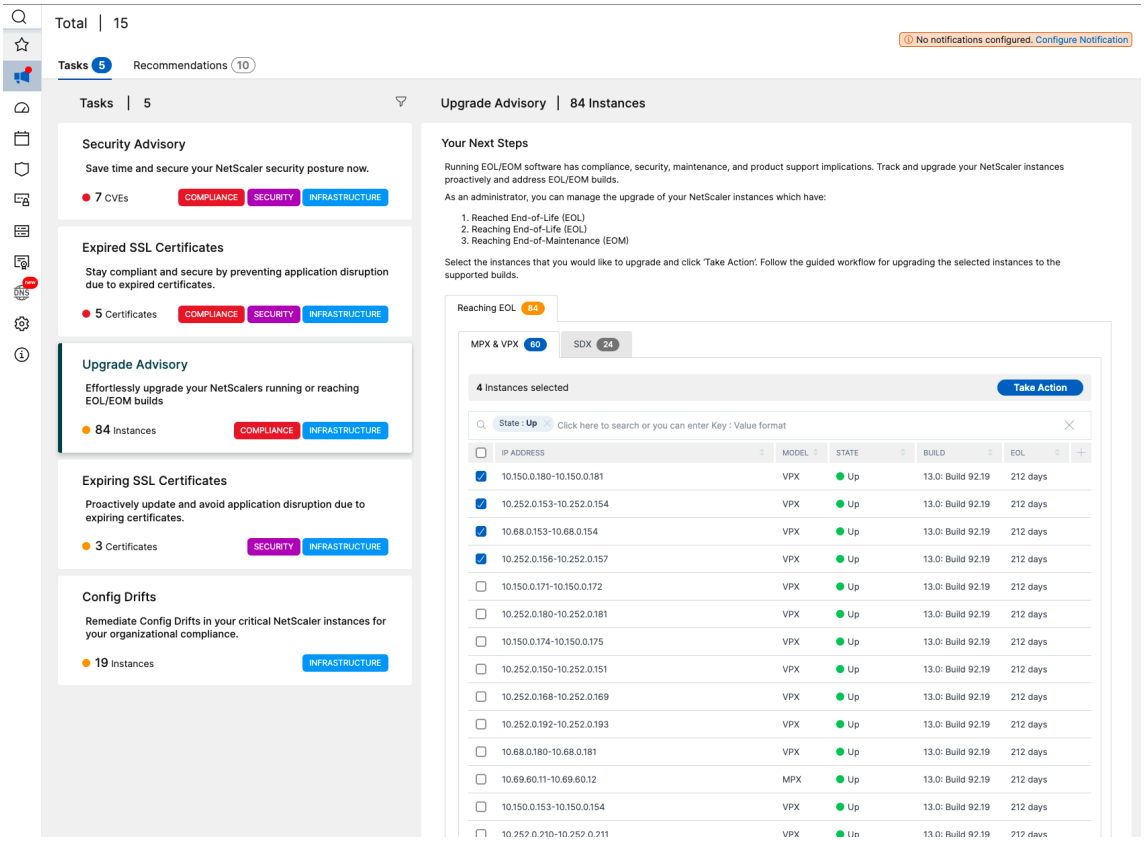
- Get instant visibility on any observations or issues that require your immediate action.
- Configure notifications to receive notification whenever NetScaler Console detects any tasks and proactively take action.
- Achieve an efficient deployment of NetScaler Console and NetScaler instances.
- Reduce 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**.



- **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).

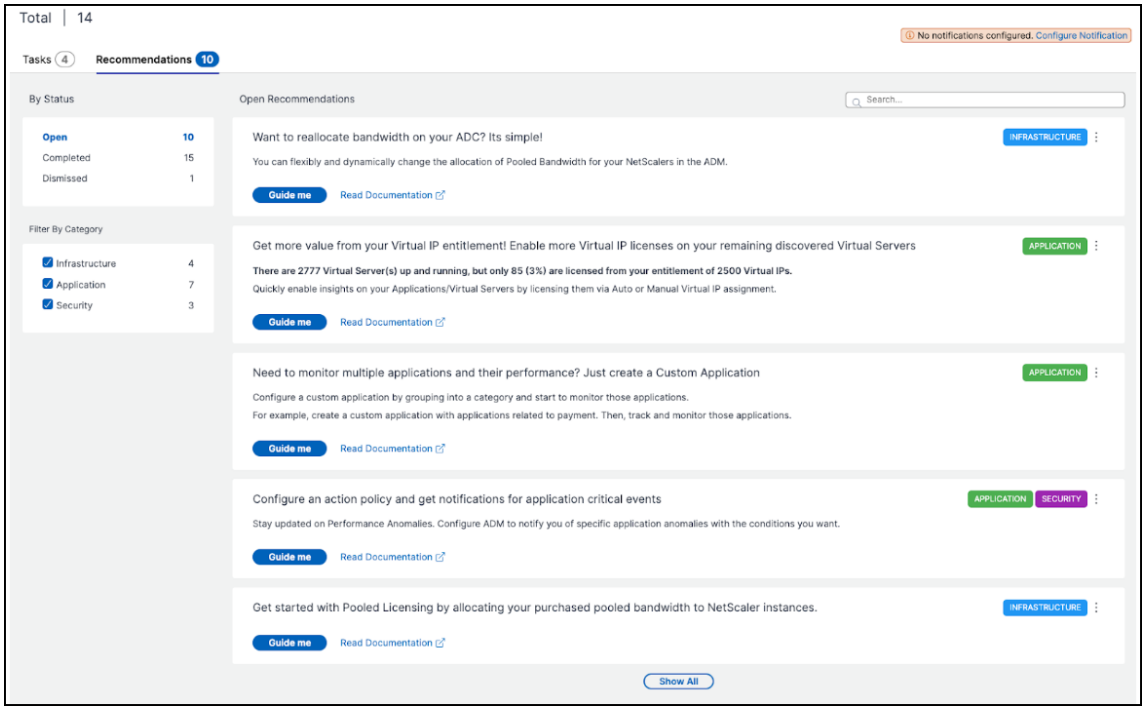
© 1997–2025 Citrix Systems, Inc. All rights reserved.



- **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.

© 1997–2025 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.
- **Expiring SSL Certificates** –Provides information about the SSL certificates that are about to expire.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.

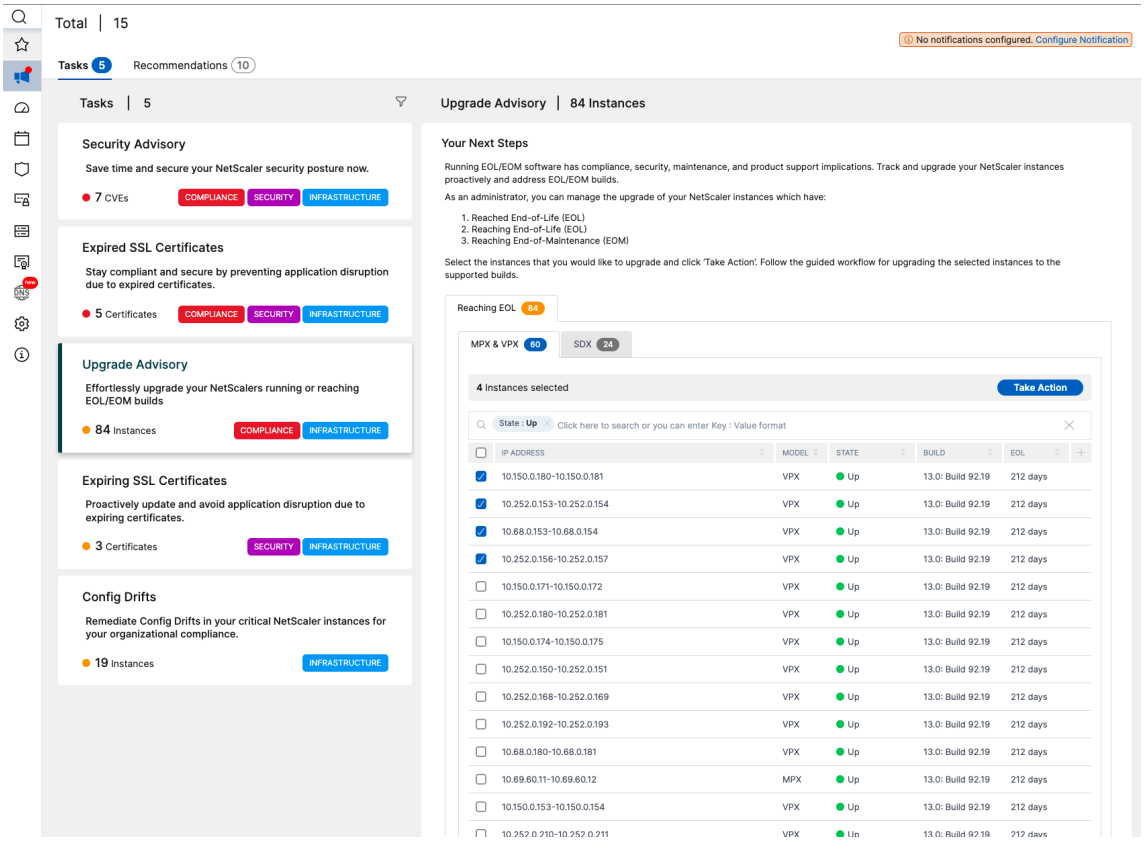
    Recommended Action: You are redirected to the **Security Advisory** page in **Infrastructure > Instance Advisory > Security Advisory**. Follow the documentation to complete the task.

  - **Affected Instances**: Displays the NetScaler instances that are affected with CVEs. To complete the task, select the instance, click **View and Remediate**.

    Recommended Action: You are redirected to the **Security Advisory** page in **Infrastructure > Instance Advisory > Security Advisory**. Follow the documentation to complete the task.

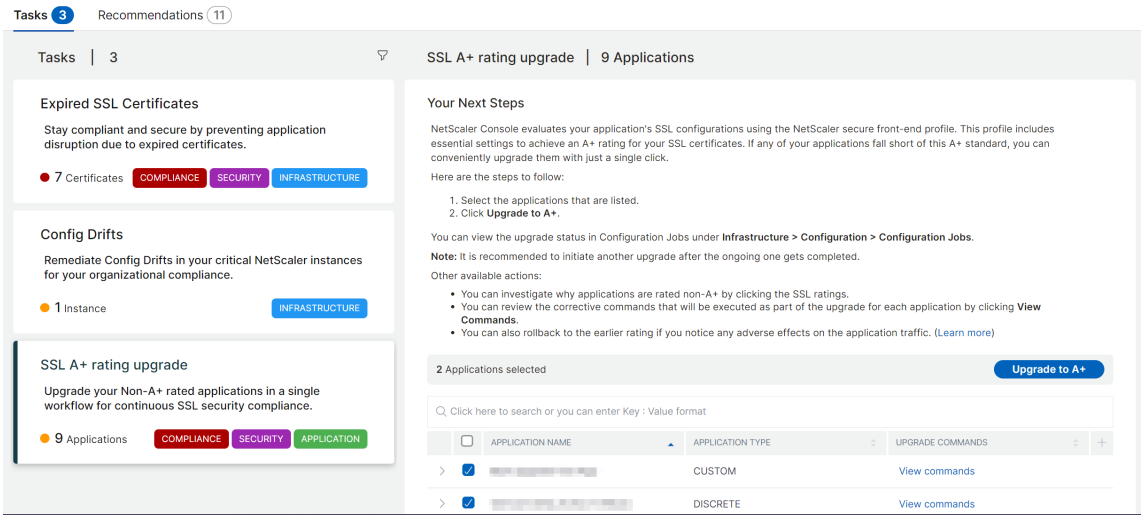
- **Upgrade Advisory**: Provides information about your NetScaler instances that have already reached or about to reach End of Life (EOL) or End of Maintenance (EOM) within 90 days.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Recommended Action: Click **Take Action** and upgrade the instances to a recommended build.

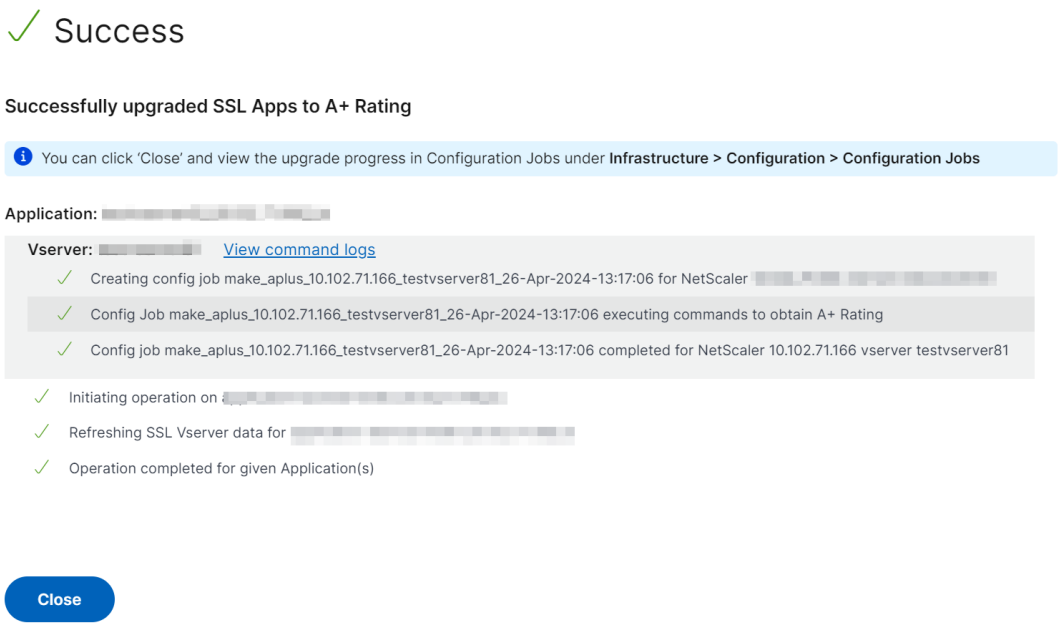
- **SSL A+ rating upgrade**: Provides information about your applications that are not compliant with an A+ rating.



Recommended Action: Select the applications from the list and click **Upgrade to A+**.

After the upgrade is successful, you can the following success message:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



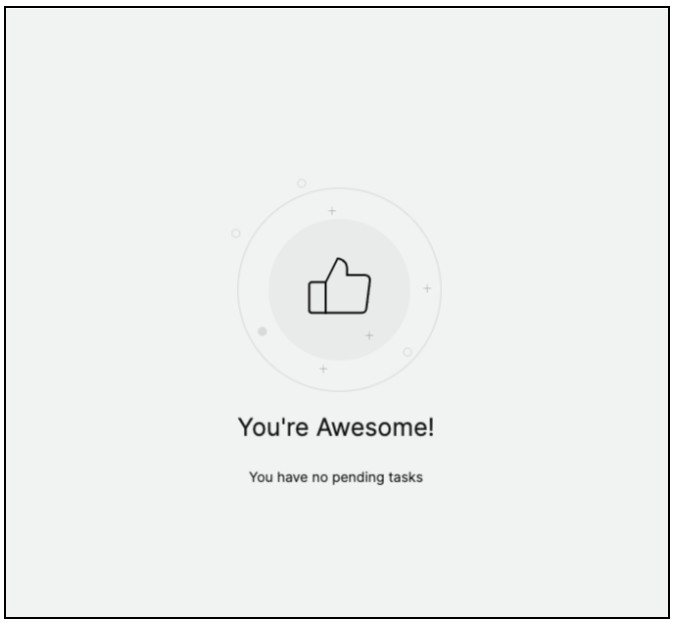
After the upgrade is completed, the application details are removed from the task.

Points to note:

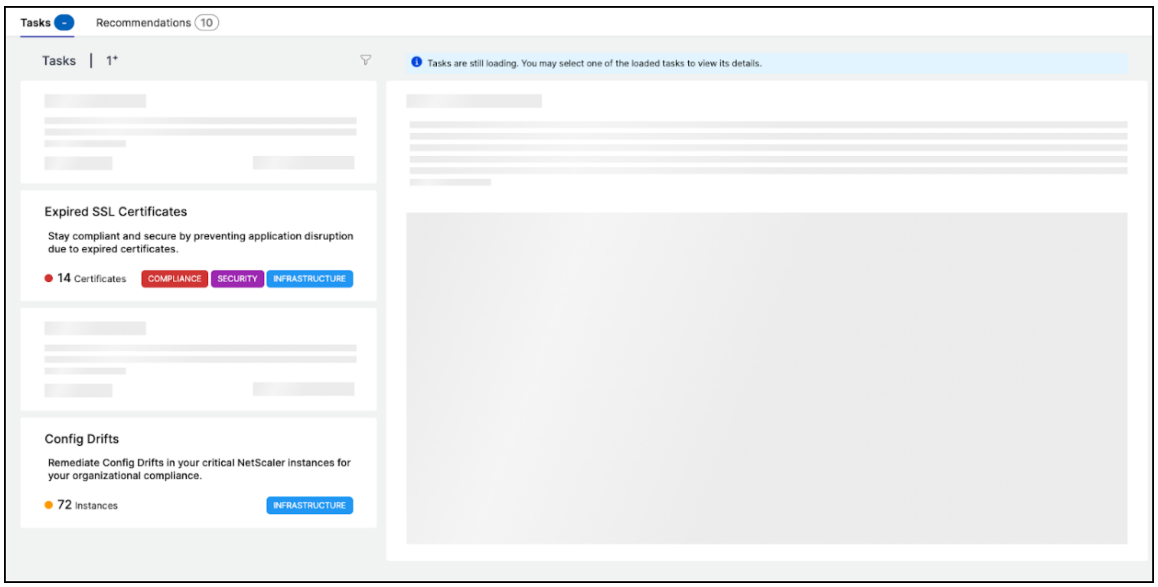
- Depending upon the number of applications selected, the duration for the upgrade completion process might vary.
- After you initiate an upgrade process, it is recommended to initiate another upgrade process after the ongoing one gets completed.
- You can also view the status for the upgrade process 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:

© 1997–2025 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.



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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 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.

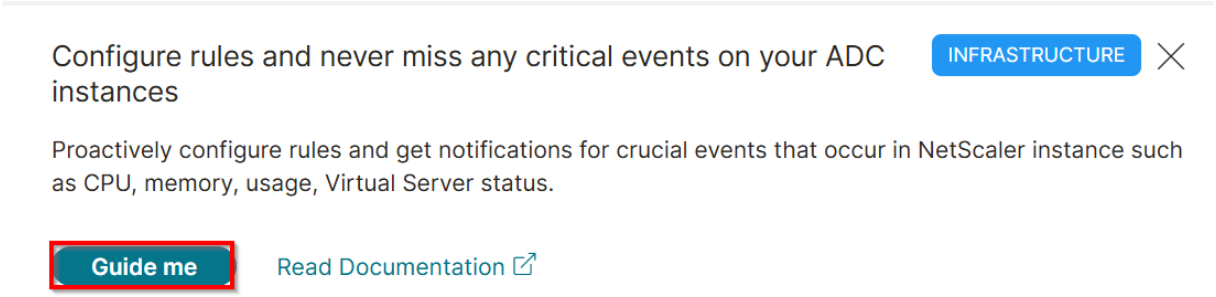
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.
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:

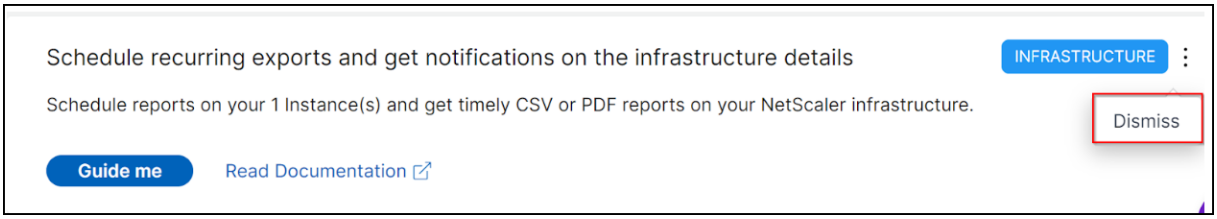
© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.

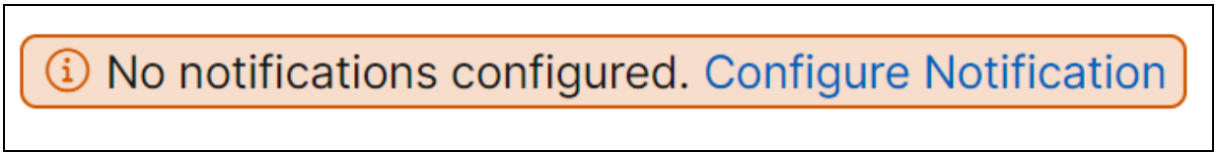
After you complete creating a rule, the recommendation is complete and it is moved to **Completed**.

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.



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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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?

   When you click **Tasks** from the left navigation pane, they are refreshed and available at the latest status. The details are fetched and updated.

A unified dashboard to view instance key metric details

January 8, 2024

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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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:

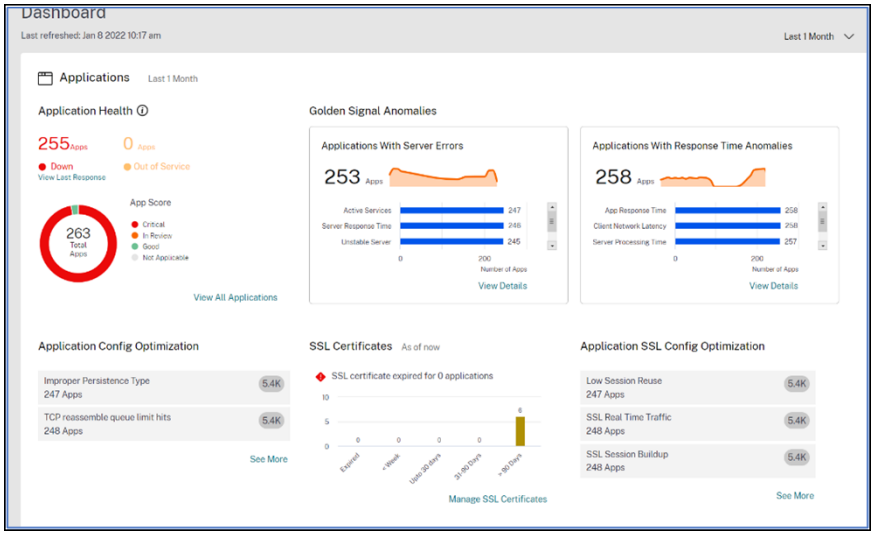
- Applications
- NetScaler Infrastructure
- Application security
- Gateway
- API analytics

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.
- **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.

© 1997–2025 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.

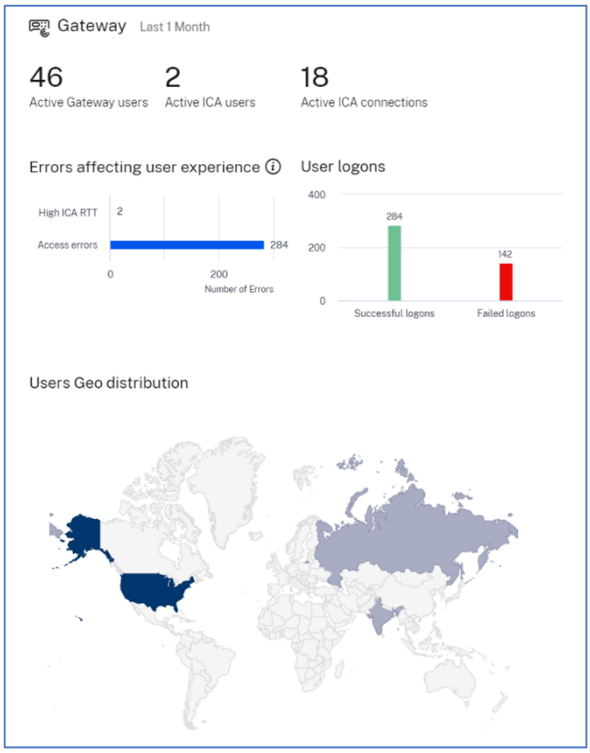


Gateway

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

locations.

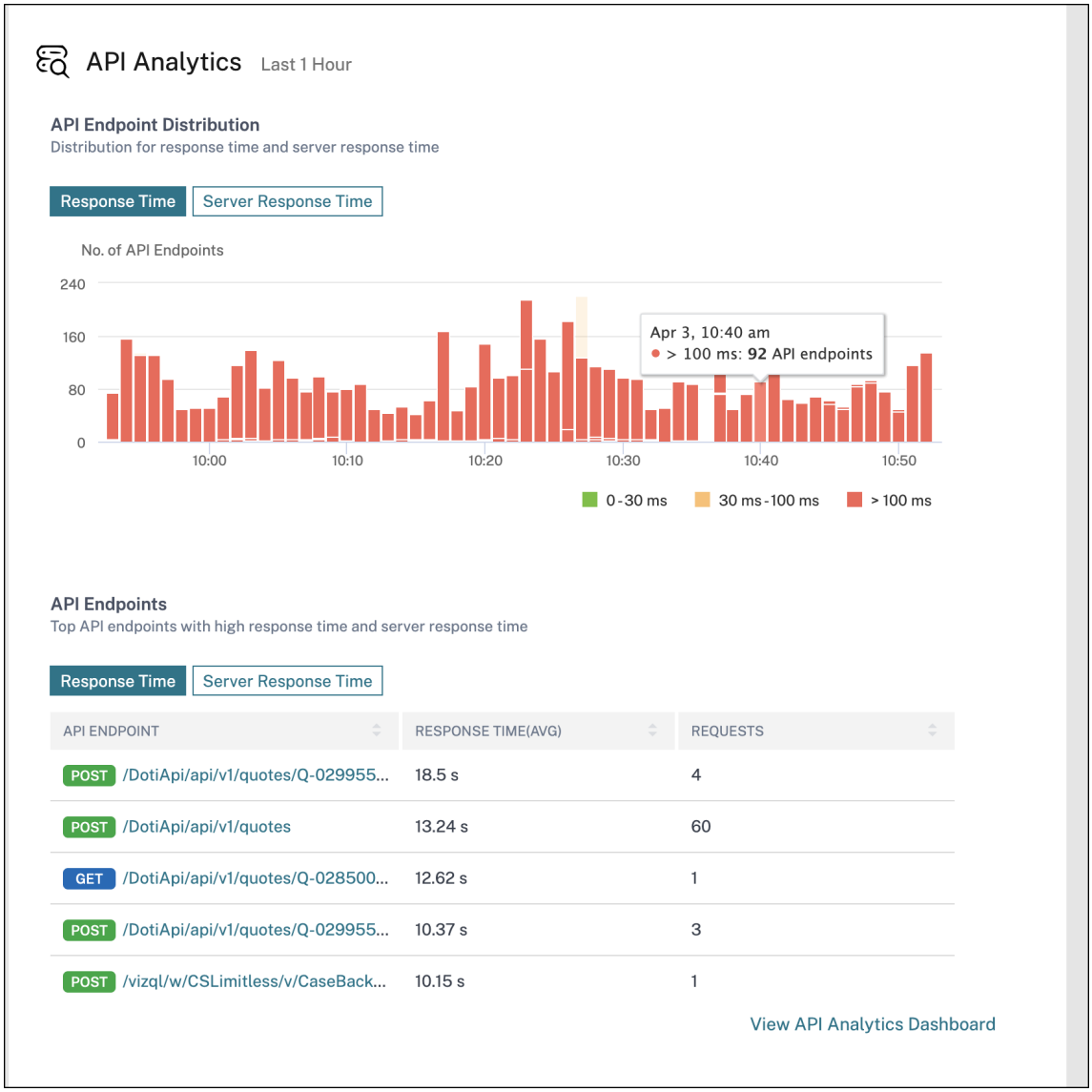


API Analytics

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

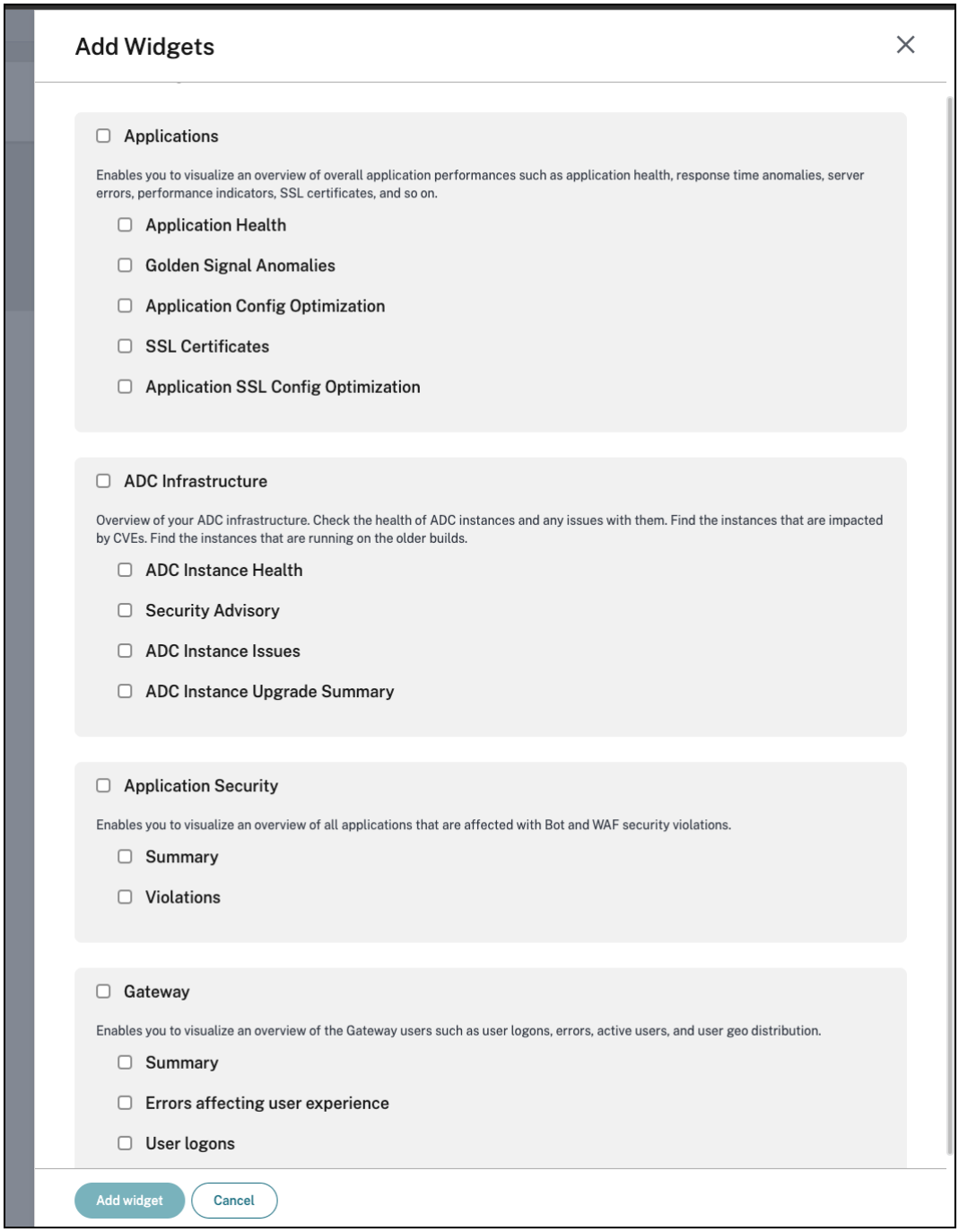


Customize dashboard

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
- 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- Reset to default
- Reset to last saved

After making changes, click **Save**.

> **Note**
>
> - By default, all widgets are displayed. If you customize the dashboard, save the changes,

© 1997–2025 Citrix Systems, Inc. All rights reserved.

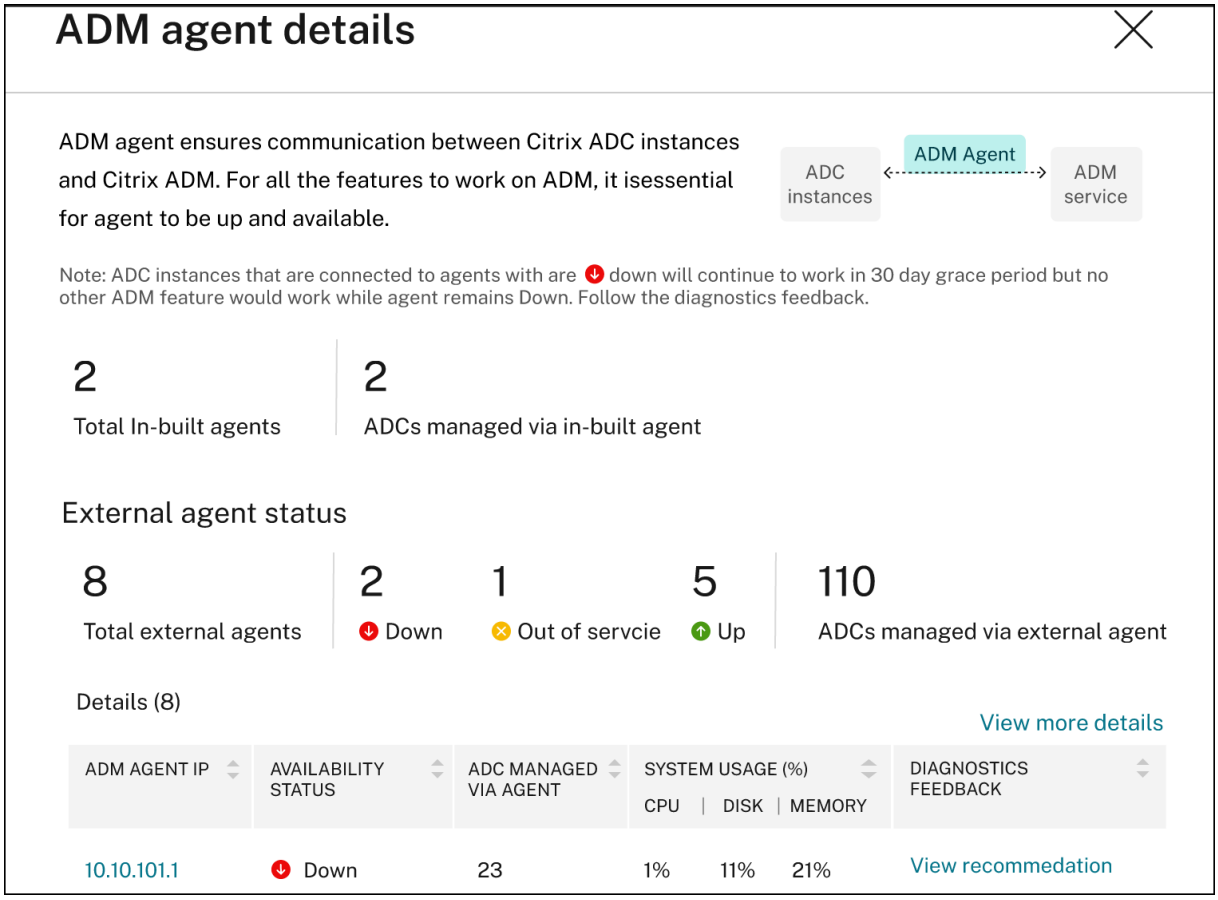
> and again use the **Reset to default** option, all widgets get added to the dashboard.
>
> - The **Reset to last saved** option loads the previously saved configuration.

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.
- **[number of agents] unavailable**. Indicates a few agents are down and not accessible.
- **All out of service**. Indicates all agents are in out of service.
- **[number of agents] 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.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Create and apply filters

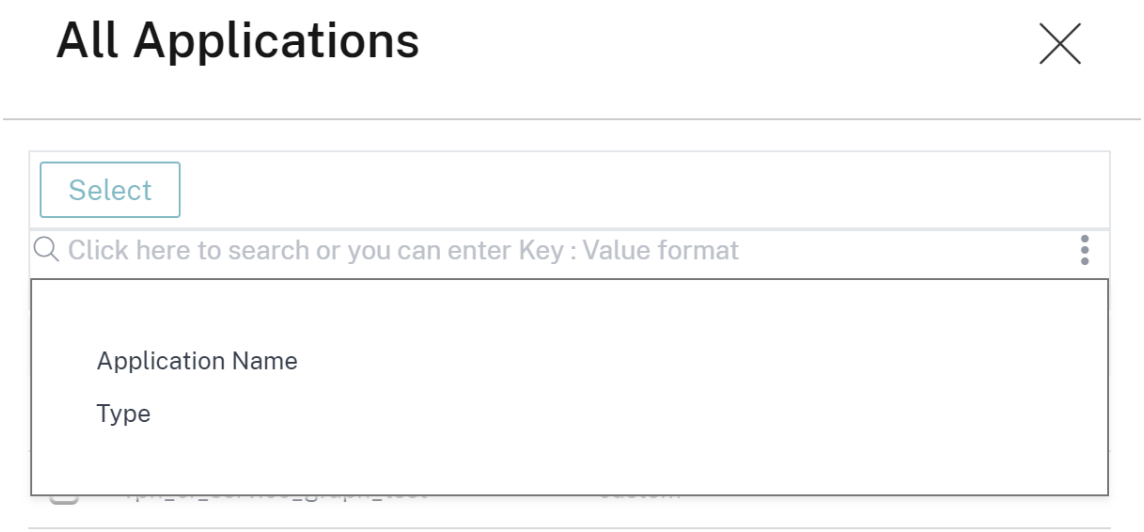
You can apply filters and view insights only for the selected instances or applications in the following:

- 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.

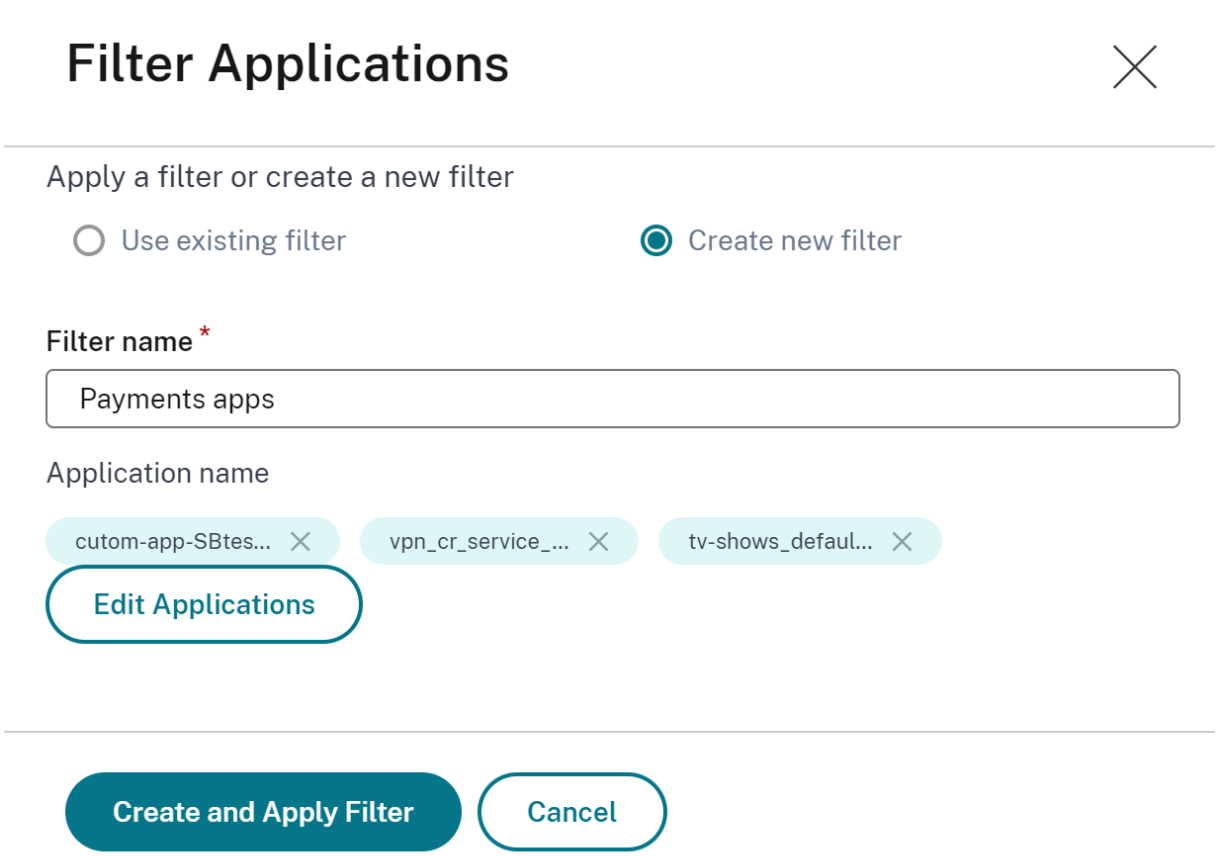
In the **Filter Applications** window:

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.



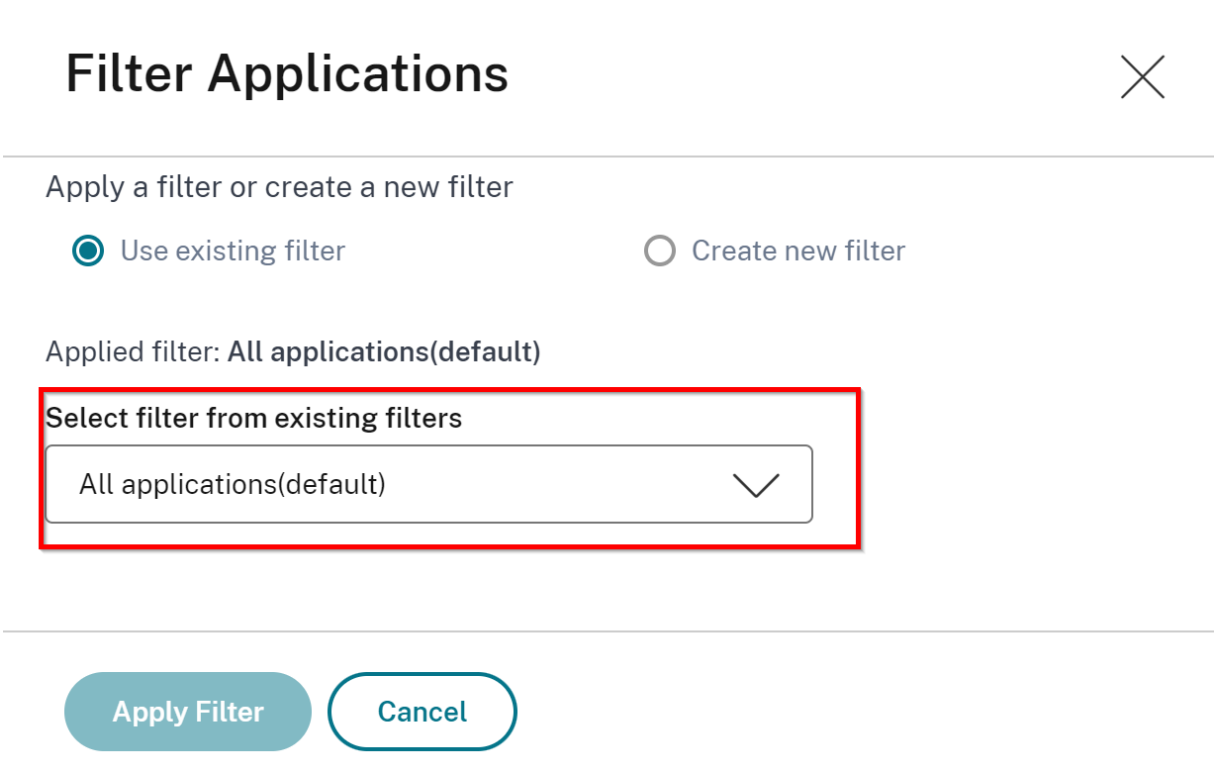
4. Click **Create and Apply filter**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



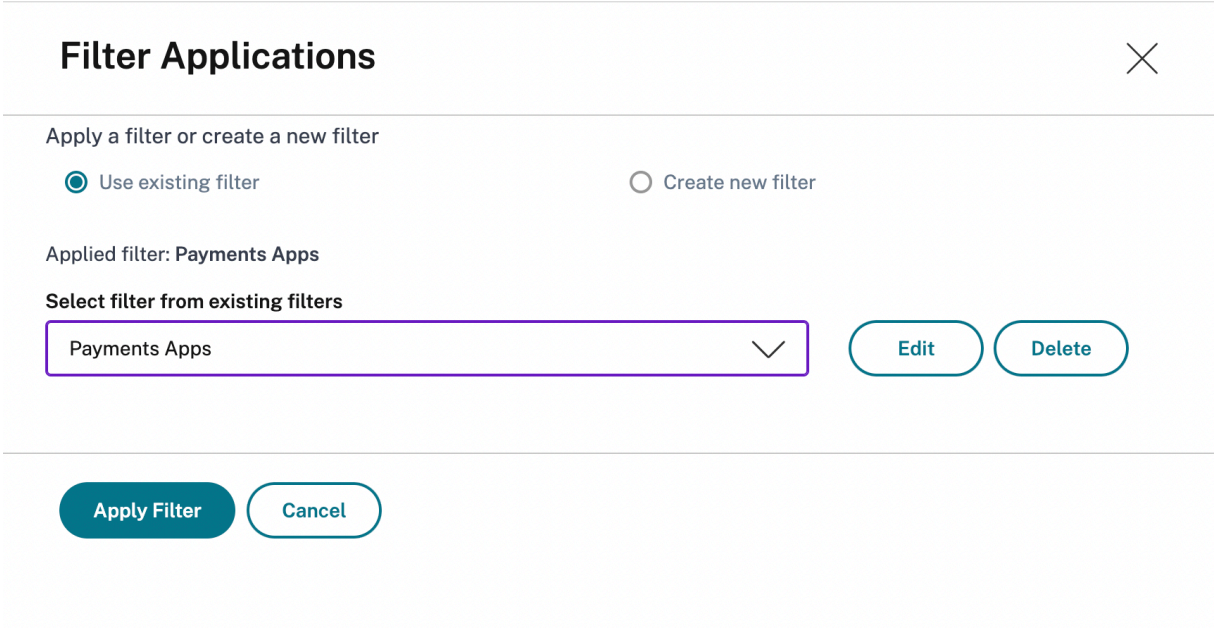
The filter is now created and applied. You can create more filters by following the same procedure. After you create filters, you can select and apply filters through the **Select filter from existing filters** list.

© 1997–2025 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**.

© 1997–2025 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

September 10, 2024

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.

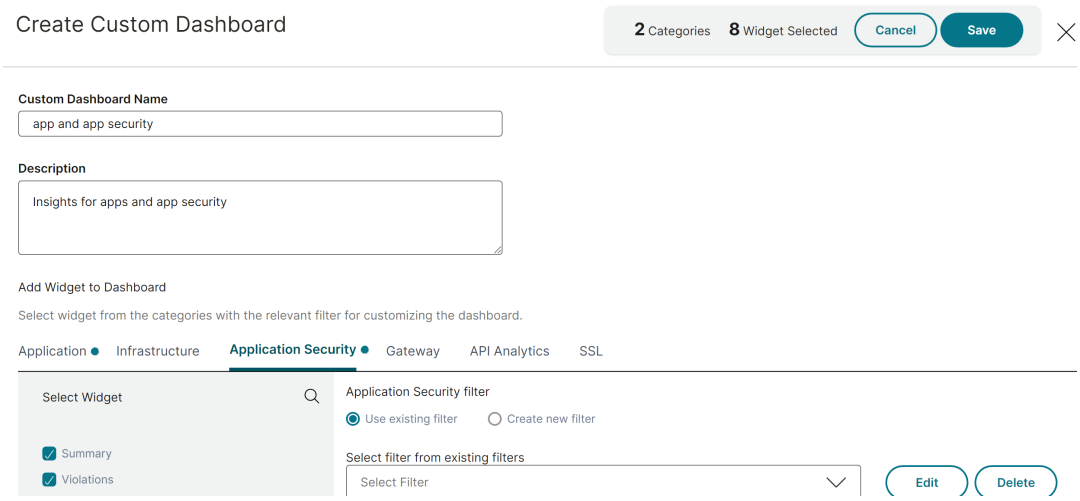
   b) **Description** - Provide a brief description to have additional details.

   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.

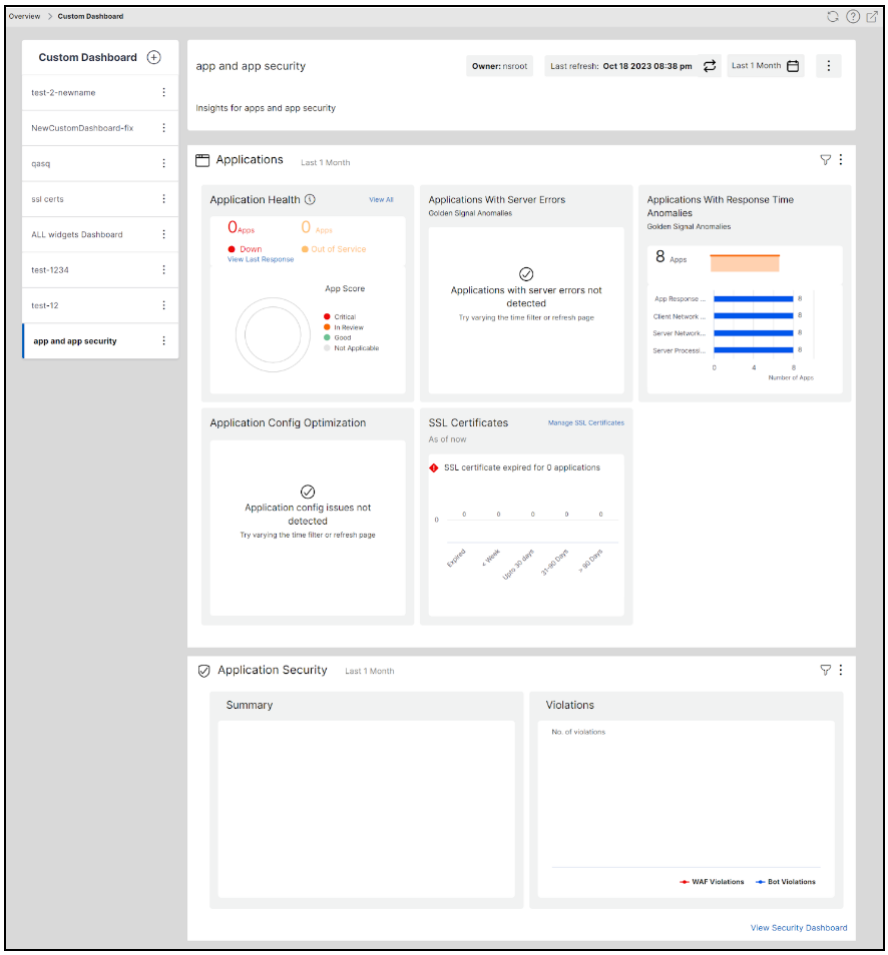
   d) **Application filter** - By default, the filter is applied to all applications. You can also create a filter and select only specific applications. For more information, see Create and apply filters.

   e) Click **Save**.

© 1997–2025 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.



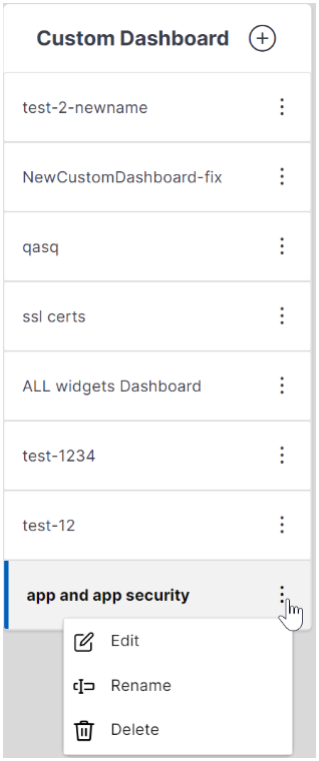
You can use the following options after you create a custom dashboard:

- **Edit**: You can edit the dashboard by adding more widgets or removing widgets, applying filters,

© 1997–2025 Citrix Systems, Inc. All rights reserved.

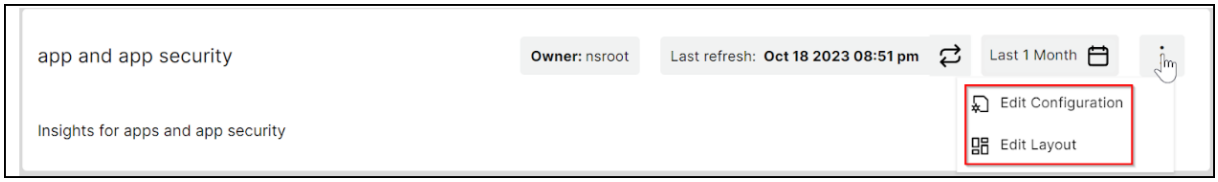
and so on.

- **Rename**: You can change the dashboard name.
- **Delete**: You can delete the dashboard.



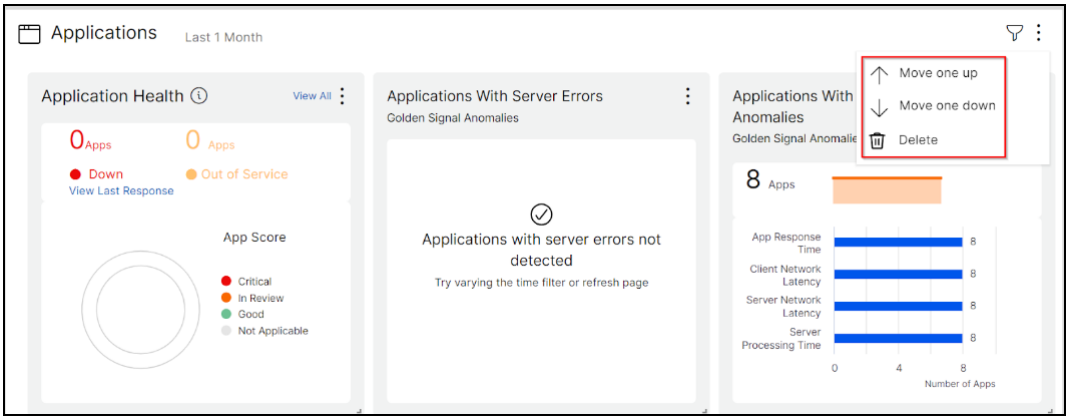
More options in the dashboard

In the custom dashboard that you have created, you can use the following options:

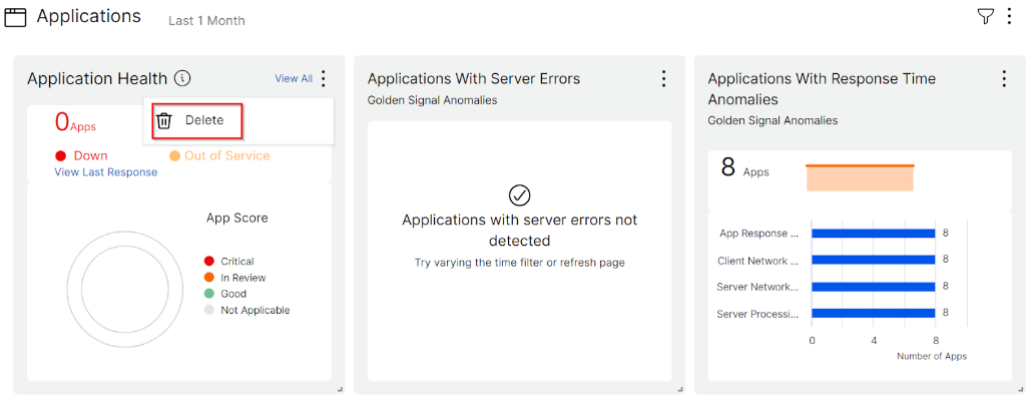


- **Edit Configuration**: You can also use this option to edit the dashboard by adding more widgets or removing widgets, applying filters, and so on.
- **Edit Layout**: You can use this option to have additional customization to the dashboard.
  - You can select to move up, down, or delete.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

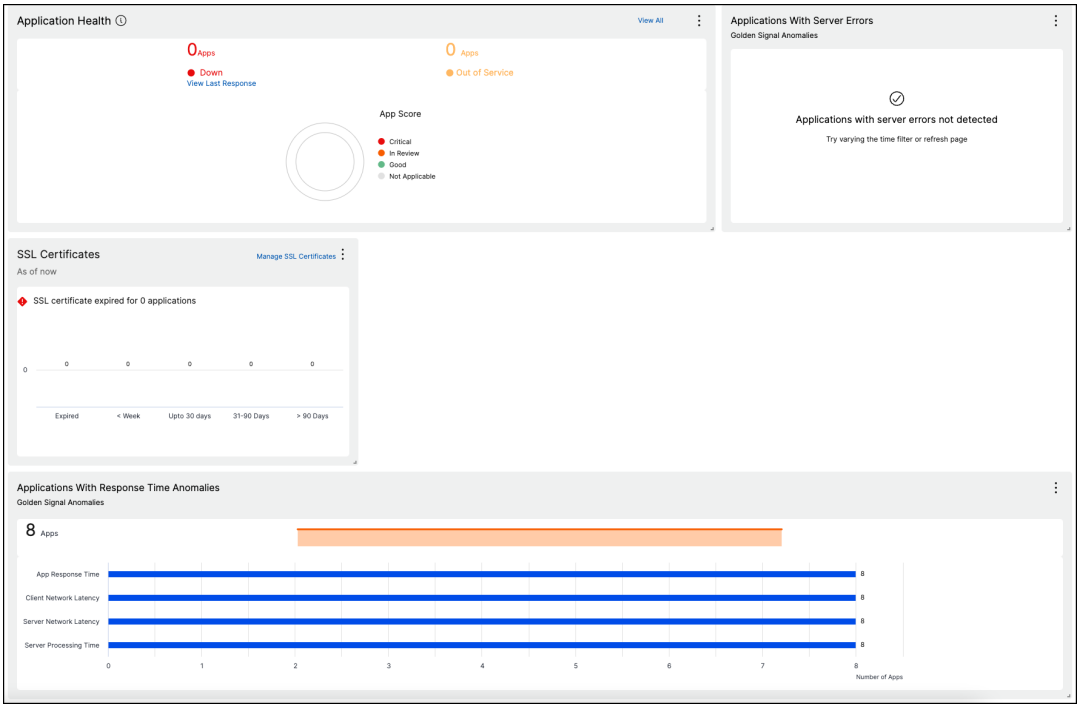


- In the Widgets, you can delete any widget by selecting the Delete option.



- Drag to place the widgets wherever you want.
- Increase or decrease the widget size to have a better visibility for certain insights.

© 1997–2025 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.

API Security

January 8, 2024

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.

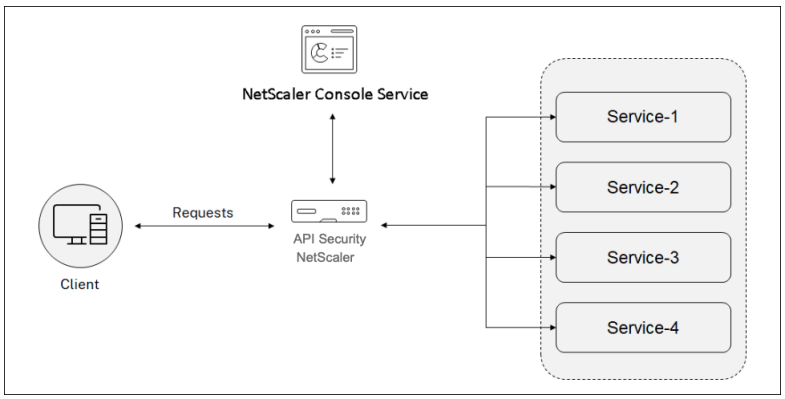
In API security, a gateway acts as the entry point for all requests to your API endpoints. And, ensures secure and reliable access to all API endpoints and microservices in your system.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:



> **Note:**
>
> In NetScaler Console, this feature is available for the users who have Premium or Advanced 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.

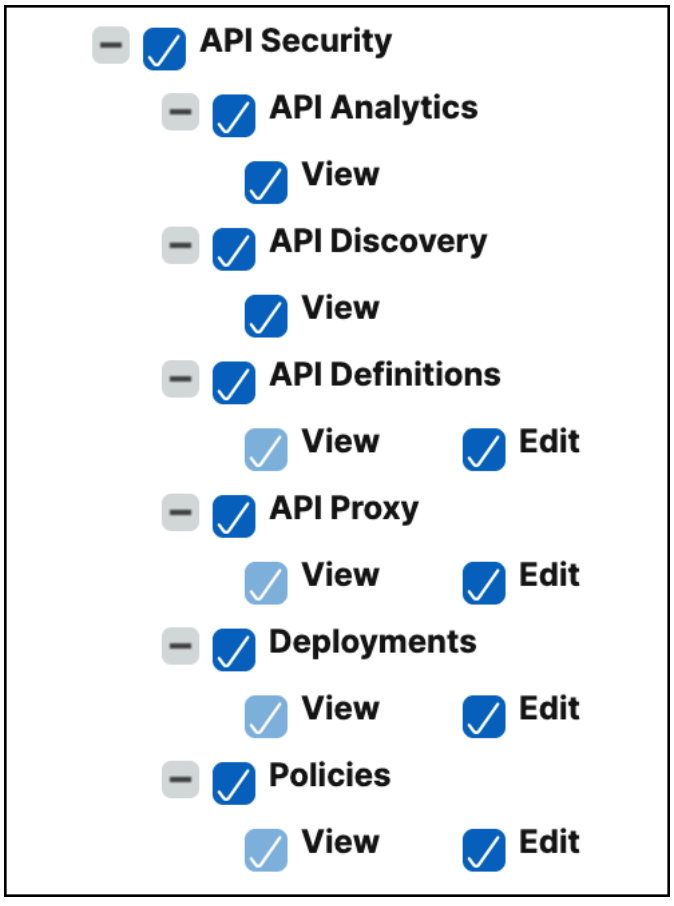
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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.
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 exam-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> ple, if you grant user access to the **Deployments** page, the following features also require user access:
>
> - StyleBooks
> - 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

July 25, 2025

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.

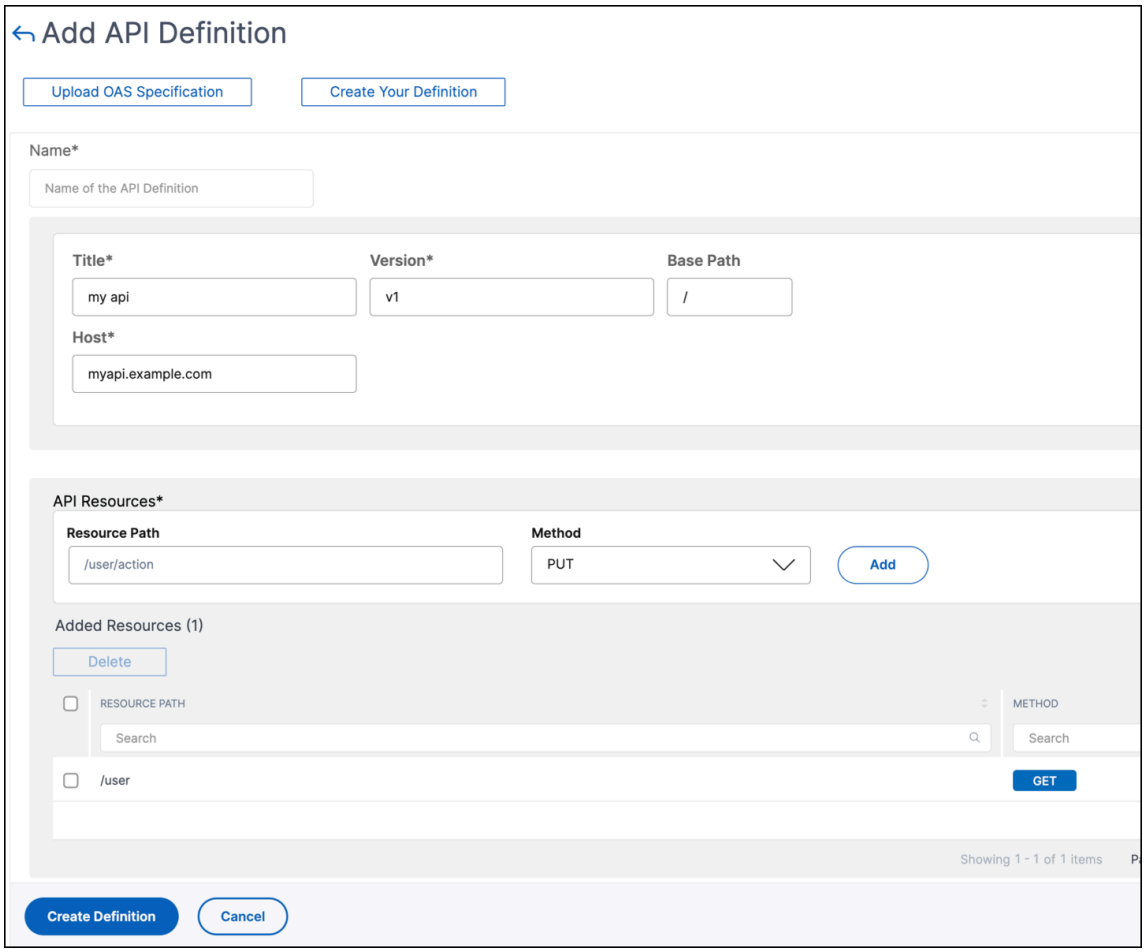
4. Browse an OAS specification from your local computer and upload to NetScaler Console.

© 1997–2025 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**.

© 1997–2025 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

January 8, 2024

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Target NetScaler Instance** - Select an NetScaler instance that acts as an API gateway.
- **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.

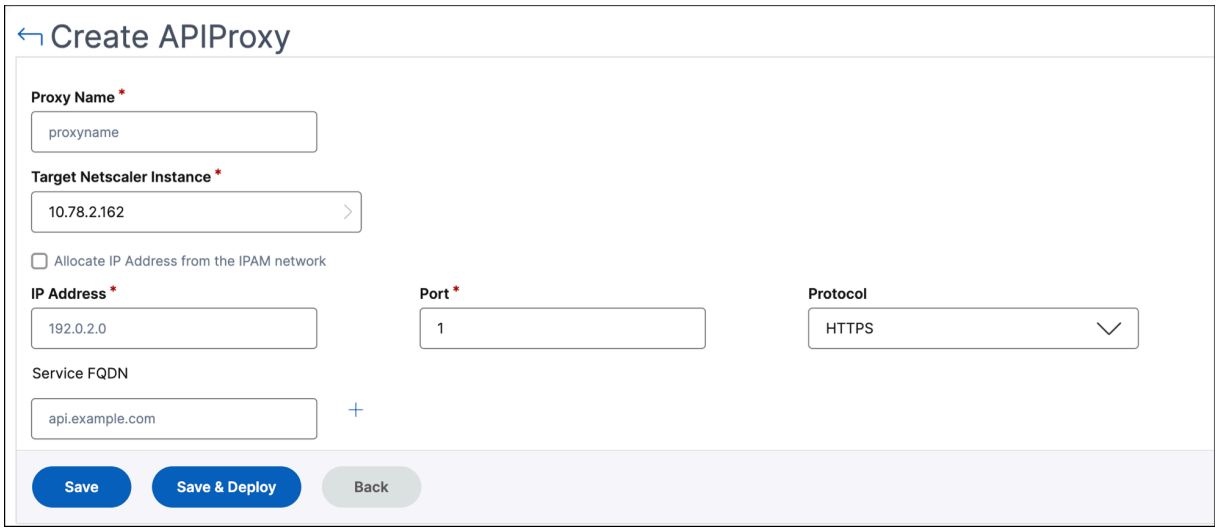
  > **Note:**
  >
  > If your existing deployments use the SSL certificate or key that are not in the NetScaler agent certificate store, you must add the certificate and key to the store with the same name.

- **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**.



© 1997–2025 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.

   > **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.

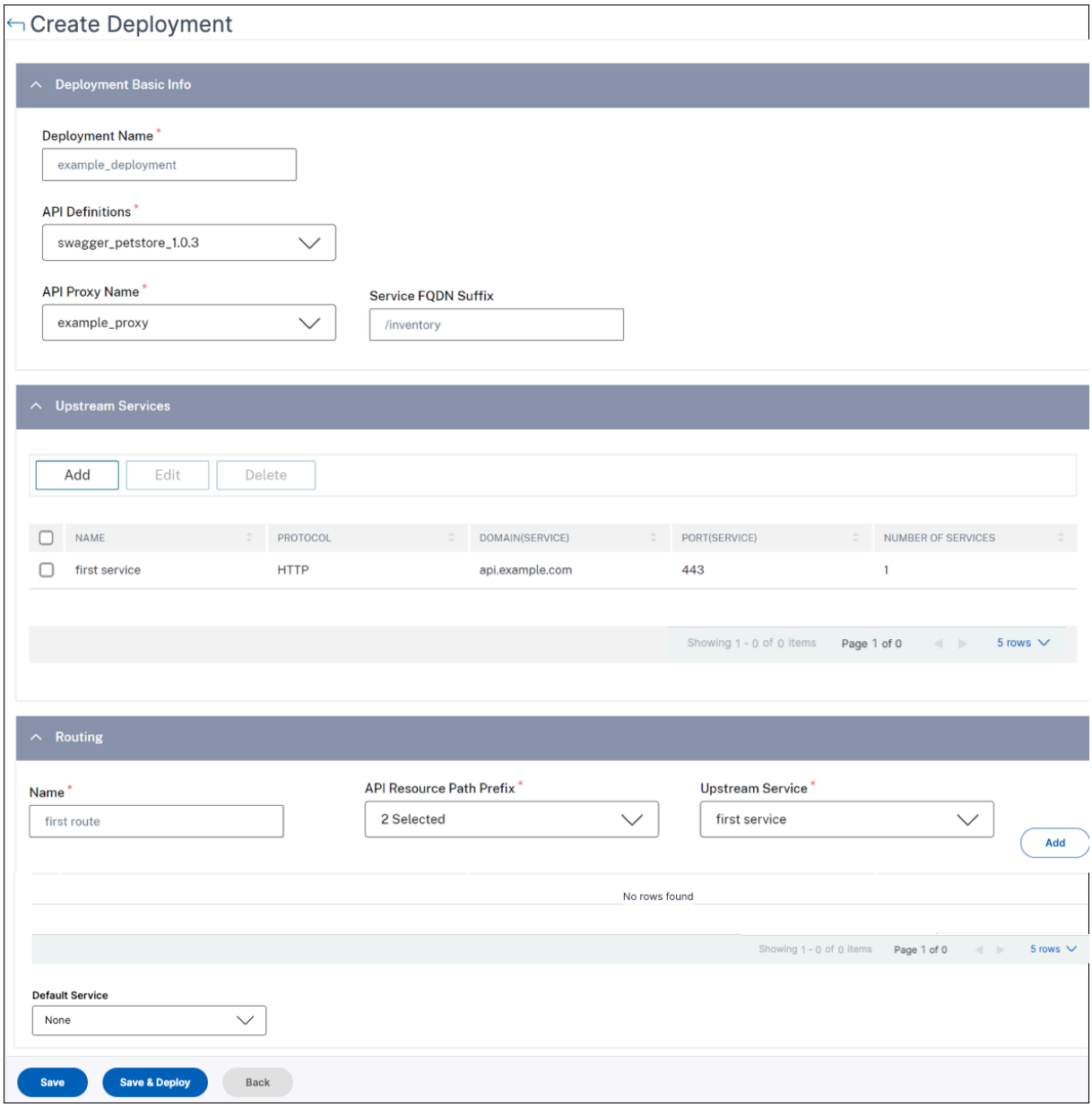
© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **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**.



© 1997–2025 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.
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

January 16, 2024

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.

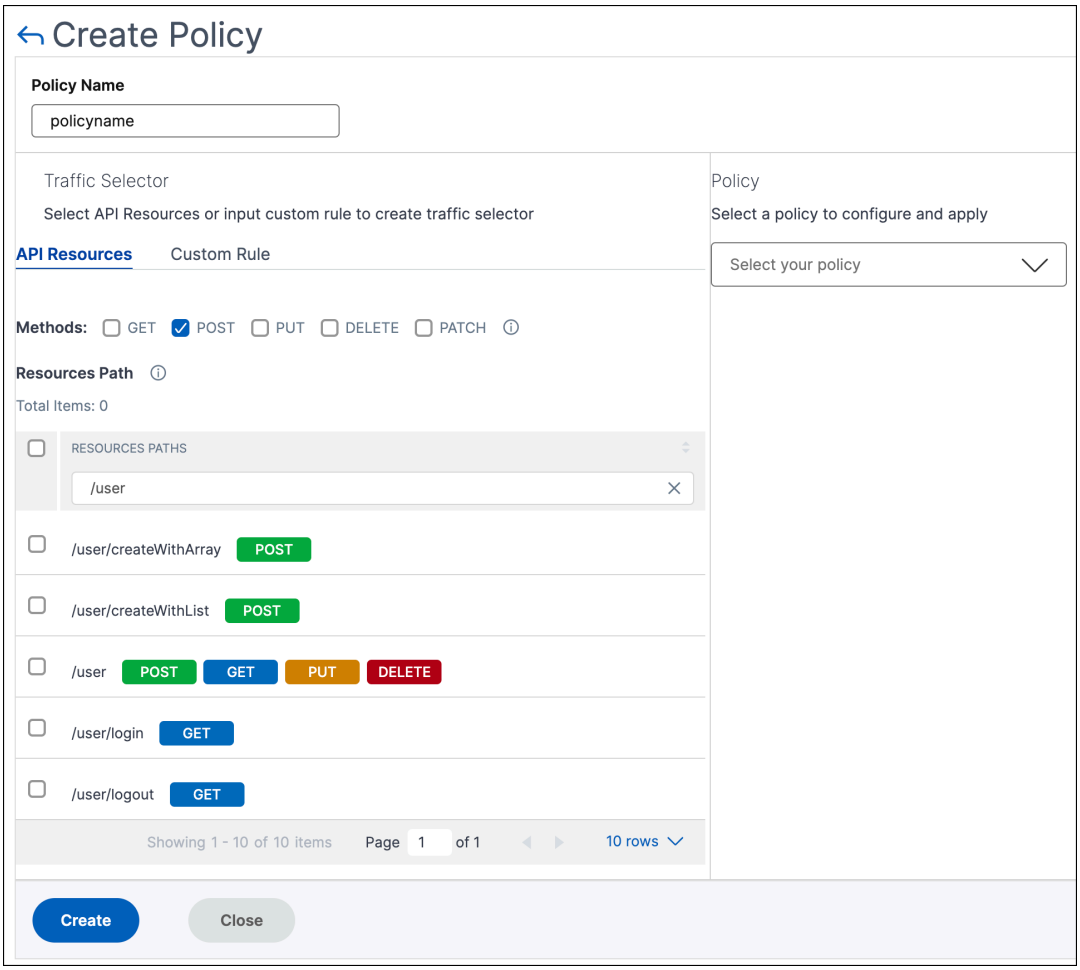
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

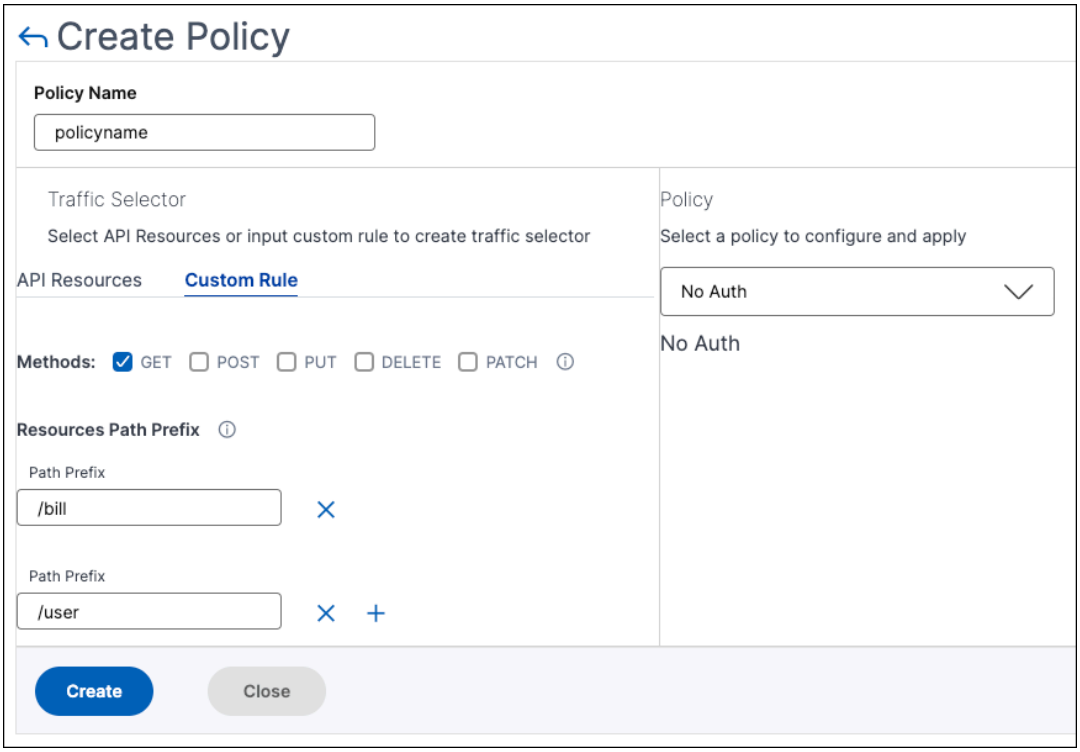


     In this example, the API resources with `/user` that have the `POST` method are listed.

   - **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.

© 1997–2025 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

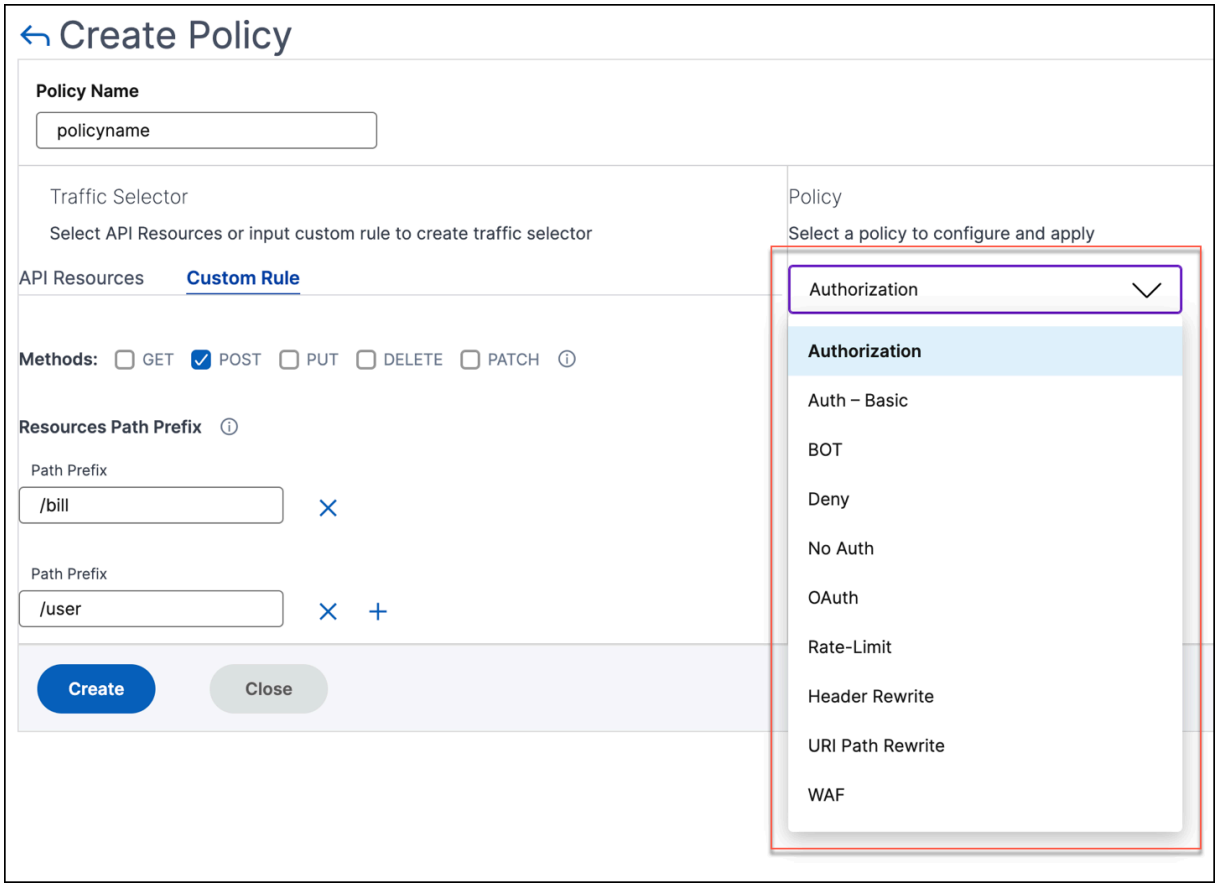
When you are configuring an API policy, you can select the following policies that you want to apply to the API resource and method:

- **Authentication and Authorization**
- **Rate limit**
- **WAF**
- **BOT**
- **Header Rewrite**
- **URI Path Rewrite**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Deny**

> **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.

© 1997–2025 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

> **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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 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).
- **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`).

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.

  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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - **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:

  1. Specify the position where you want to insert a new segment.
  2. In **Current Path Segment**, specify the text after which a new segment to be added.
  3. 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.

View API analytics

January 8, 2024

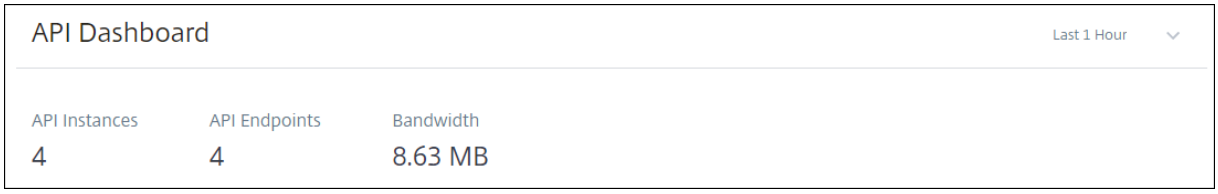
API analytics enables visibility into API traffic. This analytics allows IT administrators to monitor API instances and endpoints served by an API gateway. It provides integrated periodic monitoring of API requests.

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

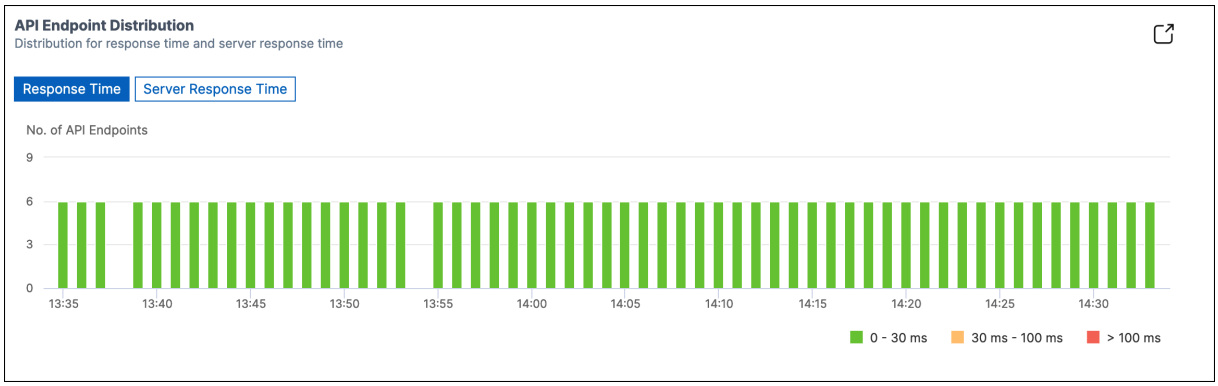
In **API Analytics**, you can monitor the response time of API instances and endpoints that are added as part of API definitions. It also displays the bandwidth consumed by API instances and endpoints.



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.



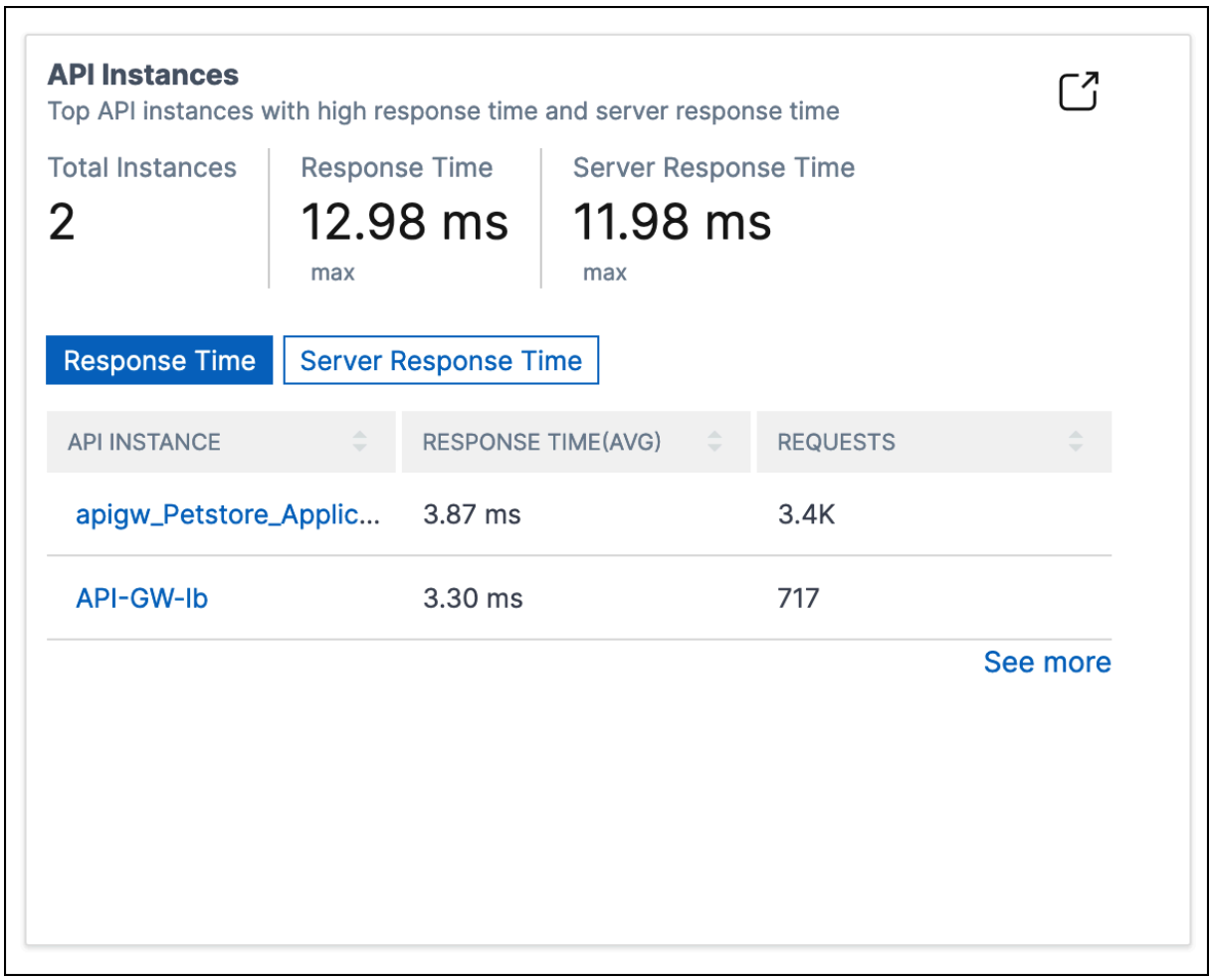
The API endpoints appear in one of the following colors depending on their response time limits:

- **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

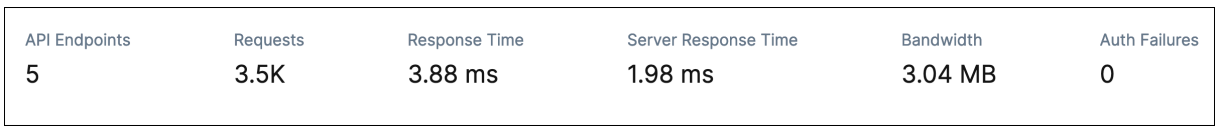
The **API Instances** tile displays the top API instances with high application and server response time.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Select an API instance to view its performance, usage, and security details. The selected API instance displays the following information:

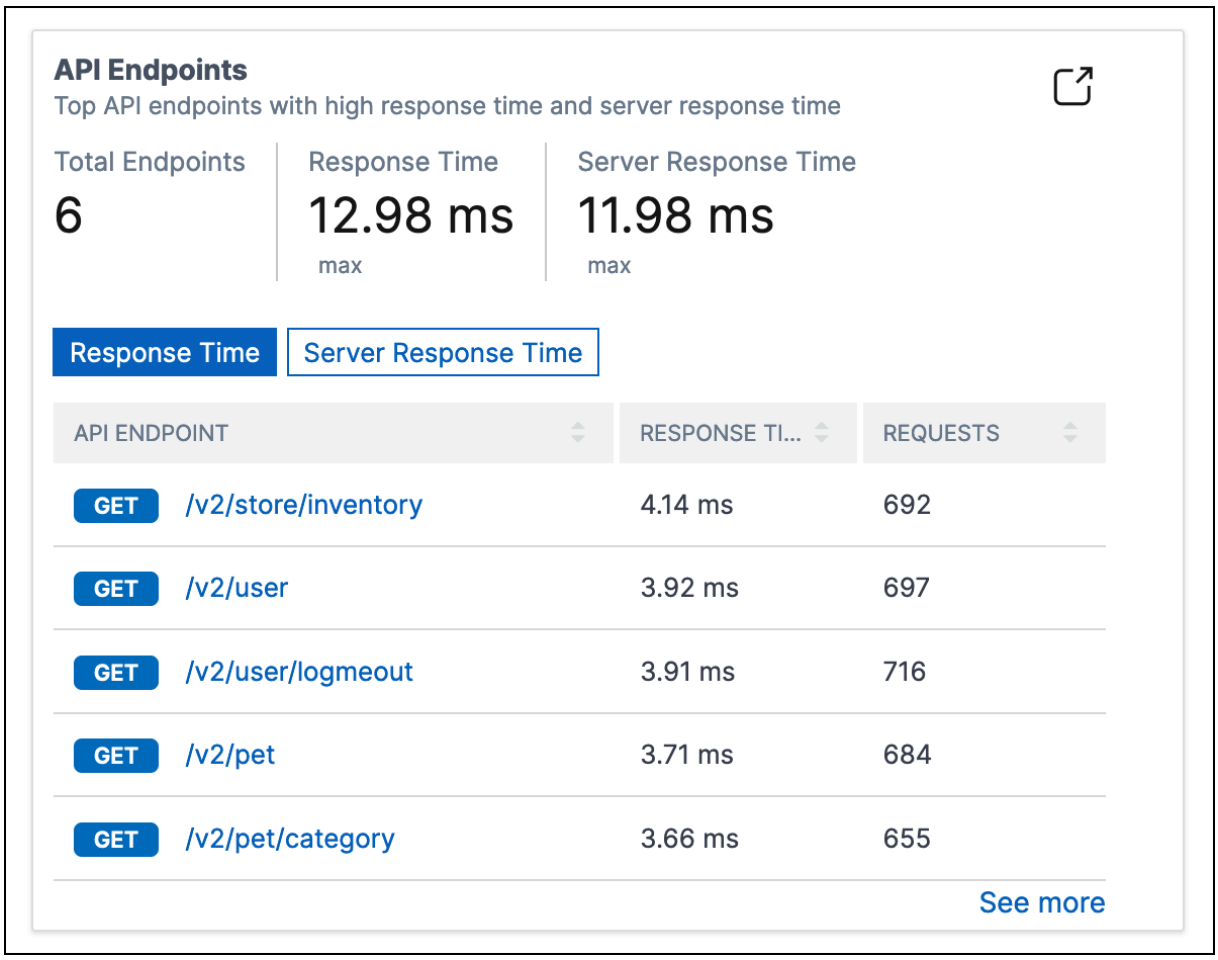
- API endpoints count
- Requests count
- Application and server response time
- Consumed bandwidth
- Authentication failures



API endpoints

The **API Endpoints** tile displays the top endpoints with high application and server response time.

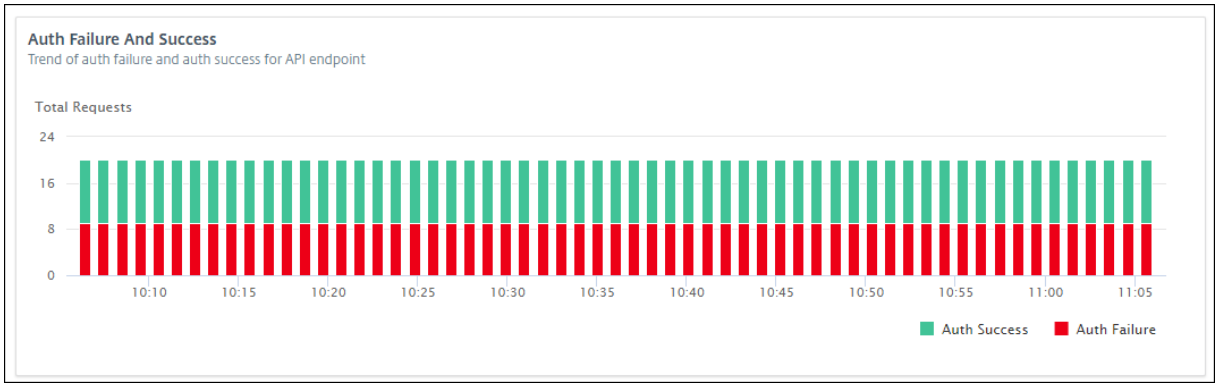
© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.



If you want to view authentication failure and success rate in an API endpoint, do the following:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:

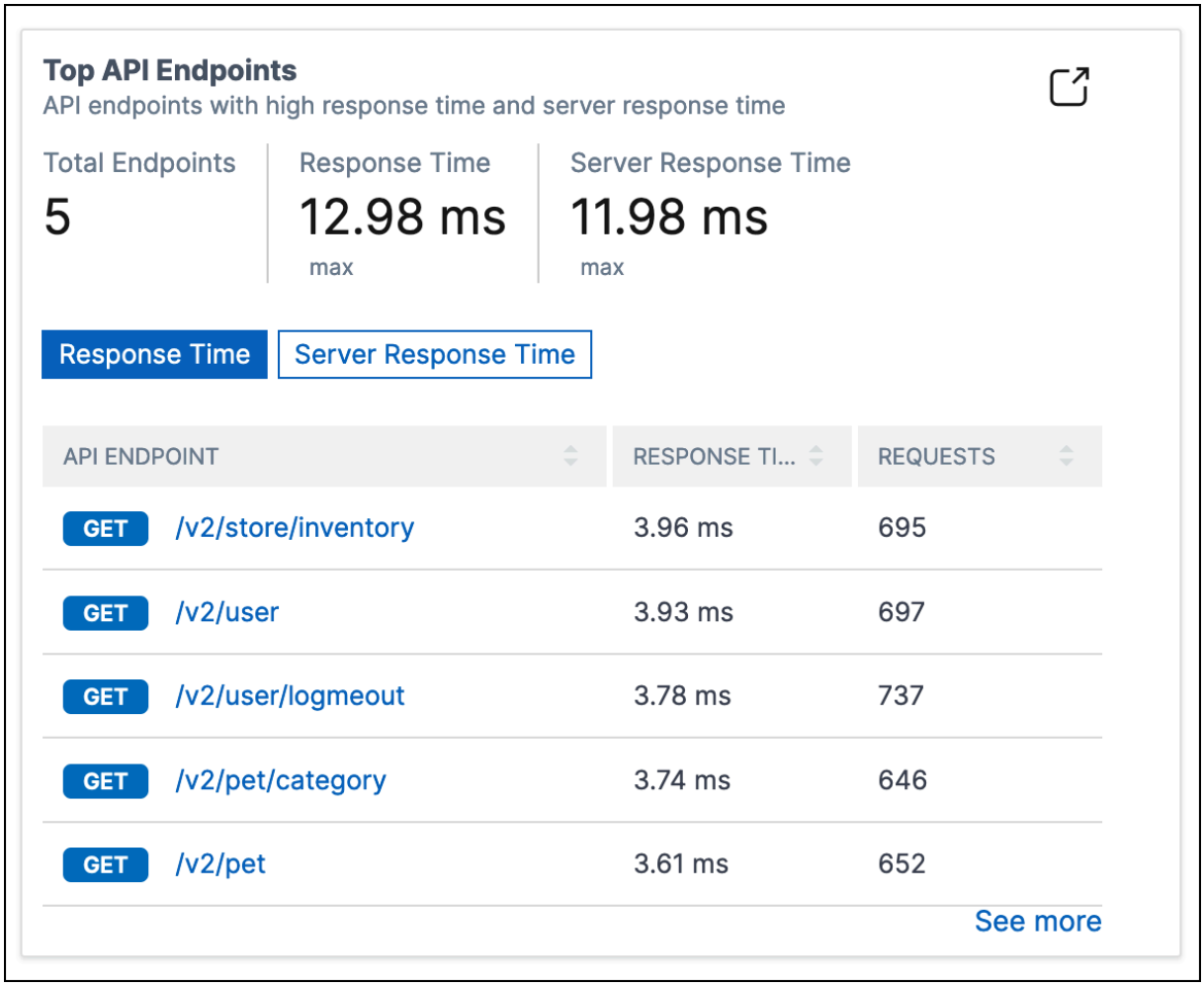
- Top API endpoints in an instance
- Most accessed APIs
- Geo-location of an endpoint
- HTTPS response status
- API requests trend
- Bandwidth consumption of an endpoint
- SSL errors and usage

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.

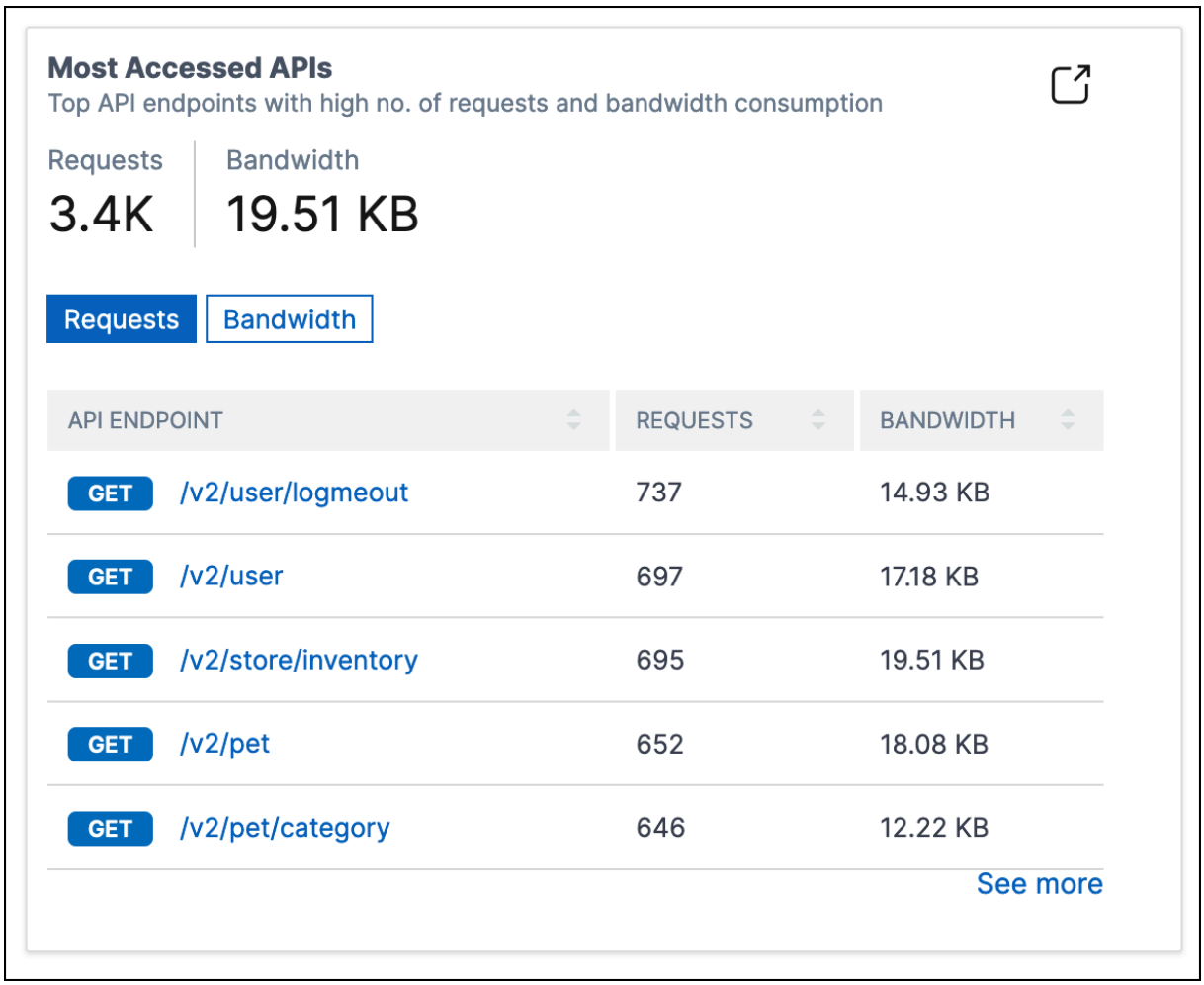
The **Top API Endpoints** tile displays the endpoints that have high application and server response time.



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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

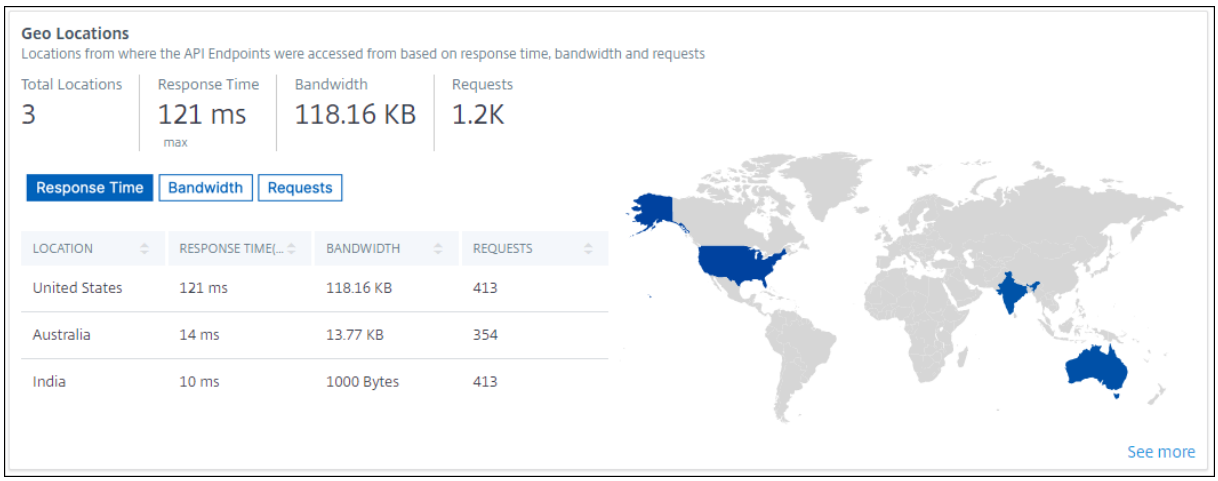


View geo-location of an endpoint

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

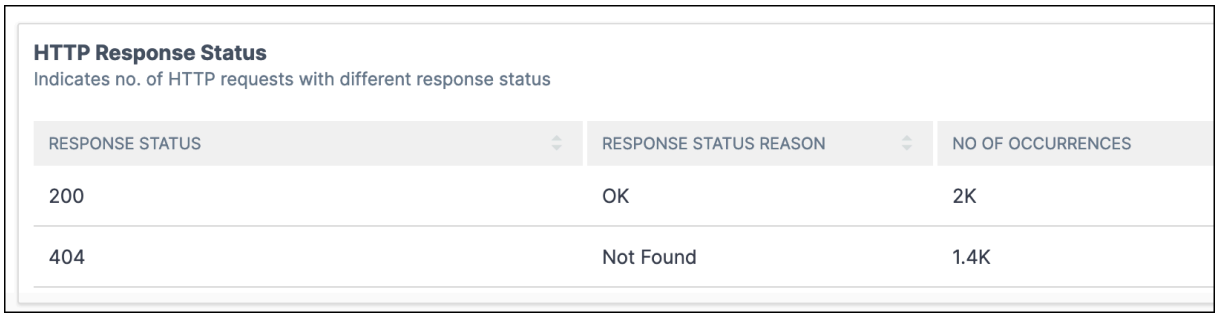


View HTTPS response status

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**.

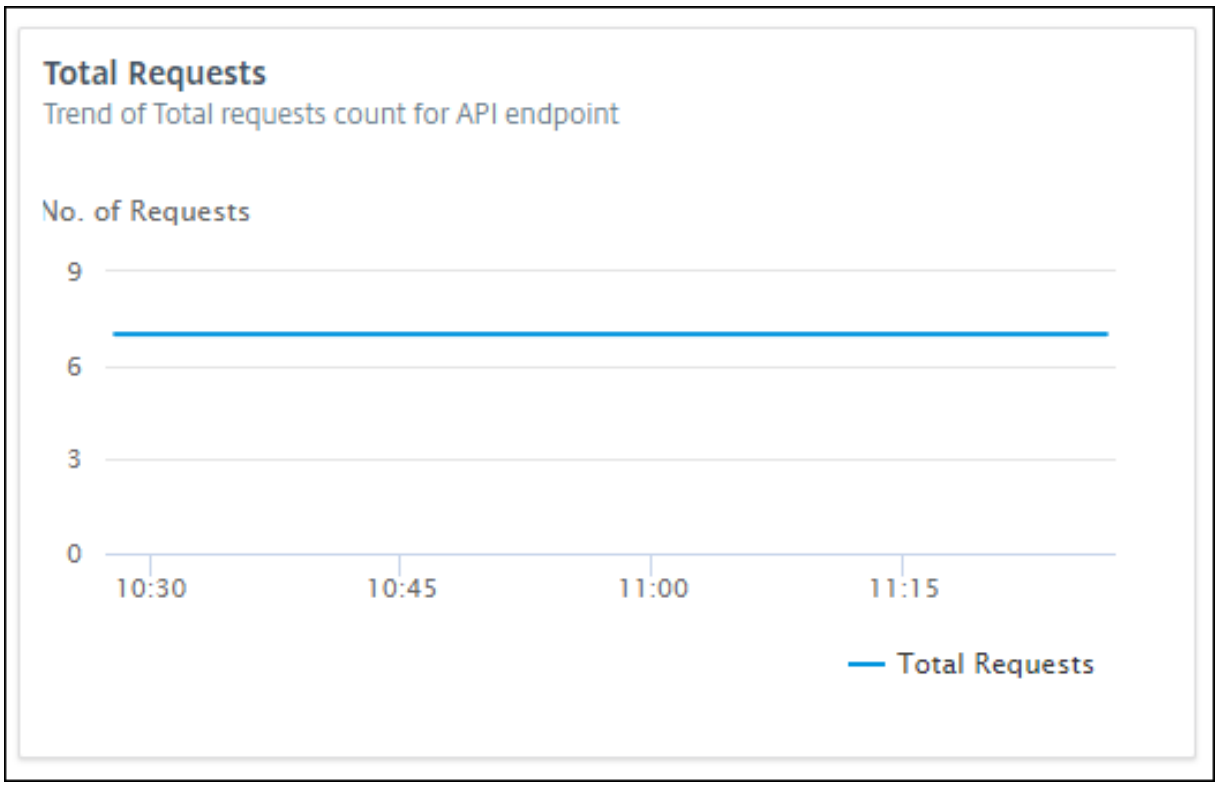
This tile appears in the **Performance and Usage** tab.



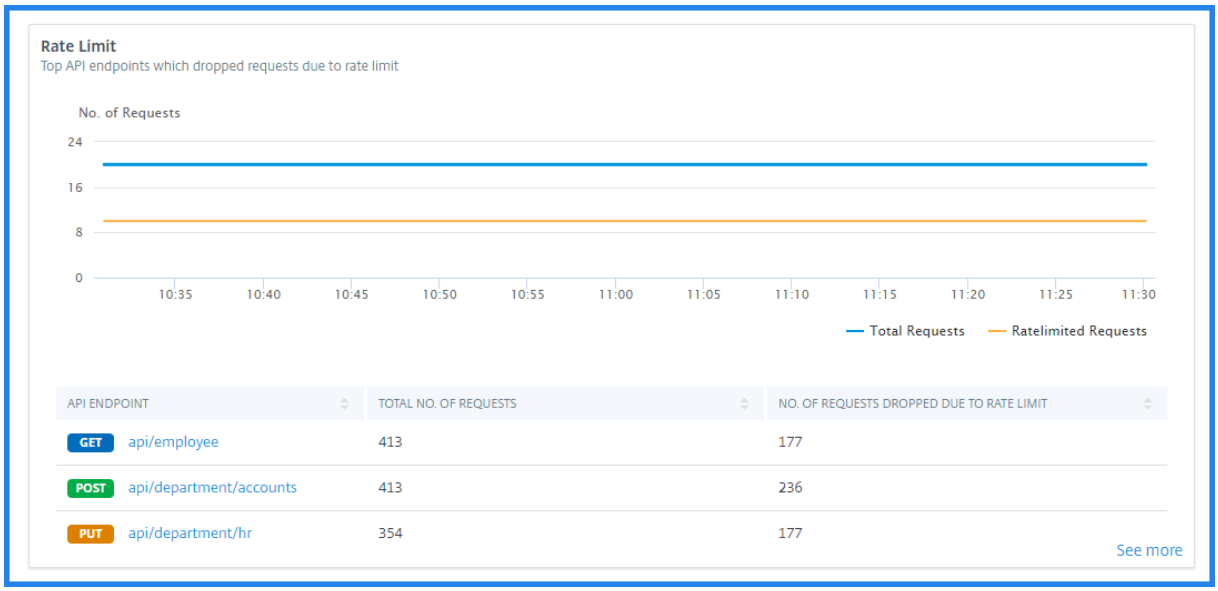
View API requests trend

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.

© 1997–2025 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.

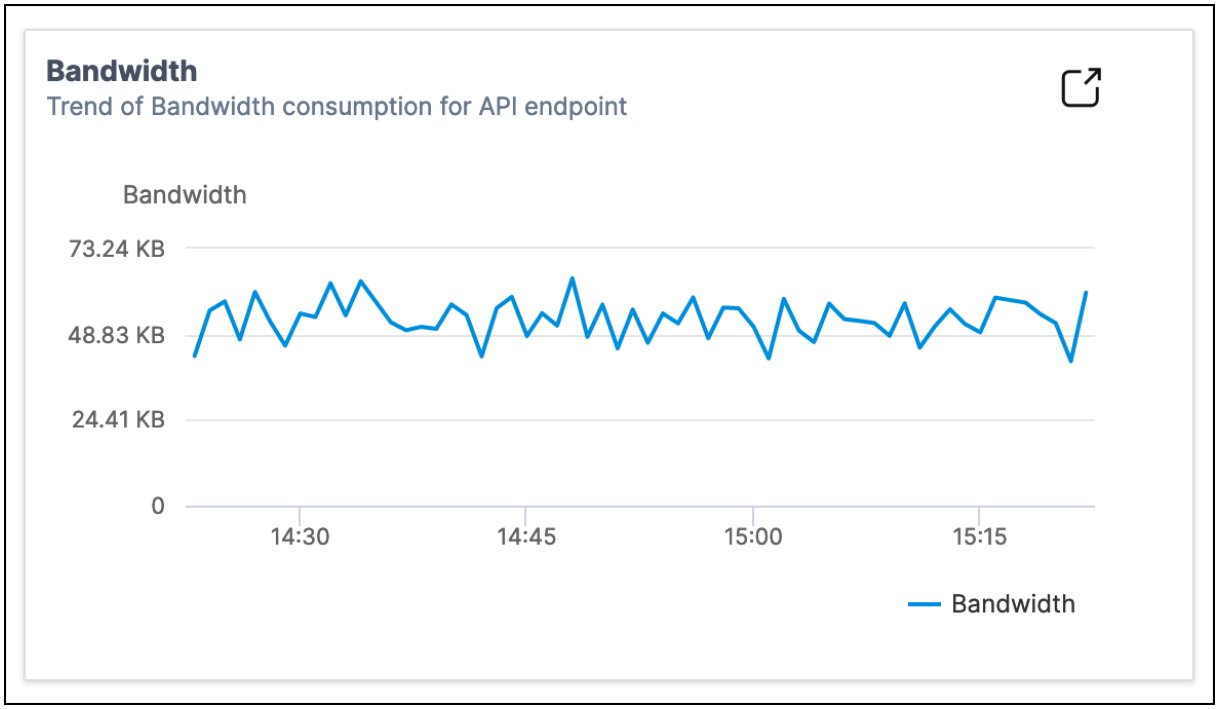


With this comparison, you can determine how many requests are dropped because of a rate limit among total requests.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

View bandwidth consumption of an endpoint

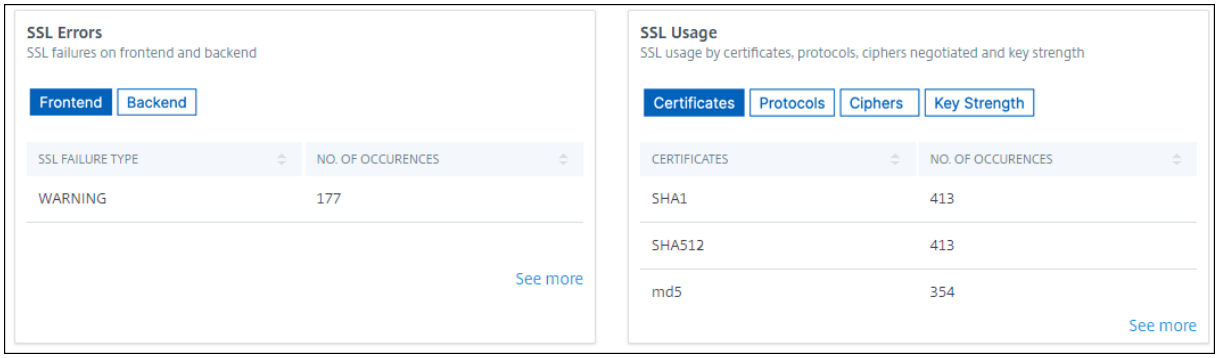
To view the bandwidth consumption trend by an endpoint, select an endpoint from the API endpoints. The **Bandwidth** tile displays a bandwidth consumption graph.



View SSL errors and usage

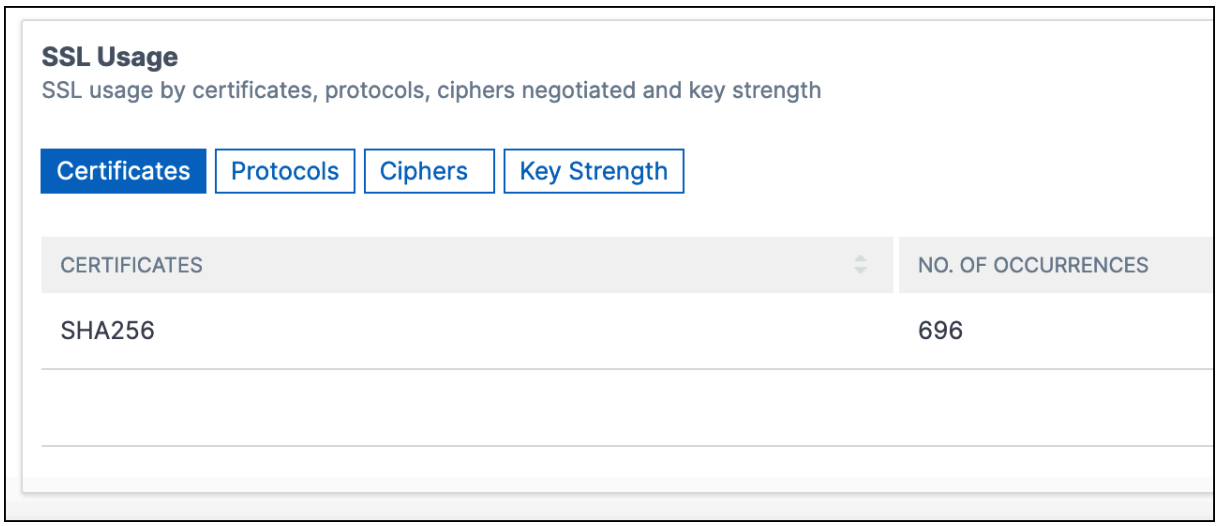
Select an instance from **API Instances**. In **Security**, the following tiles appear:

- **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Discover API endpoints

June 24, 2024

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.

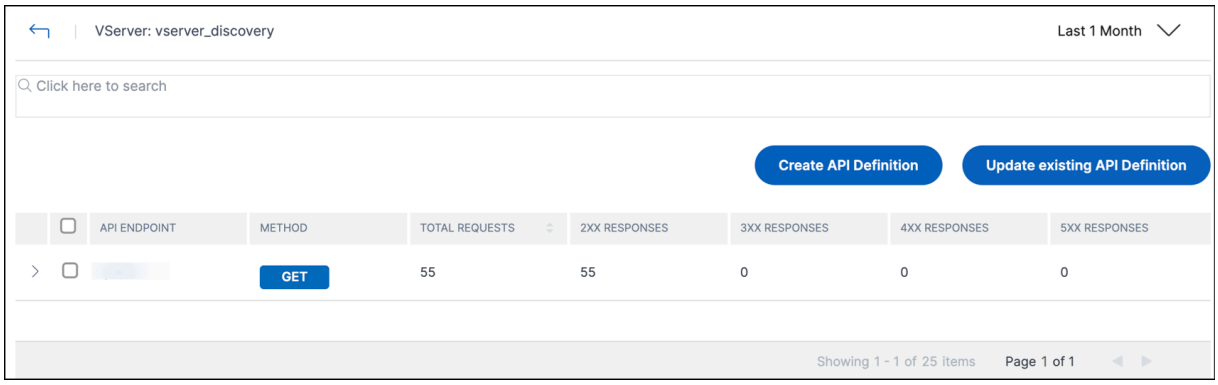
© 1997–2025 Citrix Systems, Inc. All rights reserved.

View API endpoints

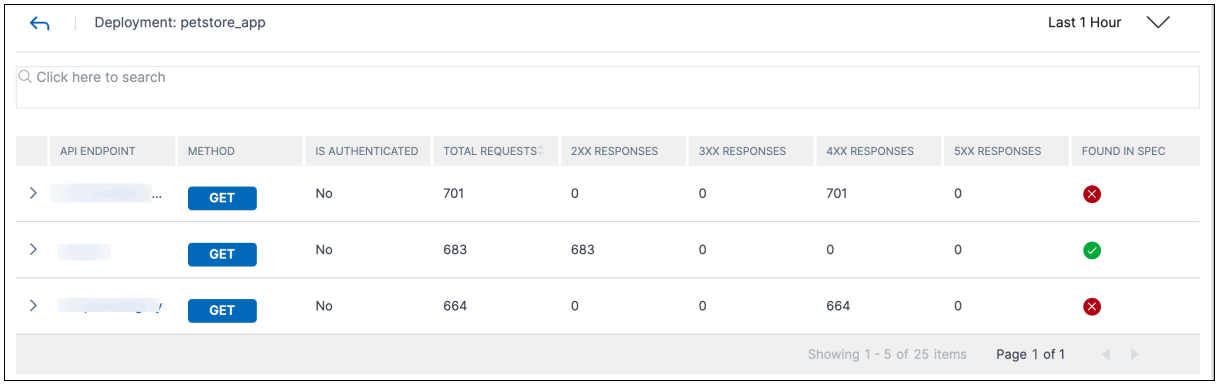
In **API Discovery**, when you select a virtual server or API deployment, the NetScaler Console GUI displays the API endpoints and their details such as:

- **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:

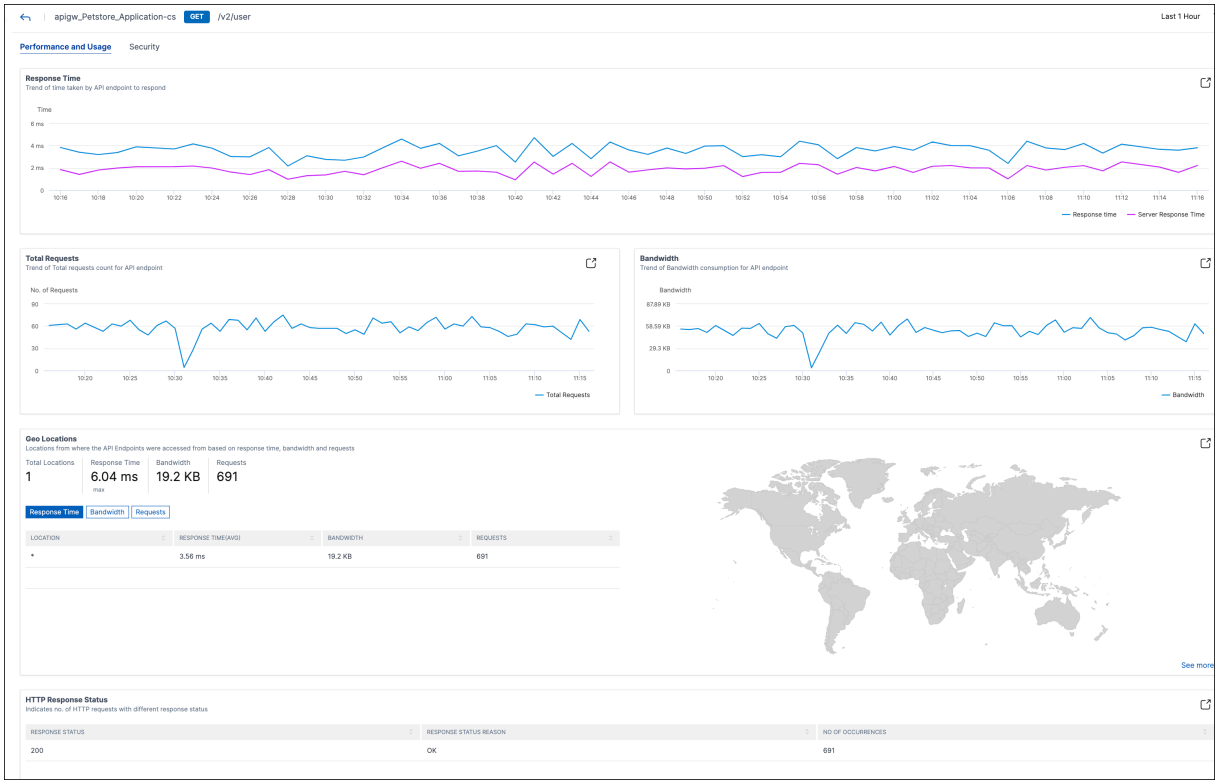


The API endpoints in API deployments are available as follows:



You can also select the required API endpoint to view its detailed analytics report.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

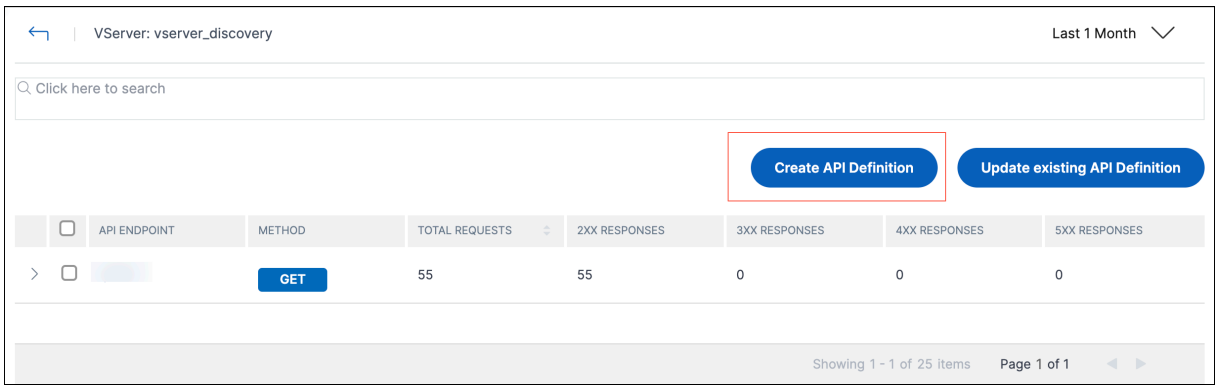


For more information about each section, see View API analytics.

Create API definitions from discovered API endpoints

To create API definitions from discovered API endpoints (API resources and methods):

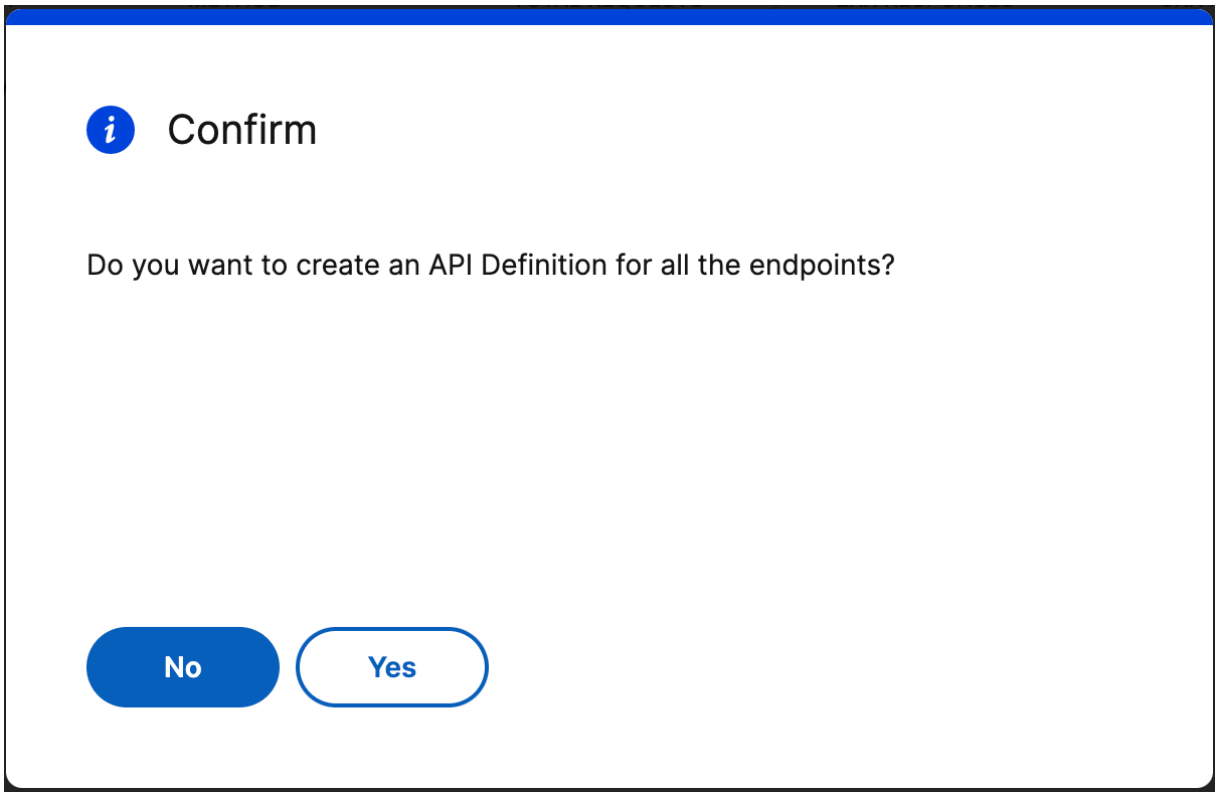
1. Navigate to **Security > API Security > API Discovery** to view the list of virtual servers and API deployments.
2. Click any virtual server in the **VServers** tab.
3. The virtual server page displays the list of discovered endpoints. Select any endpoint and click **Create API Definition**.



© 1997–2025 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.

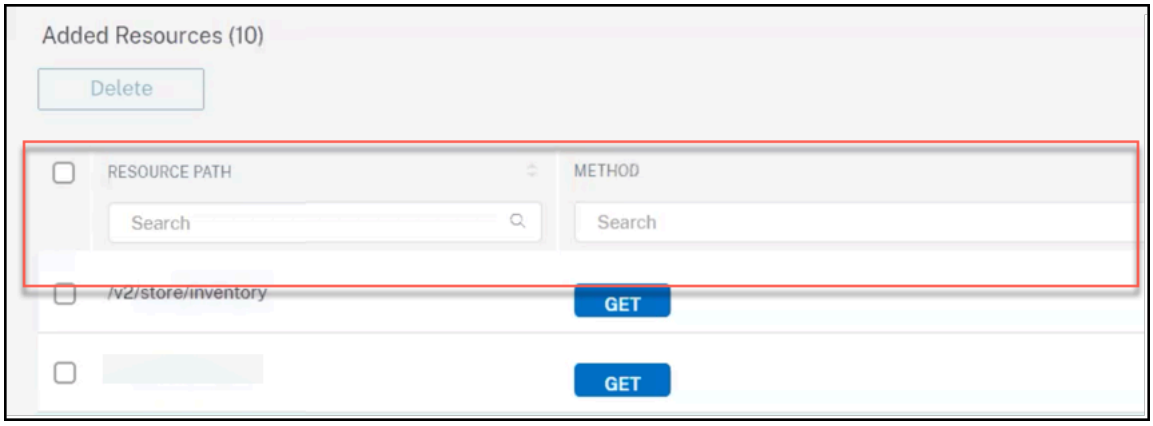
Note:

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.

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

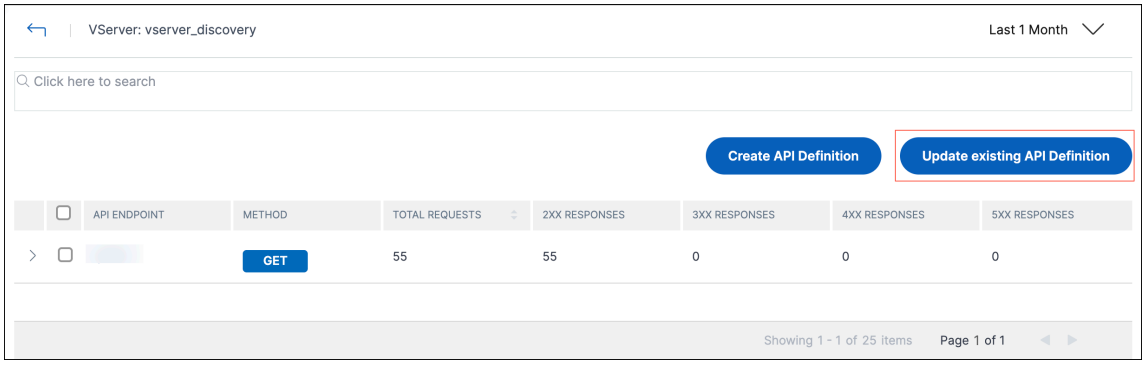
> API resources, add the resource path as "/api/products/{id}/reviews", and delete all the API endpoints with IDs such as "/api/products/123-3243-2344334/reviews".



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
   - **Existing Resources** - The API endpoints already available in the API definition

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **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

January 8, 2024

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.

© 1997–2025 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

January 8, 2024

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`

© 1997–2025 Citrix Systems, Inc. All rights reserved.

	Steps	Resource URL
2	Add an API proxy	`https://adm.cloud.com/apiproxies`
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:

```
{

"endpoints": ["/pet/categories", "/pet/findByName"],
    "get": true,
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
    "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:

```
{

    "policytype": "Ratelimit",
    "config_spec": {

        "api-resource-paths": {

            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                "],
            "get": true,
            "post": false,
            "put": false,
            "delete": false
         }
 ,
        "custom-rules": {
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
 }
,
        "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.

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": {

            "hs256": true,
            "rs256": true,
            "rs512": true
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
30            }
31
32         }
33   ,
34      "order_index": 2,
35      "policy_name": "Jwt_auth_policy"
36   }
```

For more information on each attribute, see OAuth policy

Basic authentication

The following is an example API configuration for the `BasicAuth` policy type:

```
1  {
2
3      "config_spec": {
4
5          "api-resource-paths": {
6
7              "delete": false,
8              "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                   "],
9              "get": true,
10             "post": true,
11             "put": false
12          }
13   ,
14         "custom-rules": {
15    }
16
17       }
18   ,
19      "order_index": 3,
20      "policy_name": "Auth_BaSIC",
21      "policytype": "BasicAuth"
22   }
```

For more information on each attribute, see Basic authentication policy.

No authentication

The following is an example API configuration for the `NoAuth` policy type:

```
1  {
2
3      "config_spec": {
4
5          "api-resource-paths": {
6
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
            "delete": false,
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                "],
            "get": true,
            "post": false,
            "put": false
         }
,
        "custom-rules": {
 }

    }
,
   "order_index": 4,
   "policy_name": "no_auth_policy",
   "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.

© 1997–2025 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:

```
{

    "policytype": "Header Rewrite",
    "config_spec": {

        "api-resource-paths": {

            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                "],
            "get": true,
            "post": true,
            "put": false,
            "delete": false
         }
 ,
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
        "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:

```
{

    "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",
            "old-path-value": "v2",
            "action-type": "replace path segment"
         }
,
        {
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
35
36              "insert-segment-position": "beginning",
37              "new-path-value": "begin",
38              "action-type": "insert path segment"
39           }
40   ,
41          {
42
43              "insert-segment-position": "end",
44              "new-path-value": "end",
45              "action-type": "insert path segment"
46           }
47   ,
48          {
49
50              "insert-segment-position": "before",
51              "new-path-value": "before",
52              "old-path-value": "store",
53              "action-type": "insert path segment"
54           }
55   ,
56          {
57
58              "insert-segment-position": "after",
59              "new-path-value": "after",
60              "old-path-value": "store",
61              "action-type": "insert path segment"
62           }
63
64          ]
65       }
66   ,
67          "order_index": 24,
68          "policy_name": "eats_uripathrewrite",
69          "policytype": "URI Path Rewrite ”
70   }
```

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:

```
1  {
2
3      "policytype": "Authorization",
4      "config_spec": {
5
6          "api-resource-paths": {
7
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                "],
            "get": true,
            "post": true,
            "put": false,
            "delete": false
         }
,
        "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,
            "delete": false
         }
,
        "custom-rules": {
 }
,
        "api-denytype": "RESPONDWITH"
     }
,
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
    "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

January 16, 2024

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**.

   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.

© 1997–2025 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 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.
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.

Applications

March 18, 2024

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

Web Insight dashboard

September 8, 2025

> **Note:**
>
> Starting from **14.1-51.x** release, Web Insight analytics are visible for virtual servers that are configured with an IPv6 address.

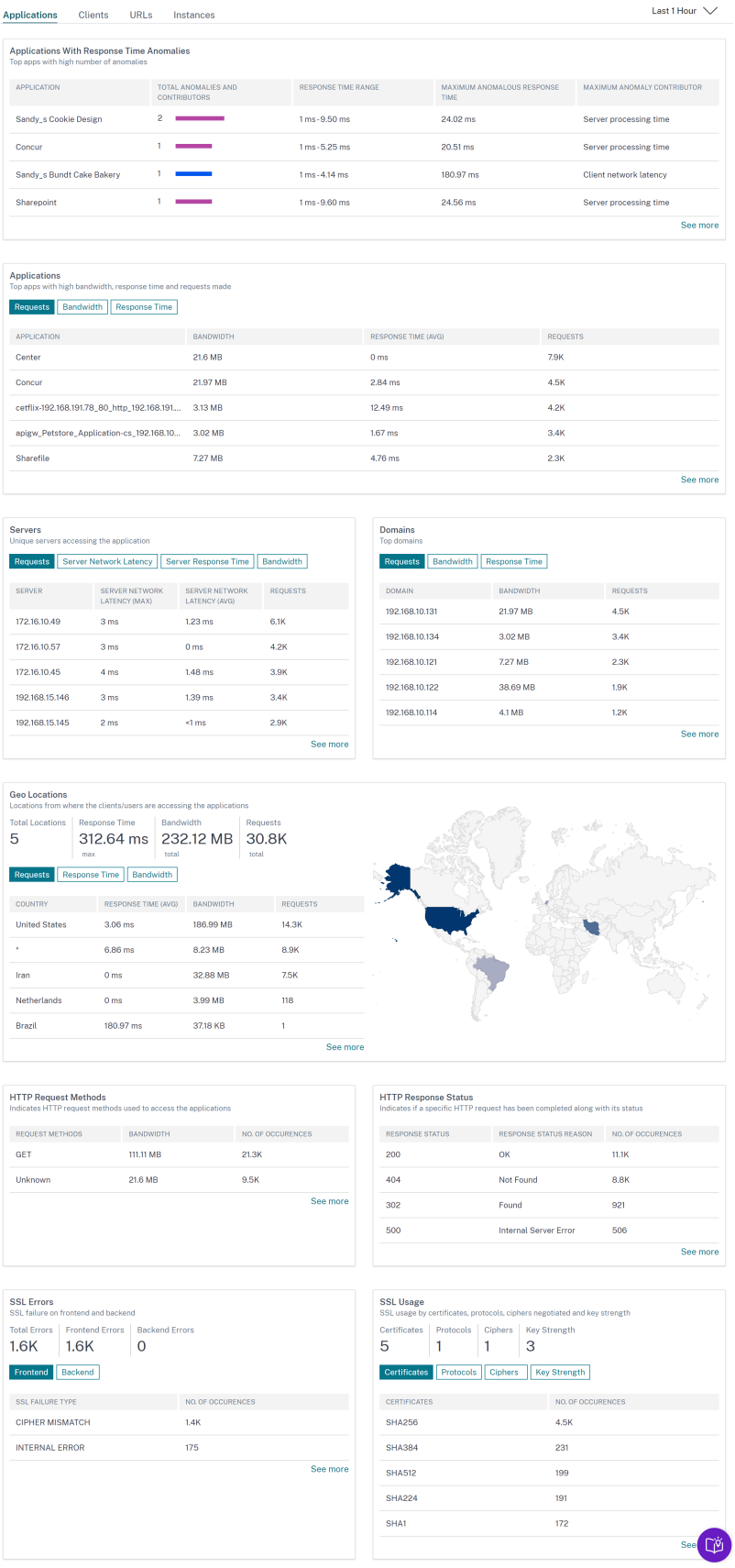
The improved Web Insight feature is augmented and provides visibility into detailed metrics for web applications, clients, and NetScaler instances. This improved Web Insight enables you to evaluate and visualize the complete application from the perspectives of performance and usage together. As an administrator, 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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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
HTTP Request Methods	Browsers		Clients
HTTP Response Status	SSL Errors		Servers
SSL Errors	SSL Usage		Operating System
SSL Usage			Browsers

© 1997–2025 Citrix Systems, Inc. All rights reserved.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

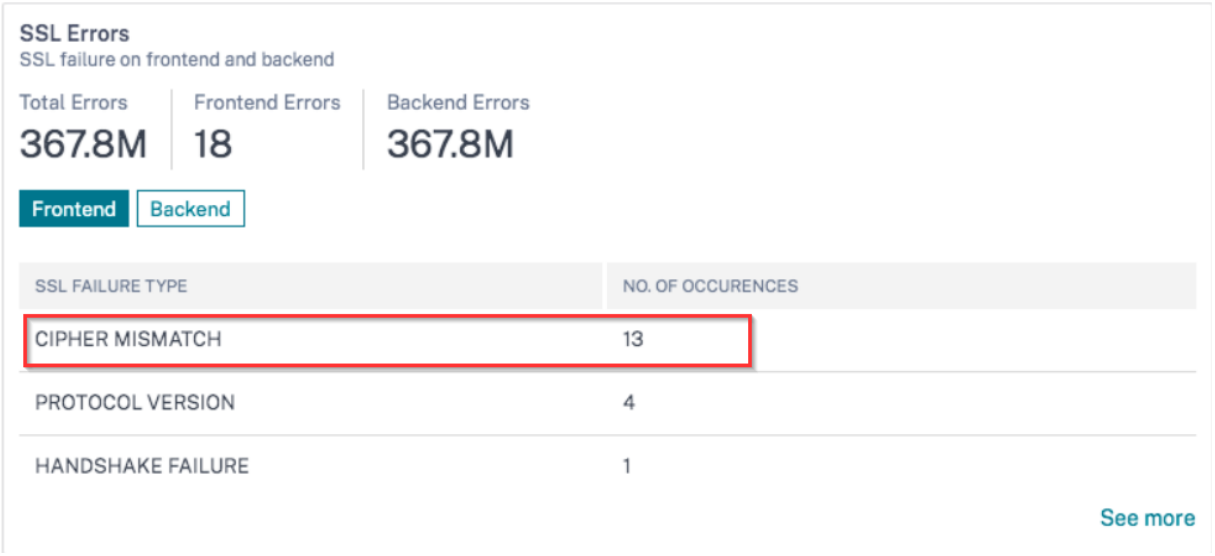
> **Note**
>
> - Starting from **14.1-1.16** or later release, when you drill down a metric, the analytics view in the time series graph displays nil values (for example, 0 ms and 0 request) for the selected duration. Earlier, if there was no traffic or transaction received for the selected duration, 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

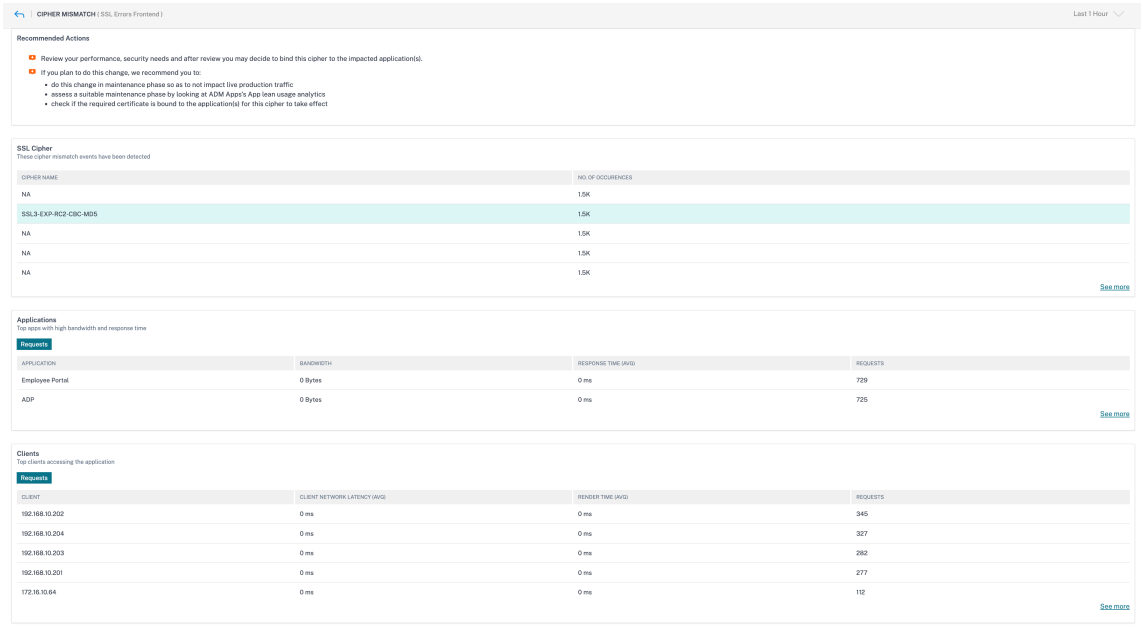
Under **SSL errors**, click an SSL parameter (Cipher Mismatch or Unsupported Ciphers) to view details such as the SSL cipher name, the recommended actions, and the details of the affected applications and clients.



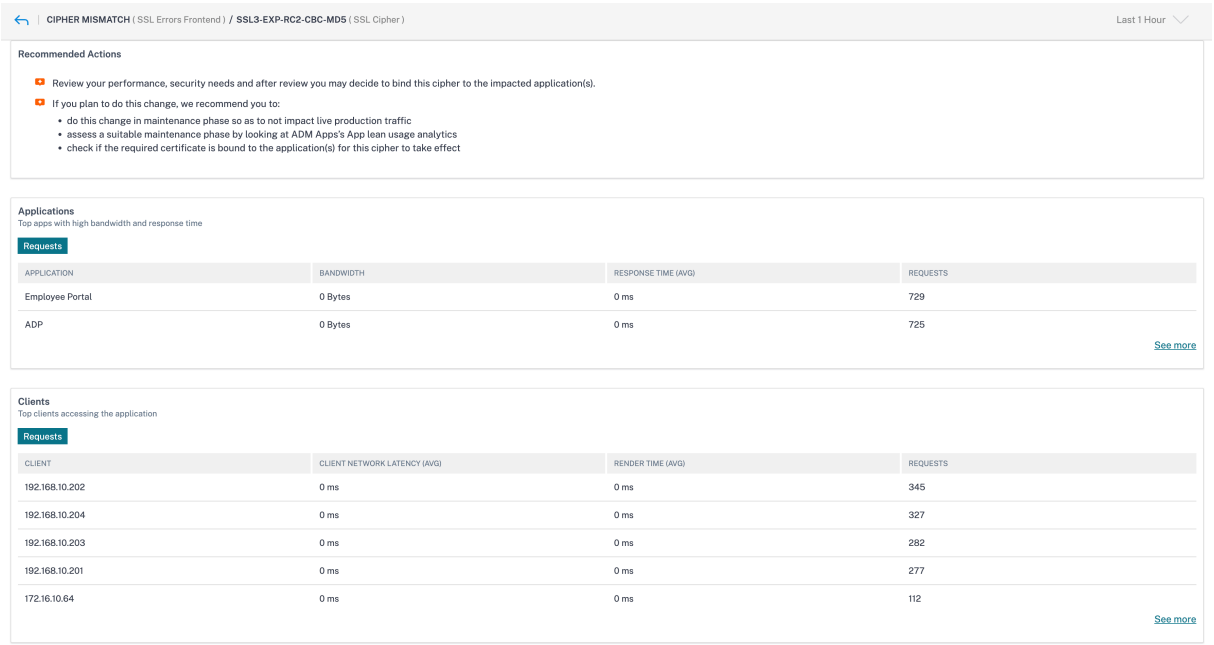
The details page appears for the selected SSL parameter. You can:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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.

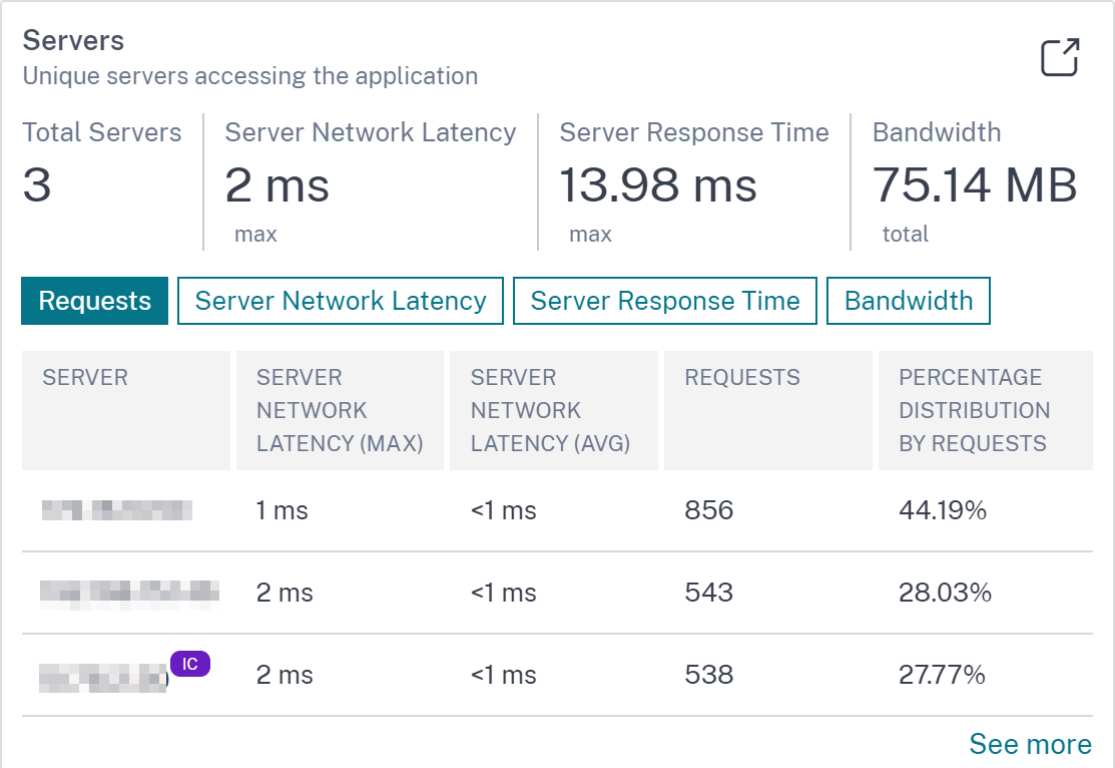


© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

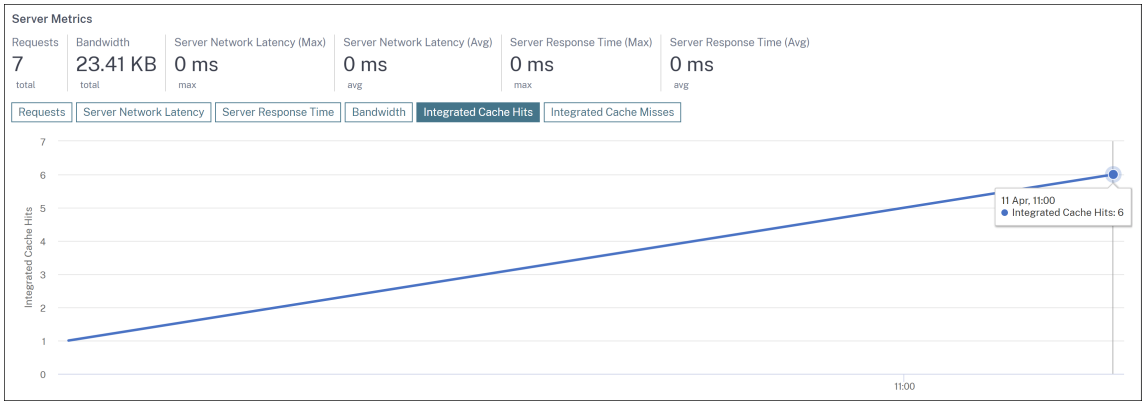


When you drill down a server to view more details, the **Server Metrics** display integrated cache hits and misses tabs.

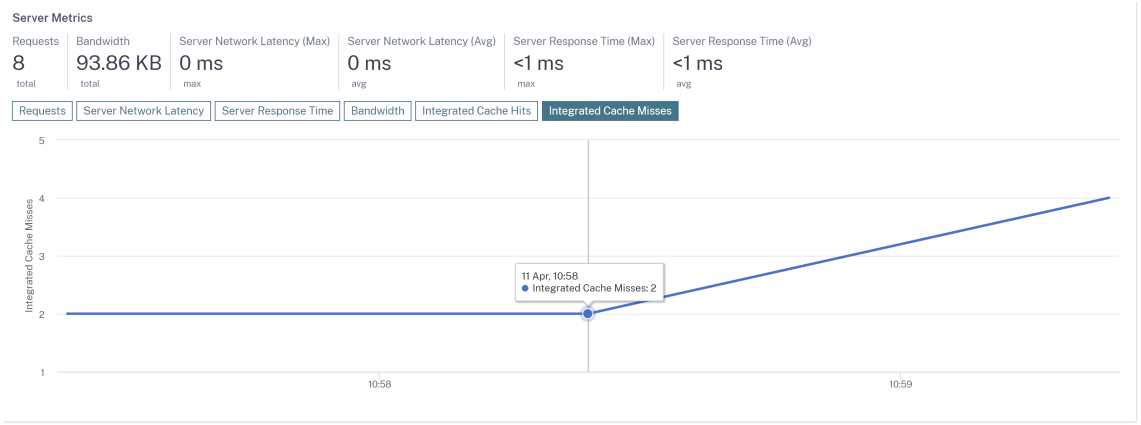
The graph view in:

- The **Integrated Cache Hits** tab enables you to view the total responses that the NetScaler appliance serves from the cache.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- The **Integrated Cache Misses** tab enables you to view the total responses that the NetScaler appliance serves from the origin server.

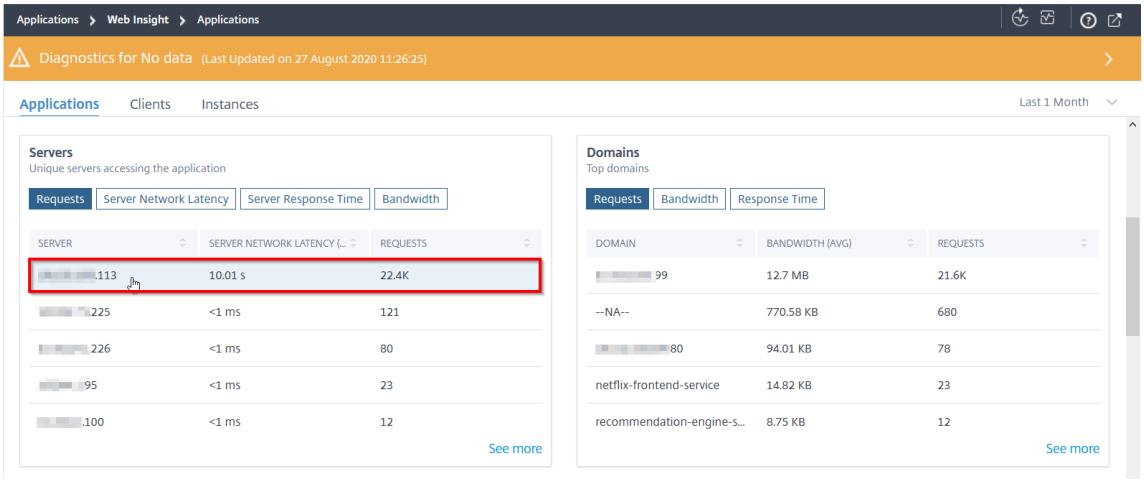


Other use case

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:

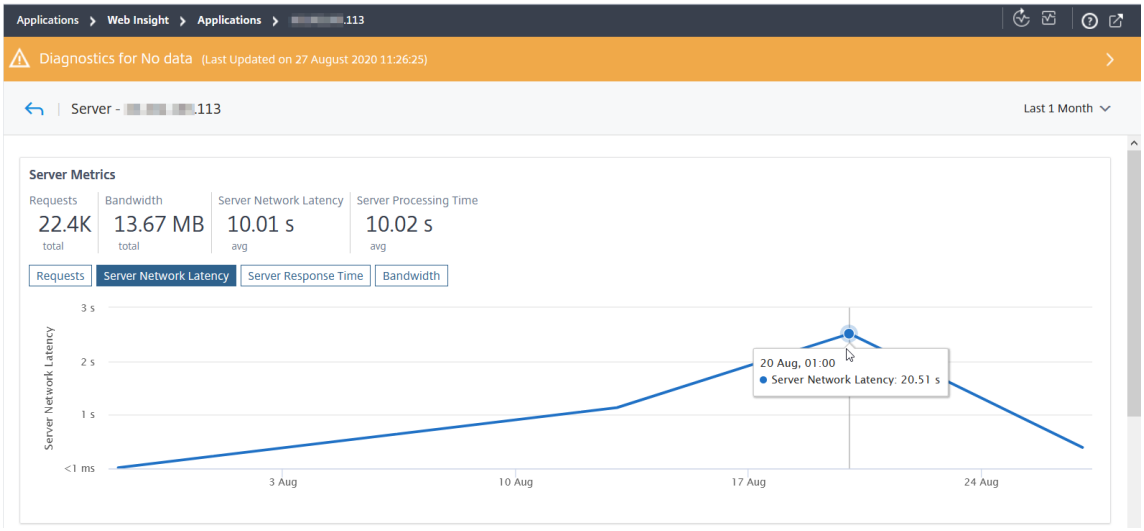
1. Select Last 1 Month from the list and from the **Applications** tab, scroll down to **Servers**, and click a server.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



The metrics details for the selected server are displayed.

2. Select the **Server Network Latency** tab to analyze the latency.



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

January 8, 2024

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

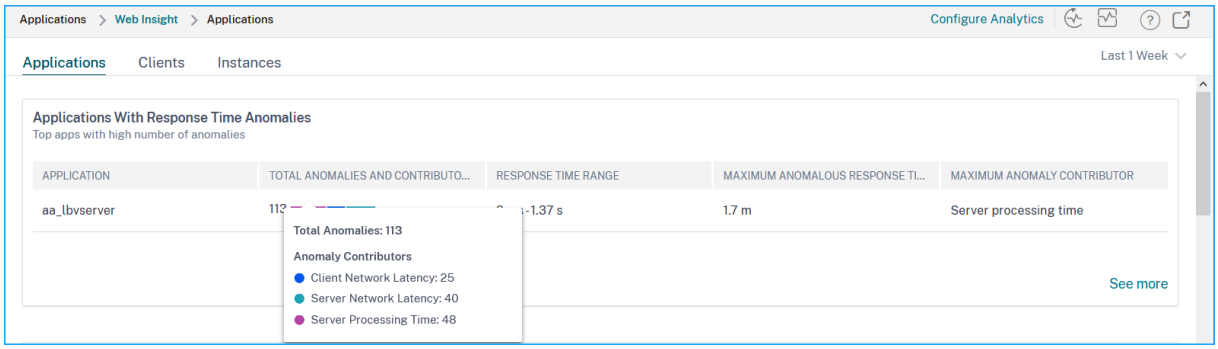
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

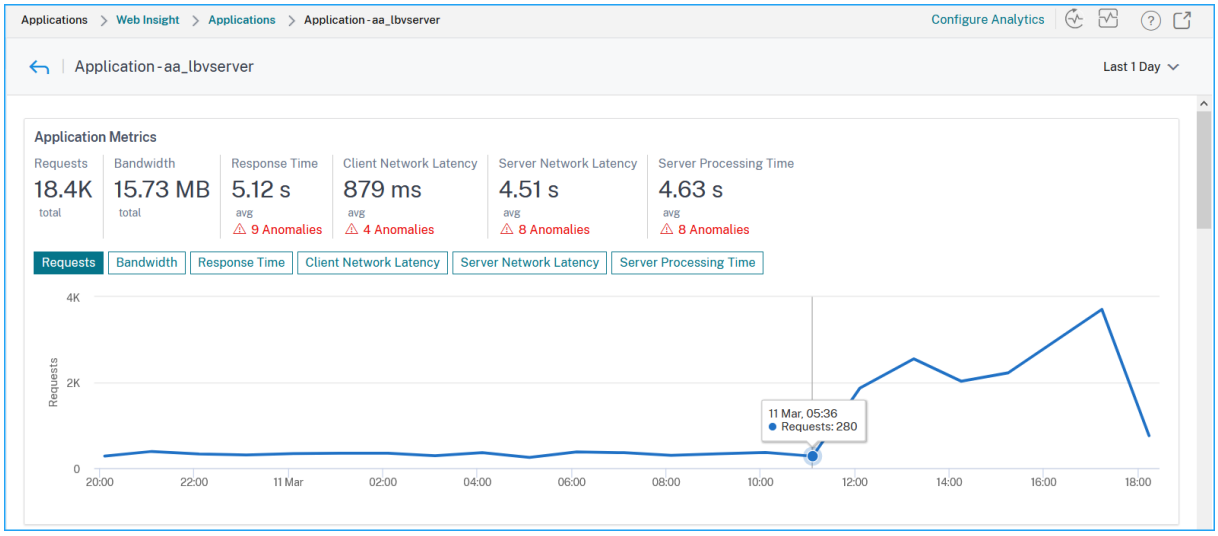


- **Application** –Denotes the application name.
- **Total Anomalies and Contributors** –Denotes the total anomalies from the application. When you hover the mouse pointer, you can view the total anomalies that are from the client network latency, server network latency, and server processing time respectively.
- **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



The **Application Metrics** enable you to view:

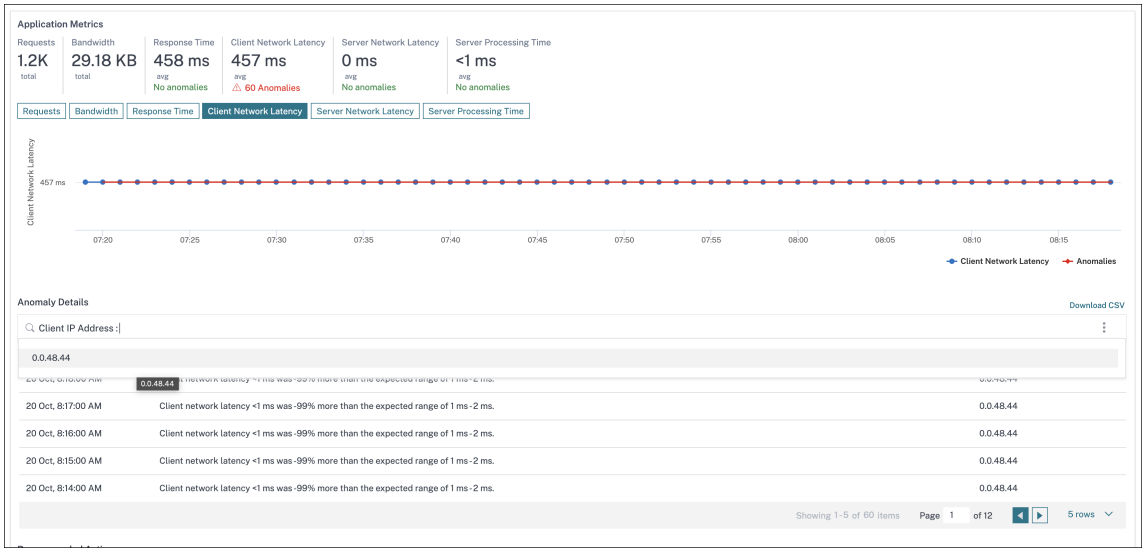
- **Summary** –An overview to visualize the application performance such as Response Time, Requests, and Bandwidth
- **Requests** –The total requests received by the application. You can also view requests from the top 5 clients based on the total requests
- **Bandwidth** –The total bandwidth processed 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:

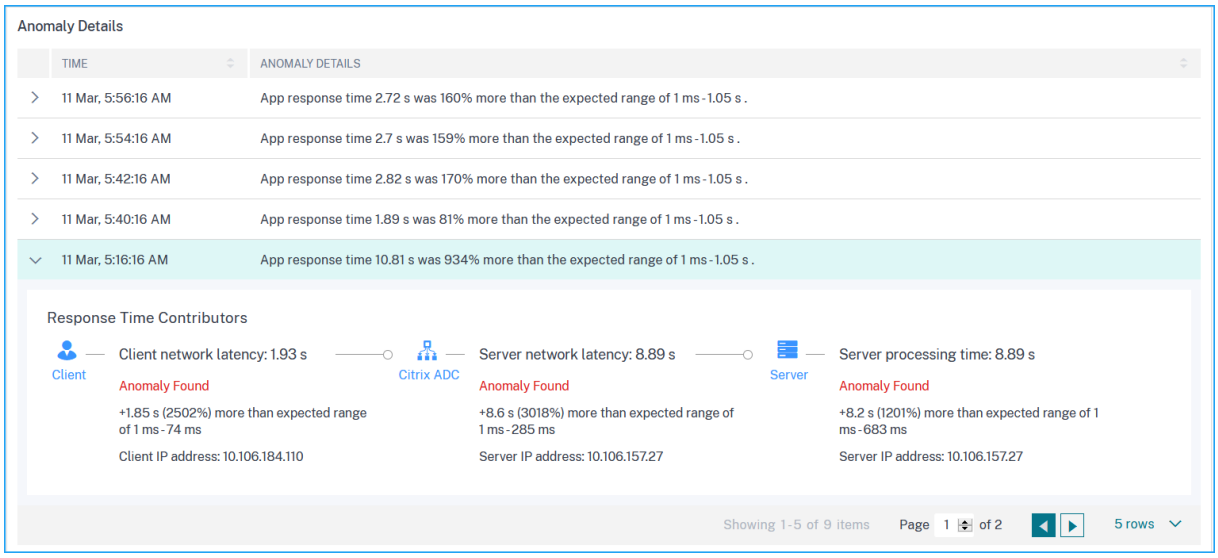
- **A search bar** - Click the search bar to view the IP address of all clients (in Client Network Latency) and servers (in Server Network Latency). You can select the IP address to filter results.
- **An export option** - Click **Download CSV** to export the details in CSV format.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



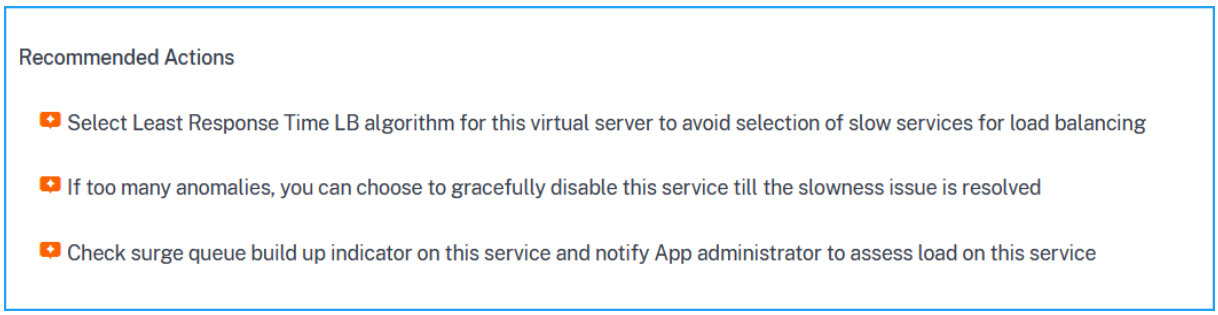
Response Time

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, 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.

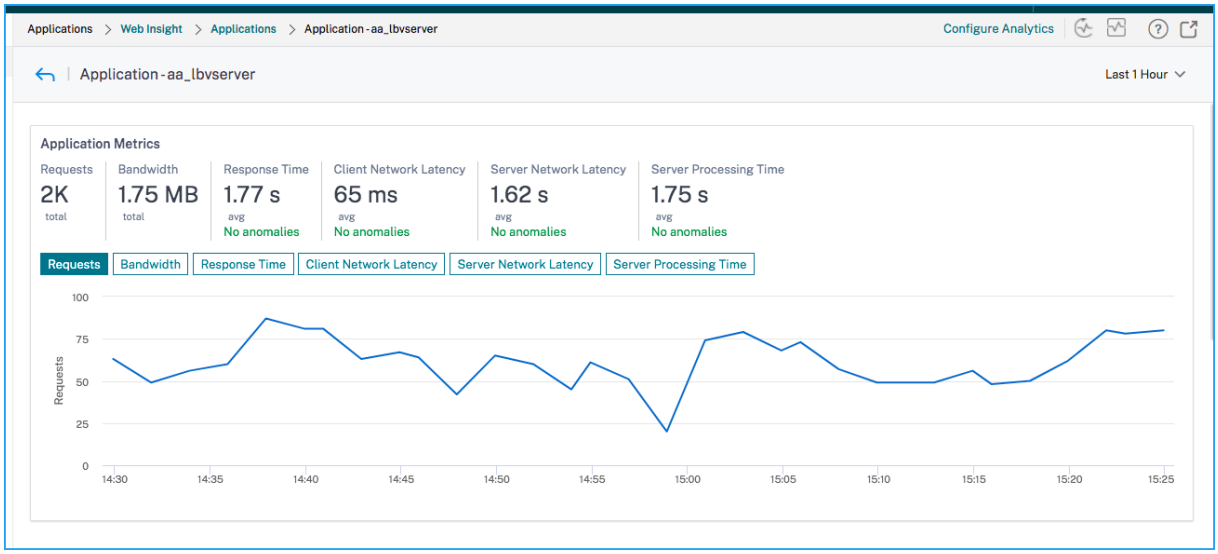
© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.



Service Graph

September 8, 2025

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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
- 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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)

  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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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.
- 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.

StyleBooks

January 8, 2024

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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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, 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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
- APIs in StyleBooks
- StyleBooks grammar

Application Security Dashboard

February 27, 2024

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

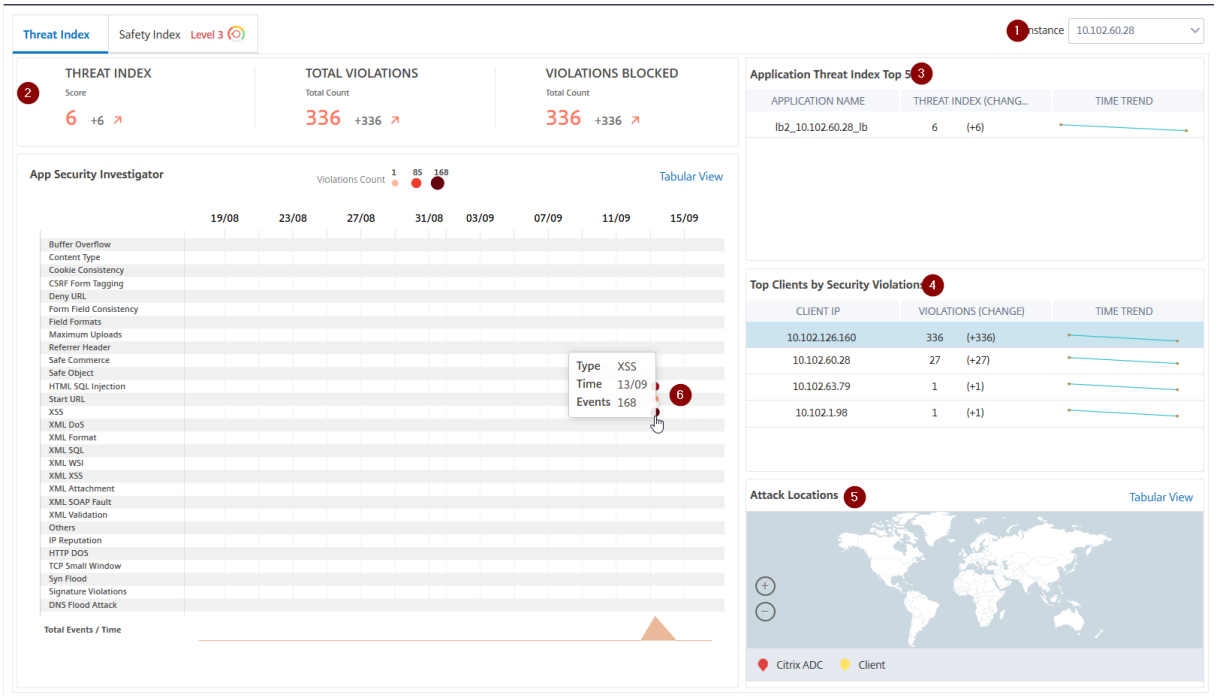
The threat index is based on attack information. The attack-related information, such as violation type, attack category, location, and client details, gives an insight into the attacks on the application. Violation information is sent to NetScaler Console only when a violation or attack occurs. Many 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

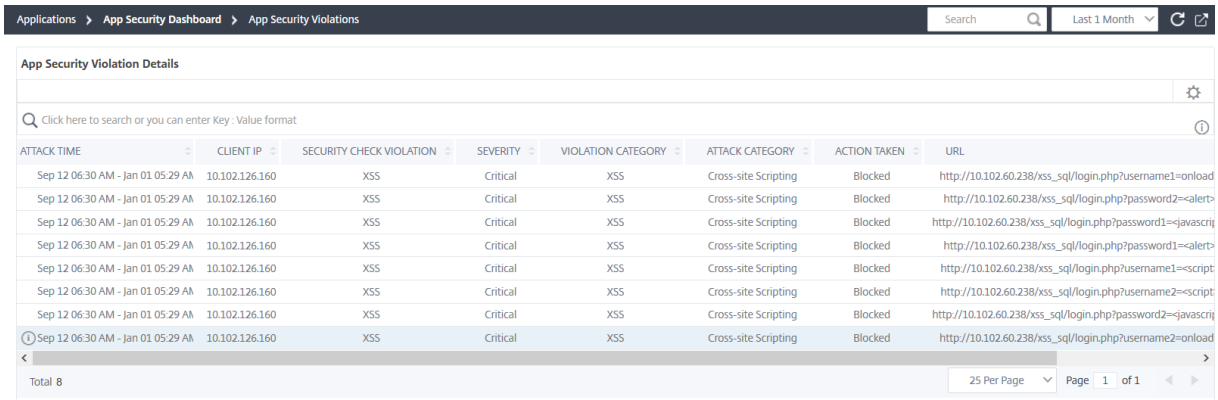
4 - Displays the security violations based on clients. The App Security Investigator graph is displayed for each client. You can click each client IP to view results.

5 - Displays the violations in map view and tabular view.

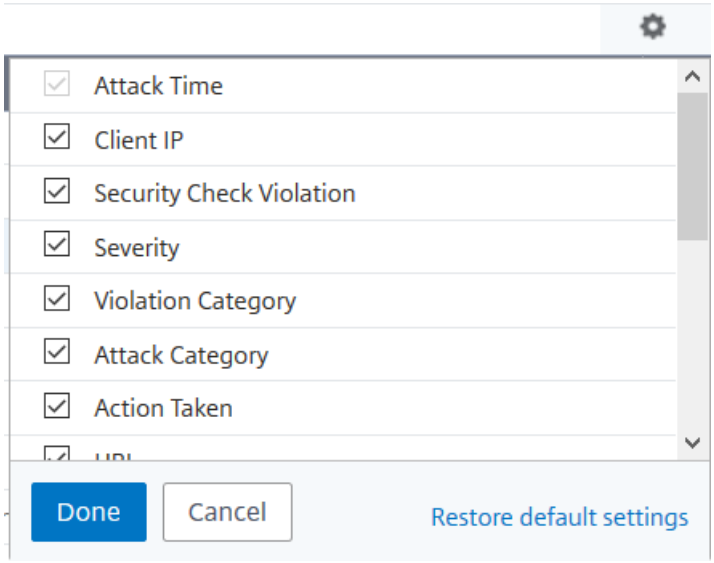
6 - Displays the violation details. When you hover the mouse pointer on the graph, the details such as violation type, time of the attack, and total events are displayed.

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.



© 1997–2025 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.

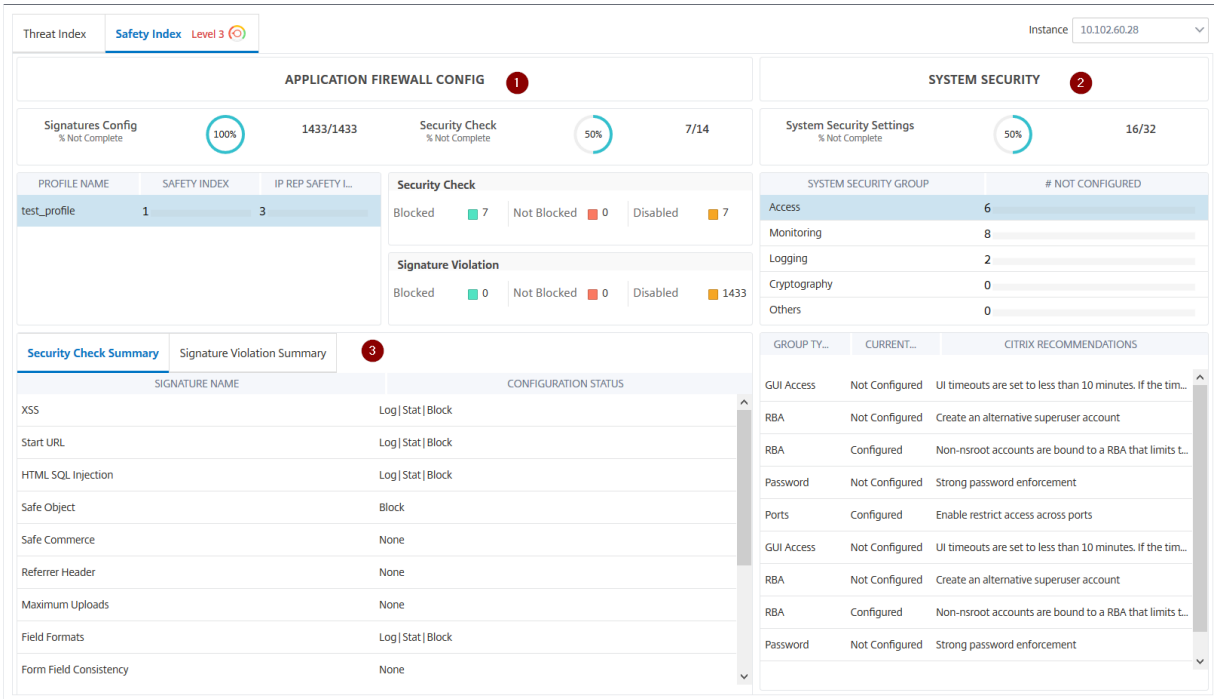
The safety index summary gives you information about the effectiveness of the following security configurations:

- **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.

© 1997–2025 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.

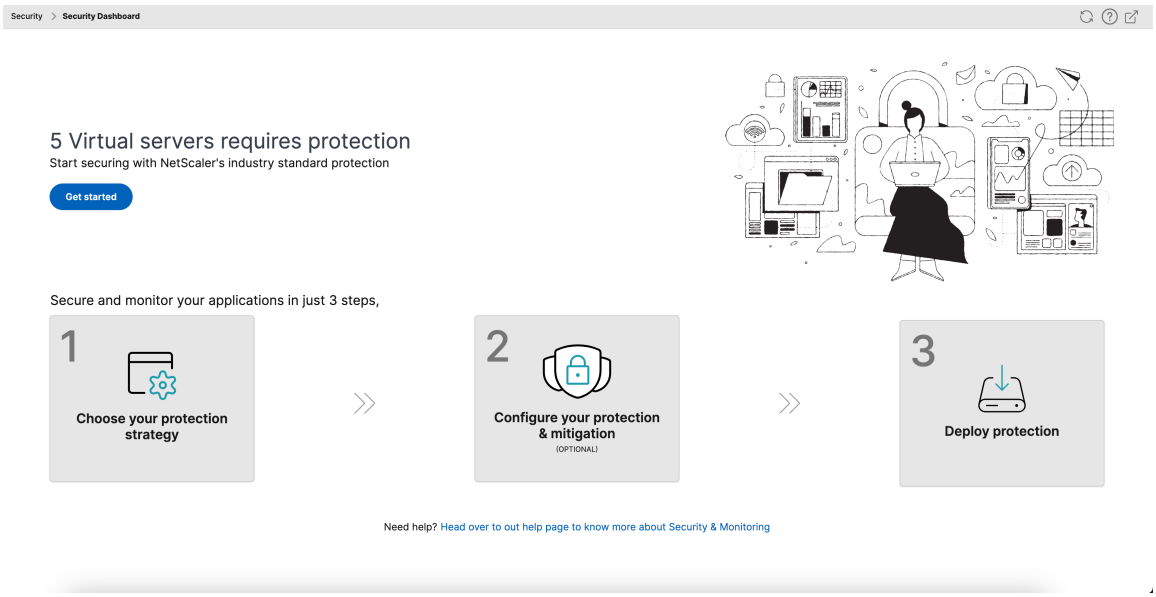
Unified Security dashboard

January 19, 2024

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**.
- The eligible virtual server types for configuring protections are load balancing and content

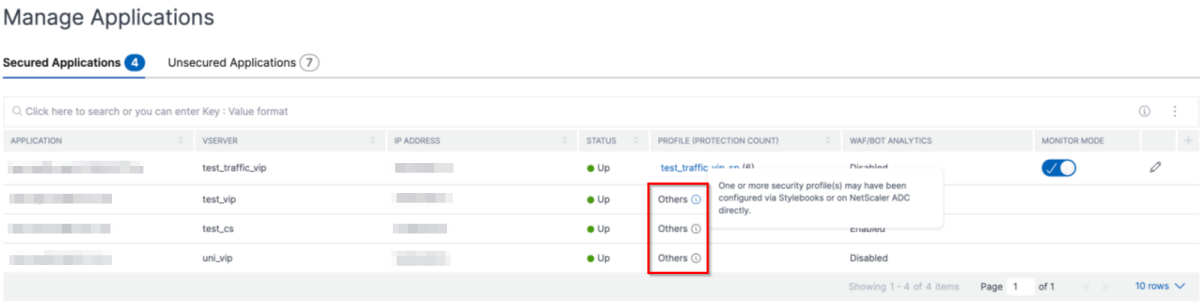
© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 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.

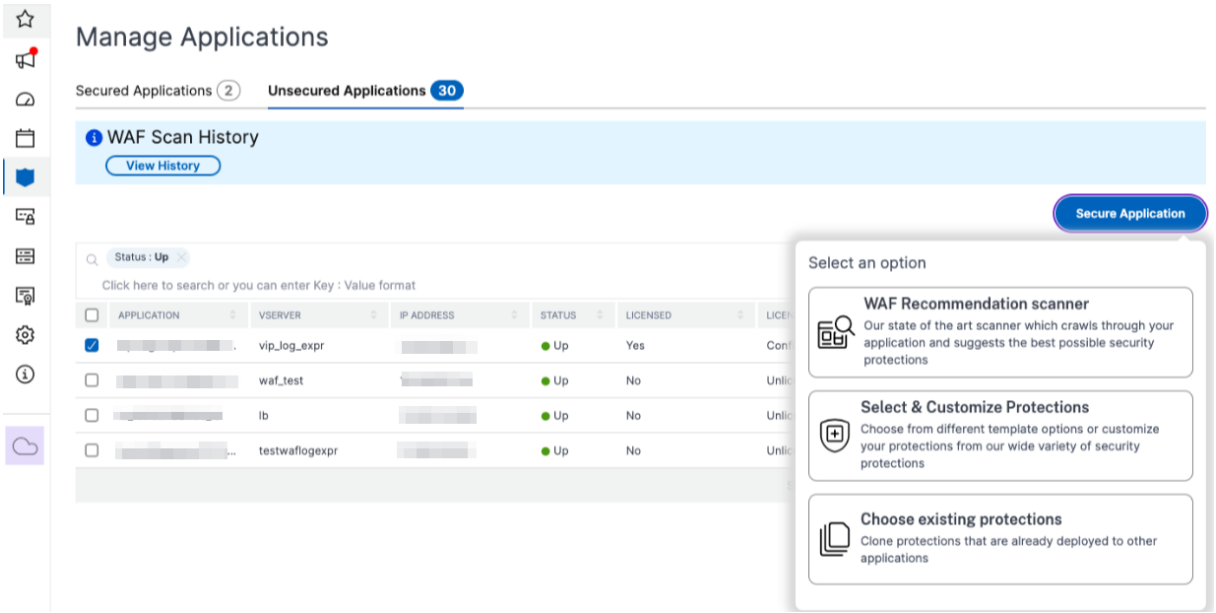
If you have already configured protections directly on the NetScaler instances or through StyleBooks, you can view the applications in the **Secured Applications** tab marked as **Others** under **Profile**.



Configure protections for unsecured applications

> **Note:**
>
> The maximum supported configuration entities (rules) in Block list is 32.

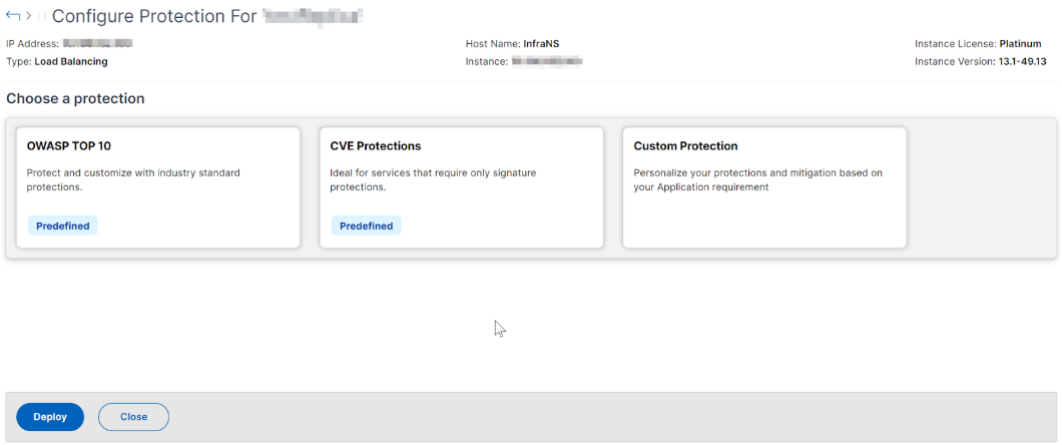
In the **Unsecured Applications** tab, select an application, and click **Secure Application**.



You can select either of the following options to protect your application:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 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.
    - **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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

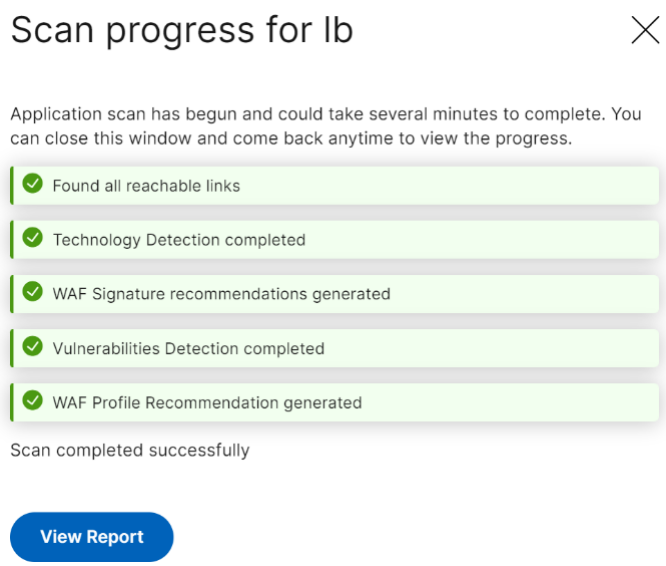
pairs, where **Field Name** is the Key and **Field Value** is the Value. Ensure that all form fields needed for login to work are added correctly, including passwords. The values are encrypted before storing it in the database. You can click **Add** to add multiple form fields. For example, **Field Name** –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**:

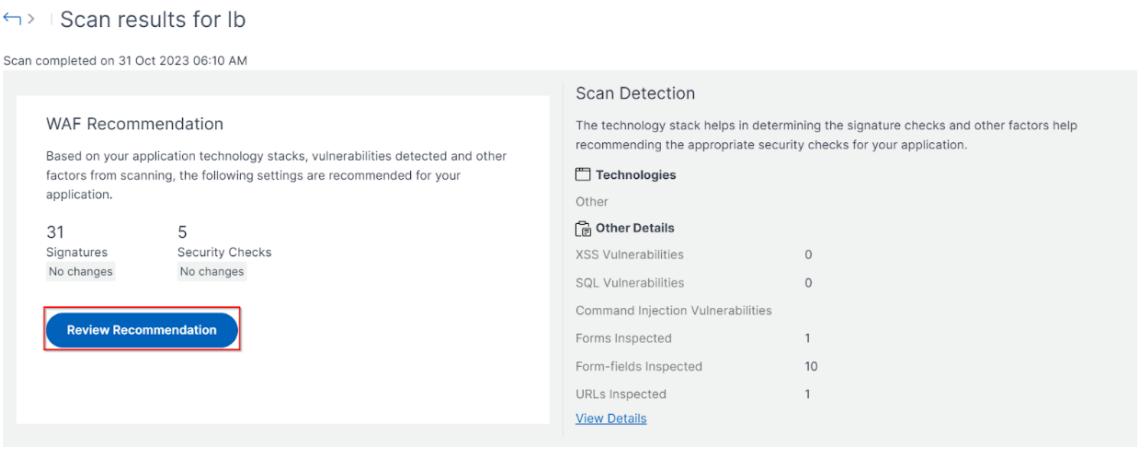
   - **Vulnerabilities to check** –Select the vulnerabilities for the scanner to detect them. Currently, this is done for SQL Injection and Cross-site scripting violations. By default, all the violations are selected. After selecting the vulnerabilities, it simulates these attacks on the application to 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.
   - **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**.

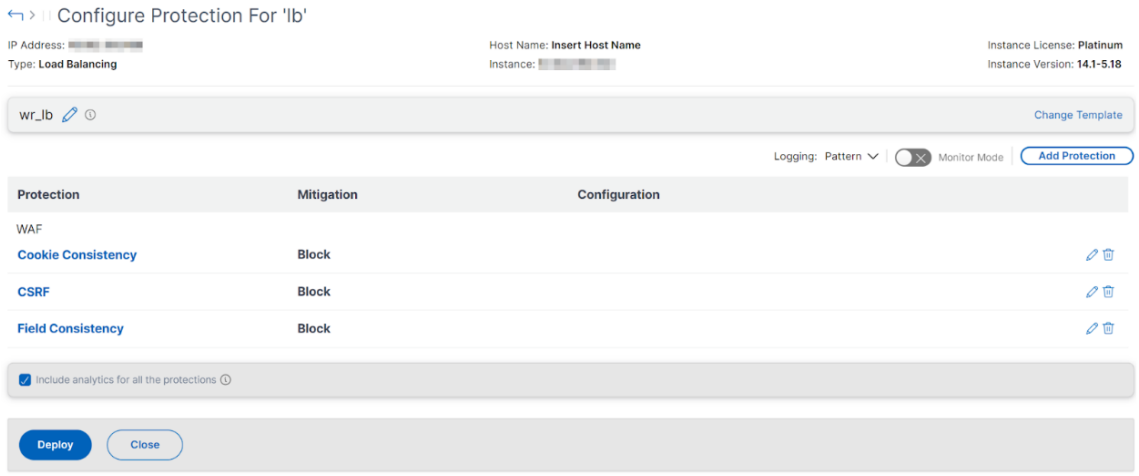


4. In the scan results page, click **Review Recommendation**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



5. Review the protections or edit/add any other protections, and click **Deploy**.



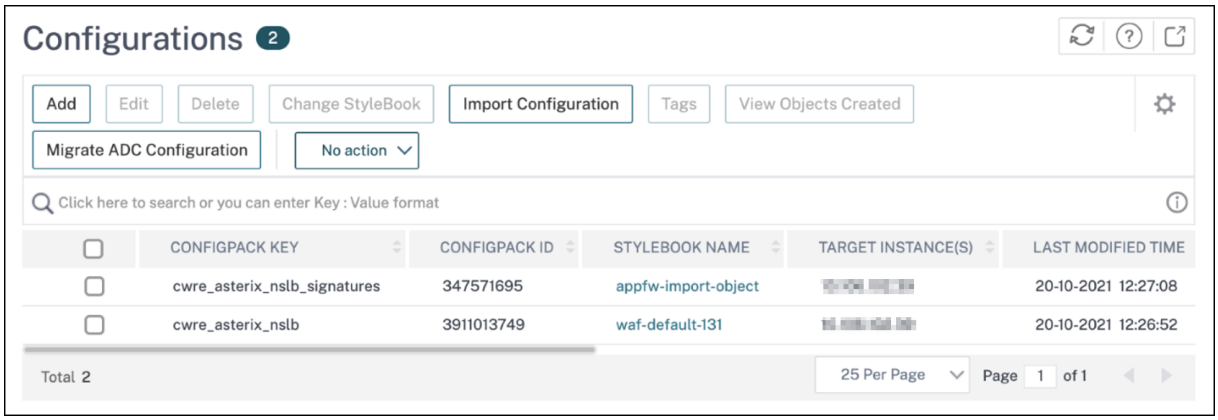
When you apply security checks successfully:

- 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.

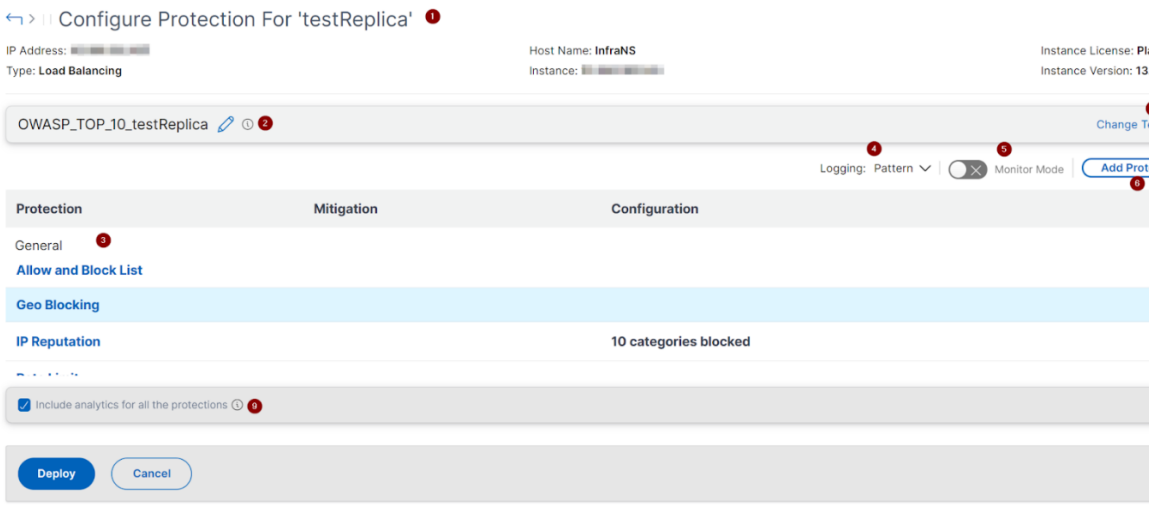
© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **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.
- **Pattern payload**. Logs violation pattern and 150 bytes of extra JSON payload.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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.

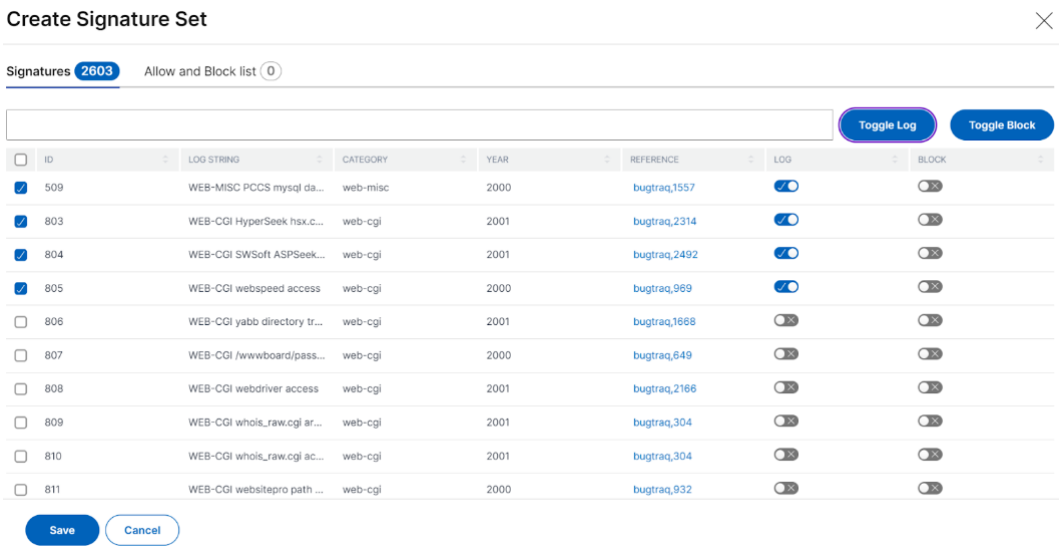
7 - Allows you to choose a new template by using the Change Template option.

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**.

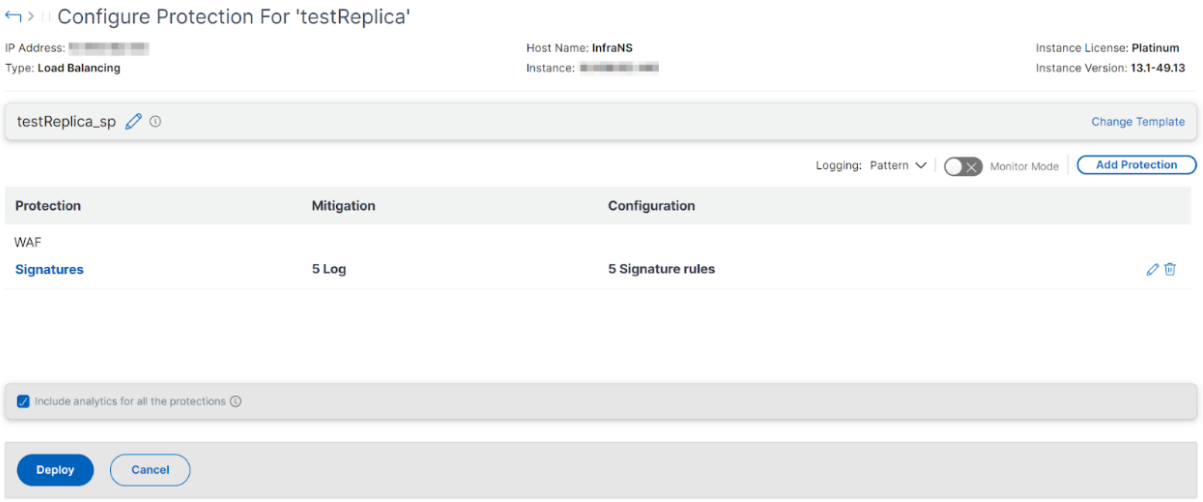
After you configure the protections, click **Deploy**.

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**.



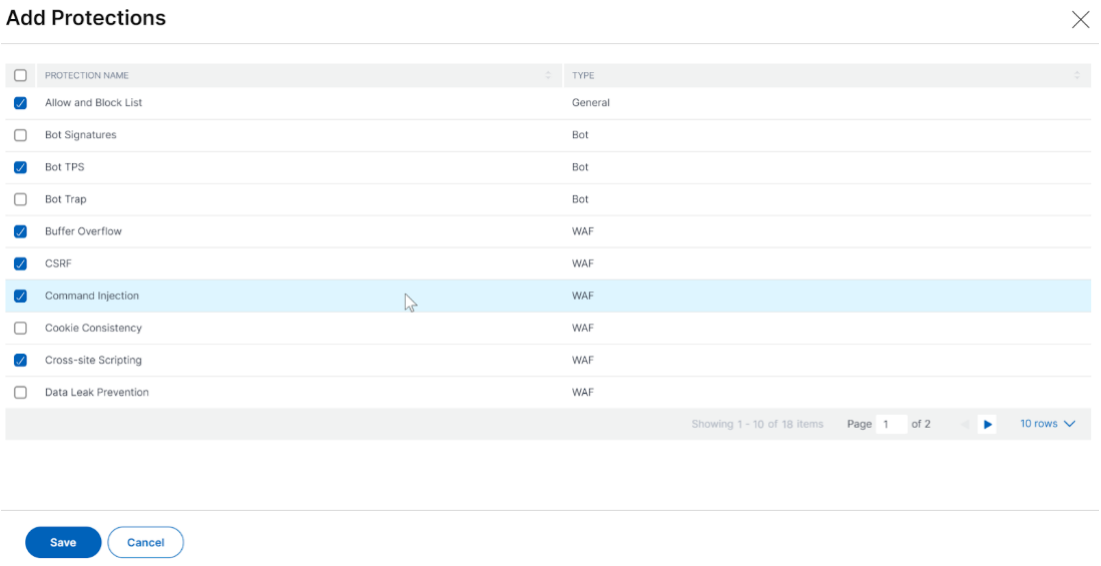
After you click **Save**, you can view the signatures added to the configuration page.

© 1997–2025 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**.

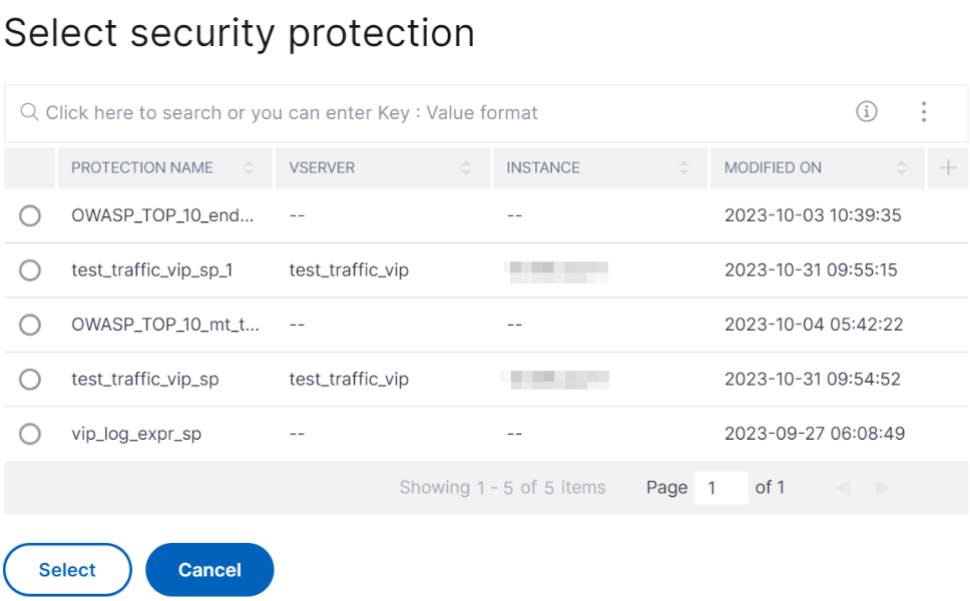


After you click **Save**, review the selected protections in the configuration page, and then click **Deploy**.

Choose existing protections

To deploy existing protections from one application to another, select an existing protection from the list.

© 1997–2025 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

February 1, 2024

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.

© 1997–2025 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**:

  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. Select the virtual servers and click **Enable Security & Analytics**.
  4. On the **Enable Analytics** window, select **WAF Security Violations** and **Bot Security Violations**, and then click **OK**.

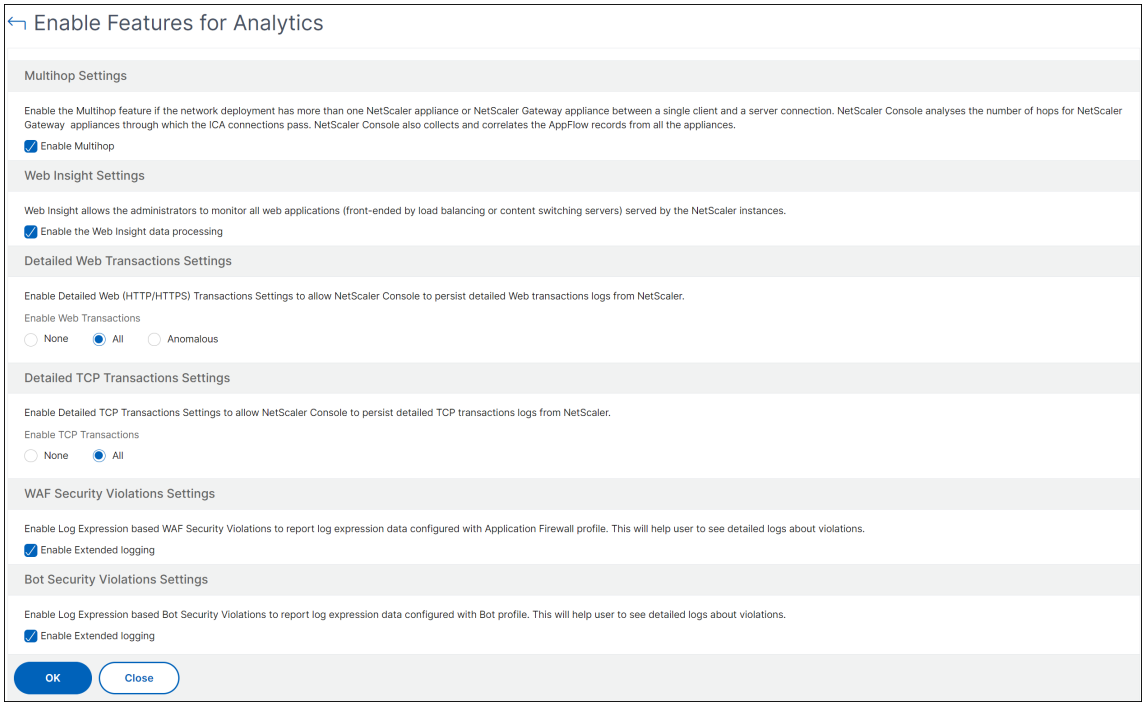
- To configure Detailed Web Transaction Settings.
- If **Metrics Collector** is enabled. For more information, see Configure Intelligent App Analytics.

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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



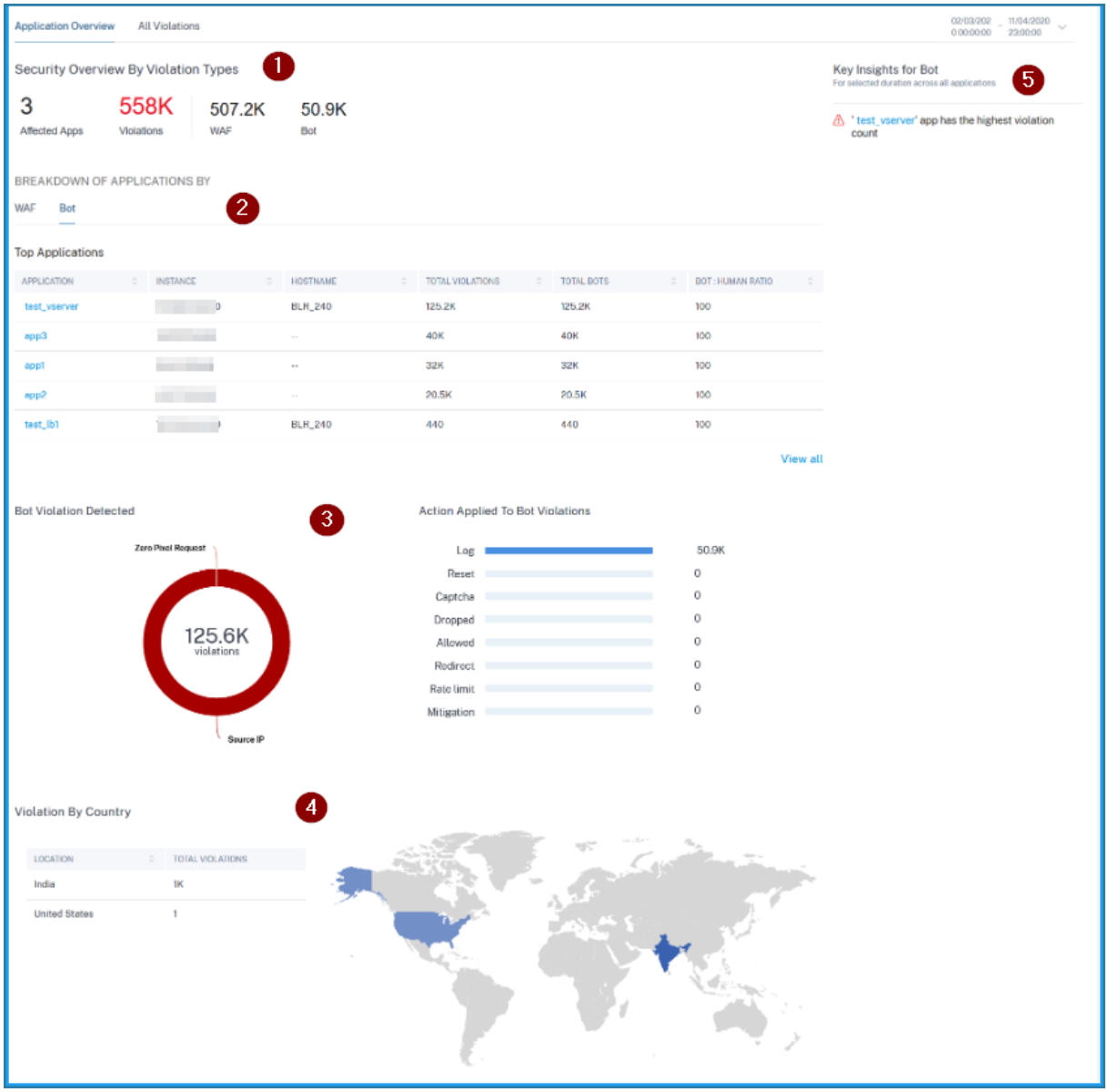
4. Click **Ok**.

Application overview

January 30, 2024

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.

© 1997–2025 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Violation categories

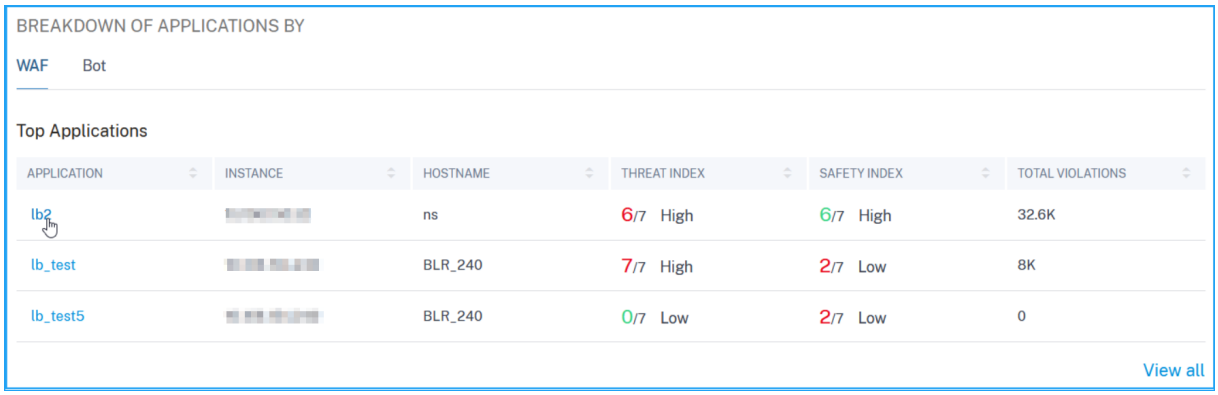
WAF	Bot
Cookie Hijack	Scraper
Infer Content Type XML	Screenshot Creator
Buffer Overflow	Search Engine
Content Type	Service Agent
Cookie Consistency	Site Monitor
CSRF Form Tagging	Speed Tester
Deny URL	Uncategorized
Form Field Consistency	Virus Scanner
Field Formats	Vulnerability Scanner
Maximum Uploads	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)
XML SOAP Fault	Zero Pixel Request
XML Validation	Source IP
Others	Host
IP Reputation	Crawler
HTTP DOS	Feed Fetcher
TCP Small Window	Link Checker

© 1997–2025 Citrix Systems, Inc. All rights reserved.

WAF	Bot
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.

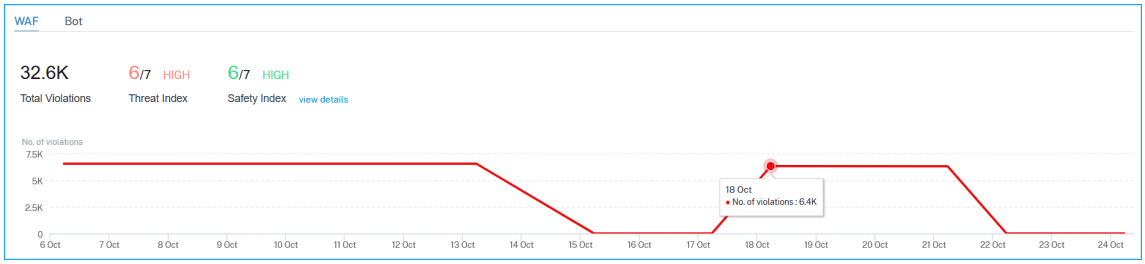


> **Note:**
>
> If you select a custom app, you can view the consolidated applications details in the **Security Overview** page. From the list, select an application to view details for the selected application.

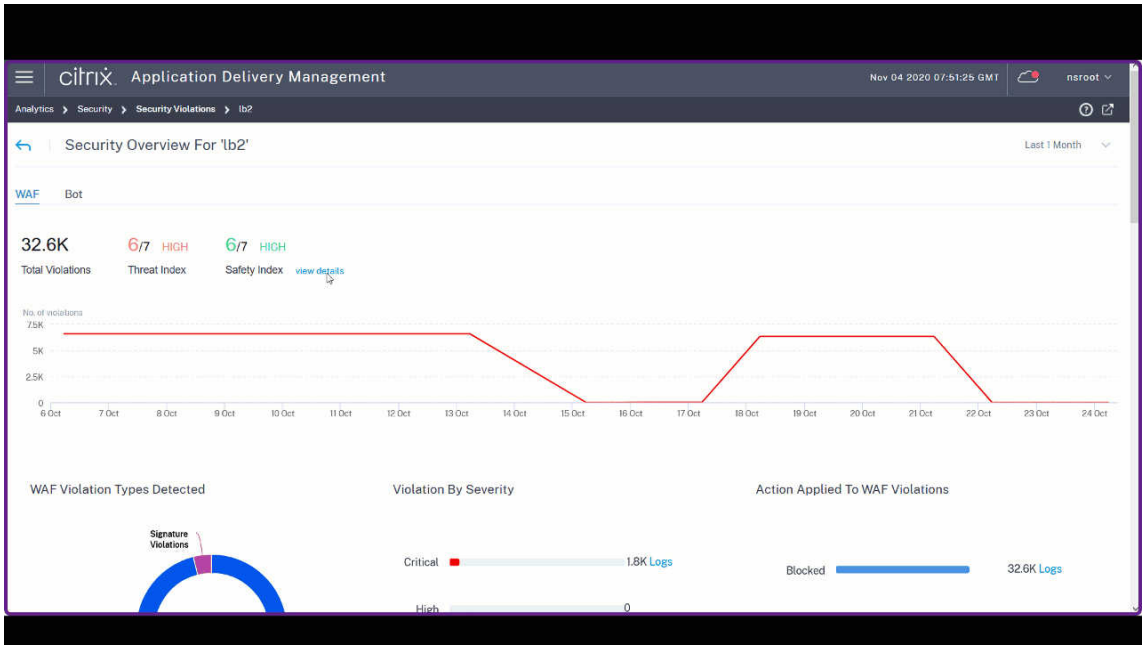
The **Security Overview** page for the selected application is displayed. Under **WAF**, you can view:

- A graph view that indicates the total violations, threat index score, safety index score for the application.

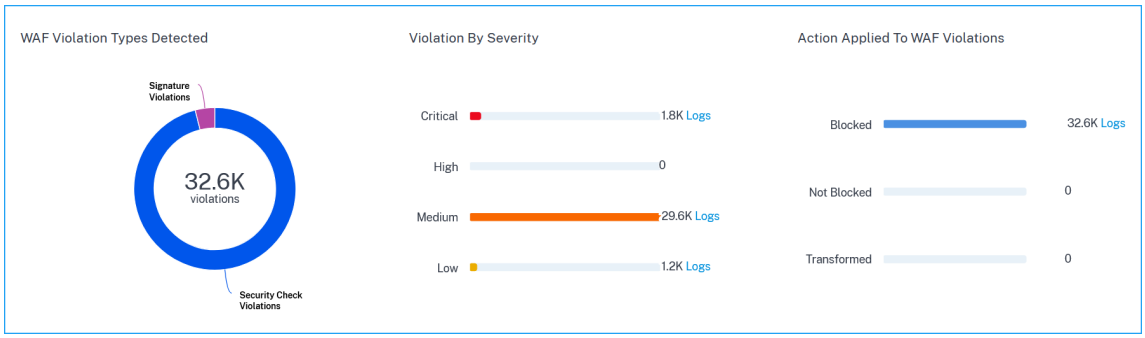
© 1997–2025 Citrix Systems, Inc. All rights reserved.



Click **View Details** to see the Application Firewall and NetScaler System Security configuration details.

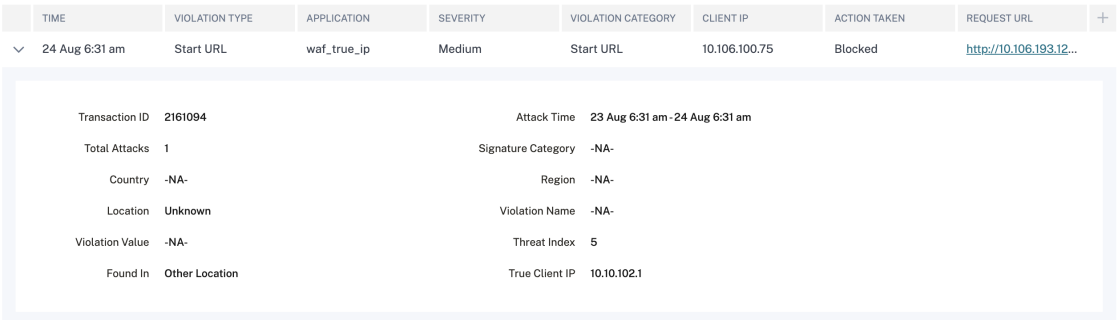


- The violations based on types, severity, and actions applied.



Click **Logs** to view details based on the severity or action taken. You can also view the client IP address.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.

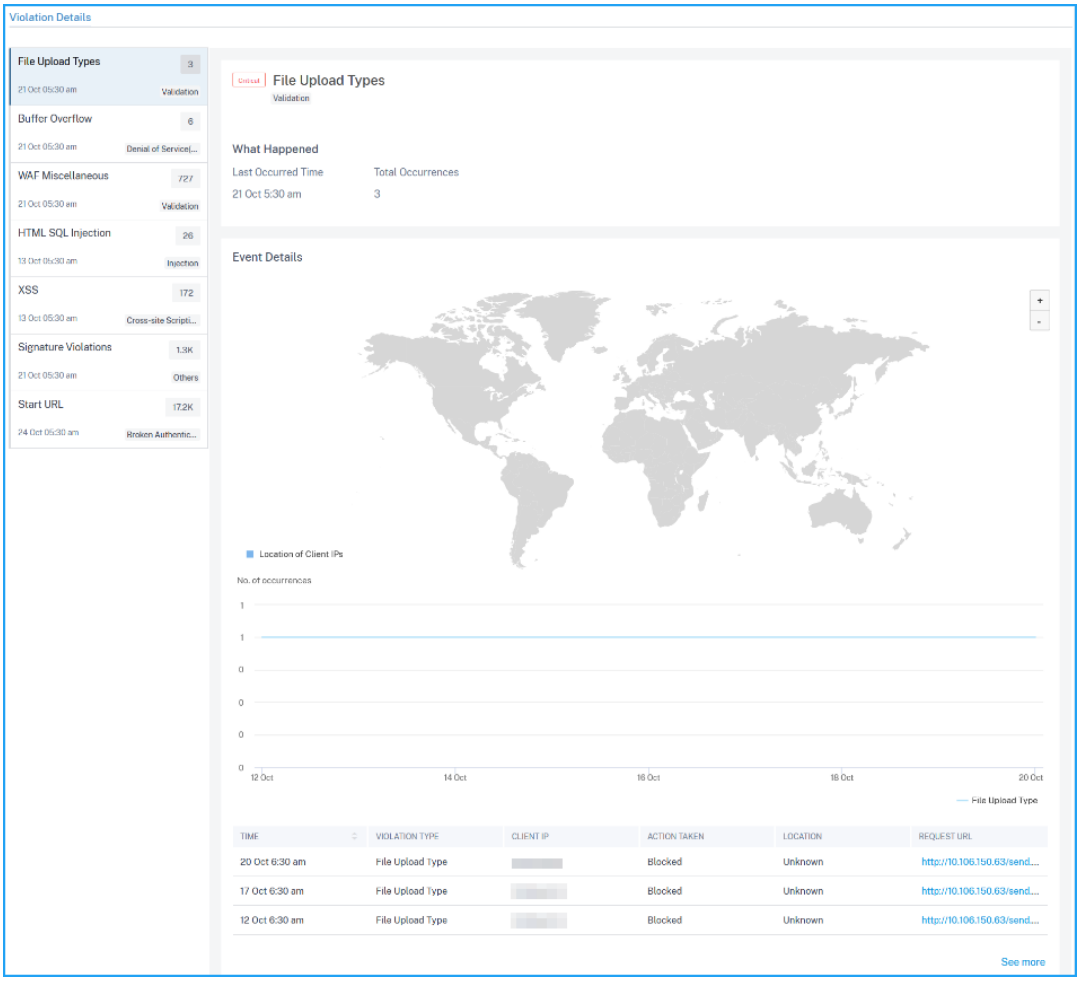
- The violations affected on the application. Under **Violation Details**, you can view the affected violation details.

  > **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:

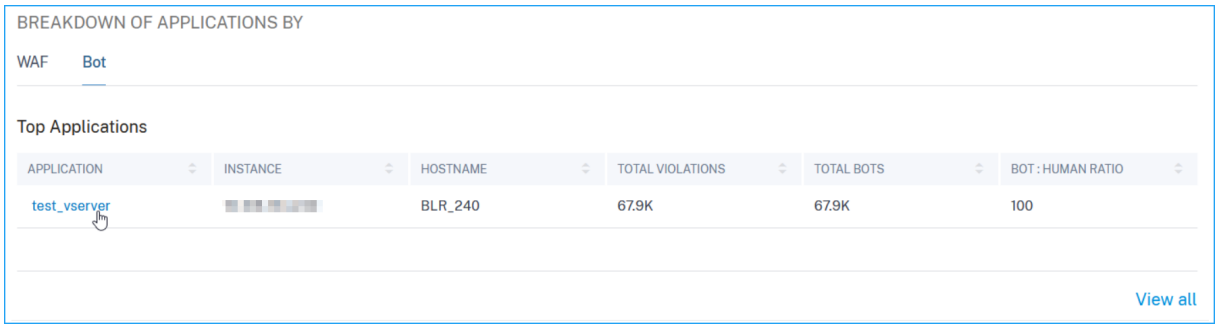
  - **What Happened** –Indicates the total occurrences and the last occurred date and time.
  - **Event Details** –Displays a geo map that indicates the client IP and other violation details such as violation type, client IP, location, and so on.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.



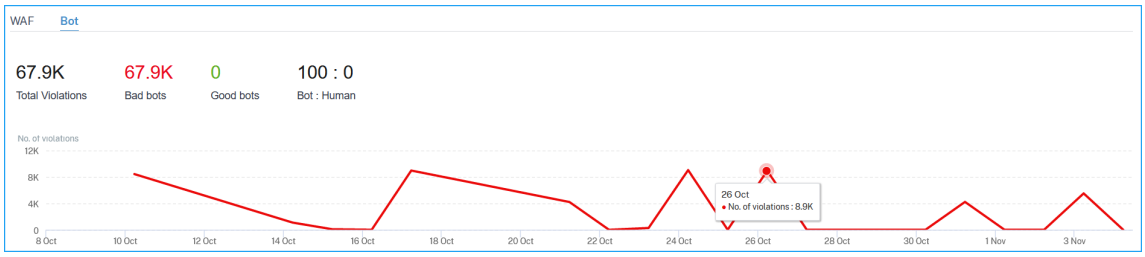
Note

© 1997–2025 Citrix Systems, Inc. All rights reserved.

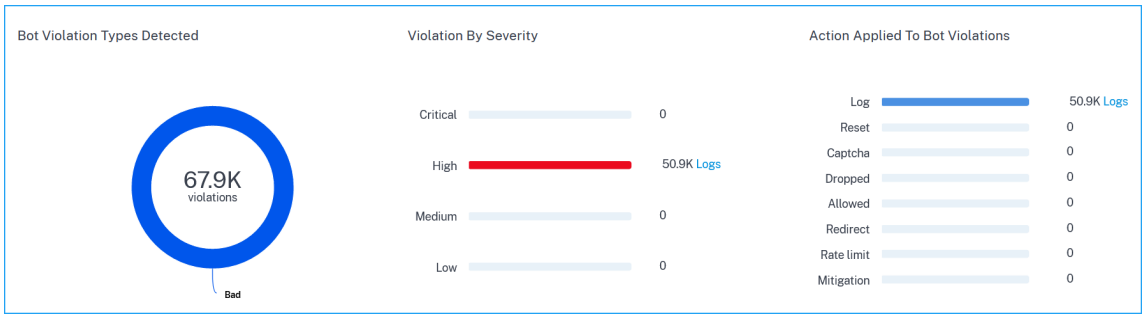
> If you select a custom app, you can view the consolidated applications details in the **Security Overview** page. From the list, select an application to view details for the selected application.

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.

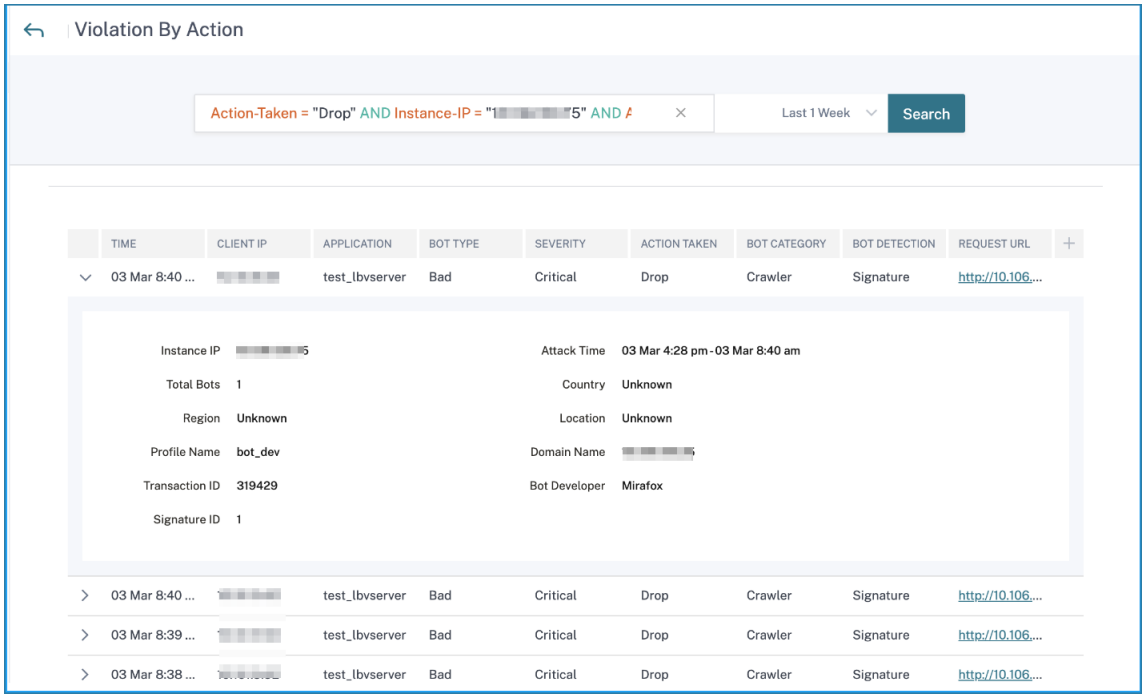


- The violations based on the bot types, severity, and actions applied.



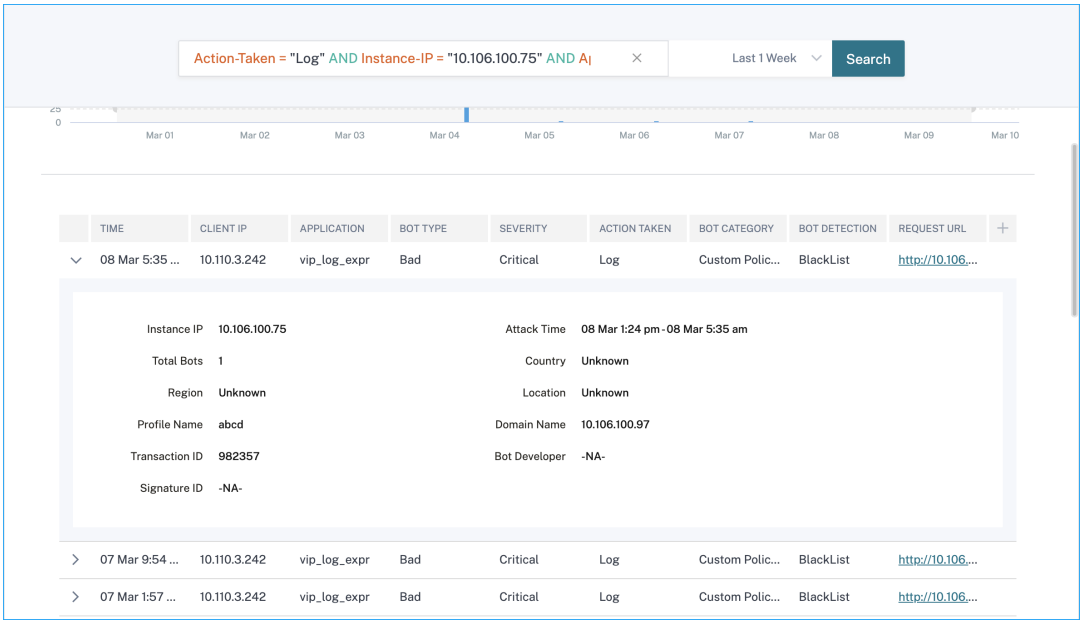
Click **Logs** to view details based on severity or actions taken. If a detected bot is a Signature type bot, you can view more details such as Bot developer and Signature ID. The Signature ID enables you to identify if the detected bot is a good bot or a bad bot.

© 1997–2025 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.

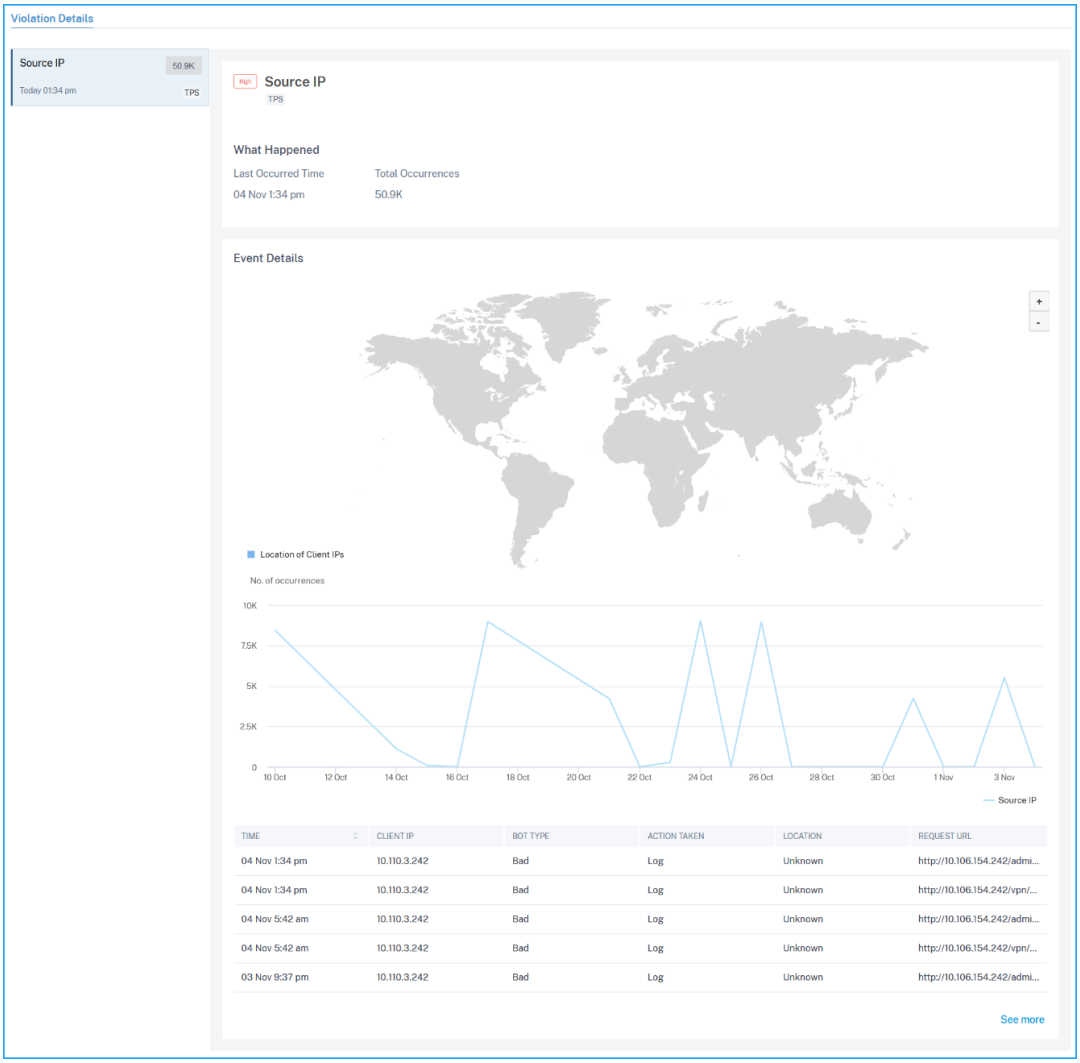
- The violations affected on the application. Under **Violation Details**, you can view the affected violation details.

© 1997–2025 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:

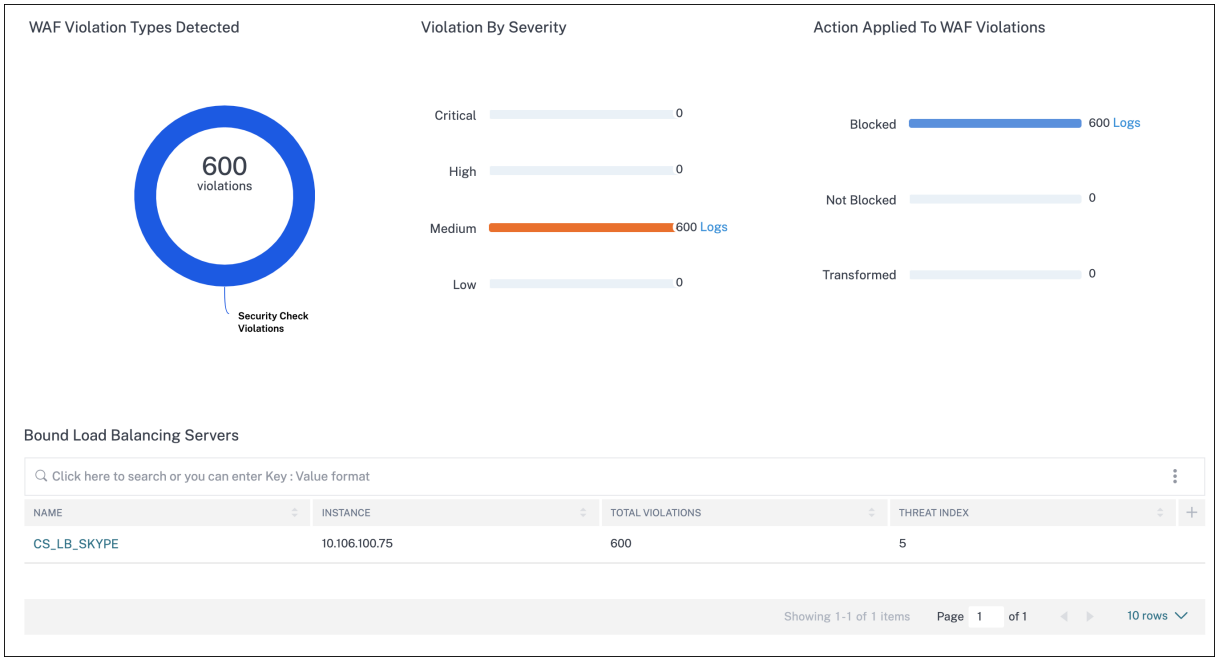
- **What Happened** –Indicates the total occurrences and the last occurred date and time.
- **Event Details** –Displays a geo map that indicates the client IP and other violation details such as violation type, client IP, location, and so on.



> **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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> switching virtual server.



View events history

You can view the signature updates in **Events**, when:

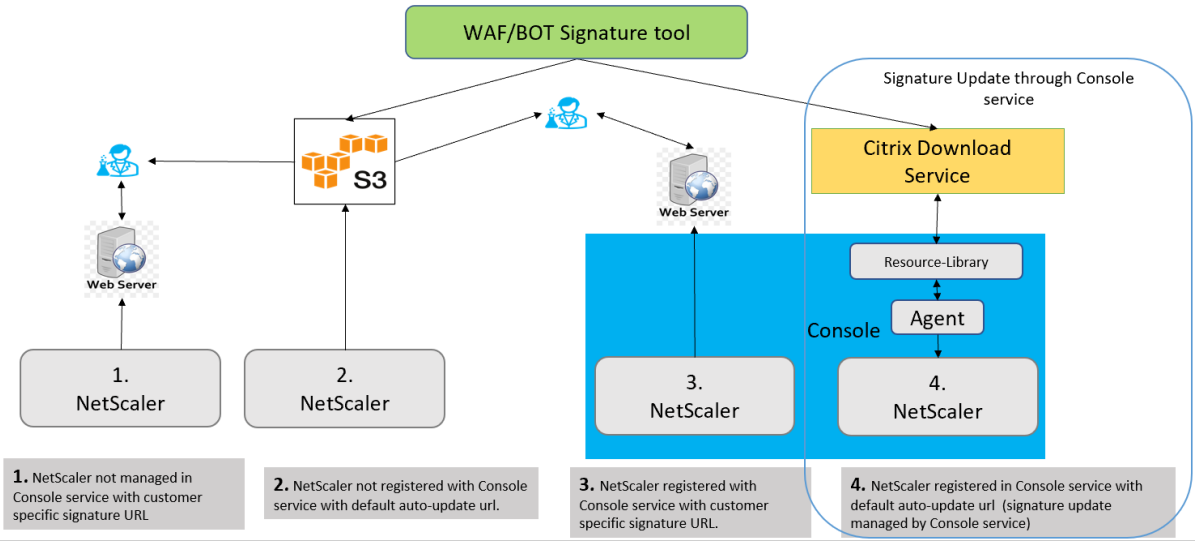
- New signatures are added in NetScaler instances.
- Existing signatures are updated in NetScaler instances.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



All Violations

February 27, 2024

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Network	WAF	Bot
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
		Cross-site scripting
		XML DoS
		XML Format
		XML WSI
		XML SSL
		XML Attachment
		XML SOAP Fault
		XML Validation
		Others
		IP Reputation
		HTTP DOS
		TCP Small Window
		Signature Violation
		File Upload Type
		JSON cross-site scripting
		JSON SQL
		JSON DOS
		Command Injection
	Cookie Hijack	Feed Fetcher
	Block Keyword	Link Checker
	JSON Block Keyword	Marketing
		Safe Commerce
		Safe Object

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Network	WAF	Bot
		HTML SQL Inject Start URL
	Command Injection Grammar JSON SQL Injection Grammar	

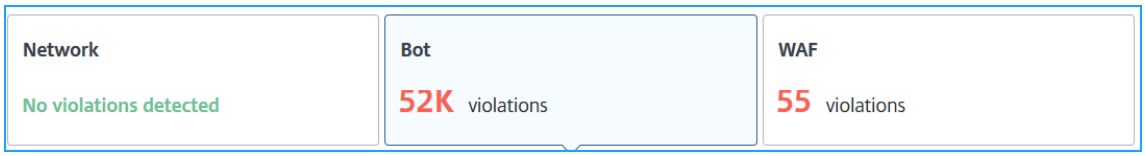
Security violations dashboard

In the security violations dashboard, you can view:

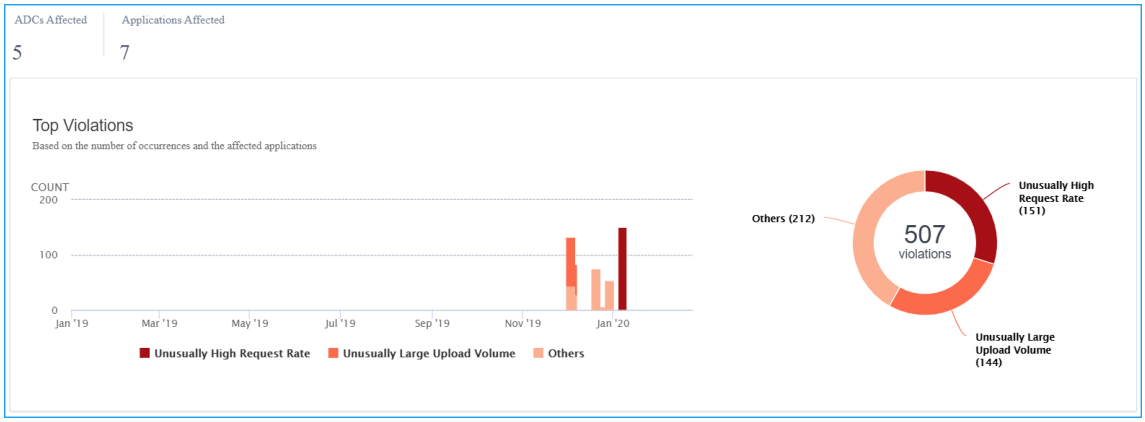
- Total violations occurred across all NetScaler instances and applications. The total violations are displayed based on the selected time duration.



- Total violations under each category.



- Total NetScaler instances affected, total applications affected, and top violations based on the total occurrences and the affected applications.



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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

API Security

January 8, 2024

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.

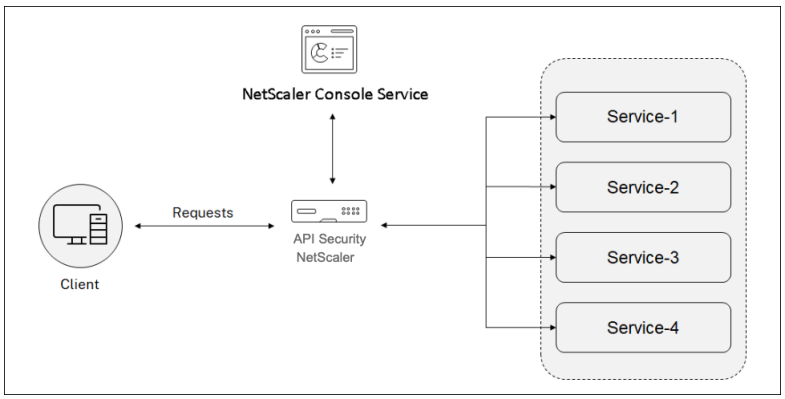
In API security, a gateway acts as the entry point for all requests to your API endpoints. And, ensures secure and reliable access to all API endpoints and microservices in your system.

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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



> **Note:**
>
> In NetScaler Console, this feature is available for the users who have Premium or Advanced 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.

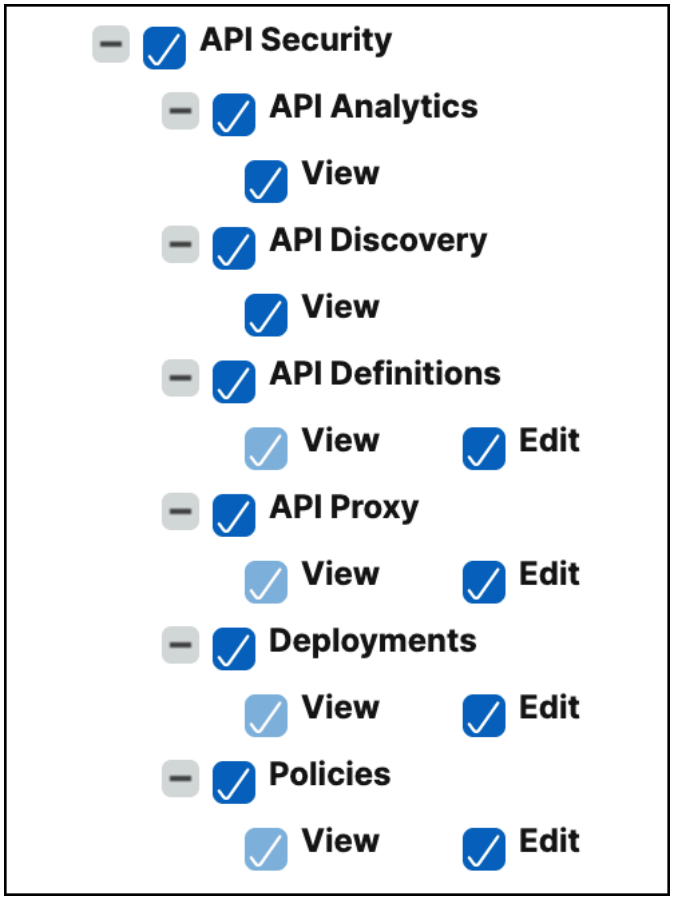
Grant API Security configuration and management permissions

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.
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
- IPAM
- Load Balancing (Under **Network Functions**)

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Content Switching (Under **Network Functions**)
- Device API Proxy (Under **API**)

For more information about access policies, see Configure access policies on NetScaler Console.

WAF learning

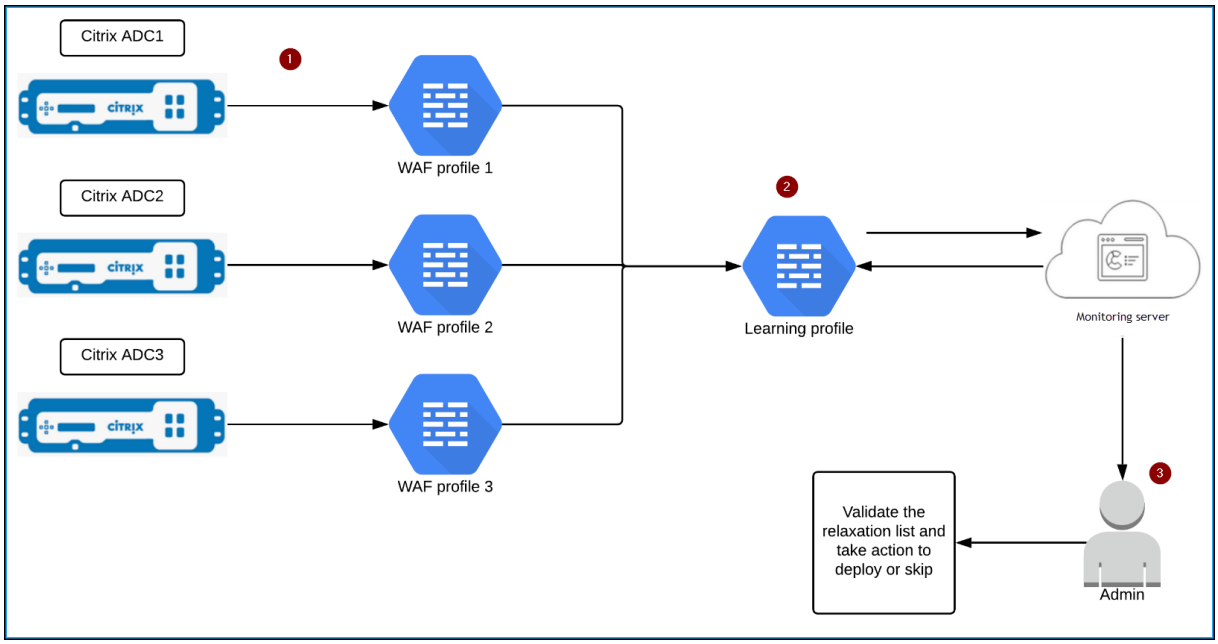
January 8, 2024

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.

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Note**
>
> For the HTML SQL Injection check, you must configure `set -sqlinjectionTransformSpecia 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

  > **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

January 8, 2024

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

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

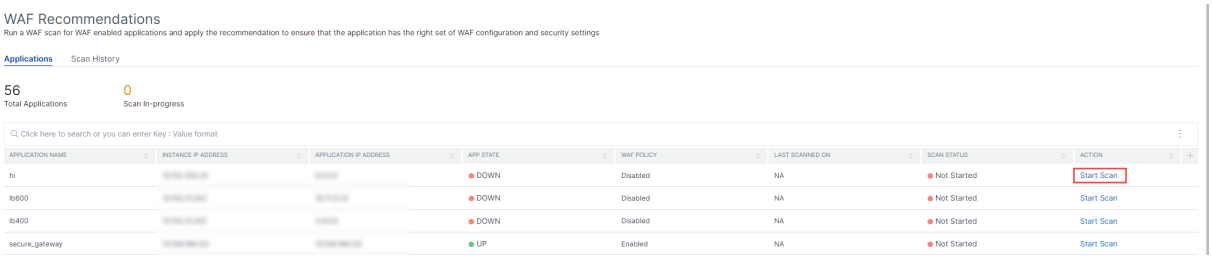
The applications:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Must have the premium license.
- Must be the load balancing virtual server.

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.

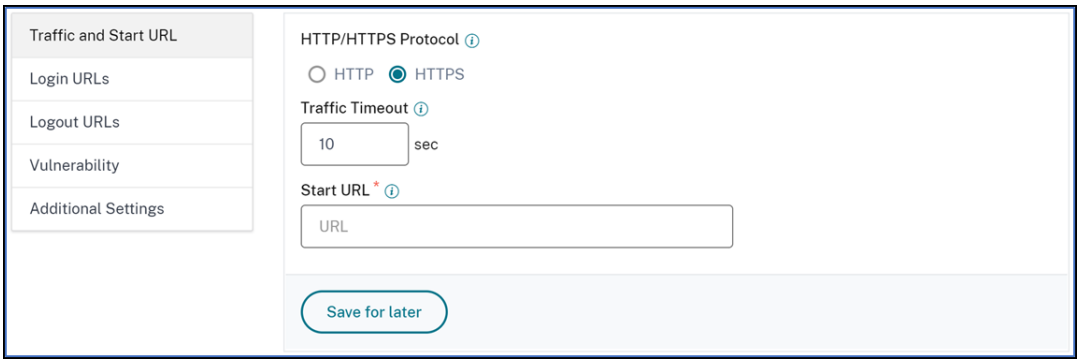


In the WAF Recommendations page:

- **Domain Name** –Specify the publicly accessible/publicly reachable domain name that is associated with the application VIP. For example: `www.example.com`.

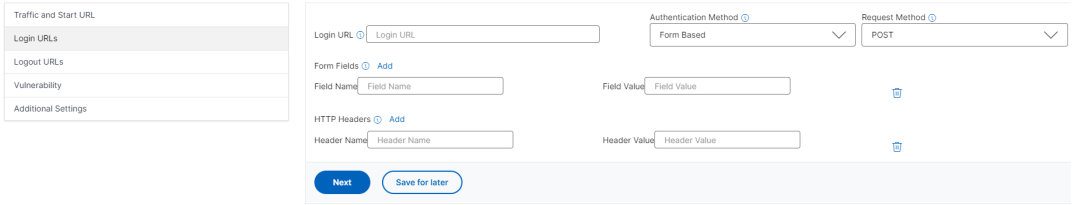
  > Note
  >
  > Start URL, Login URL and Logout URL must match the specified domain.

- **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.



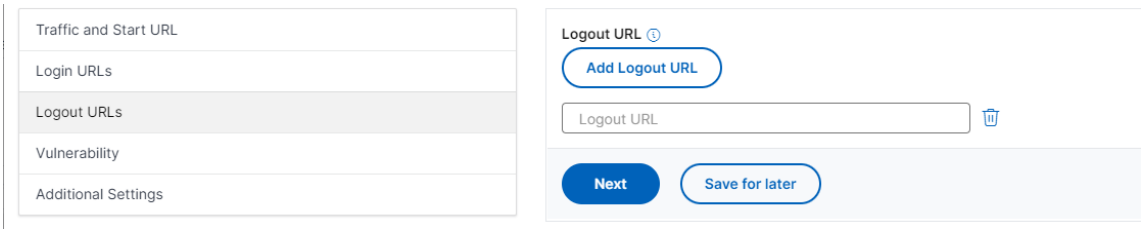
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Login URLs** –Specify the login credentials, URLs, if any, to access the application.
  - **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.

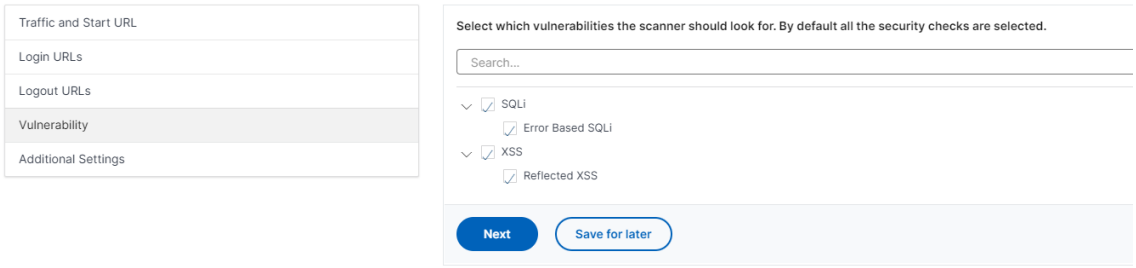


- **Logout URLs** –Specify the URL that terminates the session after accessing. For example: `https://www.example.com/customer/logout`.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

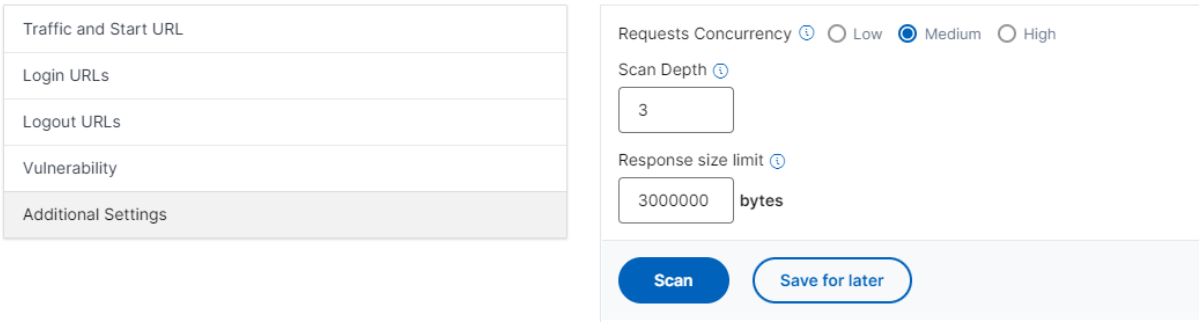


- **Vulnerability** –Select the vulnerabilities for the scanner to detect them. Currently, this is done for SQL Injection and Cross-site scripting violations. By default, all the violations are selected. After selecting the vulnerabilities, it simulates these attacks on the application to report the 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.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

WAF scan recommendation process

When you start the scan, the WAF recommendation engine:

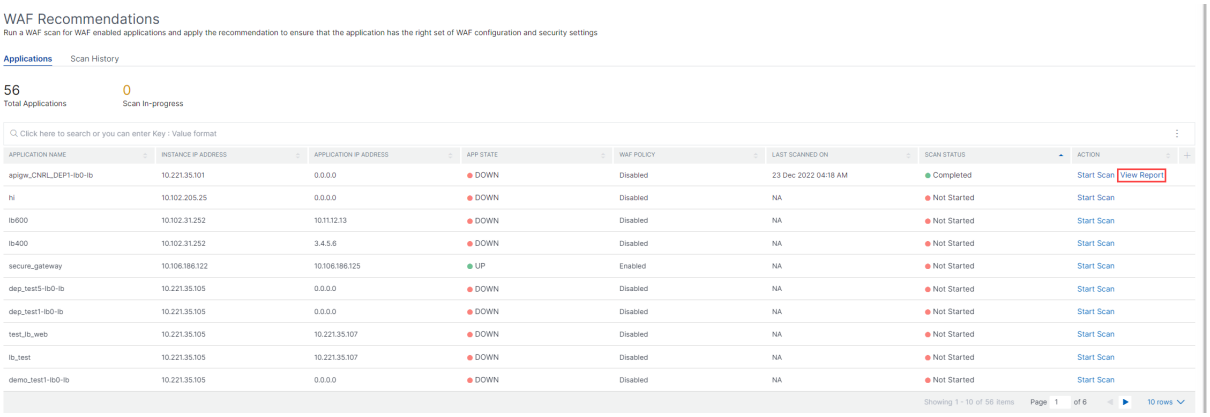
- Scans the provided web application through the provided URL.
- Inspects the web application to discover the technologies used by the web application.
- Simulates security attacks on the web application to detect potential vulnerabilities.
- Recommends signatures based on the web technologies detected.
- 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

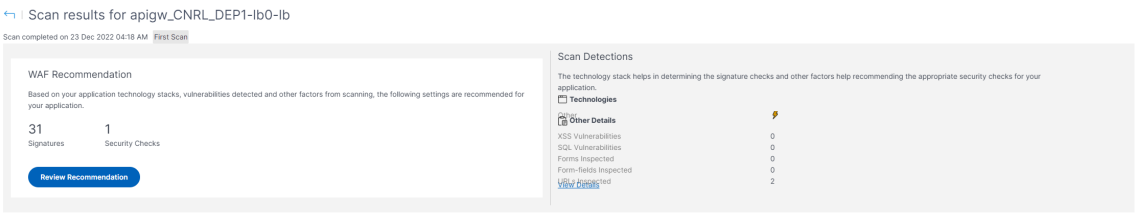
After the scan is complete, click **View Report** to view the results.



The scan result provides:

© 1997–2025 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:

- The configuration is applied on the NetScaler instance through the `appfw-import-object` StyleBook.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- The signatures file with recommendations configured is imported in the NetScaler instance.

> **Note**
>
> Signatures are supported in NetScaler 13.0 or later version.

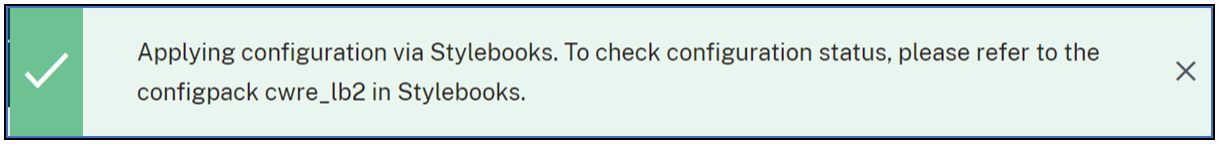
Before you proceed to apply the **Security Check** recommendations, navigate to **Applications > Configuration > Config Packs** and ensure that the signatures configpack is successfully created.

When you apply security checks successfully:

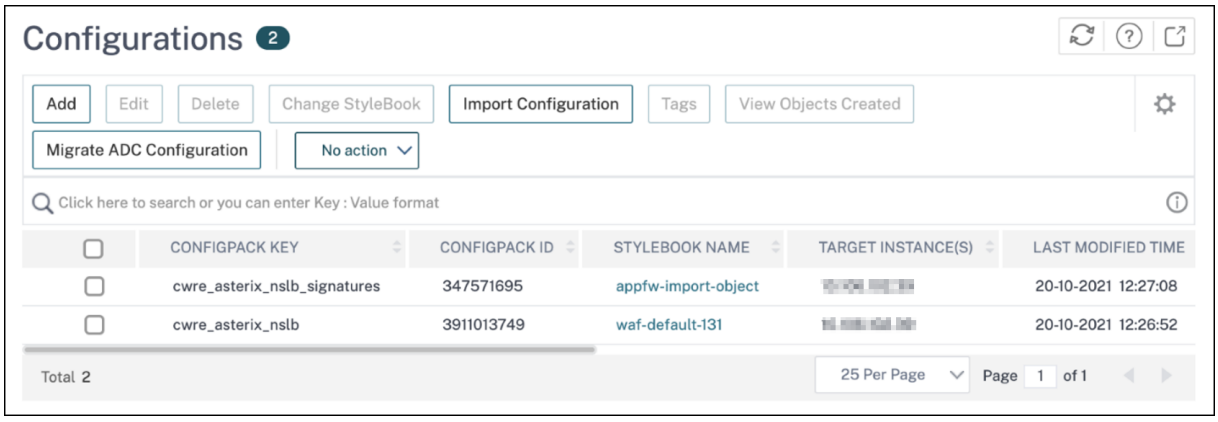
- The configuration is applied on the NetScaler instance through StyleBooks, depending upon the NetScaler version. For NetScaler 13.0, `waf-default-130` StyleBook is used and for NetScaler 13.1, `waf-default-131` stylebook is used.
- The `Appfw` profile is created on your NetScaler and bound to the application 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**.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Gateway Insight

September 8, 2025

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.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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.
  - 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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.

View Gateway Insight reports

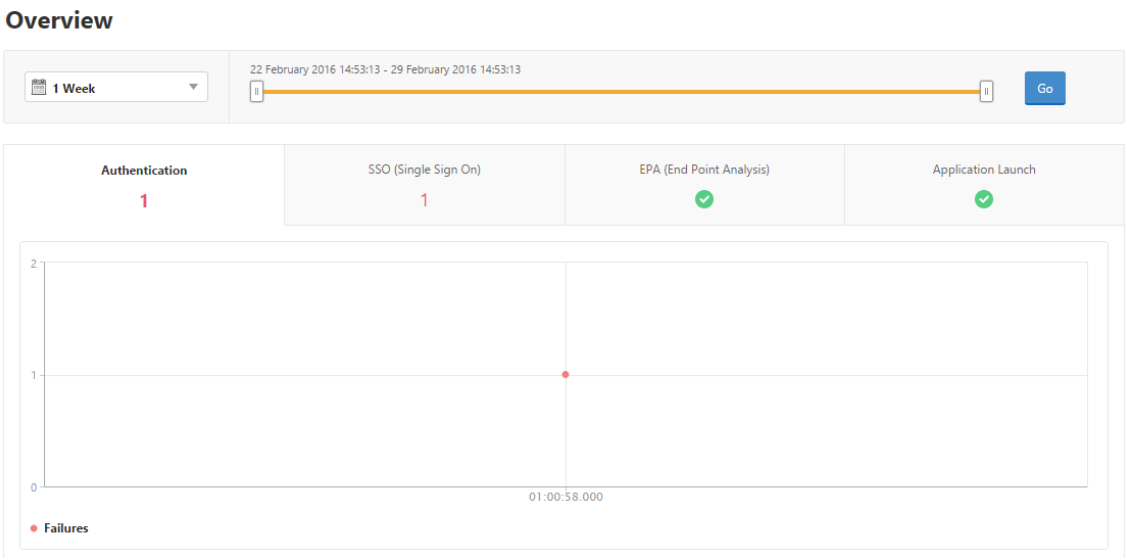
In NetScaler Console, you can view reports for all users, applications, and gateways associated with the NetScaler Gateway appliances, and you can view details for a particular user, application, or gateway. In the **Overview** section, you can view the EPA, SSO, Authentication, and Application Launch 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

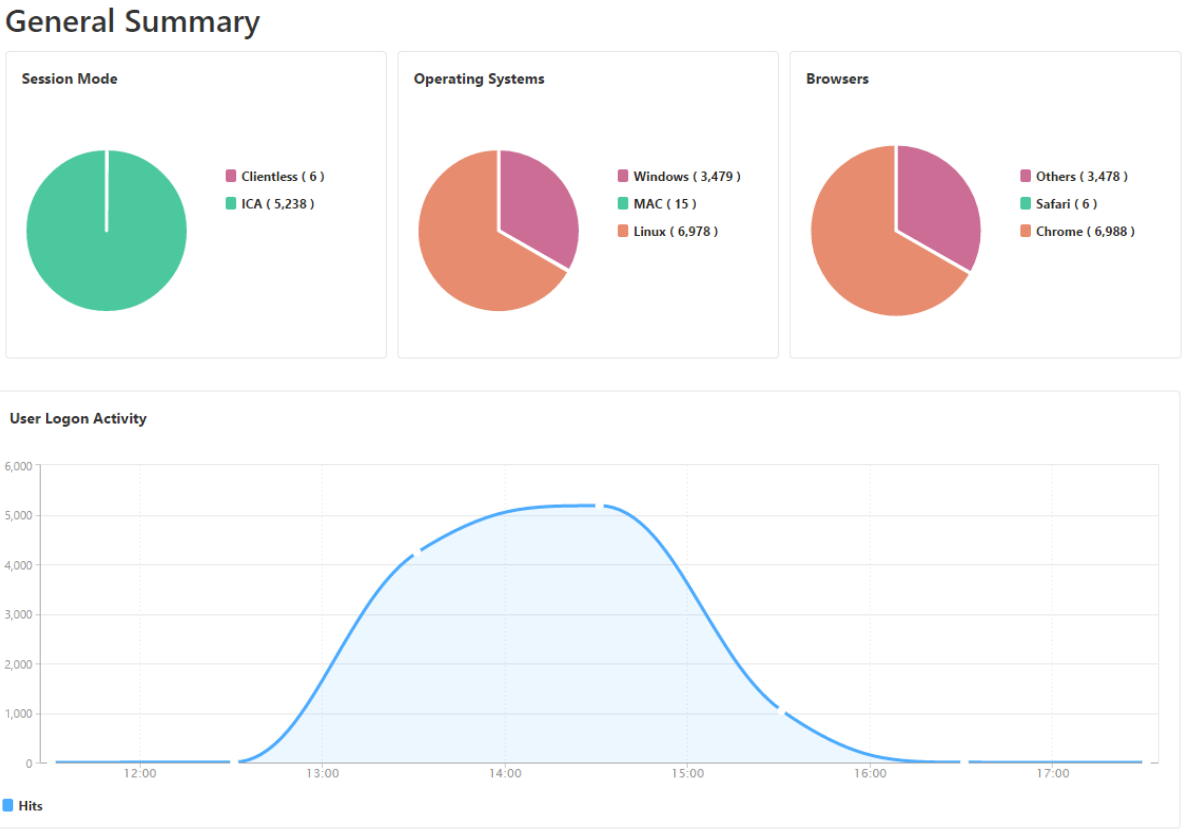
1. In NetScaler Console, navigate to **Gateway > Gateway Insight**.
2. Select the time period for which you want to view the user details. You can use the time slider to further customize the selected period. Click **Go**.
3. Click the EPA (End Point Analysis), Authentication, Authorization, SSO (Single Sign On), or Application Launch tabs to display the failure details.

© 1997–2025 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.

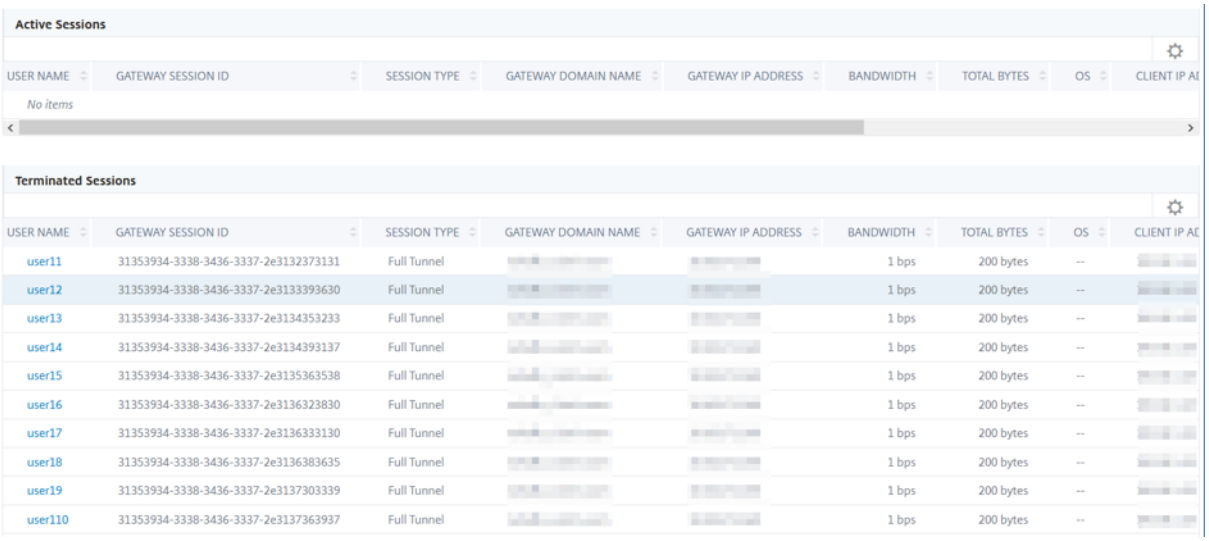


© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

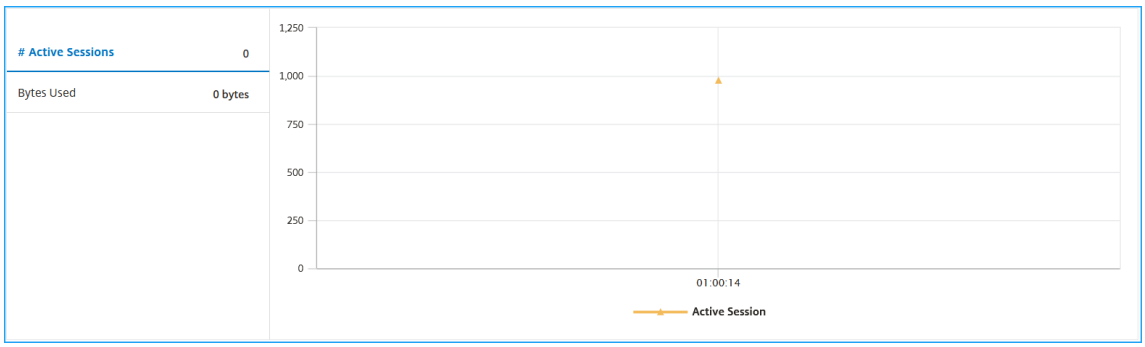


As an administrator, this view enables you to:

- 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.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

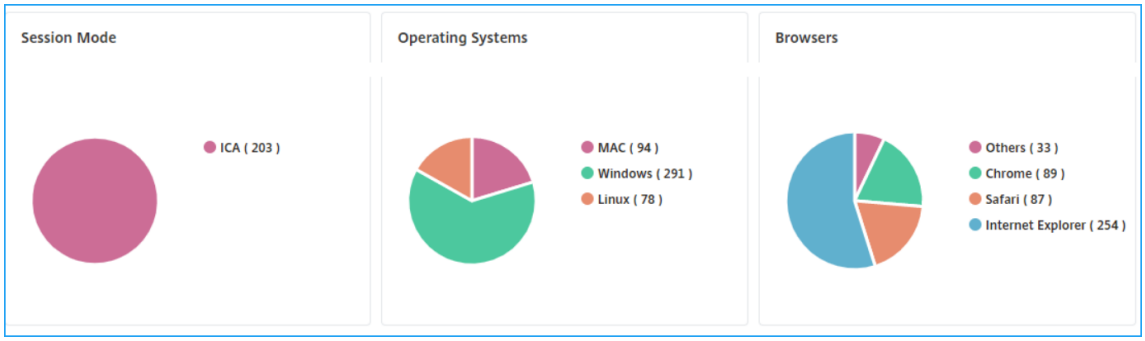
Scroll down to view a list of available users and active users.



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

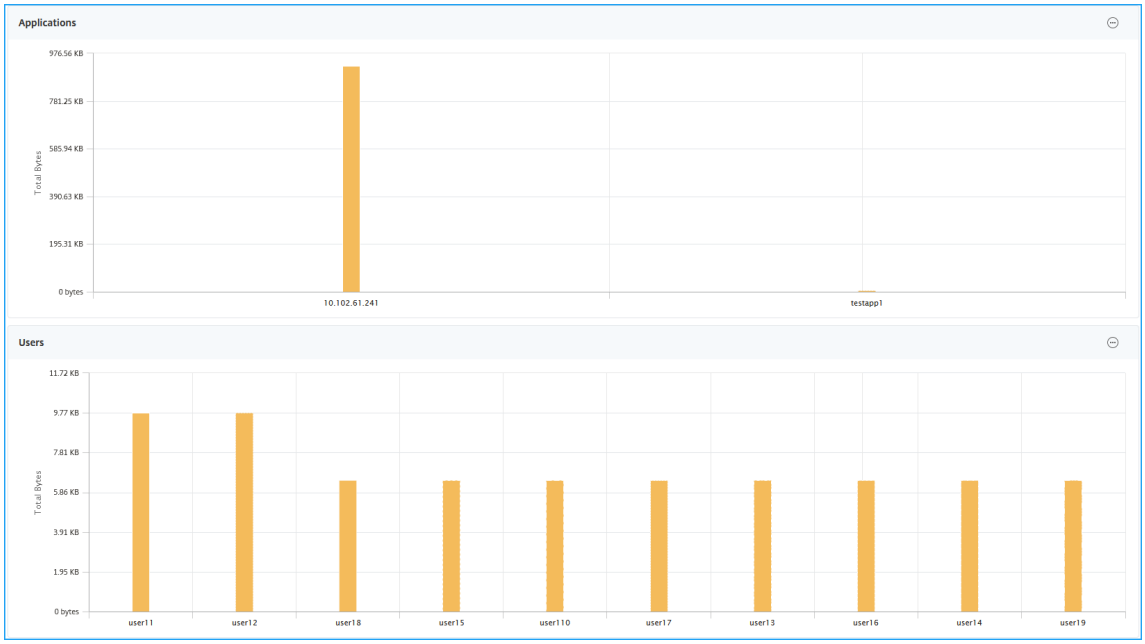
On the **Users** or **Active Users** tab, click a user to view the following user details:

- **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.

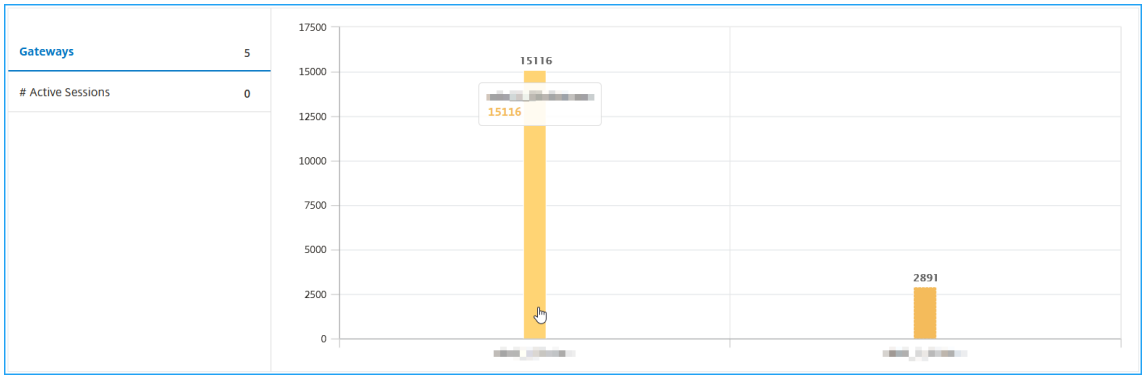


- **Users and applications for the selected gateway** - Navigate to **Gateway** > **Gateway Insight** > **Gateway** and click a gateway domain name to view the top 10 applications and top 10 users that are associated with the selected gateway.

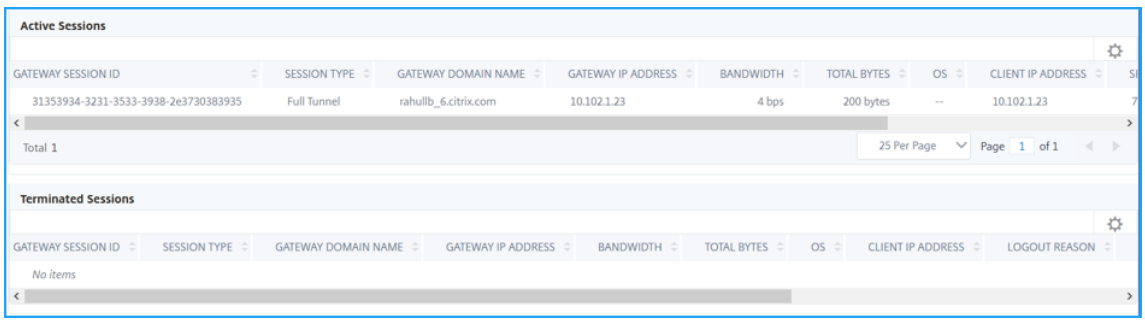
© 1997–2025 Citrix Systems, Inc. All rights reserved.



- **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.

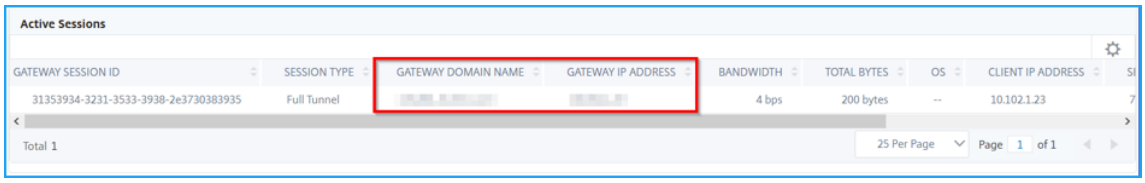


- The user **Active Sessions** and **Terminated Sessions**.

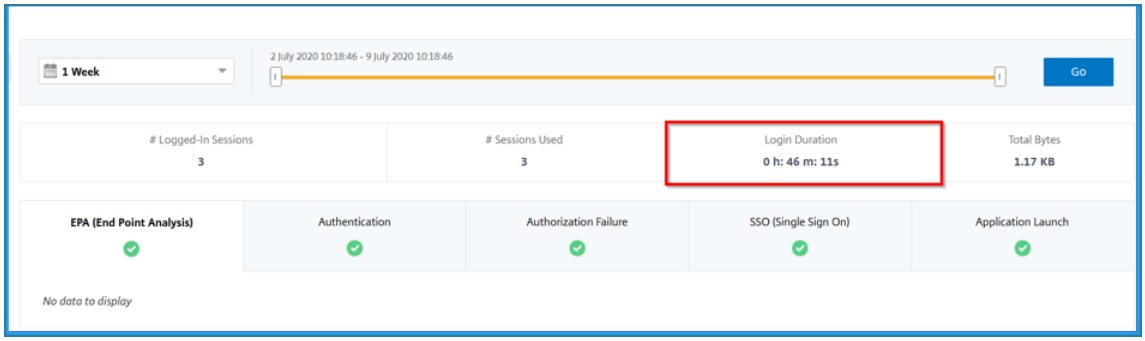


© 1997–2025 Citrix Systems, Inc. All rights reserved.

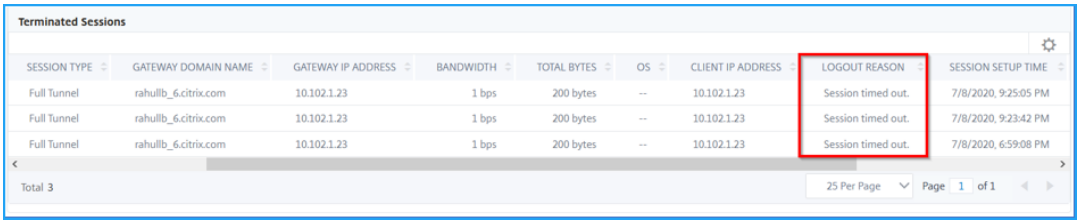
- The gateway domain name and gateway IP address in **Active Sessions**.



- 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
  - 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- 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.

    1. Navigate to **Gateway > Gateway Insight** to view the geo map
    2. 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

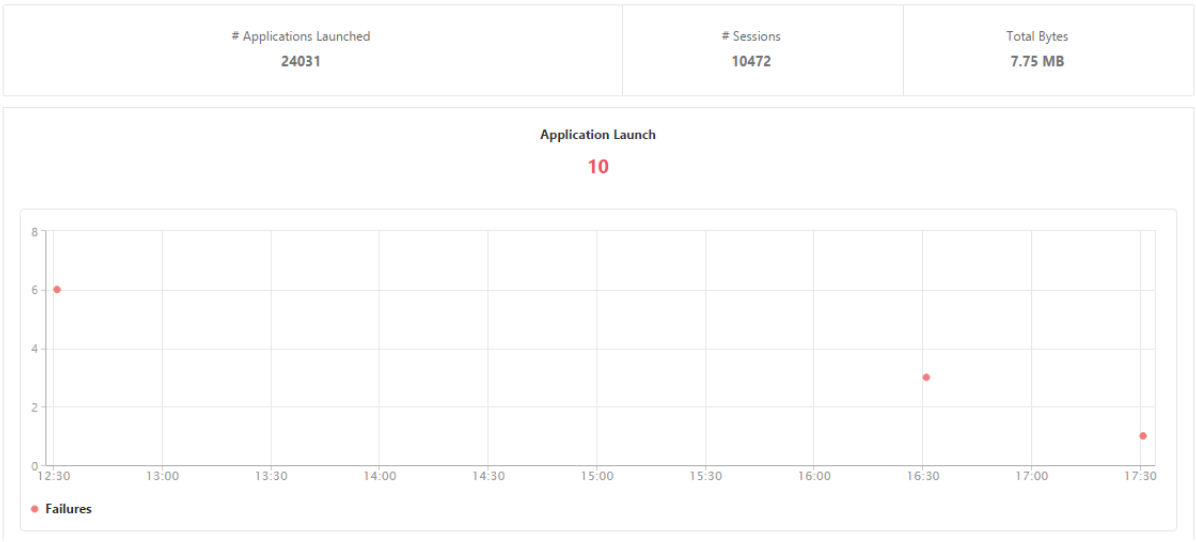
You can view the number of applications launched, number of total and active sessions, the number of total bytes and bandwidth consumed by the applications. You can view details of the users, sessions, bandwidth, and launch errors for an application.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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

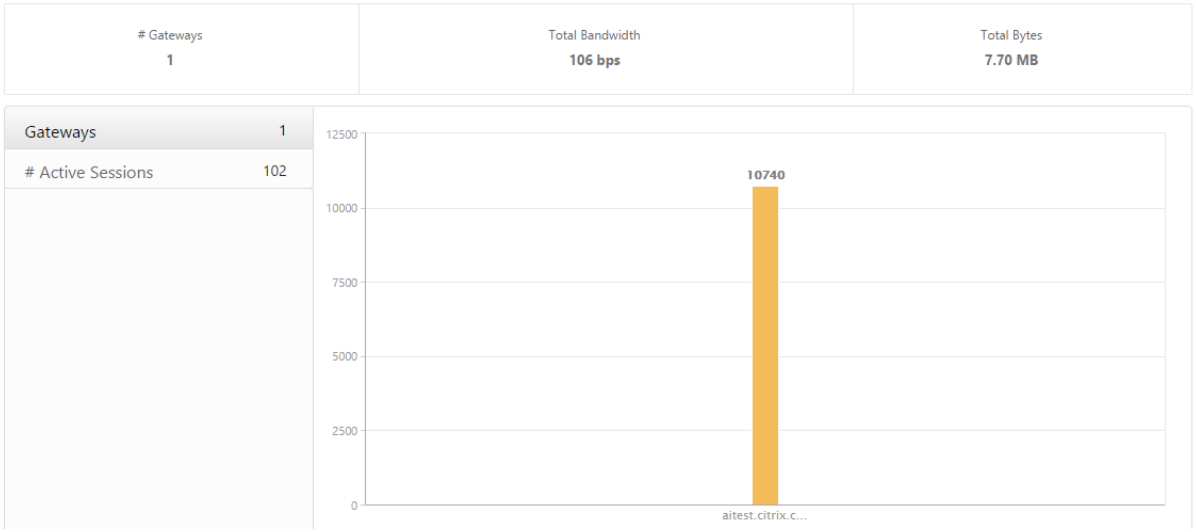
You can view the number of gateways, number of active sessions, total bytes and bandwidth used by all gateways associated with a NetScaler Gateway appliance at any given time. You can view the EPA, authentication, single sign-on, and application launch failures for a gateway. You can also view the details of all users associated with a gateway and their logon activity.

View gateway details

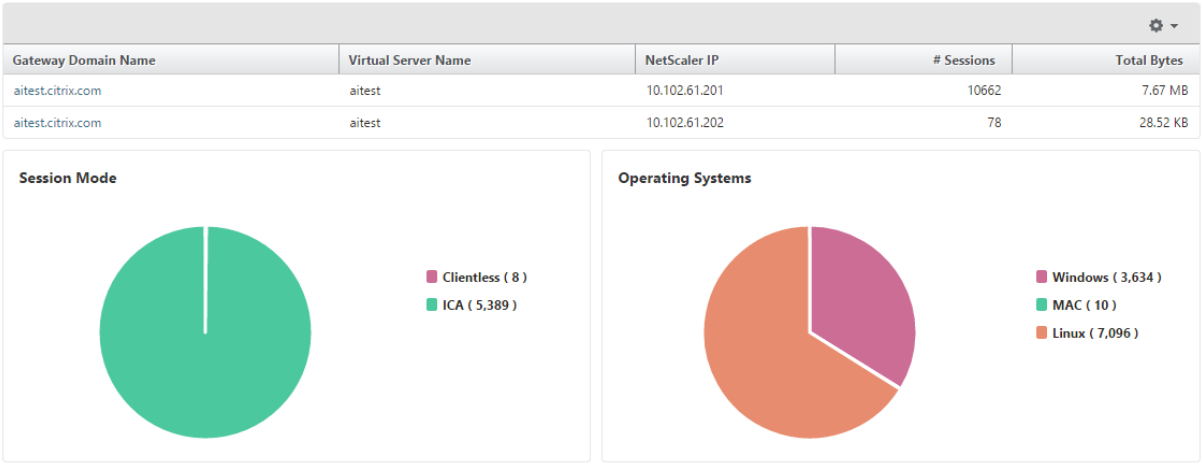
1. In NetScaler Console, navigate to **Gateway > Gateway Insight > Gateways**.
2. Select the time period for which you want to view the gateway details. You can use the time slider to further customize the selected time period. Click **Go**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**
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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

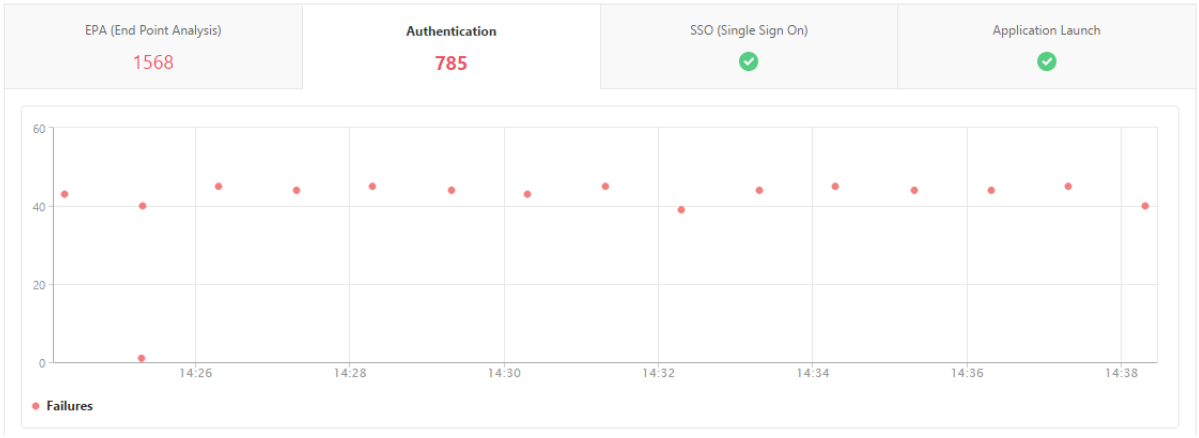
Authentication Failures

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**.
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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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

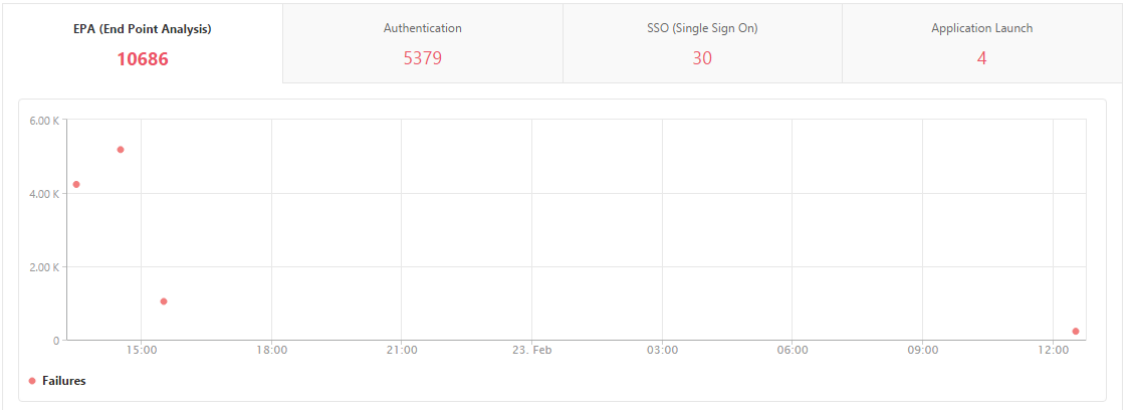
You can view EPA failures at pre- or post-authentication stage.

View EPA failure details

1. In NetScaler Console, navigate to **Gateway > Gateway Insight**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

> **Note**
>
> NetScaler Gateway doesn't report the EPA failures when the "clientSecurity"expression is configured as a VPN session policy rule.

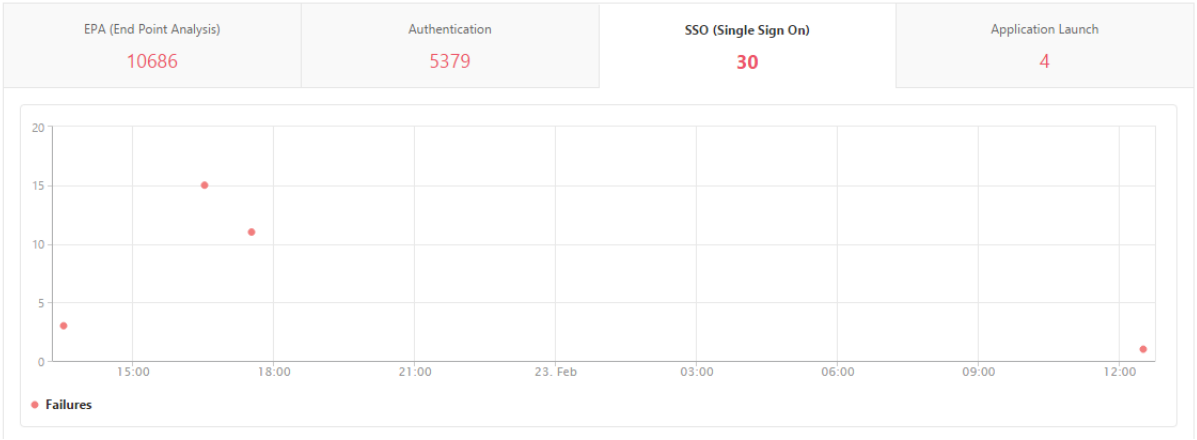
SSO Failures

You can view the all the SSO failures at any stage for a user accessing any applications through the NetScaler Gateway appliance.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

View SSO failure details

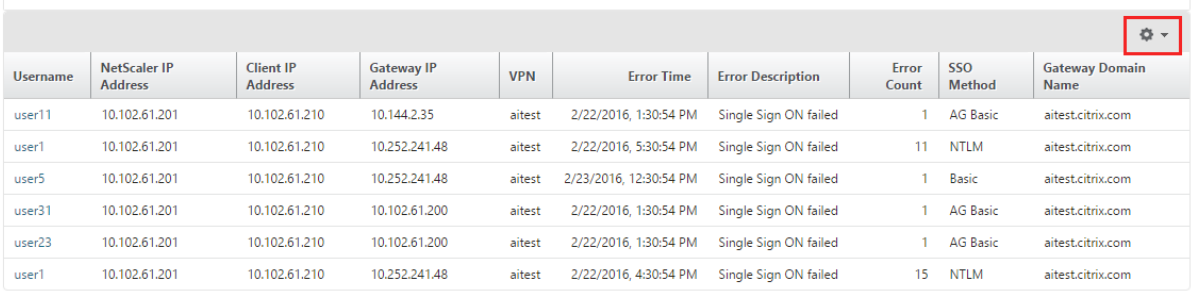
1. In NetScaler Console, navigate to **Gateway > Gateway Insight**.
2. In the Overview section, select the time period for which you want to view the SSO errors. You can use the time slider to further customize the selected time period. Click **Go**.
3. Click the **SSO (Single Sign On)** tab. You can 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.



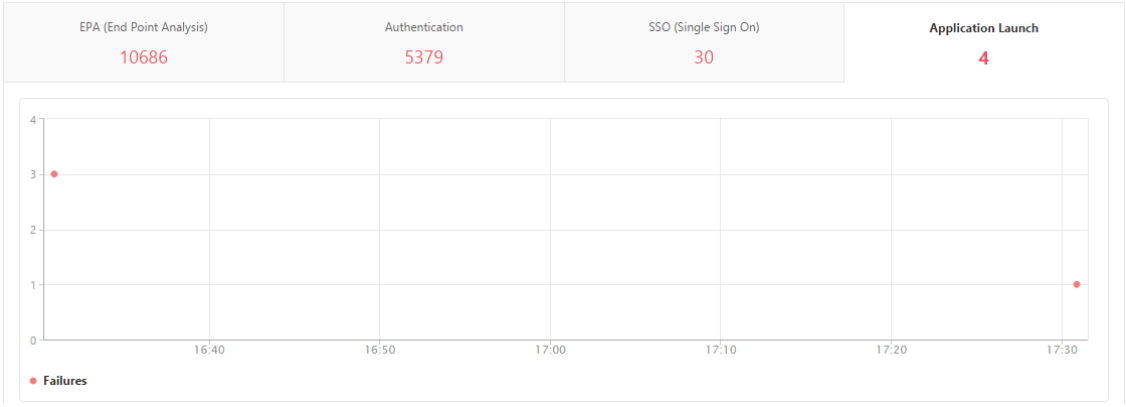
Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	SSO Method	Gateway Domain Name
user11	10.102.61.201	10.102.61.210	10.144.2.35	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

View application launch failure details

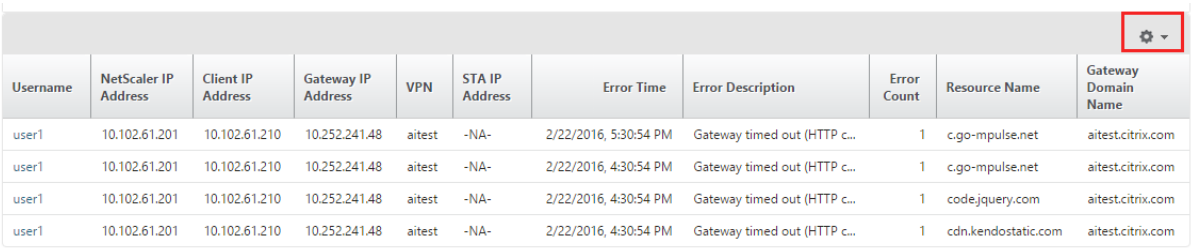
1. In NetScaler Console, navigate to **Gateway > Gateway Insight**.
2. In the **Overview** section, select the time period for which you want to view the SSO errors. You can use the time slider to further customize the selected time period. Click **Go**.
3. Click the **Application Launch** tab. You can 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.

You can customize the table to add or delete columns by using the settings option.



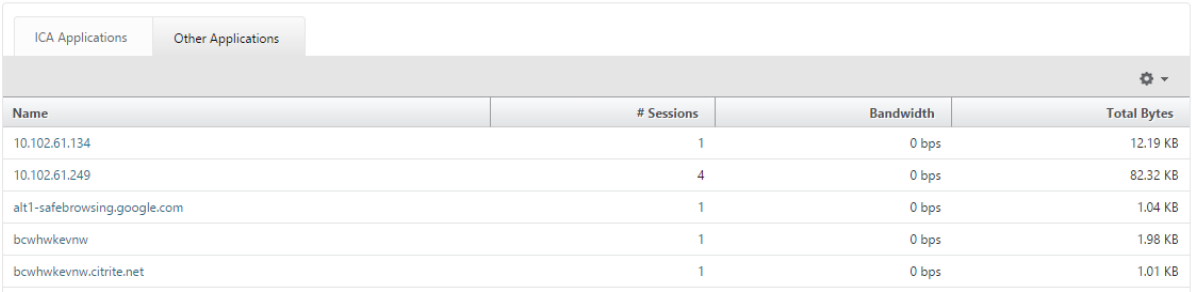
Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	STA IP Address	Error Time	Error Description	Error Count	Resource Name	Gateway Domain Name
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 5:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
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.

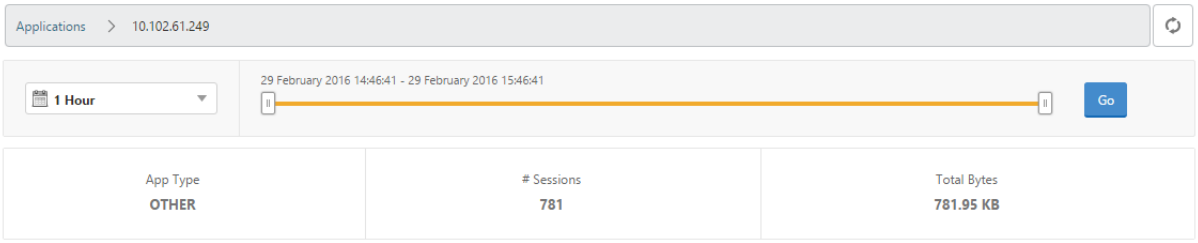
© 1997–2025 Citrix Systems, Inc. All rights reserved.

View total bytes and bandwidth consumed by an application

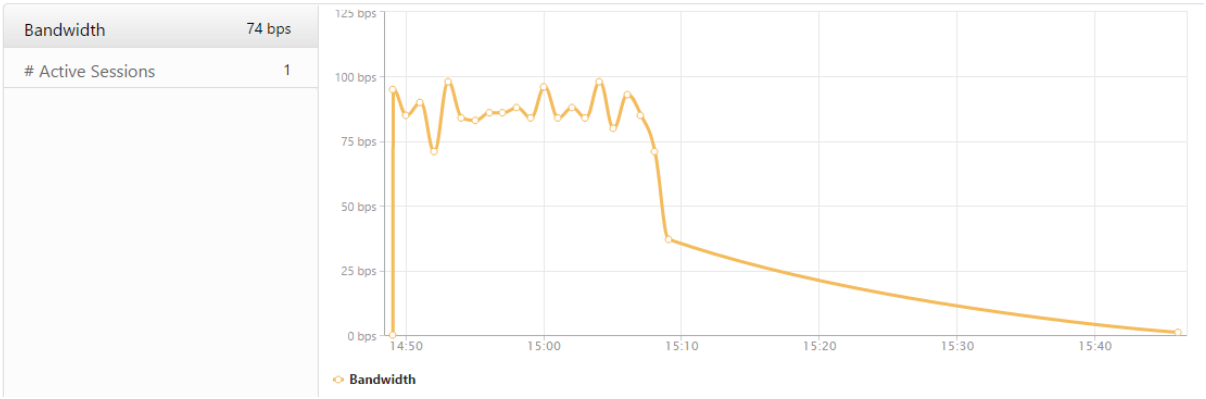
In NetScaler Console, navigate to **Gateway > Gateway Insight > Applications**, scroll down and, on the **Other Applications** tab, click the application for which you want to view the details.



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.



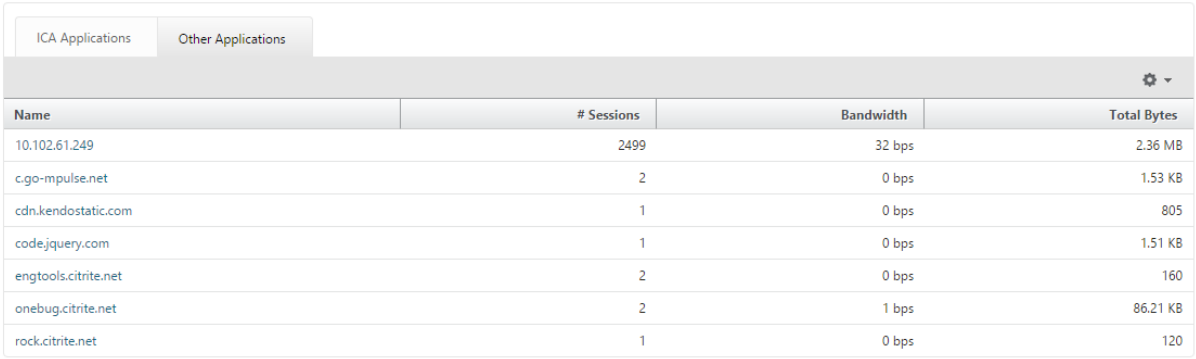
4. A user has logged on to NetScaler Gateway successfully, but is unable to access certain network resources in the internal network With Gateway Insight, you can determine whether the user has access to the network resources or not. You can also view the name of the policy that resulted in the failure.

View user access for resources

1. In NetScaler Console, navigate to **Gateway > Gateway Insight > Applications**.

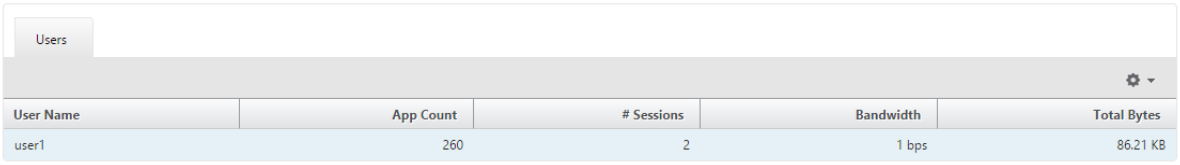
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.



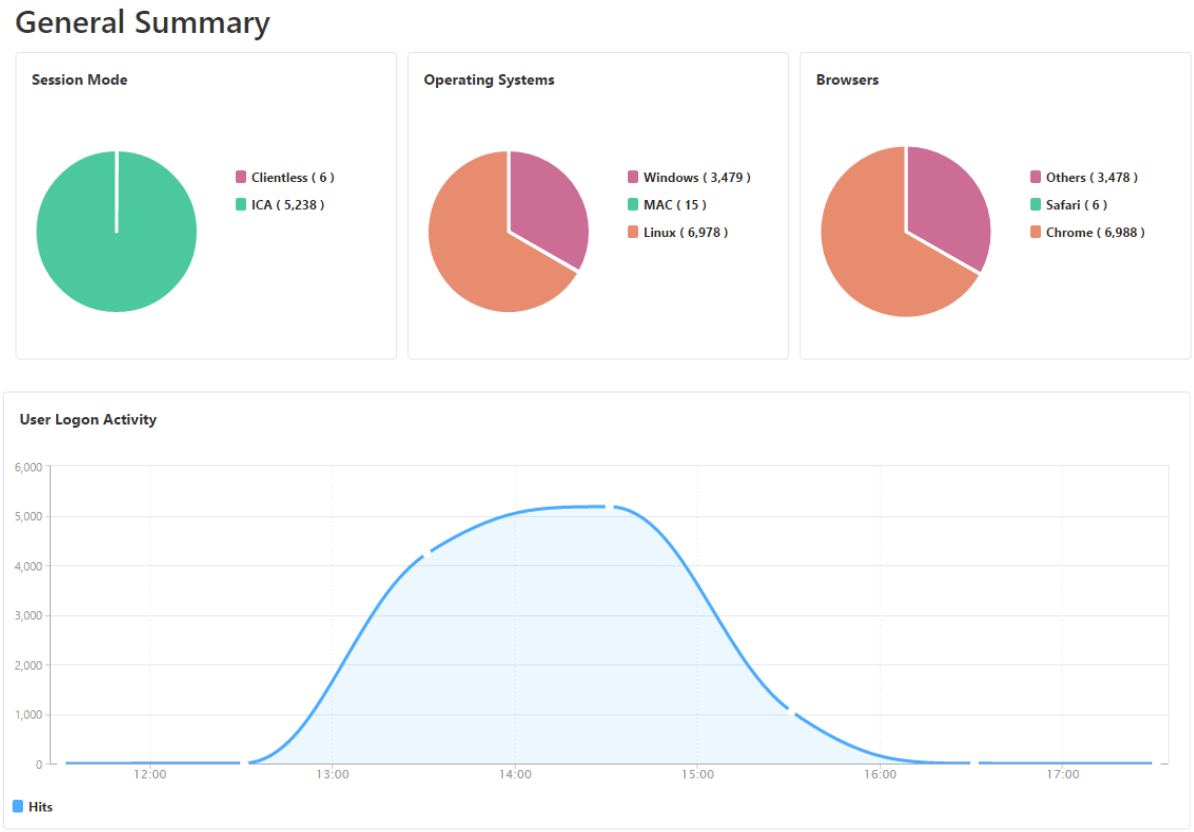
User Name	App Count	# Sessions	Bandwidth	Total Bytes
user1	260	2	1 bps	86.21 KB

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



HDX Insight

January 8, 2024

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.

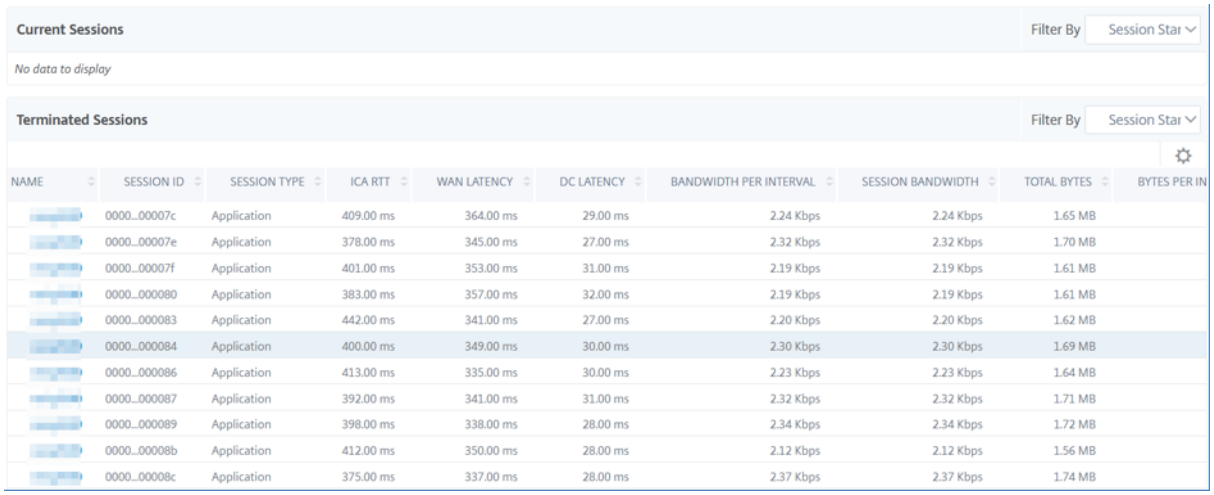
> **Note**
>
> To allow ICA round trip time calculations to be logged, enable the following policy settings:
>
> - ICA Round Trip Calculation
> - ICA Round Trip Calculation Interval

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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.



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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- WYSE Windows-based Thin Clients
- WYSE Linux-based Thin Clients
- WYSE ThinOS-based Thin Clients
- 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.

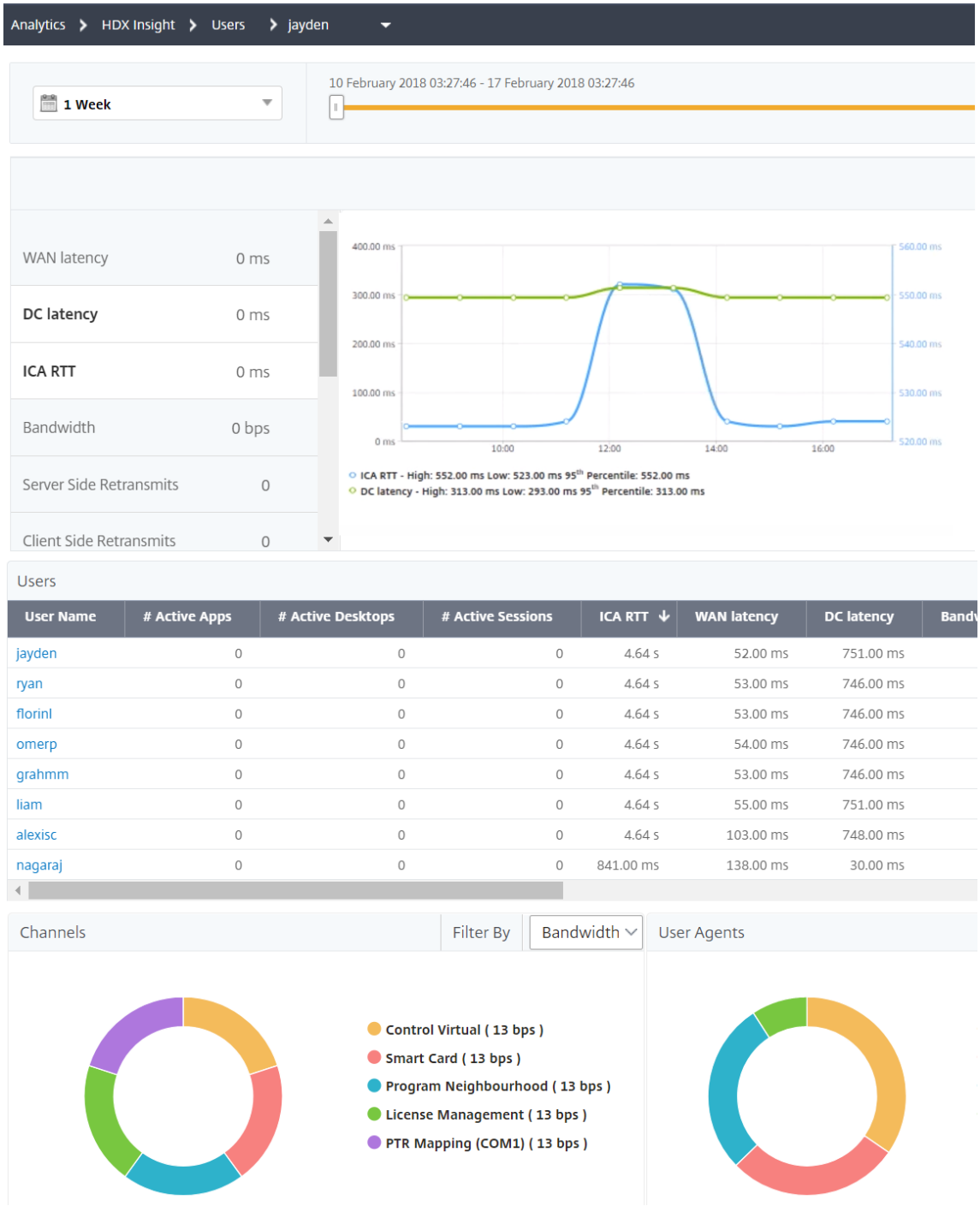
To identify the root cause of the issue, analyze the following metrics:

- WAN Latency
- DC Latency
- Host Delay

To view the client metrics:

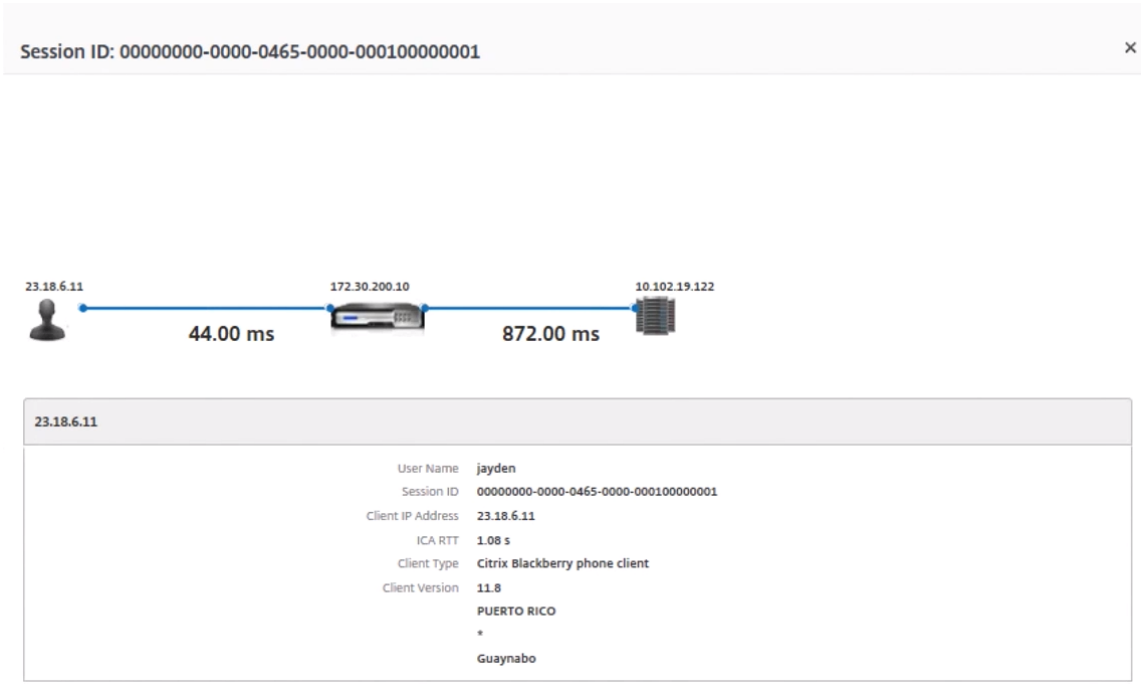
1. On the **Analytics** tab, navigate to **HDX Insight** > **Users**.
2. Scroll down and select the user name and select the period from the list. The period can be one day, one week, one month, or you can even customize the period for which you want to see the data.
3. The chart displays the ICA RTT and DC latency values of the user for the specified period as a graph.

© 1997–2025 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.

© 1997–2025 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:

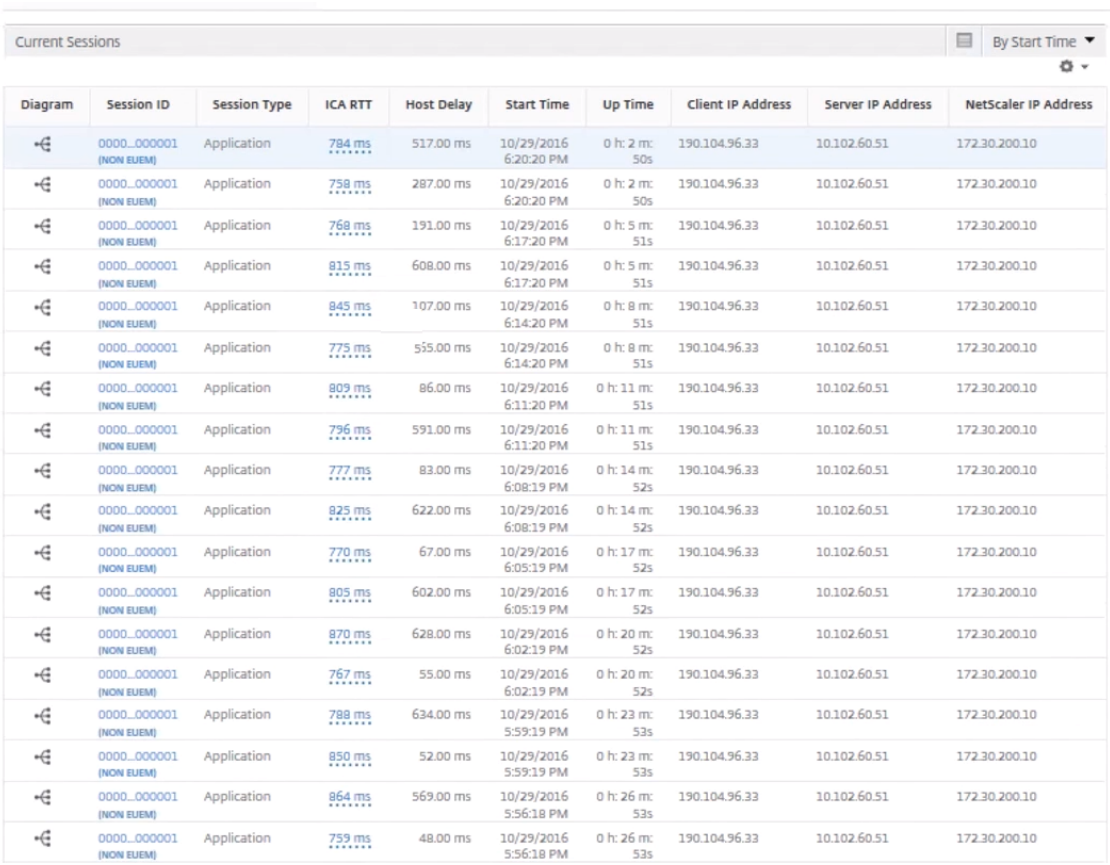
- WAN latency
- DC latency
- Host delay

To view the user metrics:

1. Navigate to **Gateway** > **HDX Insight** > **Users**.
2. Scroll down and click the user name.
3. In the graphical representation, note the WAN Latency, DC Latency and RTT values for the particular session.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

4. In the **Current Application Sessions** table, note that the host delay is high.



Current Sessions — By Start Time

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.

© 1997–2025 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

IP address block associated with City A, NetScaler Console recognizes that the traffic is originating from City A for this client.

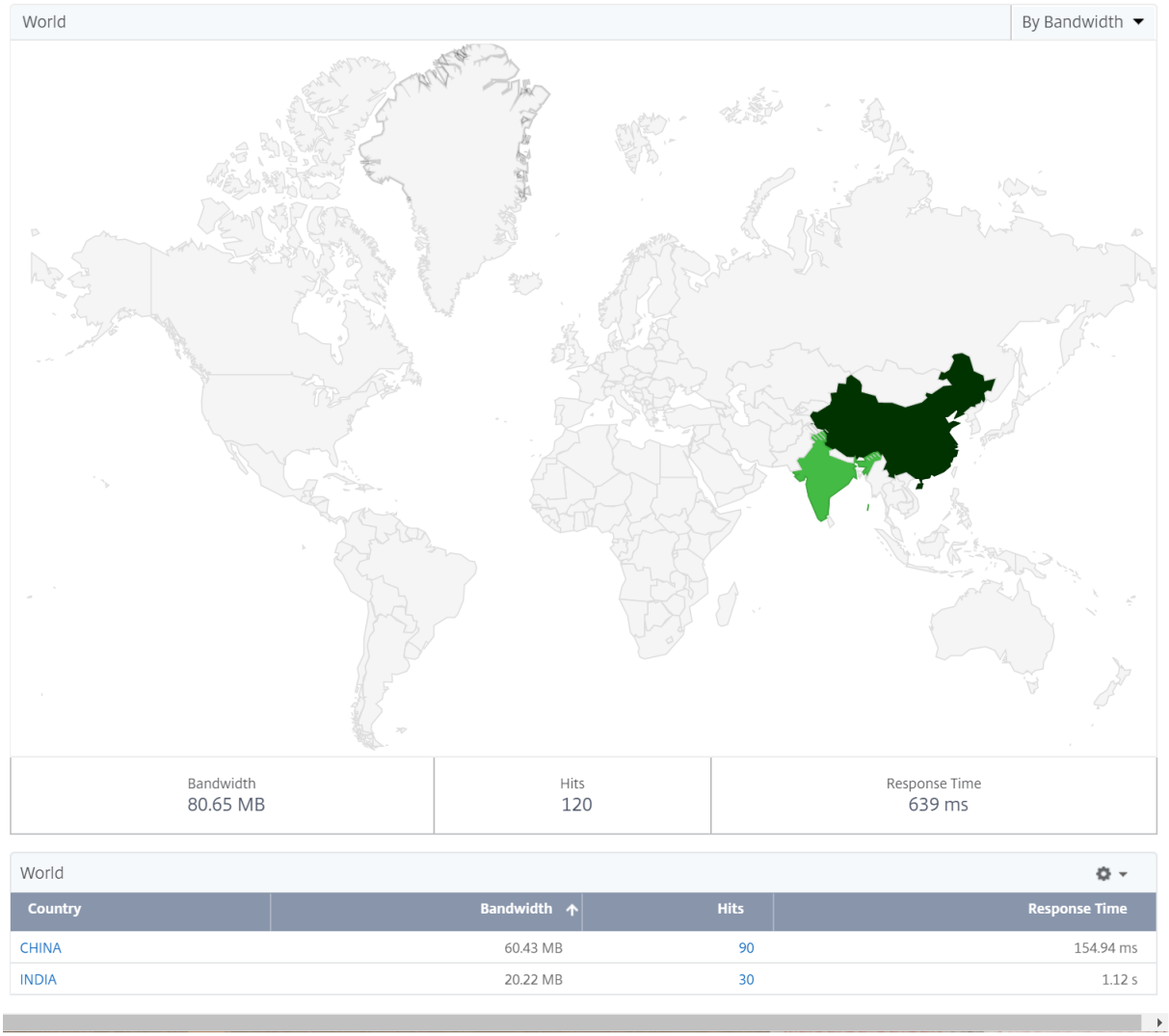
To create an IP block:

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.

© 1997–2025 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.

> **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

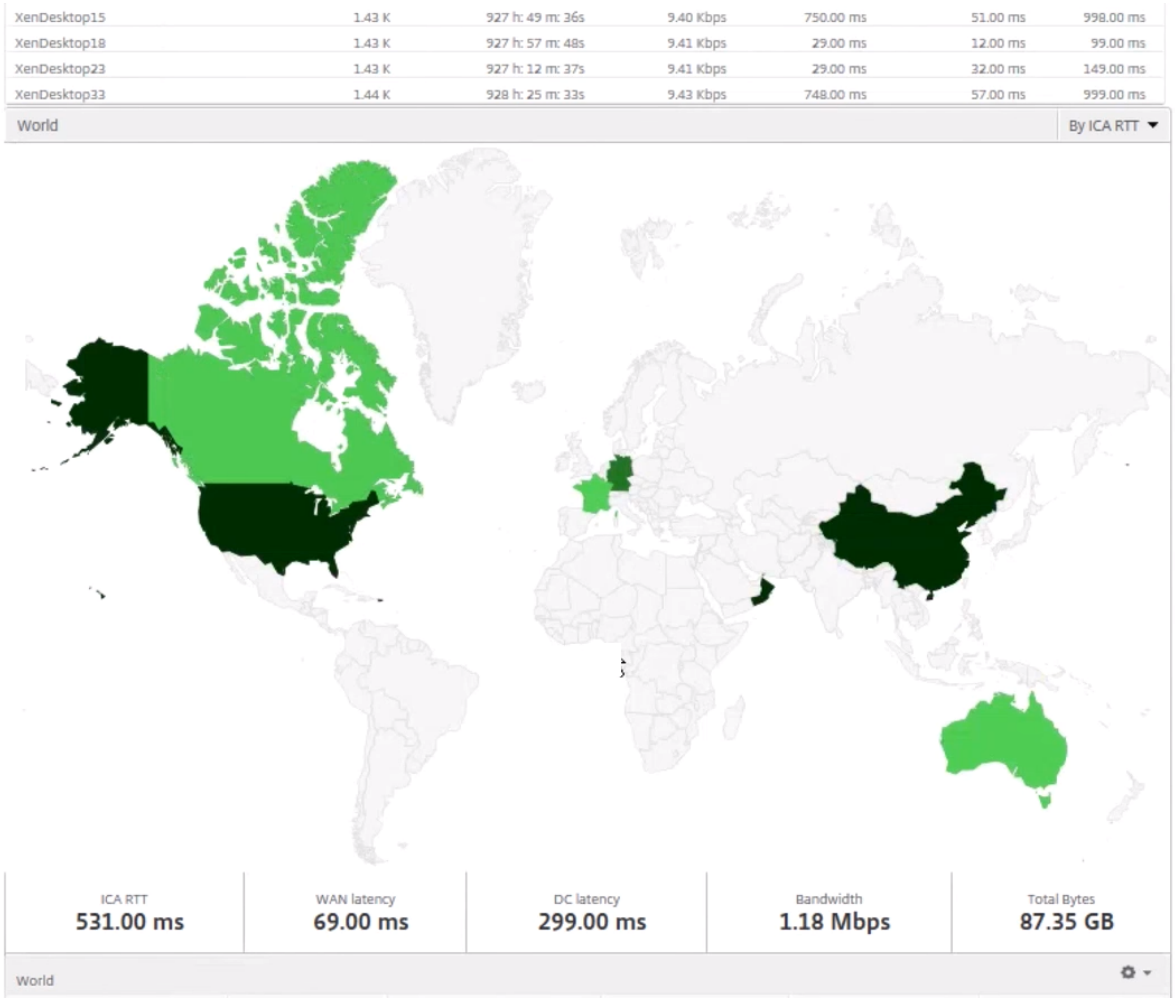
Consider a scenario in which organization ABC has 2 branch offices, one in Santa Clara and the other in India.

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.

© 1997–2025 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.

> **Note**
>
> - If you select **Weekly** recurrence, ensure that you select the weekdays on which you want

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 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

January 8, 2024

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

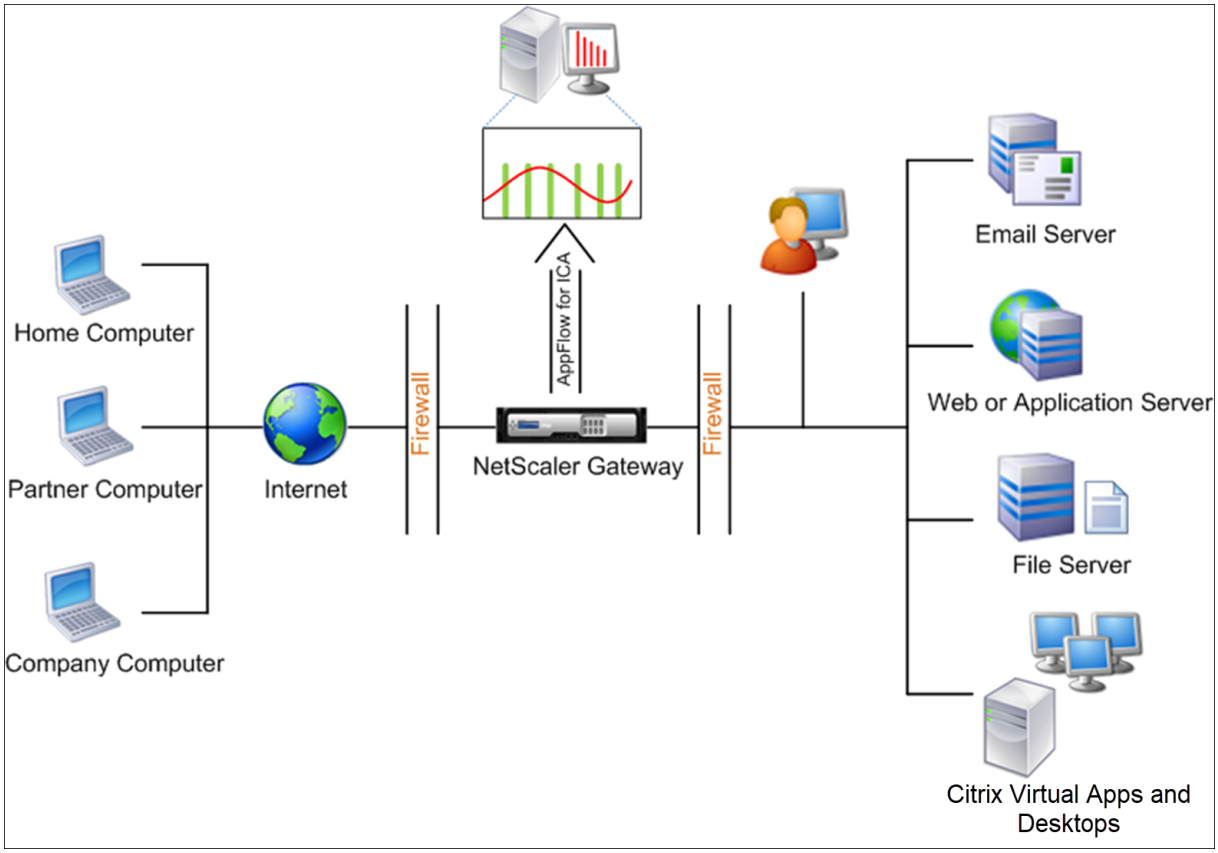
Enable data collection for NetScaler Gateway appliances deployed in single-hop mode

January 8, 2024

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

© 1997–2025 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`

© 1997–2025 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

January 8, 2024

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.

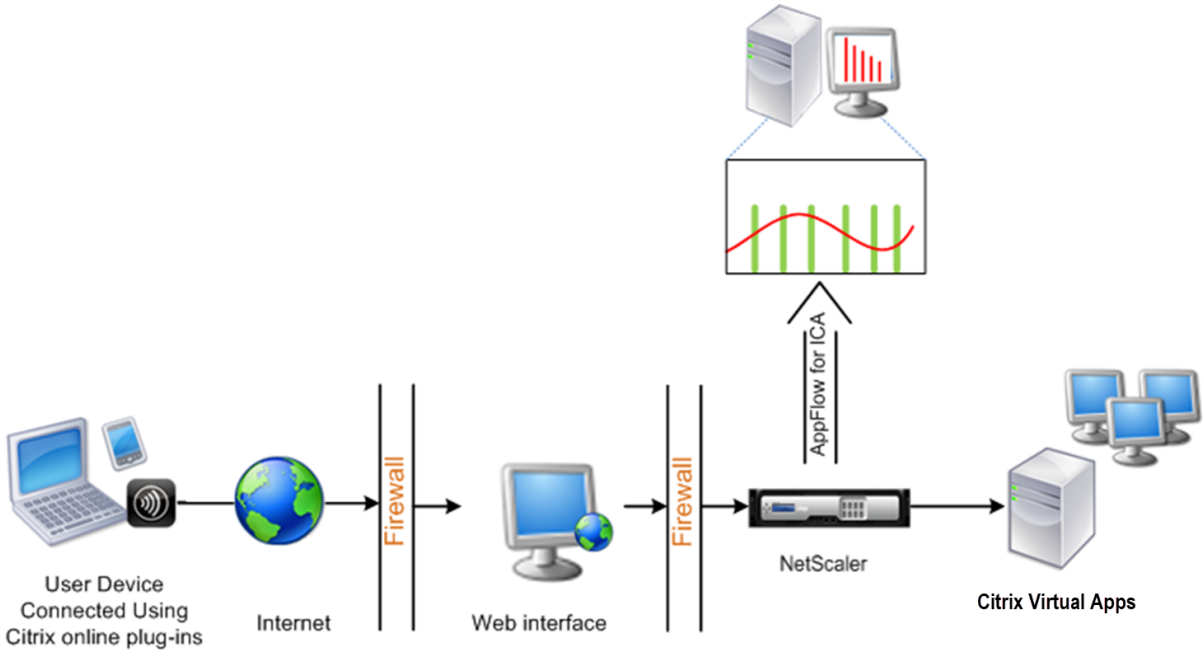
After you add the NetScaler to the NetScaler Console inventory, you must enable AppFlow for data collection. Enabling data collection depends on the device and the mode. In that case, you have to add NetScaler Console as an AppFlow collector on each NetScaler appliance, and you must configure an AppFlow 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:

© 1997–2025 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.

```
add appflow collector <name> -IPAddress <ip_addr>
```

Example:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **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
```

> **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

February 27, 2024

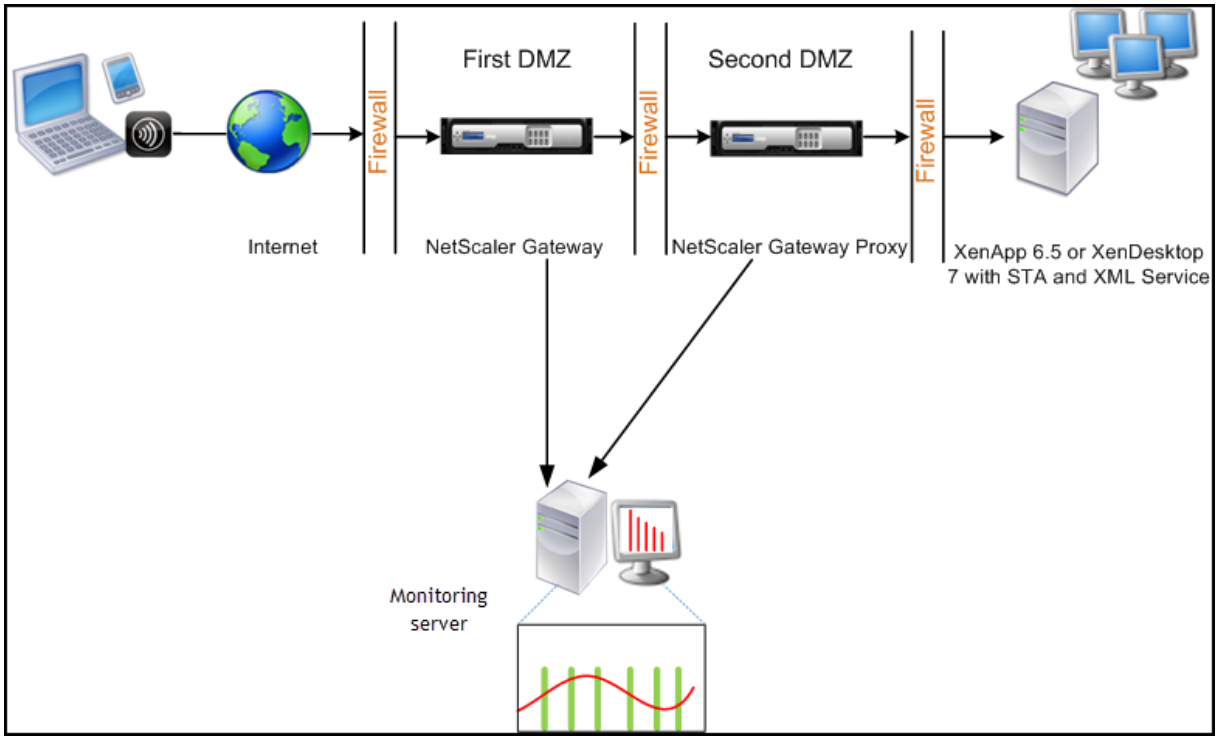
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.



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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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.

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 [**-secure** (ON OFF)] [**-imgGifToPng**] …

```
1 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>

```
1 bind vpn vserver vs1 -nextHopServer nh1
```

3. Enable double hop and AppFlow on the NetScaler Gateway in the second DMZ.

---

set vpn vserver [**-doubleHop** (ENABLED DISABLED)] [**- appflowLog** (ENABLED DISABLED)]

```
1 set vpn vserver vpnhop2 –doubleHop ENABLED –appFlowLog ENABLED
```

4. Disable authentication on the NetScaler Gateway virtual server in the second DMZ.

---

set vpn vserver [**-authentication** (ON OFF)]

```
1 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>]

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
bind vpn vserver vpn1 -policy appflowpol1 -priority 101  – type
    OTHERTCP\_REQUEST
```

6. Enable the other NetScaler Gateway appliance to export ICA records:

   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** DISABLED)]
(ENABLED

```
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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

4. Enable one of the NetScaler Gateway appliances to export TCP 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**.
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

January 8, 2024

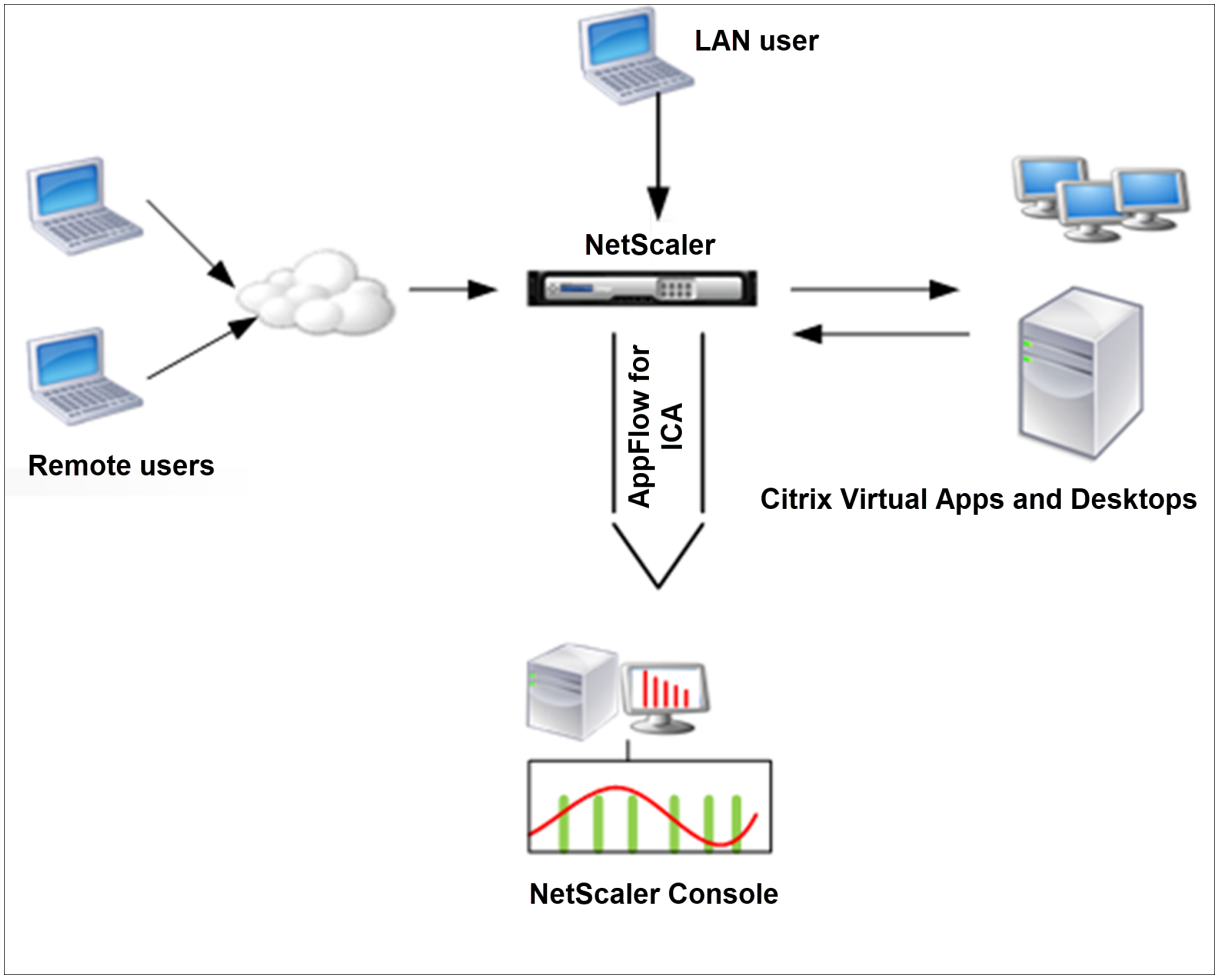
External users who access Citrix Virtual App or Desktop applications must authenticate themselves on the NetScaler Gateway. Internal users, however, might not require to be redirected to the NetScaler Gateway. Also, in a transparent mode deployment, the administrator must manually apply the routing policies, 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.



> **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.

> **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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:

```
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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
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
```

> **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

January 8, 2024

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 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 Gateway and GSLB based redirection. Eric, the Citrix Virtual Apps and Desktops admin for ABC Inc. wants to

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

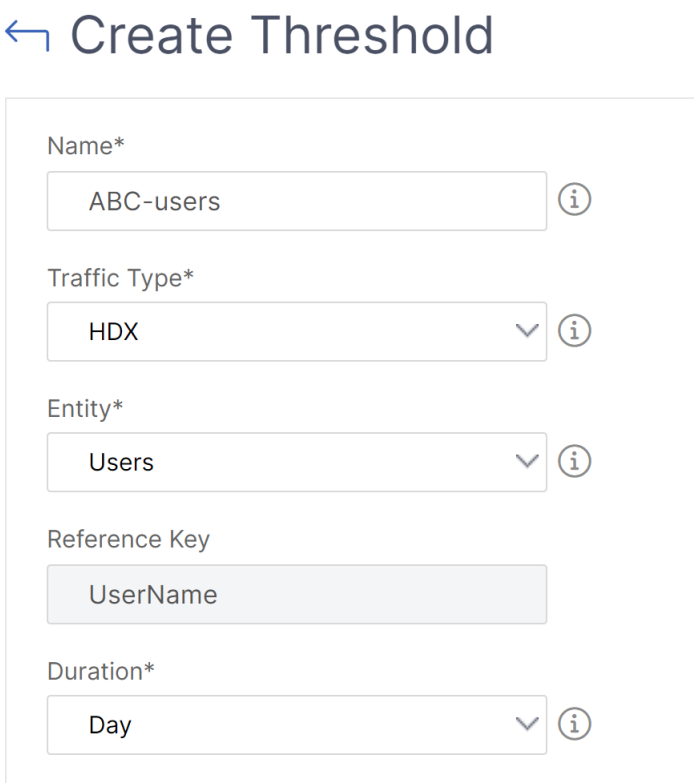
The users of ABC Inc. have a distributed presence. Some users are located close to the data center, while a few are located at further away from the data center. As the user base is distributed widely, the metrics and the corresponding thresholds also vary among these locations. For example, the ICA 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

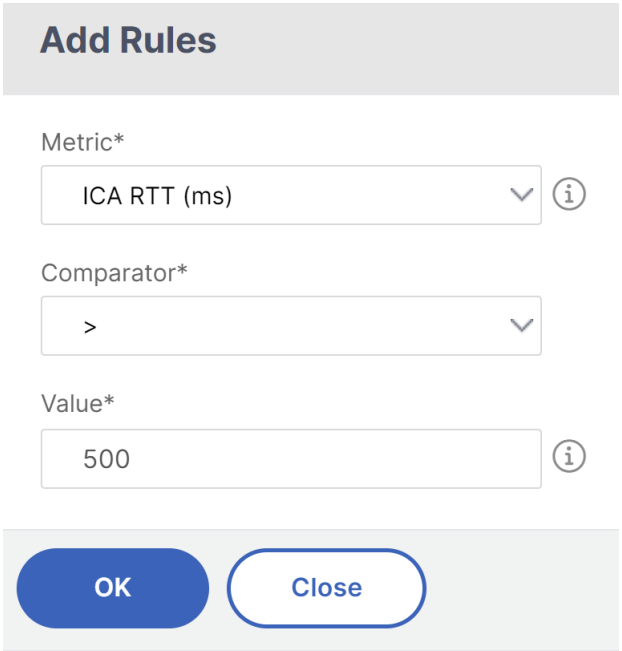
1. In NetScaler Console, navigate to **Settings> Analytics Settings > Thresholds**. On **Thresholds** page that opens, click **Add**.
2. On the **Create Thresholds and Alerts** page, specify the following details:
    a) **Name**. Type in a name for creating an event for which NetScaler Console generates 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



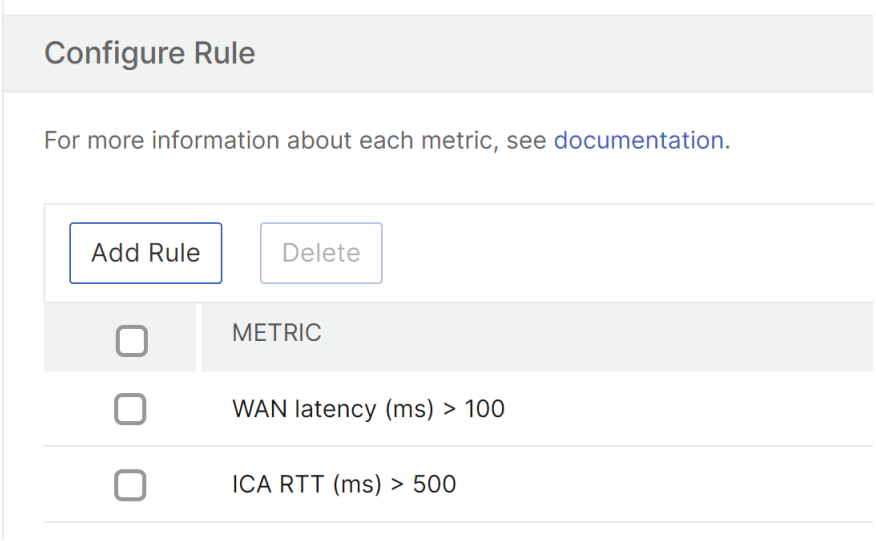
3. **Creating threshold rules group for all entities:**

   For HDX traffic, you must create a rule by clicking **Add Rule**. Enter the values in the **Add Rules** pop-up window that opens.



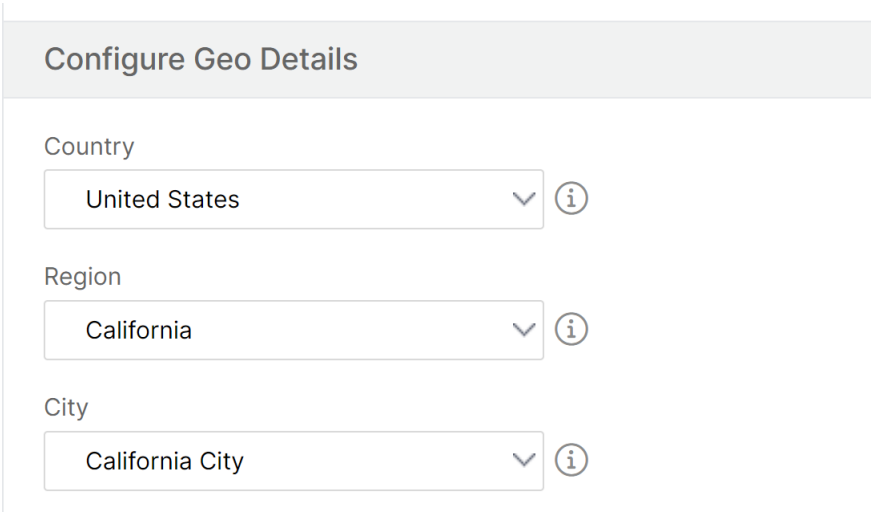
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.



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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

View HDX Insight reports and metrics

September 8, 2025

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

Troubleshoot HDX Insight issues

September 8, 2025

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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.

  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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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

  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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> Skip code 0 indicates that the record is successfully exported from NetScaler.

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_EXPAND	Failed to expand channel data
111	NS_ICA_ERR_REDUC_BYTES_V3_COR	Expander error: Bytes consumed more than bytes available
112	NS_ICA_ERR_REDUC_BYTES_OOR	Error: Uncompressed data overrun
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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Skip Code	Error message	Cause of error
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
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	Received invalid channel header
130	NS_ICA_ERR_CGP_PARSE_RECONNECT_VC	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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Skip Code	Error message	Cause of error
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
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
150	NS_ICA_ERR_SEAMLESS_INSUFFBYTE	Encountered insufficient bytes for seamless command
151	NS_ICA_ERR_EUEM_INSUFFBYTE	Encountered insufficient bytes for EUEM command

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Skip Code	Error message	Cause of error
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
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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Skip Code	Error message	Cause of error
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
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 [0
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
x8820220228], 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 [0
x8820220008], Track Flags [0x1600010c040], Skip Code [171]"
```

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 Pure ICA connections detected by NS. Incremented whenever an ICA connection based on the ICA signature on a client PCB is detected.	Stats
hdx_tot_cgp_conn	Indicates total number of CGP connections detected by NS (Session Reliability ON). Incremented whenever a CGP 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

HDX counter name	Purpose	Category(Stats/Error/Diagnostics)
hdx_tot_skip_conn	Indicates how many ICA connections were skipped by parser due to invalid ICA or CGP signature.	Stats
hdx_dbg_active_conn	Total Active EDT/CGP/ICA connections at that instant.	Stats
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 channel is required to collect statistics such as ICA RTT.	Stats/Diagnostics

© 1997–2025 Citrix Systems, Inc. All rights reserved.

HDX counter name	Purpose	Category(Stats/Error/Diagnostics)
hdx_err_disabled_sr	Session Reliability is disabled using `nsapimgr` knob. Session 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 Insight 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_disabled	Total number of NS_ICA_CAM_CHANNEL disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_usb_channel_disabled	Total number of NS_ICA_USB_CHANNEL disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_clip_channel_disabled	Total number of NS_ICA_CLIP_CHANNEL disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_ccm_channel_disabled	Total number of NS_ICA_CCM_CHANNEL disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_cdm_channel_disabled	Total number of NS_ICA_CDM_CHANNEL disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_com1_channel_disabled	Total number of NS_ICA_COM1_CHANNEL disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_com2_channel_disabled	Total number of NS_ICA_COM2_CHANNEL disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_cpm_channel_disabled	Total number of NS_ICA_CPM_CHANNEL disabled via SmartAccess policy	Diagnostics

© 1997–2025 Citrix Systems, Inc. All rights reserved.

HDX counter name	Purpose	Category(Stats/Error/Diagnostics)
hdx_sm_ica_lpt1_channel_disabled	Total number of NS_ICA_LPT1_CHANNEL disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_lpt2_channel_disabled	Total number of NS_ICA_LPT2_CHANNEL disabled via SmartAccess policy	Diagnostics
dx_dbg_sm_ica_msi_disabled	Total number of cases where MSI is disabled via SmartAccess policy	Diagnostics
hdx_sm_ica_file_channel_disabled	Total number of NS_ICA_FILE_CHANNEL is disabled via SmartAccess policy	Diagnostics
hdx_dbg_usb_accept_device	Total number of USB devices accepted	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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:

- 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Metrics information for thresholds

January 8, 2024

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)
	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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Metrics	Entity	Description
	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
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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Metrics	Entity	Description
User Agents	Hits	Total number of requests received by a user agent. For example: Chrome web browser
	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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Metric	Entity	Description
Applications	AppScore	App Score defines how well an application is performing and shows whether the application is performing well 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

Infrastructure Analytics

January 8, 2024

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
- 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

  - **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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.

    > **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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..

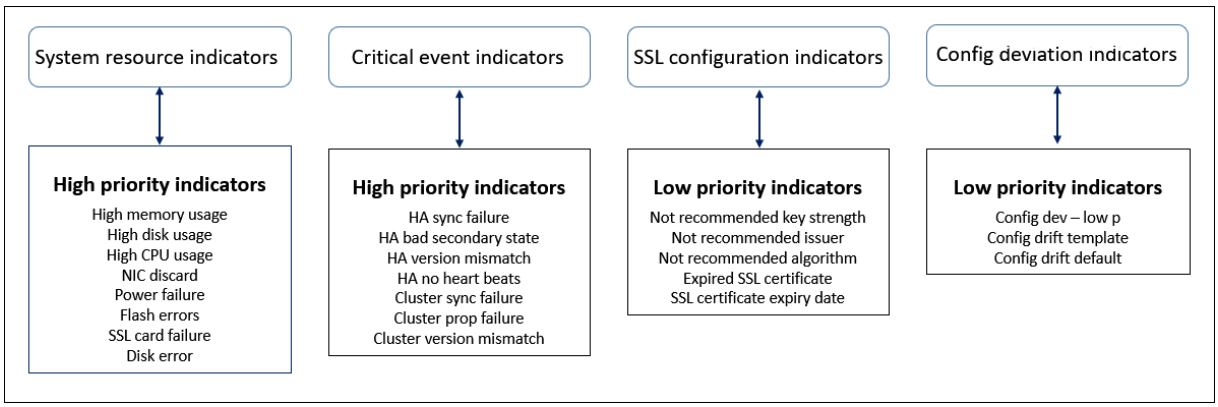
View NetScaler Capacity issues

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.

Value of health indicators

The indicators are classified into high priority indicators and low-priority indicators based on their values as follows:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.

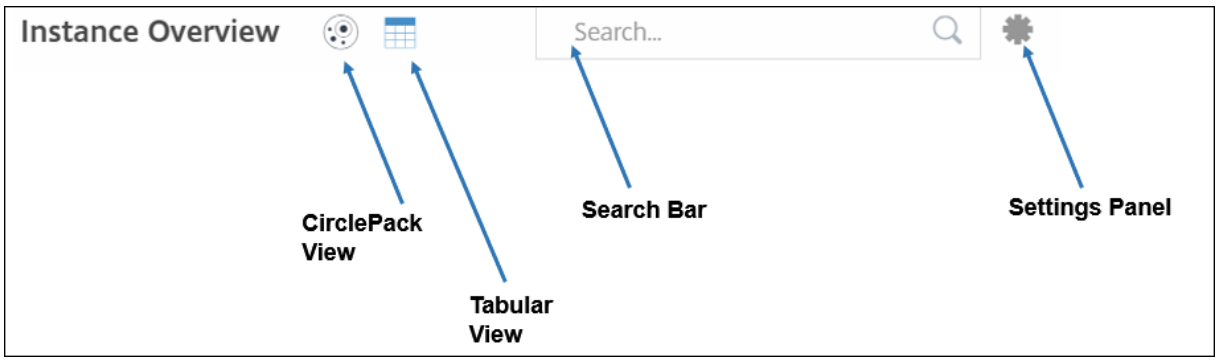
For example, CPU usage is a system resource indicator triggered when the usage value crosses the low threshold and also when the value crosses the high threshold.

Infrastructure analytics dashboard

Navigate to **Infrastructure > Infrastructure Analytics**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

The Infrastructure Analytics can be viewed in a **Circle Pack** format or a **Tabular** format. You can toggle between the two formats.

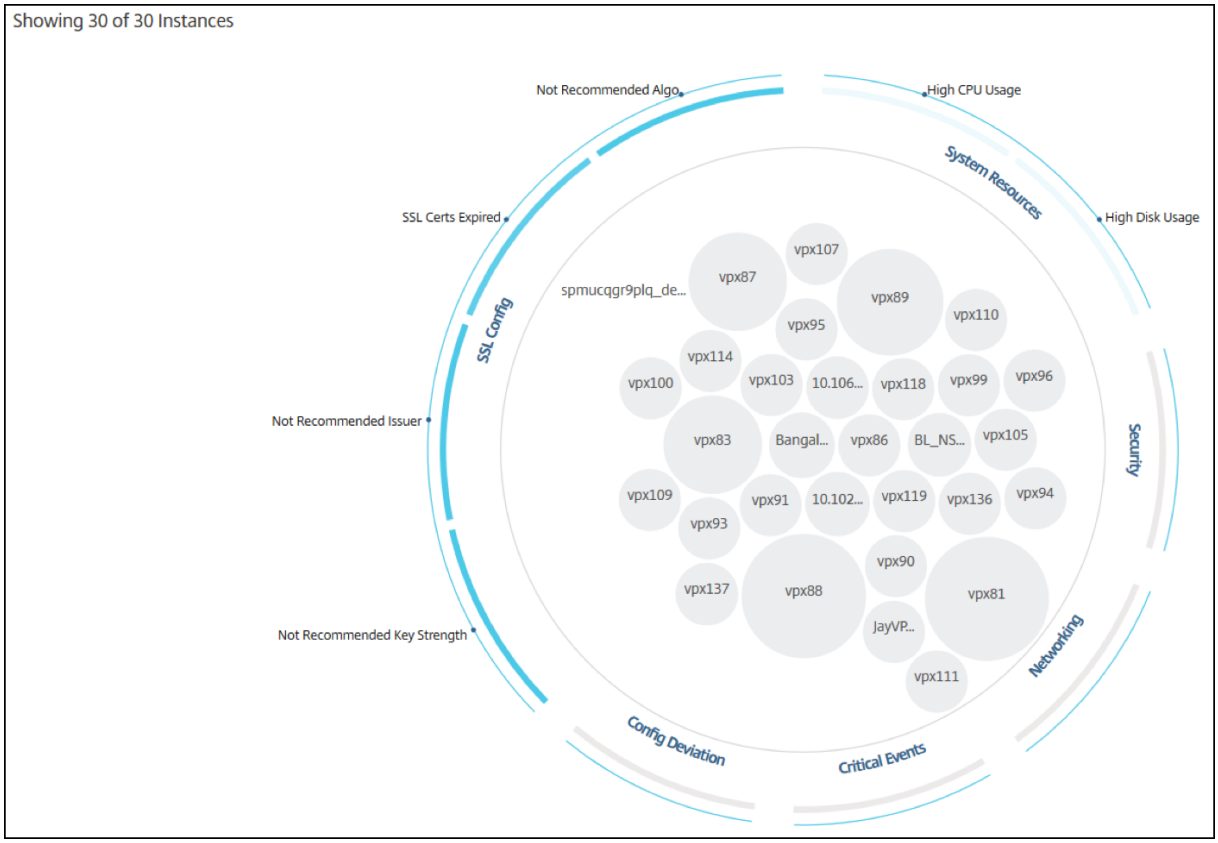


- In the Tabular view, you can search for an instance by typing the host name or the IP address in the Search bar.
- By default, Infrastructure Analytics page displays the Summary Panel on the right side of the page.
- Click the **Settings** icon to display the **Settings** Panel.
- In both the view 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.

© 1997–2025 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.

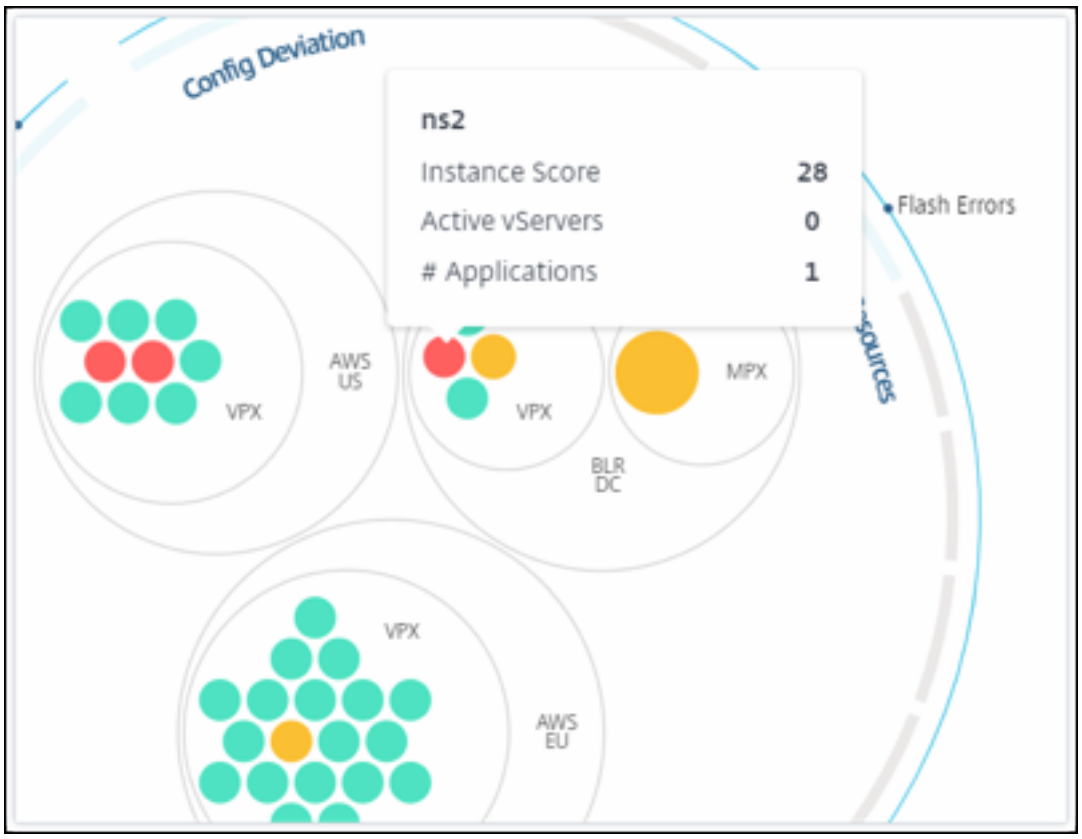
© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



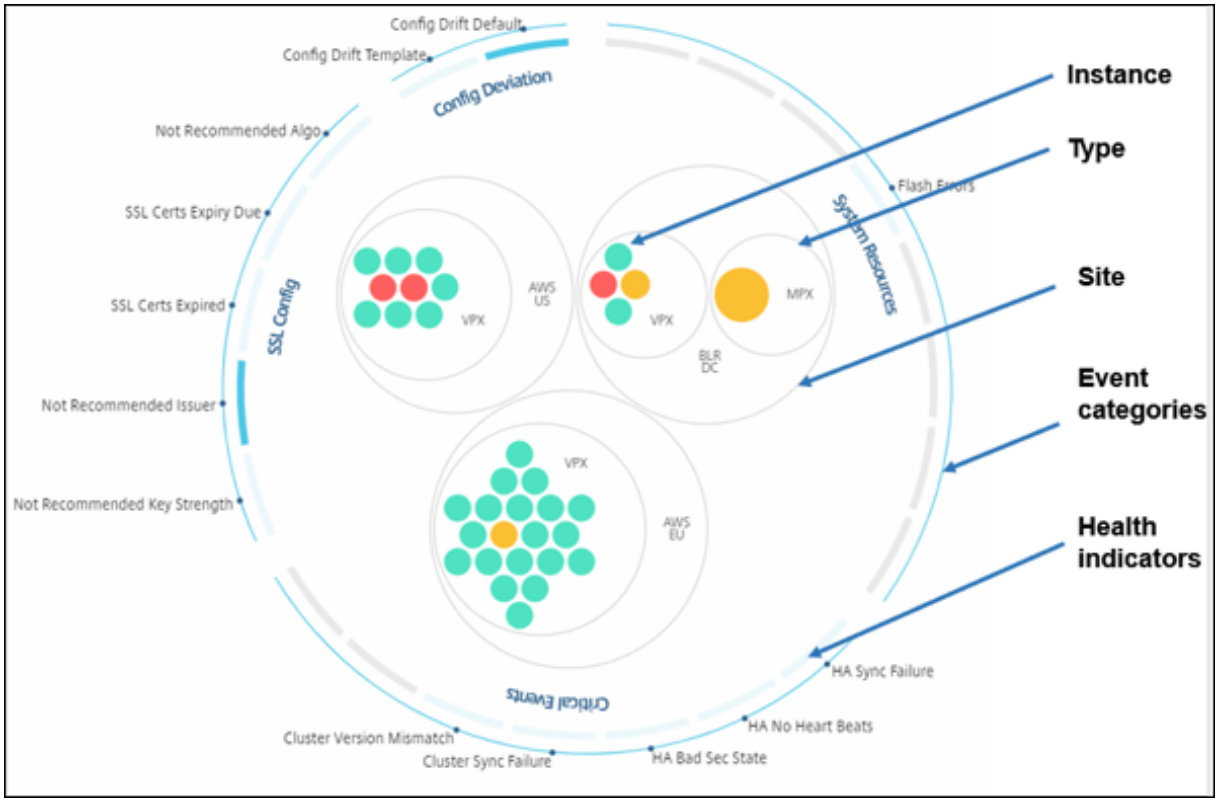
Grouped instance circles

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
- 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



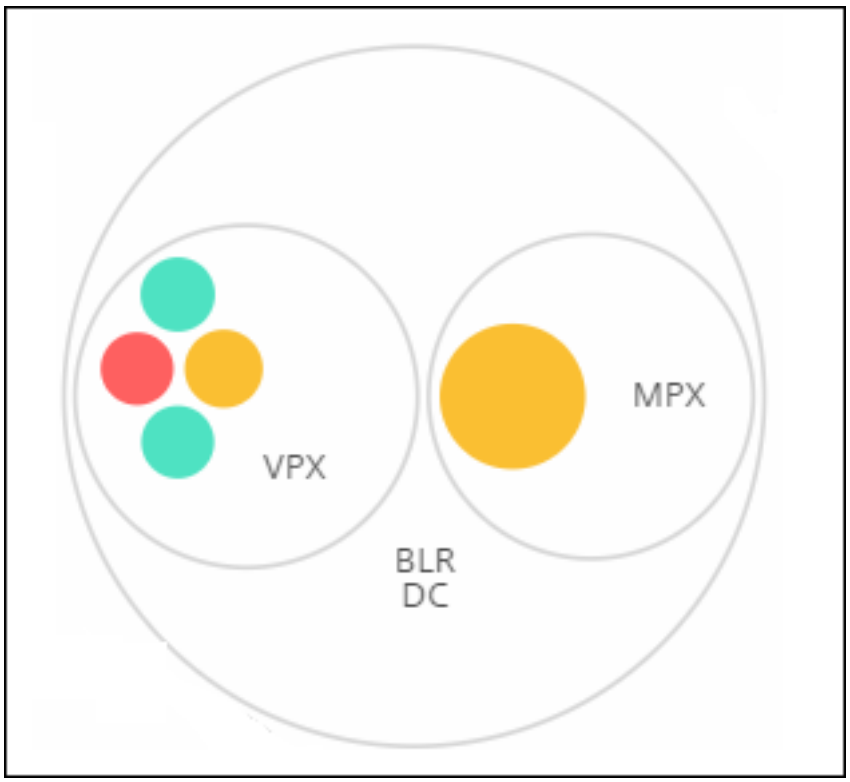
All these nested circles are bounded by two outermost circles. The outer two circles represent the four categories of events monitored by the NetScaler Console (system resources, critical events, SSL configuration, and configuration deviation) and the contributing health indicators.

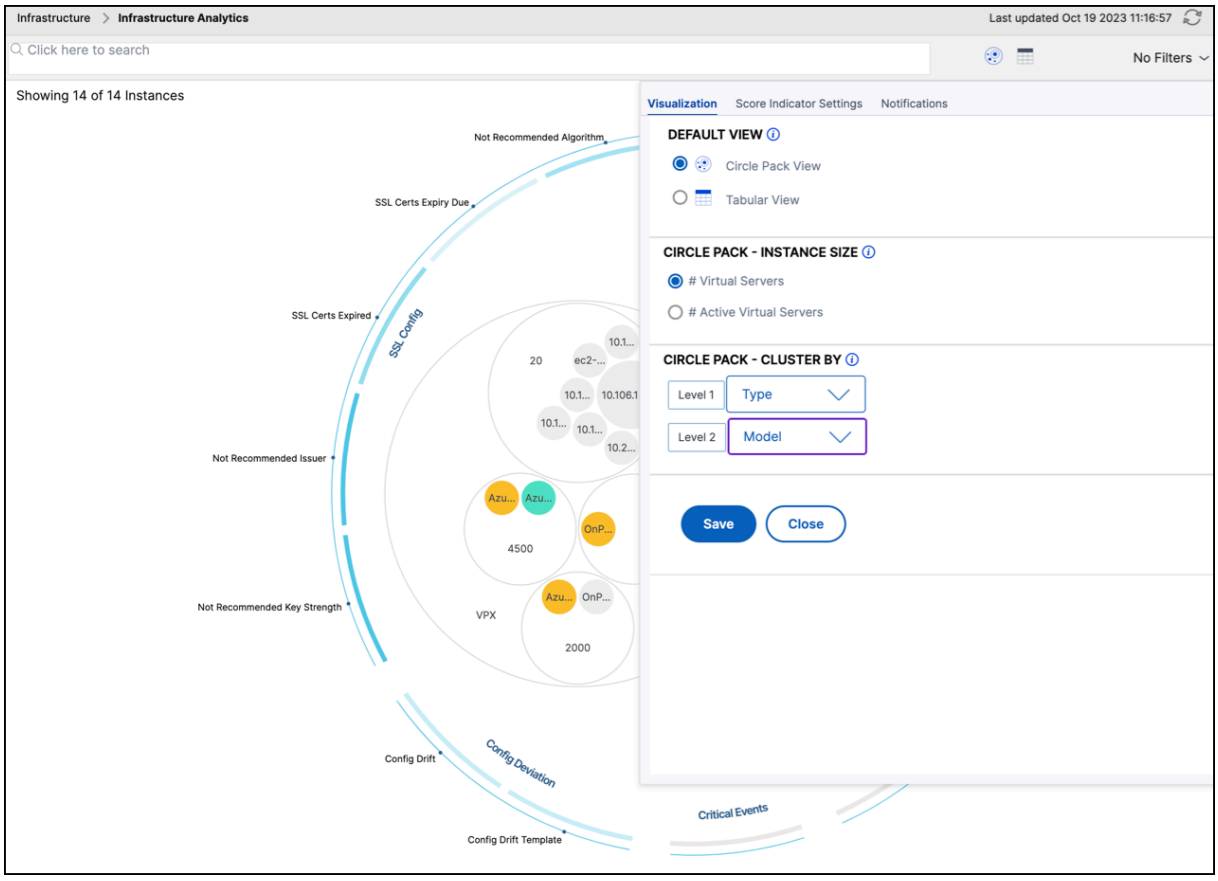
Clustered instance circles

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.





A few more examples of two-level clustering are as follows:

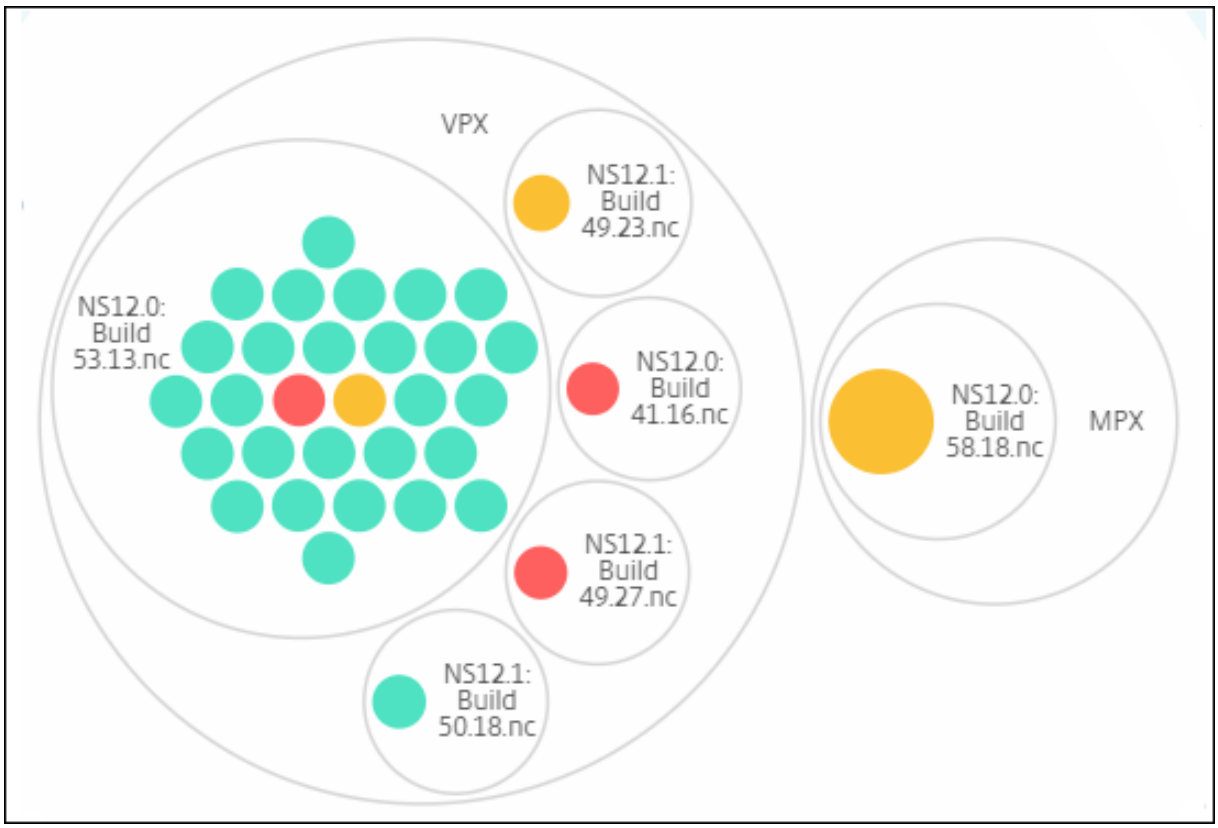
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Site and model:



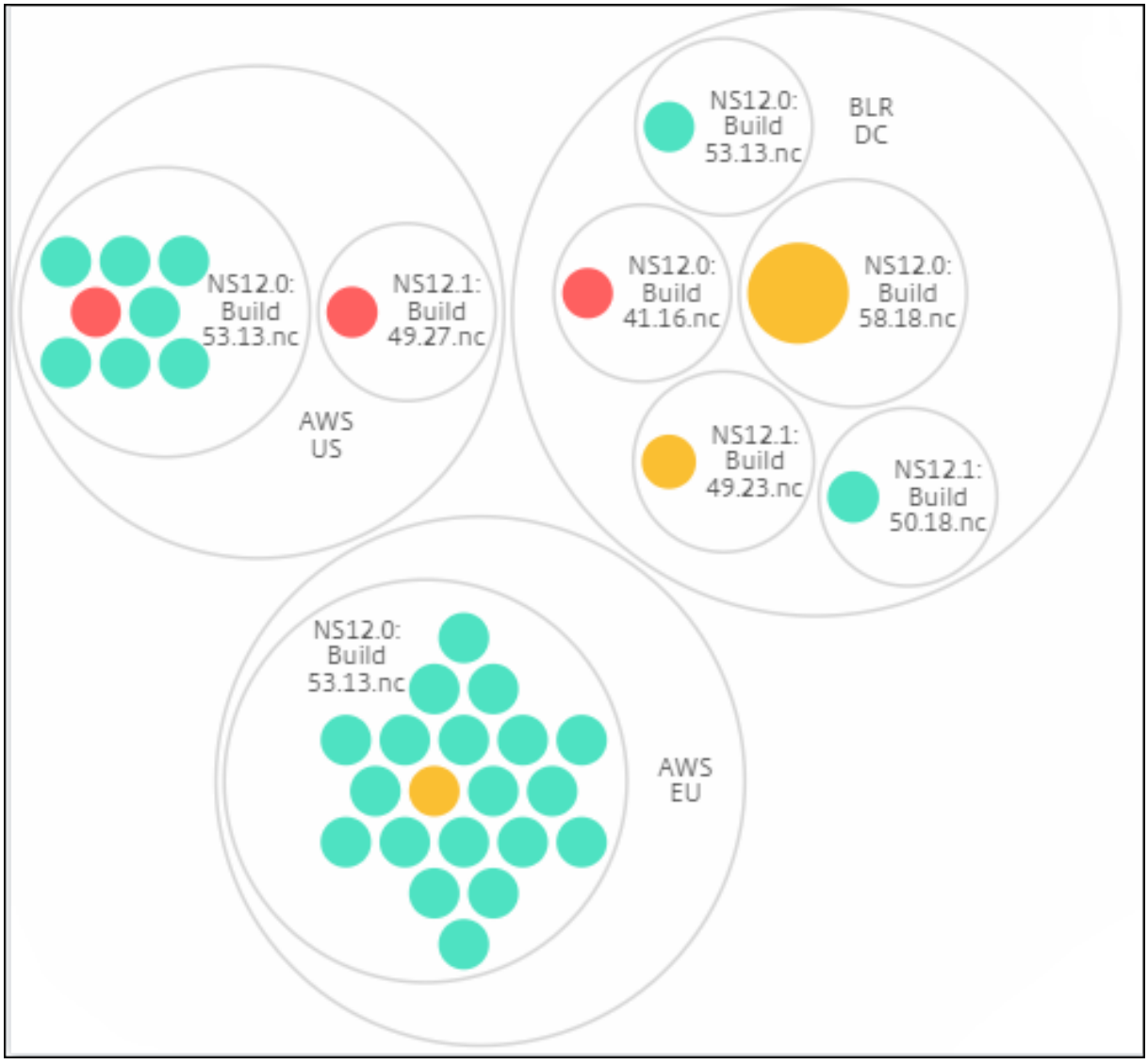
Type and version:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Site and version:

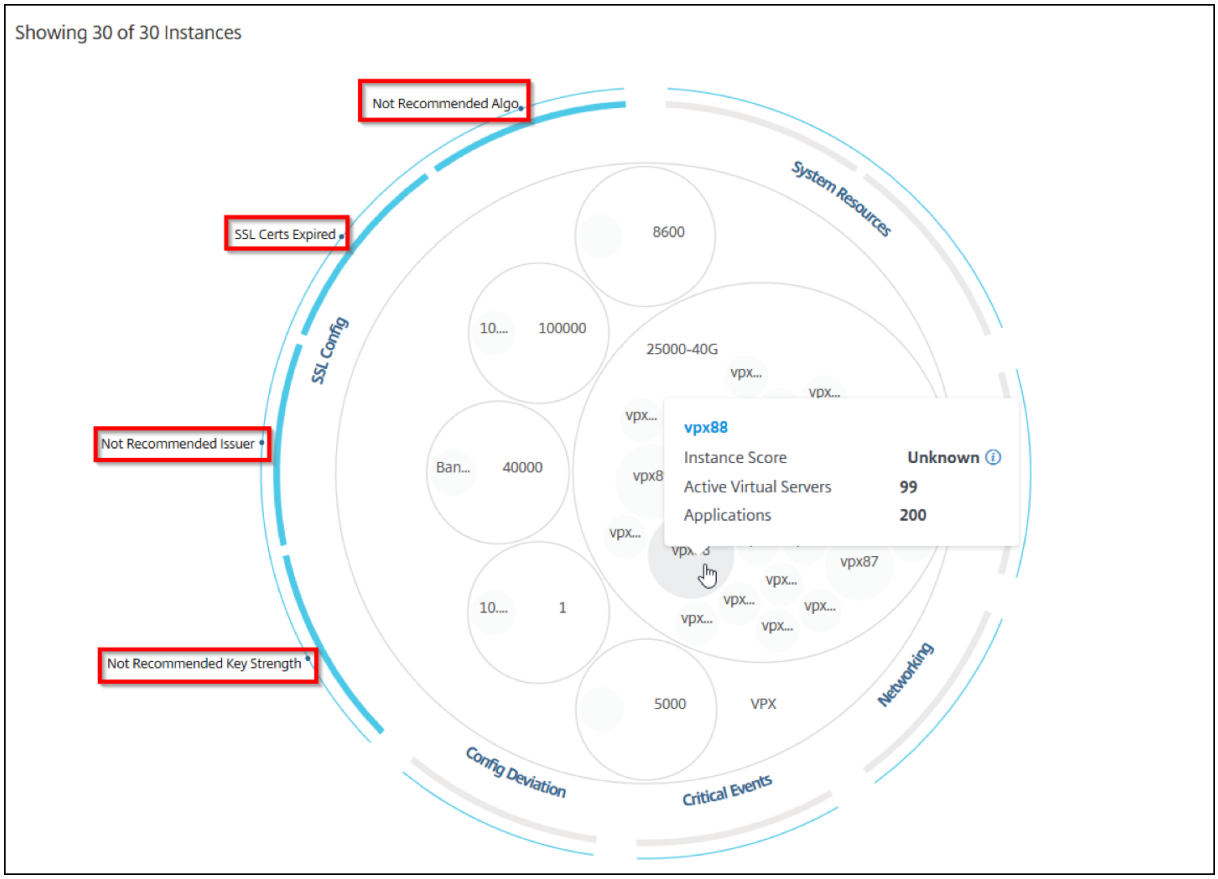
© 1997–2025 Citrix Systems, Inc. All rights reserved.



How to use Circle Pack

Click each of the colored circle to highlight that instance.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

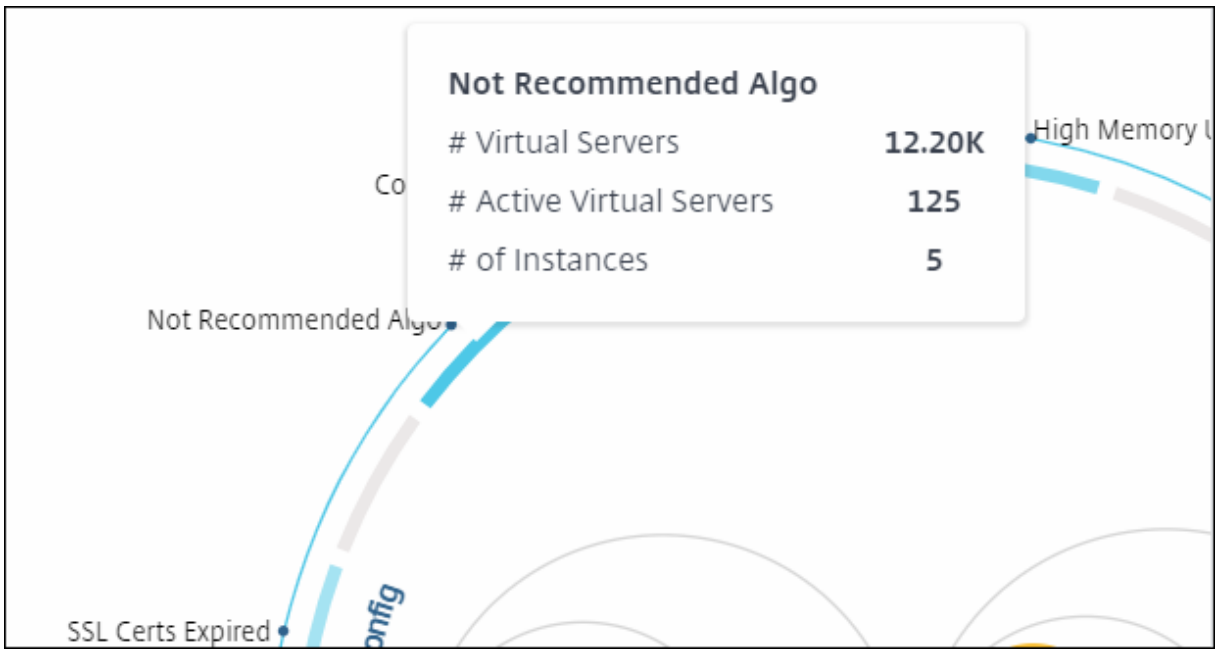


Depending on the events that have occurred in that instance, only those health indicators are highlighted on the outer circles. For example, the following two images of the Circle Pack display different sets of risk indicators, though both instances are in a critical state.



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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



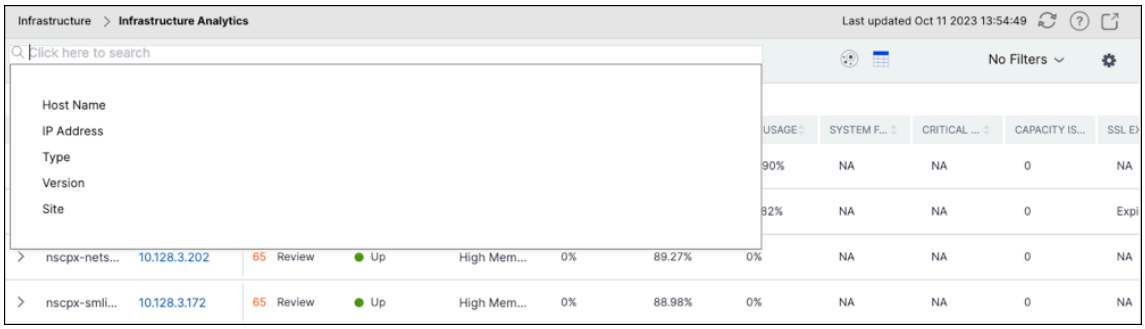
Tabular view

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



© 1997–2025 Citrix Systems, Inc. All rights reserved.

The search results work for both circle view and table view.

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:

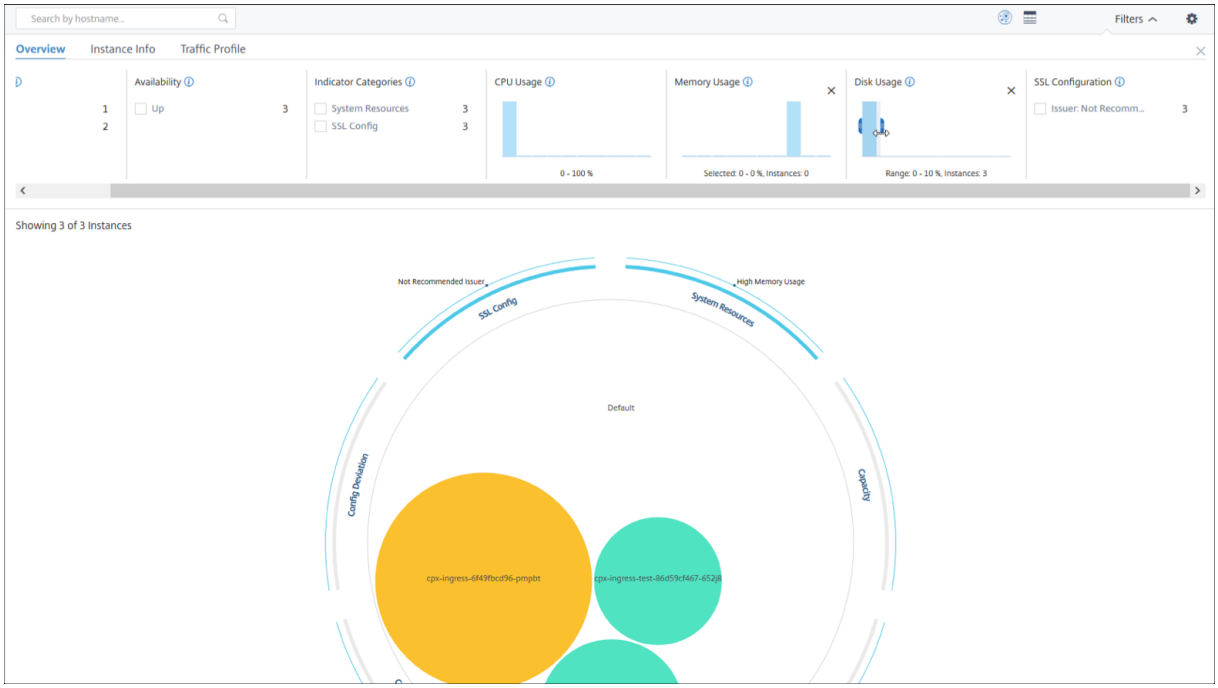
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

© 1997–2025 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.

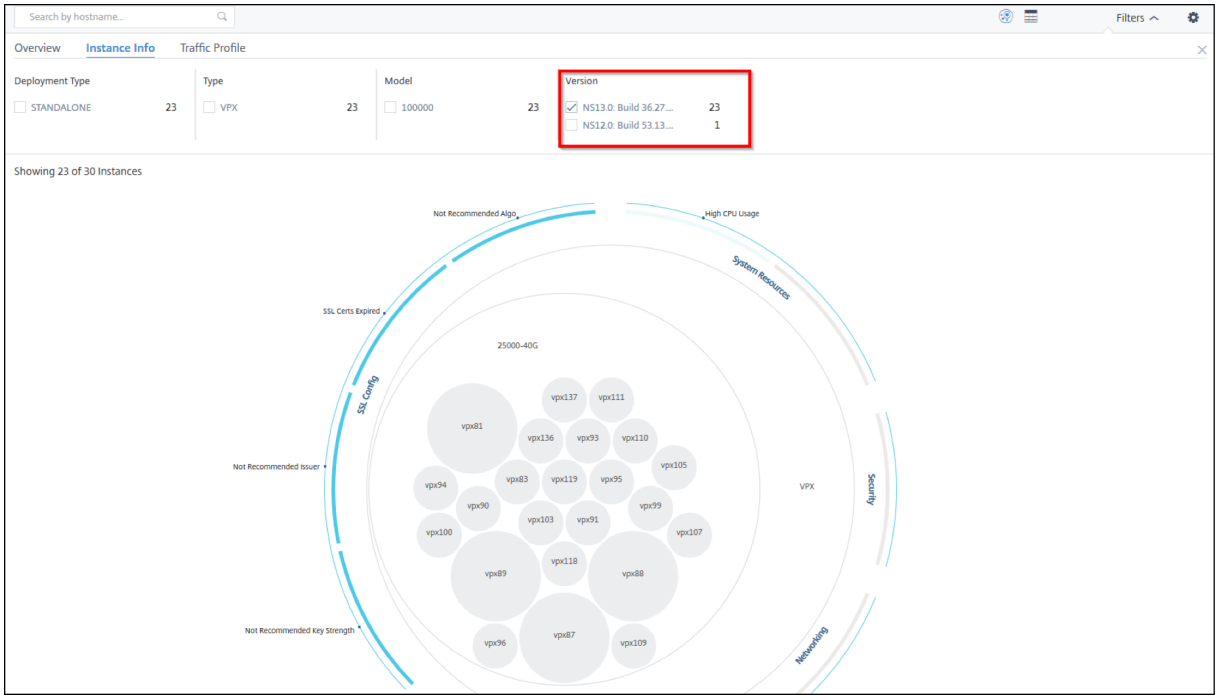
Instance info

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



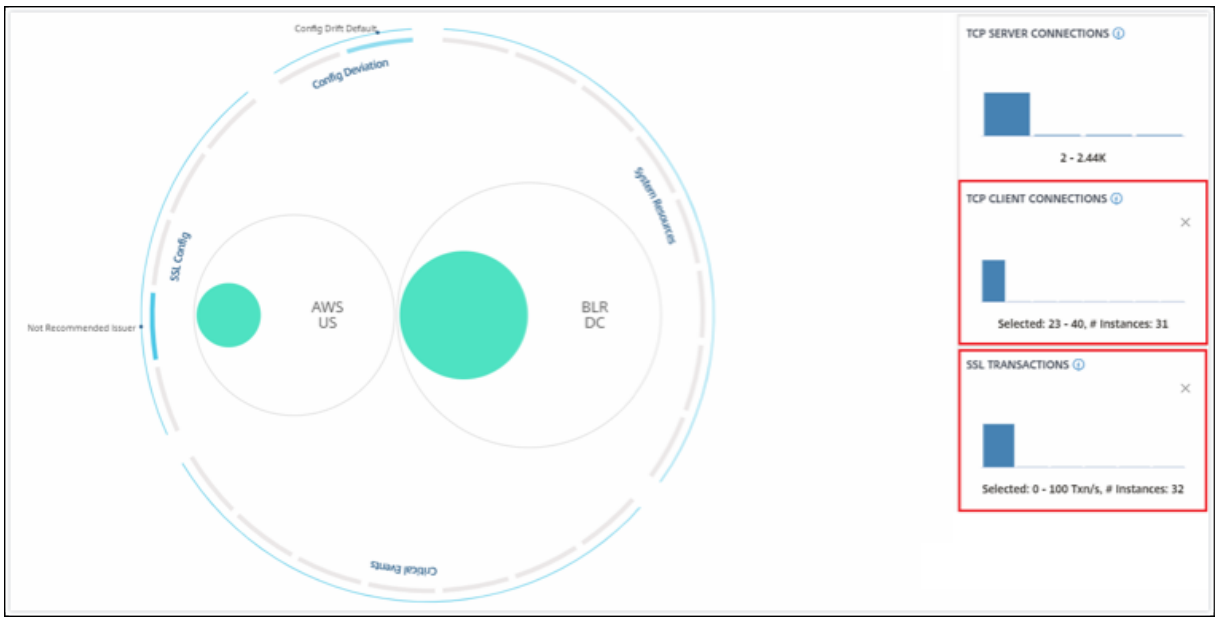
Traffic profile

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



How to use the settings panel

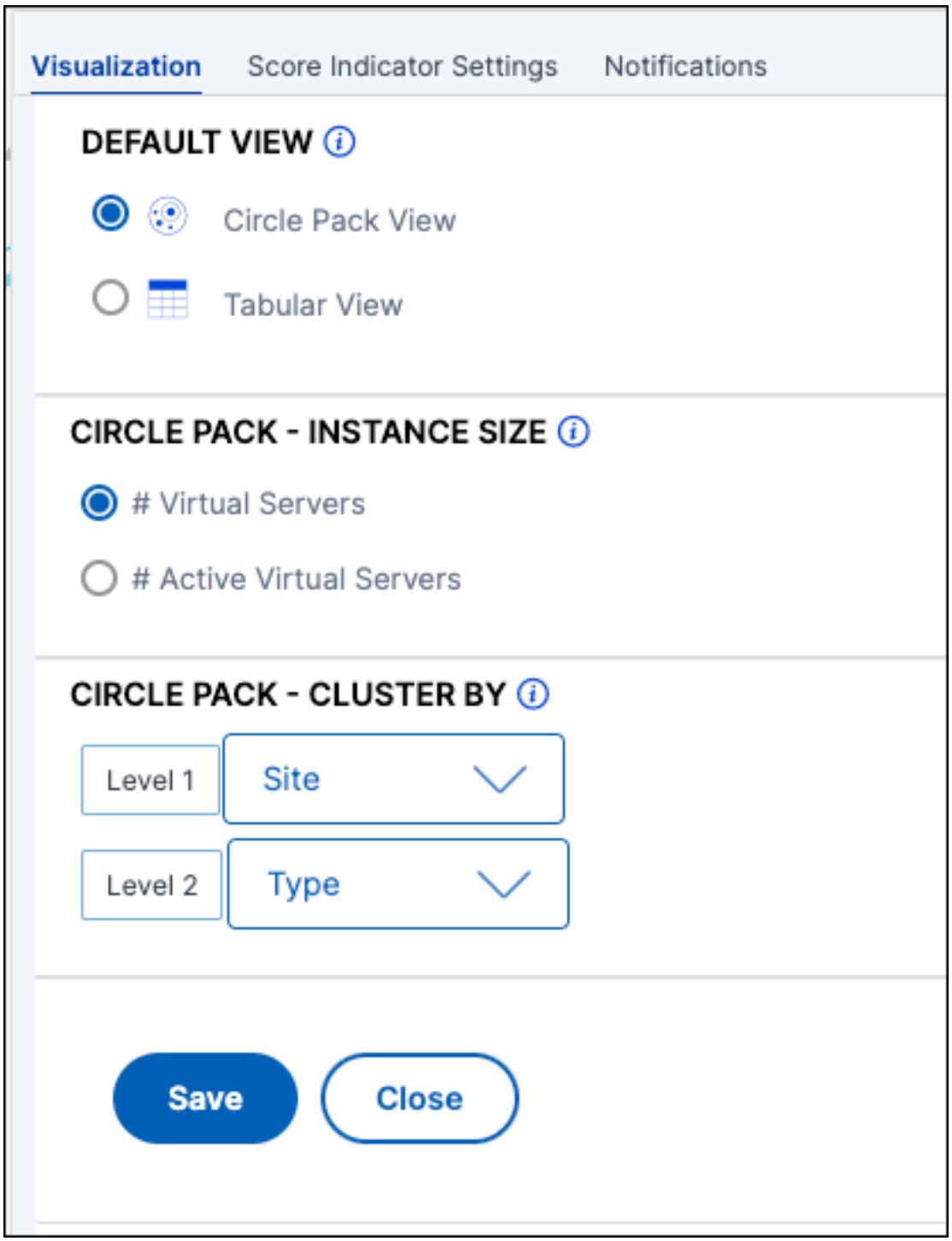
The **Settings** panel allows you to:

- 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.

© 1997–2025 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 weigh-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

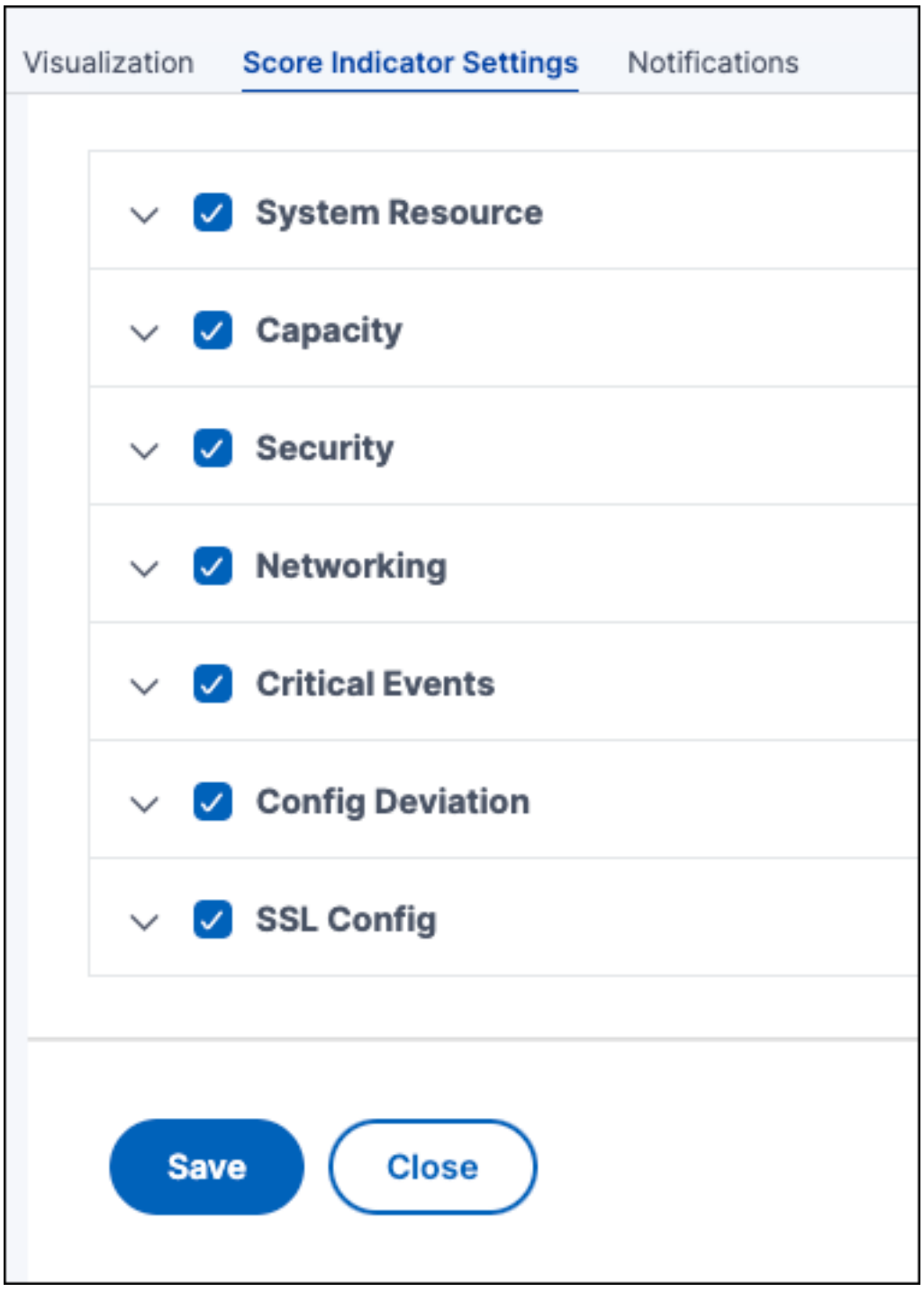
tage to determine the instance score calculation.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



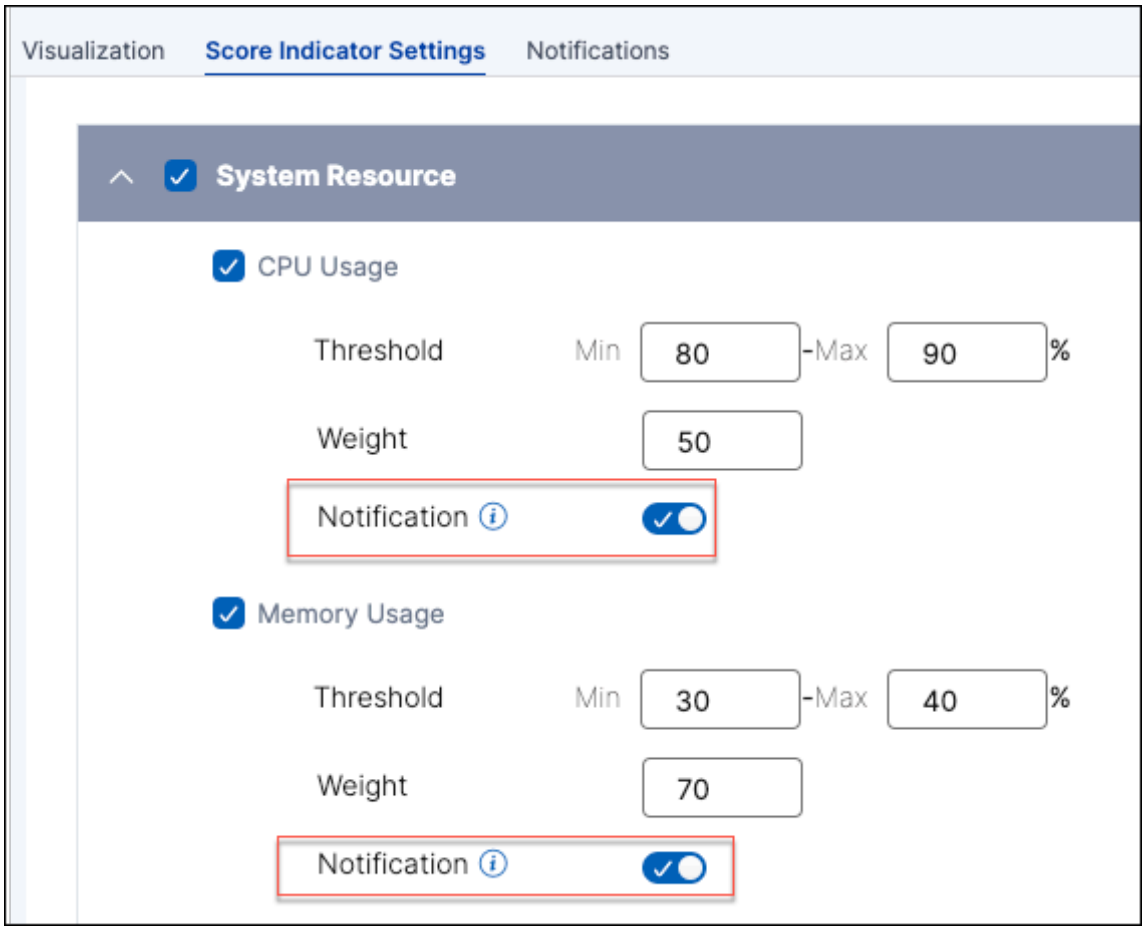
Configure notifications

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **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**.



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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

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:

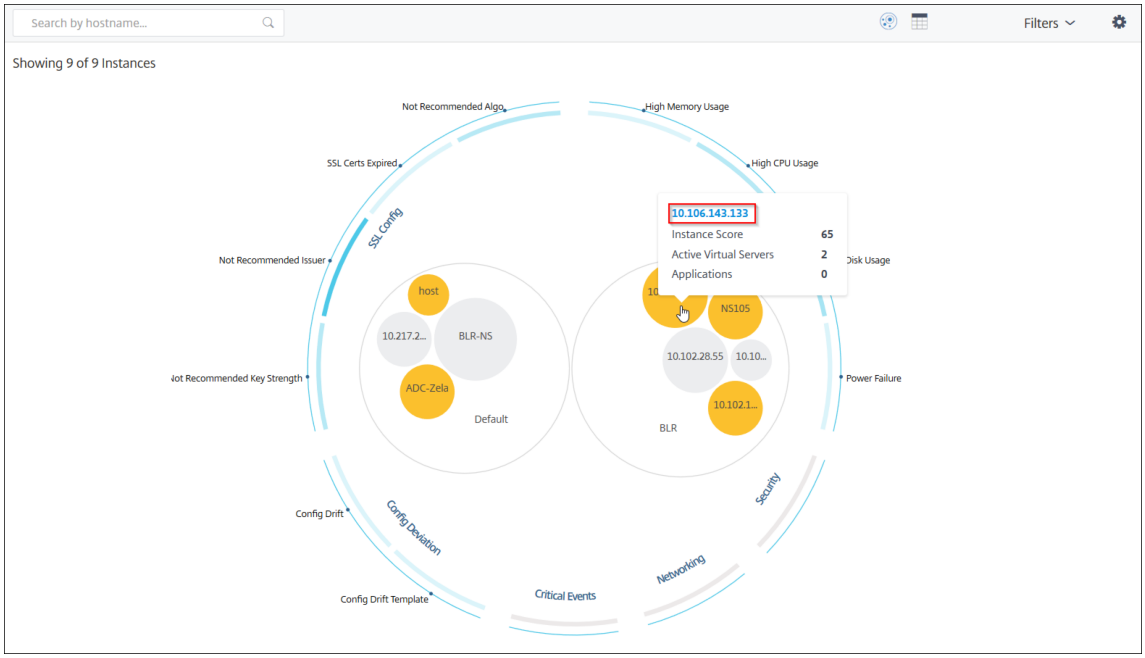
Chris also notices that another instance is in "Review"state and that there has been a config deviation recently. When he clicks the config deviation risk indicator, he notices that RC4 Cipher, SSL v3, TLS 1.0, and TLS 1.1 related configuration changes have been made which might be due to security concerns. 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

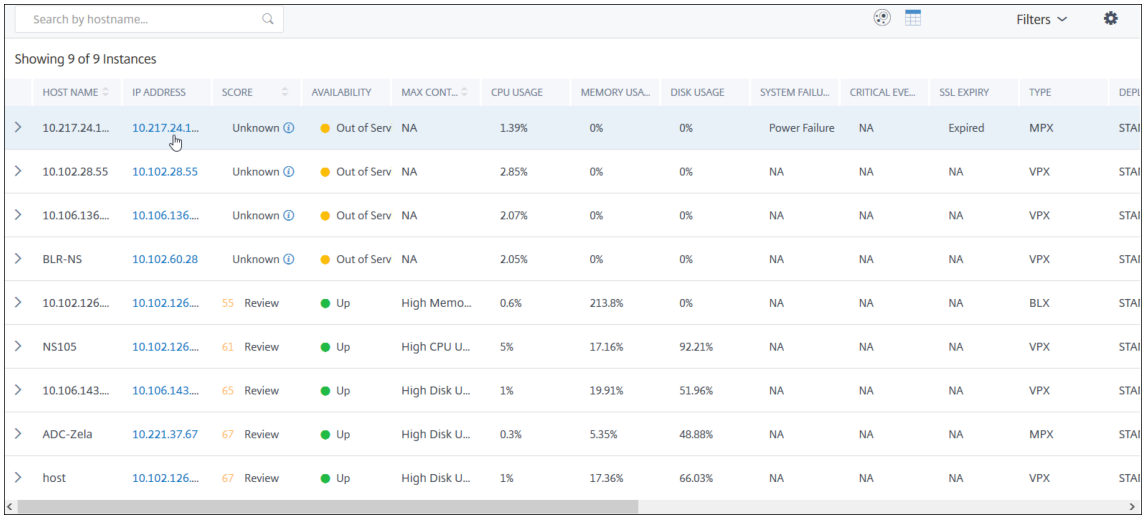
January 8, 2024

1. Navigate to **Infrastructure > Infrastructure Analytics**.
2. Click the circle pack view and select the IP address.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



You can also click an IP address from the table view.



- **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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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
- **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.

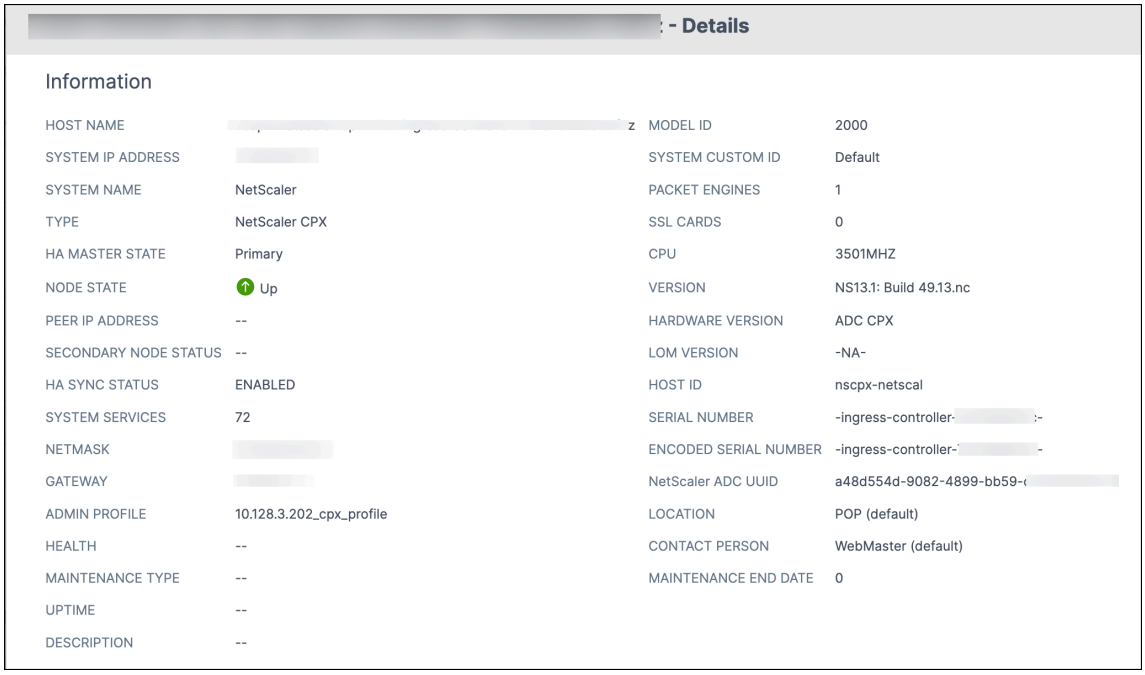
Click an IP address and in the page that appears, click **Instance Details** to view the instance details.



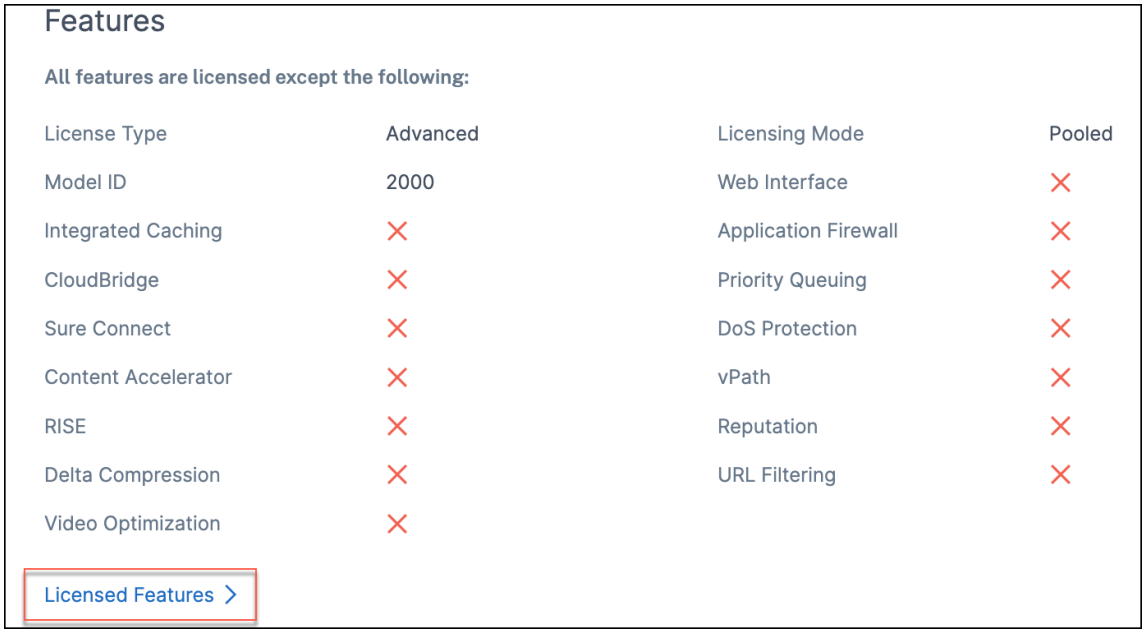
The following details are displayed:

- **Information** - Instance details such as instance type, deployment type, version, model, and so on.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

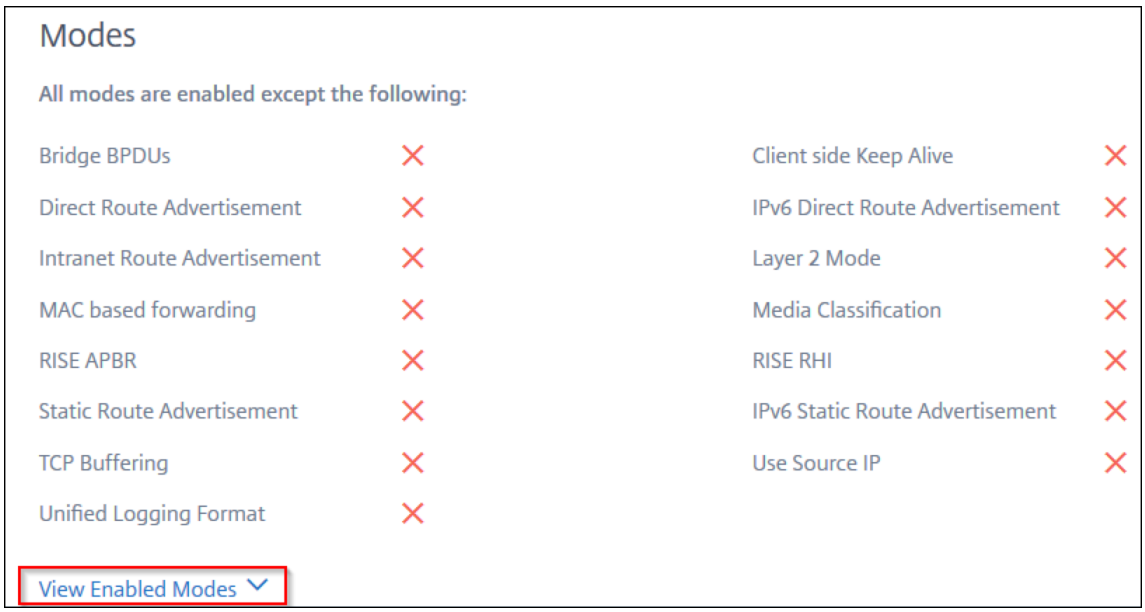


- **Features** –By default, the features that are not licensed are displayed. Click **Licensed Features** to view the features that are licensed.



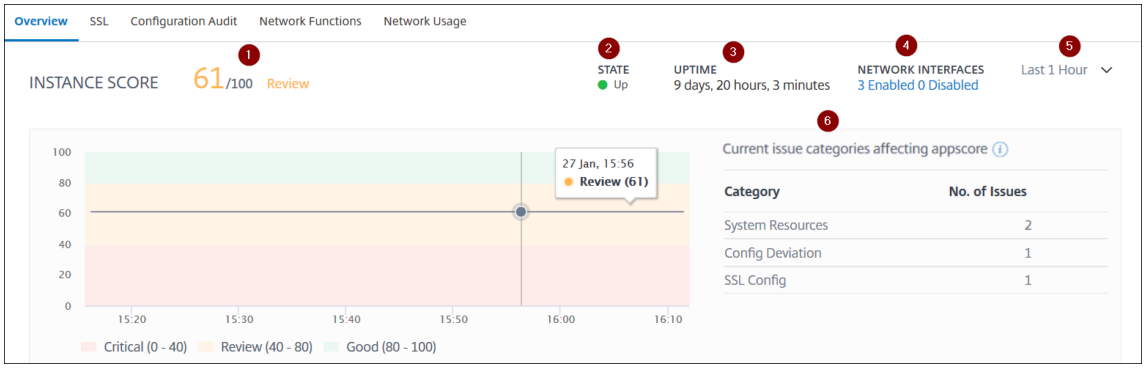
- **Modes** –By default, all modes that are disabled on the instance are displayed. Click **View Enabled Modes** to view the enabled modes on the instance.

© 1997–2025 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 **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.

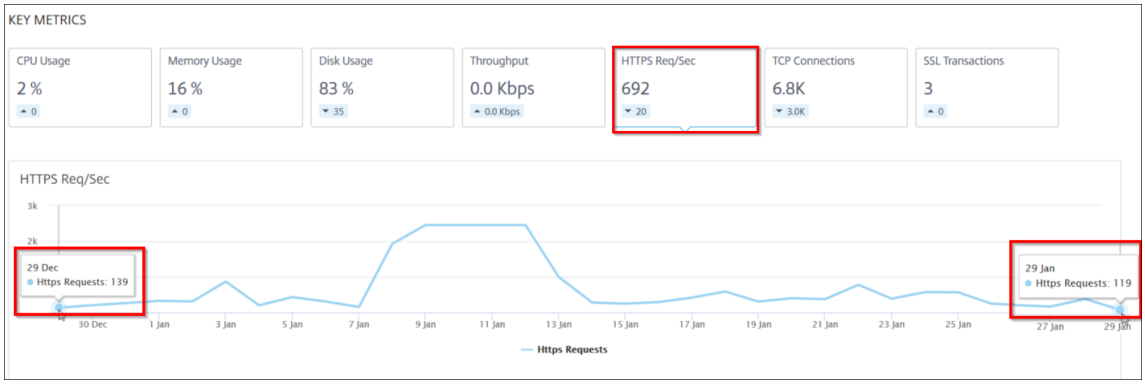
6 –Displays the total issues and issue category of the NetScaler instance.

- **Key Metrics**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.



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:

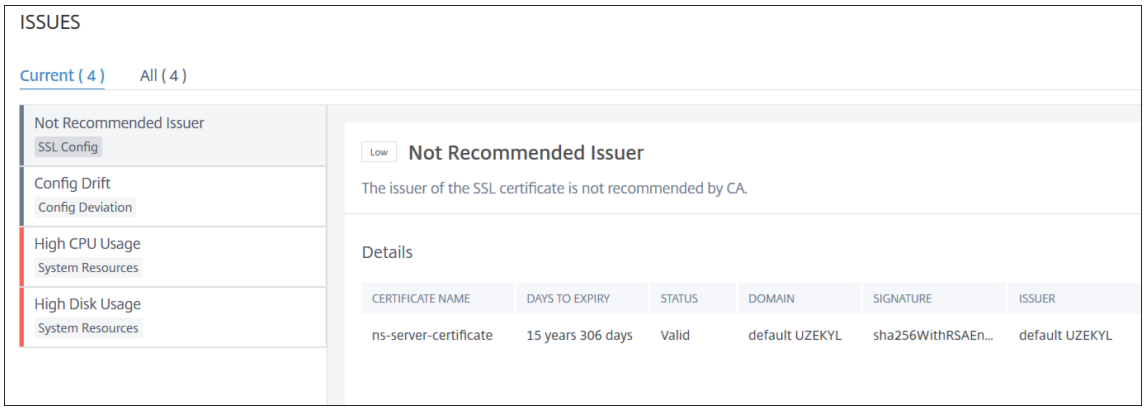
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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
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 – HA Sync Failure – HA Version Mismatch

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Issue Category	Description	Issues
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
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 issues that are currently affecting the instance score.
- The **All** tab displays all infra issues detected for the selected duration.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

View the capacity issues in an NetScaler instance

January 8, 2024

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.

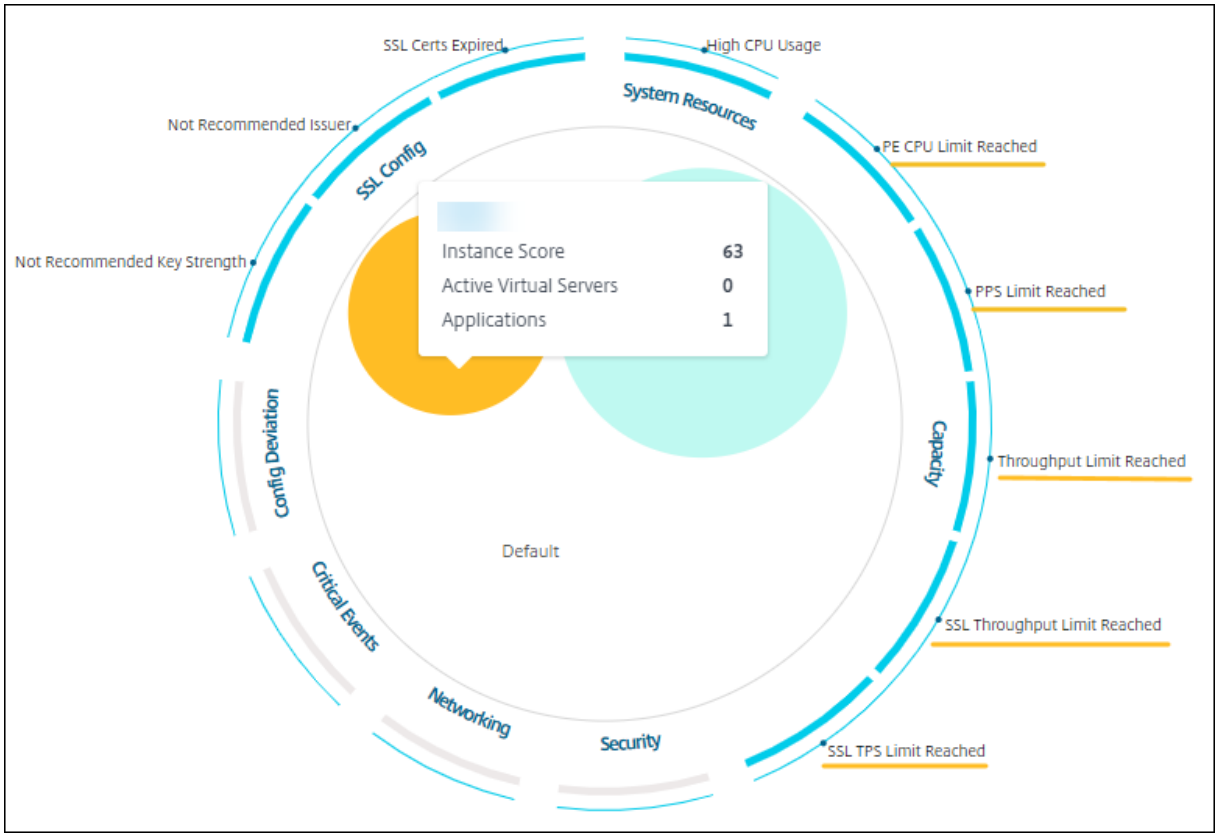
In the **Circle Pack View**, you can view the NetScaler instance capacity issues if exists.

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:



The issues are categorized on the following capacity parameters:

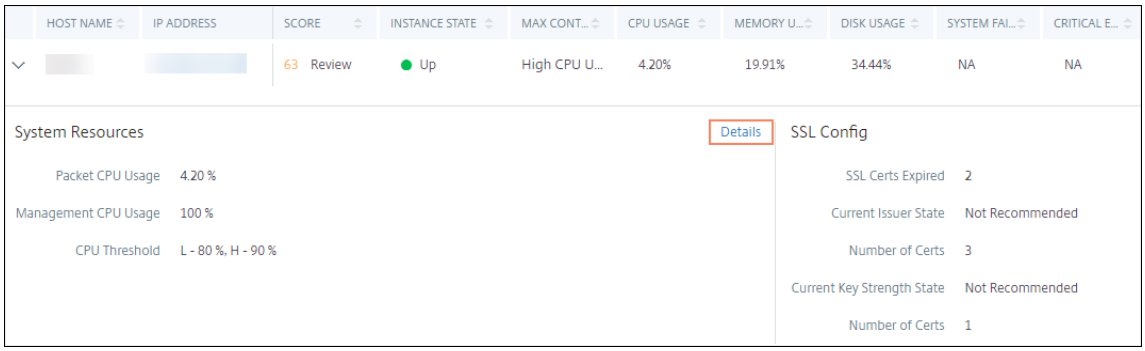
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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

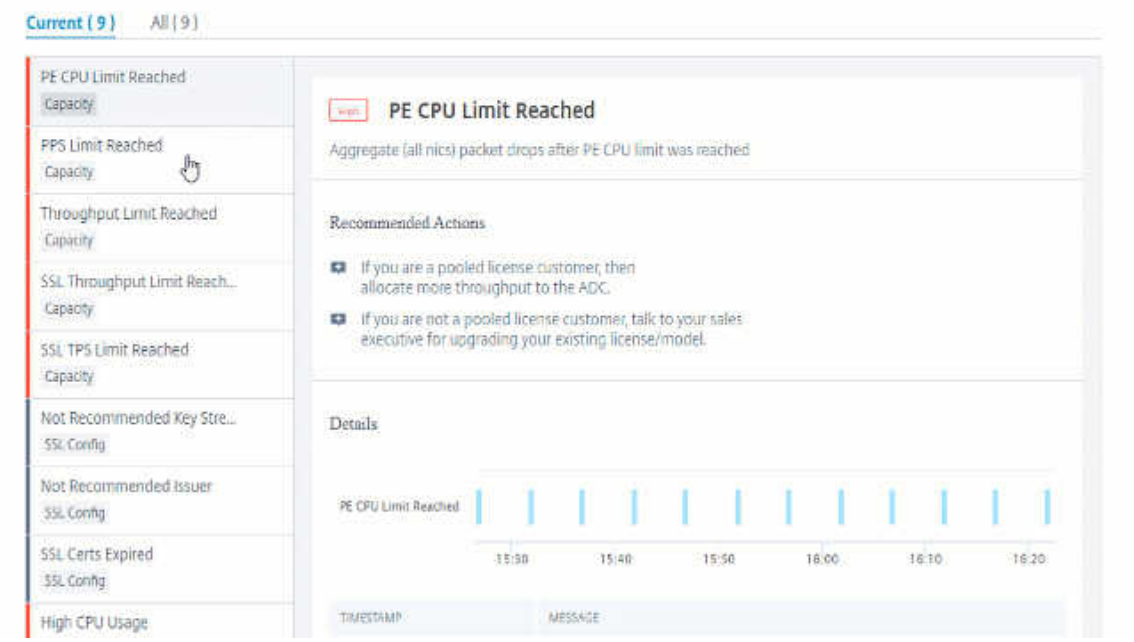
The NetScaler Console recommends actions that can solve capacity issues. To view the recommended actions, perform the following steps:

1. In **Infrastructure > Infrastructure Analytics**, select the tabular view.
2. Select the instance that has capacity issues and click **Details**.



3. In the instance page, scroll down to the **Issues** section.
4. Select each issue and view the recommended actions to resolve capacity issues.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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**.

Enhanced Infrastructure Analytics with new indicators

January 8, 2024

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

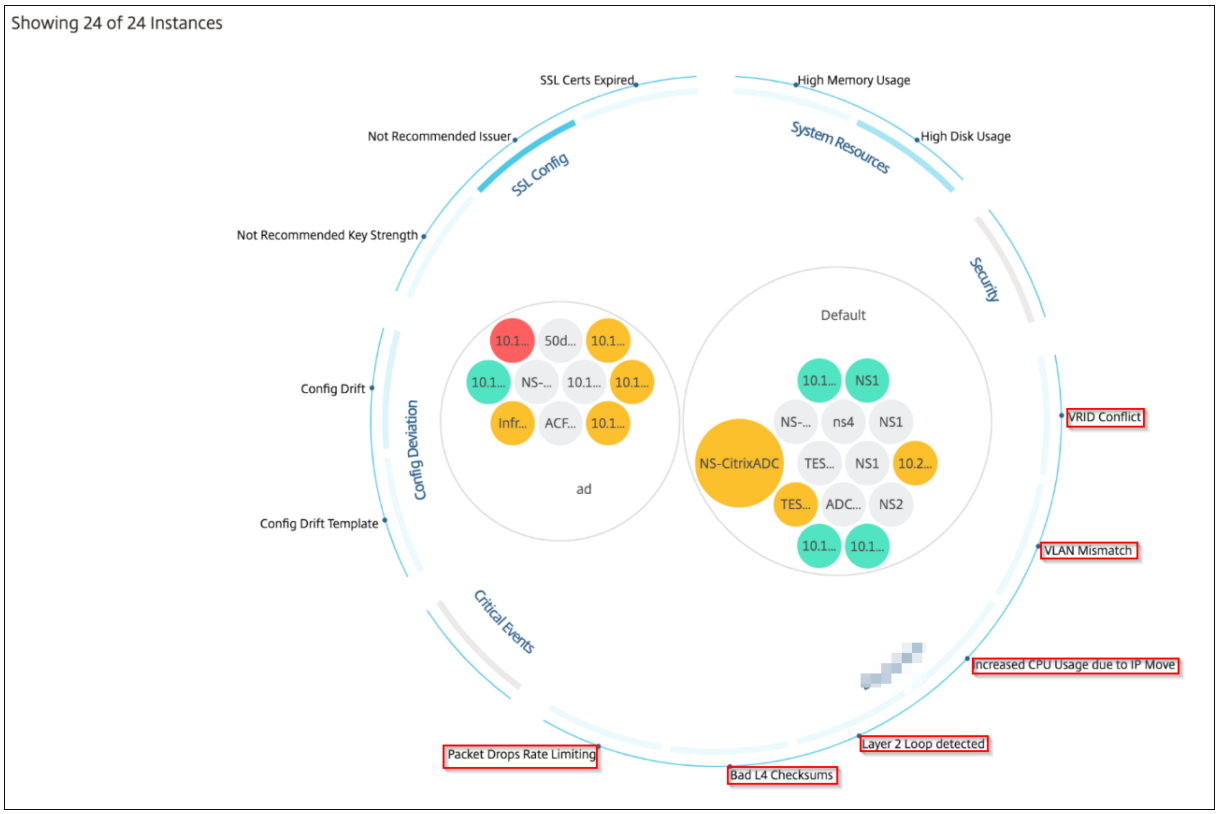
> **Note:**
>
> Rule indicators are not supported for:
>
> - NetScaler instances configured in a cluster mode.
> - NetScaler instances configured with admin partitions.

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.
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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

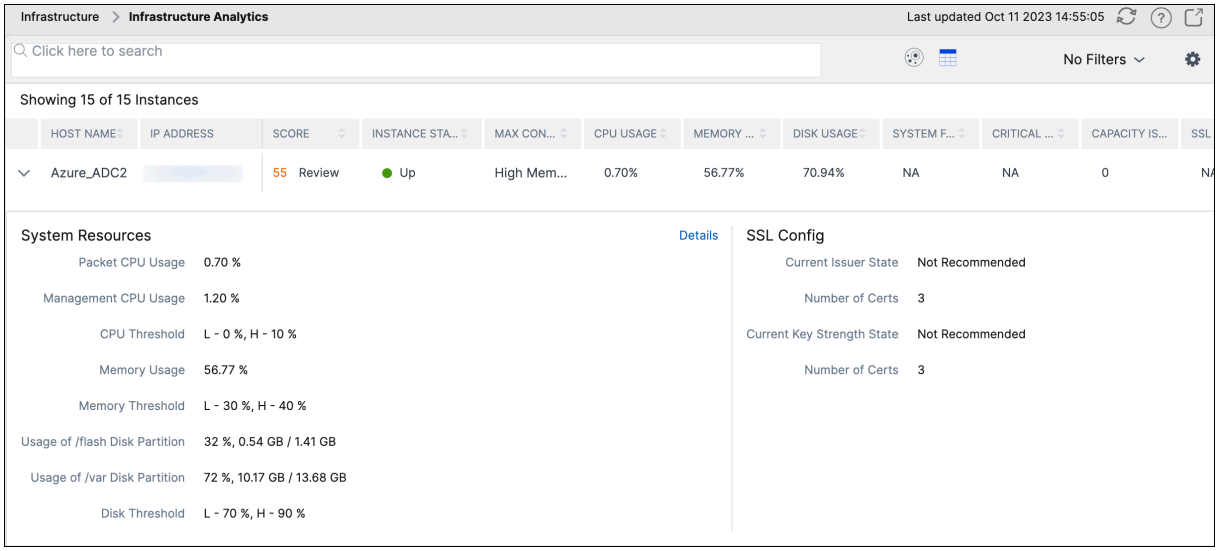
Indicator name in Infrastructure Analytics	Description
Bad L4 checksums	Detects when checksum validation for TCP packets is failed.
Increased CPU usage due to IP move	Detects if a large number of macs need to be updated.
Excessive packet steering	Detects high levels of software packet steering due to 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.



Tabular view

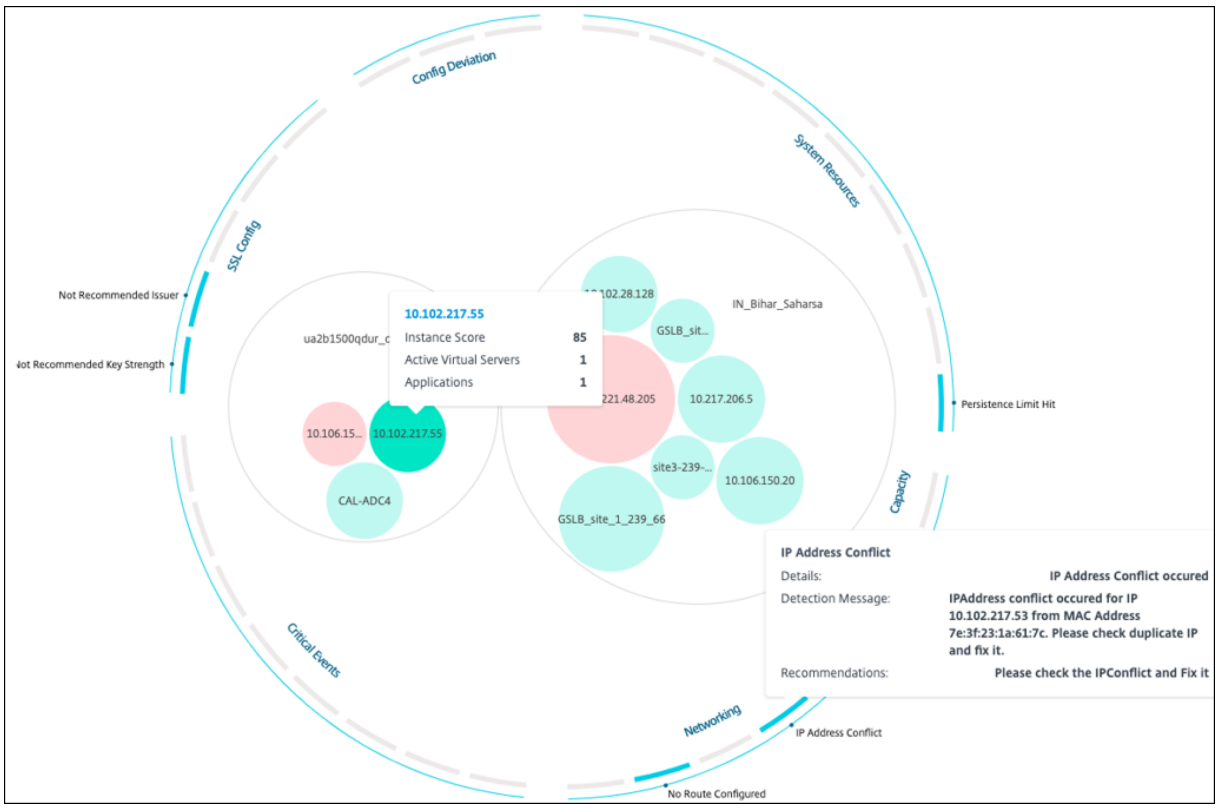
You can also view anomalies using the tabular view option in **Infrastructure Analytics**. Navigate to **Infrastructure > Infrastructure Analytics** and then click to display all managed instances. Click › to expand for details.

© 1997–2025 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Recommendations** - Indicates the troubleshooting procedure to resolve this IP address conflict

Instance management

September 8, 2025

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.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 **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

May 20, 2024

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

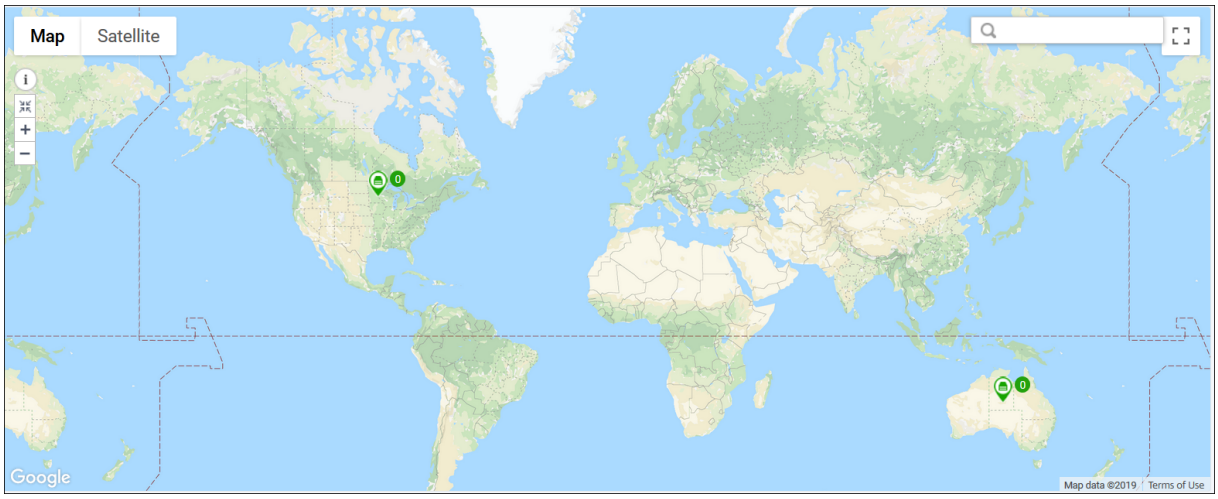
Monitoring globally distributed sites in NetScaler Console

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.

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.

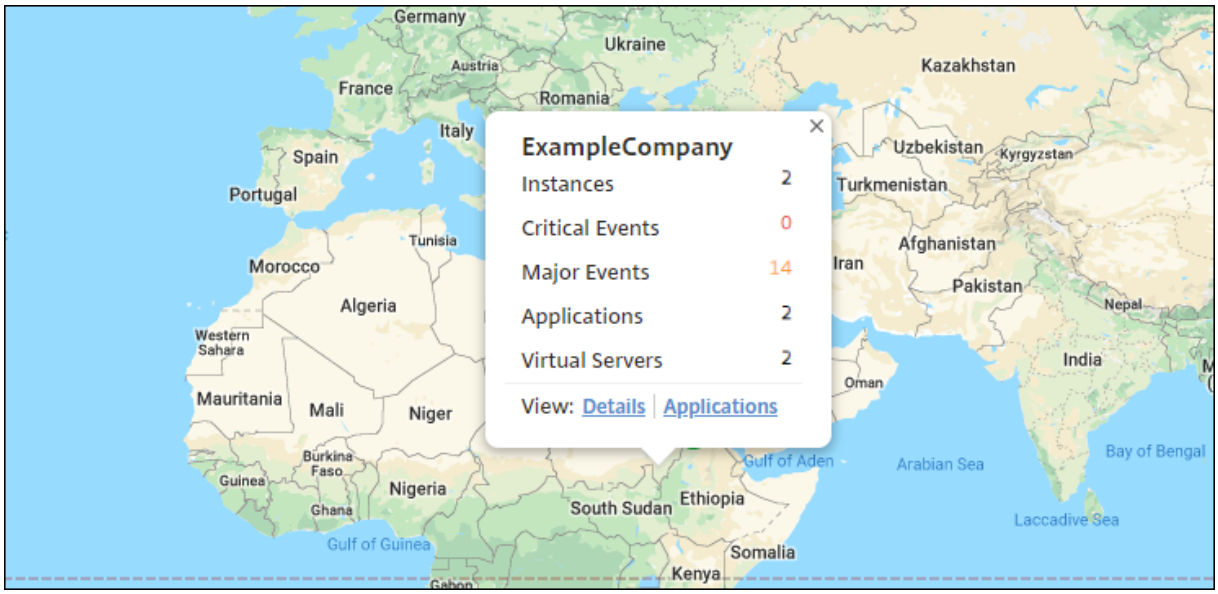


The markers also display the count of the following components on the site:

- **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Major Events**: Indicates that the count of major events occurred on the instances.

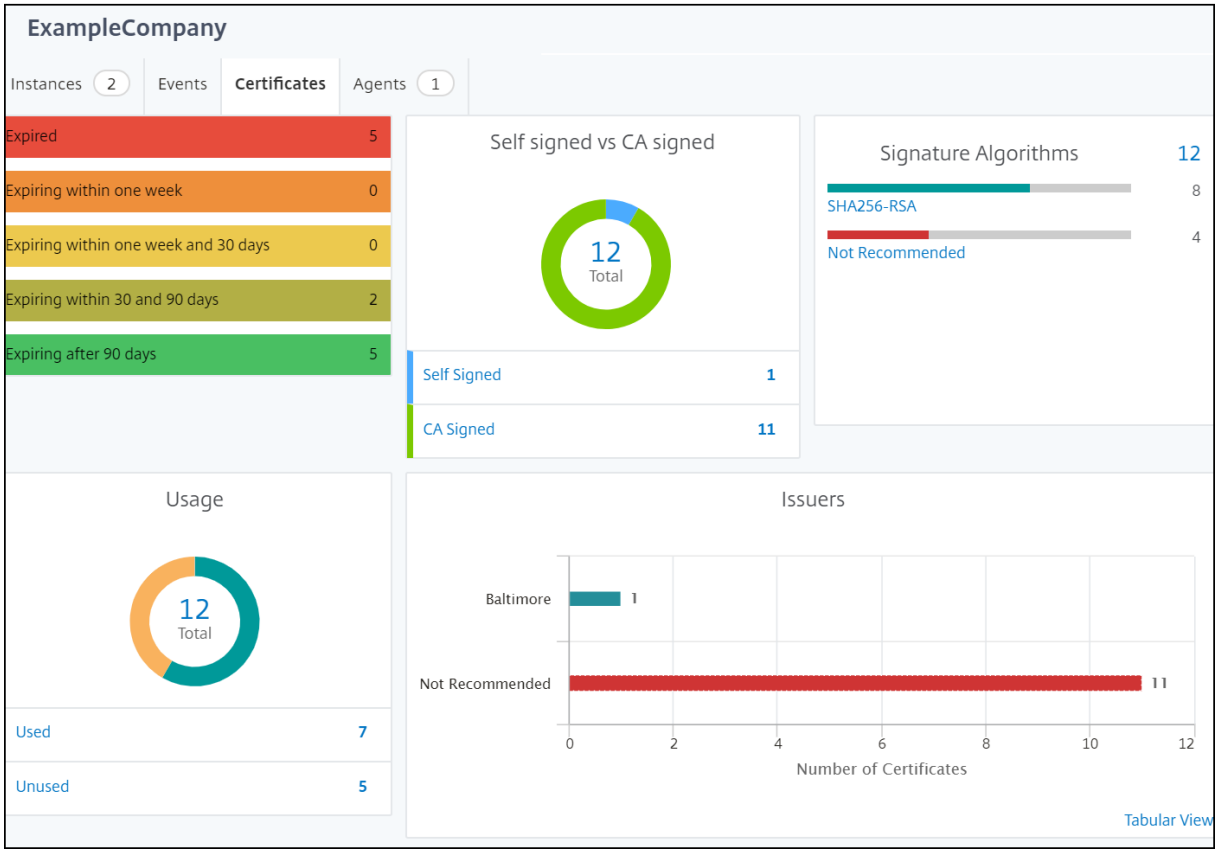


Click **Applications** to see all custom applications created in each site.

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.

© 1997–2025 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

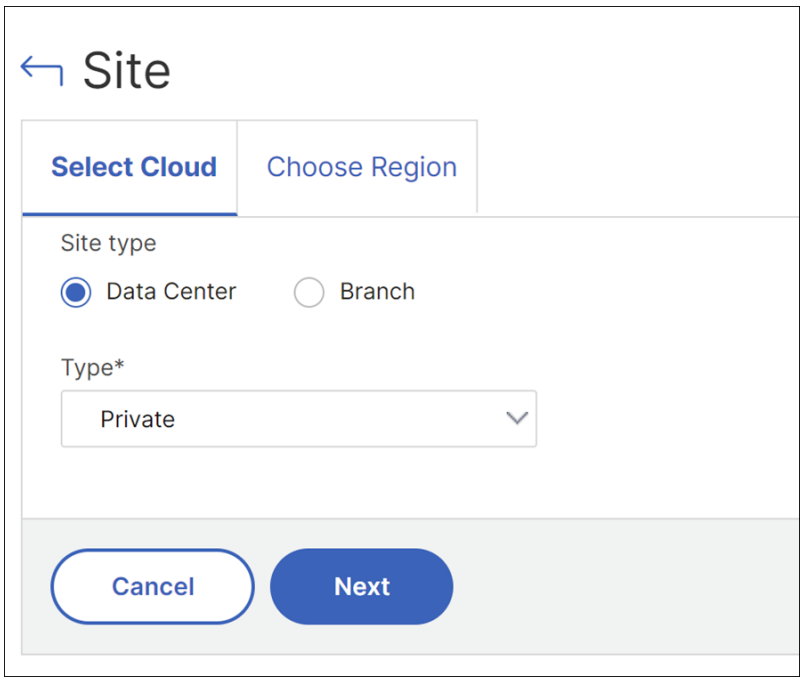
Create sites before you add instances in NetScaler Console. Providing location information allows you to precisely locate the site.

To create a site:

1. Navigate to **Infrastructure > Instances > Site**. Click **Add**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

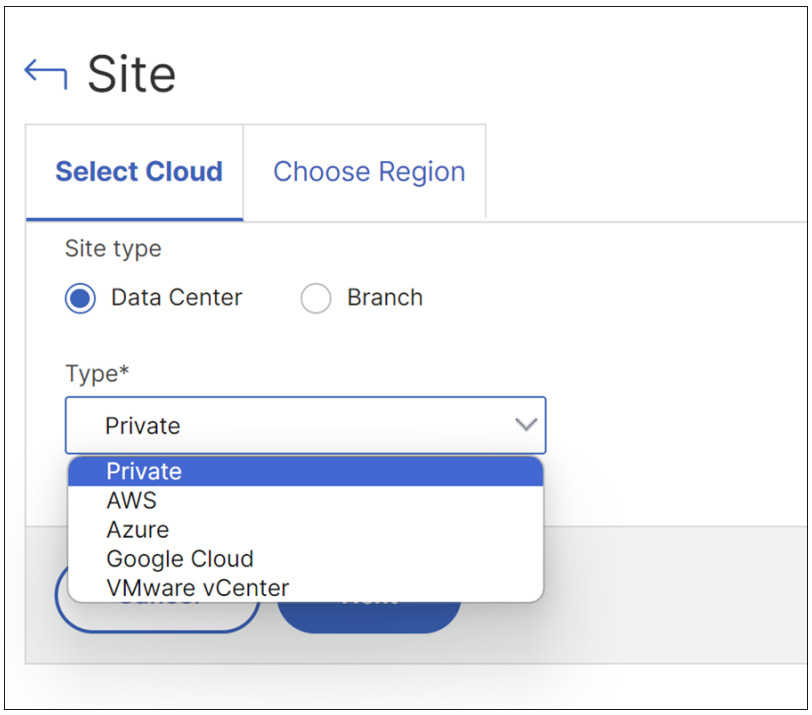
2. On the **Select Cloud** tab, choose the **Site type**. You can create a site of type **Data Center** or **Branch**.



For Data Center site type, select the **Type** from the list:

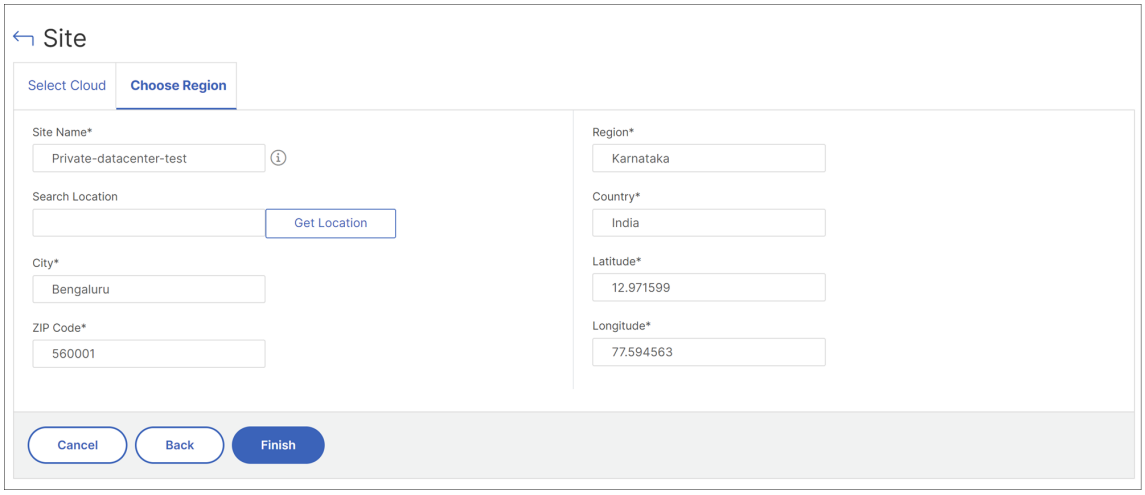
- Private
- AWS
- Azure
- Google Cloud
- VMware vCenter

© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. Click **Next**.
4. On the **Choose Region** tab, enter the following details:

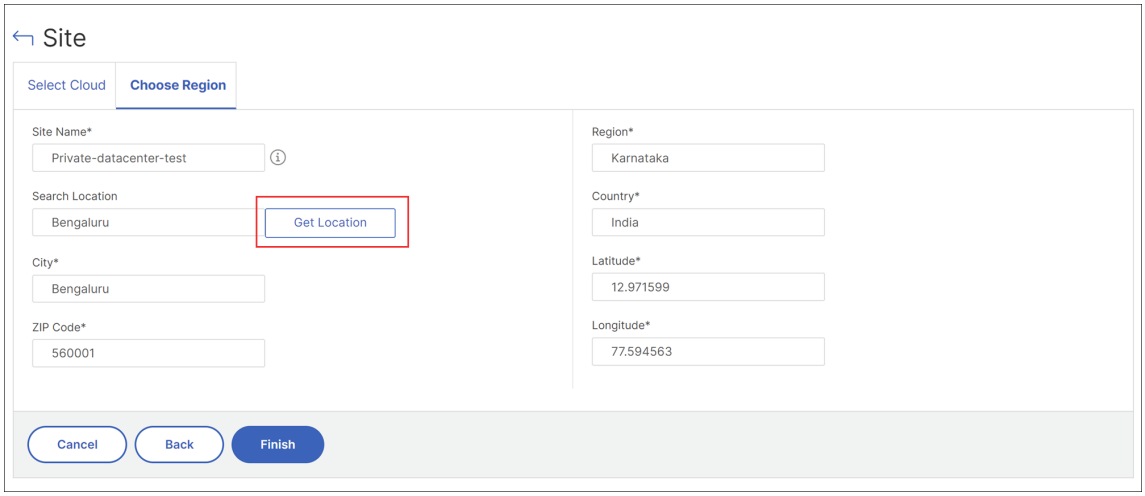
    - Site Name
    - City
    - Zip Code
    - Region
    - Country
    - Latitude
    - Longitude



Alternatively, you can enter the location in **Search Location** and click **Get Location** to precisely

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

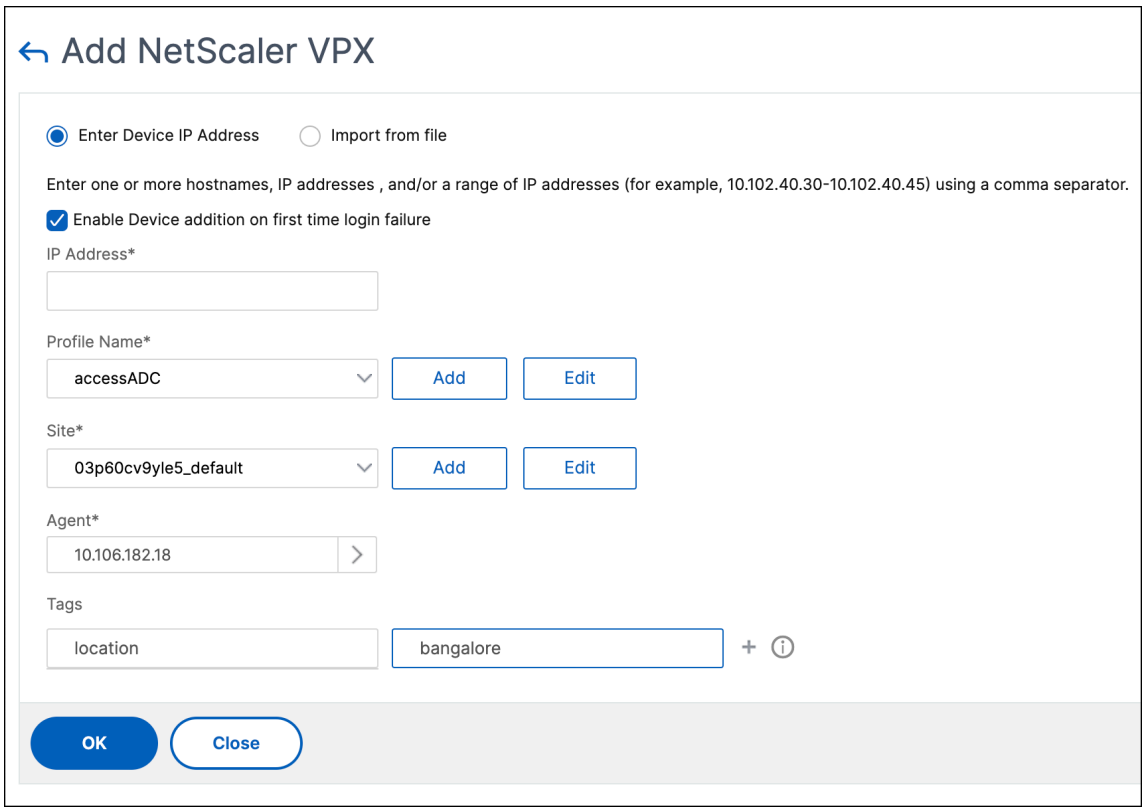
1. To delete a site, select the site and click **Delete**.
2. On the Confirm page, click **Yes**.

To add instances and select sites:

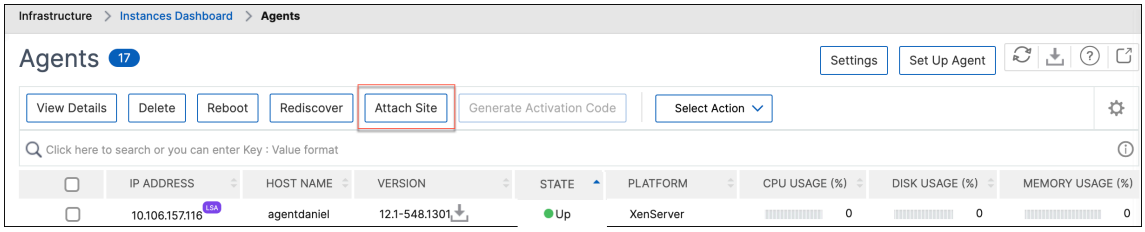
After creating sites, you must add instances in NetScaler Console. You can select the previously created site, or you can also create a site and associate the instance.

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.

© 1997–2025 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**.

© 1997–2025 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

January 8, 2024

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.

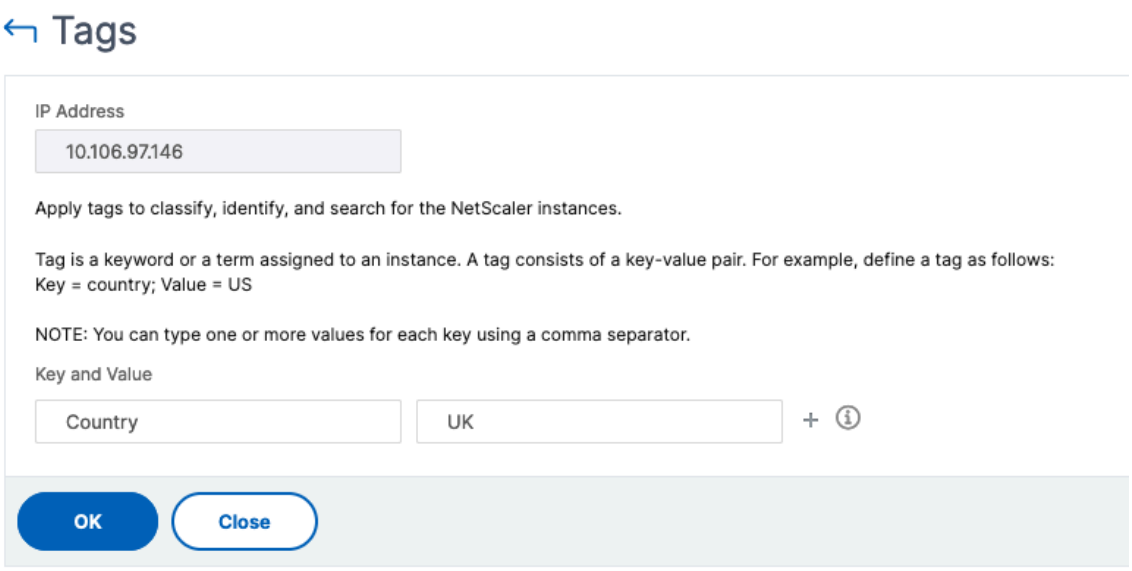
- **Use case 1**: You can create a tag to identify all instances that are located in the United Kingdom. Here, you can create a tag with the key as "Country"and the value as "UK."This tag helps you to search and monitor all those instances that are located in the UK.
- **Use case 2**: You want to search 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.
- **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.

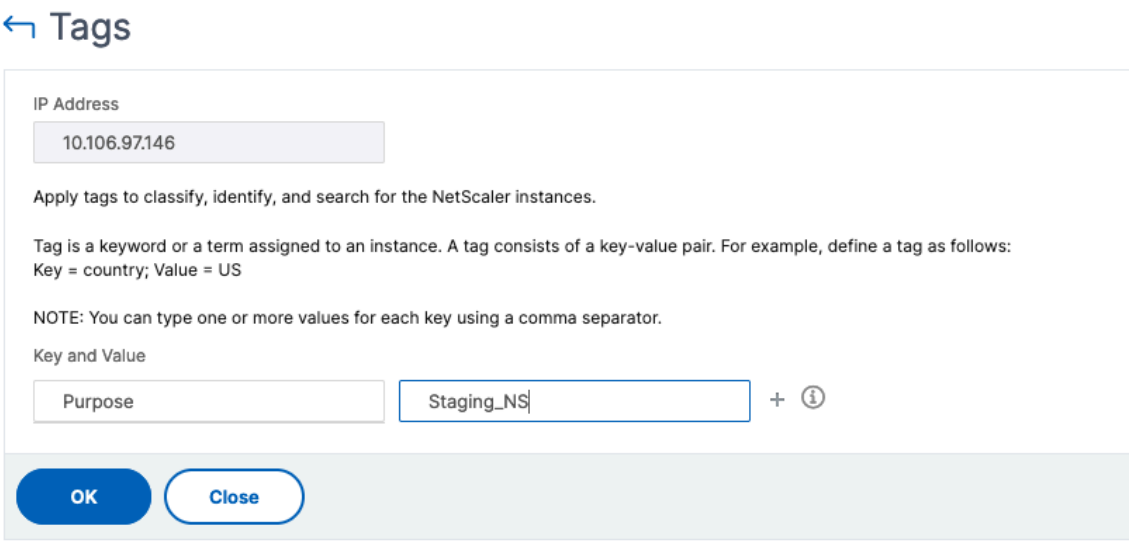
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

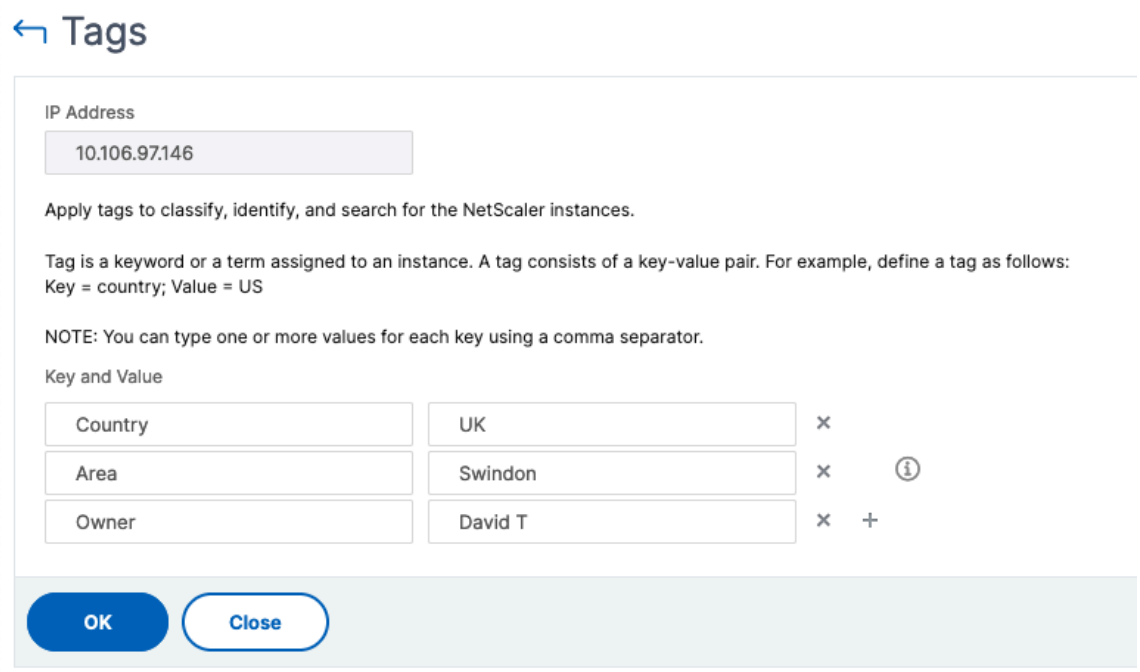
   For example, the following images show a few keywords created and their values. You can add your own keywords and type a value for each keyword.





© 1997–2025 Citrix Systems, Inc. All rights reserved.

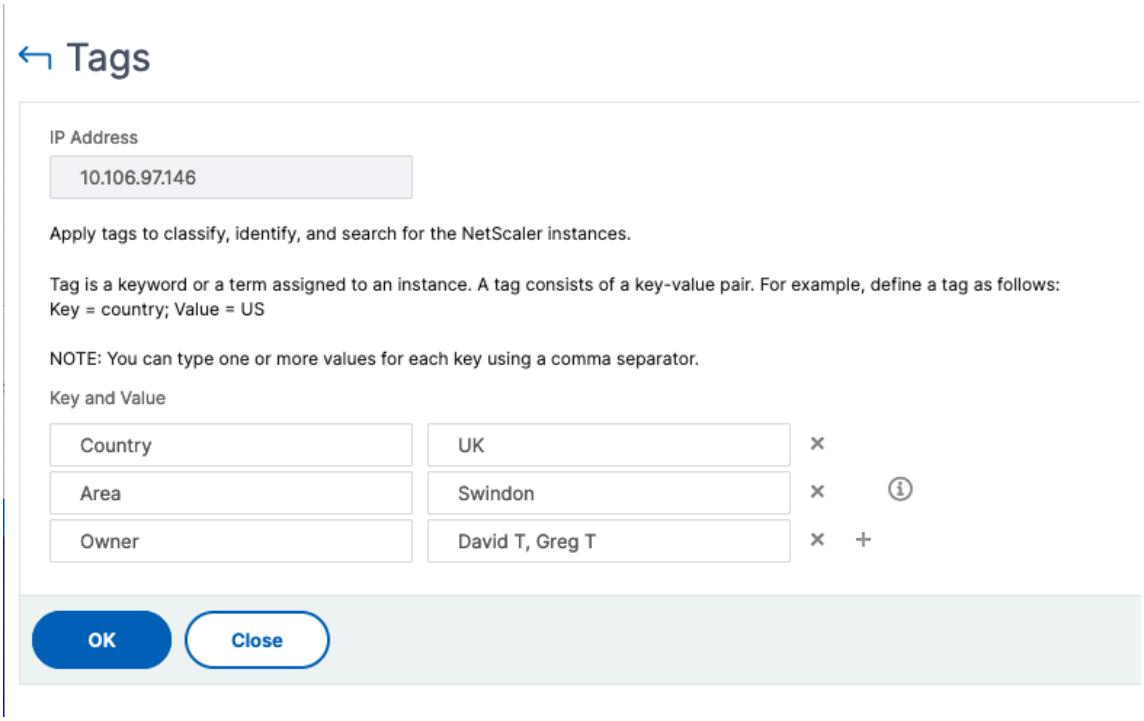
You can also add multiple tags by clicking "+". Adding multiple and meaningful tags allows you to efficiently search for the instances.



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.

© 1997–2025 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

January 8, 2024

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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 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.

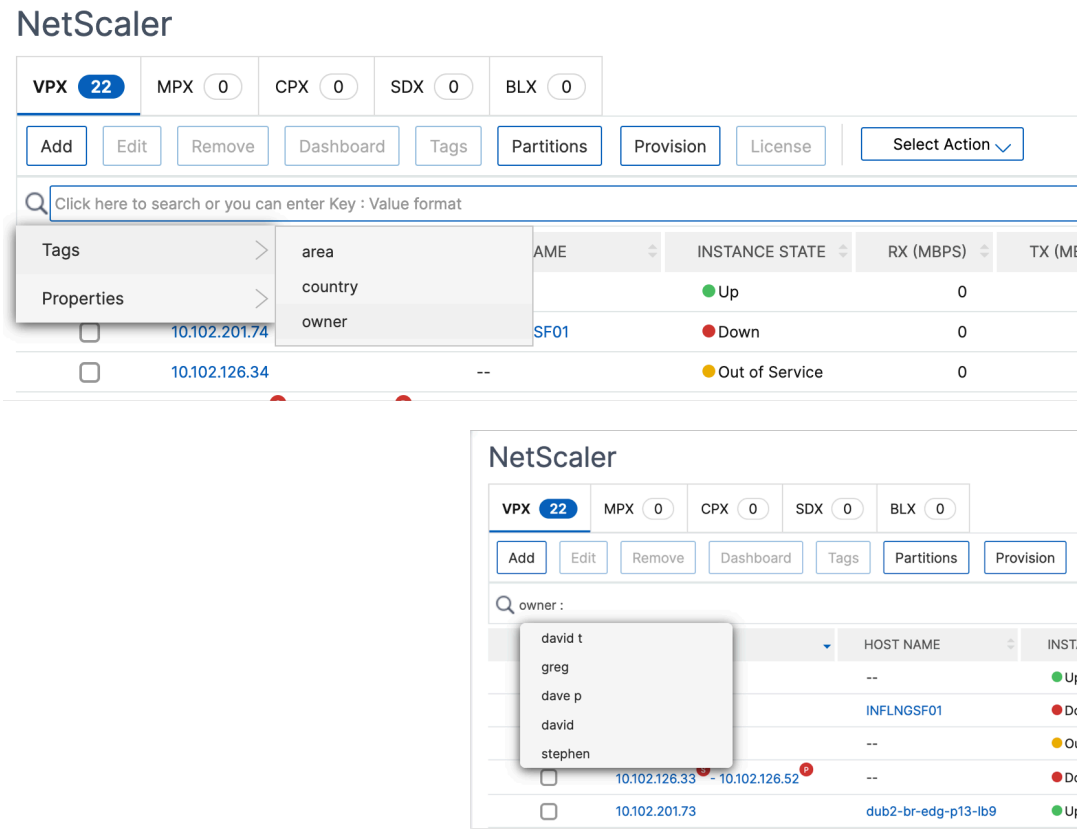
To search for NetScaler VPX instances

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.

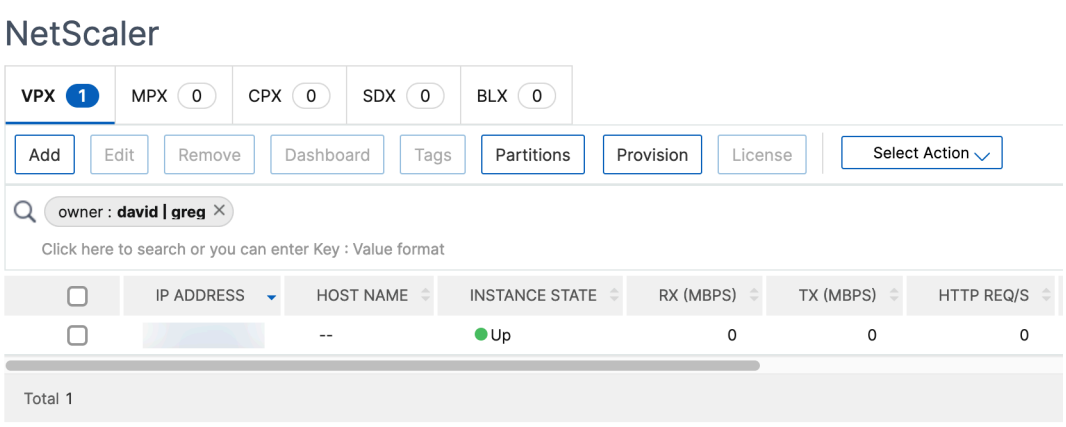
   a) Select **Tags** option and select **Owner**. Select "David T".

© 1997–2025 Citrix Systems, Inc. All rights reserved.



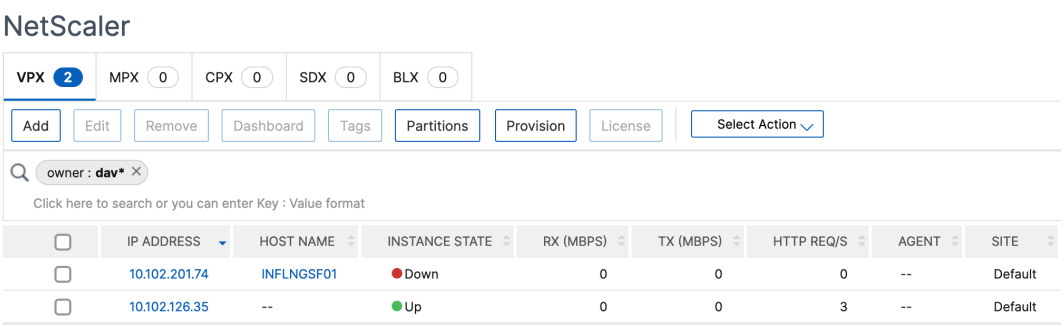
NetScaler Console supports regular expressions and wildcard characters in the search expressions.

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".

© 1997–2025 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

May 29, 2025

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.

© 1997–2025 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.

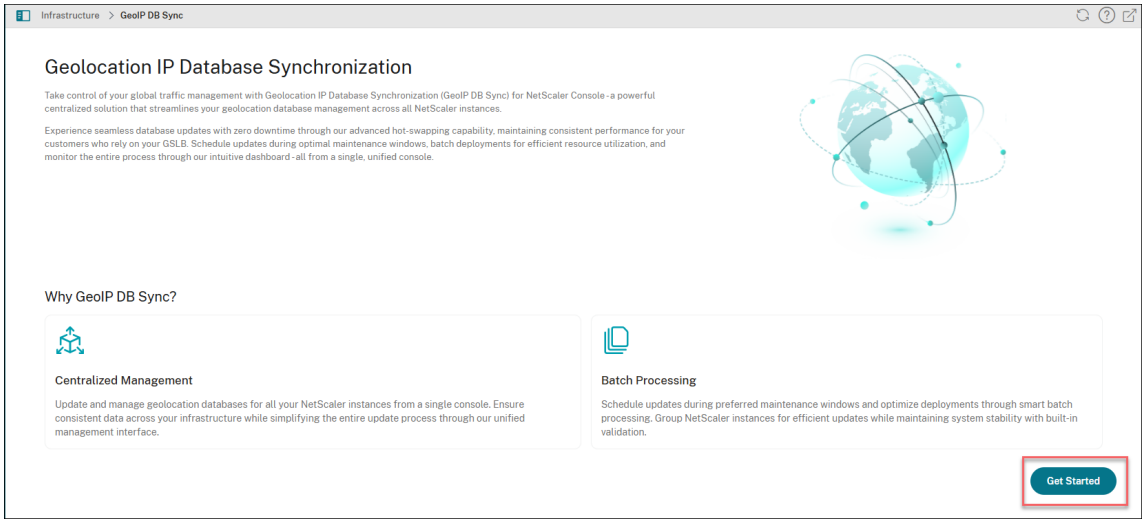
Configuring centralized GeoIP DB Updates through NetScaler Console

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.

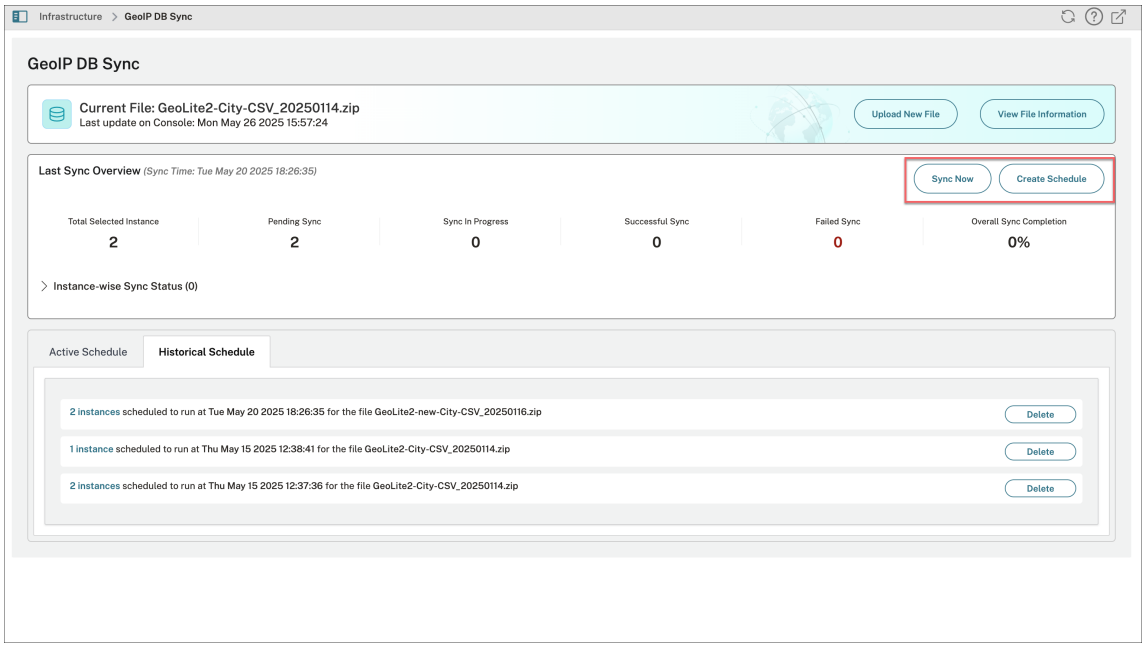
> **Notes:**
>
> - If you are uploading the GeoIP DB file for the first time, you do not see the **Appliance** option. Only if the file is already uploaded, then the **Appliance** option appears during subsequent uploads.
> - If you upload a MaxMind file, the NetScaler Console service automatically converts the file to the format that NetScaler recommends during the upload. If you upload a

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 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.

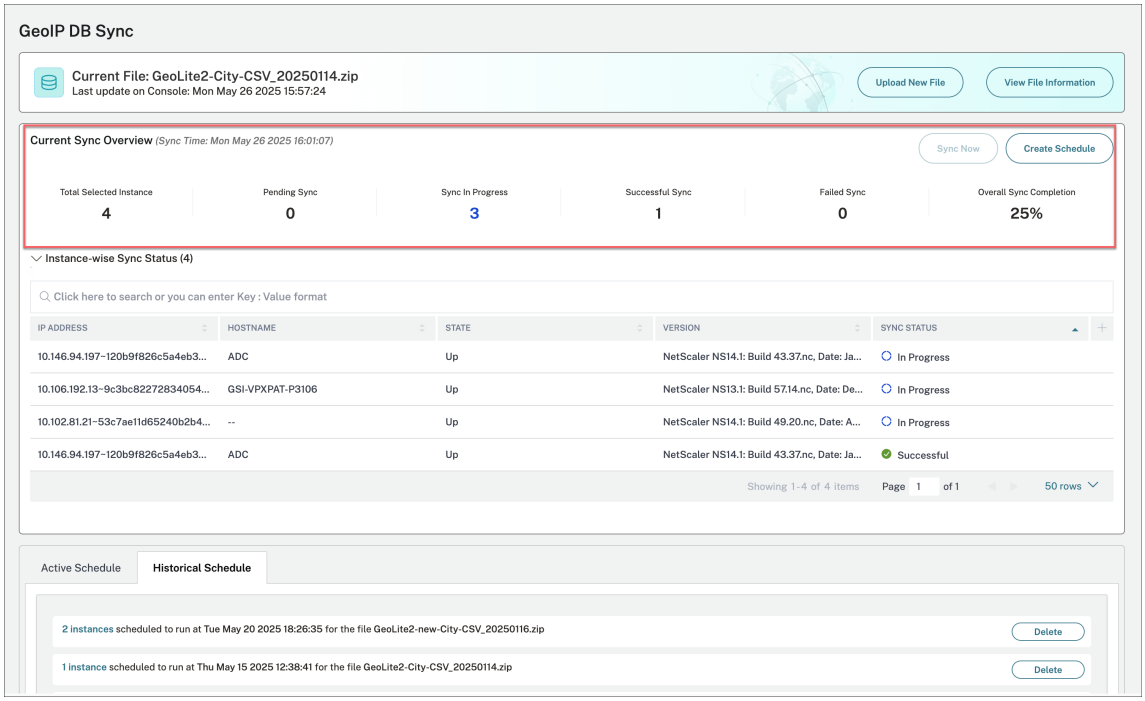
3. After the file is uploaded, you can perform one of the following actions:

   - Click **Sync Now** and then **Start Sync**: All the NetScaler instances get updated immediately.
   - Click **Create Schedule** - You can select a future date and time for updating the NetScaler instances.



4. View the progress of sync and instance-wise sync status on the **GeoIP DB Sync** page.

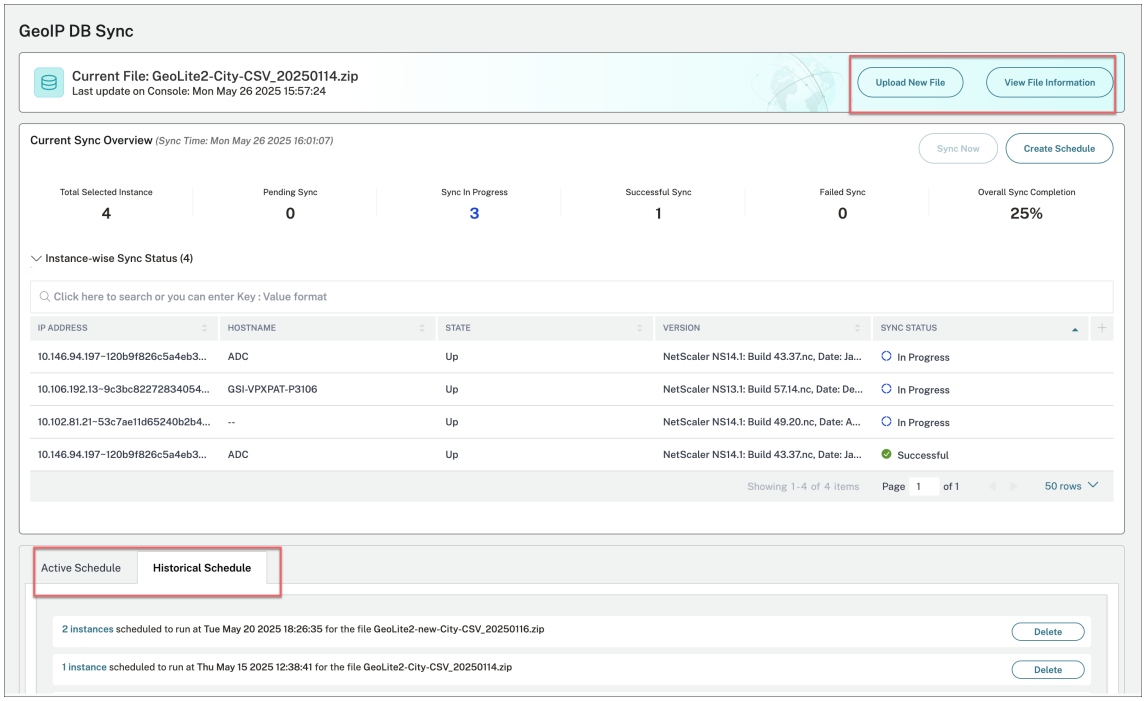
© 1997–2025 Citrix Systems, Inc. All rights reserved.



5. Based on your requirement, you can perform the following actions:

   - **Upload New File**: Click **Upload New File** to upload a GeoIP DB file from local or select an uploaded file from NetScaler Console.
   - **View File Information**: Click **View File Information** to view the previously uploaded files. If an issue arises, you can track the historical versions, upload, and sync an older GeoIP DB file.
   - **Active Schedule**: Click **Active Schedule** to view the upcoming schedules that are yet to be executed.
   - **Historical Schedule**: Click **Historical Schedule** to view the previous GeoIP DB sync activities that are completed.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Manage admin partitions of NetScaler instances

November 19, 2024

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 Create a user and Create a group.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.
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.

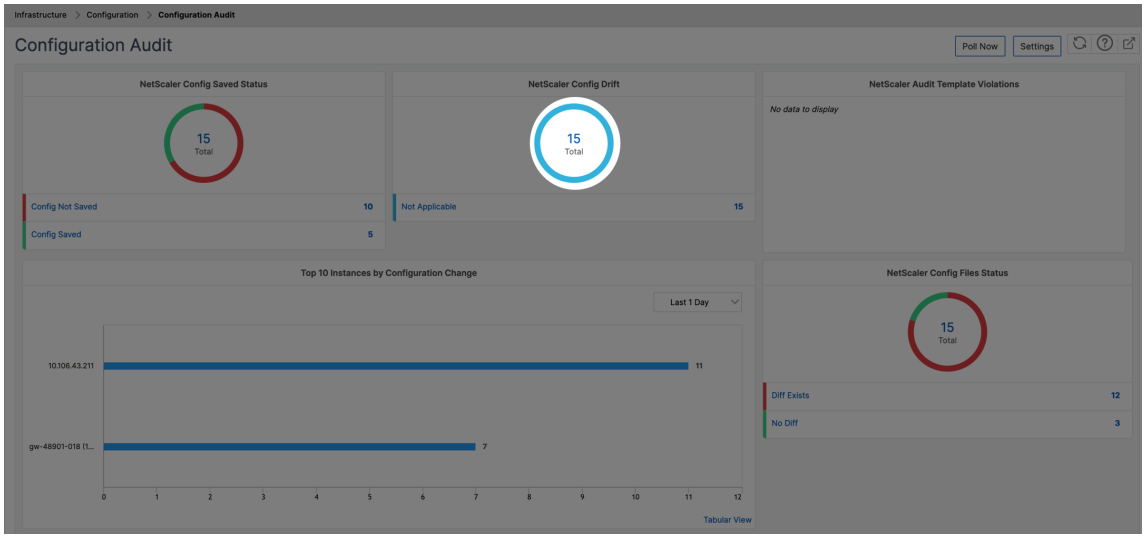
View the revision history difference

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.

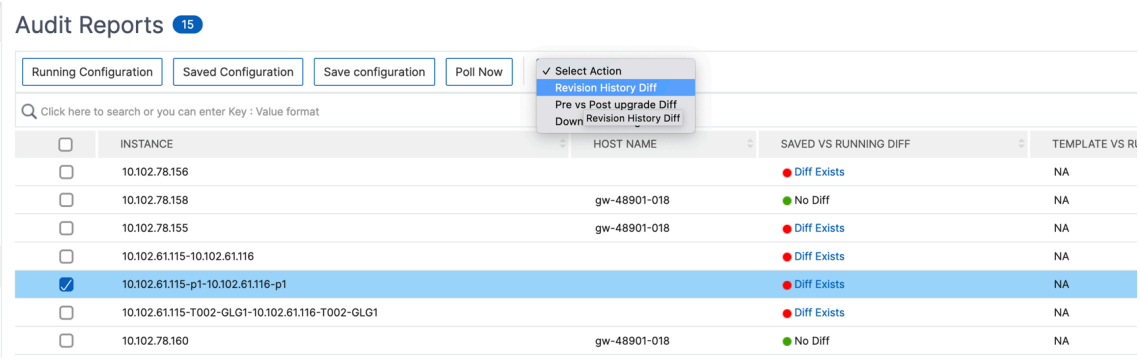
To view the revision history difference:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.



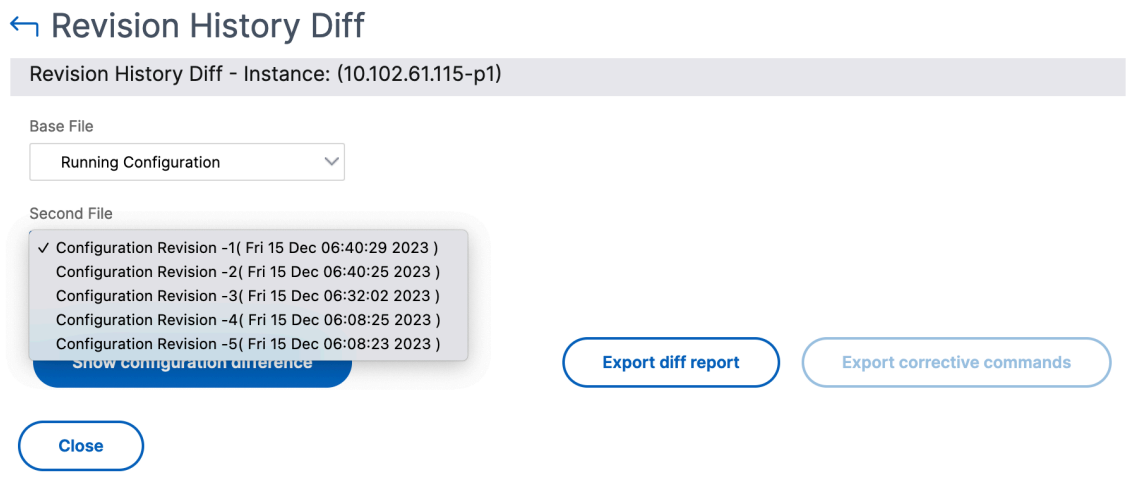
2. Select the partitioned NetScaler instance.
3. From the Action box, click **Revision History Diff.**



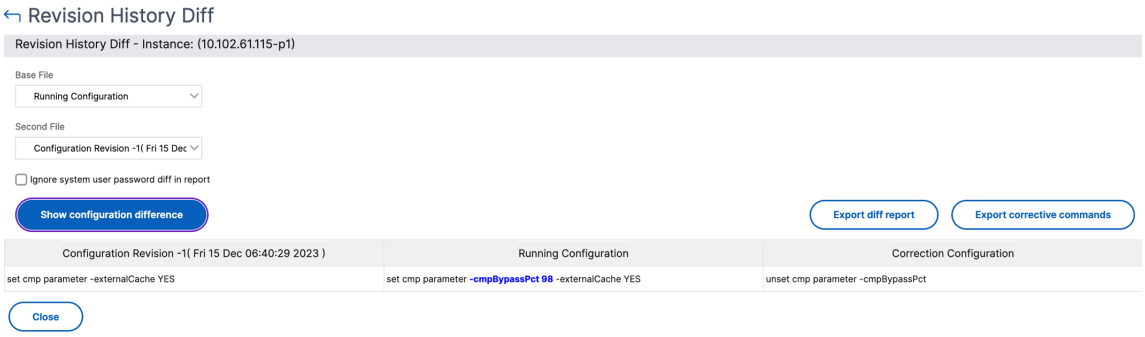
4. On the **Revision History Diff** page, select the files that you want to compare. For example, compare the Saved Configuration with Configuration Revision-2 and then, click **Show configuration difference**.

   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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

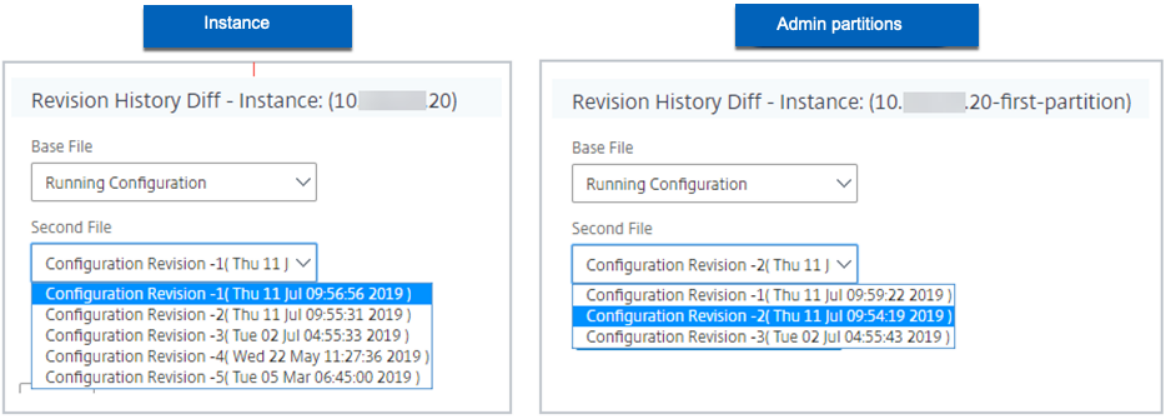


You can also view the corrective configuration commands and export these corrective commands to your local folder. These corrective commands are the commands that need to be run on the base file to get the configuration to the desired state (configuration file that is being used for comparison).



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:

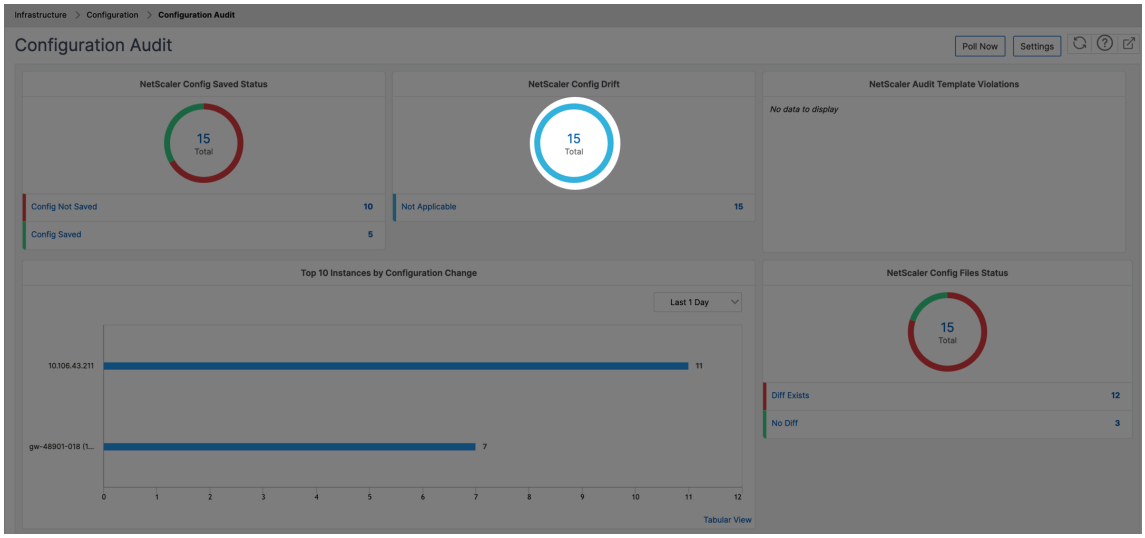
© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.

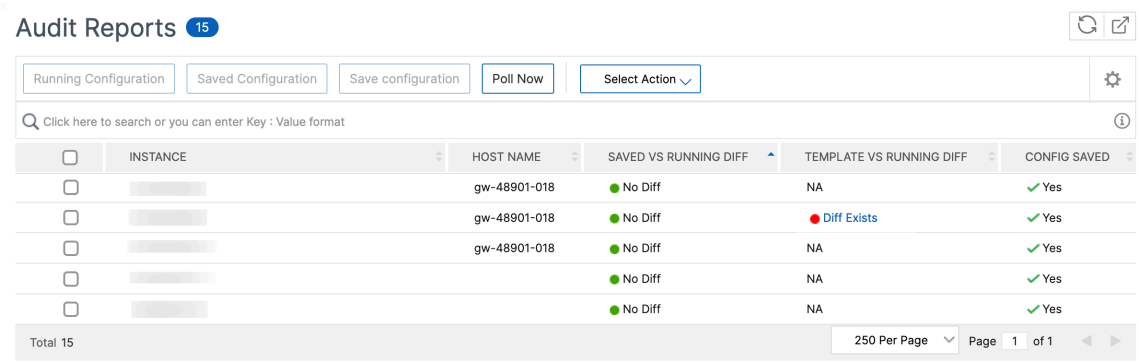


2. In the **Audit Reports** page, click the **Diff Exists** hyperlink under the Template vs Running Diff column.

   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. Along

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

July 9, 2025

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 your managed NetScaler instances by using NITRO calls and the Secure Shell (SSH) and Secure Copy (SCP) protocols.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.
   - 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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

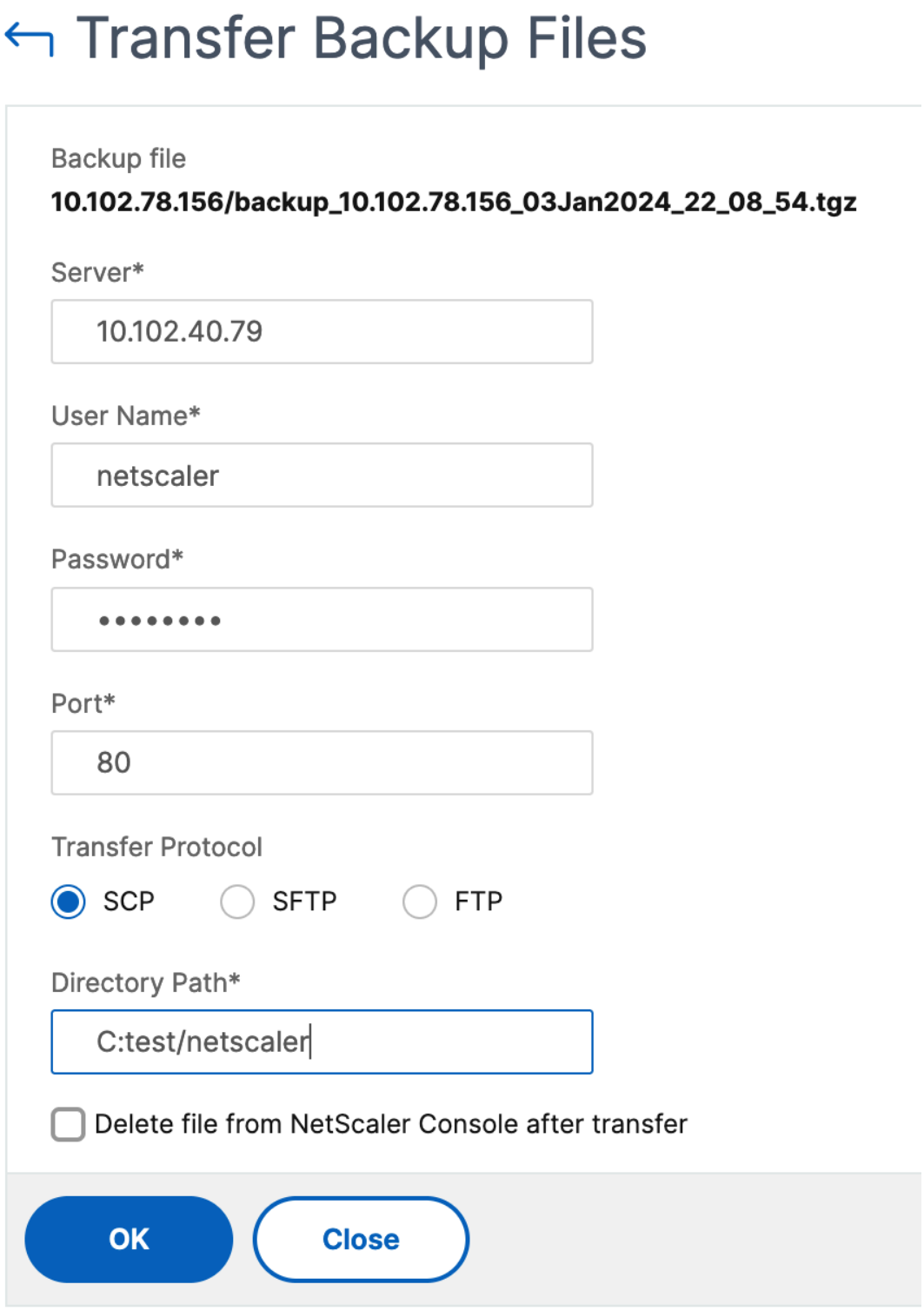
   c) **Port** –Port number of the system the files are being transferred to.

   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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Note:

The backup files from the NetScaler Console service are sent to the external server through an

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 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:

- 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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**.

   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:

© 1997–2025 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.

Force a failover to the secondary NetScaler instance

January 8, 2024

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.
- 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

January 8, 2024

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:

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

January 8, 2024

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Creating a group of instances helps you to upgrade, backup, or restore on the grouped instances at one time.

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**.

Global Server Load Balancing site groups

January 8, 2024

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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

Create SNMP managers and users for NetScaler agent

January 8, 2024

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:

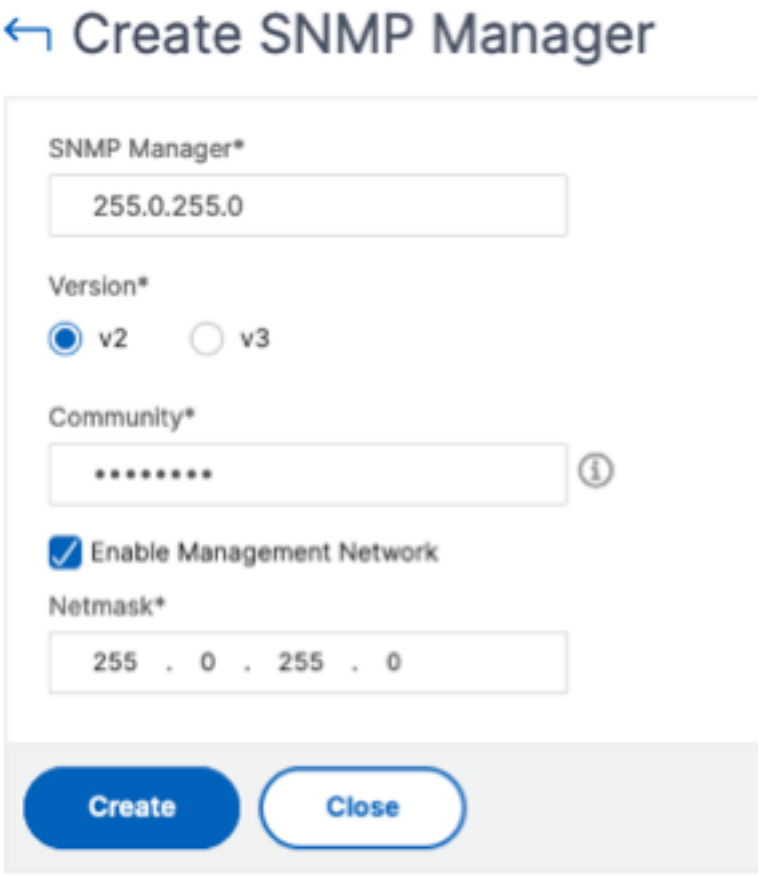
1. Navigate to **Infrastructure > Instances > Agents**, select a NetScaler agent, and click **Select Action > Manage SNMP**.
2. In the **SNMP > SNMP Manager** tab, click **Add**.
3. In the **Create SNMP Manager** page, specify the following details:

   - **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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**.



Add an SNMP v3 manager

To add an SNMP v3 Manager for the NetScaler agent:

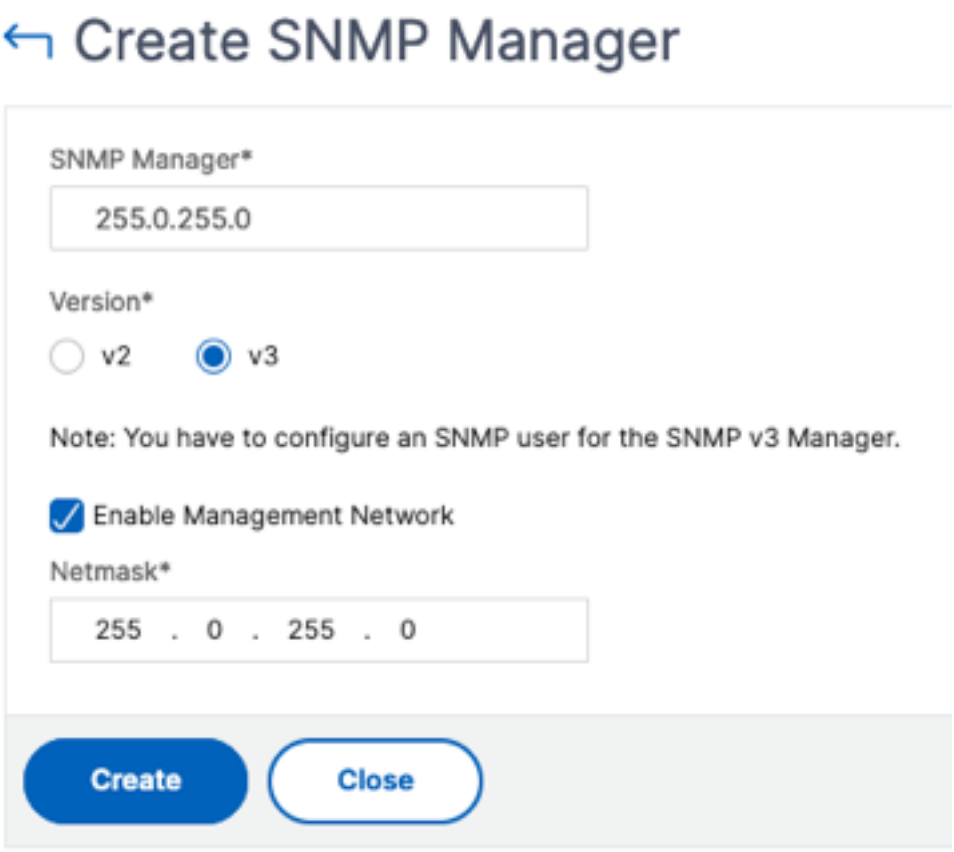
1. Navigate to **Infrastructure > Instances > Agents**, select a NetScaler agent, and click **Select Action> Manage SNMP**.
2. In the **SNMP > SNMP Manager** tab, click **Add**.
3. In the **Create SNMP Manager** page, specify the following details:

   - **SNMP Manager**. Enter the name or IP address of the SNMP Manager.
   - **Version**. Select v3.

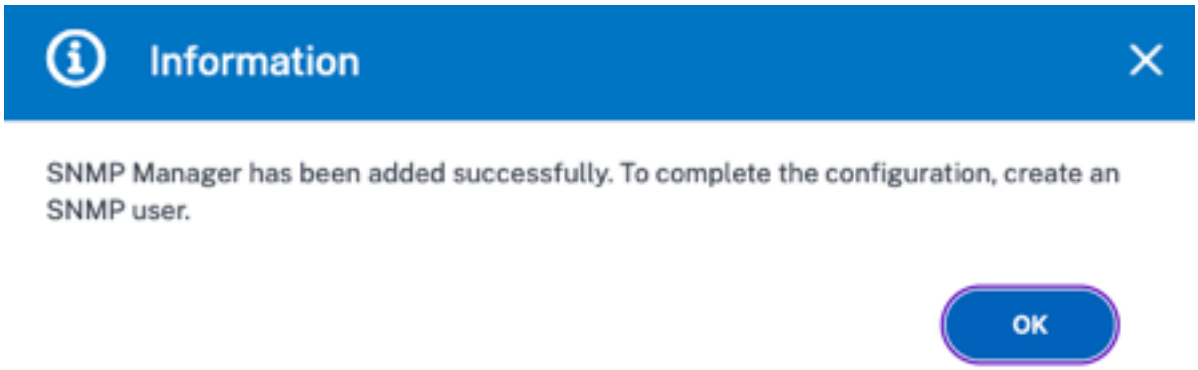
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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**.



A dialog box appears confirming that an SNMP manager is created and prompting you to configure an SNMP user.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> You must configure an SNMP user for an SNMP v3 manager. To configure the SNMP user, go to **SNMP > SNMP User**.

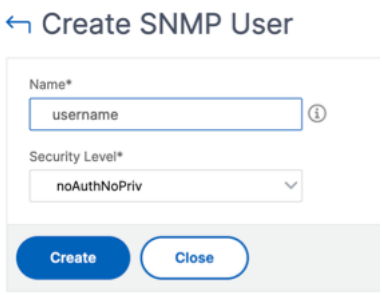
Add an SNMP user

Add an SNMP user to respond to the SNMP v3 queries from an SNMP manager.

To add an SNMP user for the NetScaler agent:

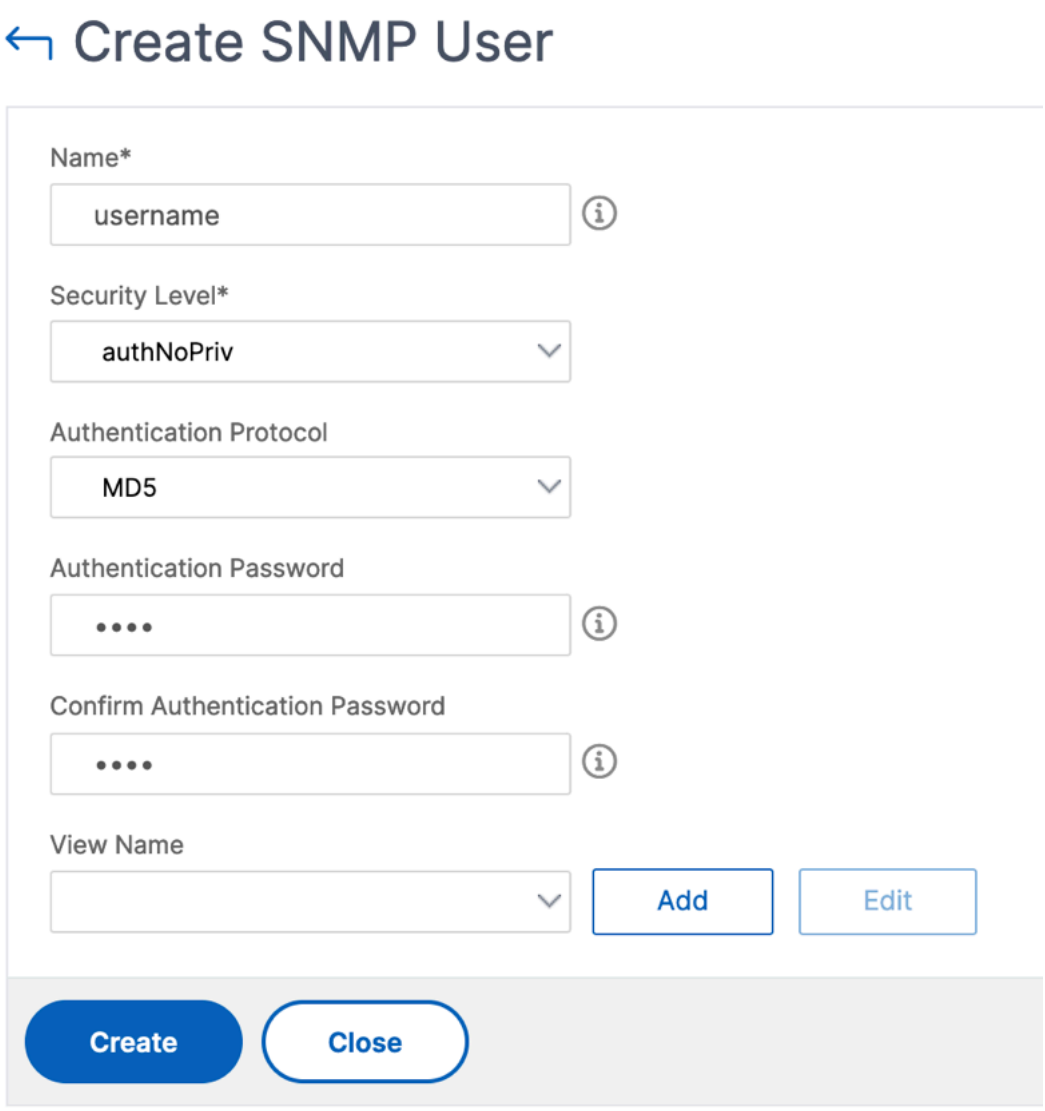
1. Navigate to **Infrastructure > Instances > Agents**, select a NetScaler agent, and click **Select Action > Manage SNMP**.
2. In the **SNMP > SNMP User** tab, click **Add**.
3. In the **Create SNMP User** page, add the following details:
   - **Name**. Enter the user name.
   - **Security Level**. 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.



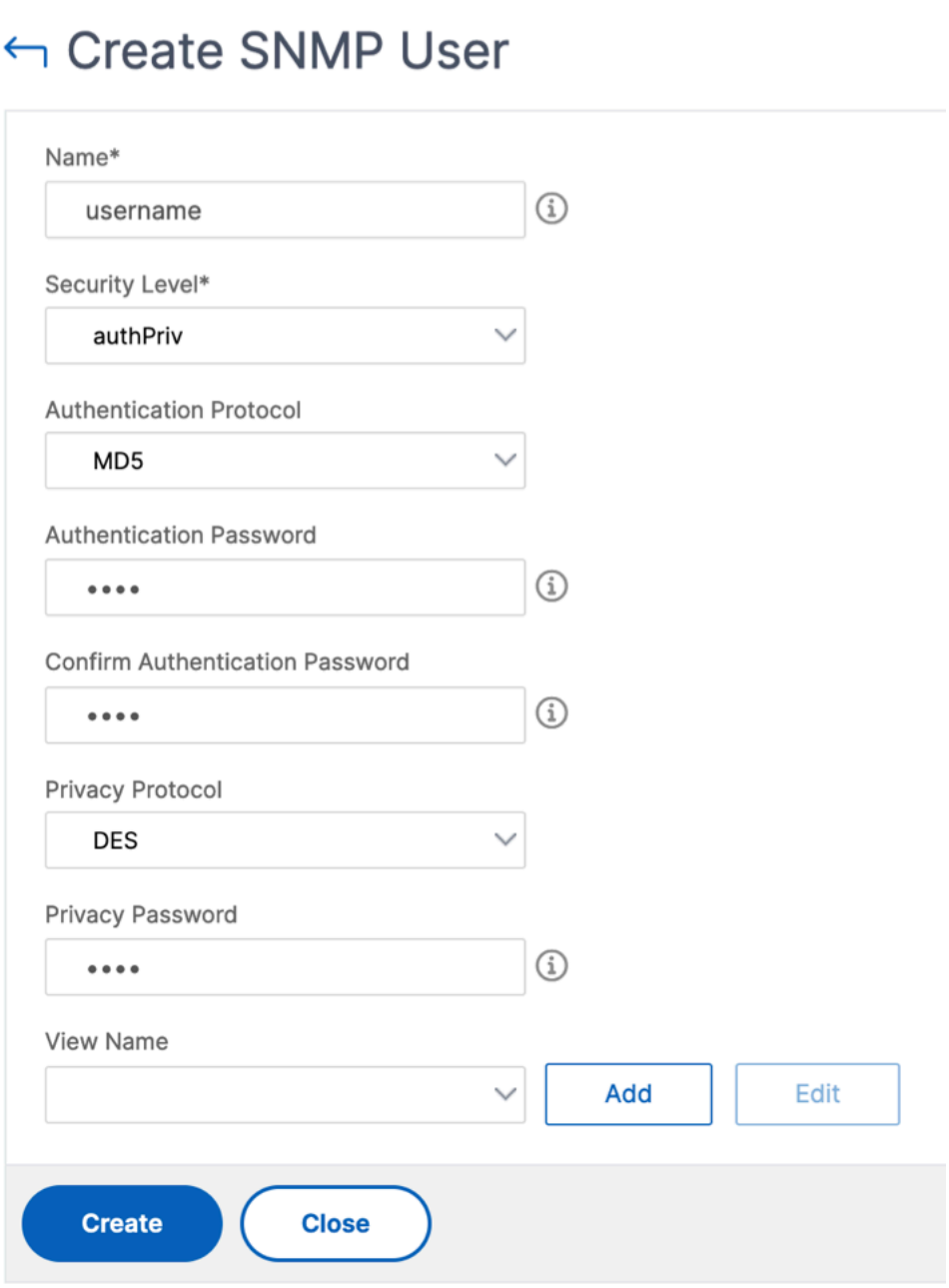
   - **authNoPriv**. Require authentication but no encryption.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- **authPriv**. Require authentication and encryption.

© 1997–2025 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.

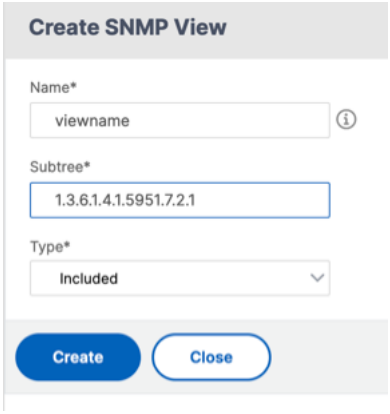
Managing SNMP views

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

March 7, 2025

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.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

3. In **Select Action**, select **Provision VPX**.

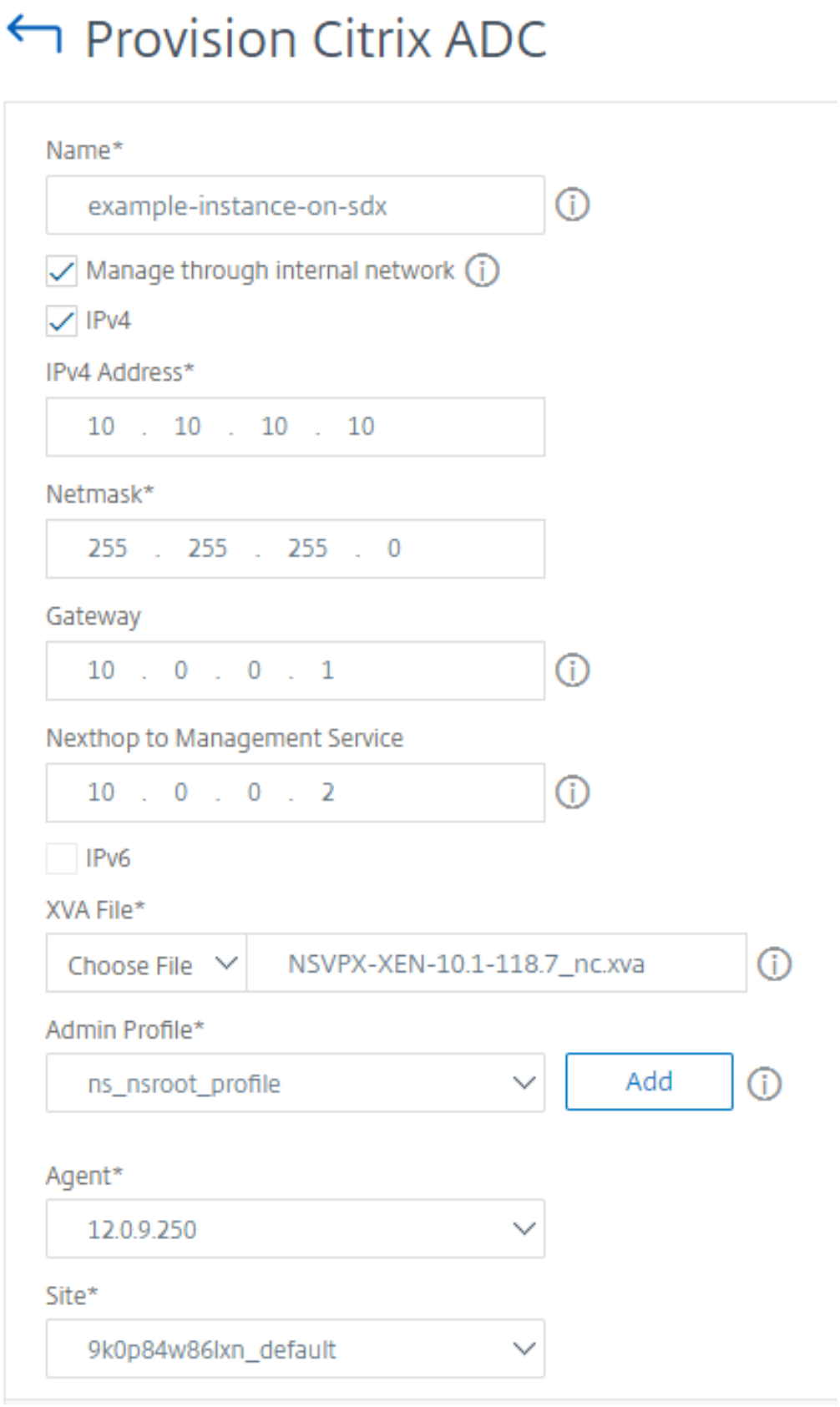
Step 1 - Add a VPX instance

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Step 2 - Allocate licenses

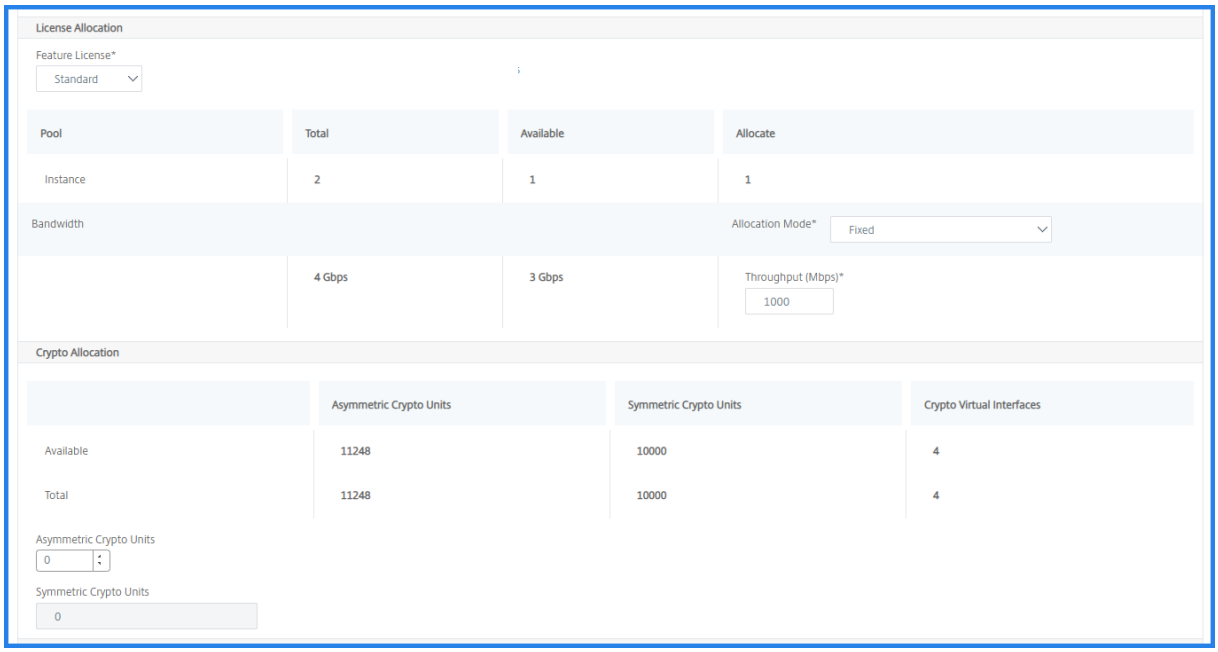
In the **License Allocation** section, specify the VPX license. You can use Standard, Advanced, and Premium licenses.

- **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.

> **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

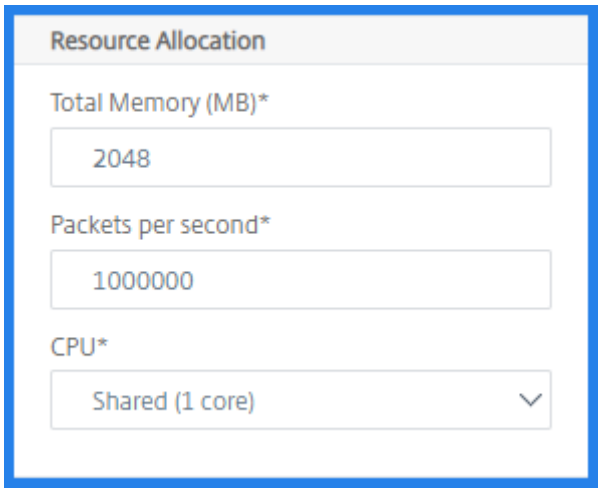
- **CPU** - Specify number of CPU cores to an instance. You can use shared or dedicated CPU cores.

  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.

  > **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.

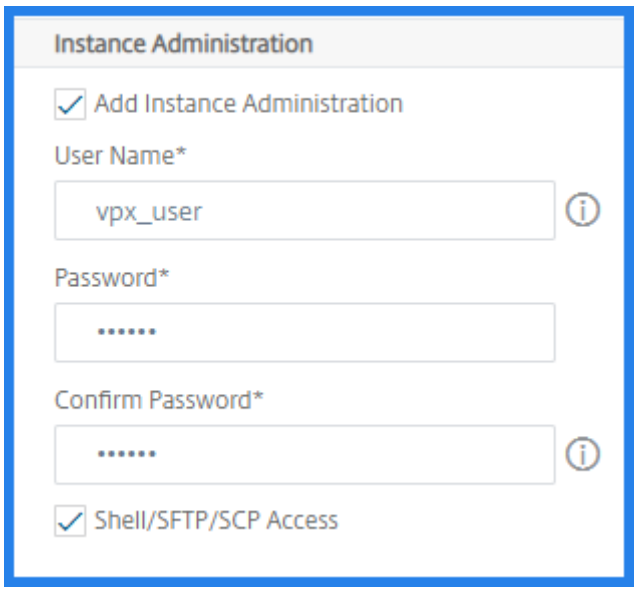
Step 4 - Add instance administration

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Step 5 - Specify network settings

Select the required network settings to an instance:

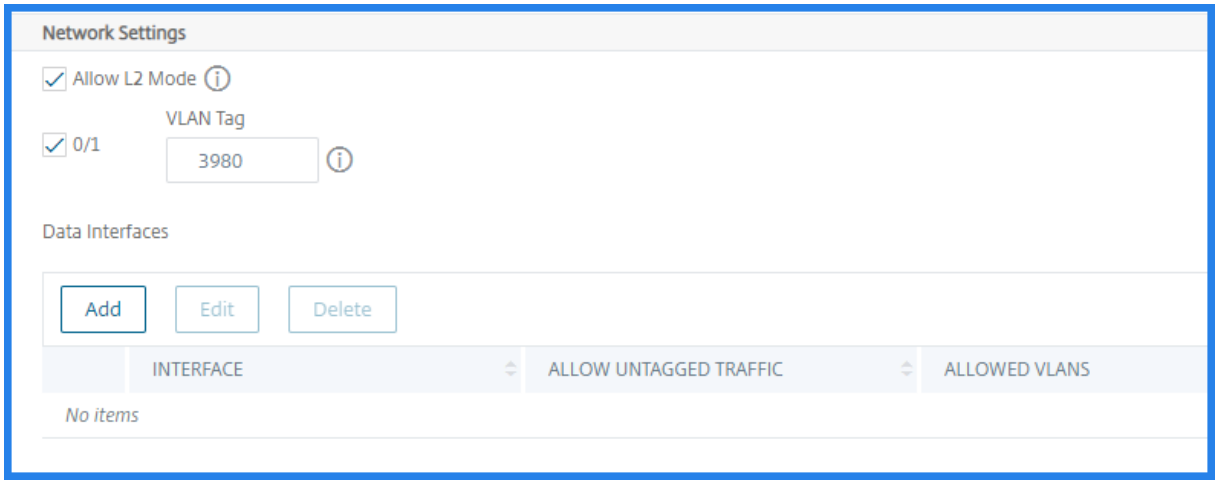
- **Allow L2 Mode under network settings** - You can allow L2 mode on the NetScaler instance. Select Allow L2 Mode under Networking Settings. Before you log on to the instance and enable L2 mode. For more information, see Allowing L2 Mode on a NetScaler instance.

  > **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



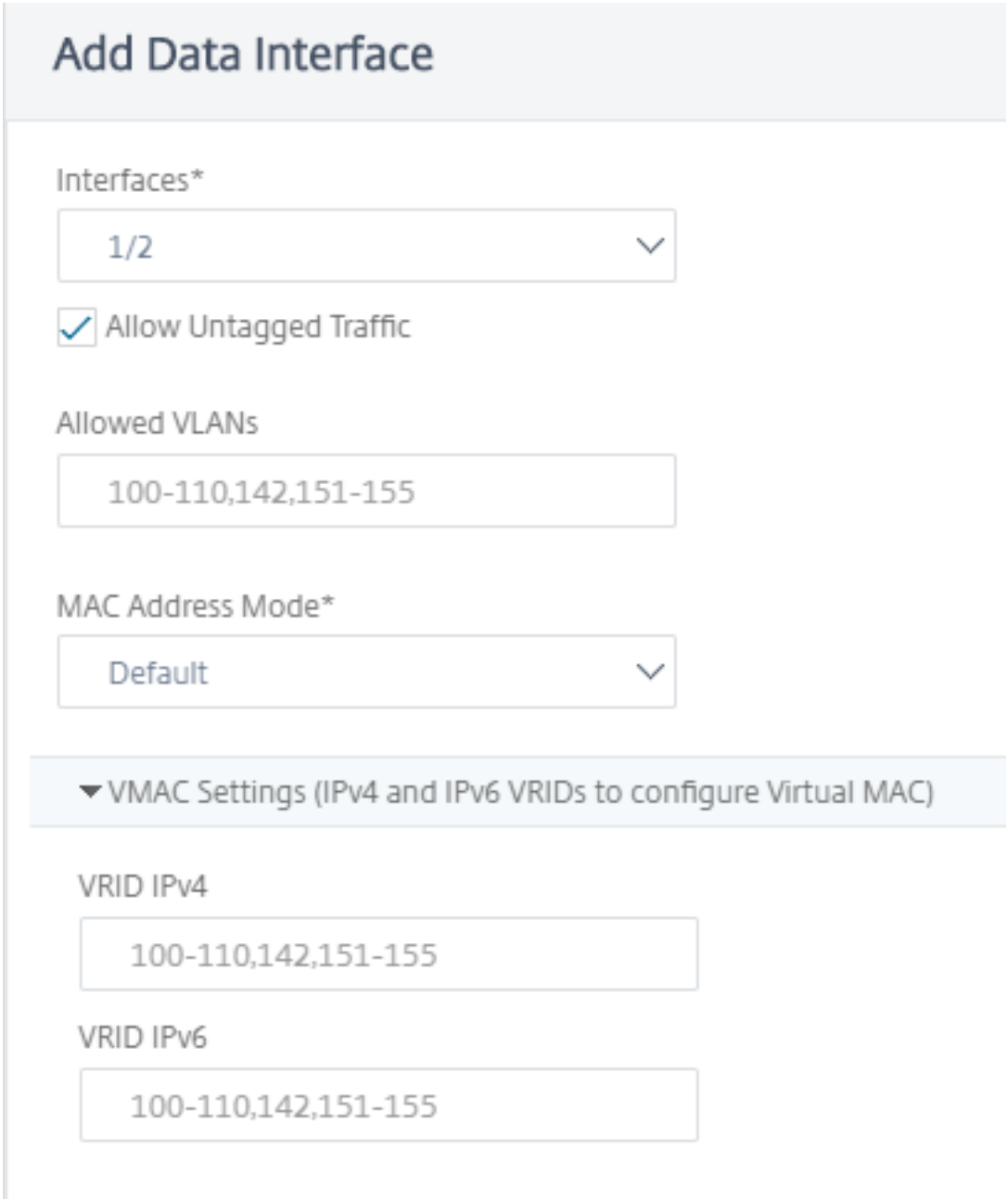
In **Data Interfaces**, click **Add** to add data interfaces and specify the following:

- **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.
  - VRID IPV6 - The IPv6 VRID that identifies the VMAC. Possible values: 1–255. For more information, see Configuring VMACs on an Interface.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.

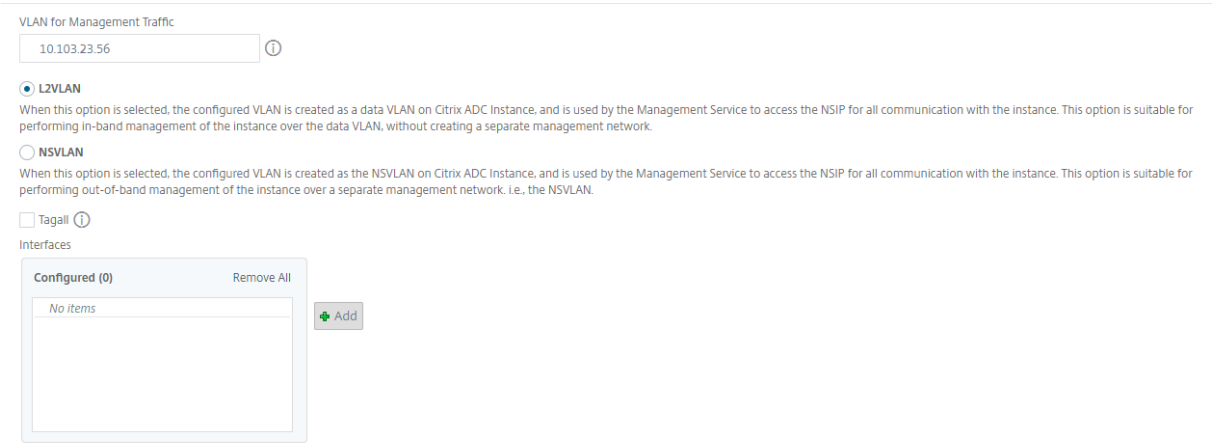
If the Management Service and the instance are in different subnetworks, specify a VLAN ID while you provision a VPX instance. Therefore, the instance is reachable over the network when it active.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

> **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.

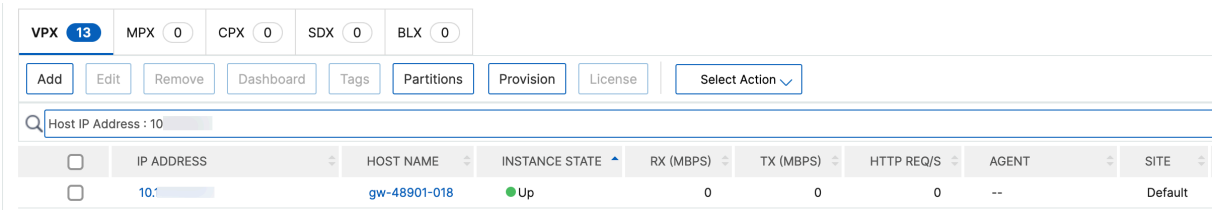


Click **Done** to provision a VPX instance.

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.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Rediscover multiple NetScaler instances

January 8, 2024

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:

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

October 7, 2024

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:

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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Polling type	Polling interval	Polled information	Protocol used	Polling interval configuration
Configuration audit polling	Every 10 hours (by default)	Configuration changes that occur on NetScaler instances (for example, running vs. saved configuration)	SSH, SCP, and NITRO call	Yes. Navigate to **Infrastructure > 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.

© 1997–2025 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				

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Polling type	Polling interval	Polled information	Protocol used	Polling interval configuration
All instances	Every 720 minutes (by default)	All entities that are configured on the 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.	NITRO call	Yes. It can be set between 30 minutes and 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

© 1997–2025 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

© 1997–2025 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.

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

January 8, 2024

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**.
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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

January 8, 2024

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

June 26, 2024

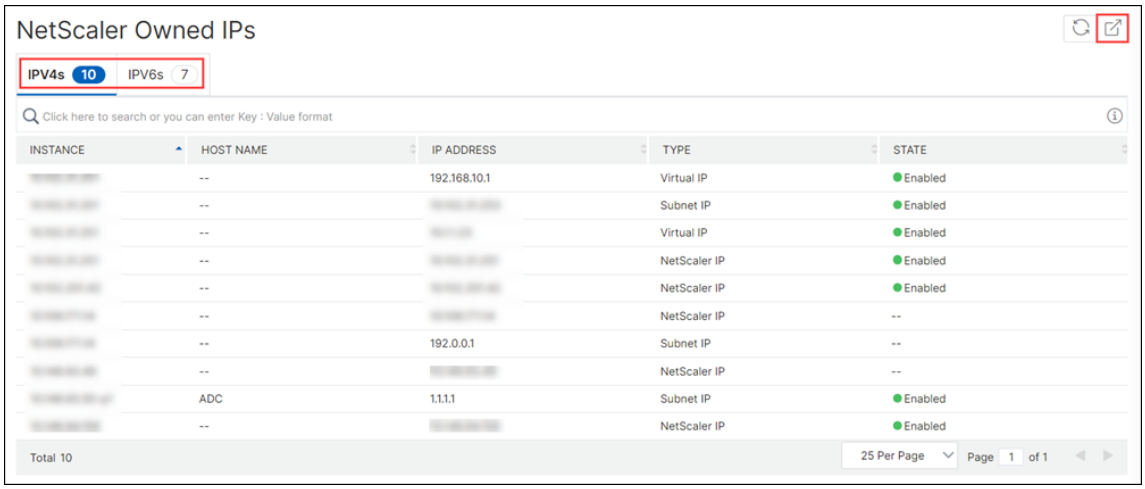
You can view the IP addresses configured on NetScaler instances directly from NetScaler Console GUI. Please note that the configuration changes and other operations can only be performed on NetScaler instances.

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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- NetScaler IP address
- Subnet IP address
- Virtual IP address
- ADNS service IP address
- GSLB IP address
- Cluster IP address
- Mapped IP address



Export NetScaler-owned IP addresses

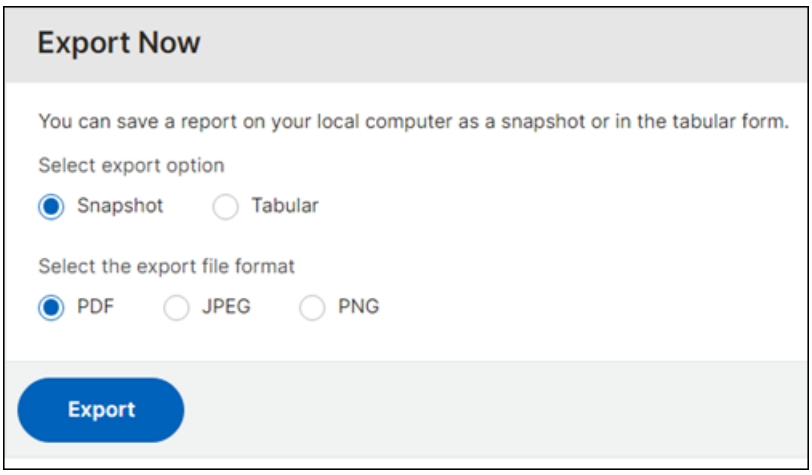
To export NetScaler-owned IP addresses, follow these steps:

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.

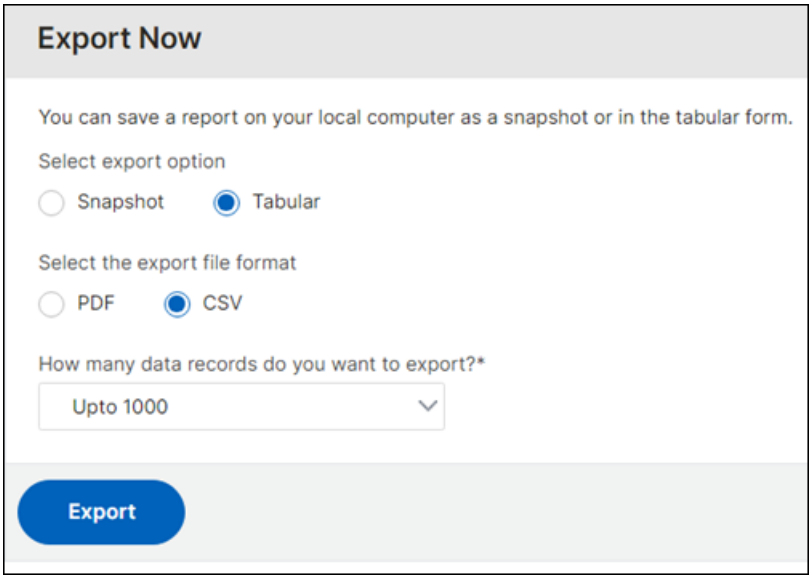
© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.
3. On the **Export Reports** page, click **Schedule Export**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:

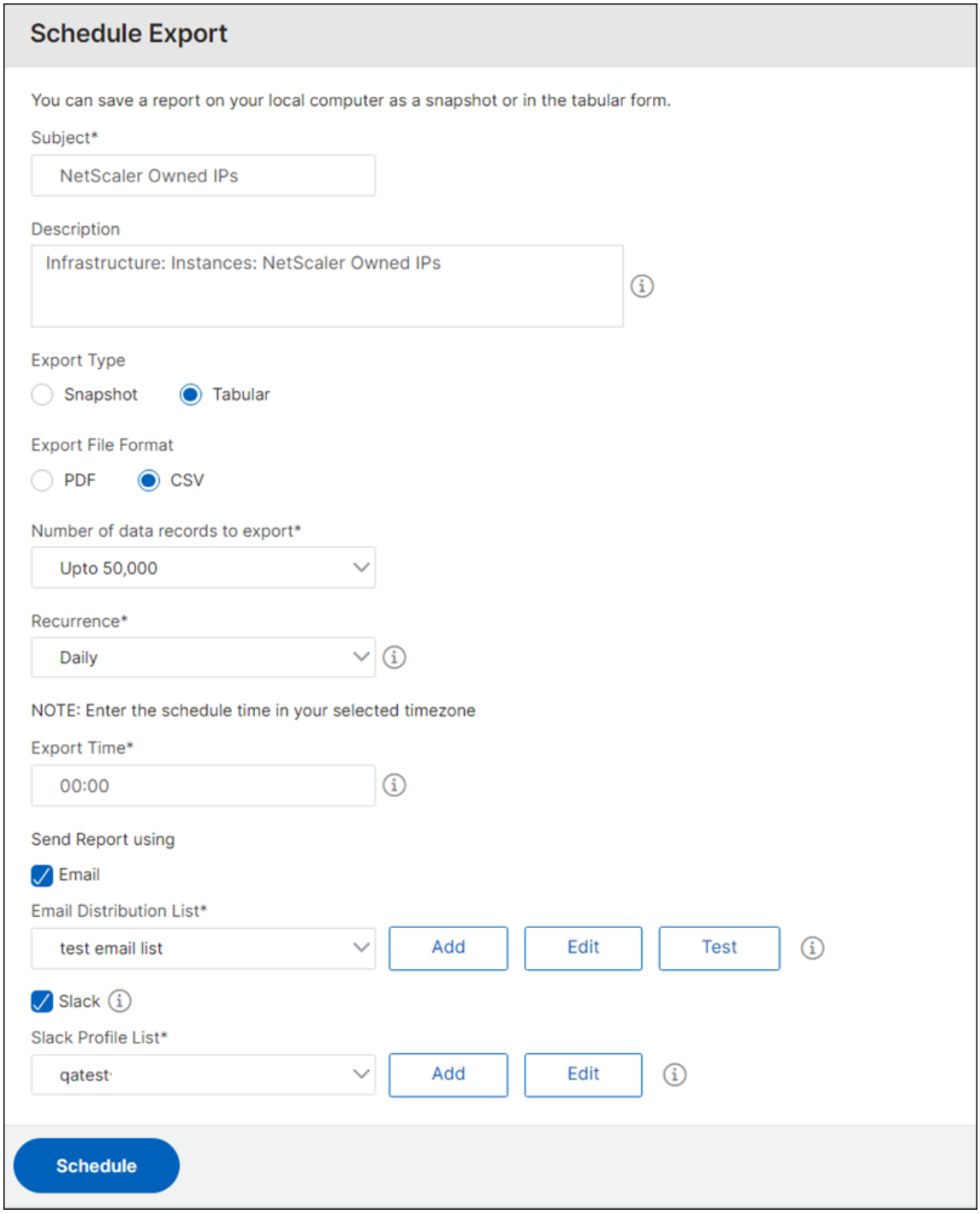
      - Select **Email** and choose the email distribution list to send the list of NetScaler-owned IP addresses.
        - To add an email distribution list, click **Add** and specify the email server details.
        - To edit an email distribution list, click **Edit**.
        - To verify that the email 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**.

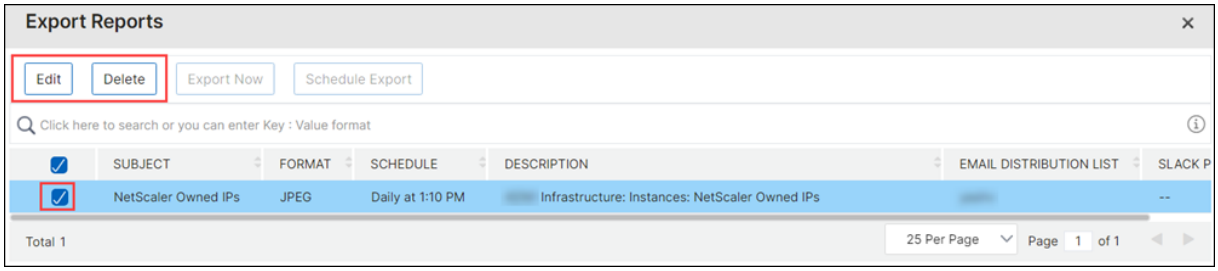
5. Click **Schedule** to schedule the export.

© 1997–2025 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



How to change the NetScaler MPX or VPX root password

November 19, 2024

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:

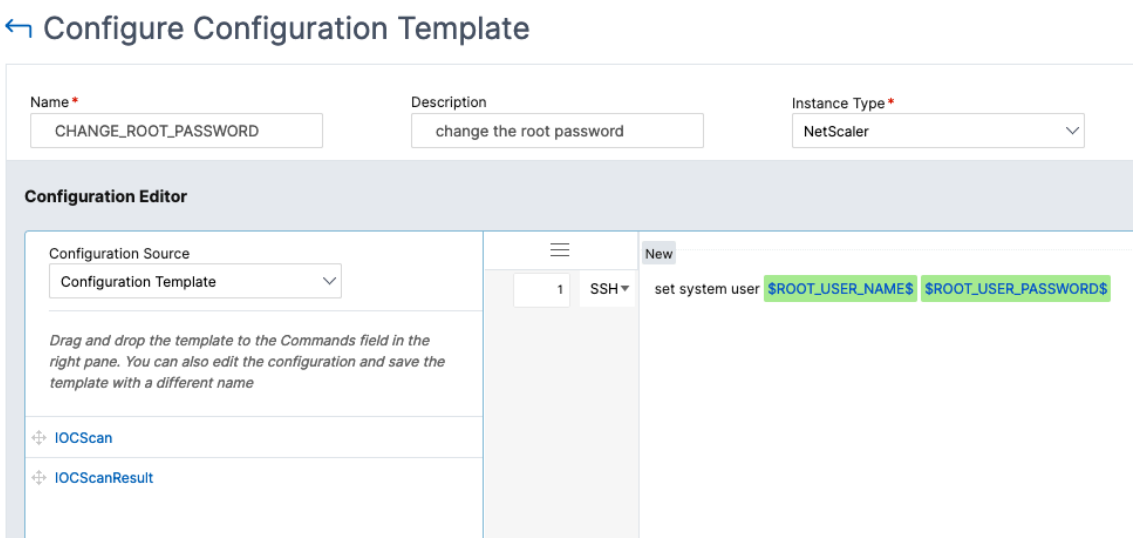
- Step 1. Create a Configuration Template.
- Step 2. Create a Configuration Job.
- Step 3. Create an admin profile and modify it.

> Note:
>
> If the NetScaler appliances are managed by other tools as well, you must change the credentials on those tools as well.

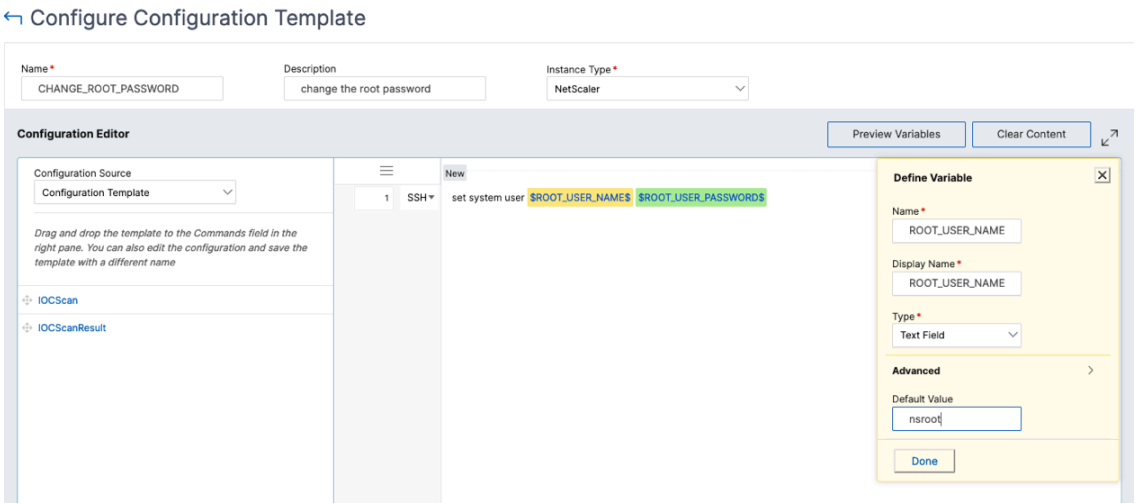
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Create a Configuration Template

1. From the NetScaler Console GUI, navigate to **Infrastructure > Configuration > 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.



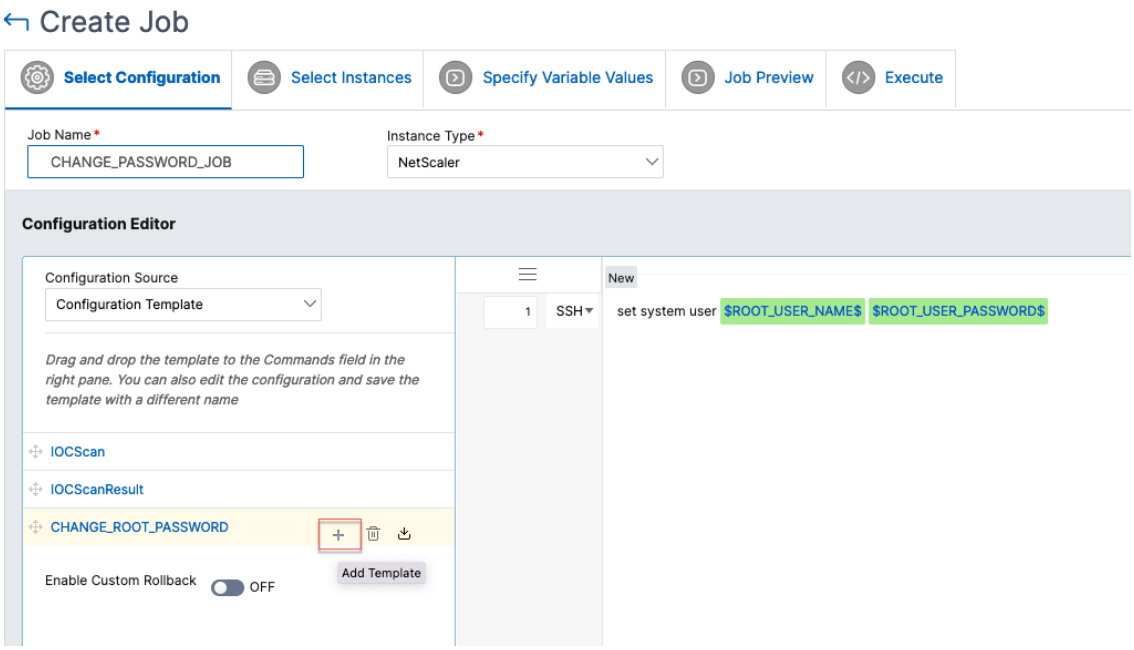
5. Select the $ROOT_USER_PASSWORD$ variable, and select **Password Field as Type**. Select **Done** to save the variable settings.
6. Select **OK** to save the Configuration Template.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

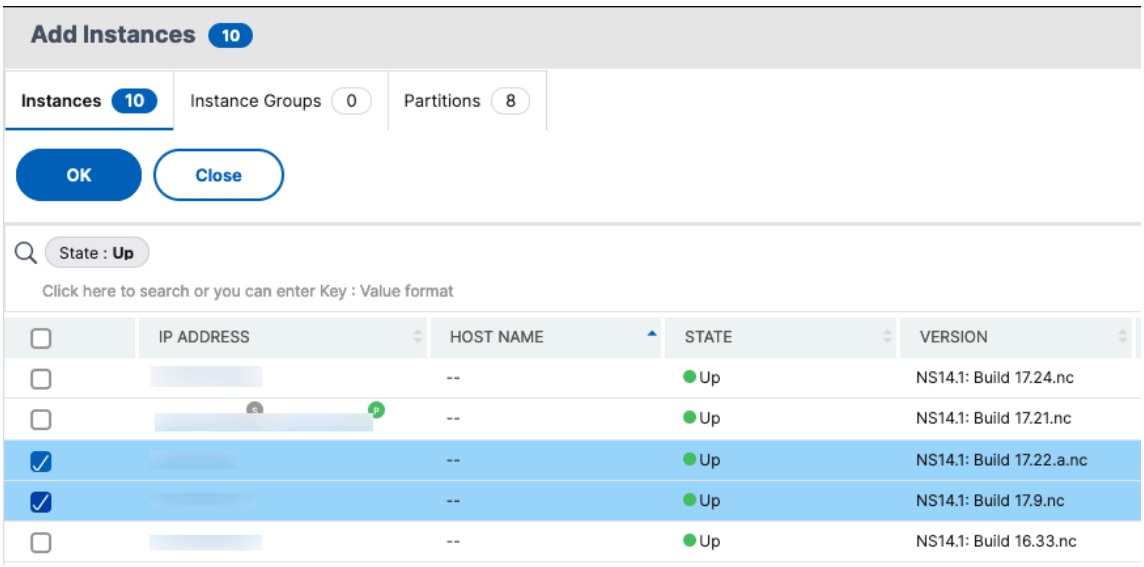
7. The new Configuration Template appears under **Configuration Templates**.

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**.



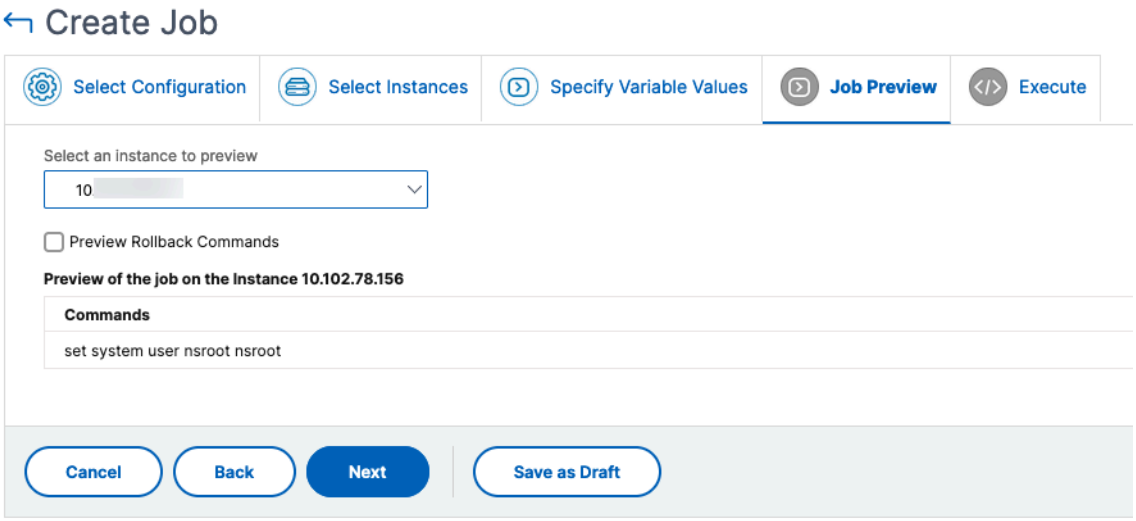
3. Select the NetScaler instance or instances for which the password must be modified.



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**.

© 1997–2025 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**.

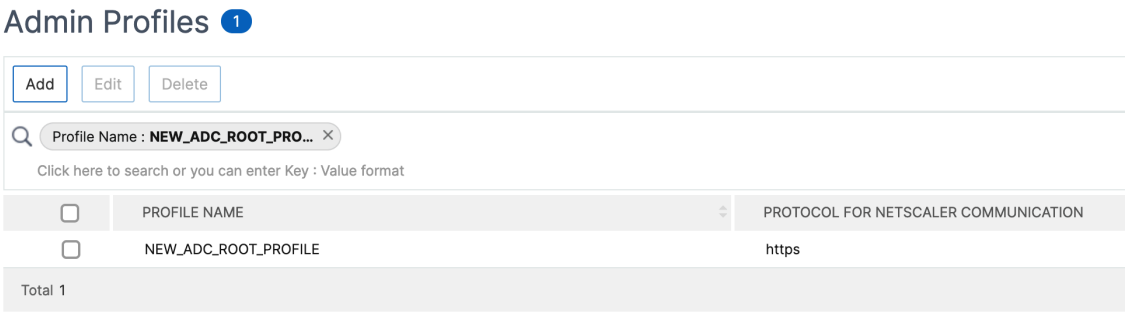


7. In the **Execute** pane, you have the choice to run the Job immediately or schedule it for later. You can also choose to run the Job in parallel on all the selected instances or do it sequentially. Select Finish after you've provided the execution details.
8. Configuration Job shows if the execution succeeded or failed.
9. Select the **Job** and click **Details**. The execution details show the status at individual instance level.

Modify the admin profile

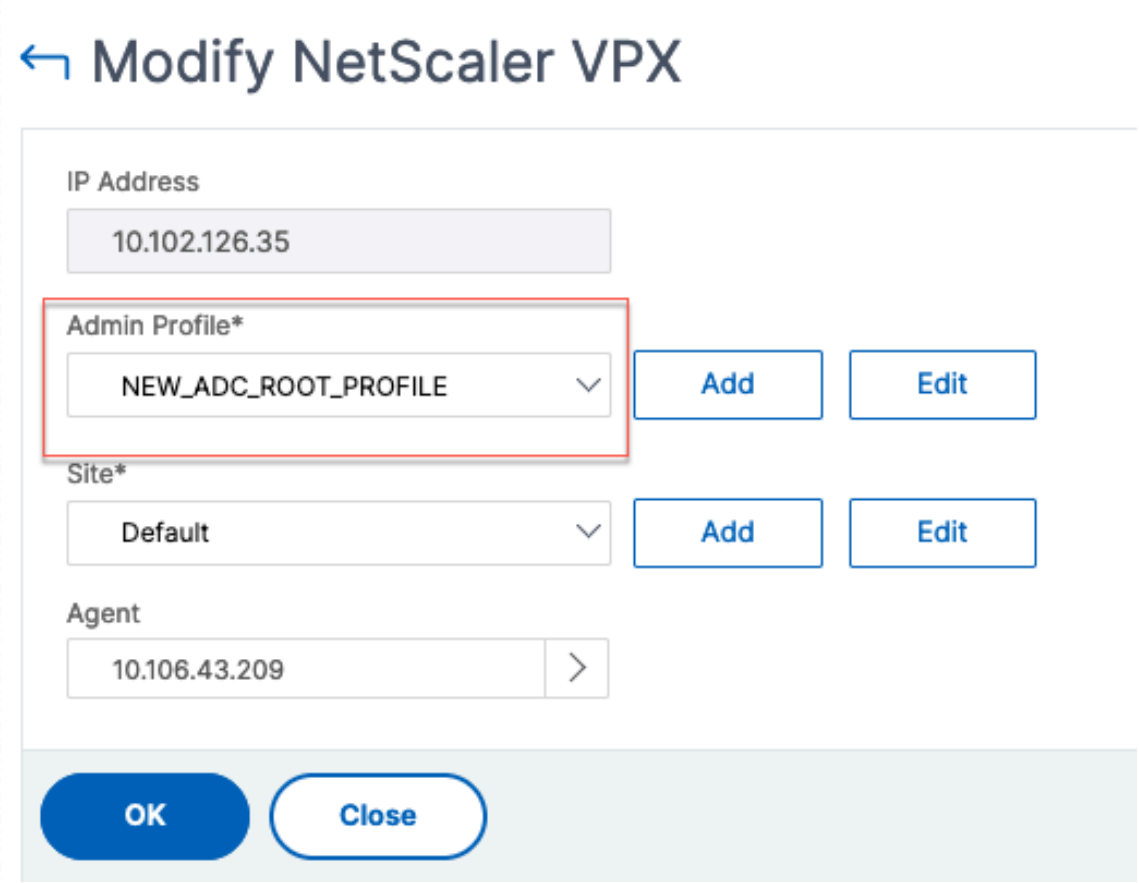
After you've modified the NetScaler passwords, you must add and modify the admin profiles of the instances. Follow these steps:

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.

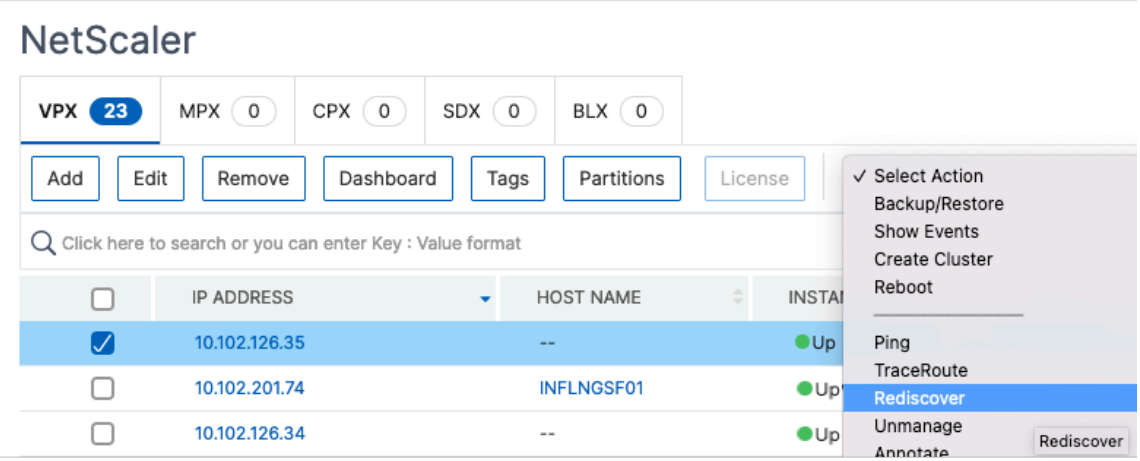


© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.
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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

January 9, 2024

Occasionally, you must change the nsroot password of the NetScaler appliance for security reasons or compliance of password rotation policy.

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

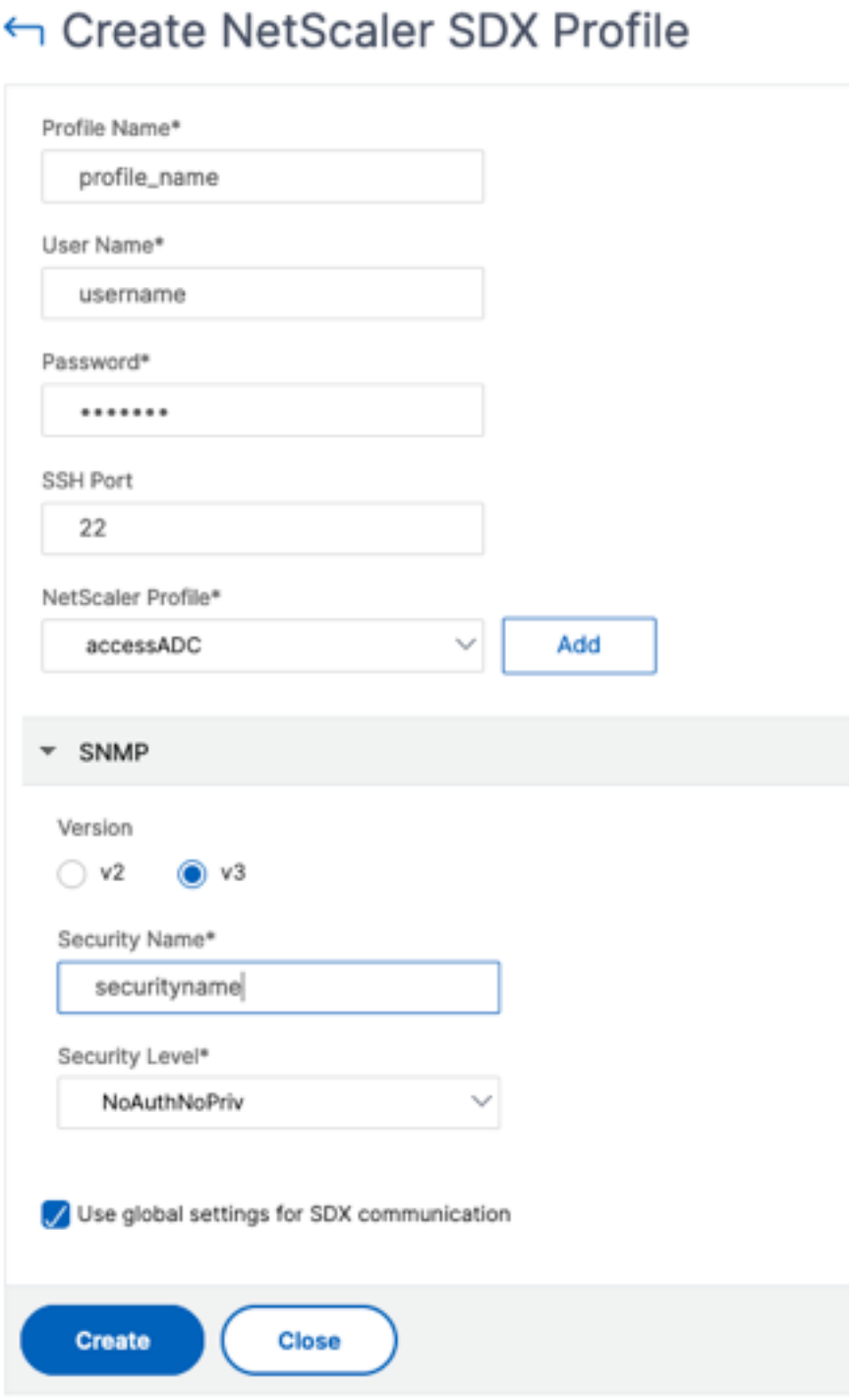
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:

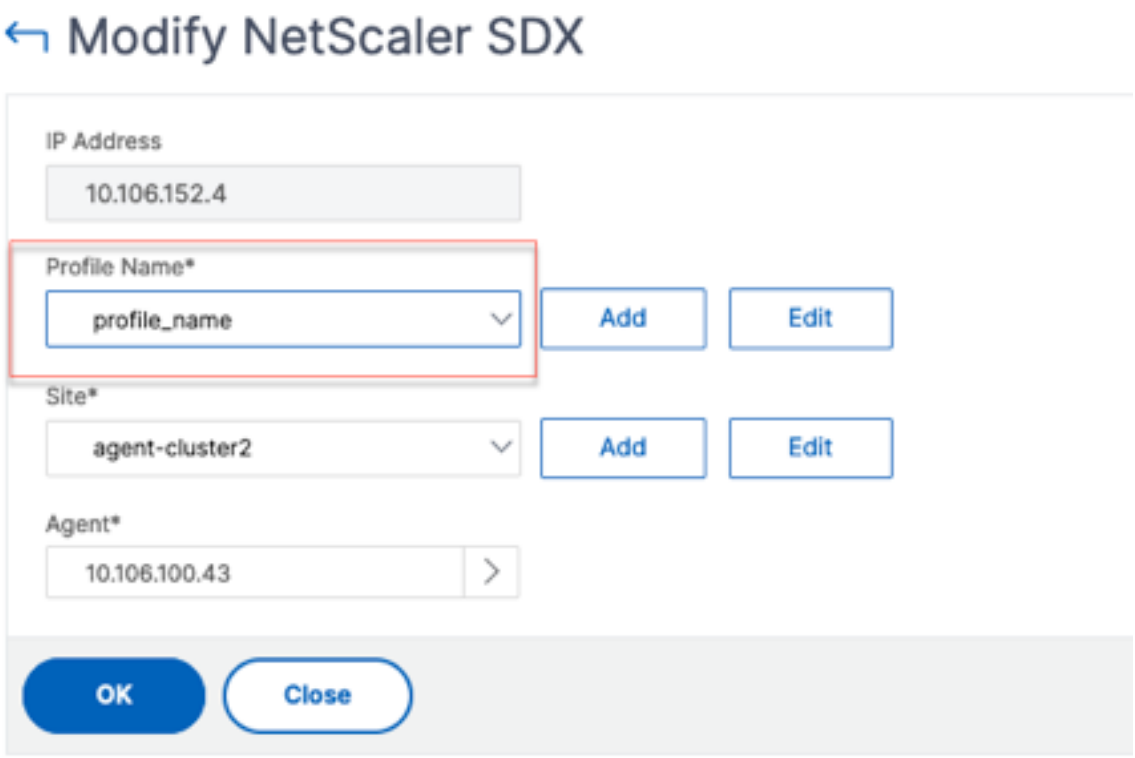
1. Navigate to **Infrastructure > Instances Dashboard > NetScaler > SDX**.
2. Select **Profiles** to see all the admin profiles.
3. Select **Add** to create an admin profile.
4. Provide new NetScaler credentials, and click **Create**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

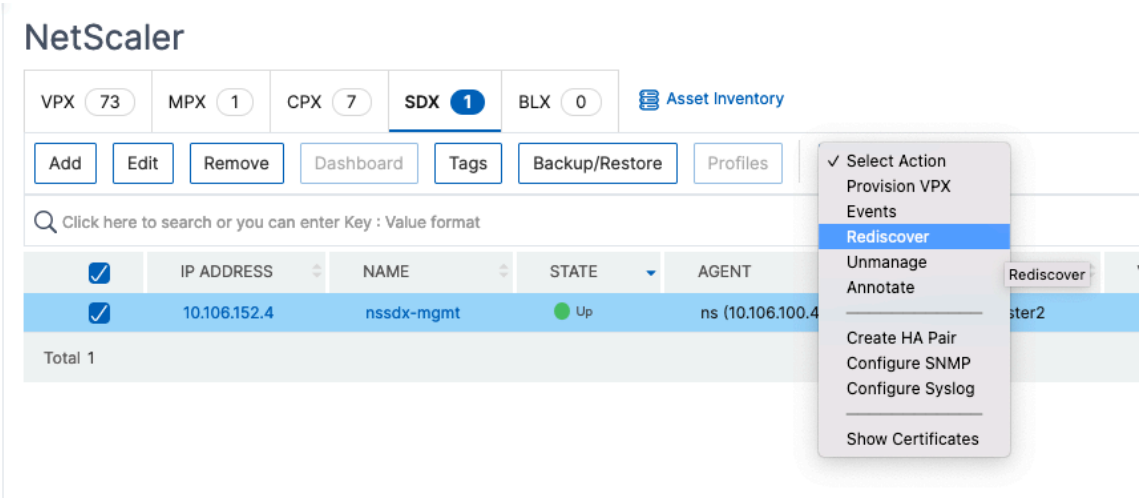


5. The newly created profile appears under **Admin Profiles**.
6. Go to **Network > Instances > NetScaler > SDX**. Select the instance for which the password has been modified, and the select **Edit**.
7. Select the newly created profile name and click **OK**.

© 1997–2025 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

How to generate a technical support bundle for a NetScaler instance

March 7, 2025

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:

- 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.

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:

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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 **Upload the Collector Archive**.
7. In the **My Citrix Account** section, enter the authentication token in the **Citrix Authentication Token** field.
8. Click **Create Technical Support**.

Events

January 8, 2024

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Use events dashboard

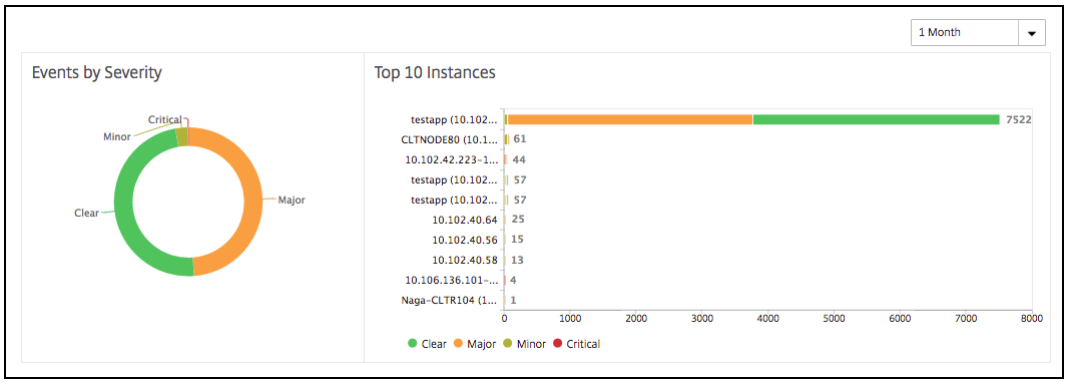
February 15, 2024

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:

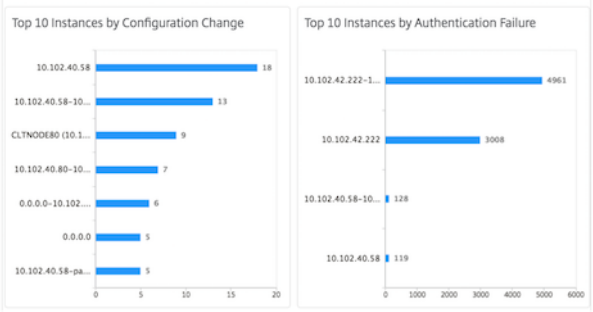
Navigate to **Infrastructure > Events > Reports**.

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.



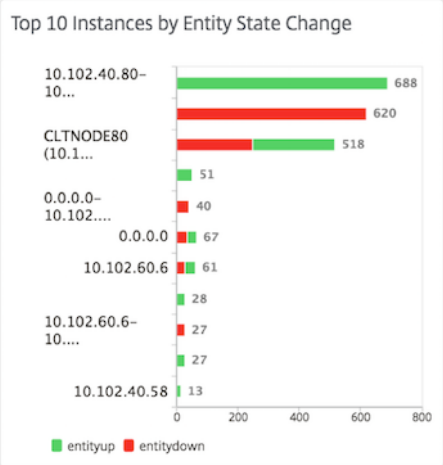
You can view more details by navigating to the NetScaler instance type (**Infrastructure > Events > Reports** > **NetScaler/ NetScaler SDX/ NetScaler**) to view the following:

- Top 10 devices by hardware failure
- Top 10 devices by configuration change
- Top 10 devices by authentication failure

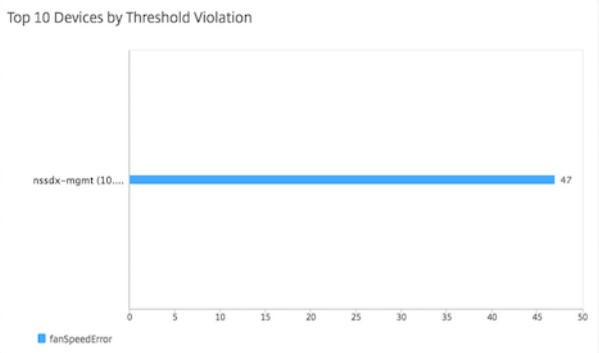


- Top 10 devices by entity state changes

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- Top 10 devices by threshold violation



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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Create event rules

April 8, 2024

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
- Citrix Application Delivery Controller (NetScaler) instances
- Category
- Failure objects
- Configuration commands
- Messages

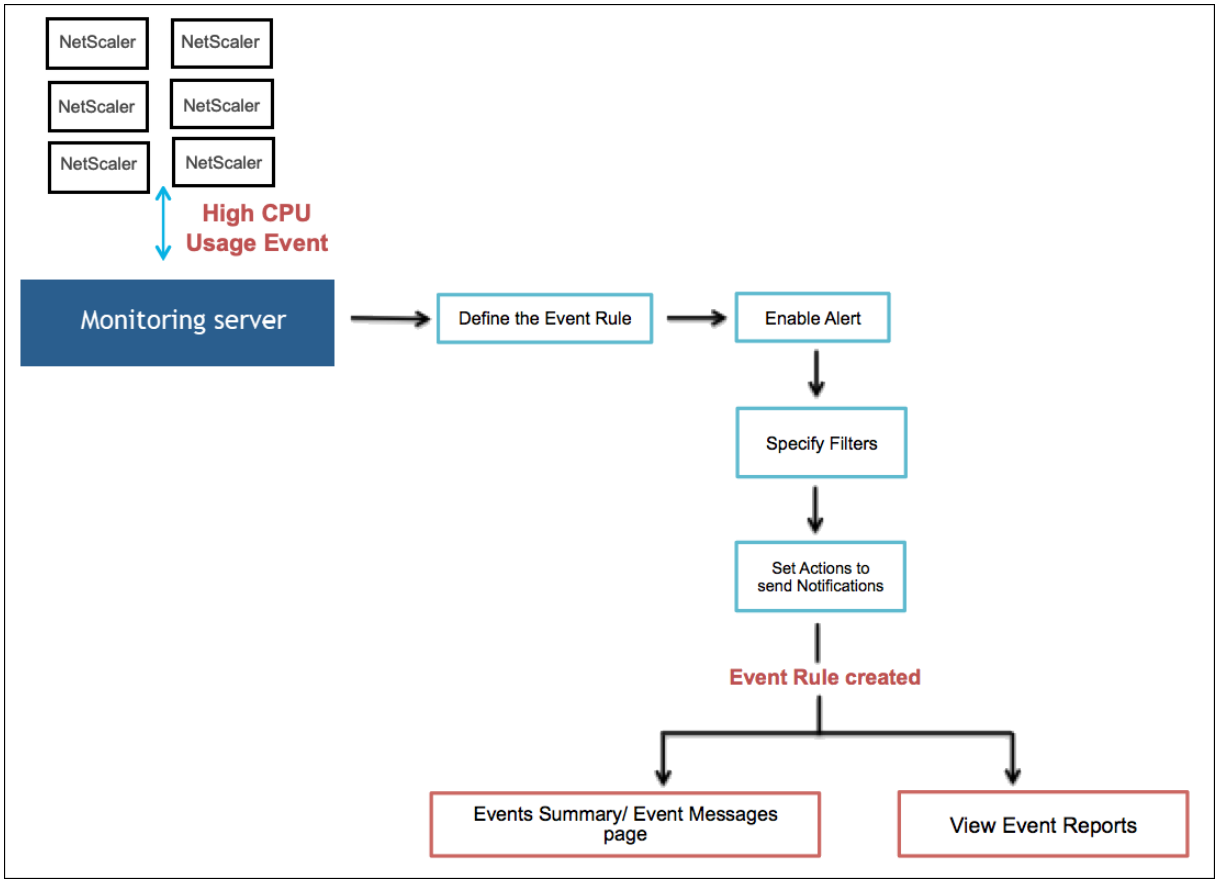
After you create events, you can assign actions to the events. For more information, see Add event rule actions.

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.

© 1997–2025 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:

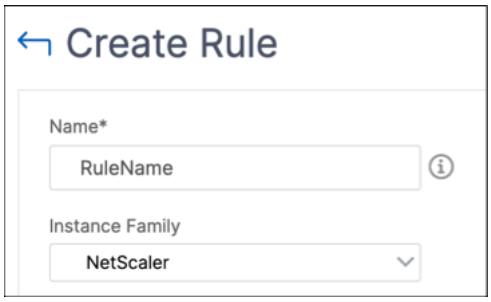
1. Specify name and instance family
2. Configure event age
3. Choose severity of the event that the rule detects
4. Specify category of the event
5. Specify NetScaler instances to which the rule applies
6. Select failure objects
7. Specify advanced filters
8. Specify actions to be taken when the rule detects an event

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



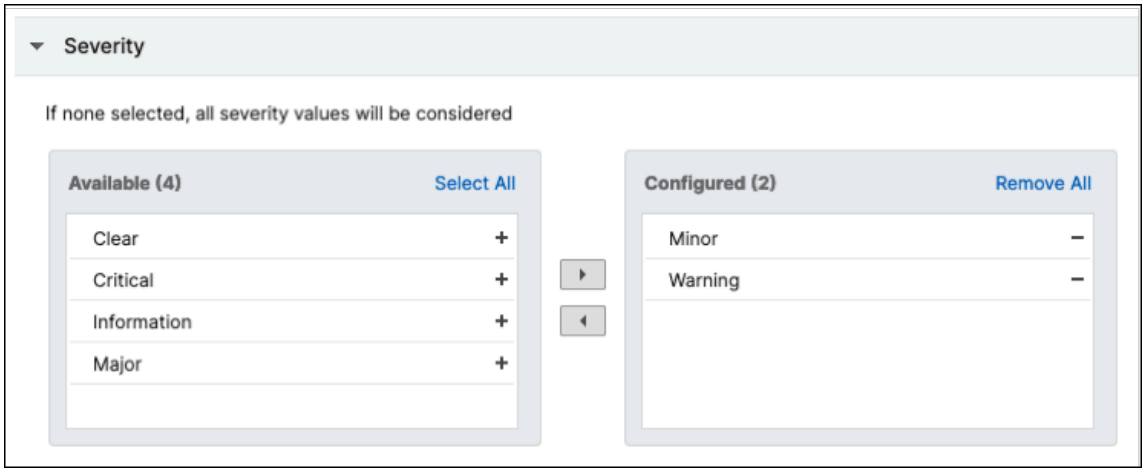
3. **Enable Advanced Filter with Regex Matching**. Select this option to include a regular expression other than asterisk (*) pattern matching. This option is applicable for failure objects, configuration commands, and messages.

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.

  > **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

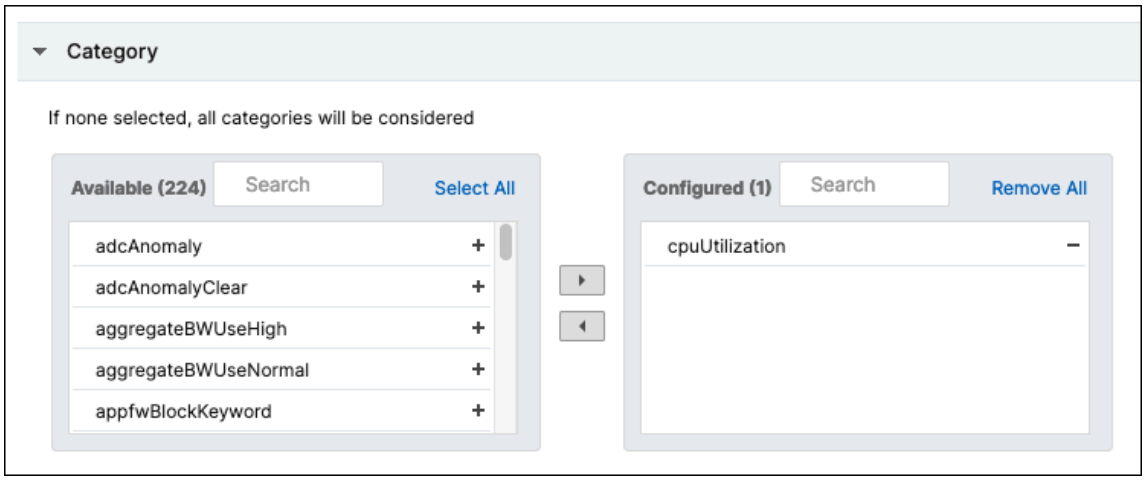
You can specify the category or categories of the events generated by your NetScaler instances. All categories are created on NetScaler instances. These categories are then mapped with the NetScaler

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

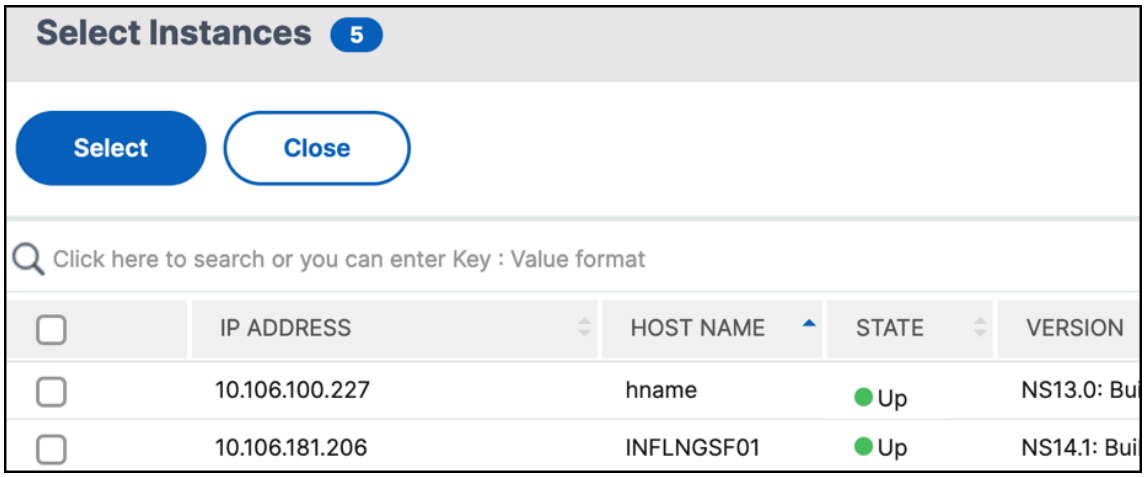
  In the example, you must choose “cpuUtilization”as the event category from the table displayed.



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**.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Step 6 - Select failure objects

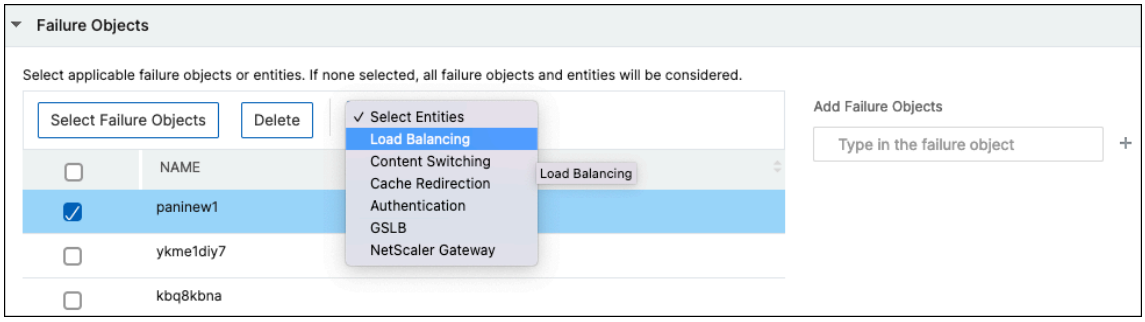
Failure objects are entity instances or counters for which an event has been generated.

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.

   > **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.



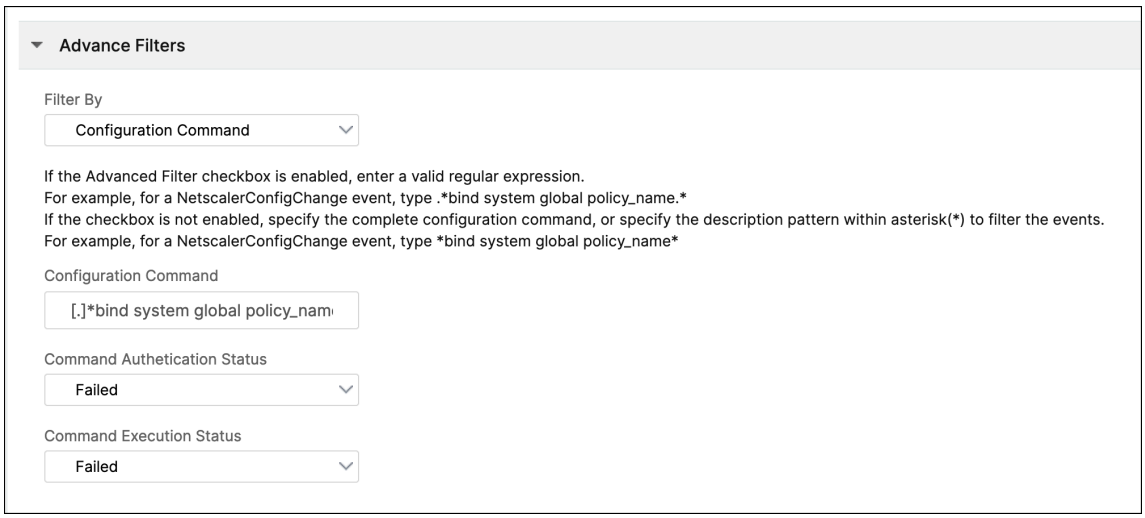
Step 7 - Specify advanced filters

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.

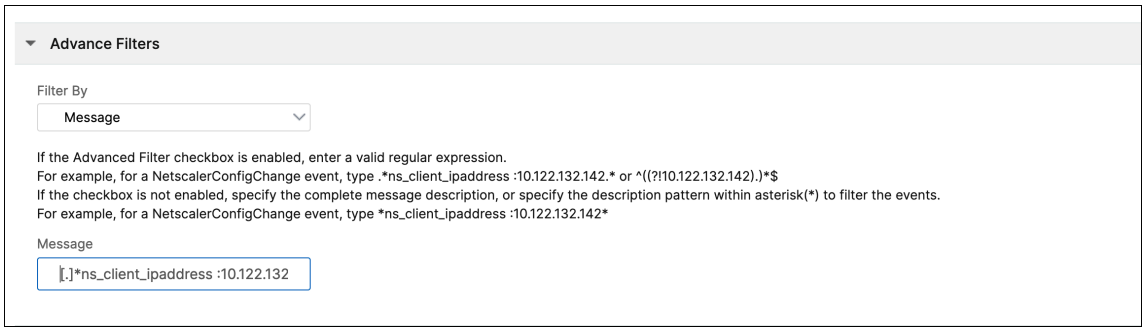
  You can also filter the event rules by the command's authentication status and its execution status. For example, for a `NetscalerConfigChange event`, type `[.]*bind system global policy_name[.]*`.

© 1997–2025 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

© 1997–2025 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.

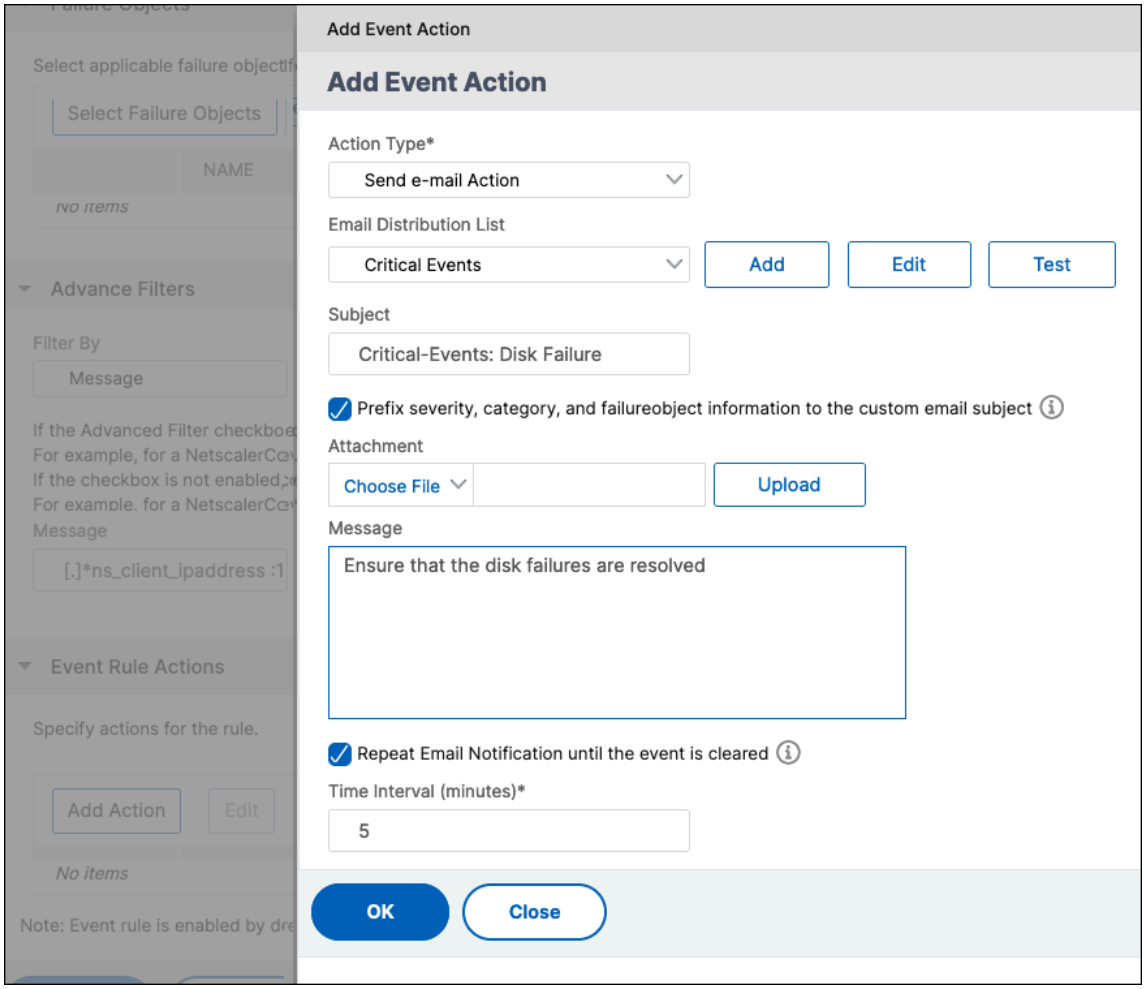
1. **Email Distribution List**. Select an email distribution list. To add a distribution list, click Add.
    a) In the **Create Email Distribution List** page, do the following:
        i. **Name**. Add a name for the distribution list.
        ii. **Email Servers**. Select an email server. You can 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.
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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.

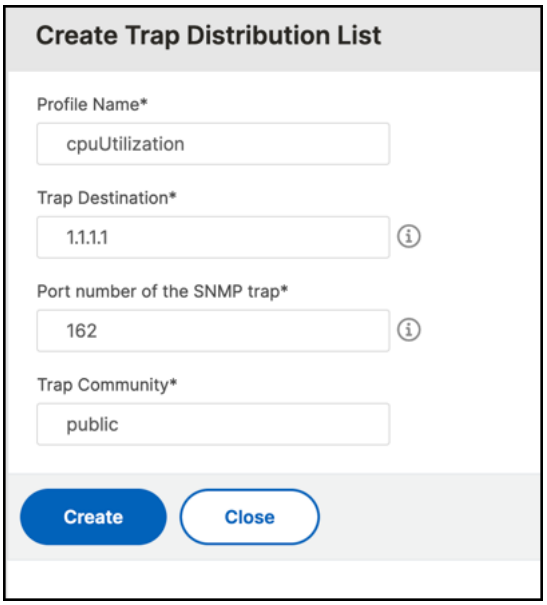
> **Note:**
>
> You can also add the email distribution lists by navigating to **Settings** > **Notifications** > **Email**. Click **Add** and create the list.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

$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.

  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":"" }
 }
'
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
12  url="http://$source/nitro/v1/config/lbvserver"
13  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.

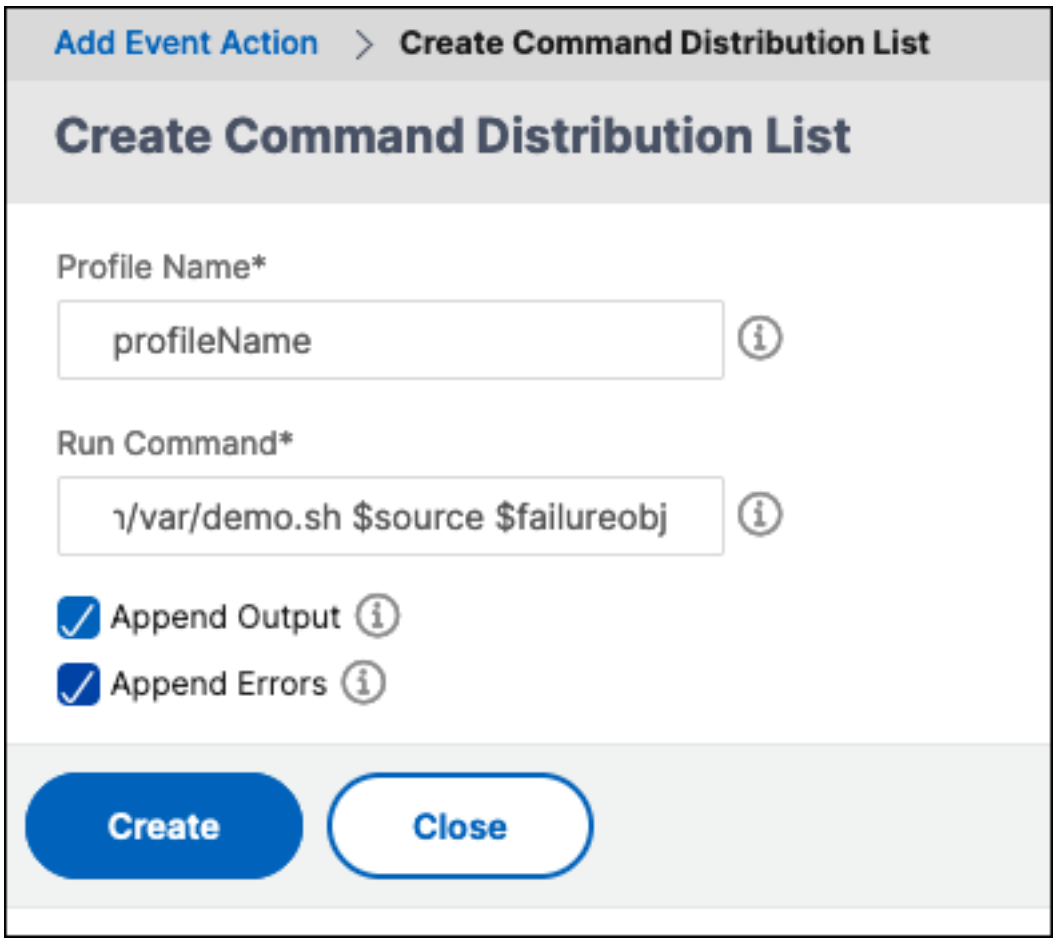
   c) Select **Append Output** and **Append Errors**

   > **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.

   d) Click **Create**.

2. In the **Add Event Action** page, click **OK**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



> **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

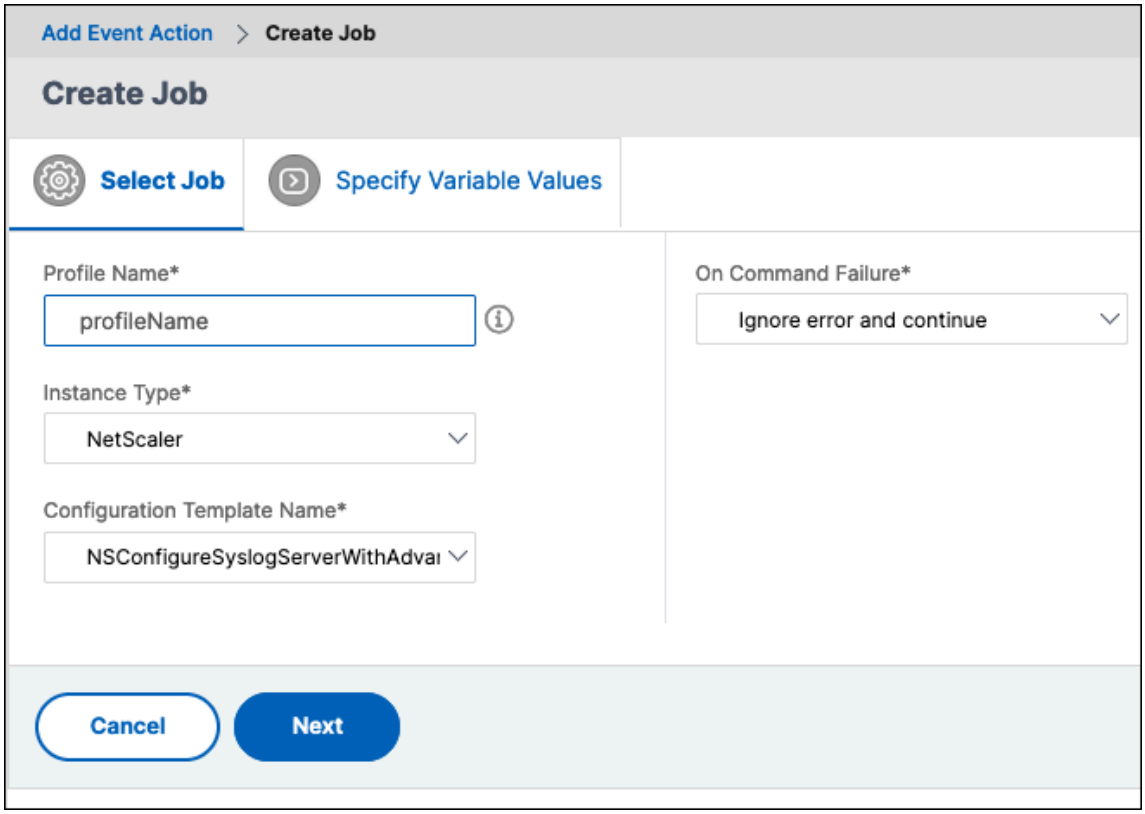
When you create a profile with configuration jobs, a job is run as a built-in job or a custom job for NetScaler and NetScaler SDX instances for events and alarms that match the filter criteria you've specified.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

b) **Specify Variable Values**. Based on the instance type selected and the configuration template chosen, specify your variable values.

c) Click **Finish** to create the job.

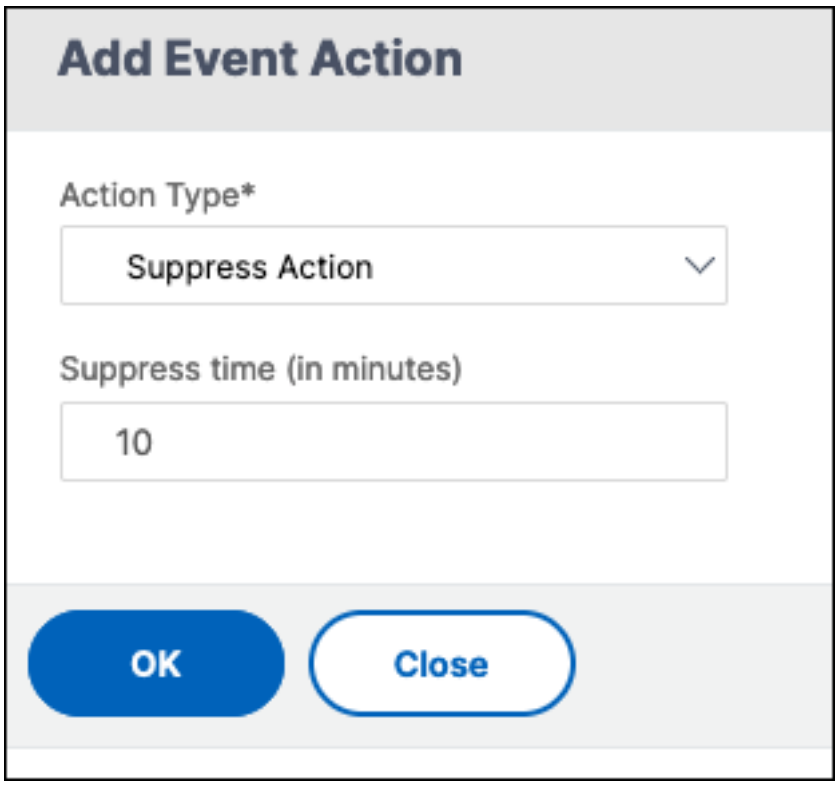


3. Click **OK**.

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.

© 1997–2025 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:
   a) **Profile Name**. Enter a profile name of your choice.
   b) **Integration Ke**y. 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

1. In **ServiceNow Profile**, select the **Citrix_Workspace_SN** profile from the list.
2. Click **OK**.

Schedule an event filter

February 14, 2024

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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

January 8, 2024

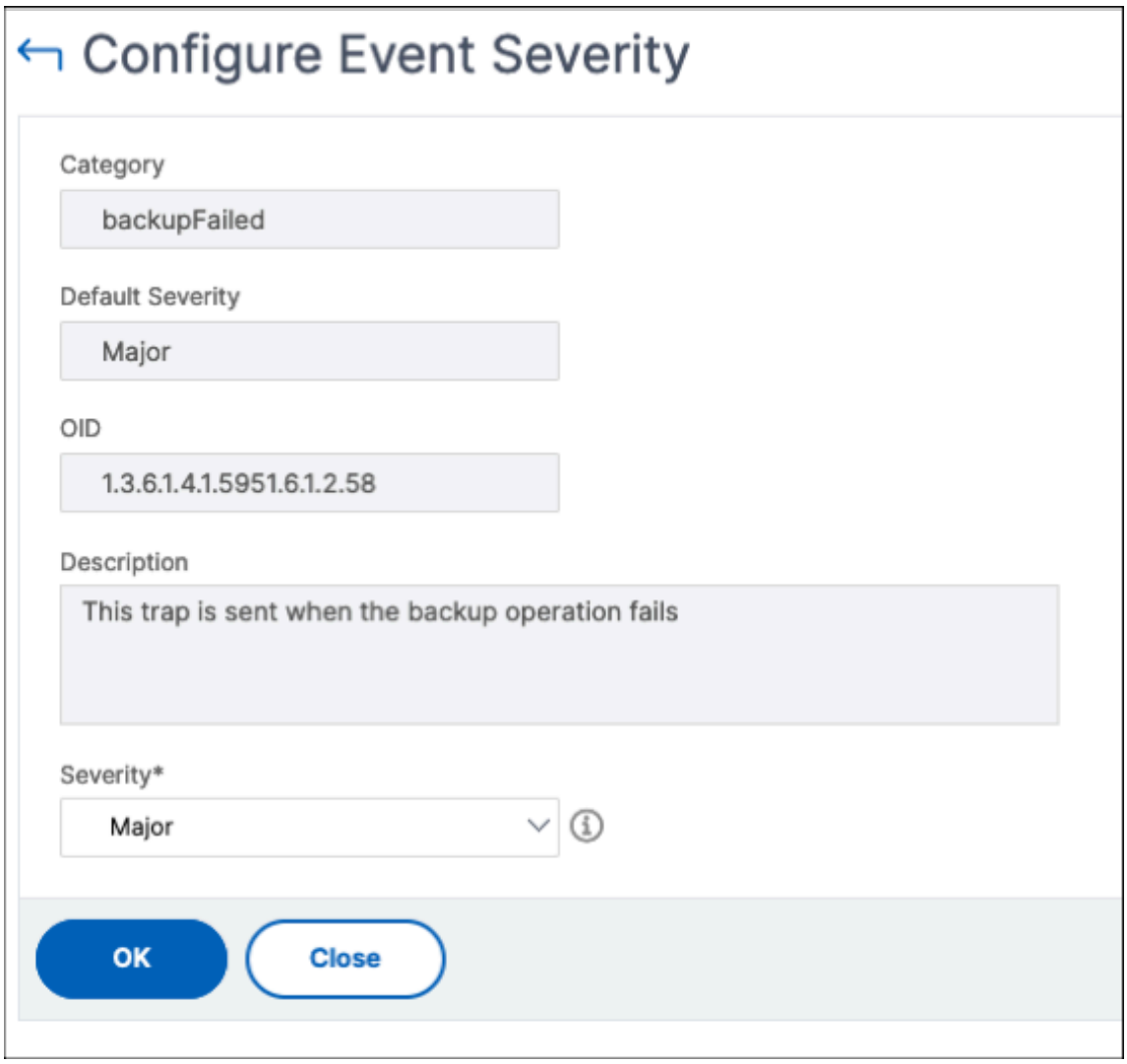
You can manage the reporting of events generated on all your devices, so that you can view event details regarding a particular event on an instance and view reports based on event severity. Also, you can create event rules that use the default severity settings, and you can change the severity settings. 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:

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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



View events summary

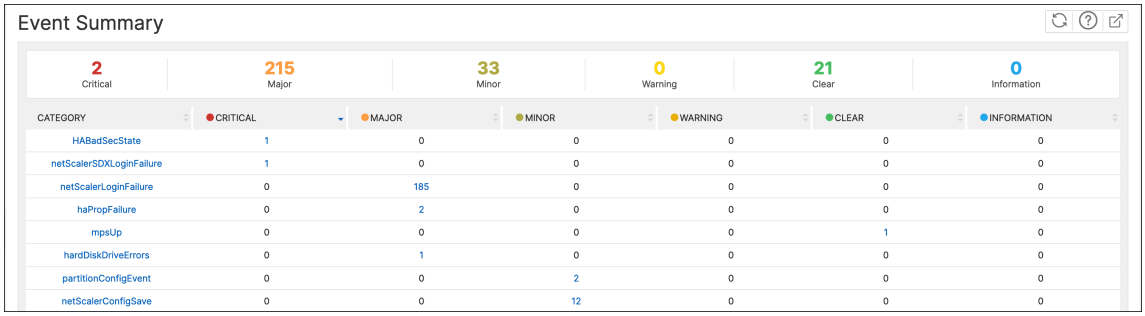
September 8, 2025

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 to the NetScaler Console. During the event, a notification is sent to an administrator, explaining the reason for

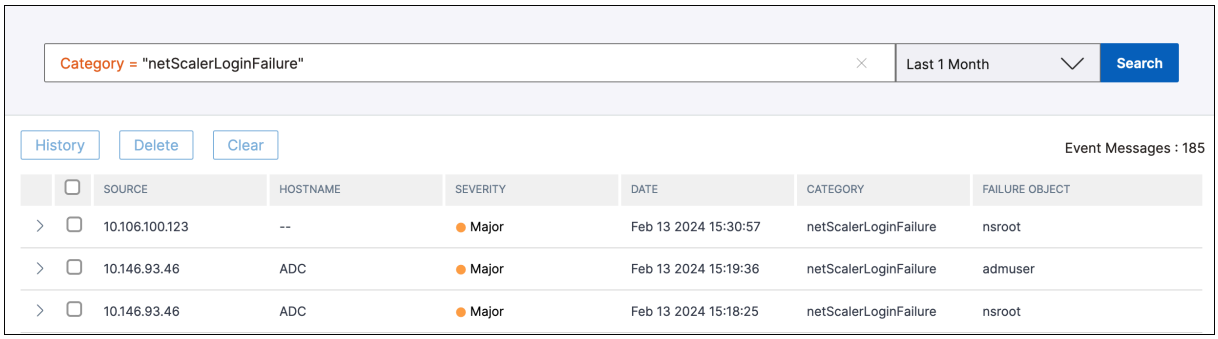
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:

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.

© 1997–2025 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.

Display event severities and SNMP trap details

February 14, 2024

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.

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,

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.



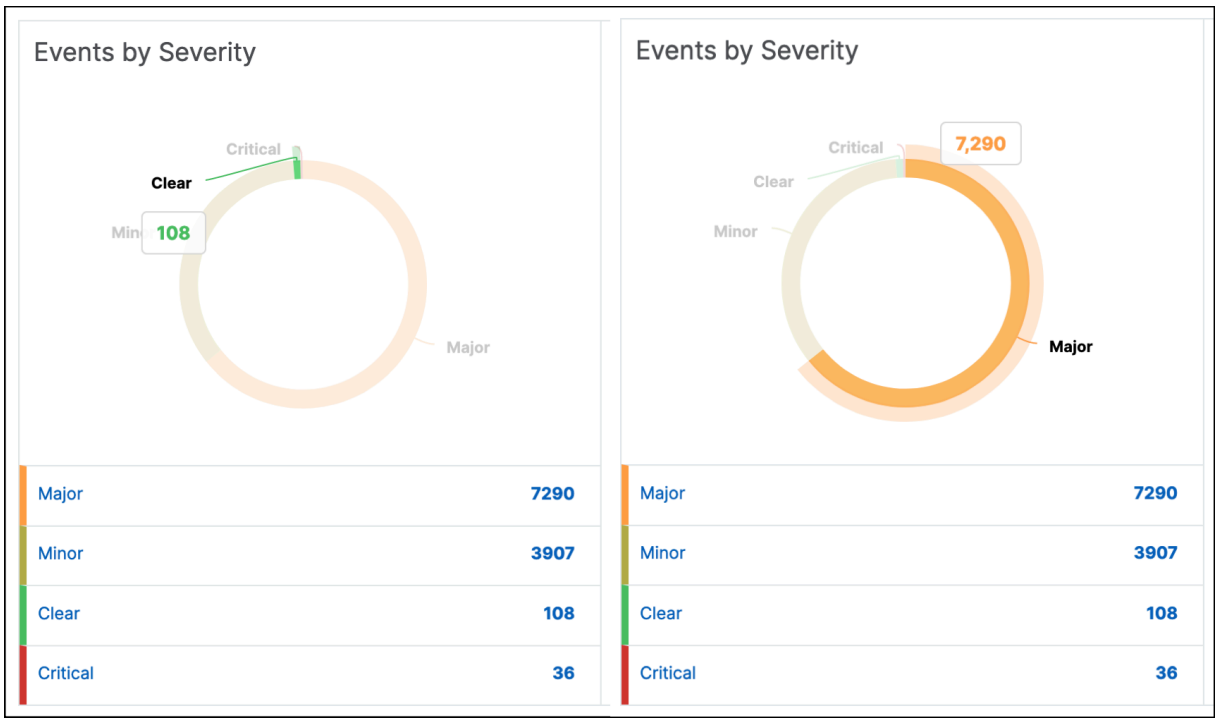
4. The **Events by Severity** donut chart displays a visual representation of all the events by their severity. Different types of events are represented as different colored sections, and the length of each section corresponds to the total number of events of that type of severity.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

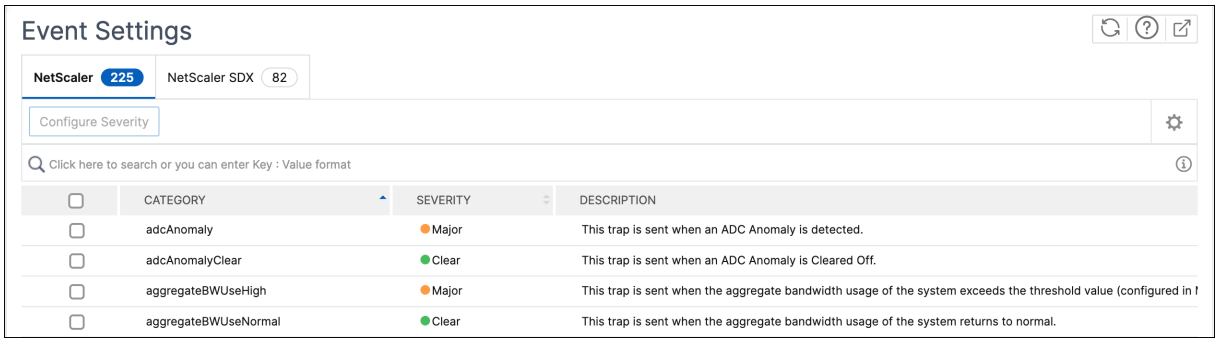


To view NetScaler SNMP trap details on NetScaler Console:

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."



© 1997–2025 Citrix Systems, Inc. All rights reserved.

View and Export syslog messages

June 6, 2024

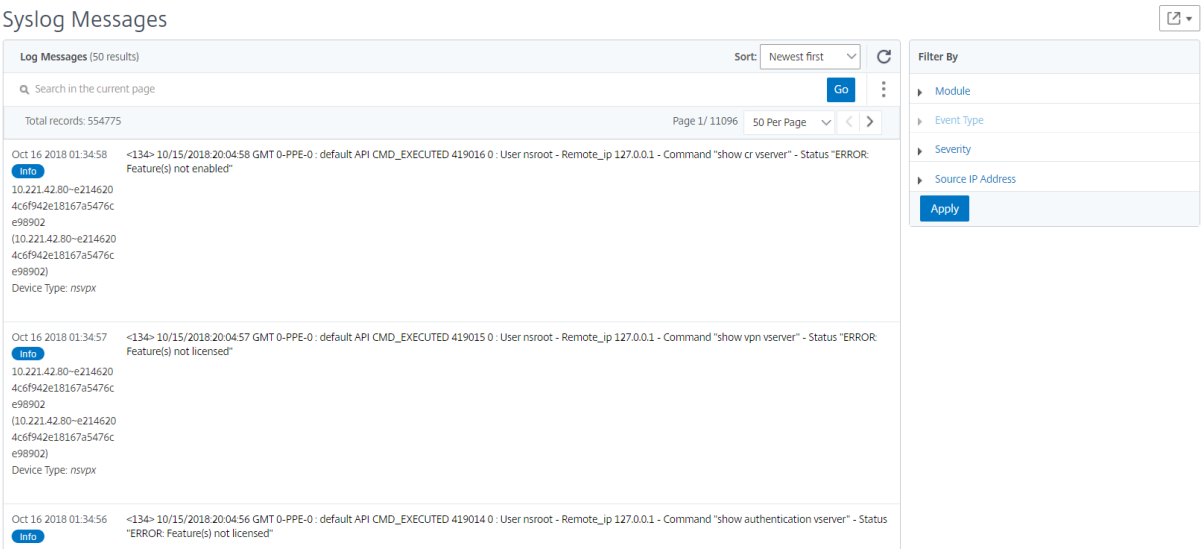
You can view syslog messages without logging into NetScaler Console, by scheduling an export of all syslog messages received on the server. You can export syslog messages that are generated on your Citrix Application Delivery Controller (NetScaler) instances in PDF, CSV, PNG, and JPEG formats. Also, 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.

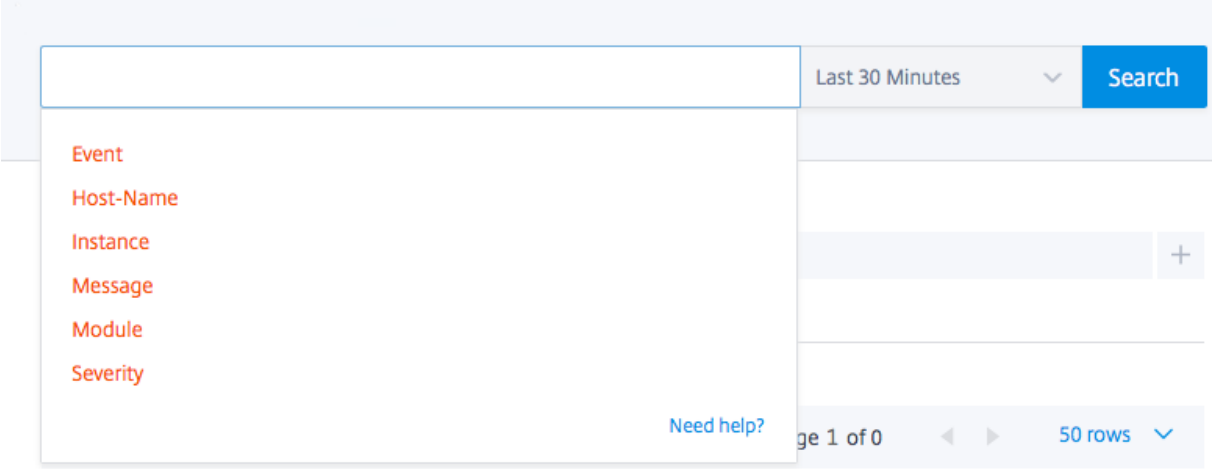


Search syslog messages

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.



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.

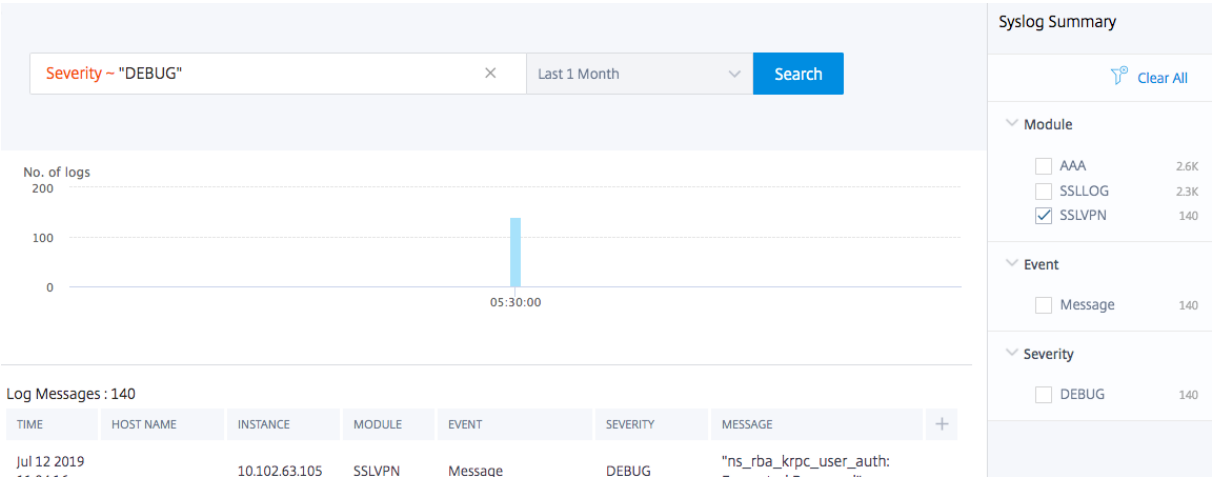
To search audit log messages for all applications present in the NetScaler Console, from the NetScaler Console GUI, navigate to **Infrastructure > Network Functions > Auditing**.

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.

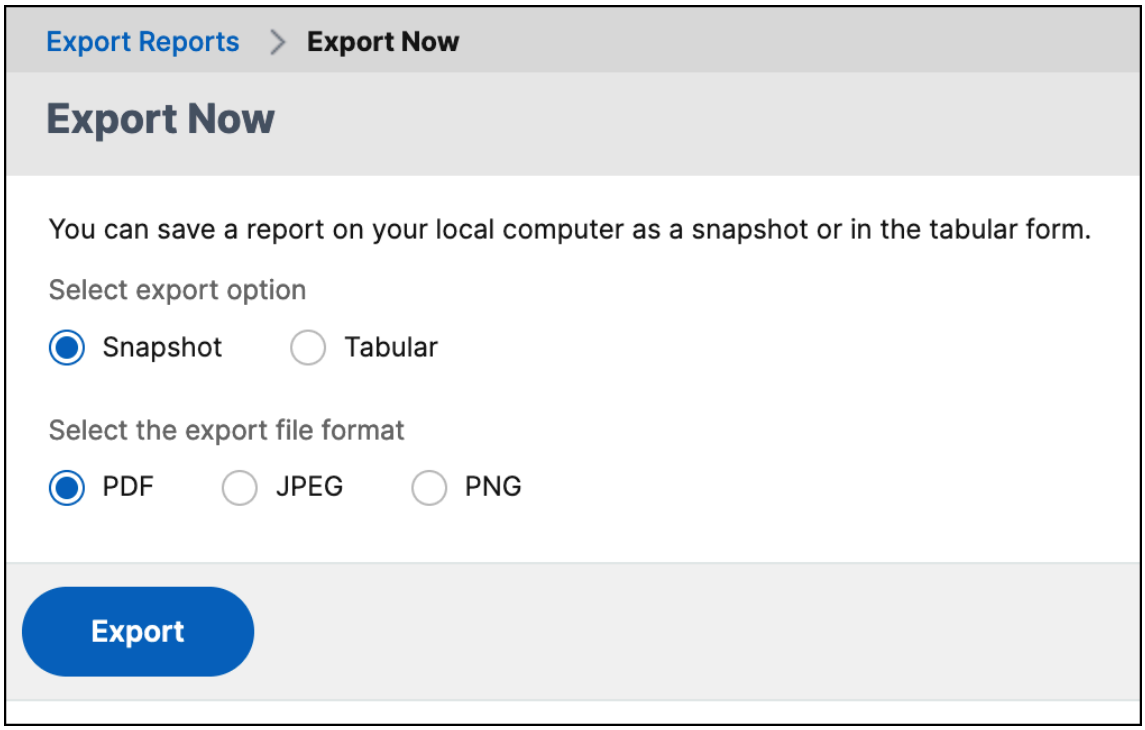
© 1997–2025 Citrix Systems, Inc. All rights reserved.



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:

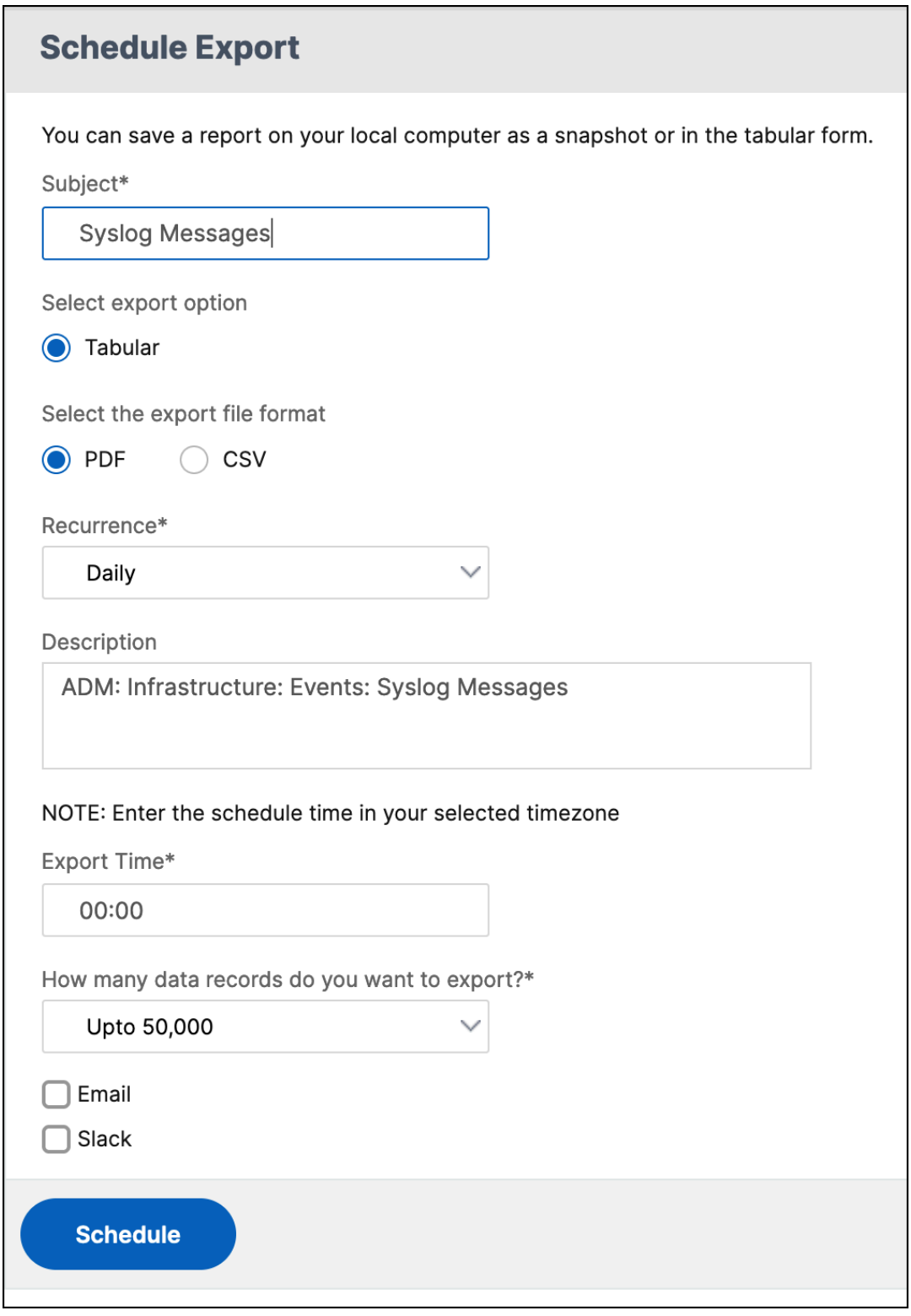
1. Navigate to **Infrastructure > Events > Syslog Messages**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 meets the scheduled time criteria. If you want to create an email distribution list, click **+** and provide mail server and mail profile details.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Suppress syslog messages

June 6, 2024

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.

> **Note:**
>
> If different users have different access to multiple NetScaler instances, different filters

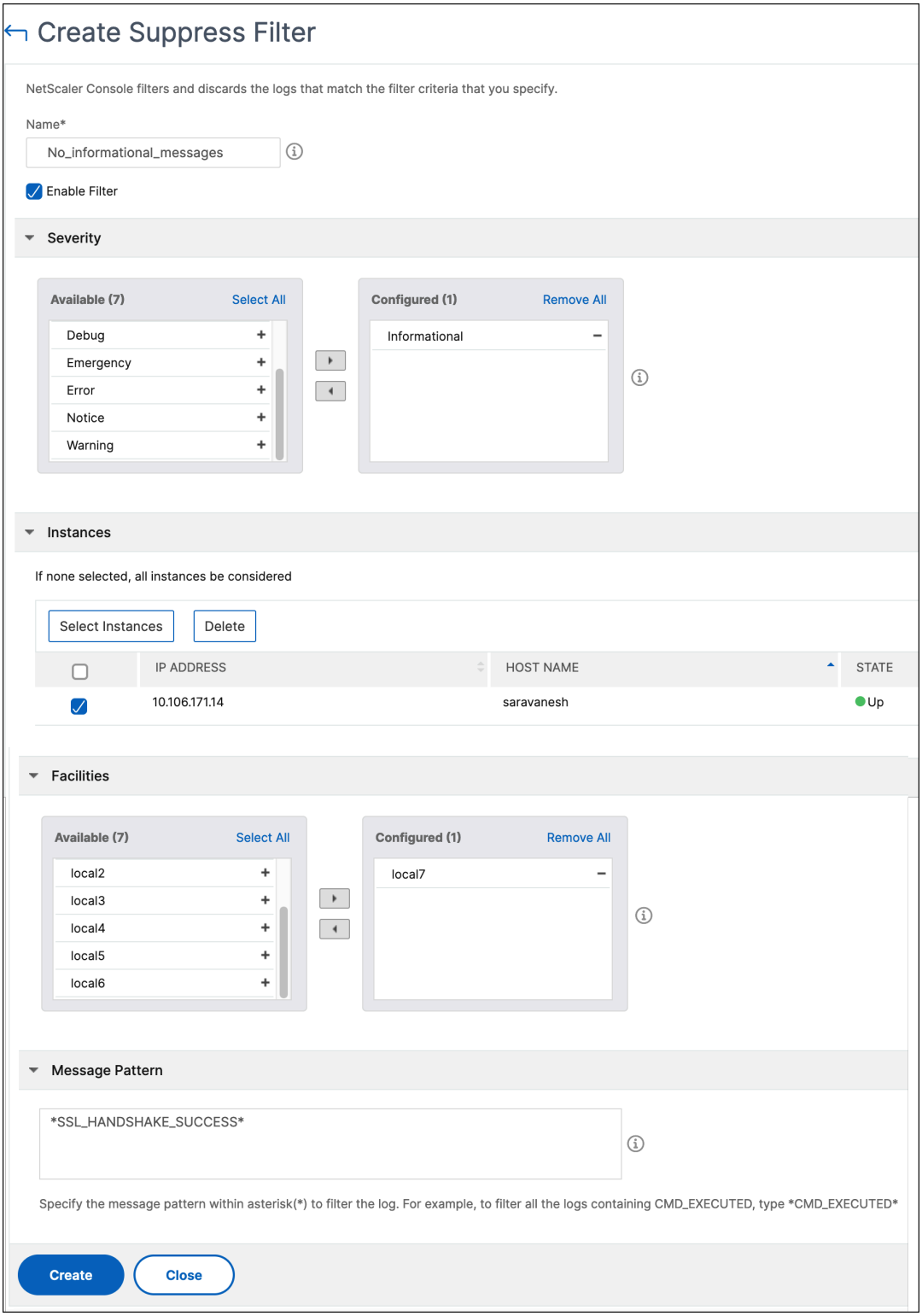
© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



d) **Facilities** - Select the facility to suppress messages based on the source that generates them.

e) **Message Pattern** - You can also type a text pattern surrounded by asterisks (*) to suppress

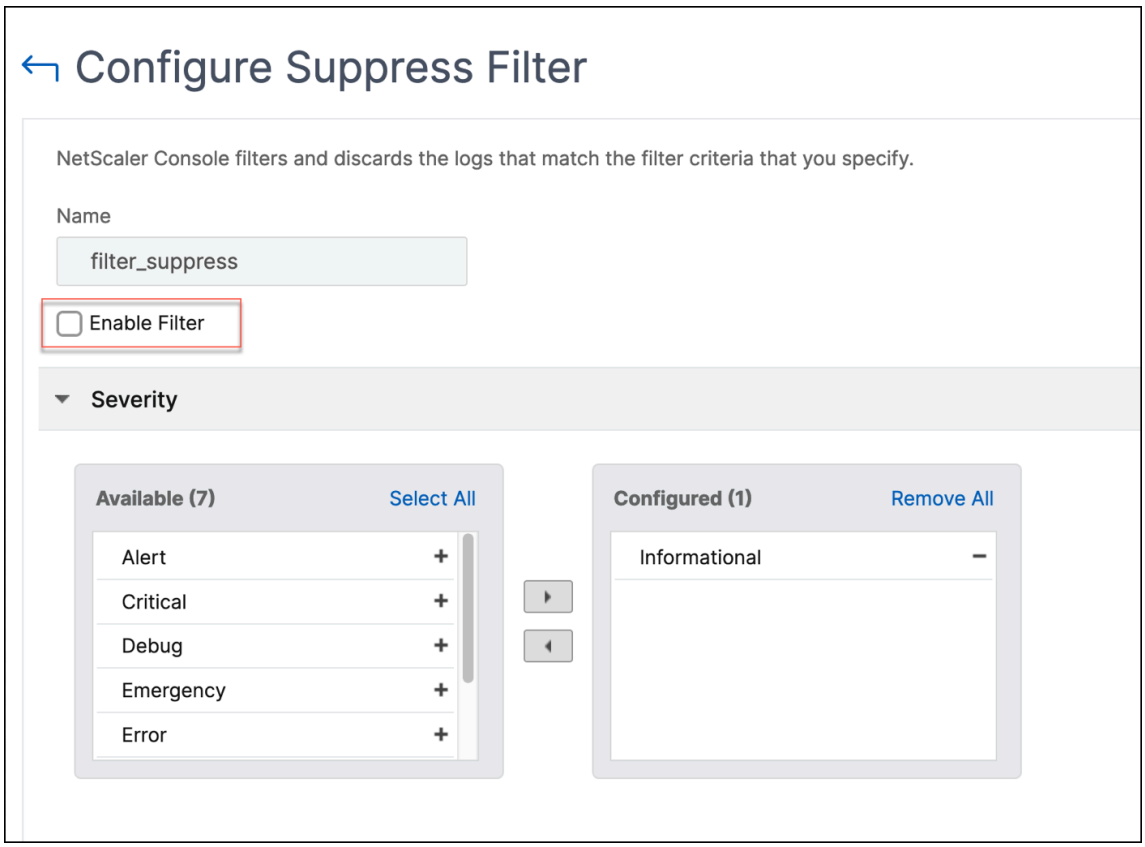
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

April 19, 2024

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 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.

Zero-touch certificate management

September 8, 2025

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,

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

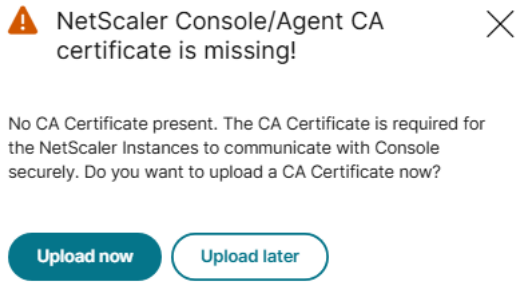
With zero-touch certificate management, the following processes are automatically done by NetScaler:

- 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
- 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:

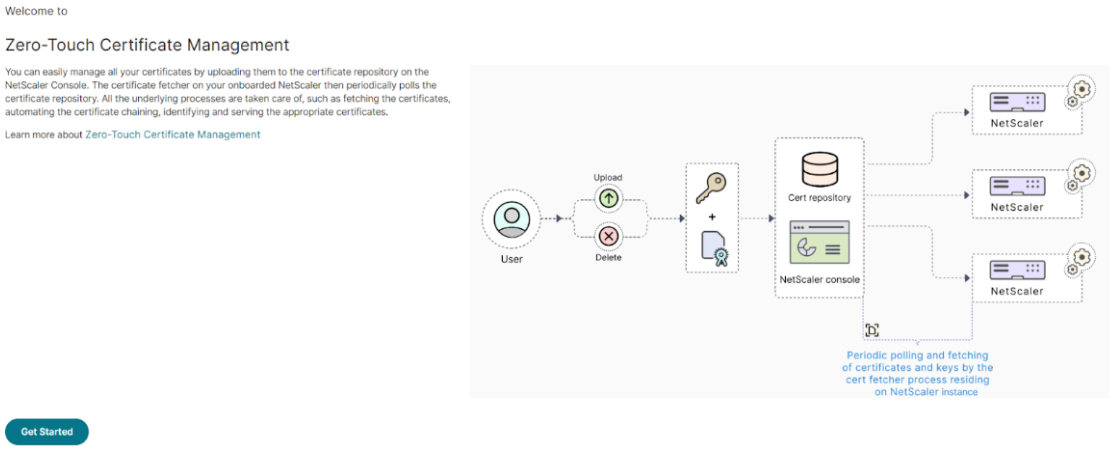
- NetScaler instances are running build 14.1-43.x or later and they are managed in NetScaler Console.
- Upload the certificates (in any format) and keys. Then, enable zero-touch on the managed NetScaler instances.
- Ensure that a valid CA certificate is present on NetScaler Console. If you have an updated 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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



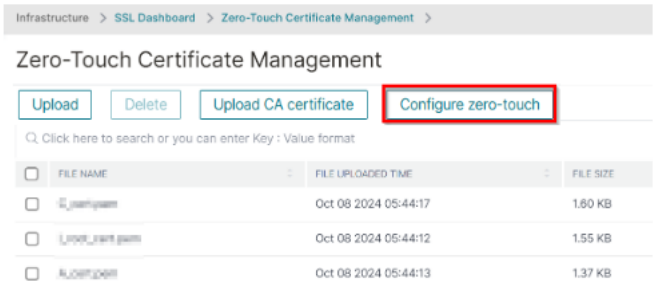
3. NetScaler instances running build 14.1-43.x or later are listed. You can either click **Configure zero-touch** to enable zero-touch or click **Skip** to proceed the next step.
4. Click **Upload** to upload all the certificates (can be in any format, such as .pem, .cer, and .crt).

> **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

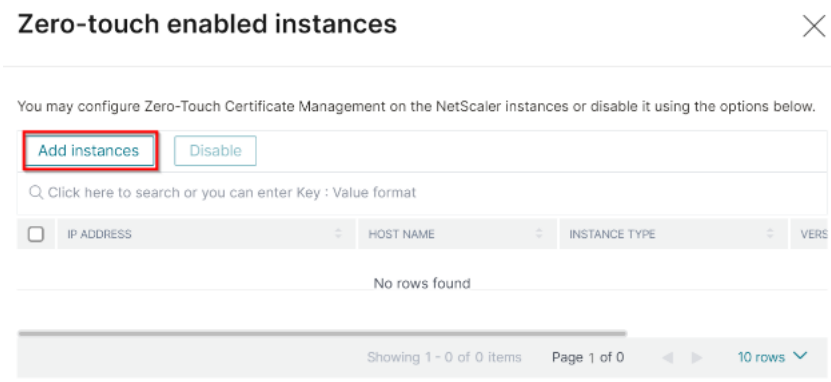
After you upload the certificates, you must enable zero-touch on the managed NetScaler instances.

1. From the **Zero-Touch Certificate Management** page, click **Configure zero-touch**.



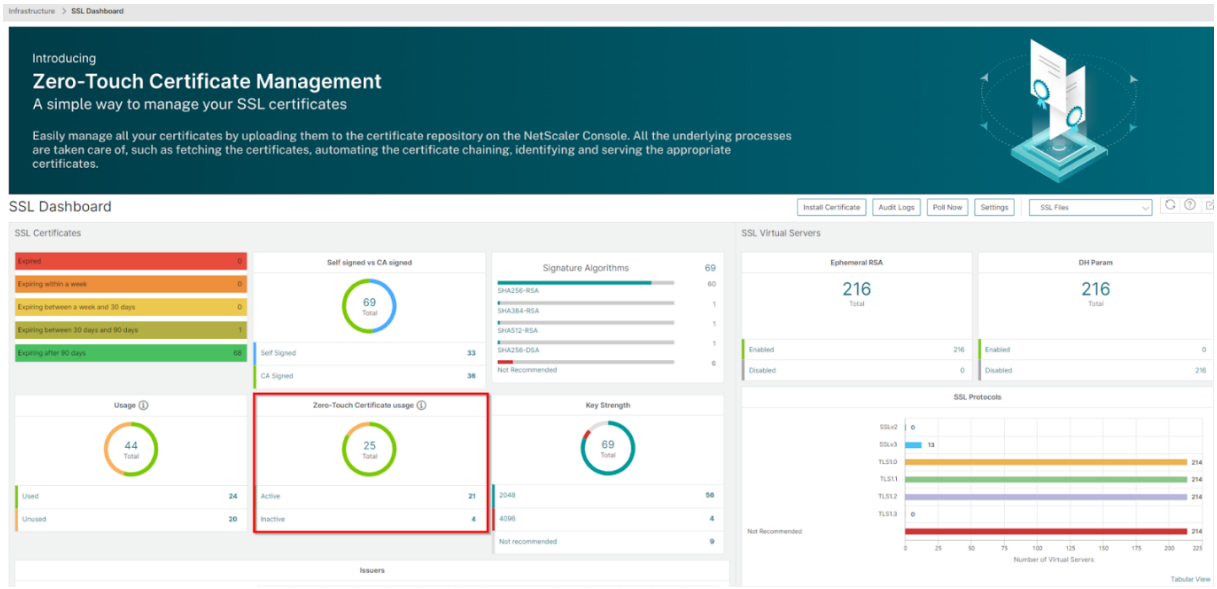
2. Click **Add instances**, select the instances, and then click **Enable**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.



Use the SSL dashboard

September 8, 2025

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

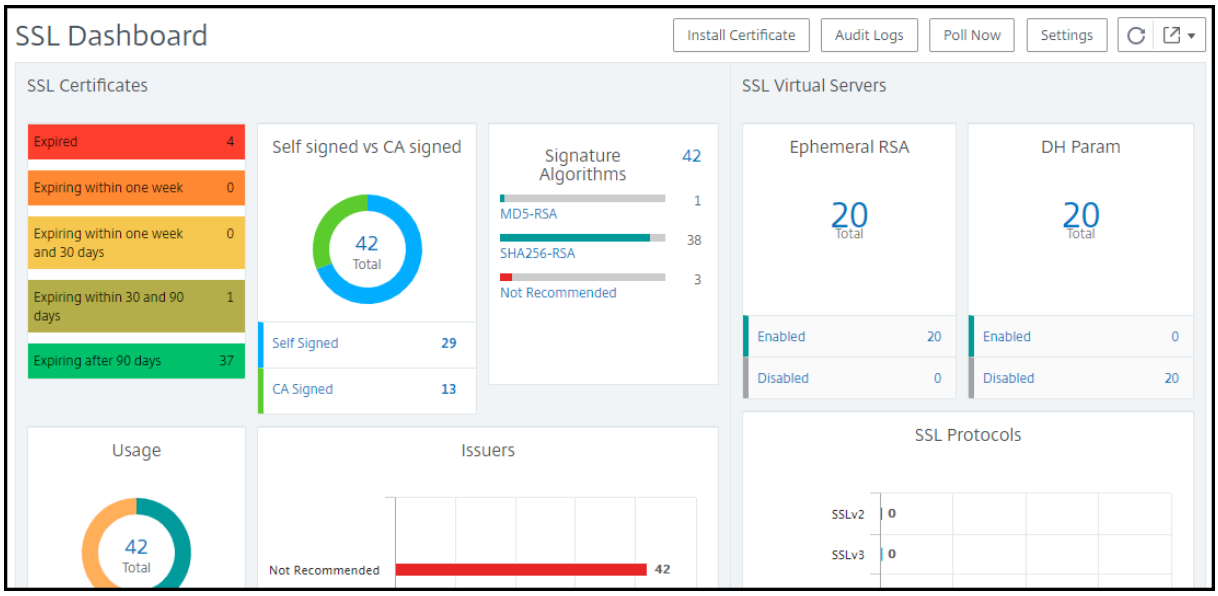
- Number of self-signed and CA-signed certificates
- Number of issuers
- Signature algorithms
- SSL protocols
- Top 10 instances by number of certificates in use

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.

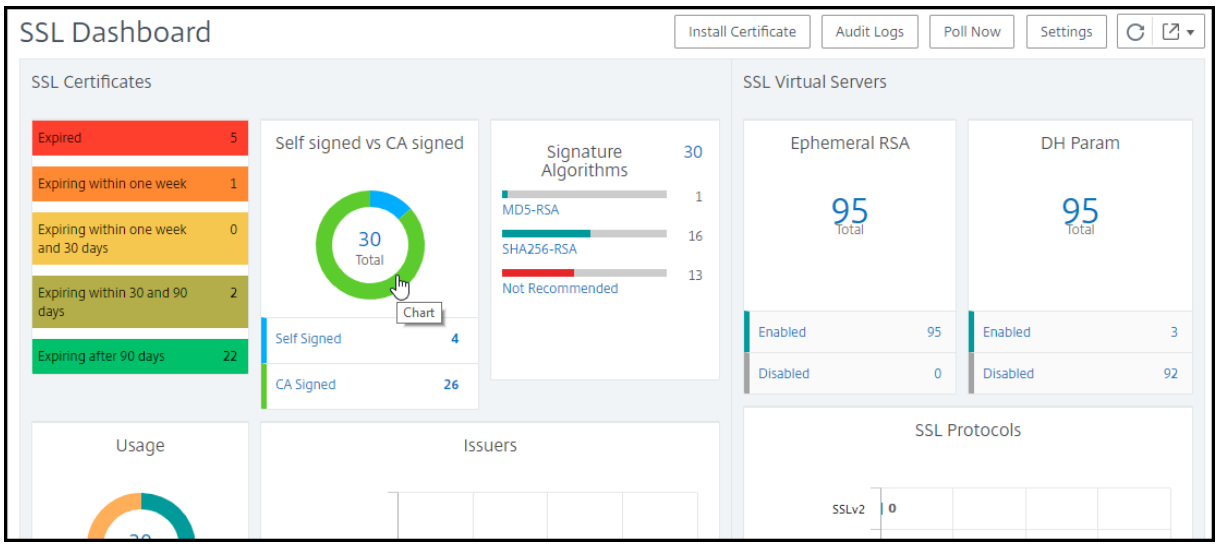
To monitor SSL certificates in NetScaler Console, navigate to **Infrastructure > SSL Dashboard**.



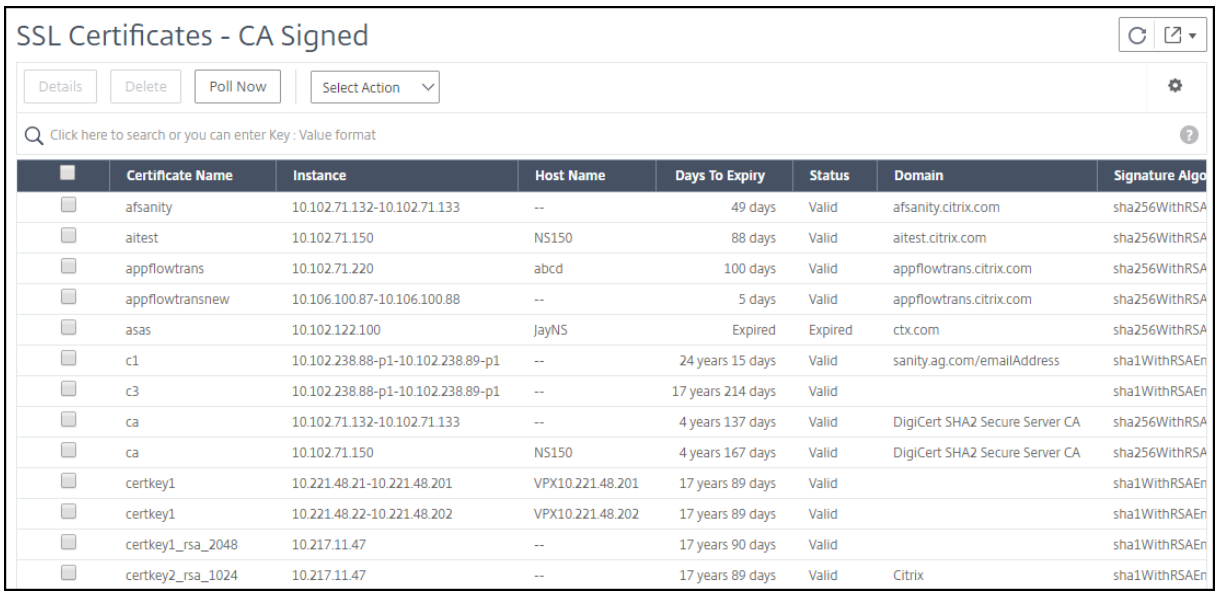
NetScaler Console allows you to poll SSL Certificates and add all the SSL certificates of the instances immediately to NetScaler Console. To do so, navigate to **Infrastructure > SSL Dashboard** and click **Poll Now**. The **Poll Now** page pops up, presenting the option to poll all NetScaler instances 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.

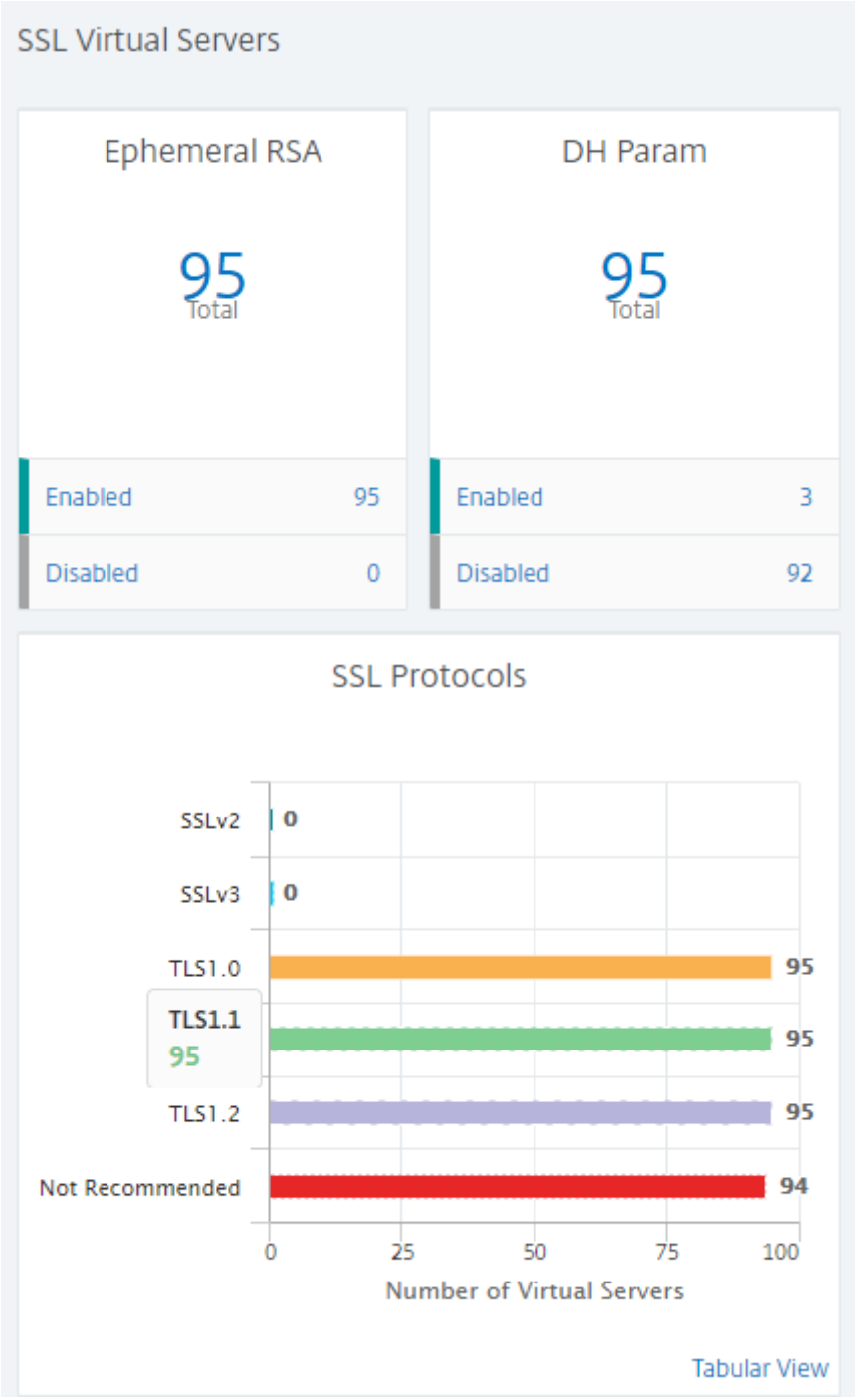


Certificate Name	Instance	Host Name	Days To Expiry	Status	Domain	Signature Algo
afsanity	10.102.71.132-10.102.71.133	--	49 days	Valid	afsanity.citrix.com	sha256WithRSA
aitest	10.102.71.150	NS150	88 days	Valid	aitest.citrix.com	sha256WithRSA
appflowtrans	10.102.71.220	abcd	100 days	Valid	appflowtrans.citrix.com	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.

© 1997–2025 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.

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.

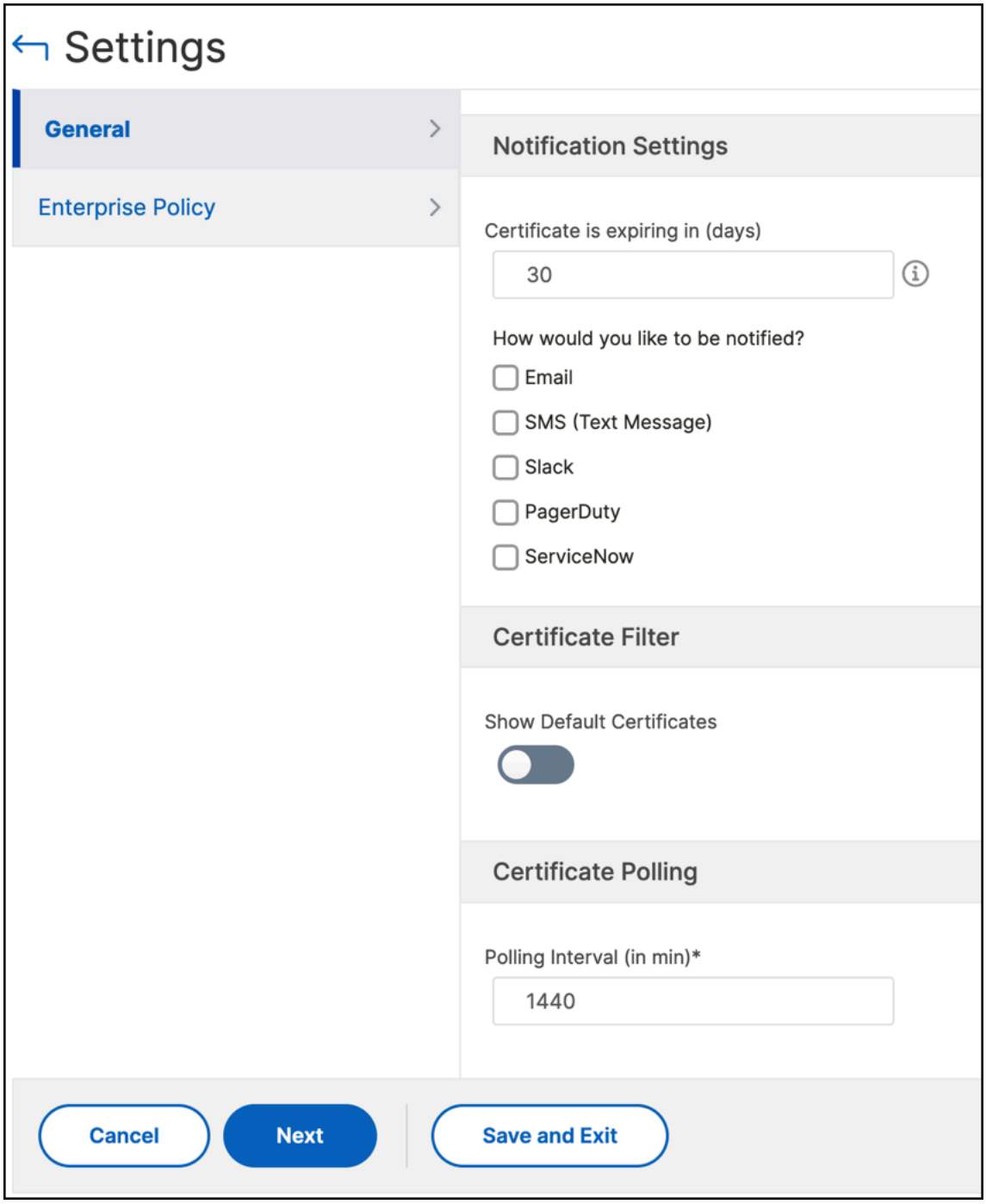
Exclude default NetScaler certificates on the SSL Dashboard

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**.

© 1997–2025 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.

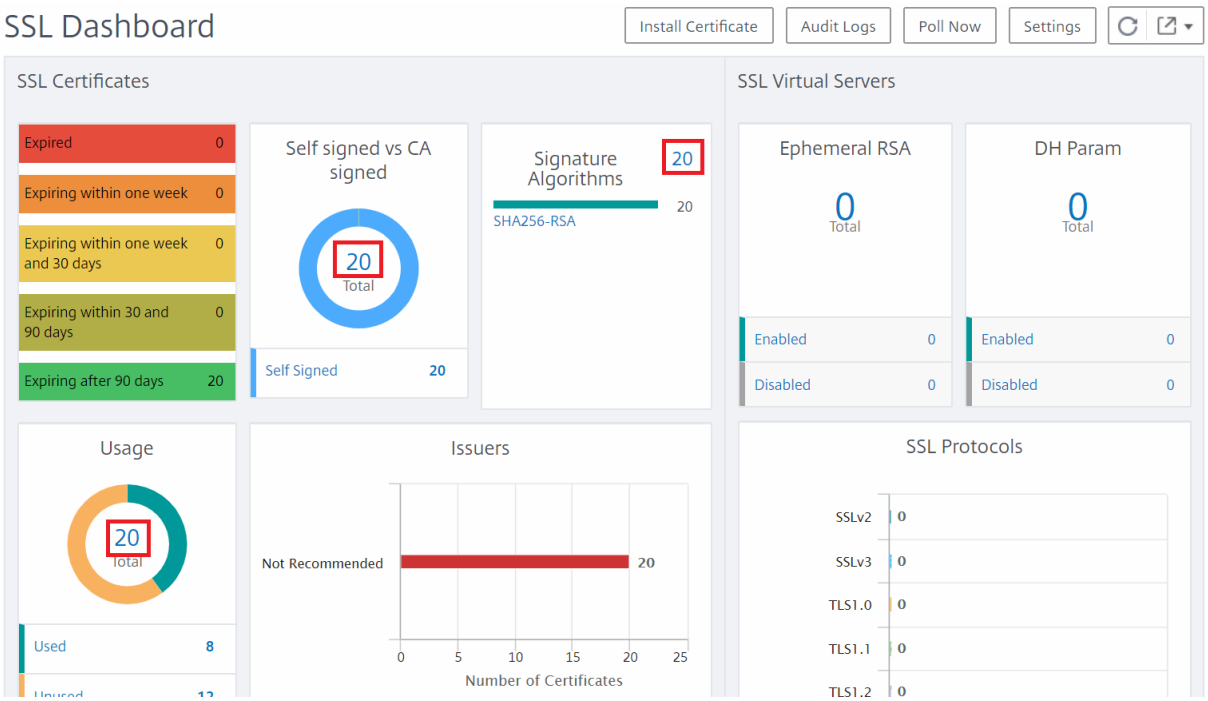
- You can select which certificates are expiring and automate certificate renewals.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Policies can be set and enforced around the types of certificates and signing authorities that are permitted.
- 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.

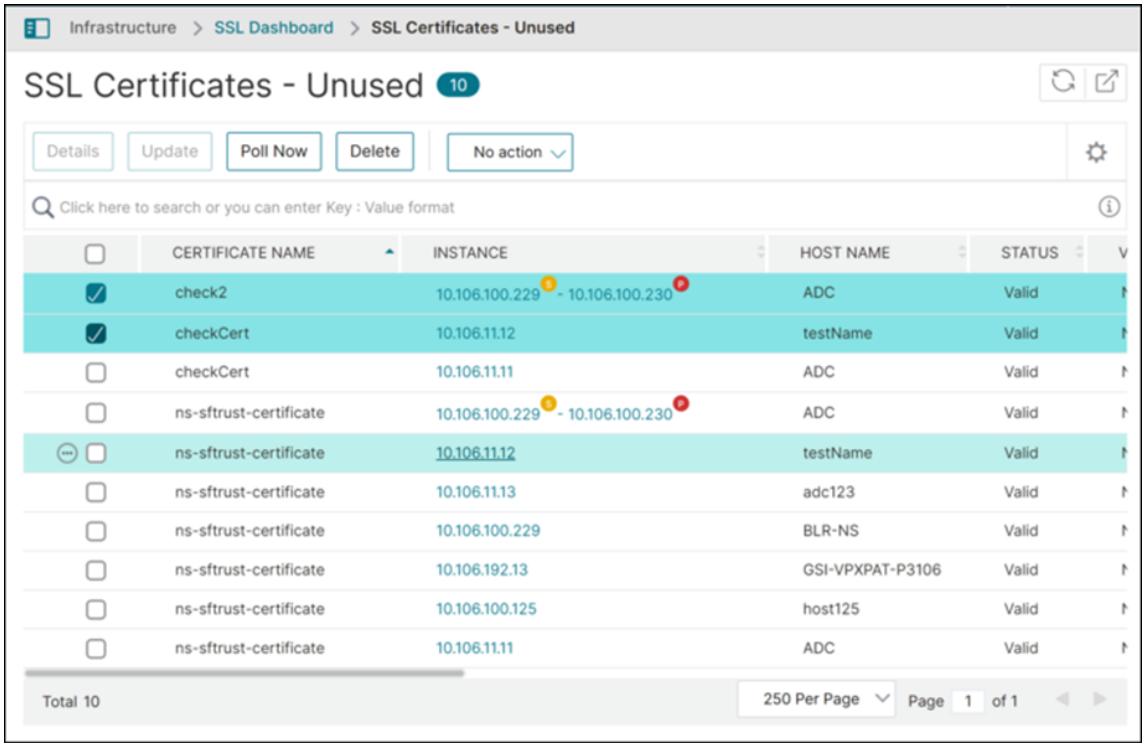
© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **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:

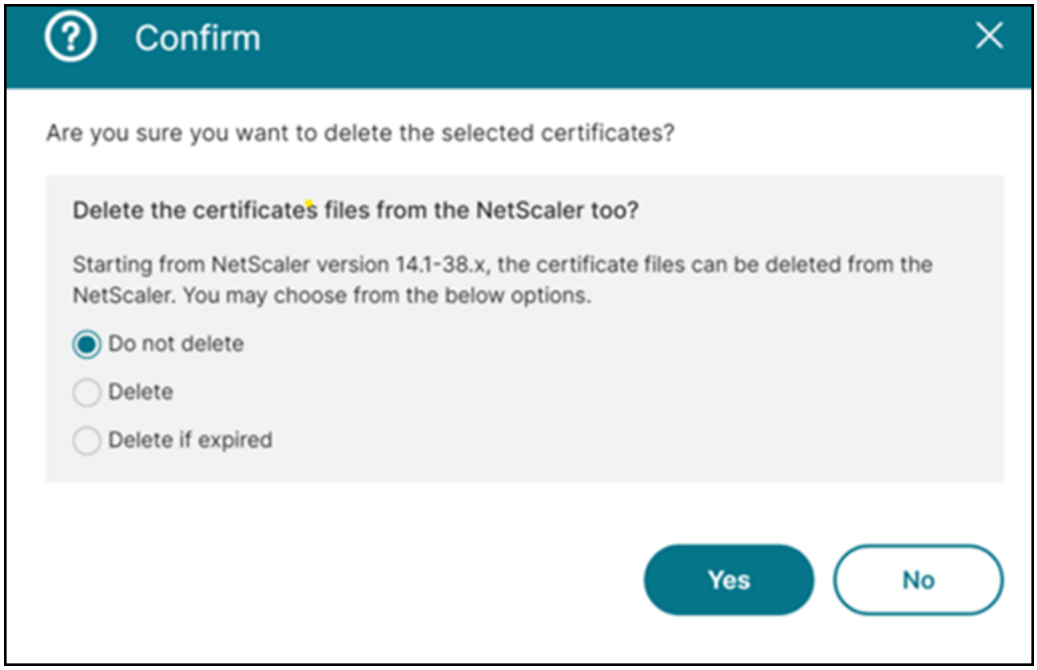
   - **Do Not Delete**: Skips the deletion of certificate files from NetScaler.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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.



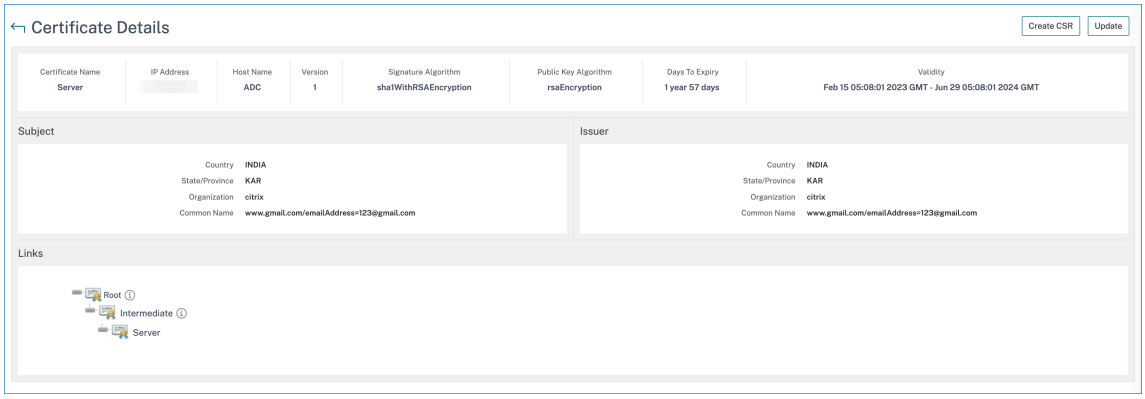
View SSL certificate chain

You can view the complete chain of links for a certificate including the intermediate certificates up to the root CA certificate.

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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Set up notifications for SSL certificate expiry

March 14, 2024

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.
    - **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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

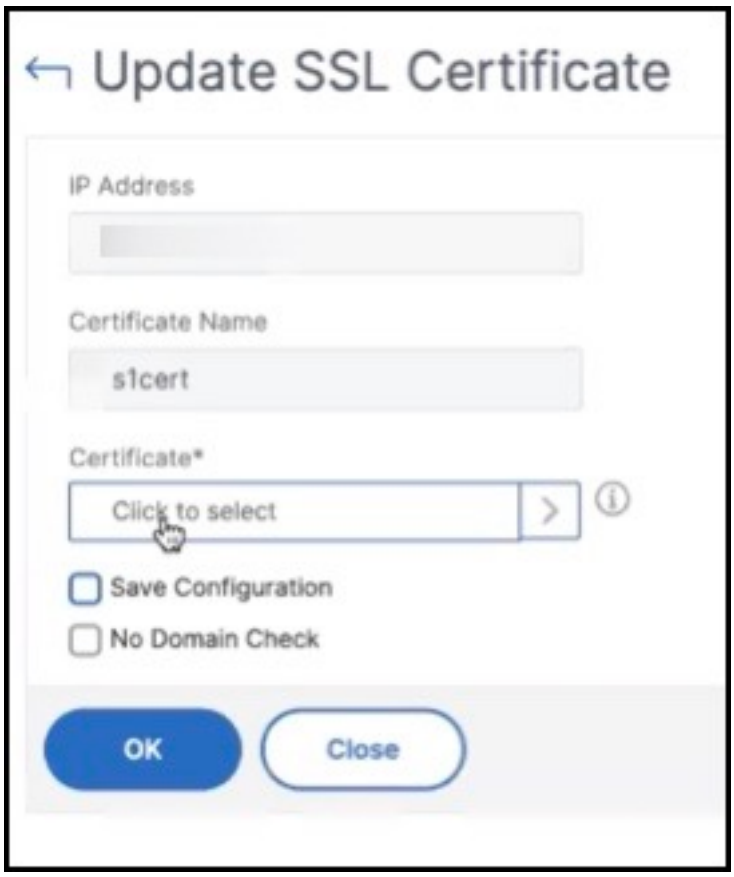
January 8, 2024

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.

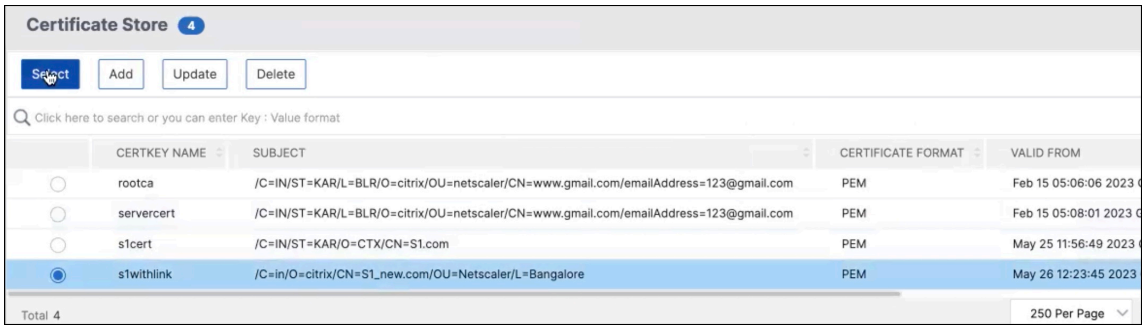
To update an SSL certificate from NetScaler Console:

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

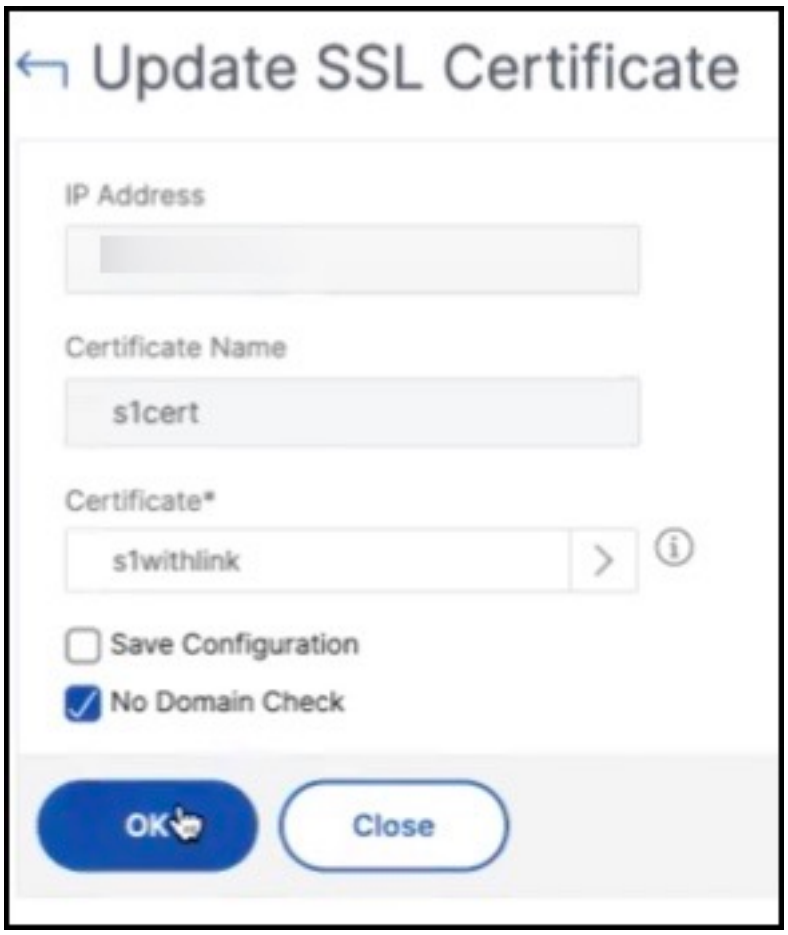


5. In the **Certificate Store** page, select the certificate file you want to add. Click **Select**.



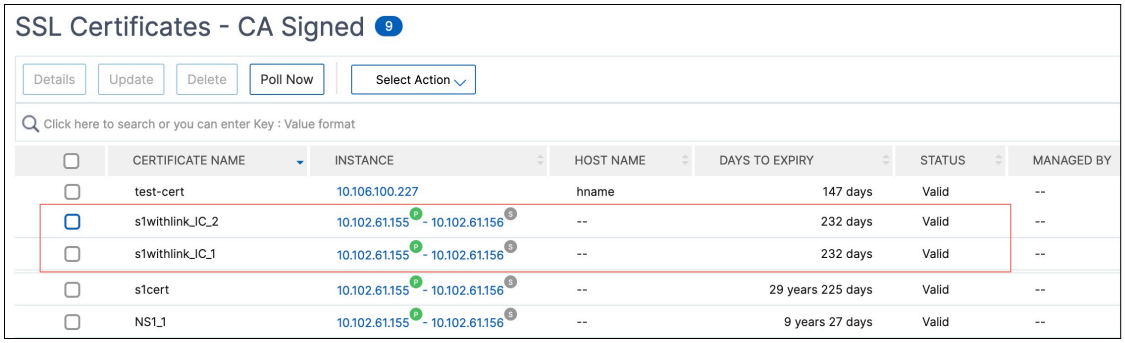
6. If the domain name of the new certificate does not match the old certificate, and you want the server to host the new domain, select **No Domain Check**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



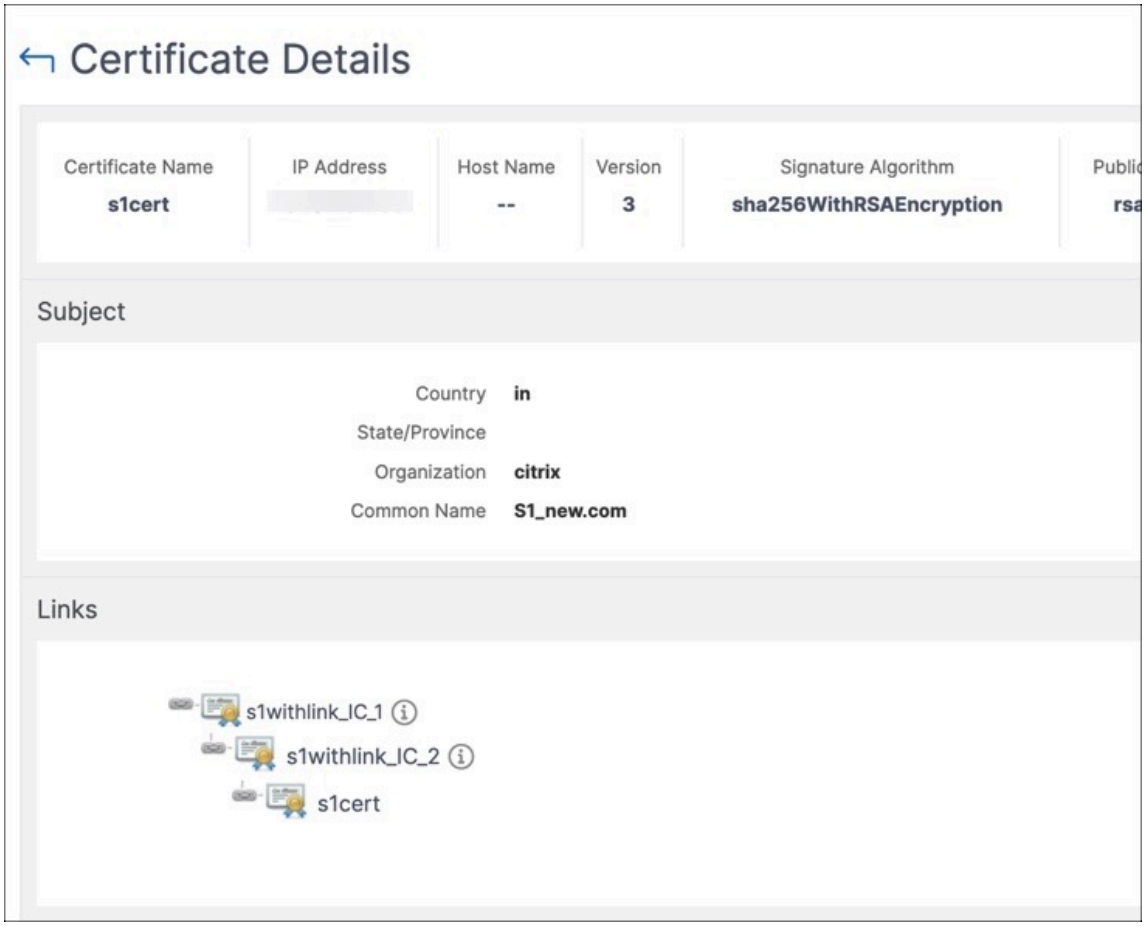
Click **OK**. All the SSL virtual servers to which this certificate is bound are automatically updated.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Install SSL certificates on a NetScaler instance

April 19, 2024

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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

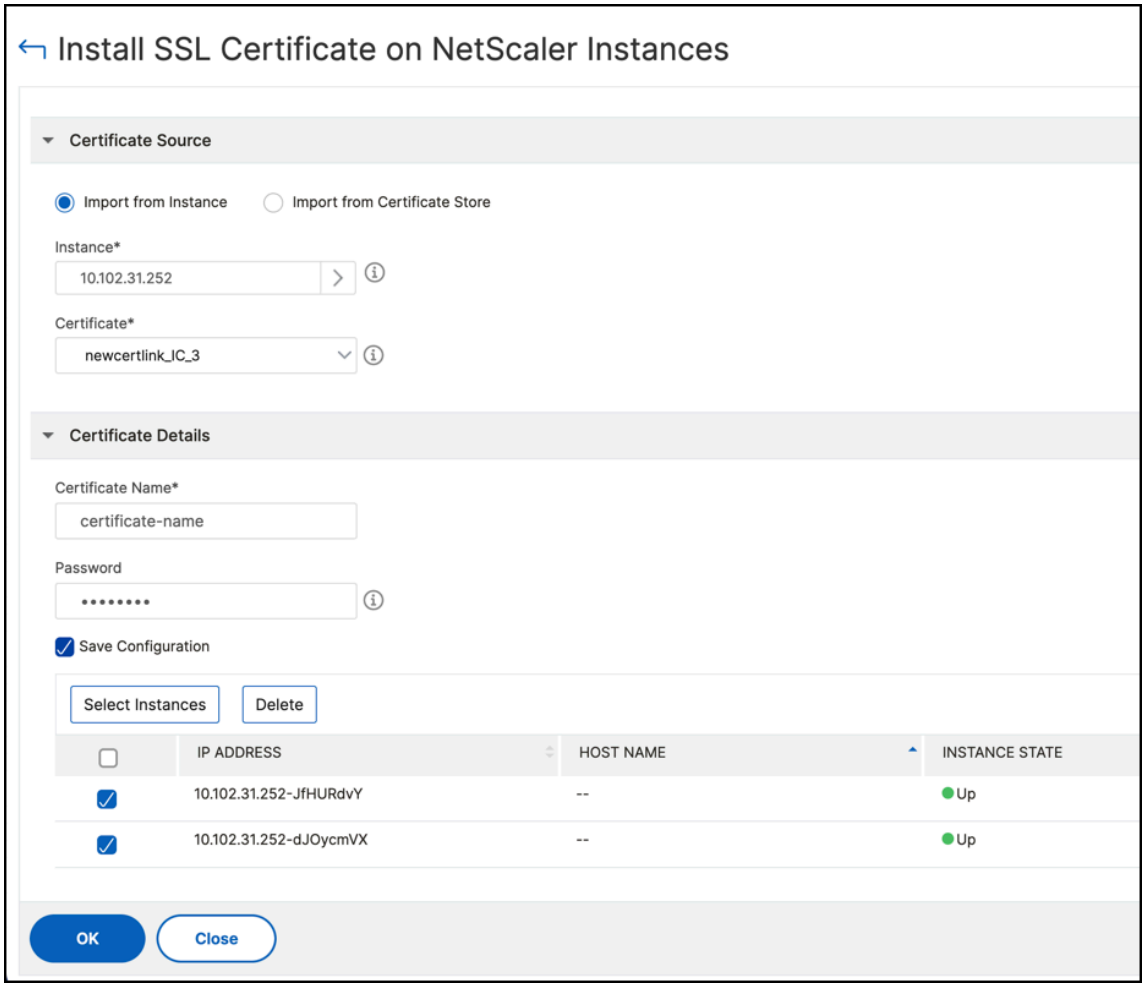
To install an SSL certificate from NetScaler Console:

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).
   - **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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Create a Certificate Signing Request (CSR)

September 8, 2025

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:

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

   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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
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

January 8, 2024

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.
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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **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

July 22, 2024

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.
    - **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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Poll SSL certificates from NetScaler instances

April 19, 2024

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**.

Use the NetScaler Console certificate store to manage SSL certificates

May 8, 2024

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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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.
   - **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

   > **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.

Configuration jobs

January 8, 2024

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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
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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> to be scheduled separated by commas.

Related Articles

- How to Use SCP (put) Command in Configuration Jobs
- How to Use Variables in Configuration Jobs
- How to Create Configuration Jobs from Corrective Commands

Create a configuration job

January 8, 2024

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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **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.

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:

© 1997–2025 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:

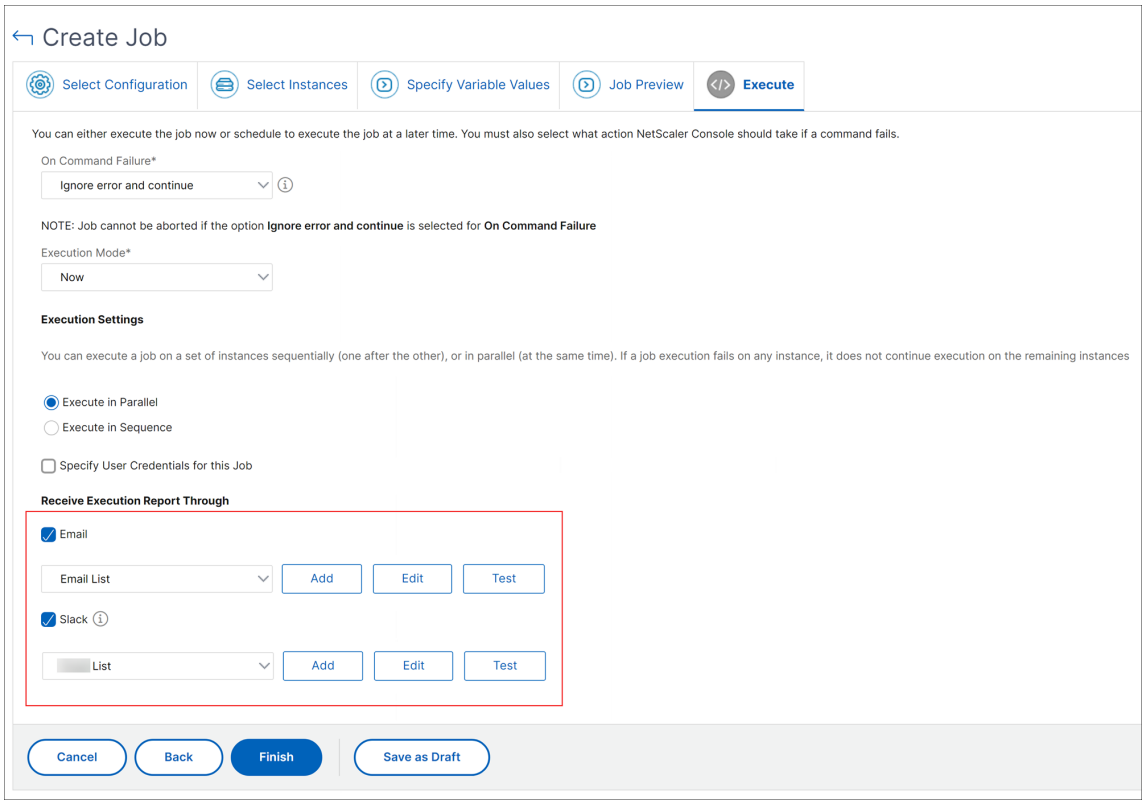
   - Select the **Email** check box and choose the email distribution list to which you want to send the execution report.

     If you want to add an email distribution list, click **Add** and specify the email server details.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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.



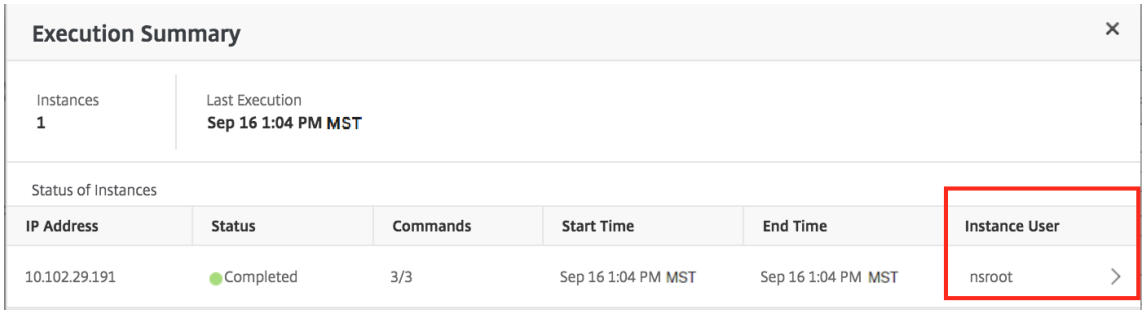
4. Click **Finish**.

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Configuration audit

January 8, 2024

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

Upgrade jobs

September 8, 2025

> **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.x (FIPS)

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> - NetScaler SVM: 14.1 51.x, 13.1 60.x
> - NetScaler Console Service: will support LAS from early September.
>
> 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.

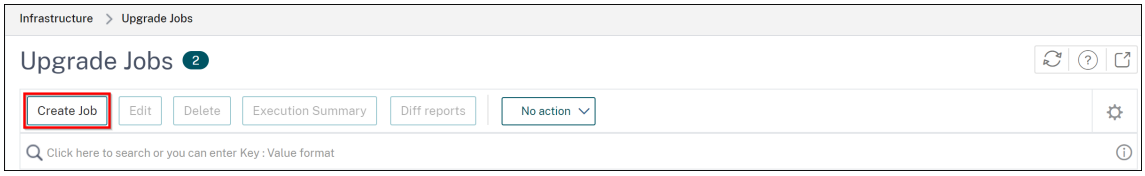
You can create the following maintenance tasks using NetScaler Console. You can then schedule the maintenance tasks at a specific date and time.

- Upgrade NetScaler instances
- 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.

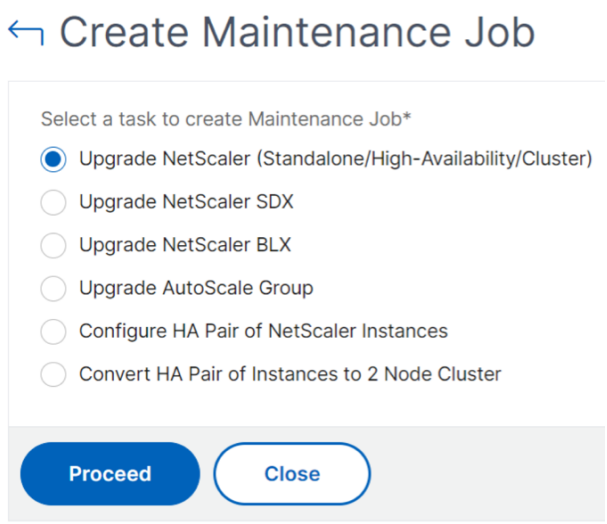
Schedule upgrading of NetScaler instances

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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.
5. Click **Next** to select the image. elect 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.

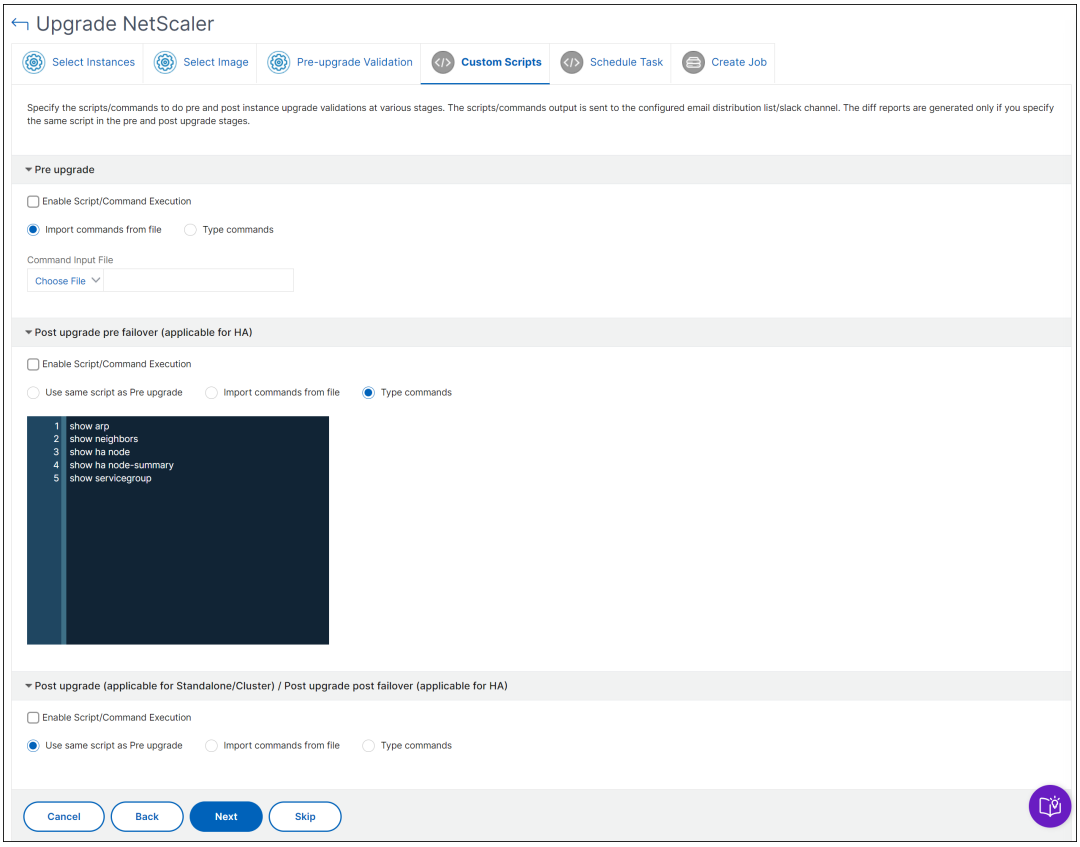
    The **Pre-upgrade validation** tab displays the failed instances. Remove the failed instances and click **Next**.

    > **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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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.

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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Specify the **Execution Date** and **Start Time** when you want to upgrade another instance in the HA pair.

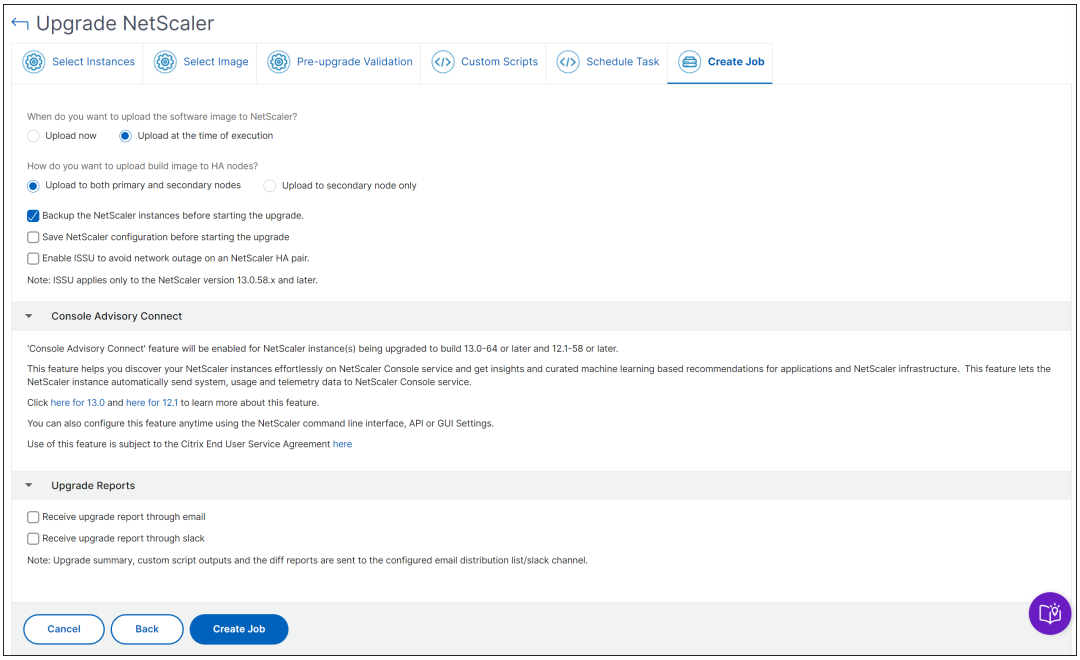
9. Click **Next**. In **Create Job**, specify the following details:

   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** - ISSU ensures the zero downtime upgrade on an NetScaler high-availability pair. This option provides a migration functionality that honors the existing connections during upgrade. So, you can upgrade an NetScaler HA pair without downtime. Specify the ISSU migration timeout in minutes.

   - **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.
   - **Receive Execution Report through slack** - Sends the execution report in slack. To add a Slack profile, see Create a Slack profile.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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**

© 1997–2025 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.

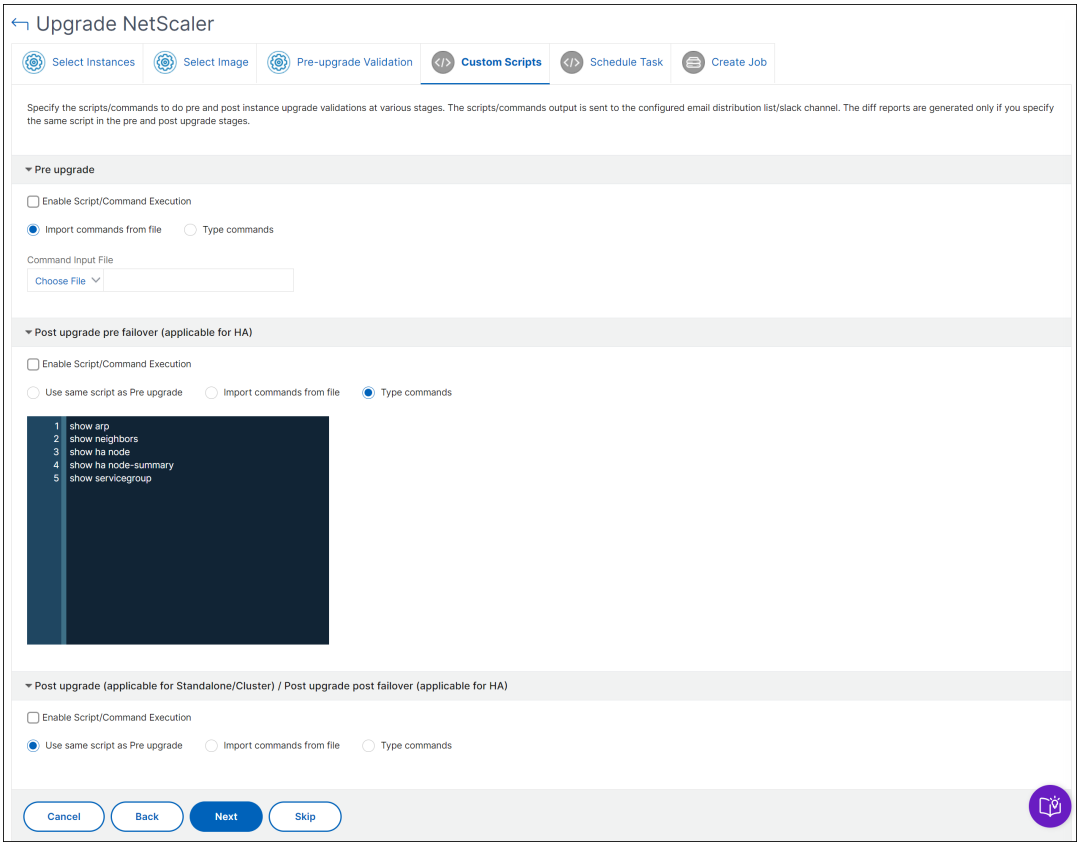
   The **Pre-upgrade validation** tab displays the failed instances. Remove the failed instances and click **Next**.

   > **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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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.

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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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** - 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 HA pair without downtime. Specify the ISSU migration timeout in minutes.

    - **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.
    - **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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.
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 **Now** from the **Execution Mode** list to upgrade a NetScaler instance now, and click **Finish**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

5. To upgrade a NetScaler HA pair 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**.
6. 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.

Use jobs to upgrade NetScaler instances

September 13, 2024

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

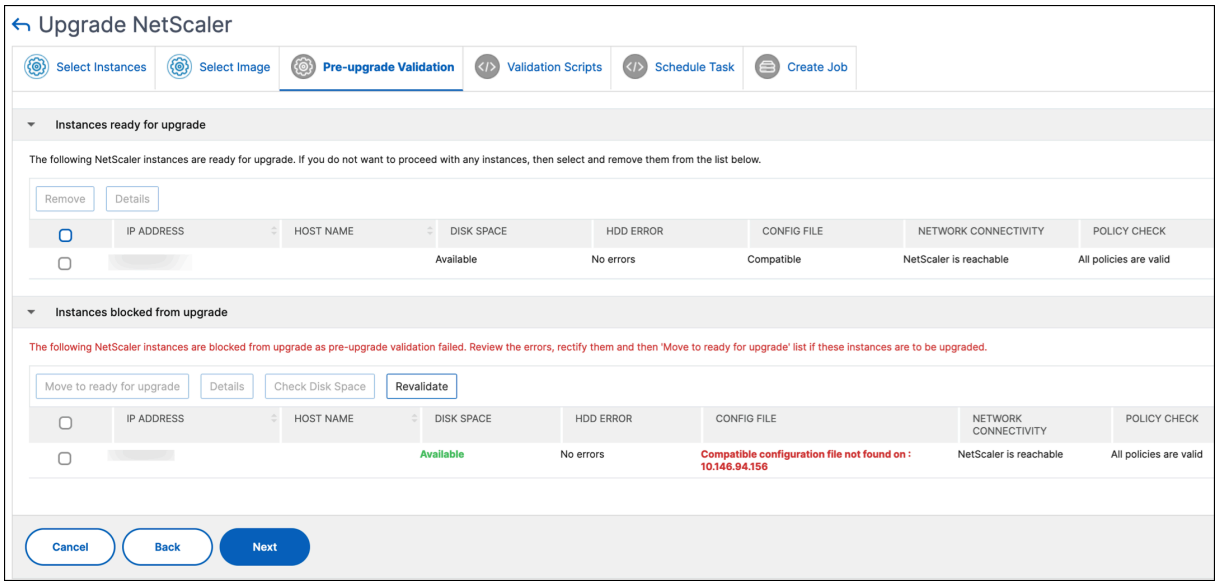
applicable for the features that are supported by the NSPEPI tool. For more information, see Upgrade considerations for configurations with classic policies.

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**.



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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

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

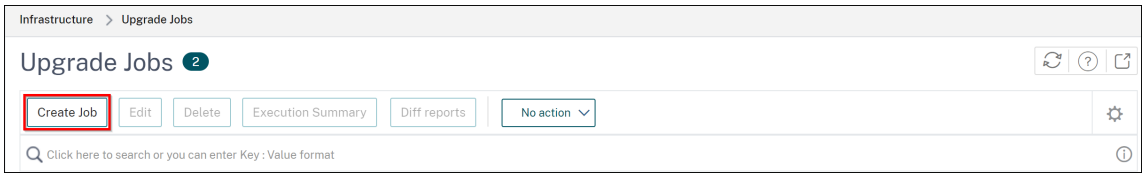
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Disk usage
- hardware issues

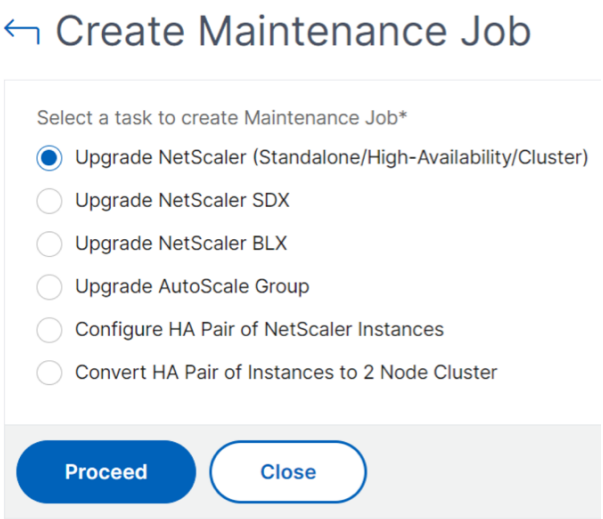
Create a NetScaler upgrade job

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**.



> **Note:**
>
> To upgrade Autoscale groups, see Upgrade an Autoscale group.

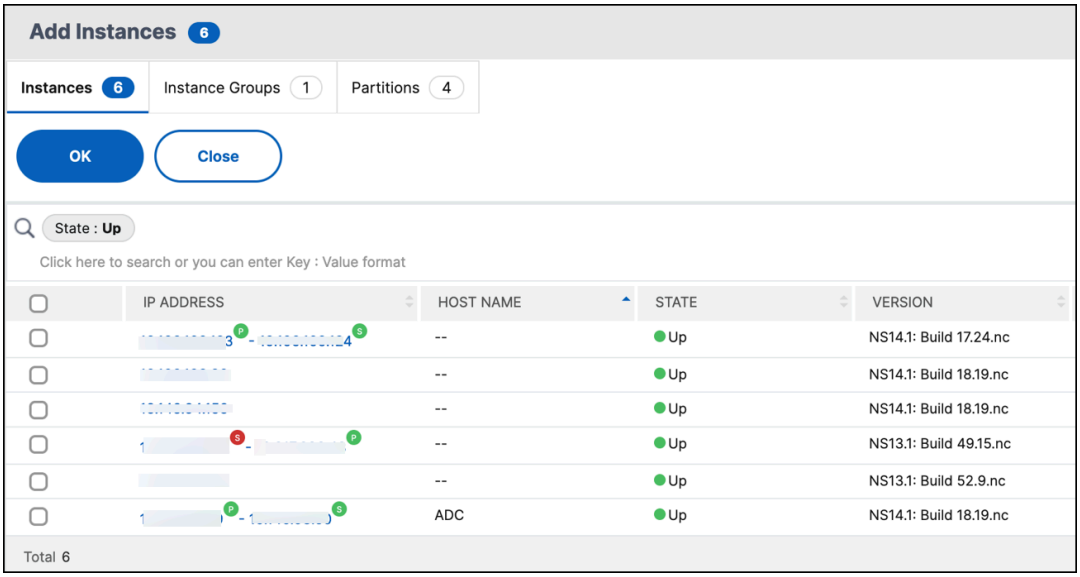
3. In the **Select Instances** tab,

   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’).

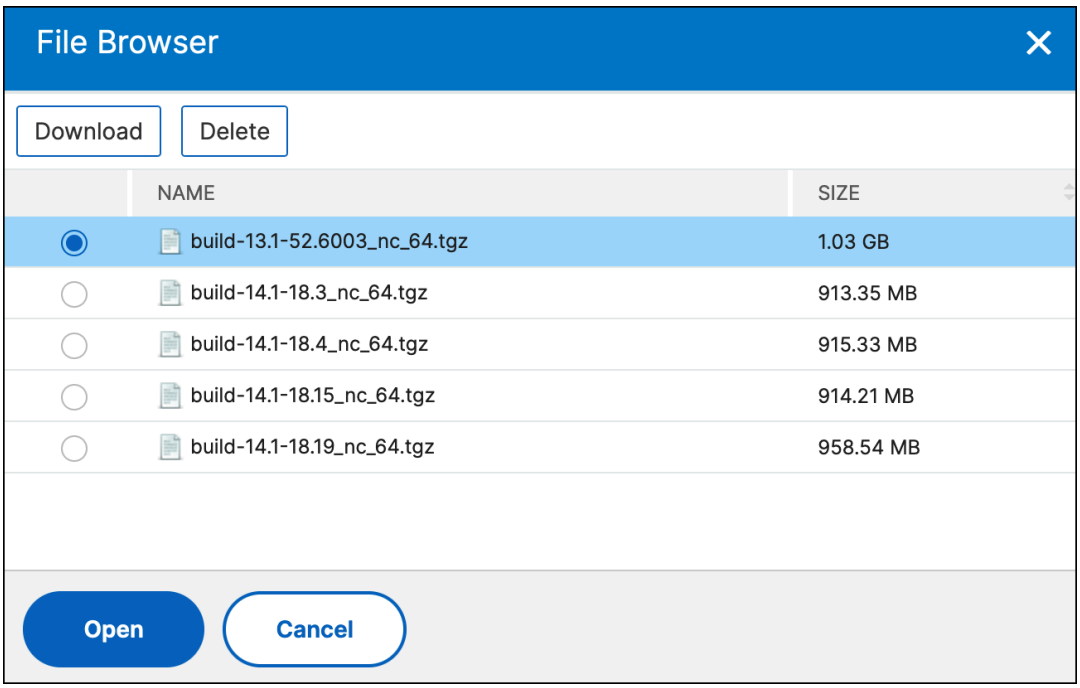
© 1997–2025 Citrix Systems, Inc. All rights reserved.



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

© 1997–2025 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.

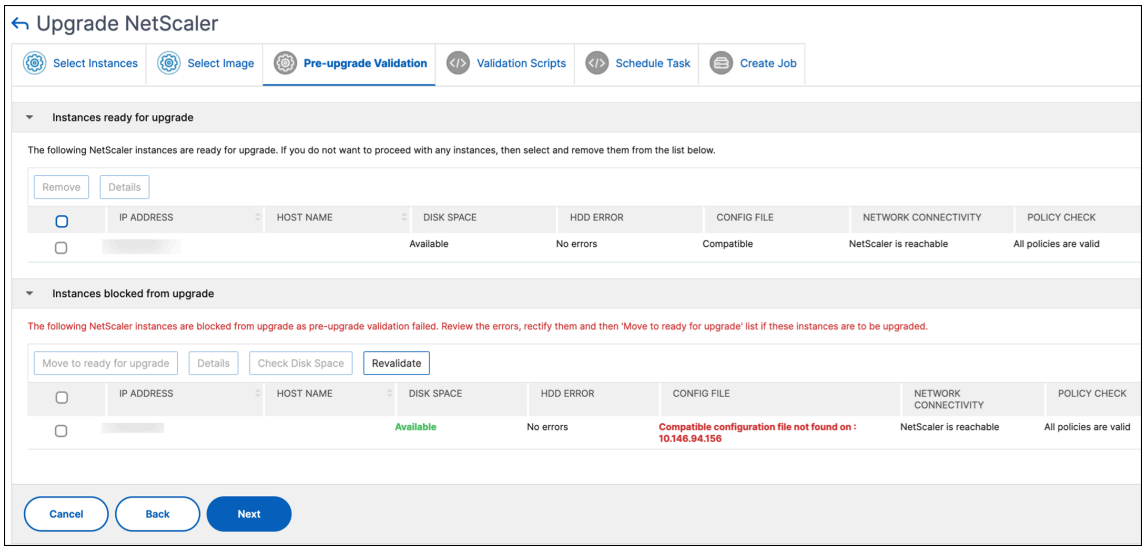
Click **Next** to start the pre-upgrade validation on the selected instances.

> **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.

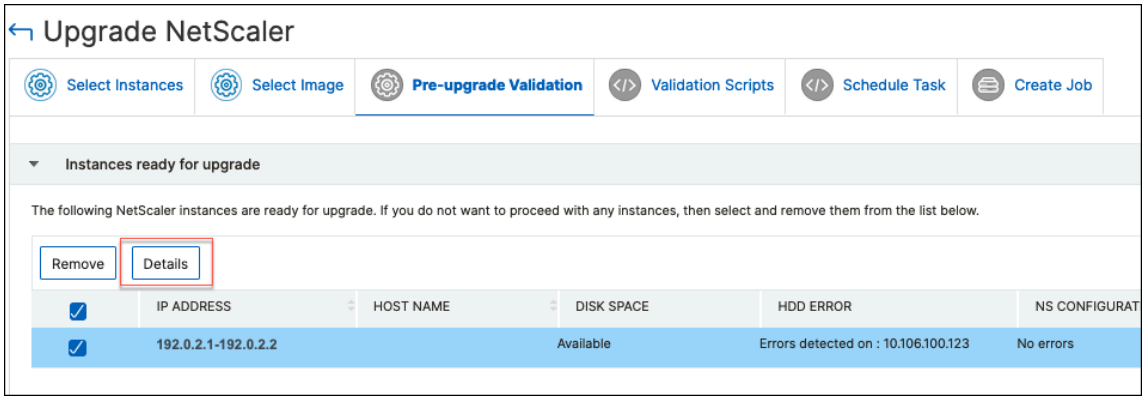


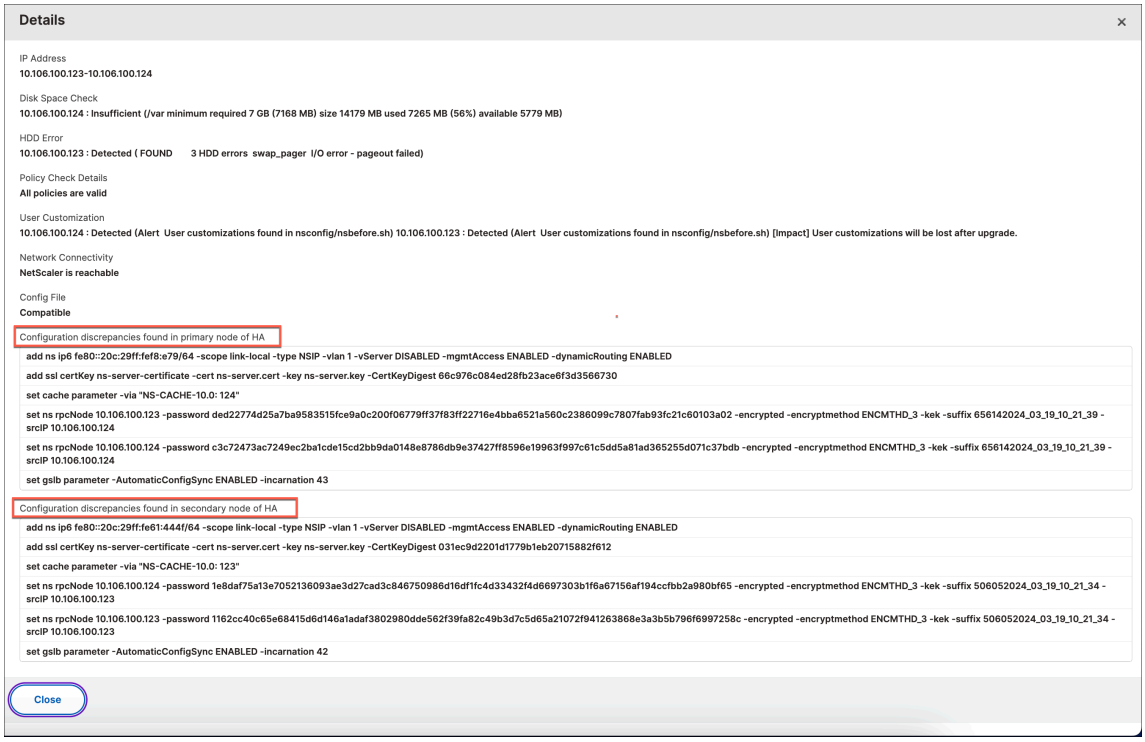
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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**.





- **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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.

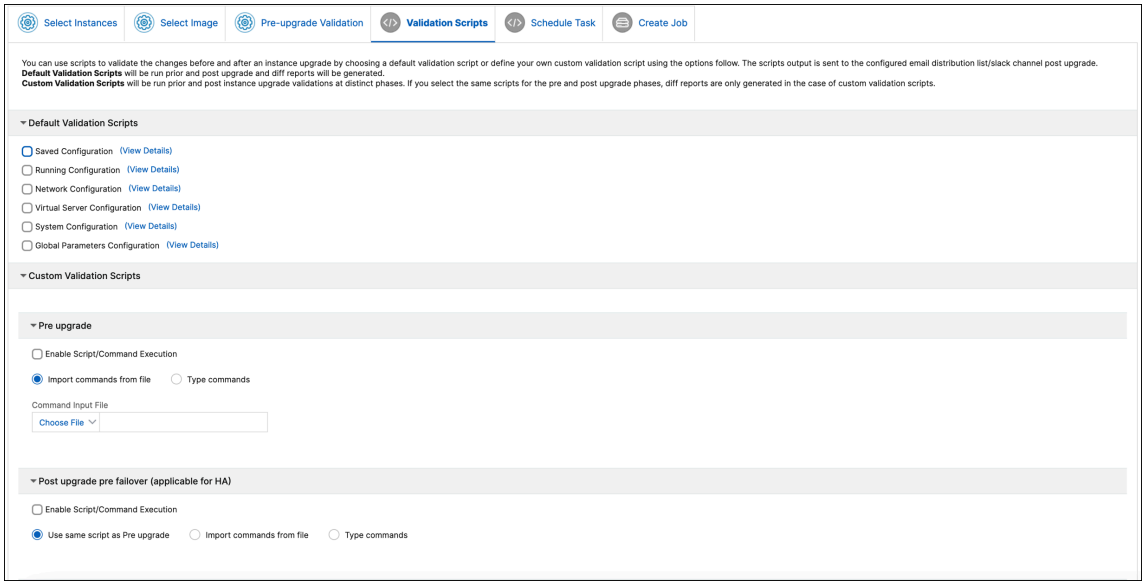
> **Note:**
>
> You can ignore the following discrepancies that may appear in the configuration discrepancies sections:
>
> - Device-specific configurations like IP addresses.
> - Encrypted passwords or certificates, which may differ between nodes, even if the password is the same.
>
> You can review 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:

   - **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.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

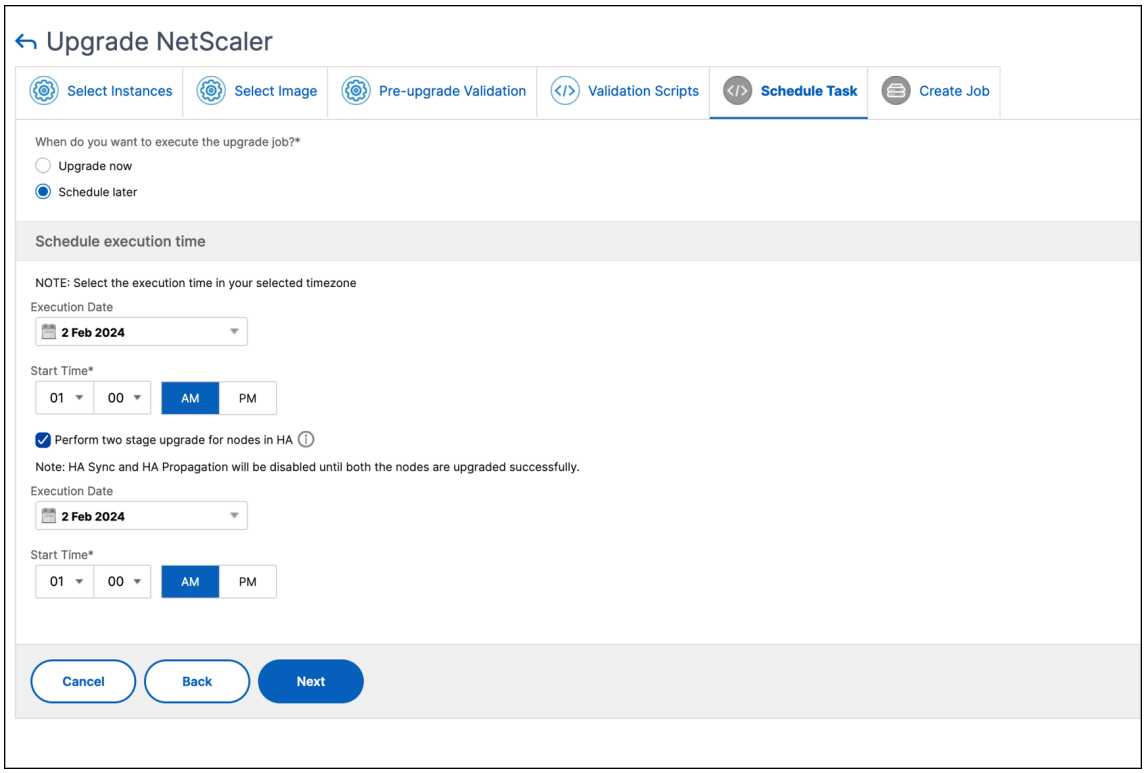
To know the set of commands in each configuration, click **View Details**.
For more information, see Use custom scripts.

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.



   For more information, see NetScaler high-availability pair.

8. In **Create Job**, specify the following details:

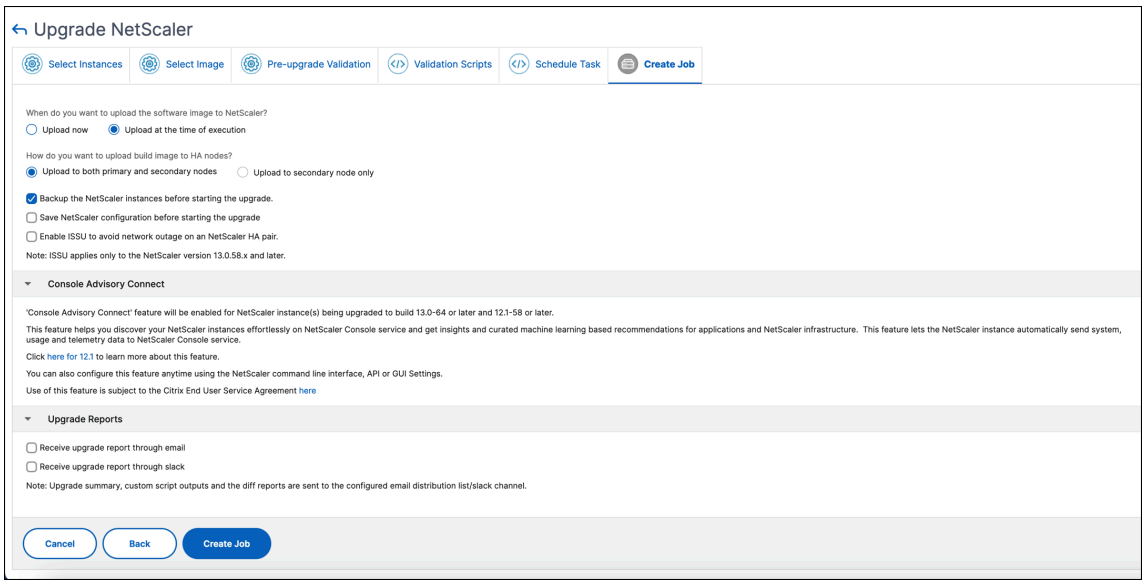
   If you schedule the upgrade job, you can specify when you want to upload the image to an instance:

   - **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.



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**.

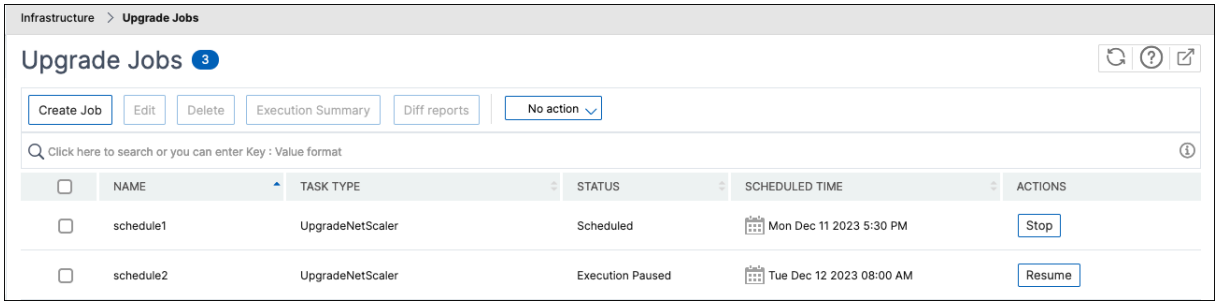
The upgrade job appears in the **Infrastructure > Upgrade Jobs**. When you edit an existing job, you can switch to any tabs if the required fields are already filled. For example, if you are in the **Select Configuration** tab, you can switch to the **Job Preview** tab.

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**.

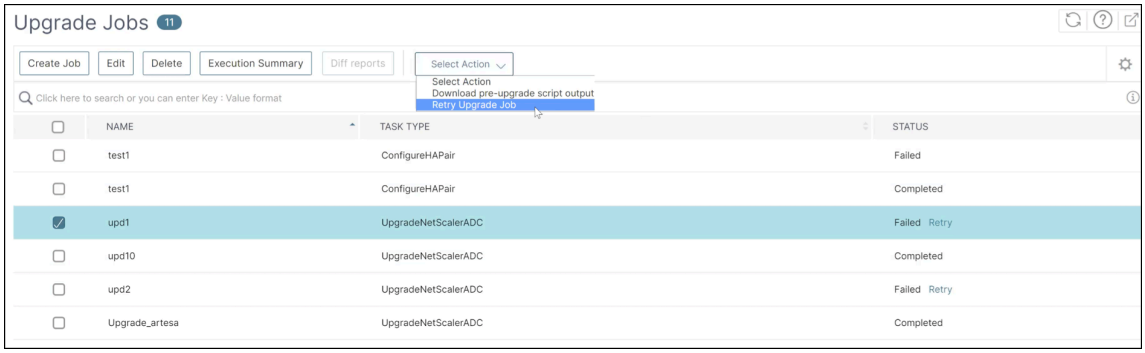
© 1997–2025 Citrix Systems, Inc. All rights reserved.



> **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.

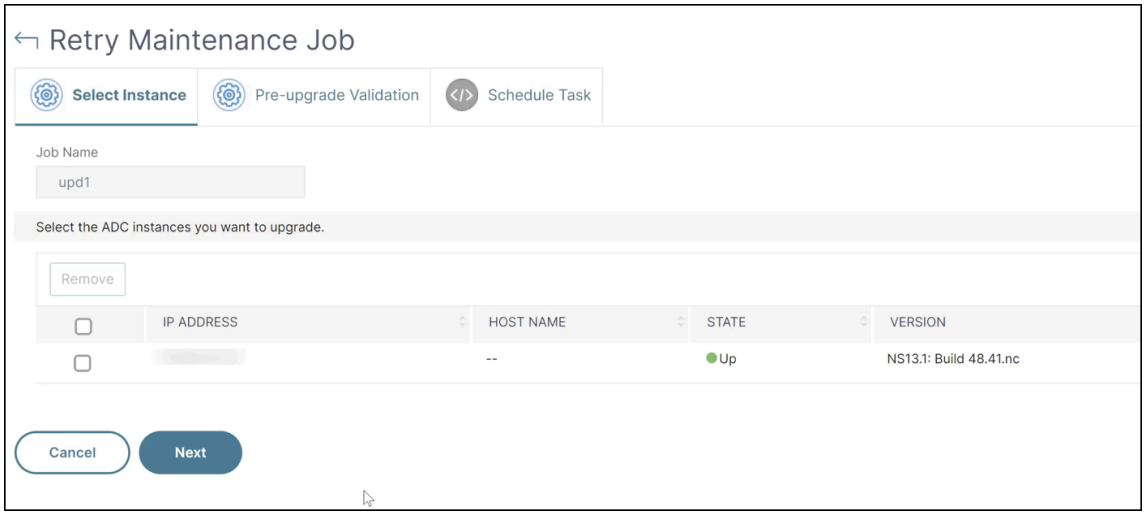


2. In **Select Instance**, specify the following details:

   - **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.

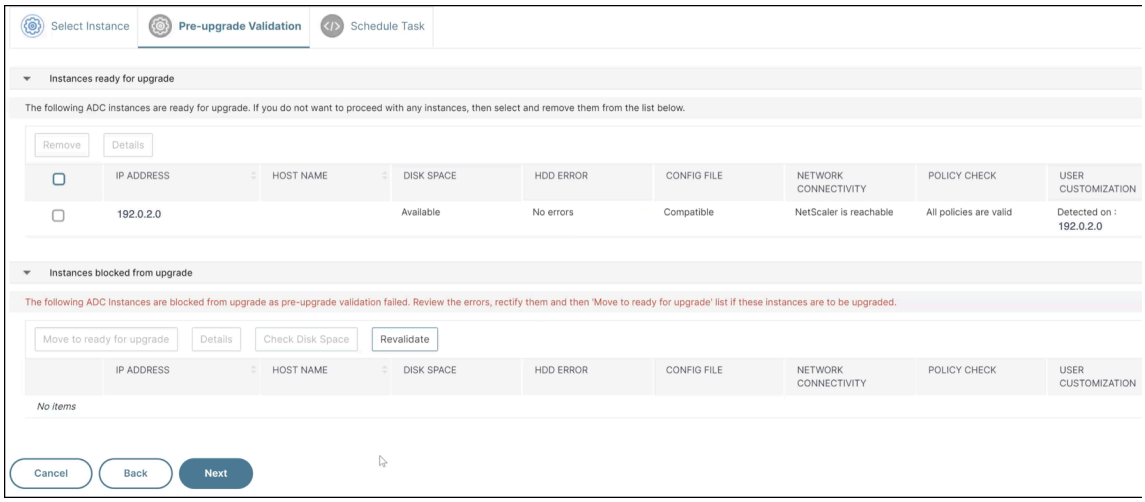
© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. 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.
   - **Policy Check**: If NetScaler Console finds unsupported classic policies, you can remove such policies to create an upgrade job.



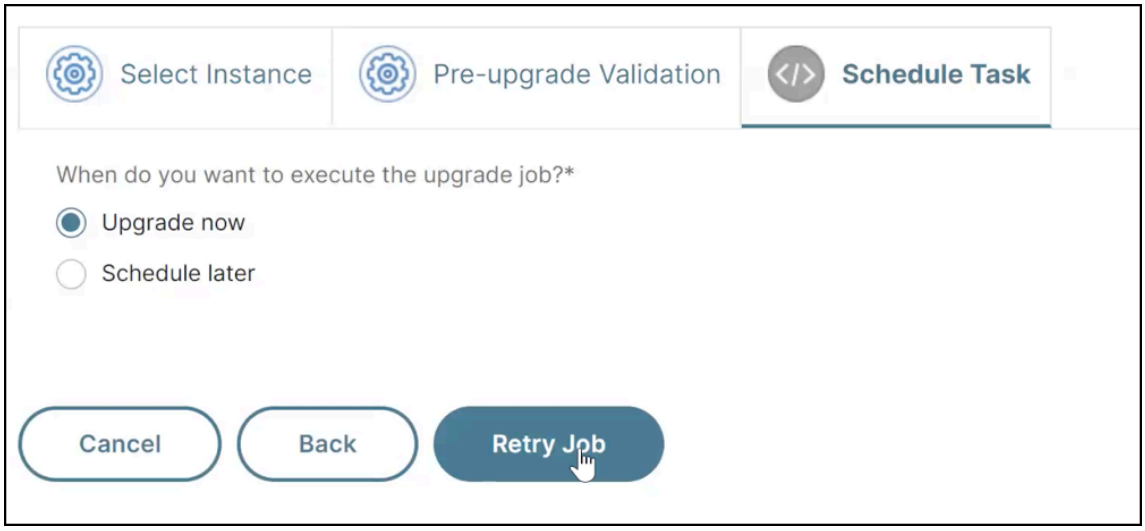
   Click **Next**.

4. In **Schedule Task**, select one of the following options:

   - **Upgrade now**: The upgrade job runs immediately.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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.



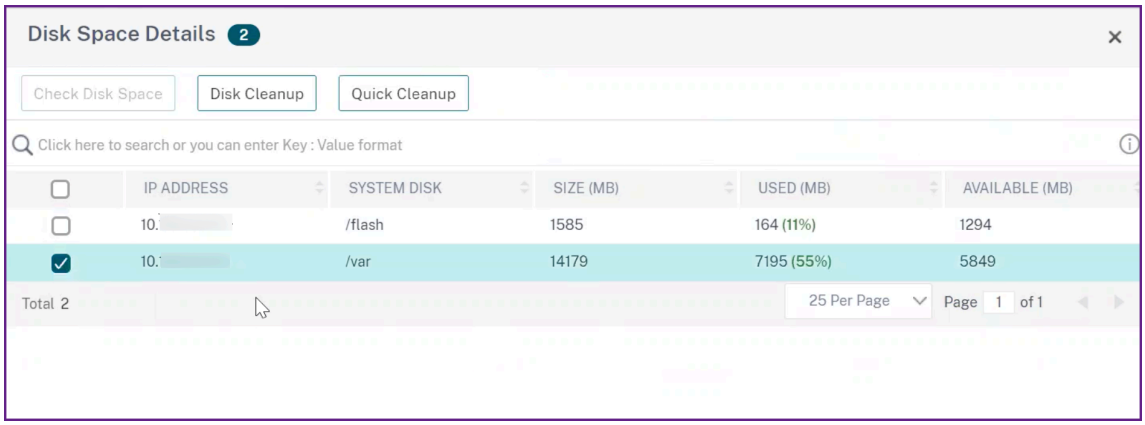
Click **Retry**.

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.

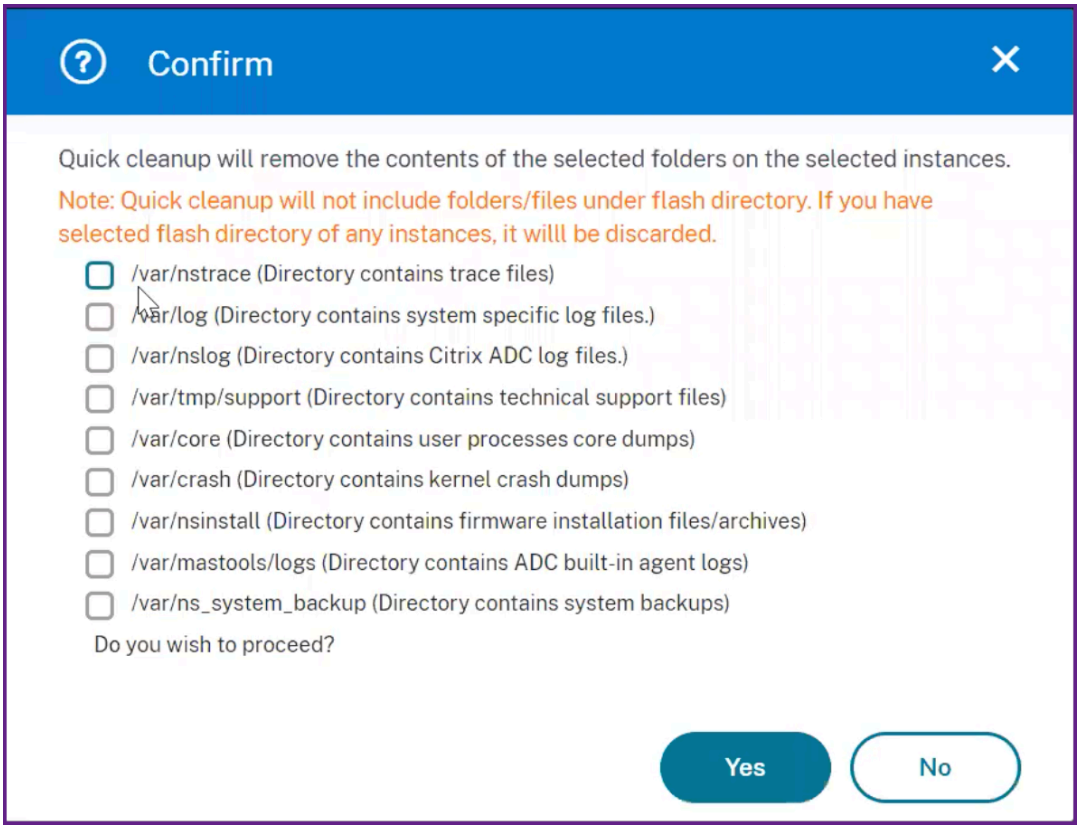


© 1997–2025 Citrix Systems, Inc. All rights reserved.

3. In the **Disk Space Details** pane, select the instance that requires cleanup and do one of the following:

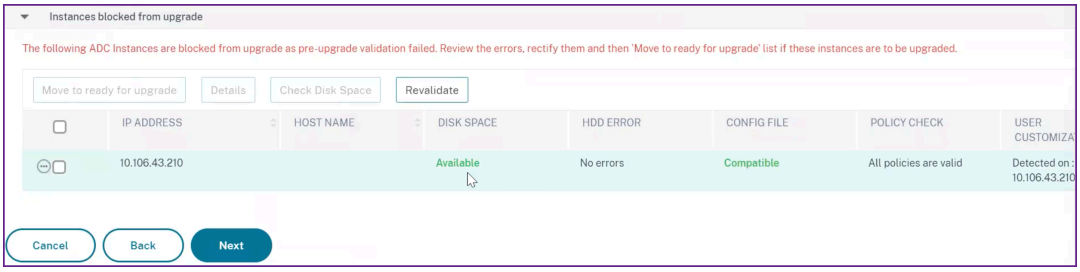
   a) **Disk Cleanup** - Navigate to the required folders or directories and delete them to free up disk space.

   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**.



   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.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.
- 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.

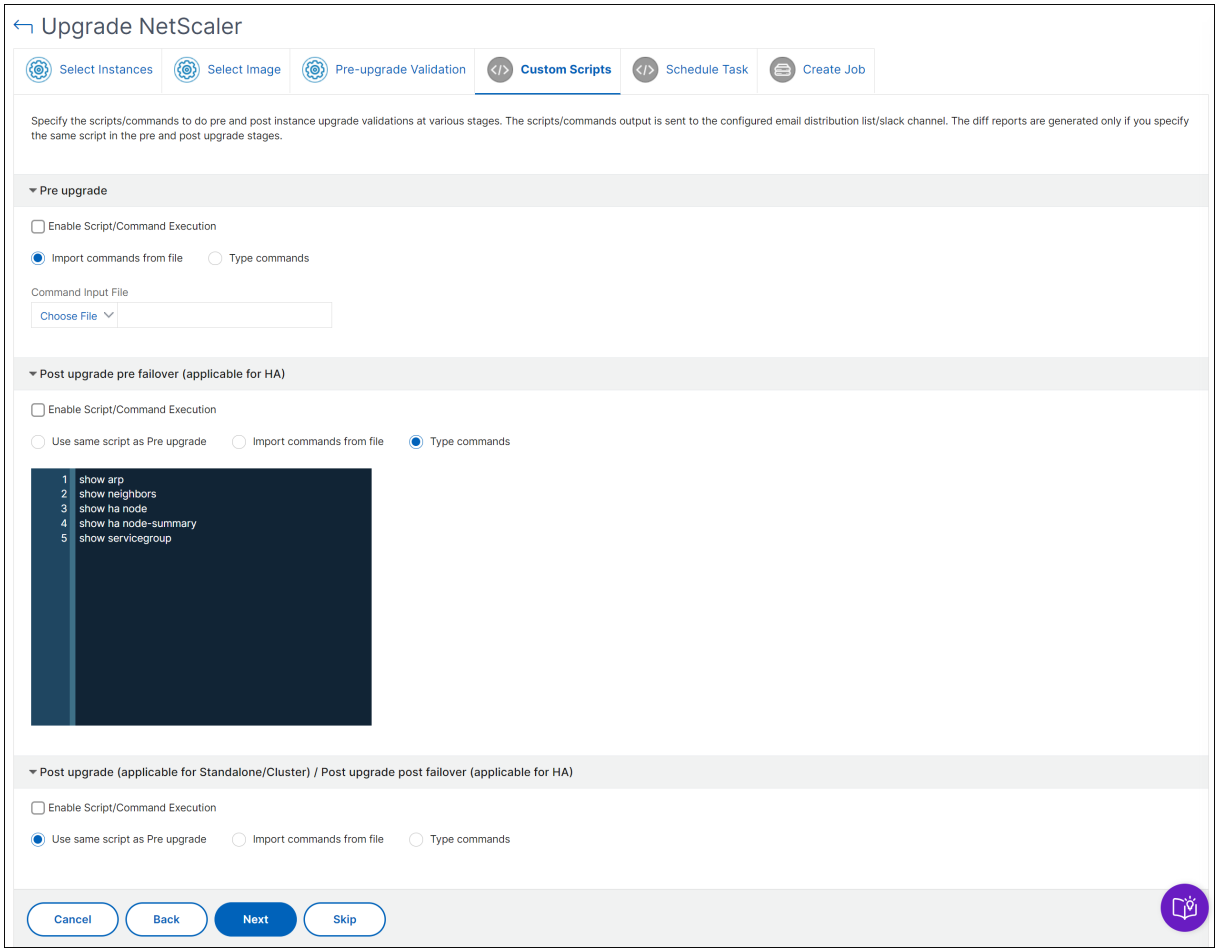
> **Note:**
>
> - Ensure to enable script or command execution at the required stages. Otherwise, the specified scripts do not run.
> - The diff report is generated only if you specify the same script in the pre-upgrade and post-upgrade stages. So, ensure to select **Use same script as Pre-upgrade** 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



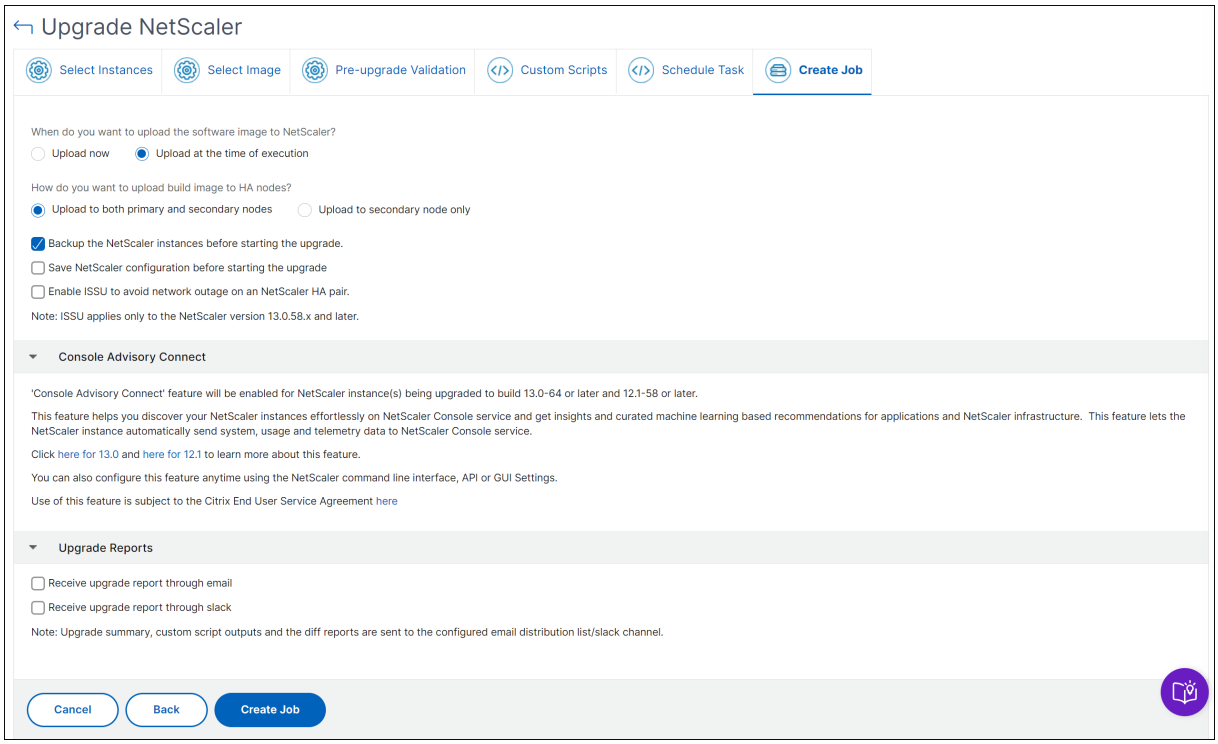
NetScaler upgrade options

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.

© 1997–2025 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)
Schedule later	**Upload at time of execution** (default option)	**Upload to both primary and secondary nodes** (default option)

© 1997–2025 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?
Schedule later (when **Perform two stage upgrade for nodes in HA** is selected)	**Upload at time of execution** (default option)	**Upload now** **Upload to secondary node only** (default and only option) **Upload now**

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.

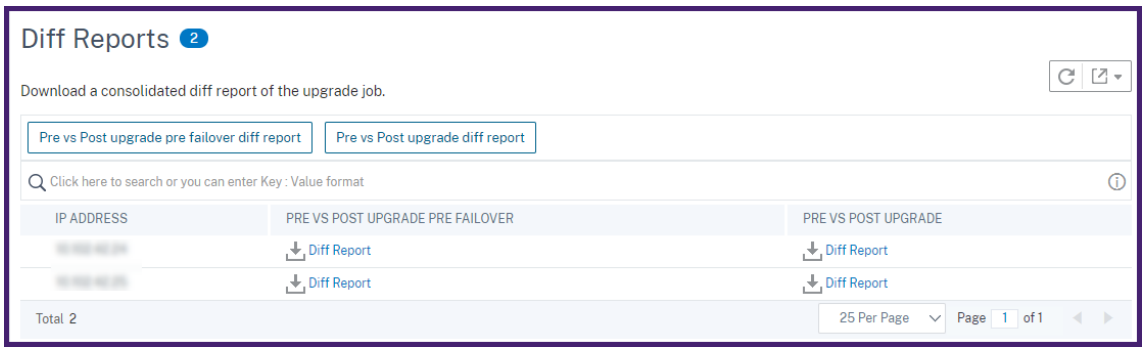
To download a diff report of an upgrade job, do the following:

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**

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Network functions

January 8, 2024

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

January 8, 2024

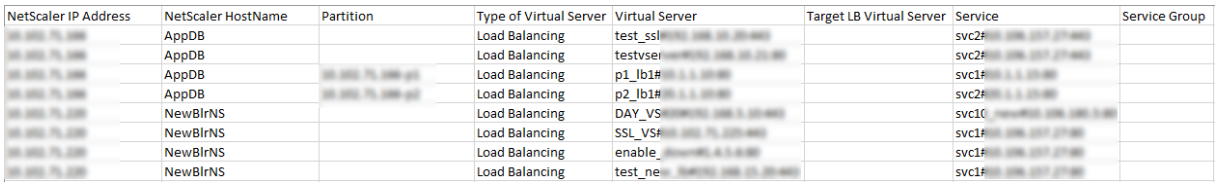
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

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]	AppDB		Load Balancing	testvser[redacted]		svc2#	
[redacted]	AppDB	[redacted]	Load Balancing	p1_lb1#		svc1#	
[redacted]	AppDB	[redacted]	Load Balancing	p2_lb1#		svc2#	
[redacted]	NewBlrNS		Load Balancing	DAY_VS[redacted]		svc1(	
[redacted]	NewBlrNS		Load Balancing	SSL_VS#		svc1#	
[redacted]	NewBlrNS		Load Balancing	enable_[redacted]		svc1#	
[redacted]	NewBlrNS		Load Balancing	test_ne[redacted]		svc1#	

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_addr
  ……..,server_membern_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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. Click **Generate Report**.
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.

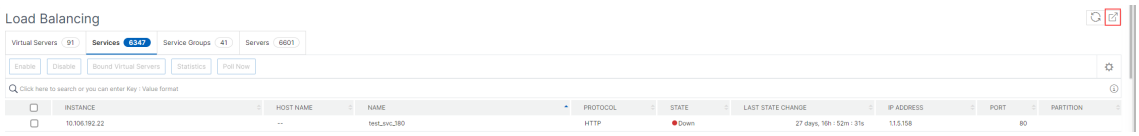
      vi. Click **Schedule** to complete the process.

© 1997–2025 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

January 8, 2024

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Target LB virtual server

  > **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.

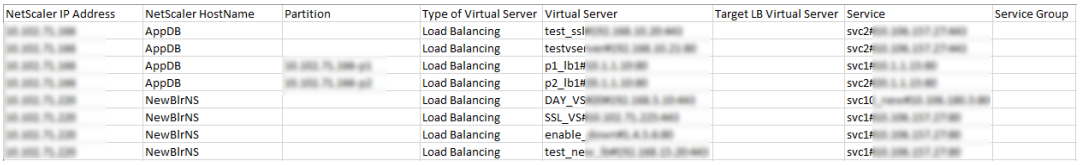
To export and schedule network functions reports:

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.



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]	

   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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

January 8, 2024

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:

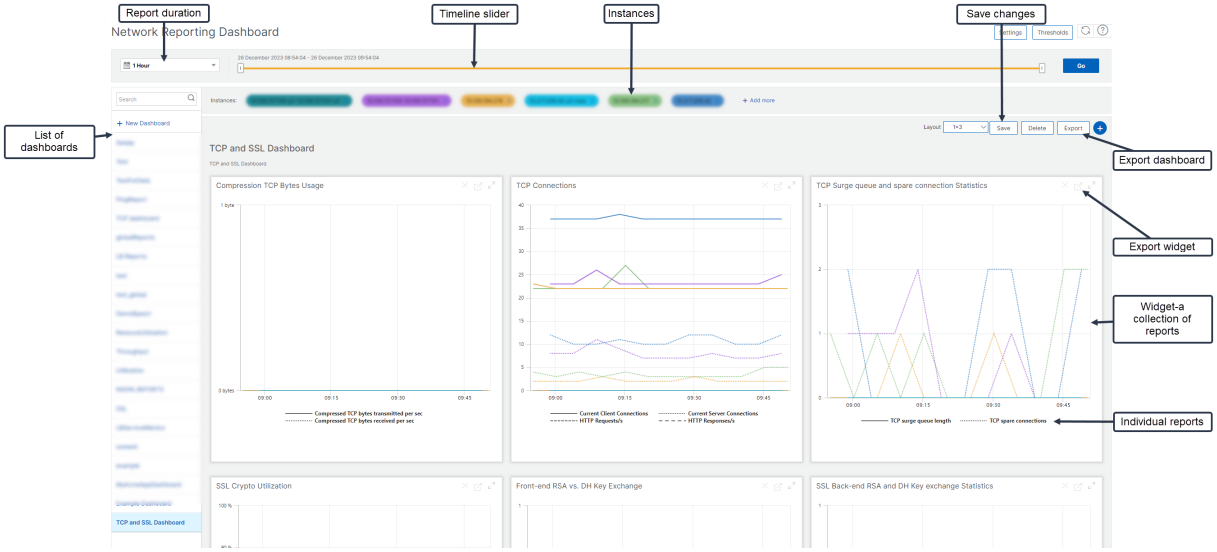
- Load balancing servers, services, and service groups
- Content switching servers
- Cache redirection servers
- Global service load balancing (GSLB)
- Authentication
- NetScaler Gateway

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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



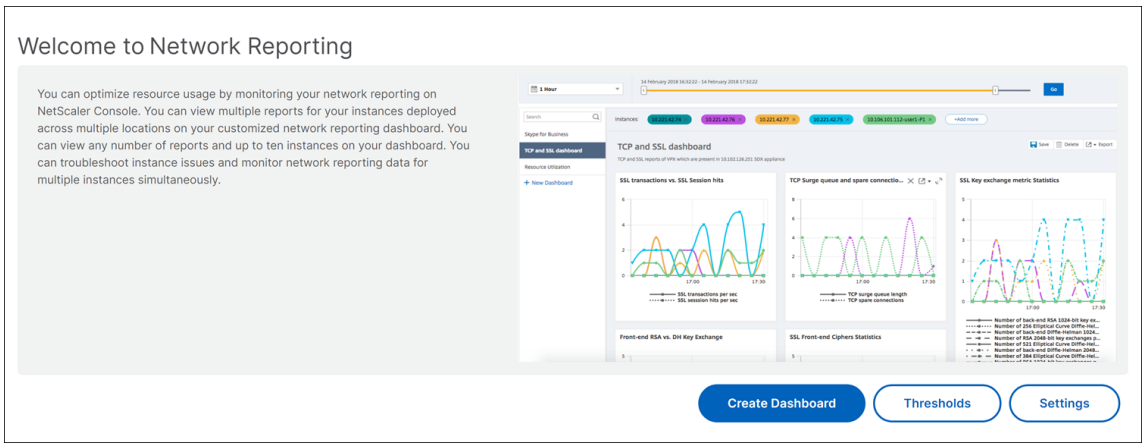
- The left side panel lists all the custom dashboards that are created in NetScaler Console. You can click one of them to view the various reports that the dashboard is composed of. For example, a TCP and SSL dashboard contains various reports related to TCP and SSL protocols.
- You can customize each 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.
- 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:

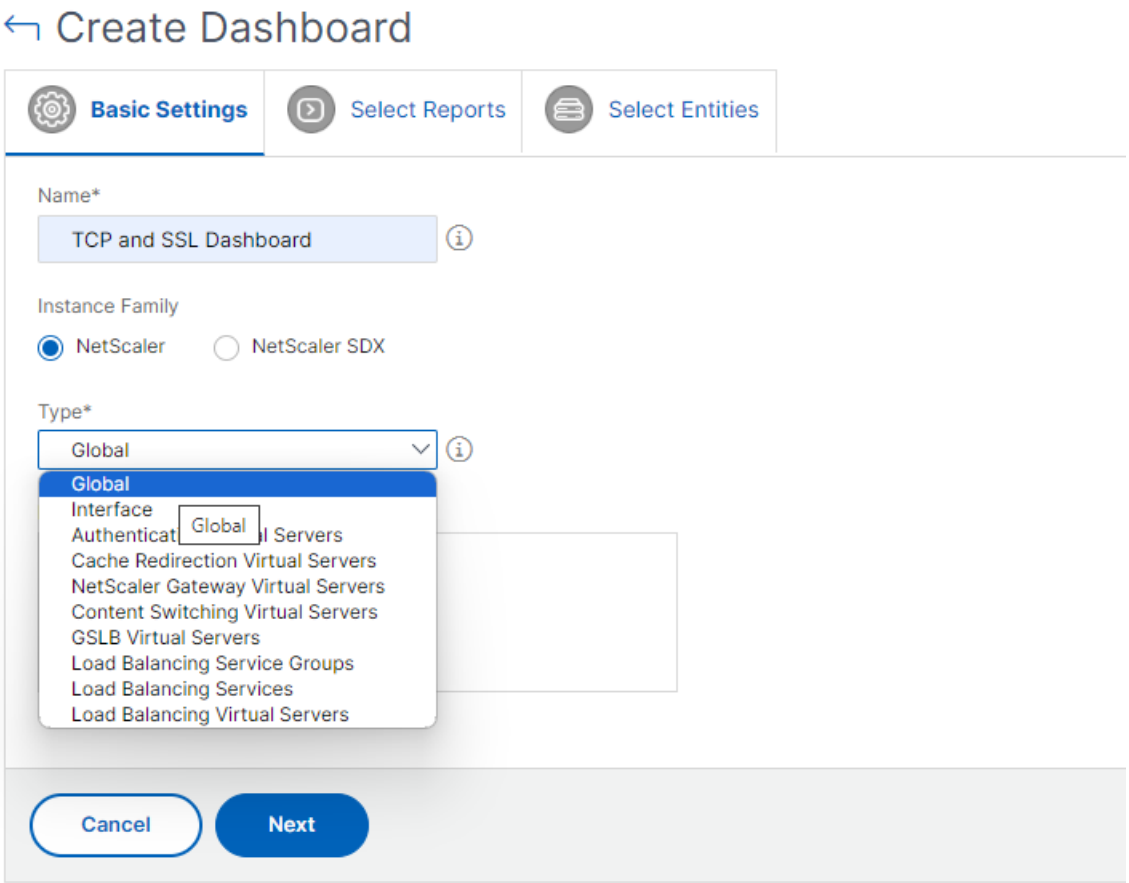
1. In NetScaler Console, navigate to **Infrastructure > Network Reporting**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.



4. In the **Basic Settings** tab, enter the following details:

   a) **Name**. Type the name of the dashboard.

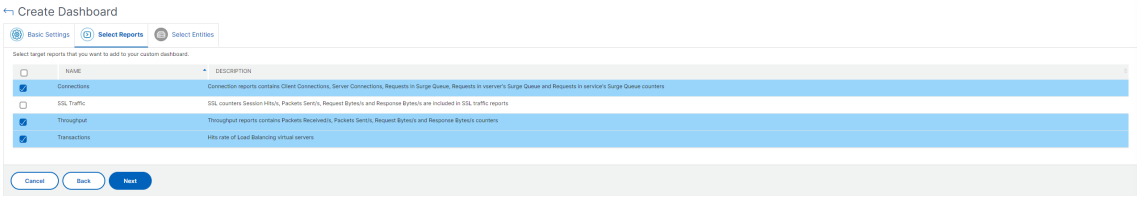
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

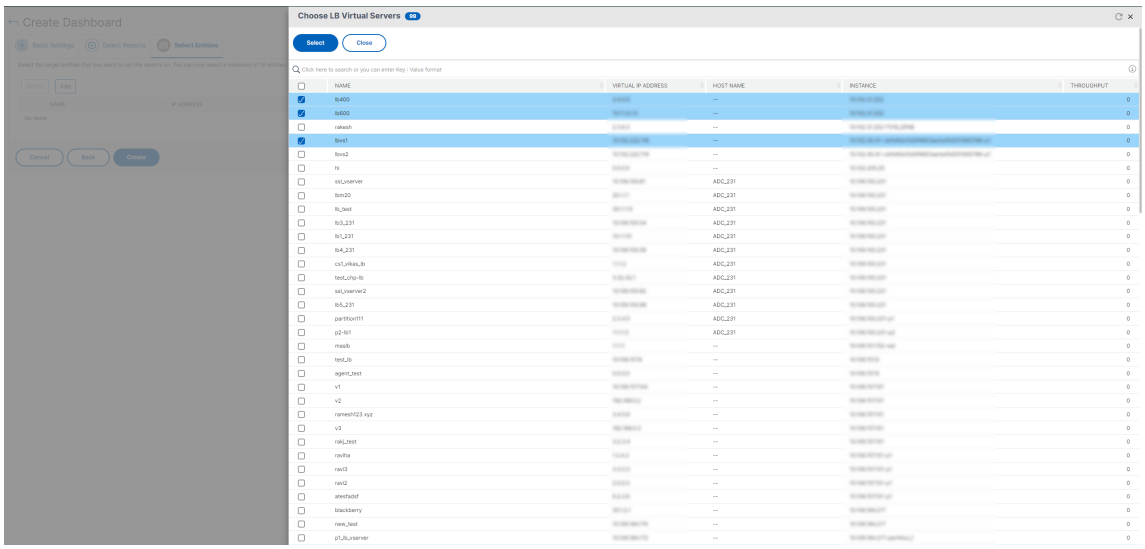
5. Click **Next**.
6. In the **Select Reports** tab, select the reports required. In this example, you can select transactions, connections, and throughput. Click **Next**.



7. In the **Select Entities** tab, click **Add**.

   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.

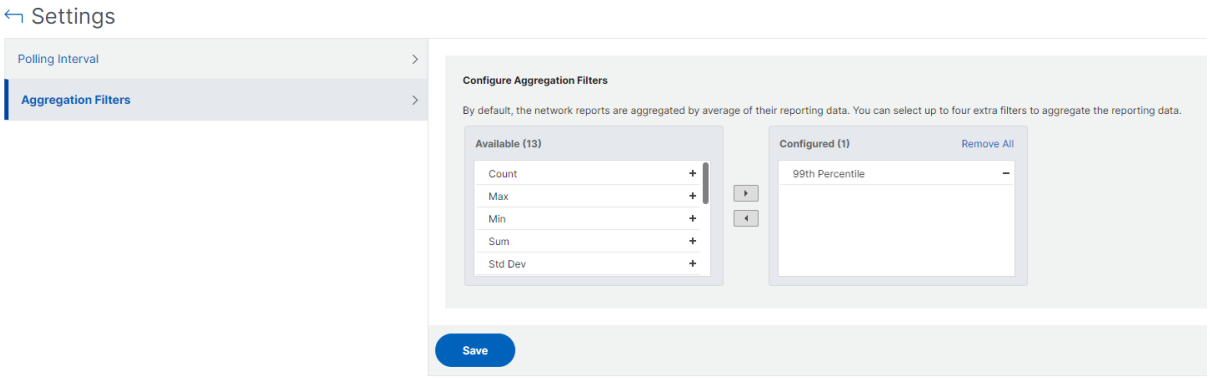
> **Note**
>
> Currently, any changes that you make to legends or filters cannot be saved.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.



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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

> **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.

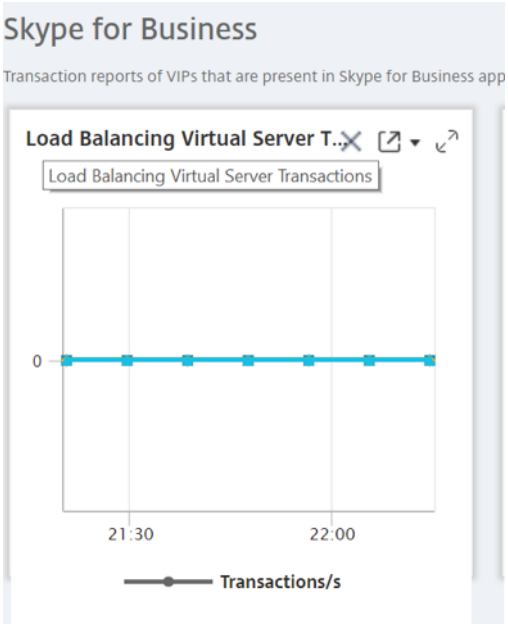
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

> **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**.



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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:

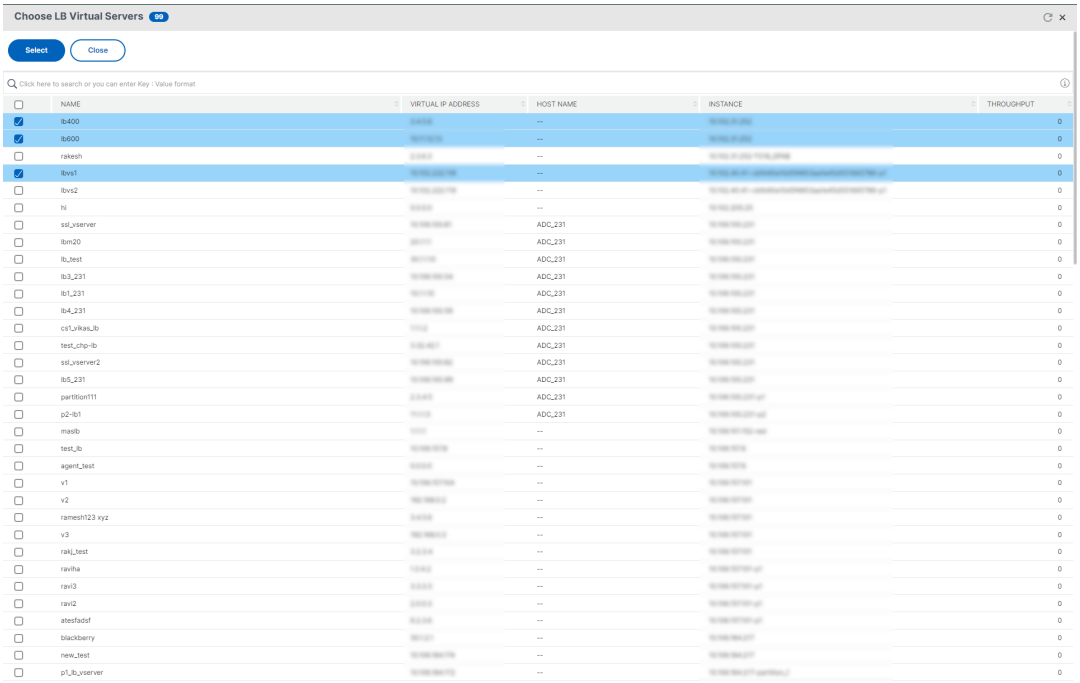
1. In NetScaler Console, navigate to **Infrastructure > Network Reporting > Thresholds**. Under **Thresholds**, click **Add**.
2. On the **Create Threshold** page, specify the following details:
    - **Name**. Name of the threshold.
    - **Instance Type**. A NetScaler instance.
    - **Report Name**. 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 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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.



  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**.

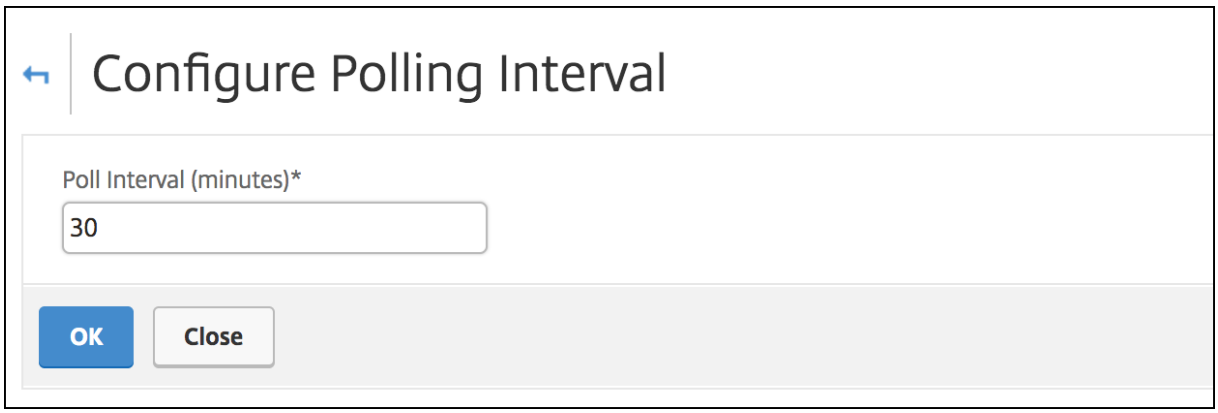
Set Performance Polling Interval for Network Reports

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

> **Note**
>
> The value that you can specify cannot exceed 90 days or be less than 1 day.

Provisioning NetScaler VPX Instances on AWS

September 8, 2025

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Term	Definition
Virtual Private Cloud (VPC)	A web service for provisioning a logically isolated section of the AWS cloud where you can launch AWS resources in a virtual network that you define.

Prerequisites

This document assumes the following:

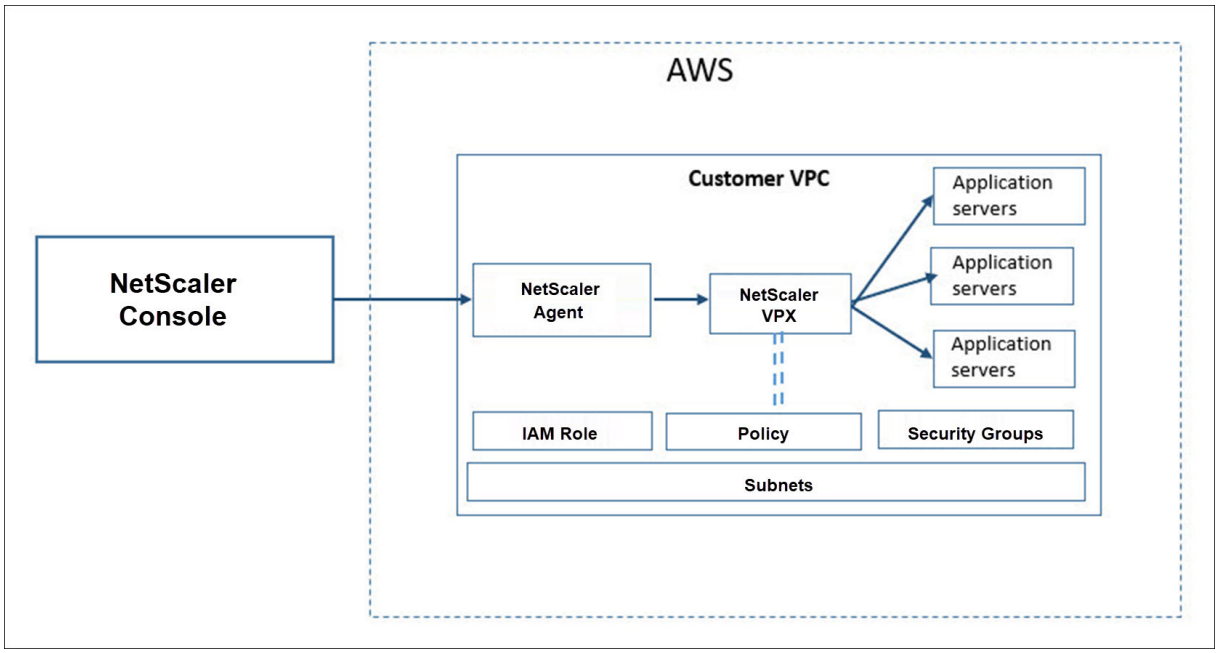
- You possess an AWS account.
- You have created the required VPC and selected the availability zones.
- You have added the agent in AWS.

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.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Configuration tasks

Perform the following tasks on AWS before you provision NetScaler VPX instances in NetScaler Console:

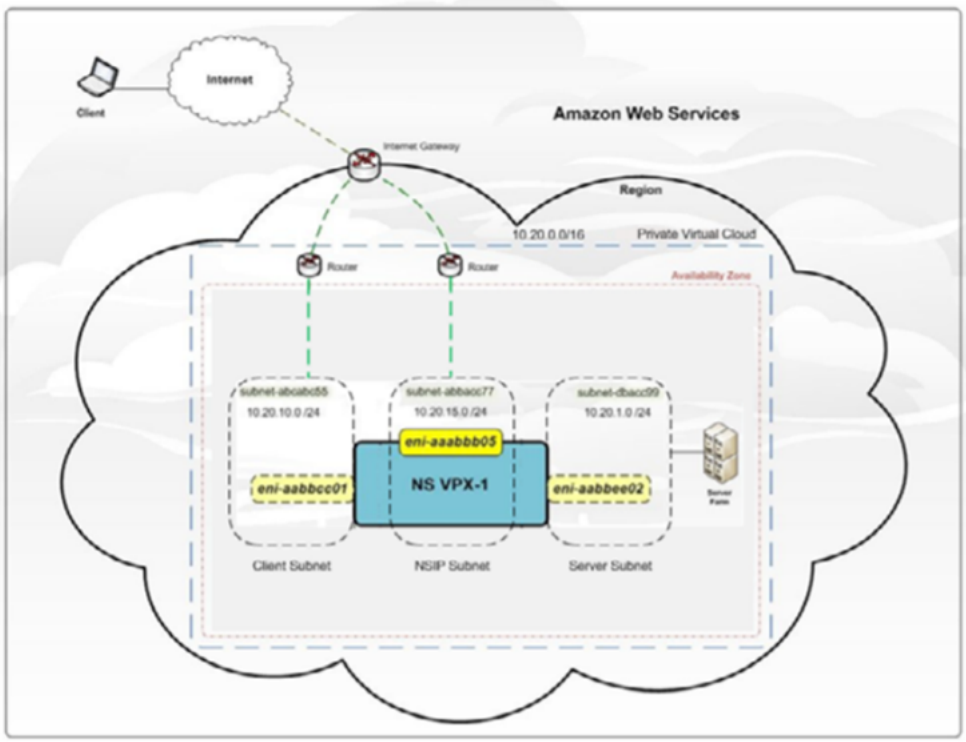
- Create subnets
- Create security groups
- Create an IAM role and define a policy

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 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

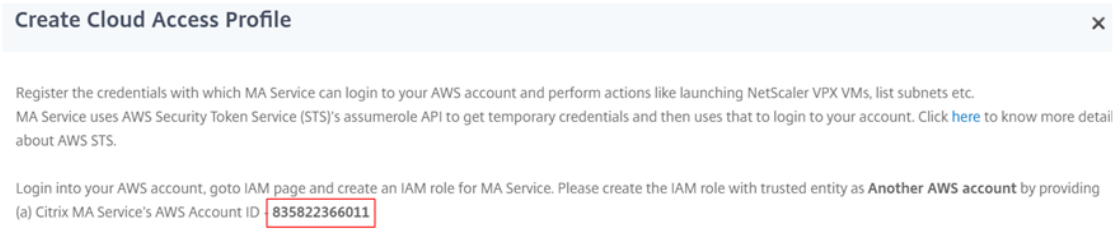
For more information on security groups, see Security Groups for your VPC.

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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
{

"Version": "2012-10-17",
"Statement":
[
    {

         "Effect": "Allow",
        "Action": [
            "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",
            "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",
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
                "ec2:AllocateAddress",
                "ec2:ReleaseAddress",
                "ec2:DisassociateAddress",
                "ec2:GetConsoleOutput"
            ],
                "Resource": "*"
        }

    ]
     }
```

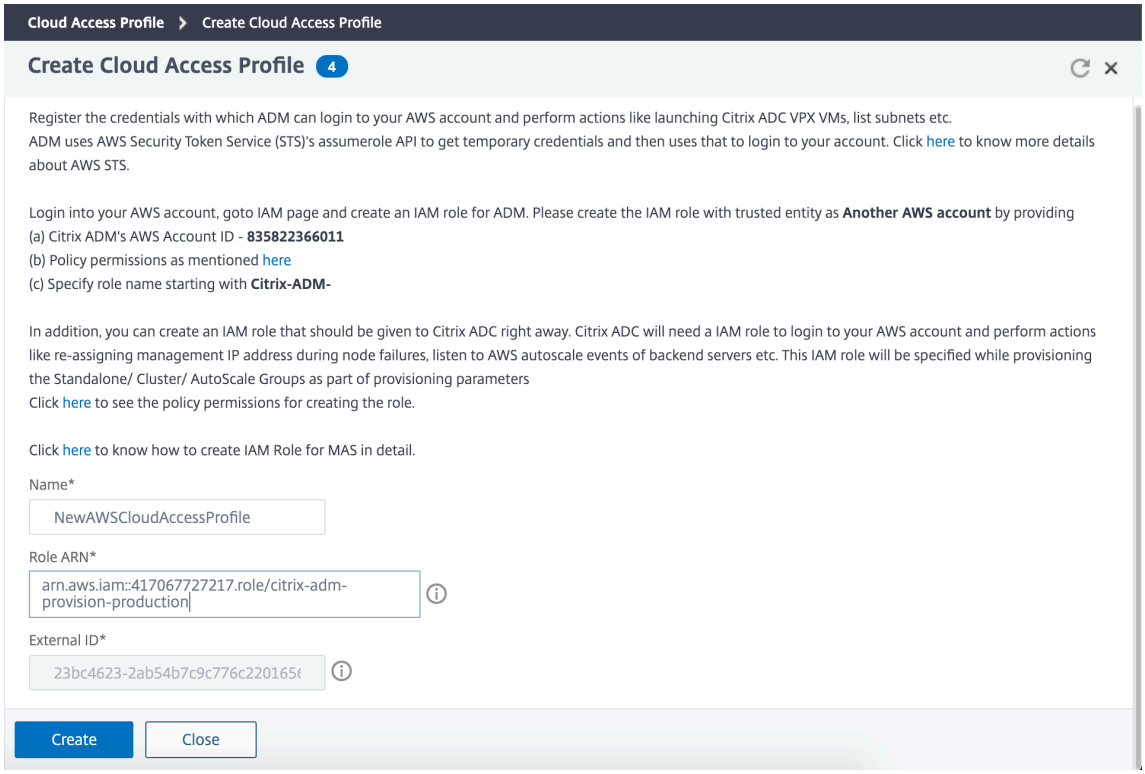
7. Copy and paste the list of permissions in the JSON tab and click **Review policy**.
8. In **Review policy** page, type a name for the policy, enter a description, and click **Create policy**.

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.

© 1997–2025 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.

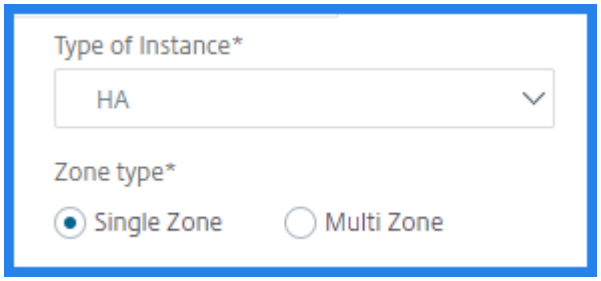
   - **Standalone:** This option provisions a standalone NetScaler VPX instance on AWS.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **HA:** This option provisions the high availability NetScaler VPX instances on AWS.

  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**.

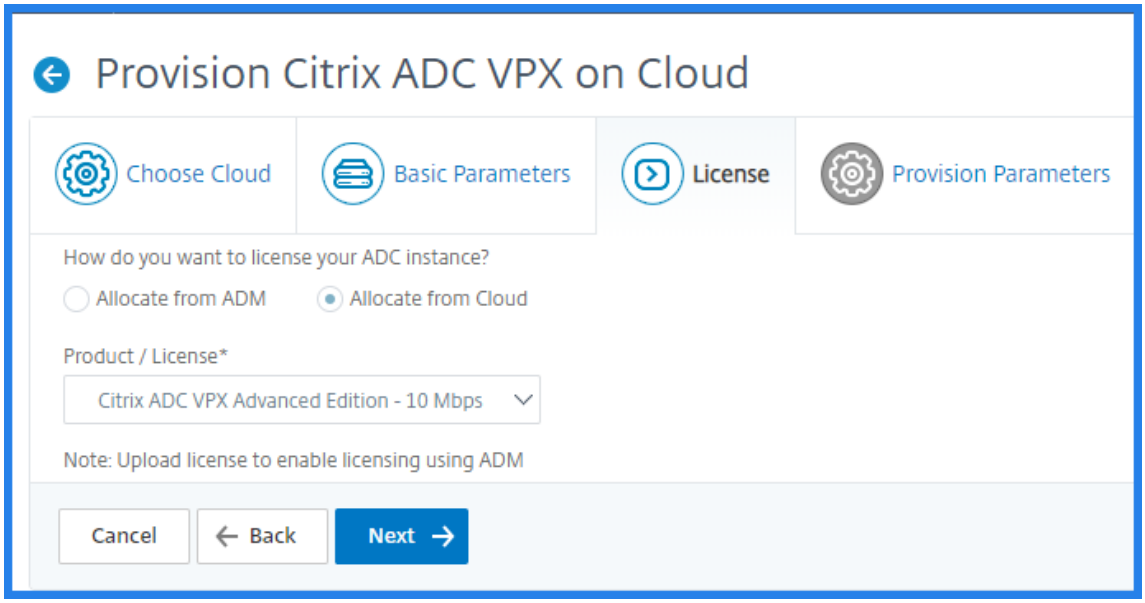
5. In the **License** tab, Select one of the following modes to apply license to a NetScaler instance:

   - **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.

© 1997–2025 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**.
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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

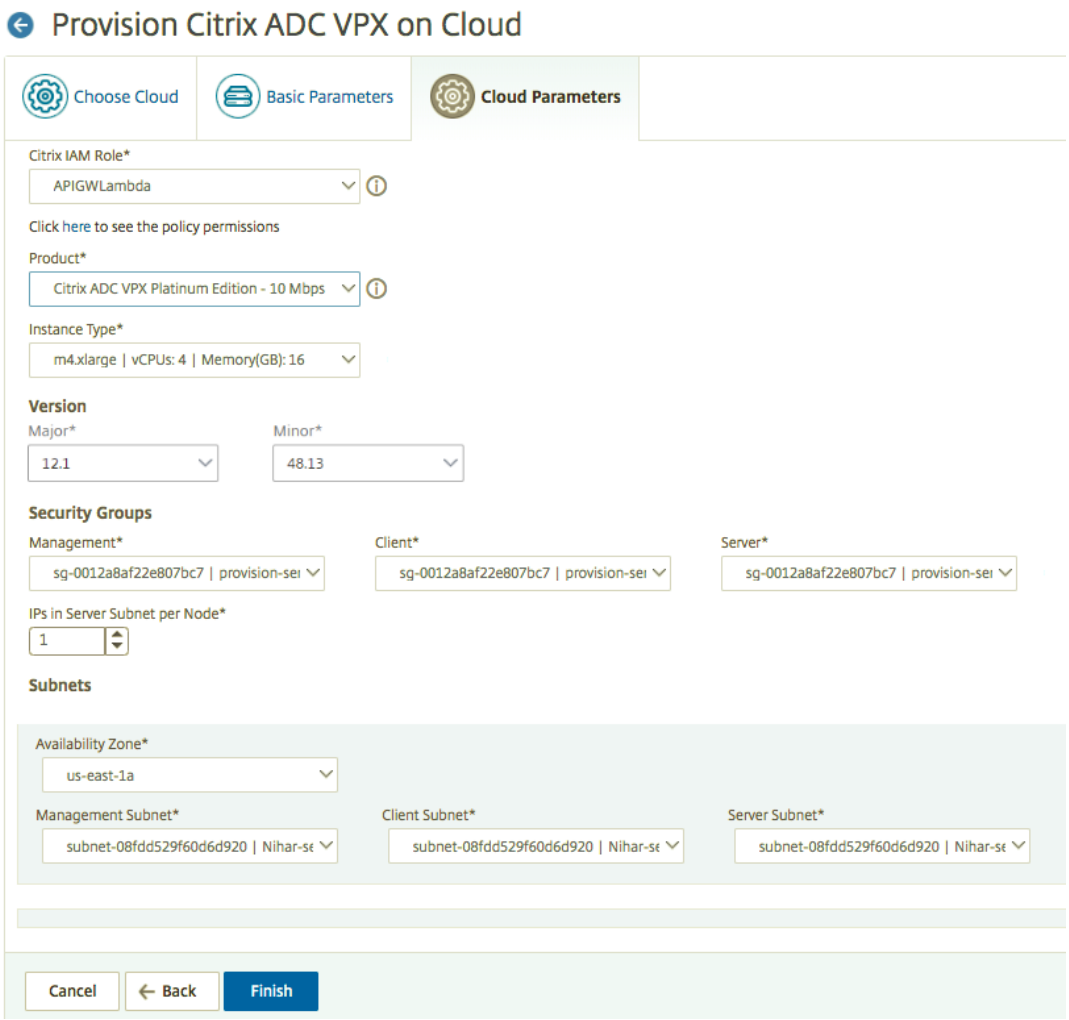
d) Select the **Version** of NetScaler that you want to provision. Select both **Major** and **Minor** version of NetScaler.

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**.



The NetScaler VPX instance is now provisioned on AWS.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **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.

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.

Manage the Kubernetes cluster for Service Graph

January 8, 2024

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

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.

   ```
   1 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`.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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
   ```

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.

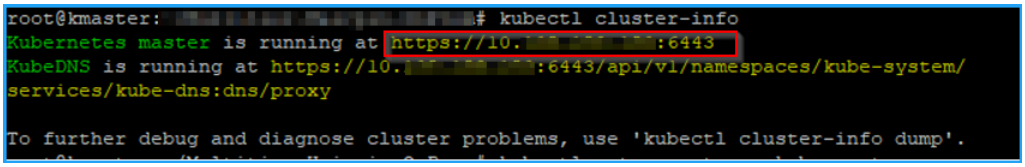
To register the Kubernetes cluster:

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>
      ```

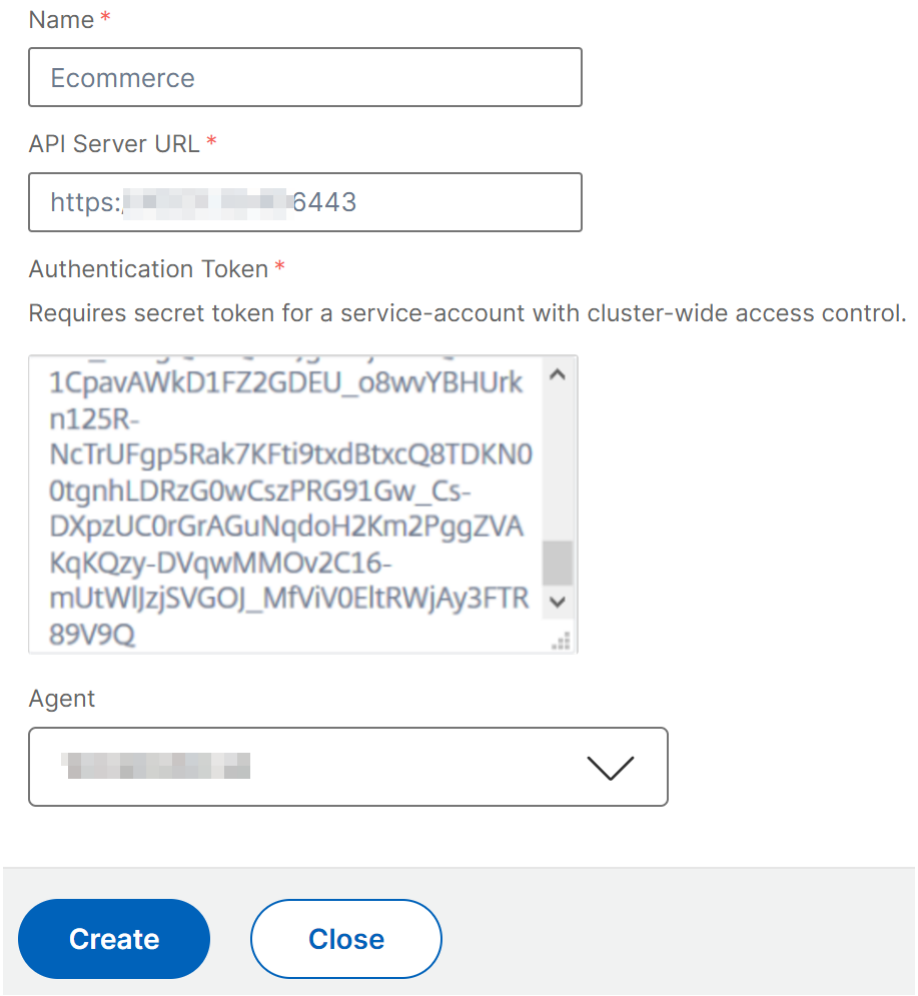
© 1997–2025 Citrix Systems, Inc. All rights reserved.

ii. Copy the token that is generated and paste it as the Authentication Token

For more information, see Kubernetes documentation.

d) Select the agent from the list.

e) Click **Create**.



License Activation Service

September 8, 2025

> **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 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.x (FIPS)
> - NetScaler SVM: 14.1 51.x, 13.1 60.x
> - NetScaler Console Service: will support LAS from early September.
>
> 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.

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:

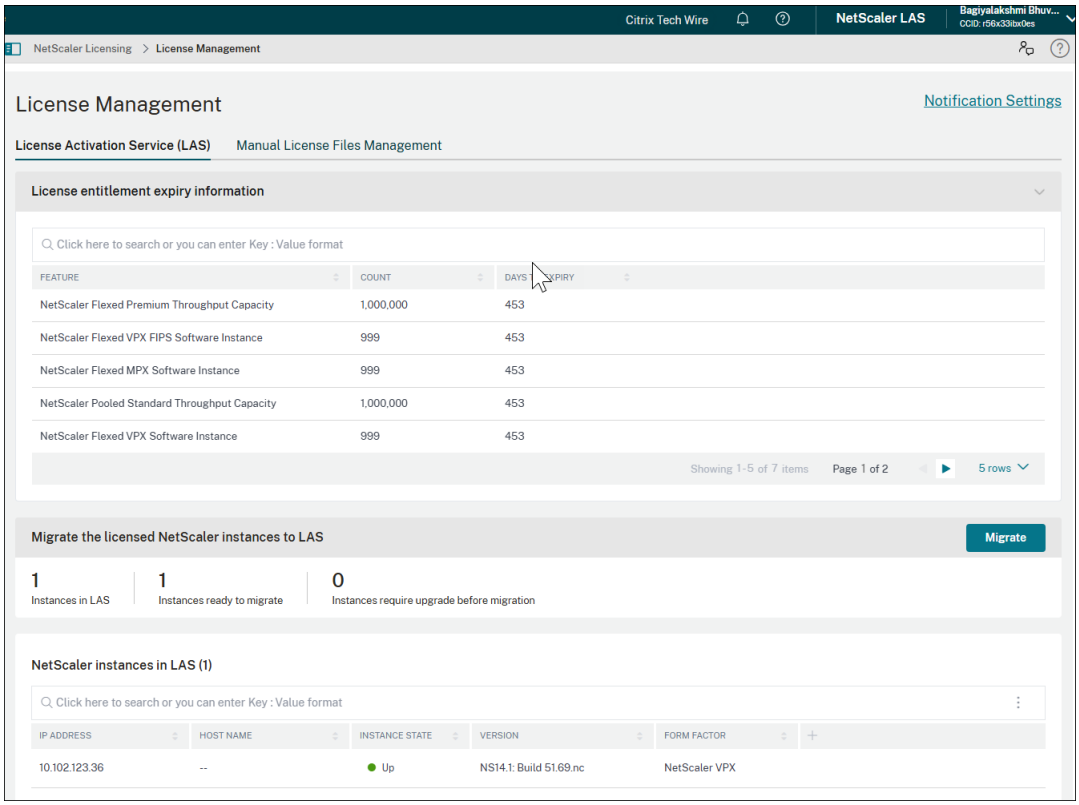
- Automated entitlement delivery through an entitlement blob.
- The external agent for licensing communication is optional.
- LAS eliminates the need for Z-Cap software license files on the NetScaler MPX and SDX instances.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 Licenses > License management > License Activation Service (LAS)** tab.



NetScaler version compatibility for LAS

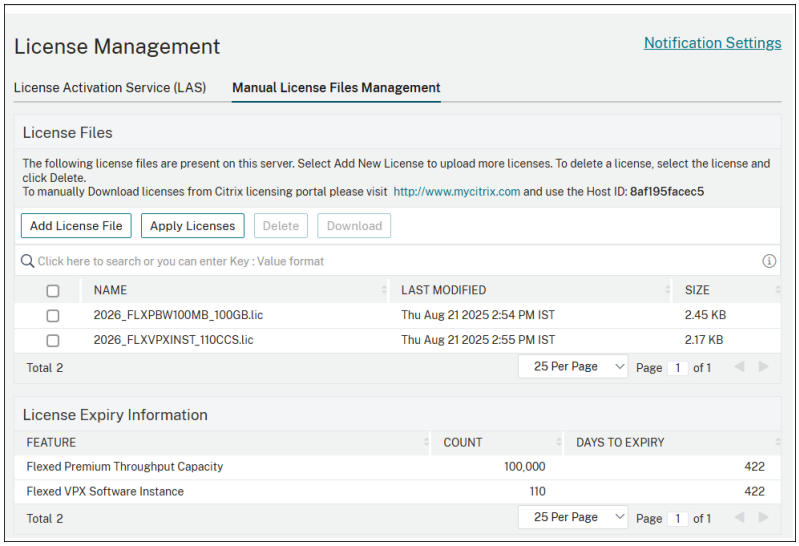
To use LAS, your NetScaler instances must be running one of the following minimum versions:

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

> **Notes:**
>
> To use LAS, ensure 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

With file-based licensing, your applied entitlements and configurations are visible under **NetScaler Licenses > License management> Manual License File management**.



> **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, CICO, are not supported with LAS.

Transition to LAS

When you navigate to **NetScaler Licenses > 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

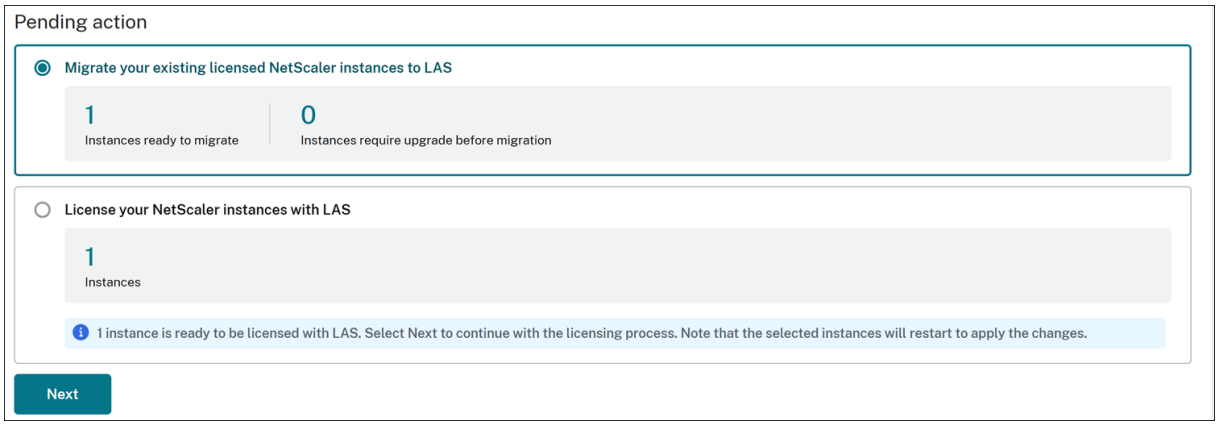
The GUI adjusts dynamically depending on whether you are a first-time LAS user (with Zero instances migrated) or an existing user (who has already moved some instances to LAS and is now adding

© 1997–2025 Citrix Systems, Inc. All rights reserved.

more).

First-Time LAS user

As a first-time user, you see a list of pending actions.



License NetScaler instances with LAS

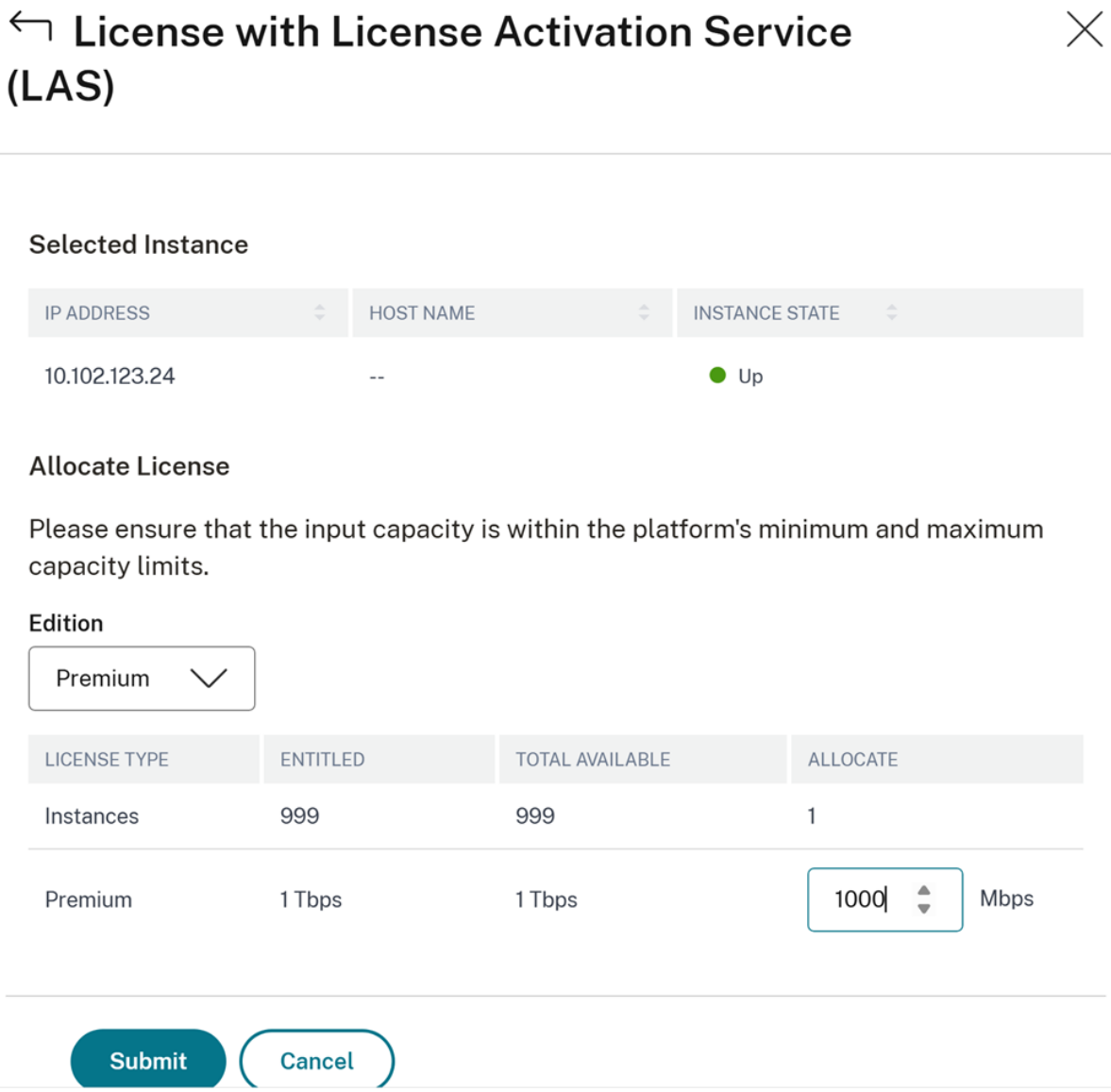
The **License NetScaler instances with LAS** section lists NetScaler instances that are currently unlicensed or that do not use a Flexed bandwidth or Pooled bandwidth file-based license.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

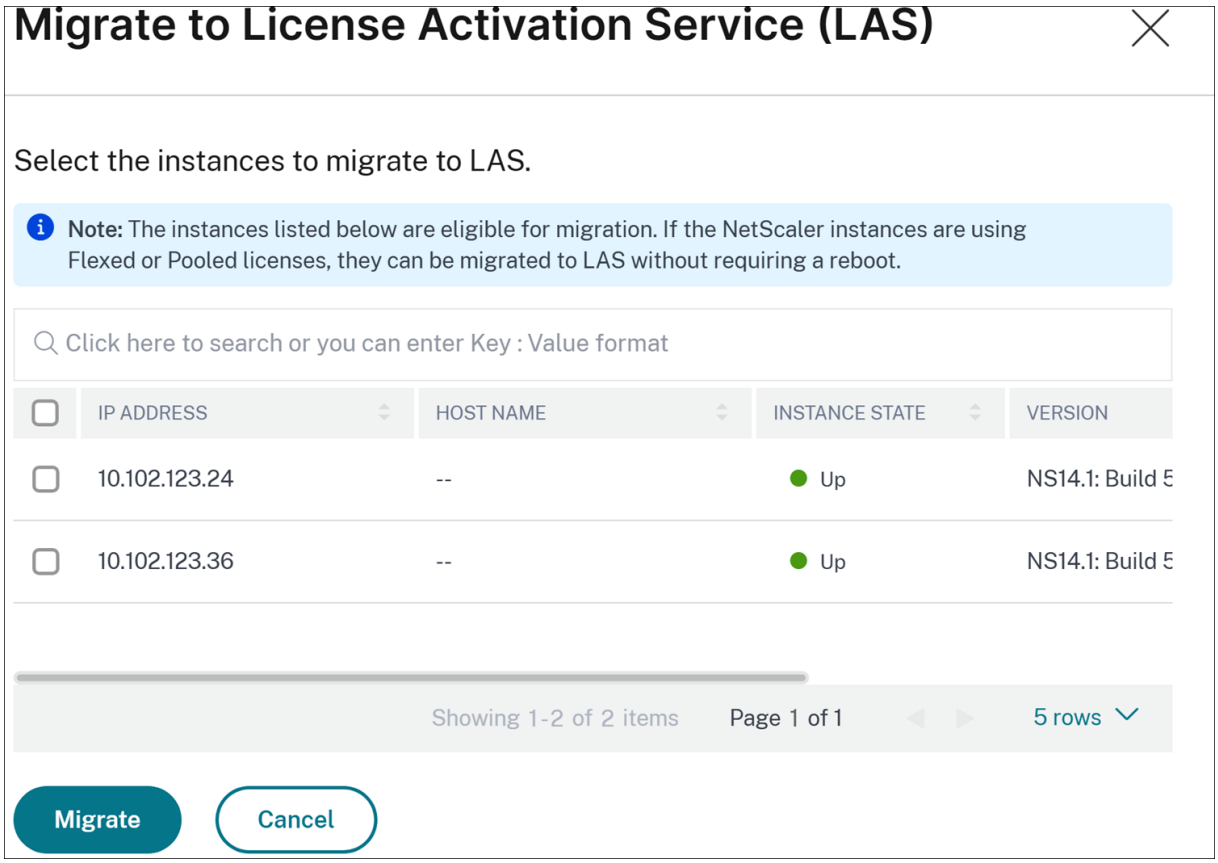


Migrate existing licensed instances to LAS

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**.
    2. Select the instances and click **Migrate**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- **Instances require upgrade before migration:** List the instances that are to be upgraded to a compatible version or builds before migration.

  Prerequisite:

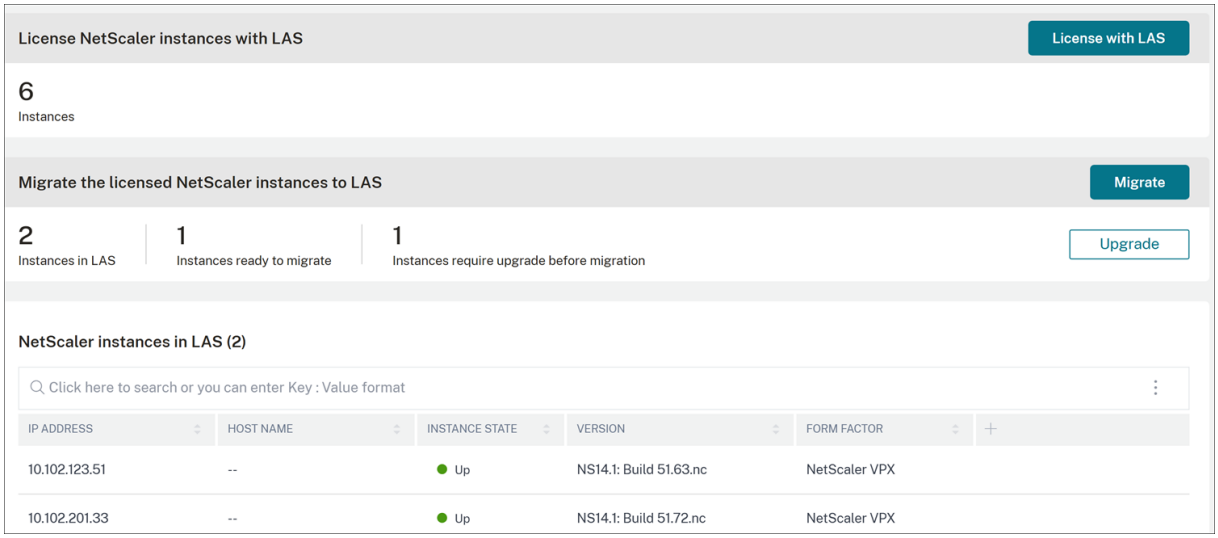
  To use LAS-based licensing, the edition of your NetScaler instance must match the edition of your Pooled or Flexed file-based license. Ensure that you change the instance's edition to match the new license before you begin the migration.

  1. Select **Migrate your existing licensed NetScaler instances to LAS**, click **Upgrade**.
  2. In **Upgrade NetScaler** page, select the instance and upgrade the instances to versions or builds compatible with LAS.

Existing LAS User

If you are an existing user, you see the following GUI.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Note: CPX instances will not be listed here under 'instances licensed with LAS'. To see which CPX instances are listed with LAS, you can refer to Flexed Dashboard page.

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.

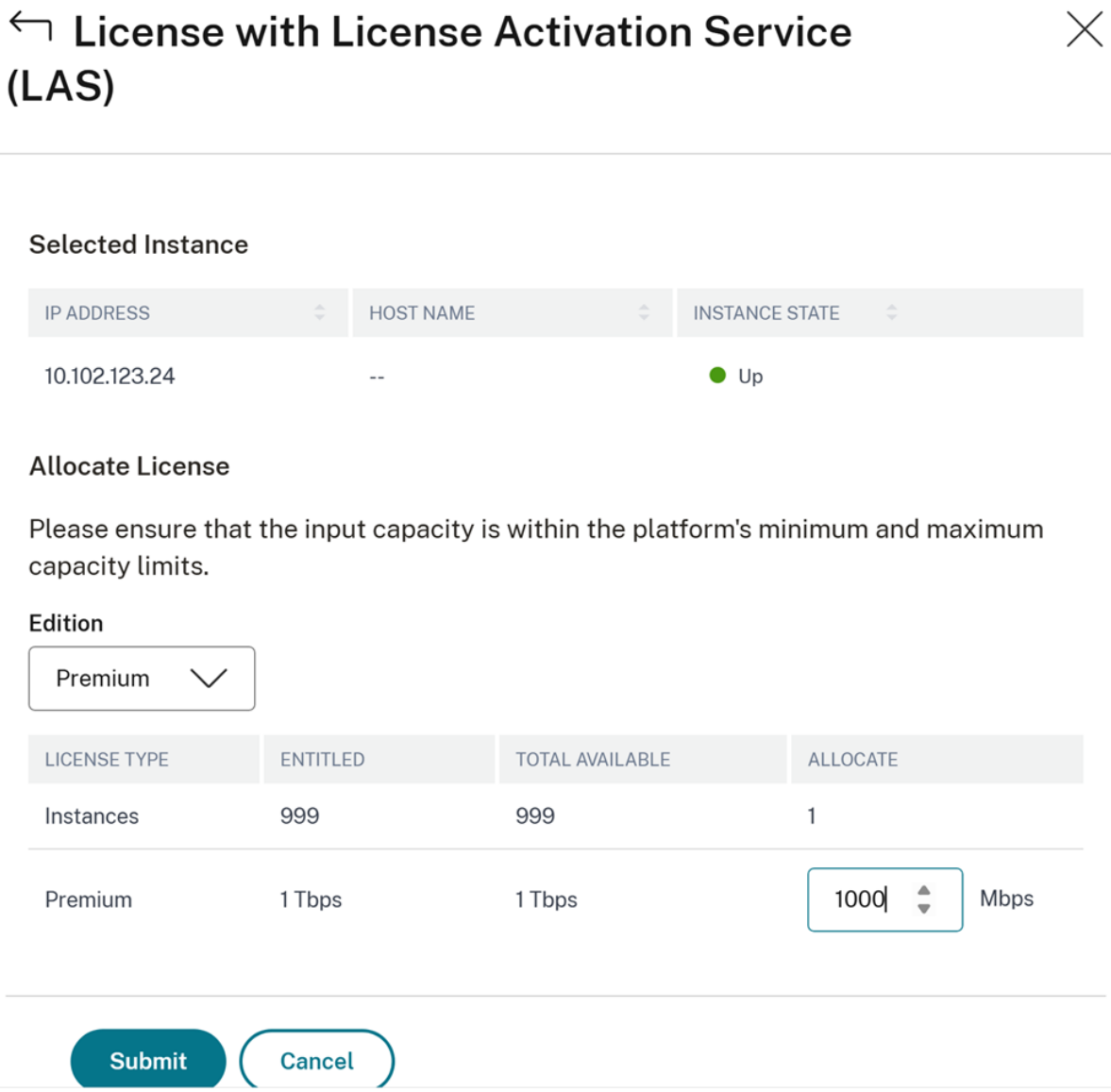
To license an instance, perform the following steps:

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.

© 1997–2025 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:

  1. Select **Migrate the licensed NetScaler instances to LAS**, click **Migrate**.
  2. Select one or more NetScaler instances, and migrate the selected instances to LAS.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Applying these changes restarts the selected instances, except for SDX instances.

- **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.

  1. Select **Migrate the licensed NetScaler instances to LAS**, click **Upgrade**.
  2. Select one or more NetScaler instances, and upgrade the instances to a compatible version or build.

License management

September 8, 2025

> **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.x (FIPS)
> - NetScaler SVM: 14.1 51.x, 13.1 60.x
> - NetScaler Console Service: will support LAS from early September.
>
> 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 Cit-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> rix 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.

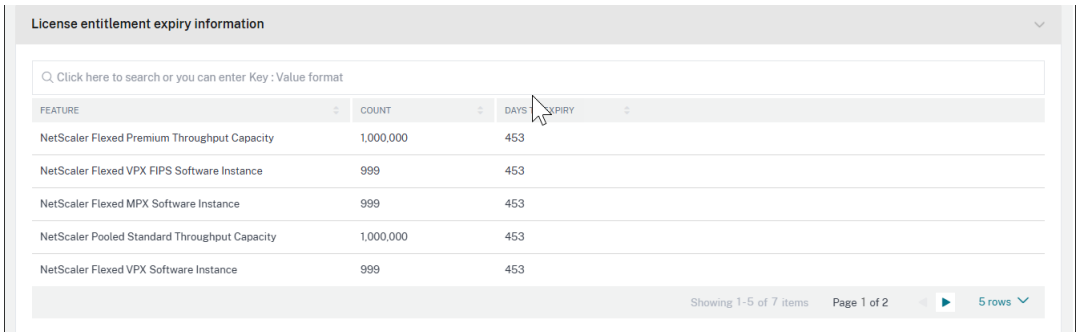
> **Note:**
>
> To use LAS, add your NetScaler® instance as a managed instance.

License expiry information

View license expiry

1. Navigate to **NetScaler Licensing > License Management**.
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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.

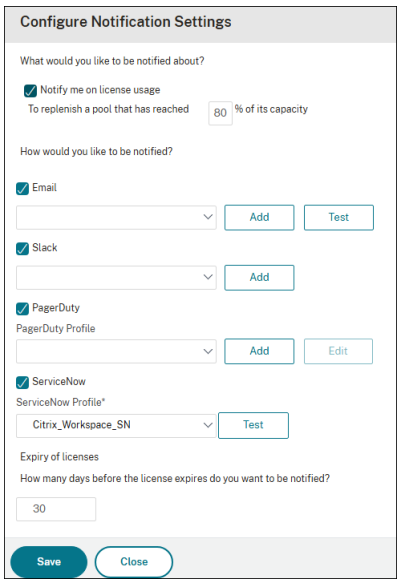
As an administrator, you also receive a notification email for the license end date if email notification is configured in **Notifications settings**. A notification email is sent in the frequency of 60, 30, 20, and 10 days before the license end date.

Notification settings

To set up notifications for expiring Flexed or Pooled licenses managed by LAS, follow these steps:

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**.

© 1997–2025 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.
    - **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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.
   - **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.

Manually managed entitlements (file-based licenses)

The following sections are applicable for manually managed entitlement (file-based licensing).

© 1997–2025 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 FIPS HW participate in Flexed licensing	Download this file	On NetScaler MPX

© 1997–2025 Citrix Systems, Inc. All rights reserved.

File name contains	Description	Download information	Where to upload/apply the license
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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

License File	Apply on
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:

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.

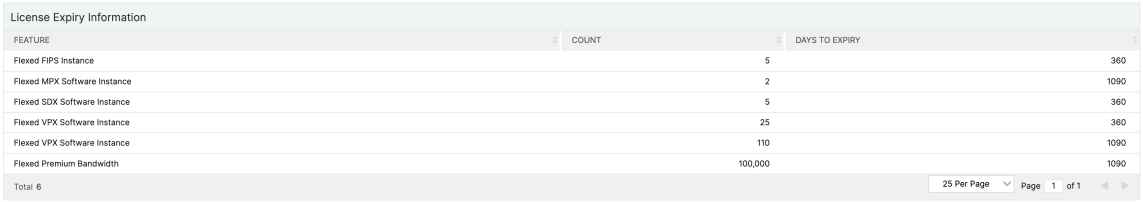
1. Navigate to **NetScaler Licensing > License Management**.
2. In the **License Files** section, click **Add License File** and select one of the following options:
   - **Upload license files from a local computer**: If a license file is already present on your local computer, you can upload it to 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:**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 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).

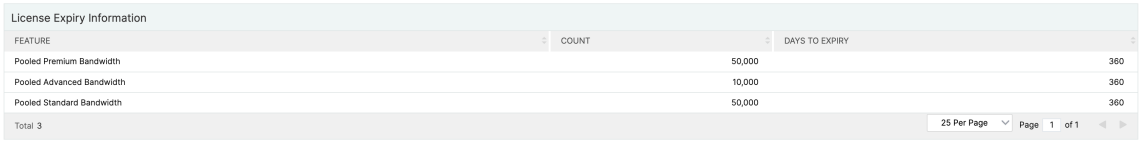


License Expiry Information

FEATURE	COUNT	DAYS TO EXPIRY
Flexed FIPS Instance	5	360
Flexed MPX Software Instance	2	1090
Flexed SDX Software Instance	5	360
Flexed VPX Software Instance	25	360
Flexed VPX Software Instance	110	1090
Flexed Premium Bandwidth	100,000	1090

Total 6 — 25 Per Page — Page 1 of 1

The following screenshot shows the Pooled Standard, Advanced, and Premium bandwidth available and the days to expiry (contract end date).



License Expiry Information

FEATURE	COUNT	DAYS TO EXPIRY
Pooled Premium Bandwidth	50,000	360
Pooled Advanced Bandwidth	10,000	360
Pooled Standard Bandwidth	50,000	360

Total 3 — 25 Per Page — Page 1 of 1

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.
    - **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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.
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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.
    - **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.

Minimum and maximum capacity for checkout

September 8, 2025

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **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.x (FIPS)
> - NetScaler SVM: 14.1 51.x, 13.1 60.x
> - NetScaler Console Service: will support LAS from early September.
>
> 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.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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
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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Product line	Minimum bandwidth (Gbps)	Maximum bandwidth (Gbps)	Minimum bandwidth unit
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
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

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)

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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
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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Product line	Minimum bandwidth (Gbps)	Maximum bandwidth (Gbps)	Minimum instances	Maximum instances	Minimum bandwidth unit
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
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

© 1997–2025 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

Table 6. Zero capacity license requirement for different form factors

Product line	Zero Capacity Hardware
MPX	License required
SDX	License required

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Product line	Zero Capacity Hardware
VPX	-
CPX	-
BLX	-

NetScaler agent behavior

September 8, 2025

> **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.x (FIPS)
> - NetScaler SVM: 14.1 51.x, 13.1 60.x
> - NetScaler Console Service: will support LAS from early September.
>
> 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.

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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, configure the agent cluster support feature. For more information, see Configure agent cluster support.

> **Note:**
>
> If you are using a built-in agent, you can only transition to LAS-based licensing through the NetScaler Console GUI.

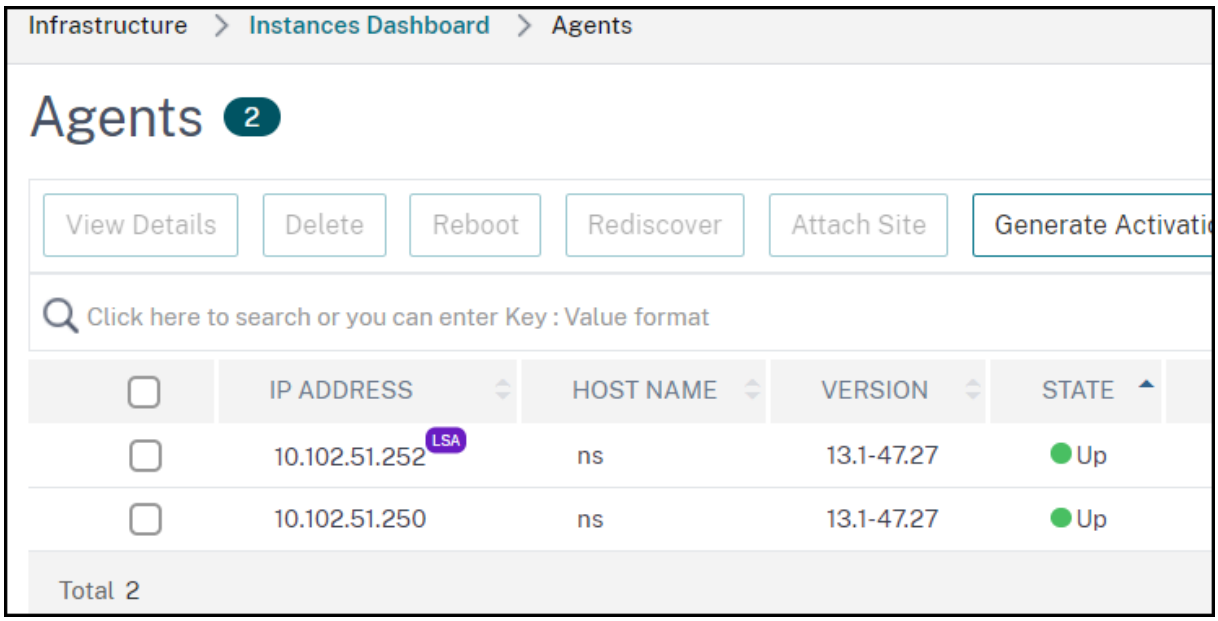
Manually managed entitlement (file-based licensing)

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.

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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> NetScaler built-in agent cannot be assigned the LSA role.

Flexed license

September 8, 2025

> **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.x (FIPS)
> - NetScaler SVM: 14.1 51.x, 13.1 60.x
> - NetScaler Console Service: will support LAS from early September.
>
> 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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):

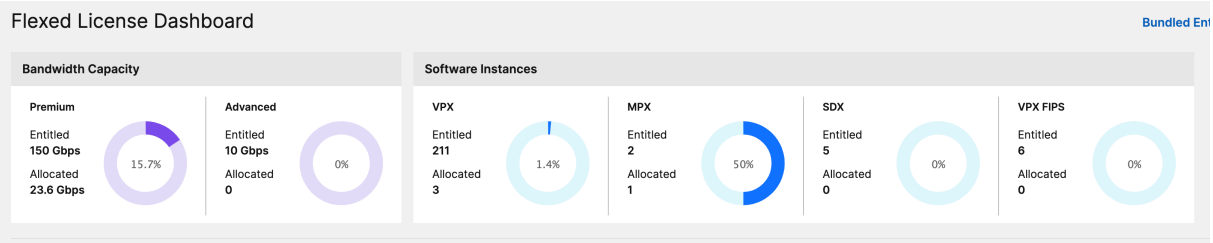
When using manually managed entitlements (file-based licensing), perform the following steps:

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.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **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.

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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 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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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.

Configure license

September 8, 2025

> **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.x (FIPS)
> - NetScaler SVM: 14.1 51.x, 13.1 60.x
> - NetScaler Console Service: will support LAS from early September.
>
> 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.

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 checks the allo-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

cated 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 when you configure the agent. For more informatiion about built-in agent, see Configure Built-in Agent for NetScaler Console On-Prem.
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

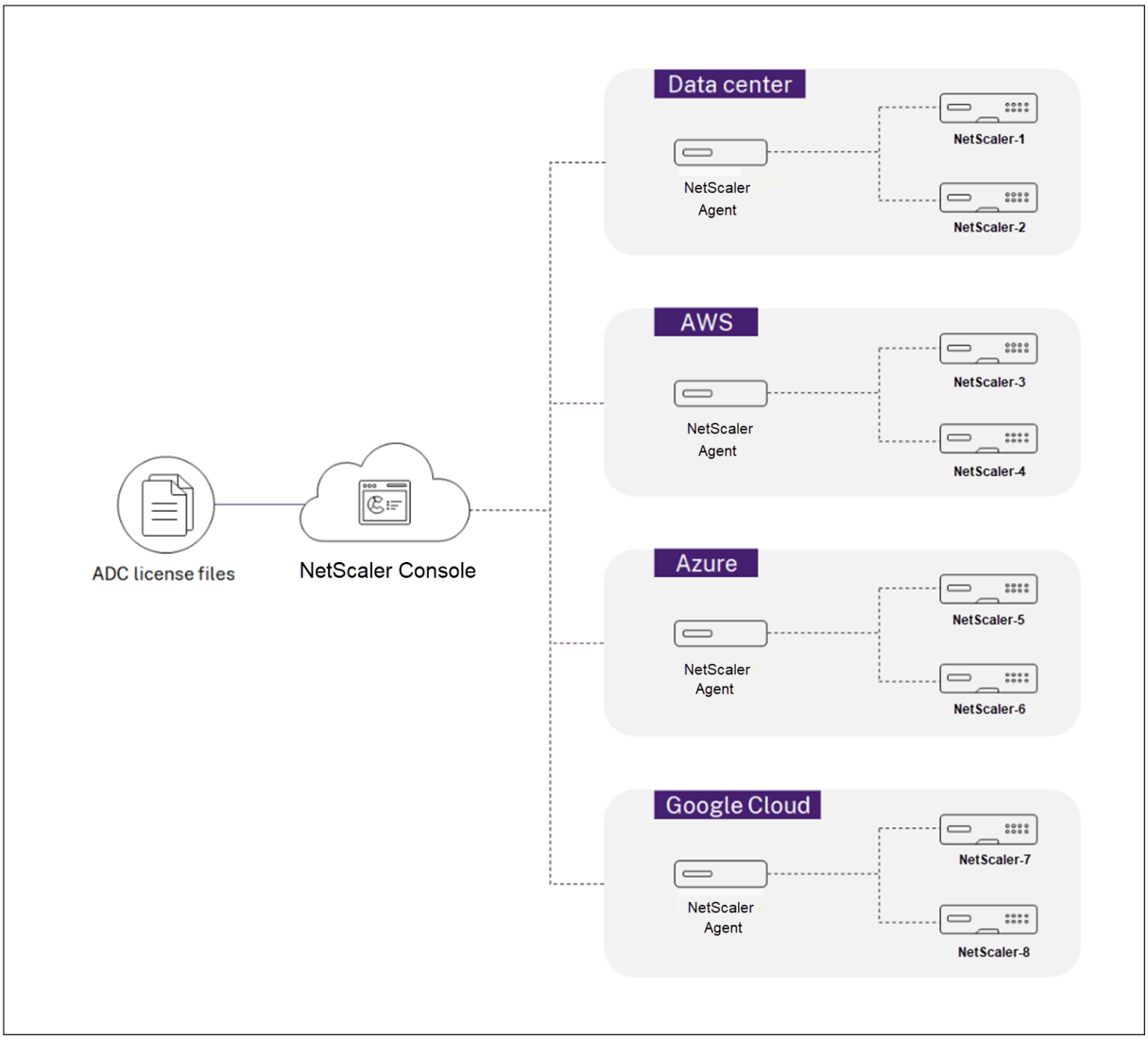
Manually managed entitlements (file-based licensing)

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.

© 1997–2025 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- The 27000 and 7279 ports are available to check out licenses from NetScaler Console to an instance. See, System requirements.

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.

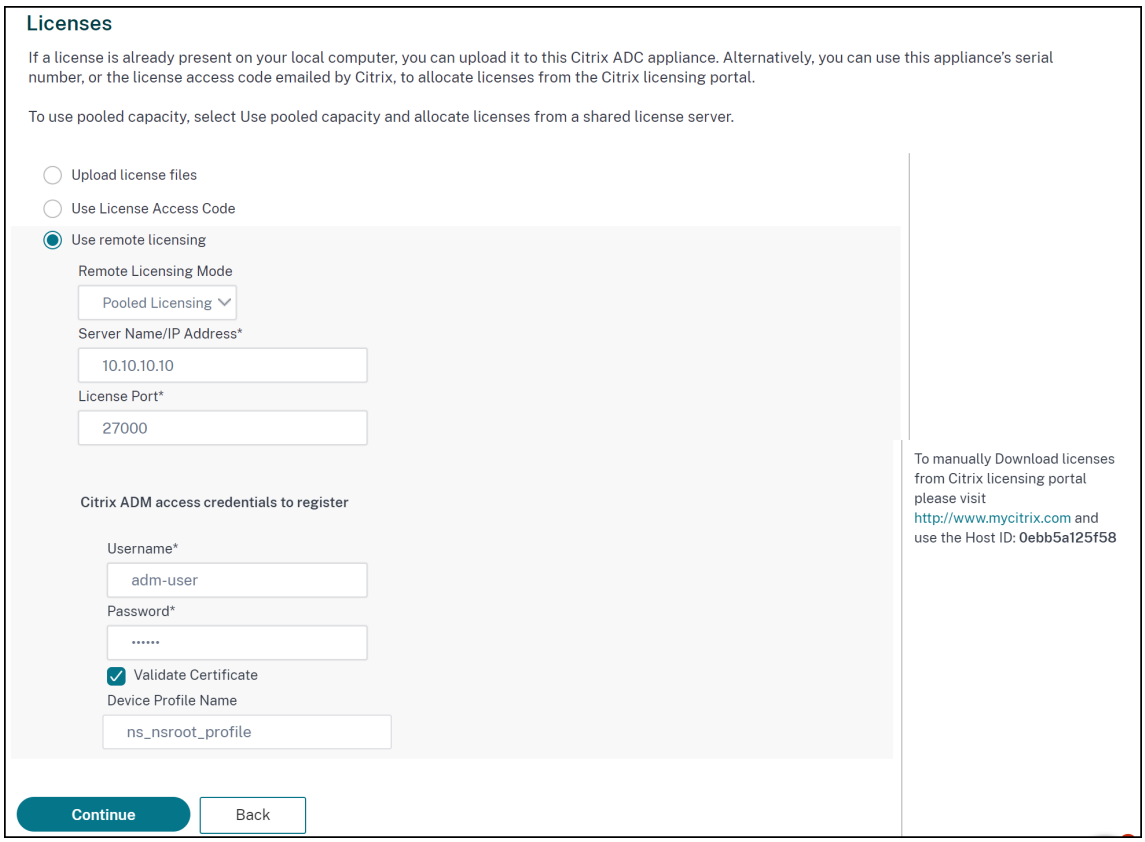
© 1997–2025 Citrix Systems, Inc. All rights reserved.

6. The default license port is 27000.
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.

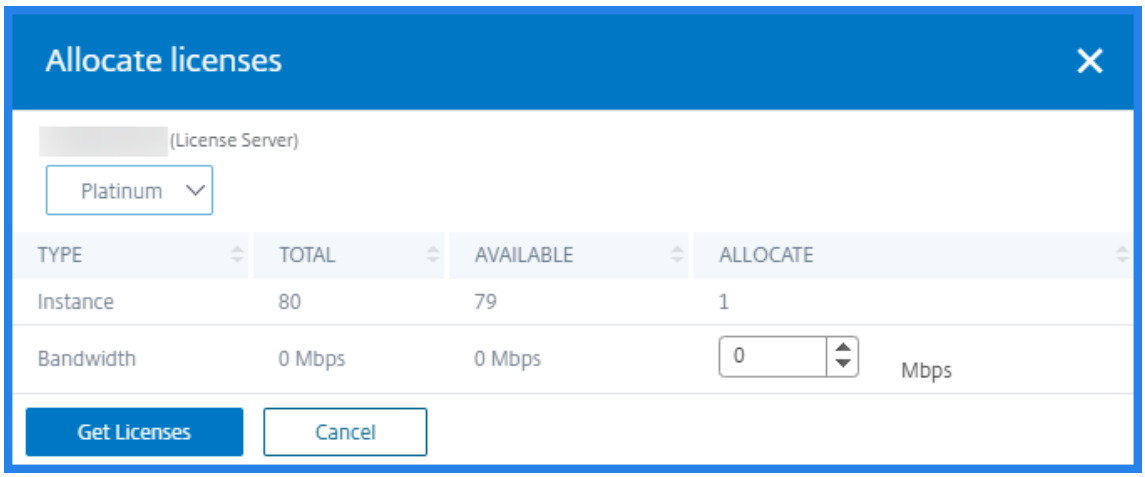
8. Under **Device Profile Name**, specify the instance profile that NetScaler Console can use to access the instance. This instance profile contains the user name and password of the instances that you want to add to NetScaler Console. The default profile is **ns_nsroot_profile**. If you have changed the default admin credentials of your instances, you can define a custom instance profile name.



9. In **Allocate licenses**, select the license edition and specify the required bandwidth.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:

```
> 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

   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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **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
- 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

> **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 Allocate Flexed licenses to 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).
- **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

License dashboard

September 8, 2025

> **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.x (FIPS)
> - NetScaler SVM: 14.1 51.x, 13.1 60.x
> - NetScaler Console Service: will support LAS from early September.
>
> 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 procededing further.

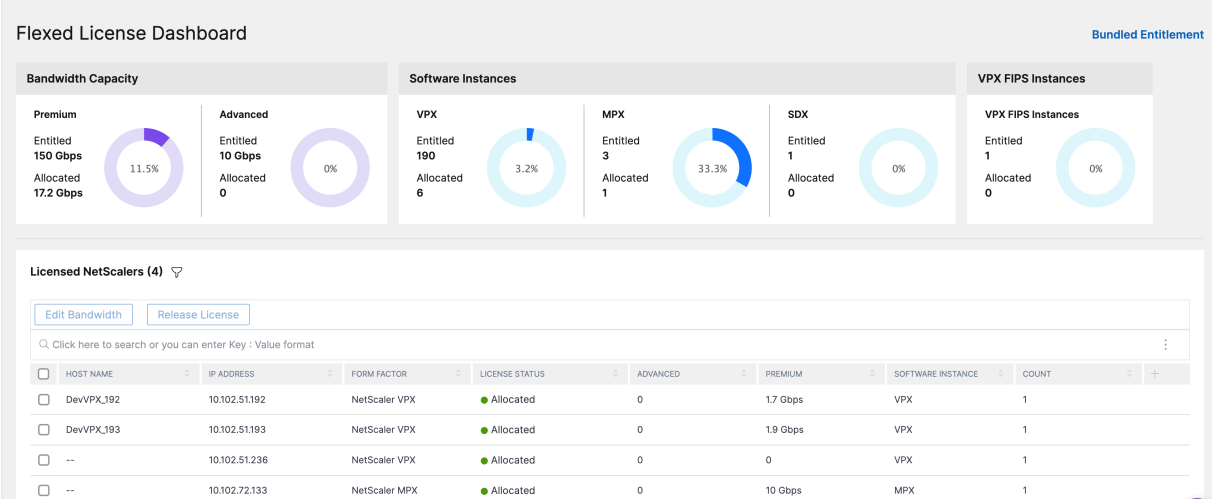
> **Notes:**
>
> - If you had pooled licenses earlier, and now purchased and applied Flexed licenses, the combined entitlement now appears in the Flexed license dashboard.
> - If you have only pooled licenses, check the Pooled license dashboard.
> - If you have only Flexed licenses, or both Flexed and Pooled licenses, check the Flexed license dashboard.
> - **Point to note based on licensing method:**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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.



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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - 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**.
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:

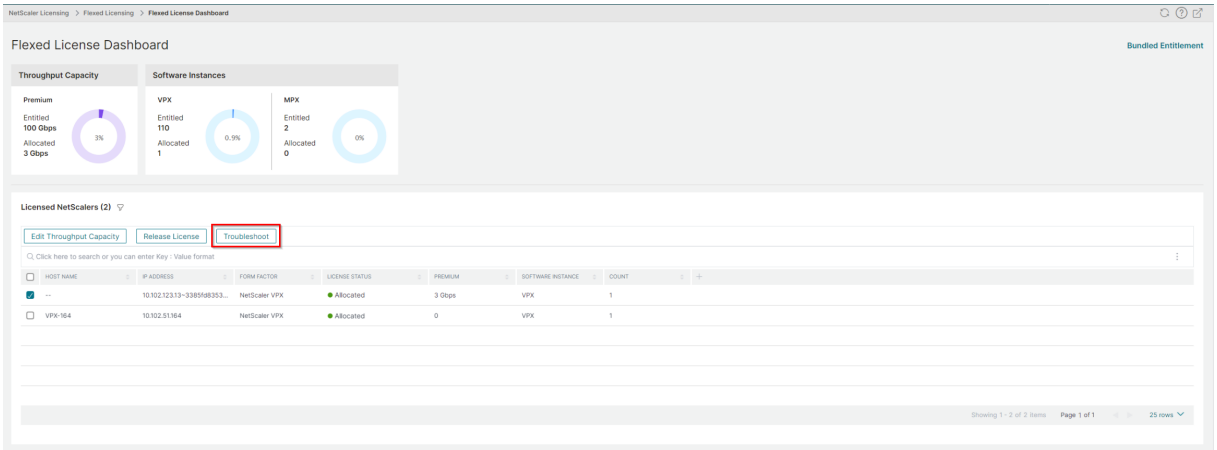
- Releases all the licenses, which are checked out on that instance, to the license server.
- Deletes the license server configuration on that instance.

If you select **Yes**, your NetScaler instance becomes unlicensed and cannot process any traffic.

Troubleshoot licensing issues

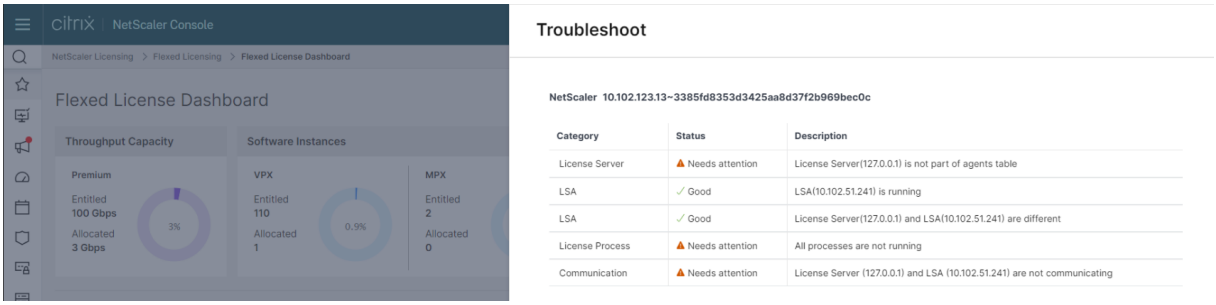
You can use the **Troubleshoot** option to view and analyze few licensing related issues.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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:



License reporting

September 8, 2025

> **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.

© 1997–2025 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.x (FIPS)
> - NetScaler SVM: 14.1 51.x, 13.1 60.x
> - NetScaler Console Service: will support LAS from early September.
>
> 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:

> **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).

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

> **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.

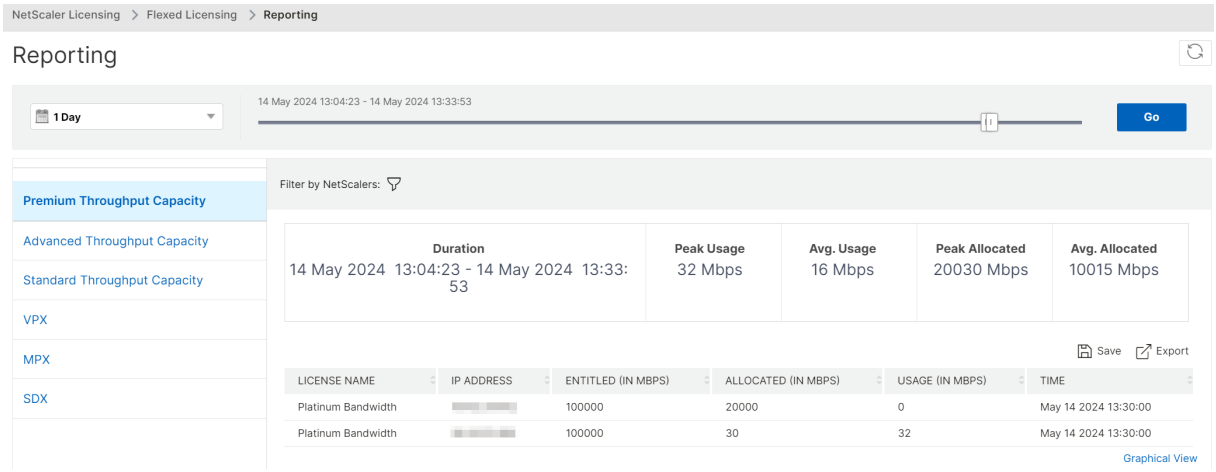
- **Peak usage** = The sum of the highest datapoint (Mbps) from the 24 hours of all NetScaler instances. For example, if the highest datapoint from the 24-hour duration for NetScaler A is 30 Mbps, NetScaler B is 45 Mbps, and NetScaler C is 120 Mbps, then the peak usage is displayed as 195 Mbps (30 + 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).

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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):

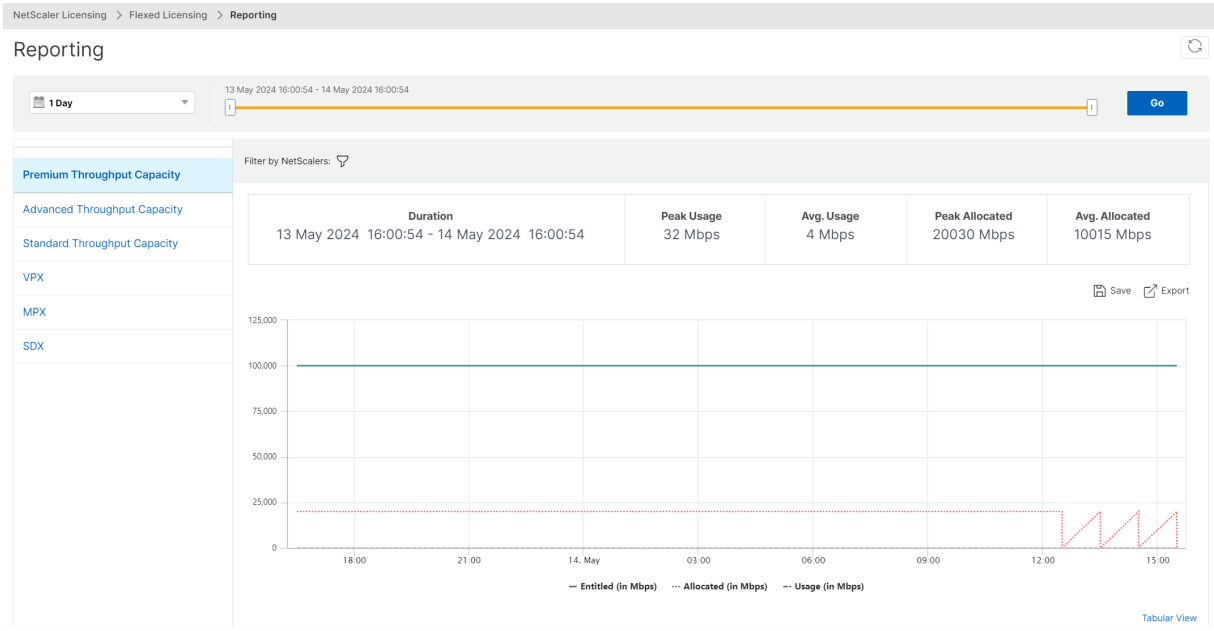


The following details appear on the dashboard:

- **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):

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Transition to Flexed licensing

September 8, 2025

> **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.x (FIPS)
> - NetScaler SVM: 14.1 51.x, 13.1 60.x
> - NetScaler Console Service: will support LAS from early September.
>
> 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.

© 1997–2025 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.

Read the following note before procededing further.

> **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).

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

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.
5. Warm reboot NetScaler.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.
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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

September 8, 2025

> **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.x (FIPS)
> - NetScaler SVM: 14.1 51.x, 13.1 60.x
> - NetScaler Console Service: will support LAS from early September.
>
> 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 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.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:

    1. Navigate to **System > Licenses > Manage Licenses**.
    2. Click **Release Allocation** to release the allocation.
    3. 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:
  1. Navigate to **System > Licenses > Manage Licenses**.
  2. Click **Release Allocation** to release the allocation.
  3. 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.
- 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:
  1. Navigate to **System > Licenses > Manage Licenses**.
  2. Click **Release Allocation** to release the allocation.
  3. 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Configure NetScaler Console server only as the Flexed or Pooled license server

September 8, 2025

> **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.x (FIPS)
> - NetScaler SVM: 14.1 51.x, 13.1 60.x
> - NetScaler Console Service: will support LAS from early September.
>
> 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.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

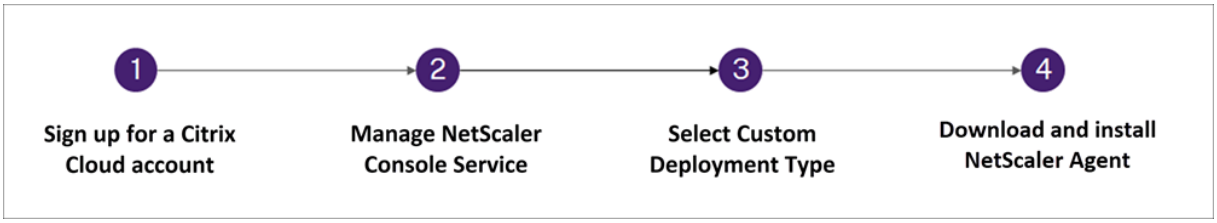
Therefore, configure the NetScaler Console only for the Pooled licensing feature. The NetScaler Console receives only licensing data from all NetScaler instances. So, you can adhere to the regulatory mandate and dynamically allocate Pooled capacity licenses across globally deployed NetScaler instances.

This document explains how to configure the NetScaler Console only for the Pooled licensing feature.

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.

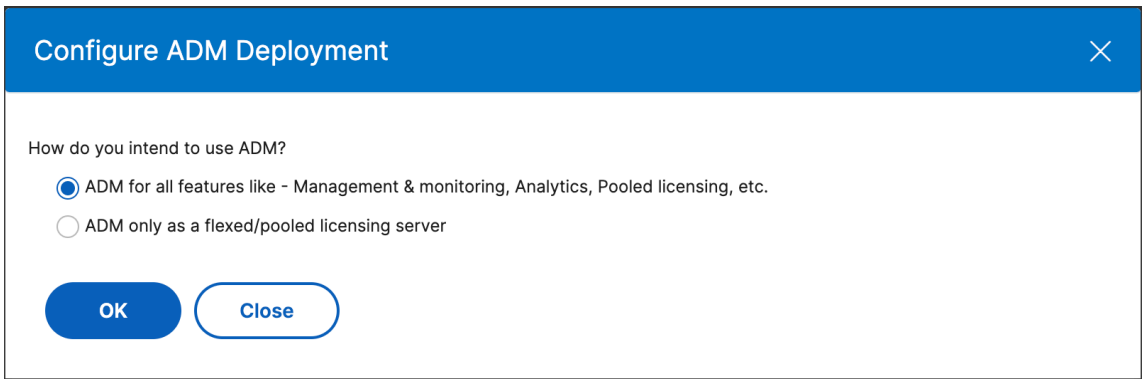
After you complete the onboarding steps, configure the NetScaler Console only for the Pooled licensing feature.

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**.

© 1997–2025 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> restrict such operations, disable user accesses for other administrators using an appropriate access policy. For more information, see Configure Access Policies on NetScaler Console.

Pooled capacity

September 8, 2025

> **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.x (FIPS)
> - NetScaler SVM: 14.1 51.x, 13.1 60.x
> - NetScaler Console Service: will support LAS from early September.
>
> 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **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.

Upgrade a perpetual license in NetScaler MPX to NetScaler Pooled capacity

September 8, 2025

> **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.x (FIPS)
> - NetScaler SVM: 14.1 51.x, 13.1 60.x
> - NetScaler Console Service: will support LAS from early September.
>
> 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 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 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.

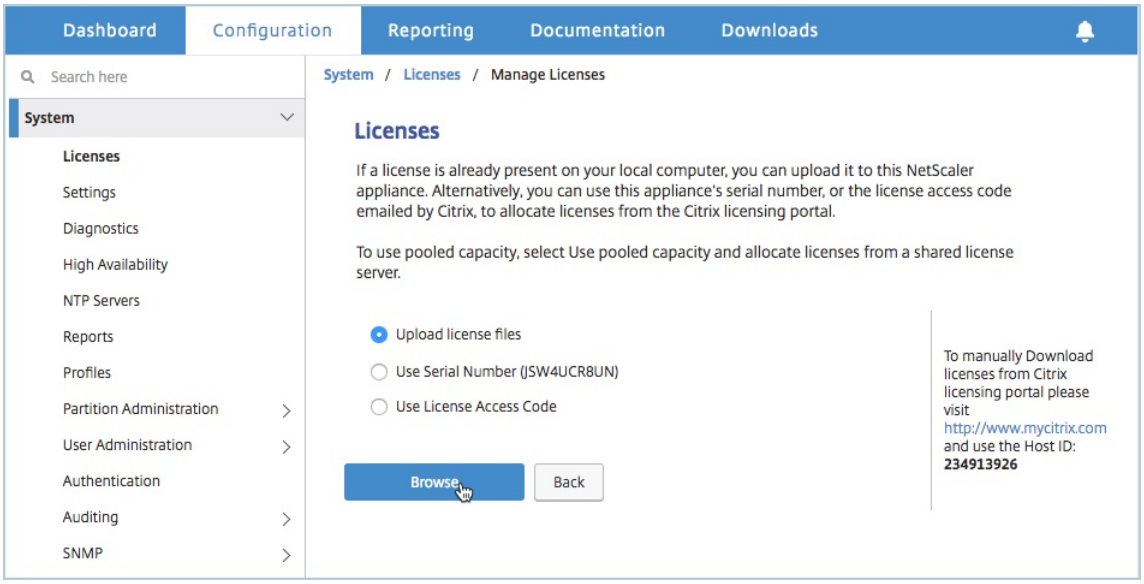
You can also configure the NetScaler Pooled capacity license for NetScaler instances configured in high availability mode. To configure NetScaler Pooled capacity license for NetScaler MPX instances in high availability mode, see Upgrading the perpetual license in NetScaler MPX high availability pair 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:

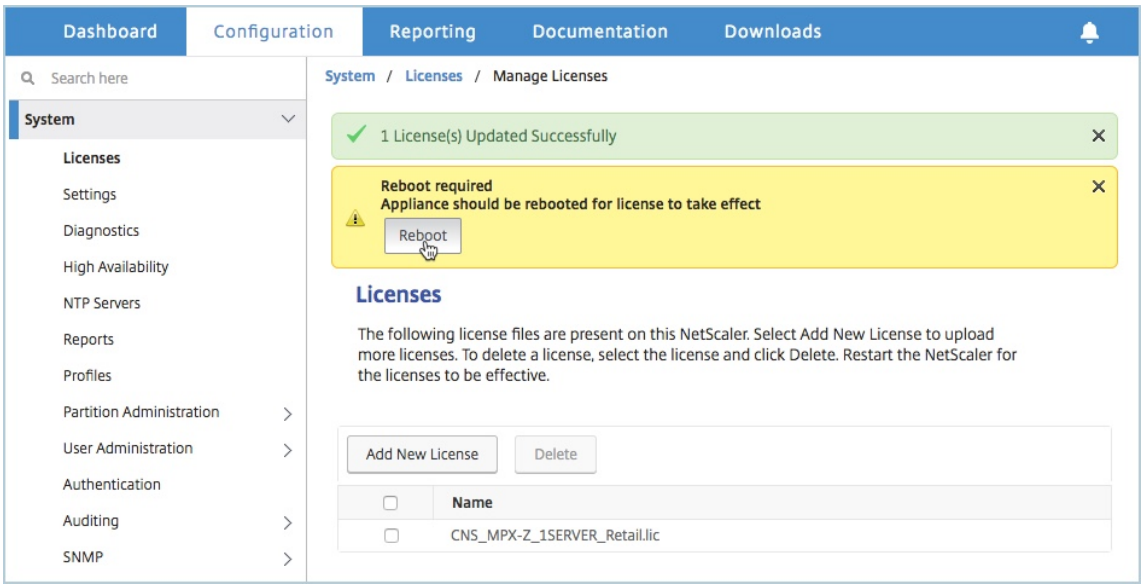
1. In a Web browser, type the IP address of the NetScaler appliance, such as http://192.168.100.1.
2. In **User Name** and **Password** fields, type the administrator credentials.
3. On the **Welcome** page, click **Continue**.
4. Upload the zero capacity license (MPX-Z license). On the Configuration 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



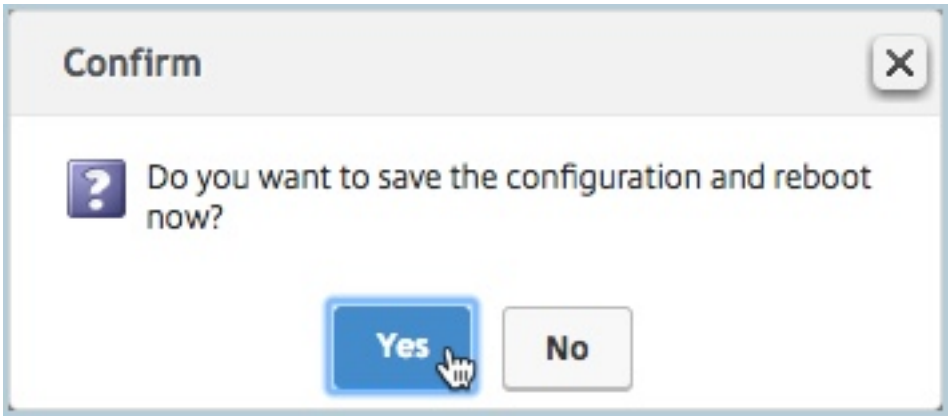
7. After the license is uploaded, click **Reboot** to reboot the appliance.

> **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.

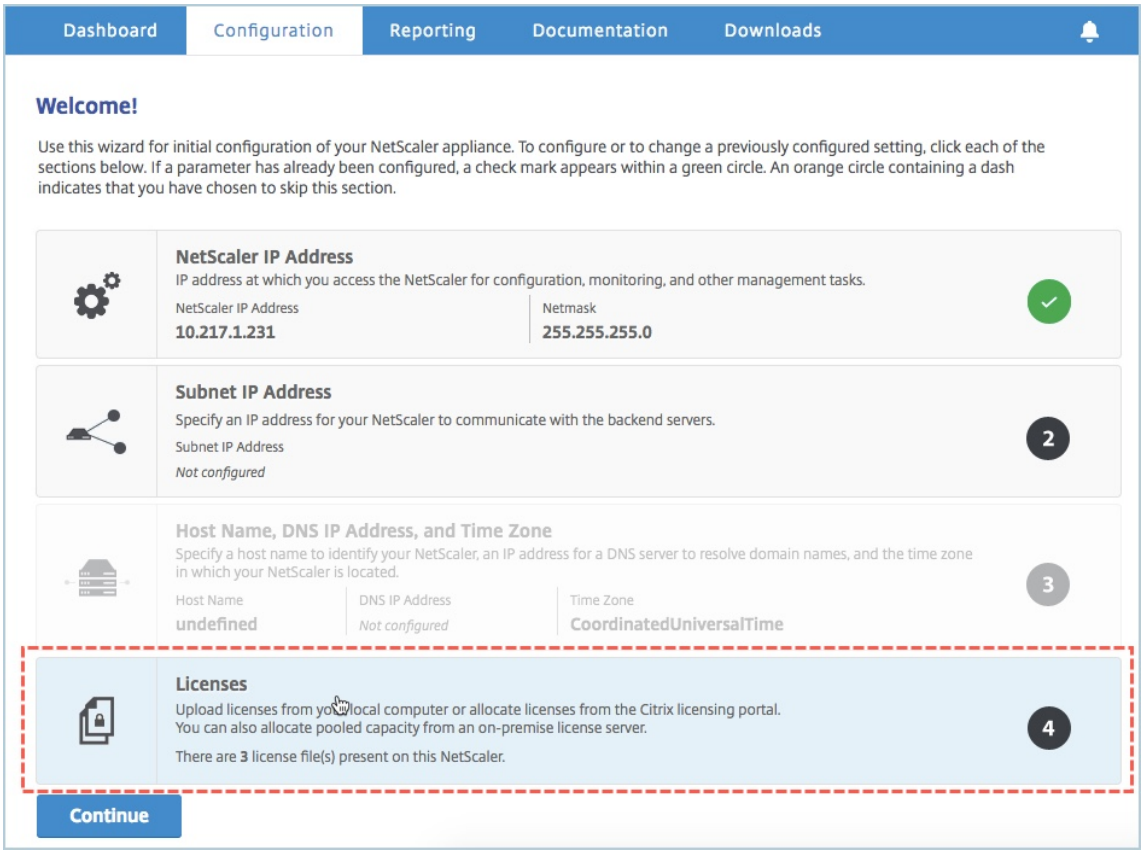


8. On the **Confirm** page, click **Yes**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

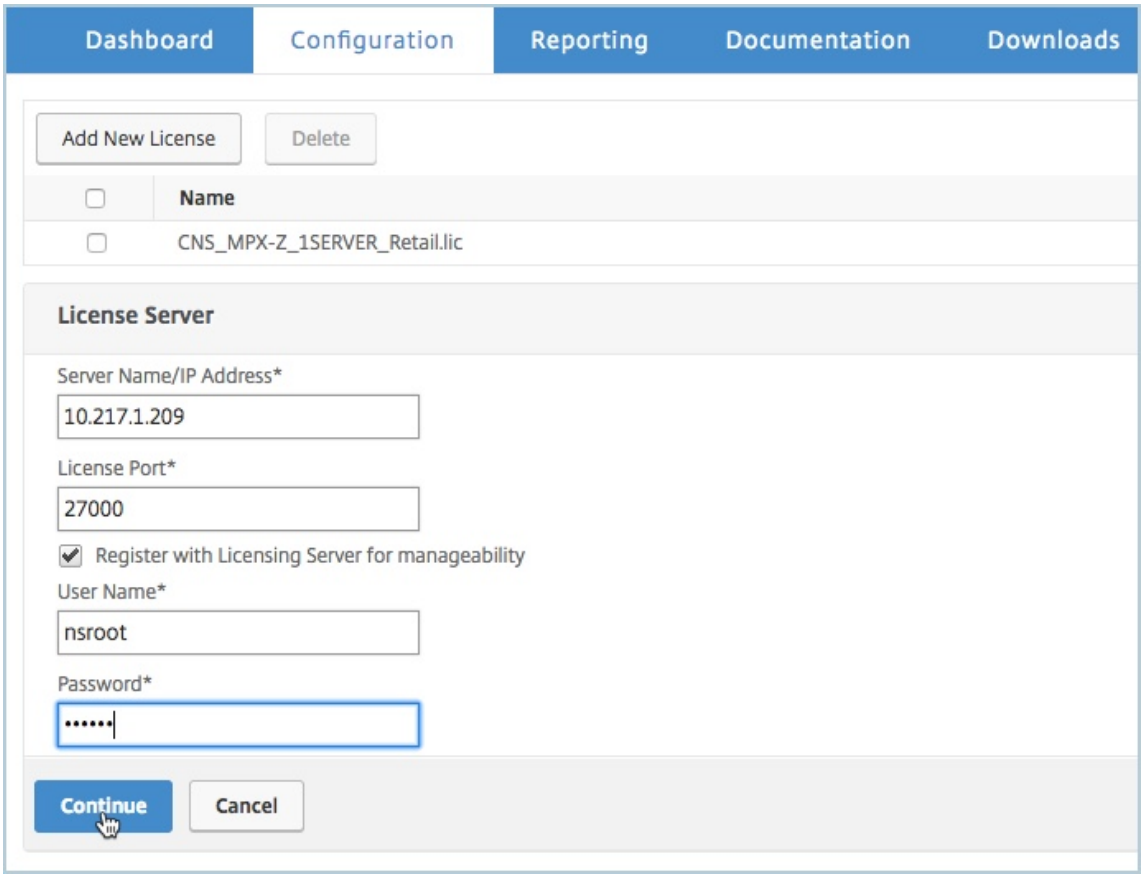


9. After the appliance reboots, logon to the appliance.
10. On the Welcome page, click the **Licenses** section.



11. In the **License Server** section, do the following:

© 1997–2025 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.

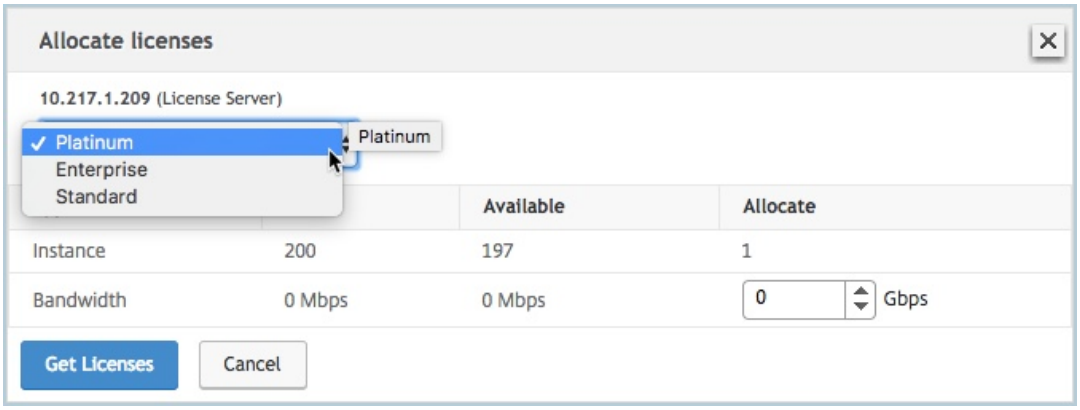
c) If you want to manage your instance's pool licenses through NetScaler Console, select the **Register with Licensing Server for manageability** checkbox and enter NetScaler Console credentials.

d) Click **Continue**.

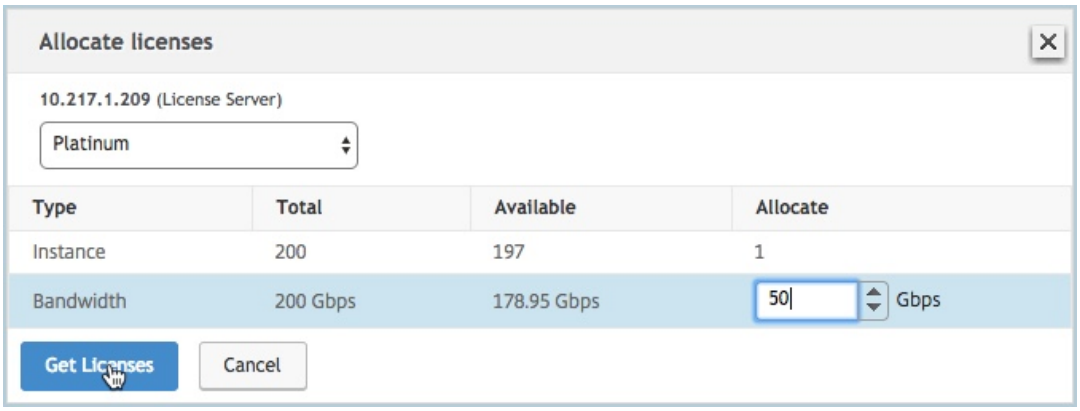
12. In the Allocate licenses window, do the following:

a) Select the license edition from the drop-down list.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

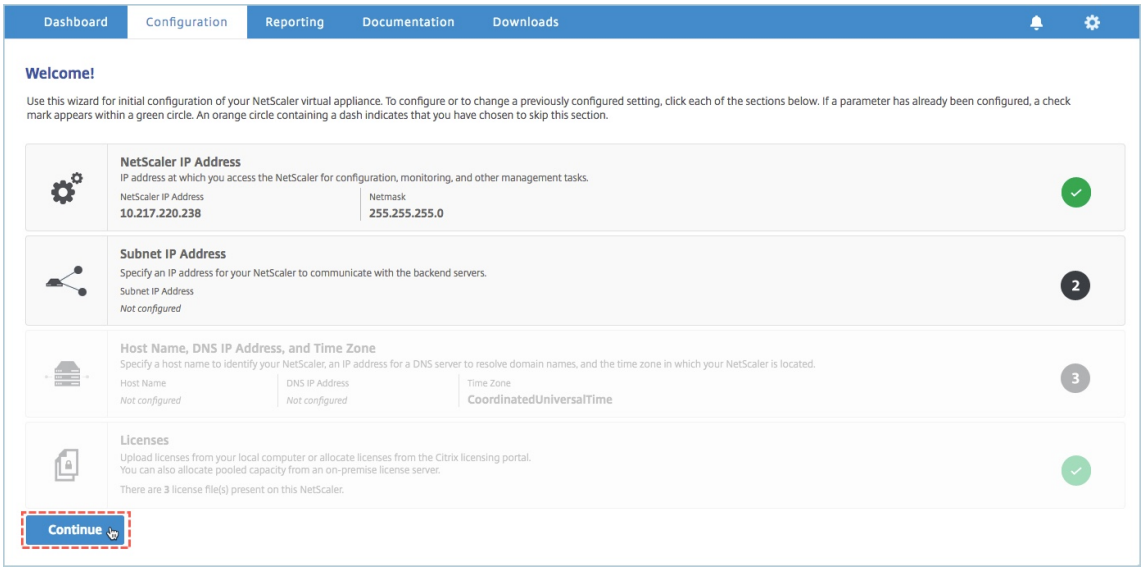


b) Allocate the bandwidth to the NetScaler appliance from the **Allocate** menu and click **Get Licenses**.



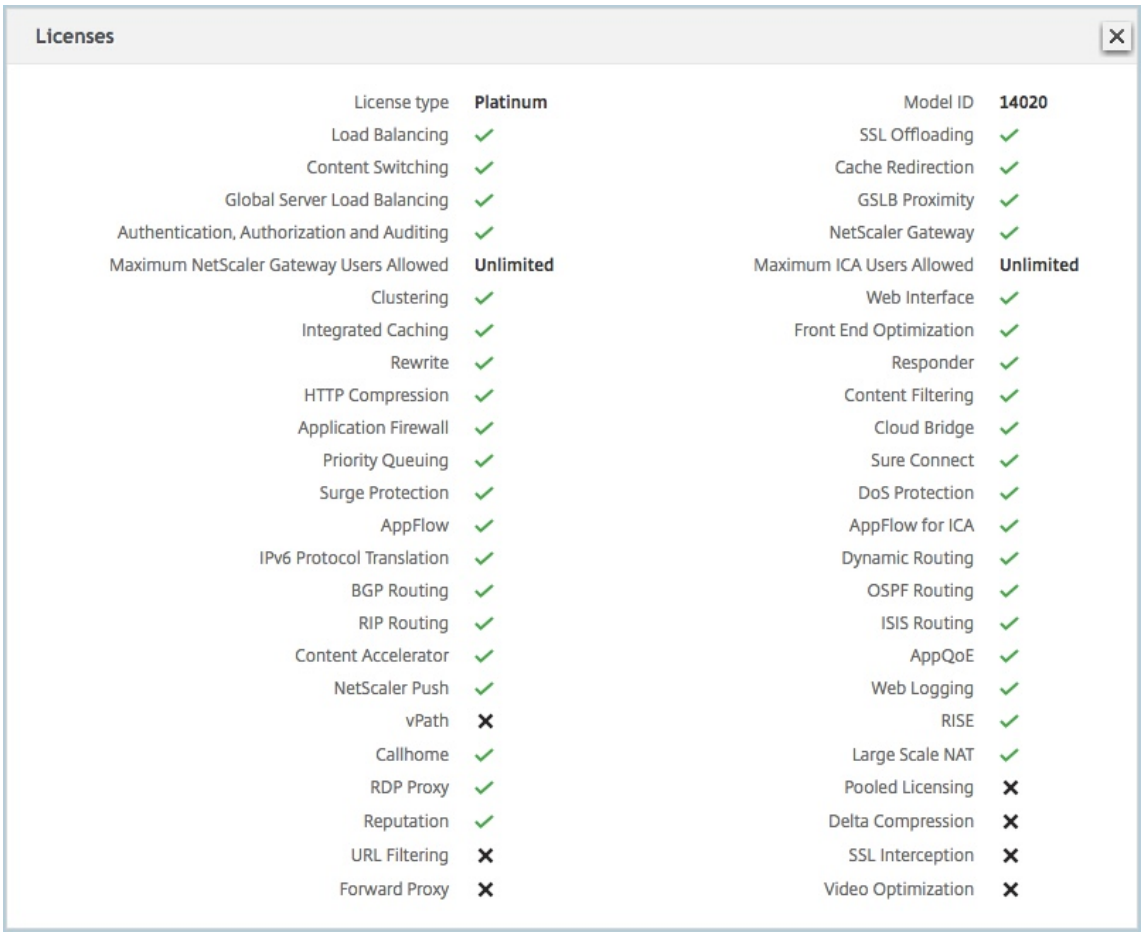
c) When prompted, click **Reboot** to reboot the appliance.

13. Once the NetScaler MPX appliance reboots, logon to the NetScaler MPX appliance. On the **Welcome** page, click **Continue**.

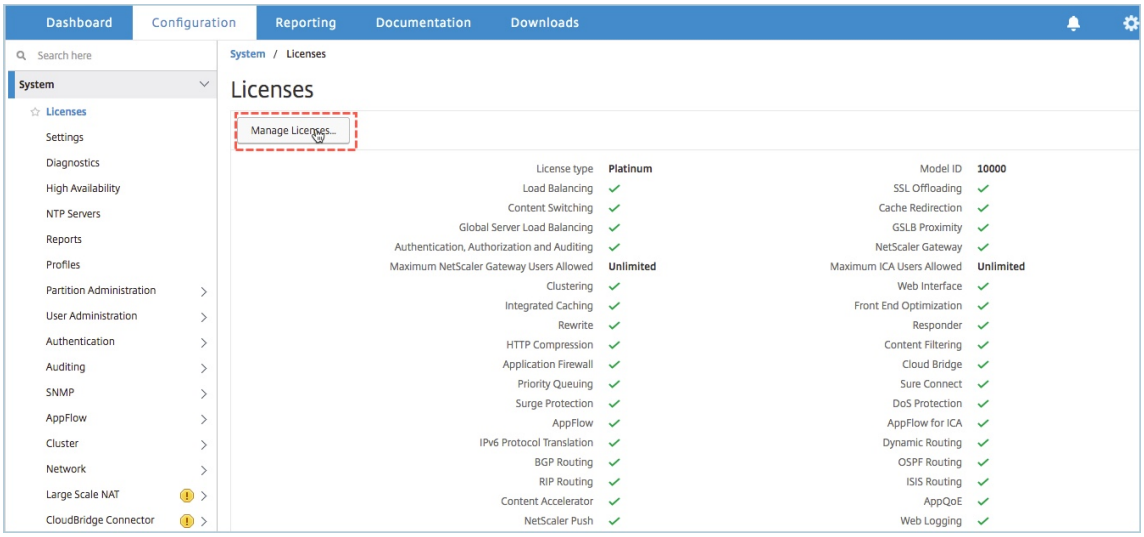


© 1997–2025 Citrix Systems, Inc. All rights reserved.

The **Licenses** page lists all the licensed features.

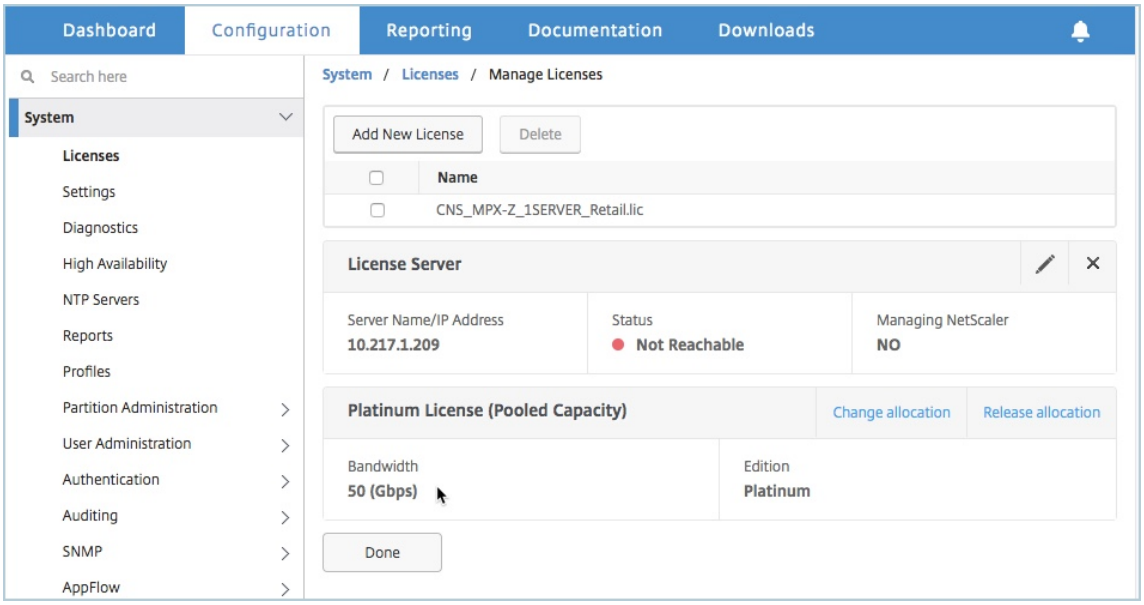


14. Navigate to **System > Pooled Licensing** and click **Manage Licenses**.



On the **Manage Licenses** page, you can view the details of the license server, license edition and the allocated bandwidth.

© 1997–2025 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

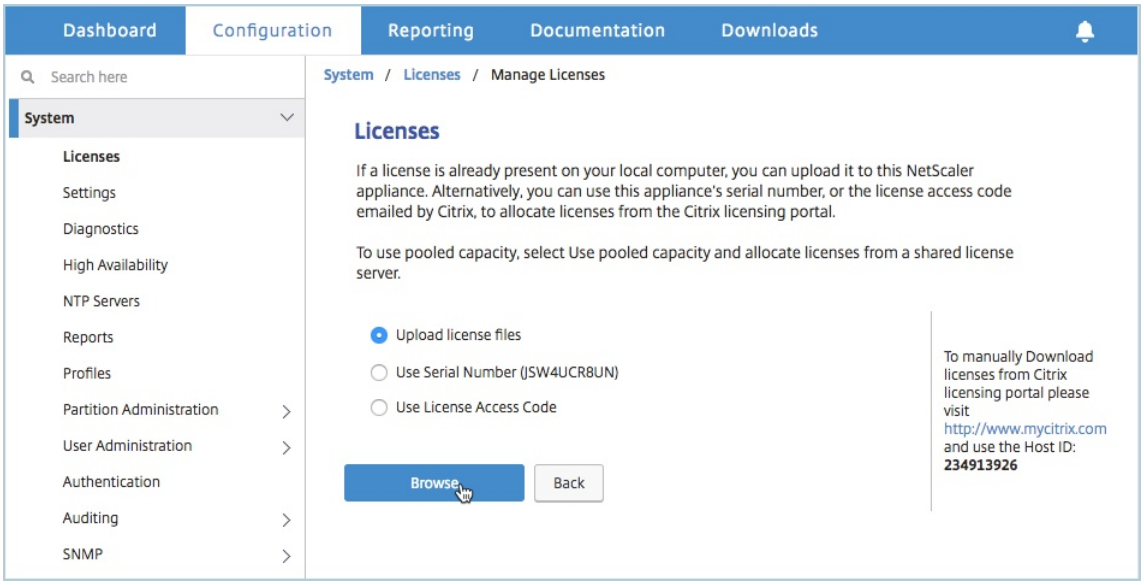
Make sure that you upload the MPX-Z license to both the primary and secondary instances in the HA pair.

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**.

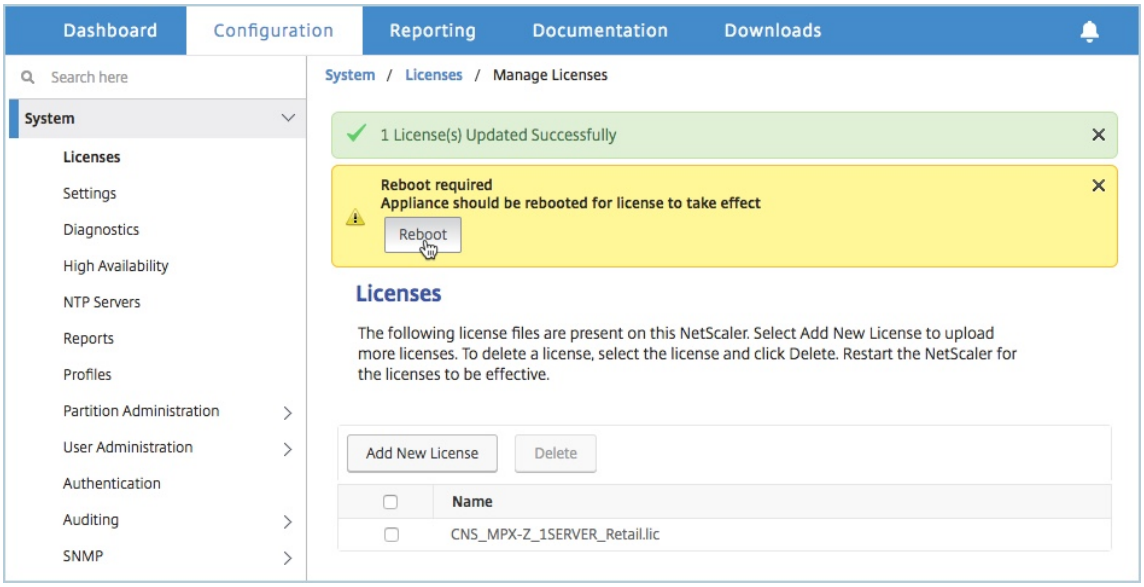
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.



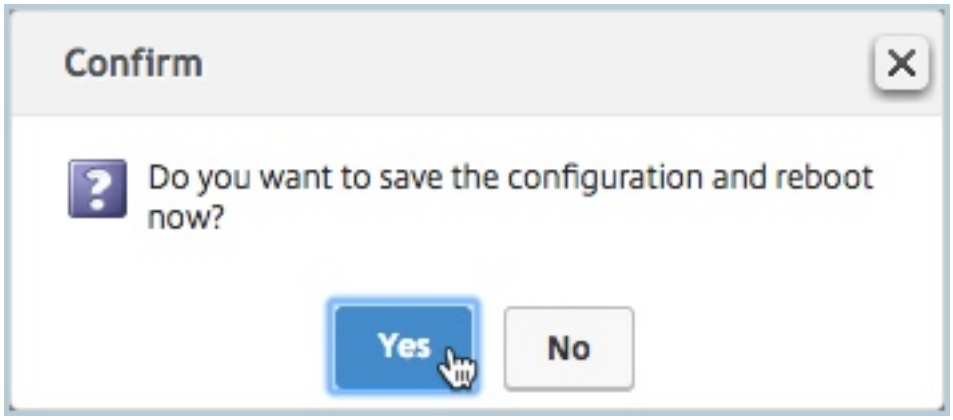
Once the license is uploaded you are prompted to reboot the appliance.

7. Click **Reboot** to reboot the appliance.



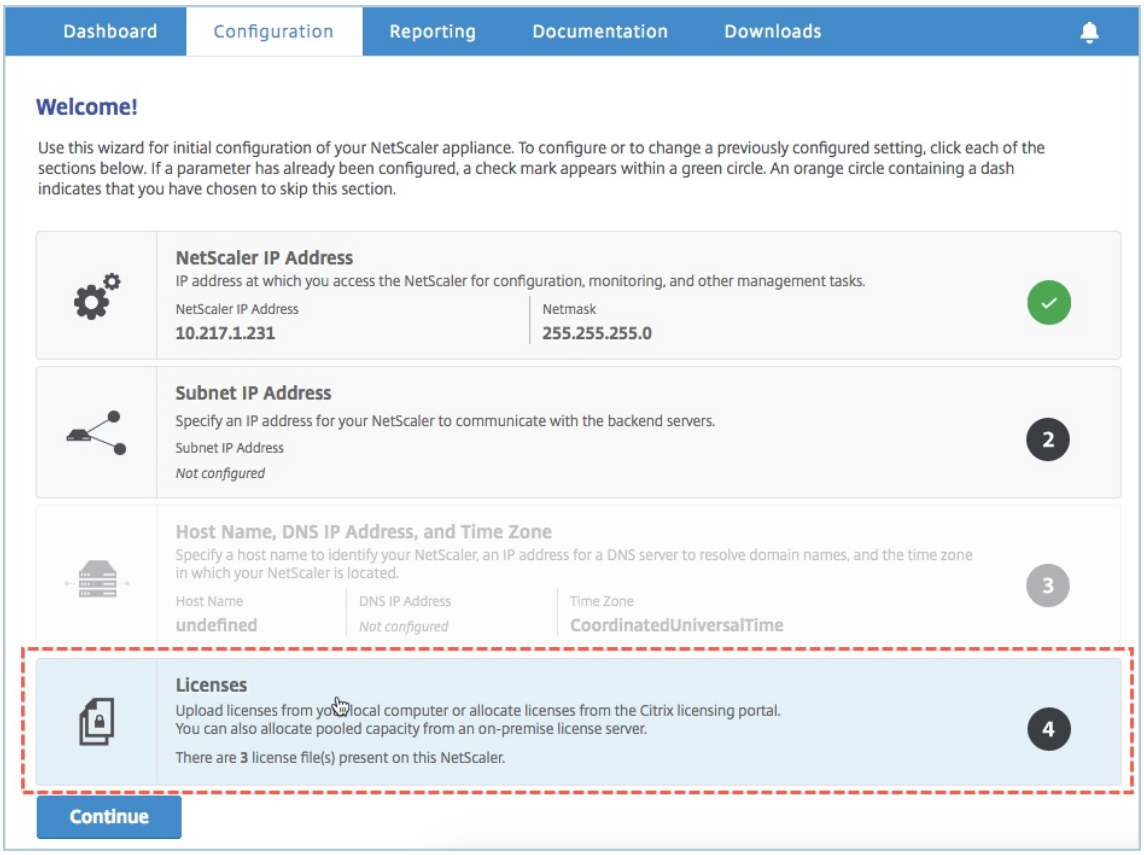
8. On the **Confirm** page, click **Yes**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



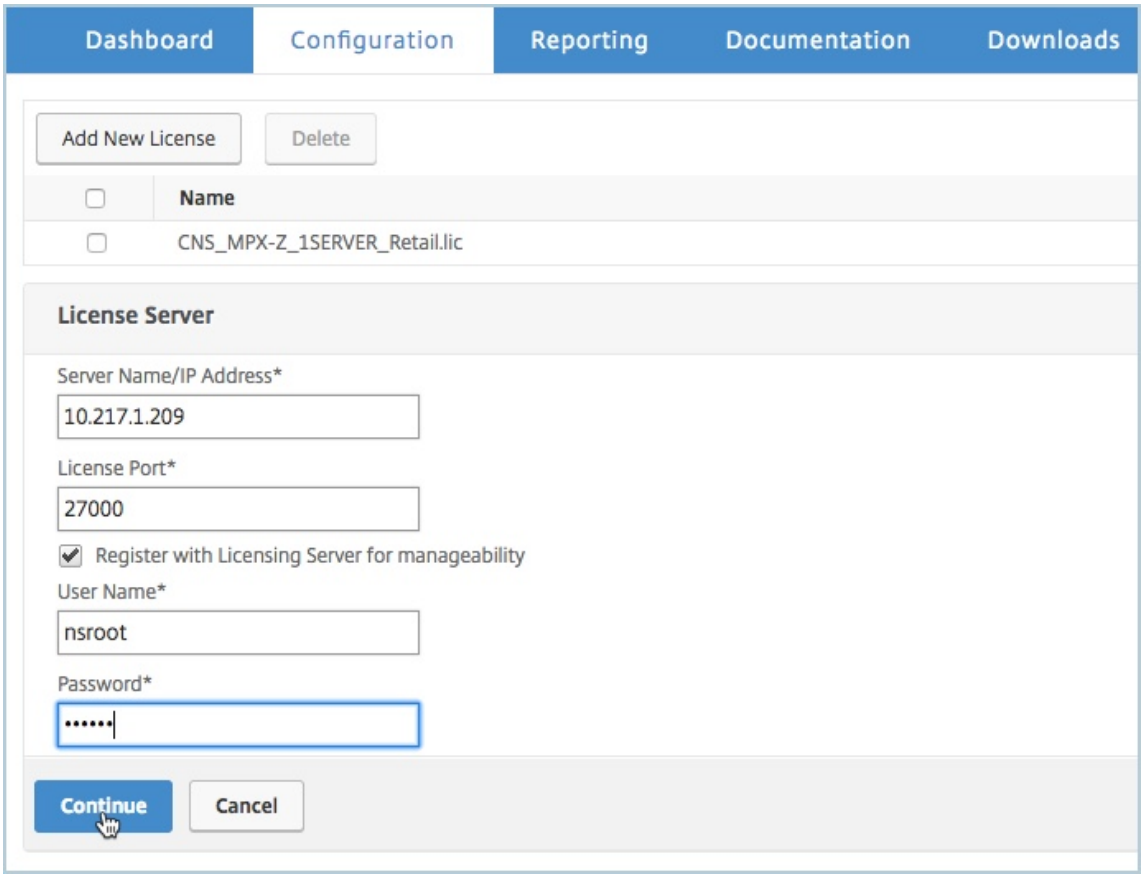
To upgrade an exisiting HA setup to NetScaler Pooled capacity:

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:

© 1997–2025 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.

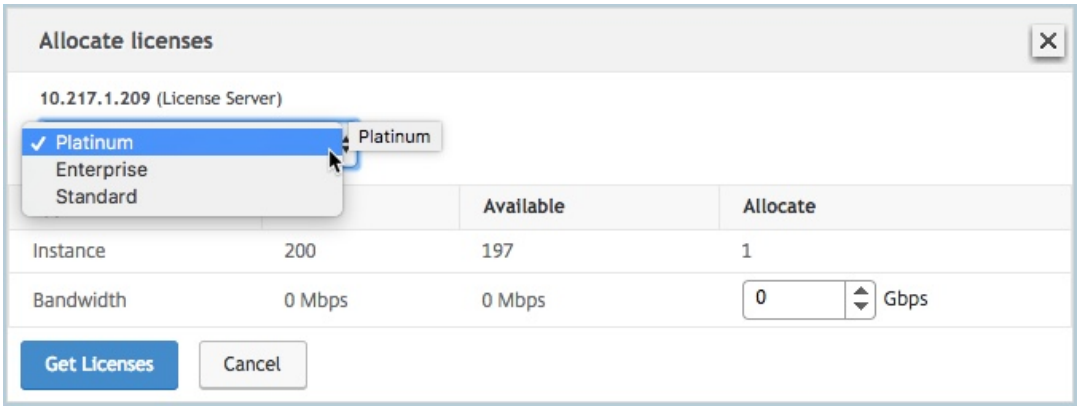
c) If you want to manage your instance's pool licenses through NetScaler Console, select the **Register with Licensing Server for manageability** checkbox and enter NetScaler Console credentials.

d) Click **Continue**.

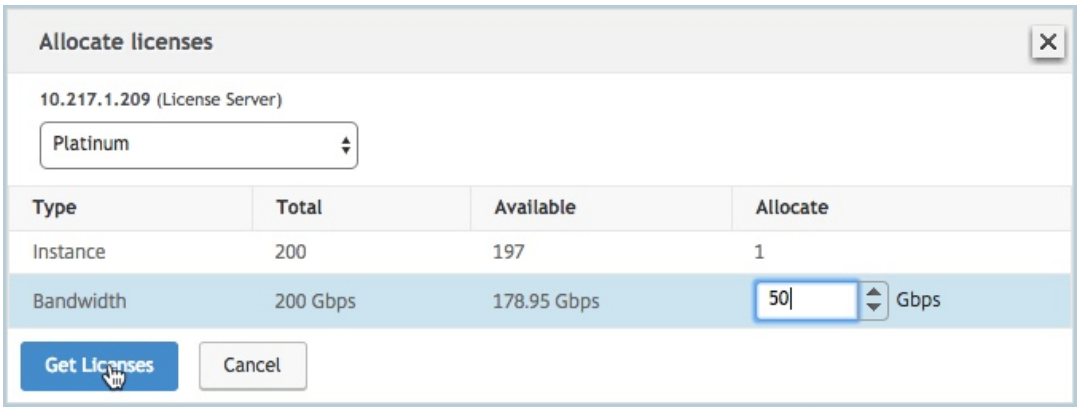
5. In the **Allocate licenses** window, do the following:

a) Select the license edition from the drop-down list.

© 1997–2025 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.

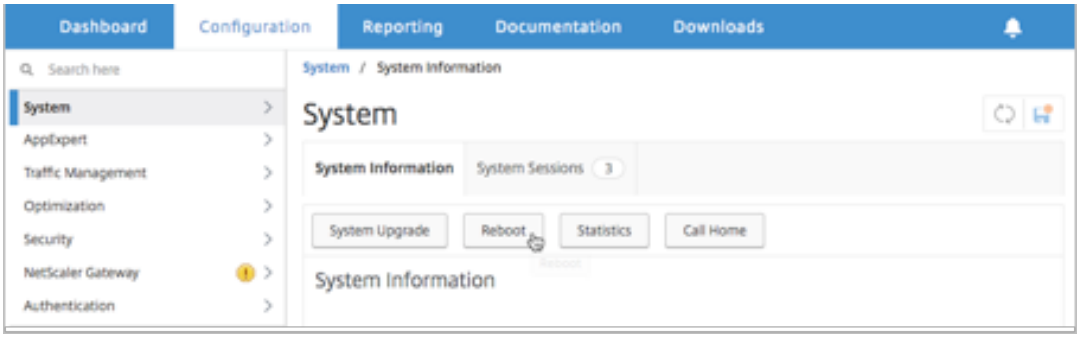
b) In **User Name** and **Password** fields, type the administrator credentials.

c) On the **Welcome** page, click **Continue**.

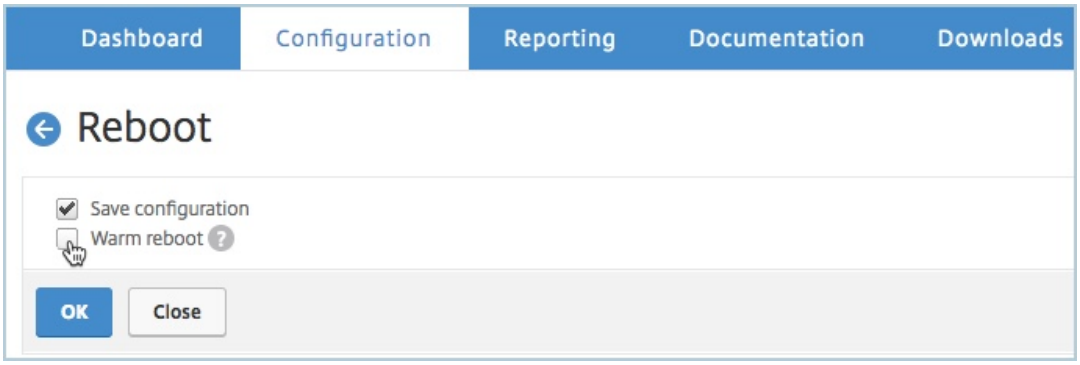
d) On the **Configuration** tab, click **System**.

e) On the **System** page, click **Reboot**.

© 1997–2025 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

September 8, 2025

> **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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 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.x (FIPS)
> - NetScaler SVM: 14.1 51.x, 13.1 60.x
> - NetScaler Console Service: will support LAS from early September.
>
> 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.

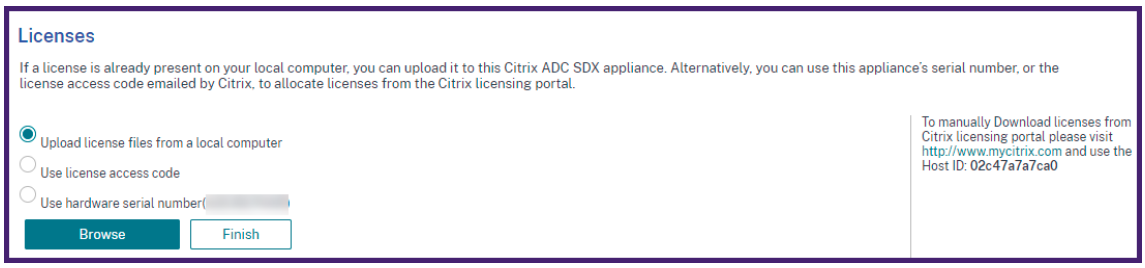
> **Note**
>
> For upgrading the SDX appliance to NetScaler Pooled capacity license, you must upload the SDX-Z license to the appliance.
>
> Ensure you have the permission to add NetScaler instances in NetScaler Console.

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**.

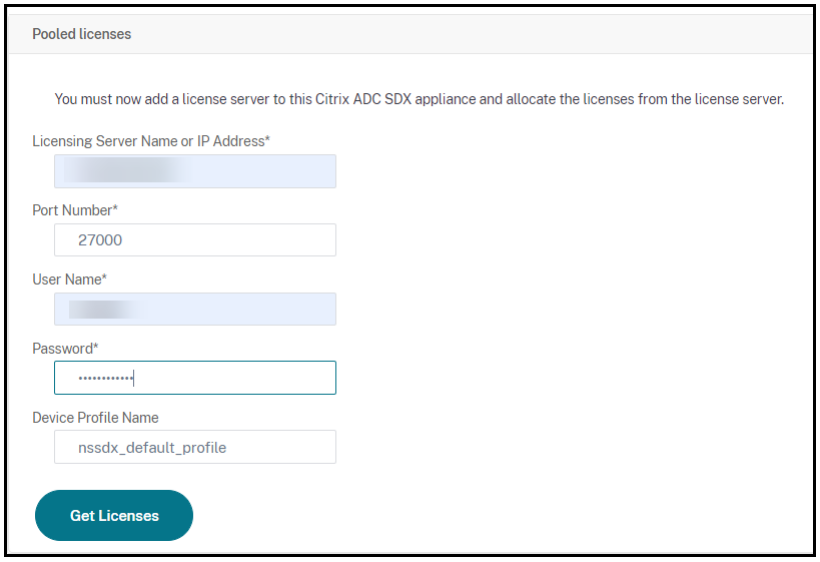
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:



   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.

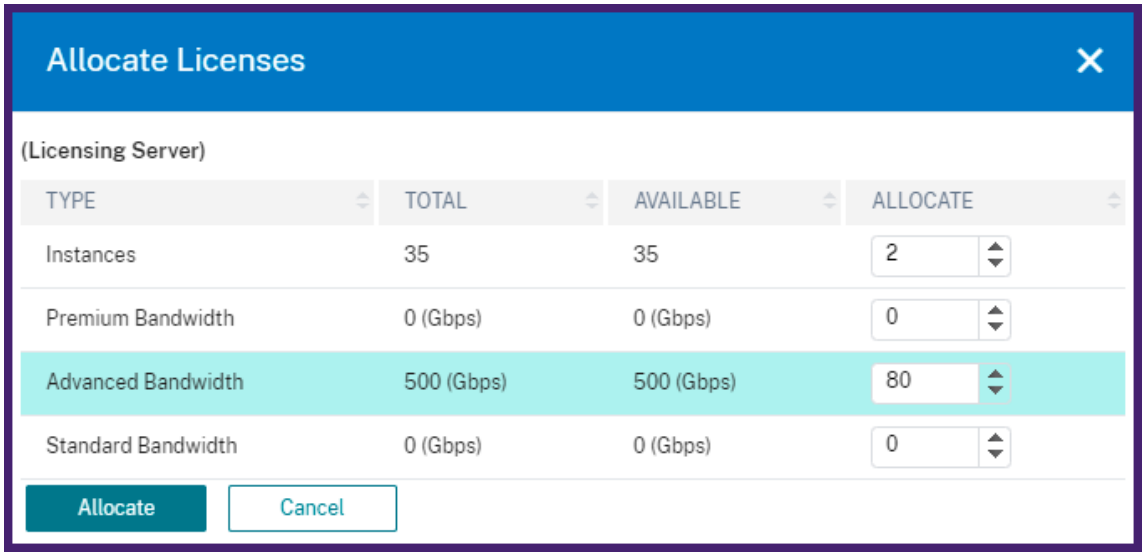
      If you are using an agent to communicate with the NetScaler Console server, specify the agent's IP address.

   b) In the **Port Number** field, enter the license server port. Default value: 27000.

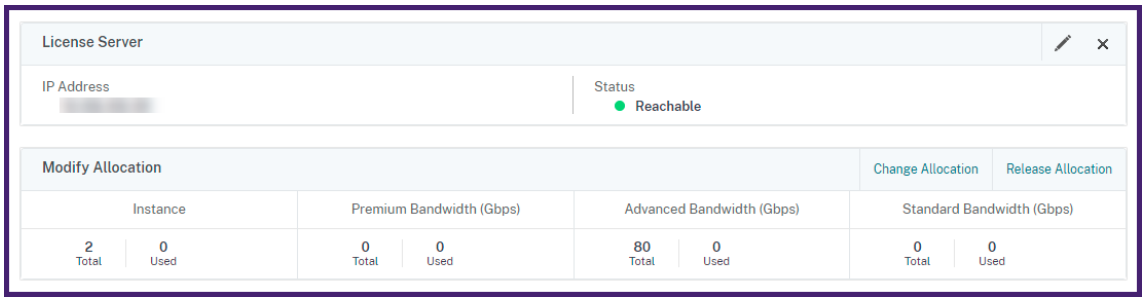
   c) Click **Get Licenses**.

8. In the **Allocate Licenses** window, specify the required instances and bandwidth and click **Allocate**.

© 1997–2025 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.

NetScaler VPX check-in and check-out licensing

September 8, 2025

> **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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 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.x (FIPS)
> - NetScaler SVM: 14.1 51.x, 13.1 60.x
> - NetScaler Console Service: will support LAS from early September.
>
> 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, 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**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 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.

   > **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
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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
```

4. To assign a license to a NetScaler VPX instance, enter the following command:

```
set capacity  –platform V\[S/E/P\]\[Bandwidth\]
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

NetScaler virtual CPU licensing

September 8, 2025

> **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.x (FIPS)
> - NetScaler SVM: 14.1 51.x, 13.1 60.x
> - NetScaler Console Service: will support LAS from early September.
>
> 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **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.

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

September 8, 2025

> **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.x (FIPS)
> - NetScaler SVM: 14.1 51.x, 13.1 60.x
> - NetScaler Console Service: will support LAS from early September.
>
> 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 main-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> tenance 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 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

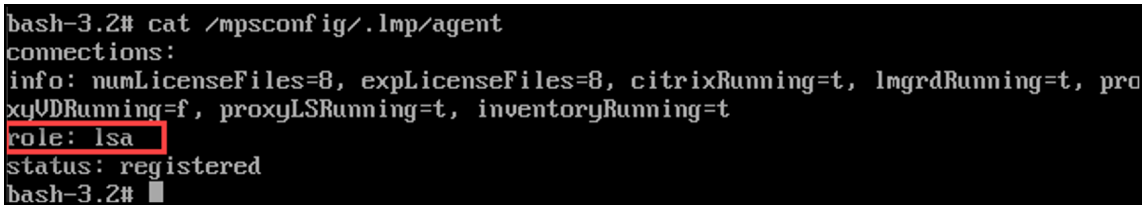
> **Note:**
>
> During this transition, NetScaler functionality is not impacted.

2. How can we determine which agent hosts the License Server role?

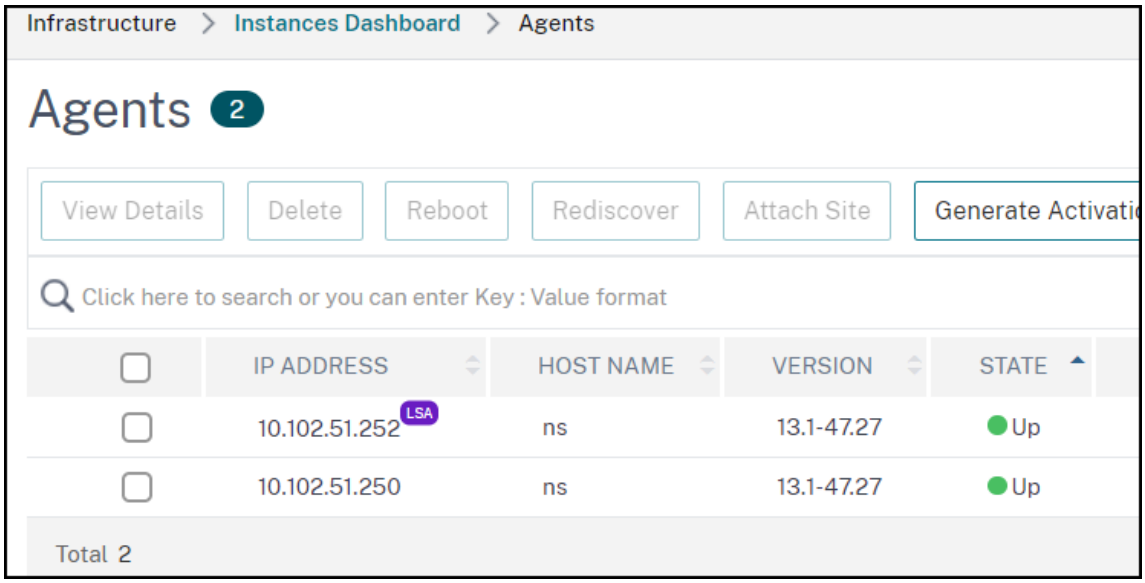
   Answer: To know which agent is hosting the LSA role, you can run the following command in the shell:

   ```
   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.

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

Troubleshoot Pooled capacity license issues

September 8, 2025

> **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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

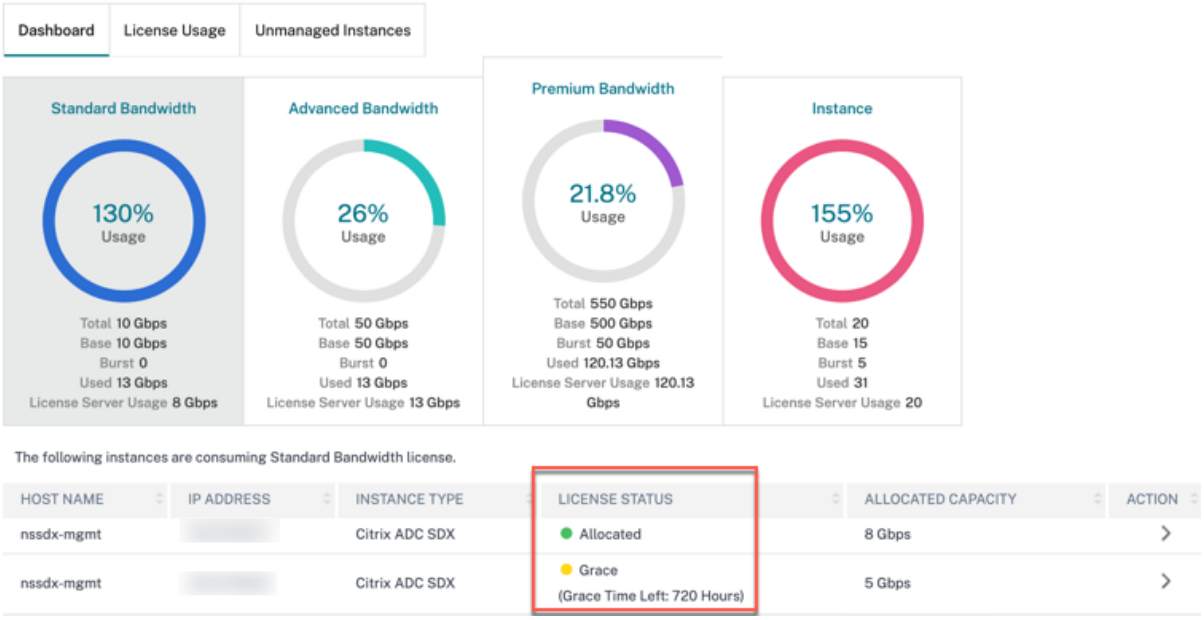
> licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.
>
> The minimum required NetScaler versions that are LAS compatible are:
>
> - NetScaler ADCs: 14.1 51.x, 13.1 60.x, 13.1 37.x (FIPS)
> - NetScaler SVM: 14.1 51.x, 13.1 60.x
> - NetScaler Console Service: will support LAS from early September.
>
> 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 scenario are applicable for manually managed entitlement (file-based licenses).

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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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 rebooted or NetScaler Console HAS failover is triggered.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Status	What it means
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.

- Connection to license server (NetScaler Console or agent) has severed for more than 15 minutes. Verify if the license server is up and reachable.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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.

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).

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

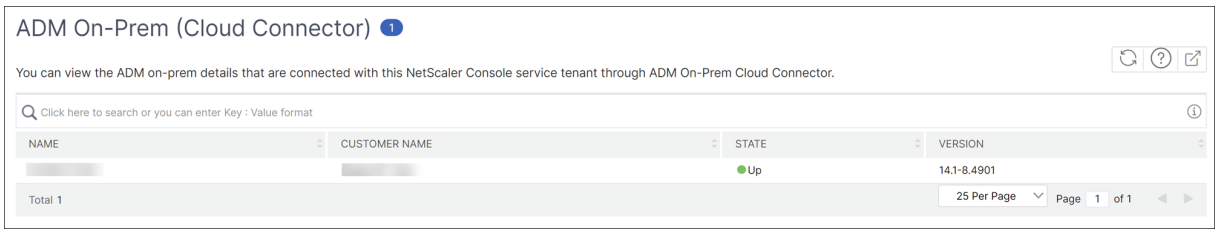
Parameter	Description
$source	This parameter corresponds to the source IP address of the received event.
$category	This parameter corresponds to the type of traps defined under the category of the filter.
$entity	This parameter corresponds to the entity instances or counters for which an event has been 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.

Console on-prem instances connected with Console service using Cloud Connect

January 15, 2025

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.



© 1997–2025 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

July 1, 2025

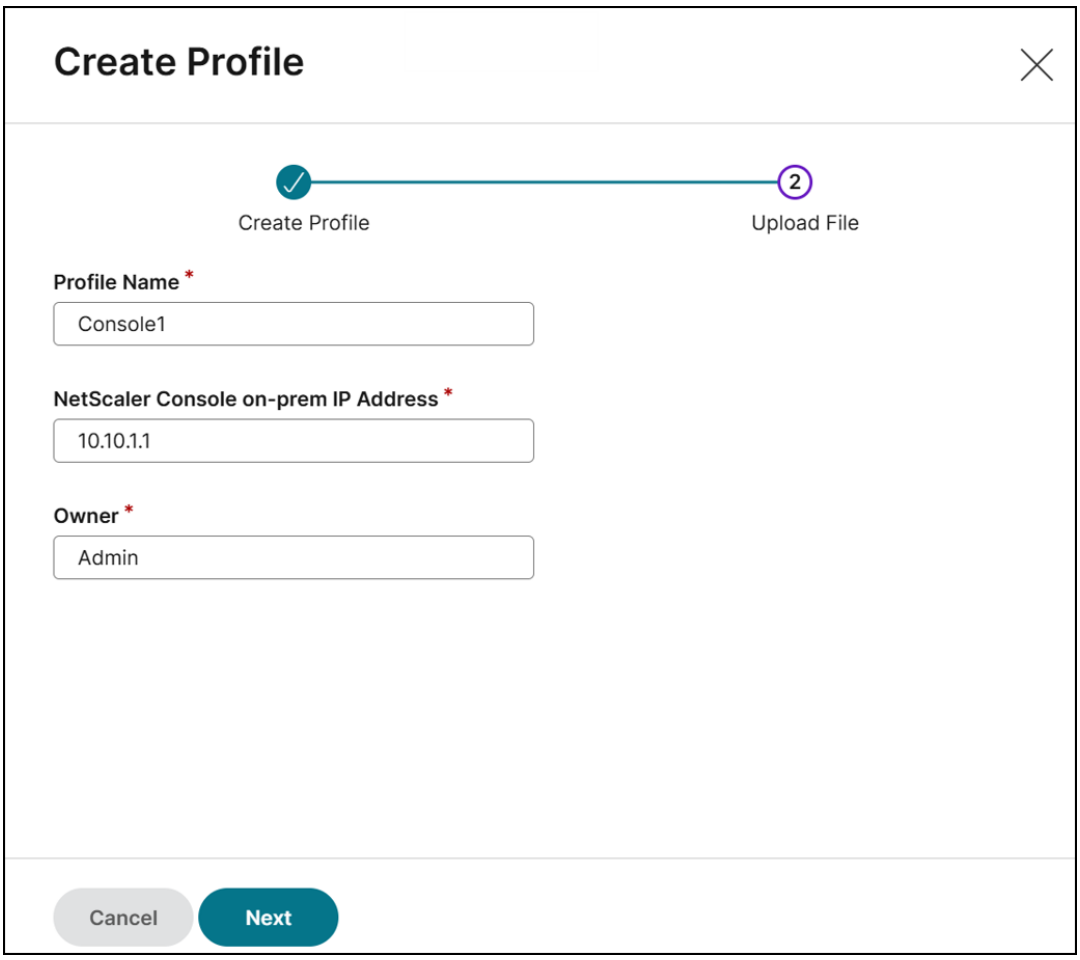
This page is applicable only for NetScaler on-prem users who opted the manual mode to upload their telemetry data to NetScaler Console service. Ensure that you have downloaded the telemetry data from your NetScaler Console on-prem (click **Download Telemetry** from the **NetScaler Telemetry** homepage 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.

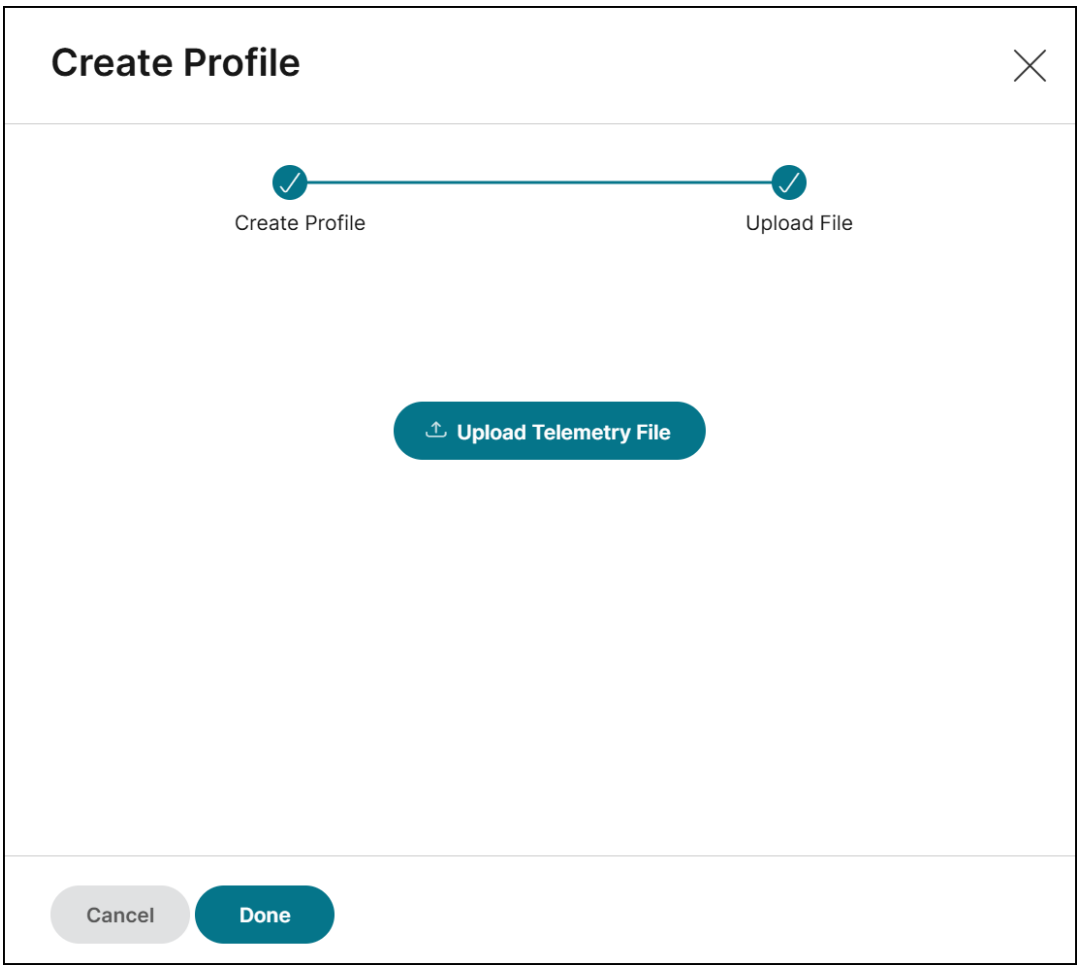
© 1997–2025 Citrix Systems, Inc. All rights reserved.



d) Click **Next**.

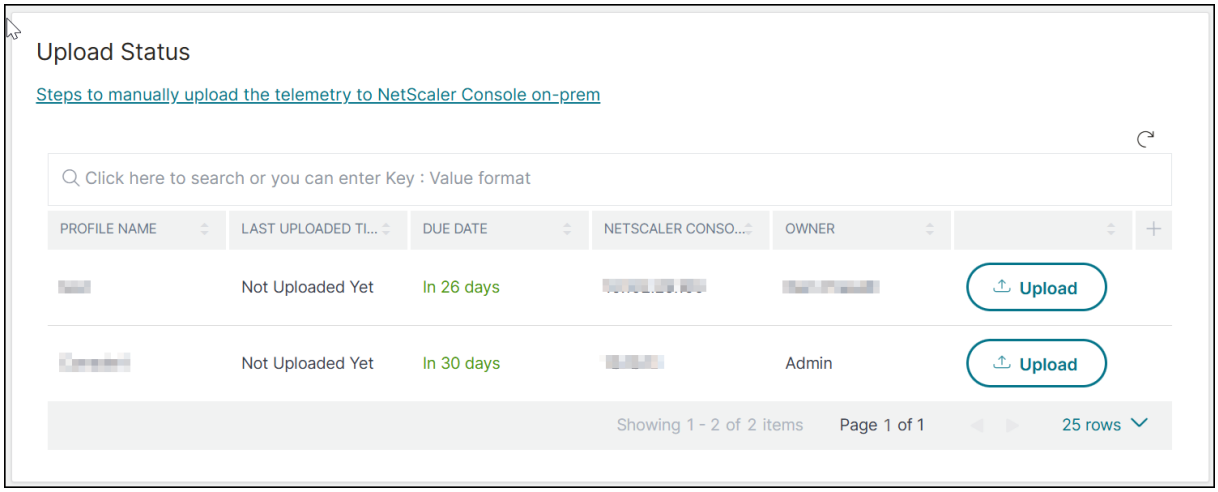
The profile name is created. You can either upload the telemetry file and click Done or upload it later.

© 1997–2025 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:



© 1997–2025 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.

Configure analytics on virtual servers

February 6, 2025

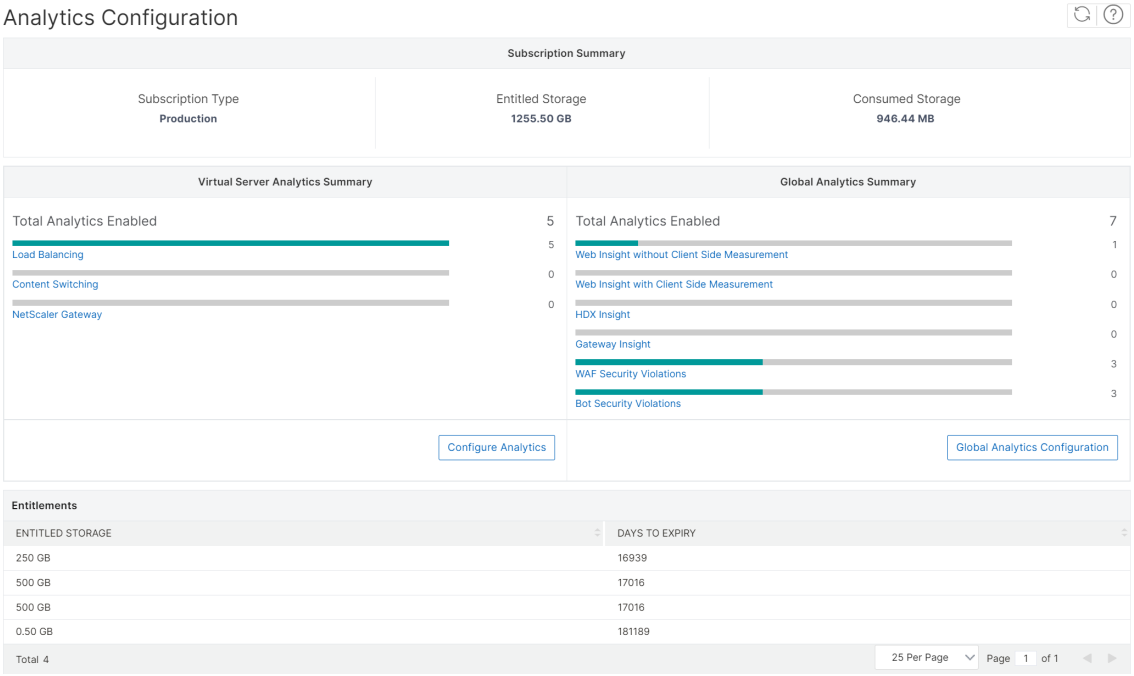
Starting from 14.1-21.x build, all the discovered virtual servers and the subsequent virtual servers are automatically licensed. You can proceed to configure analytics.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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
   - 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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.
     >
     > 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **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.

   > **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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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
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.

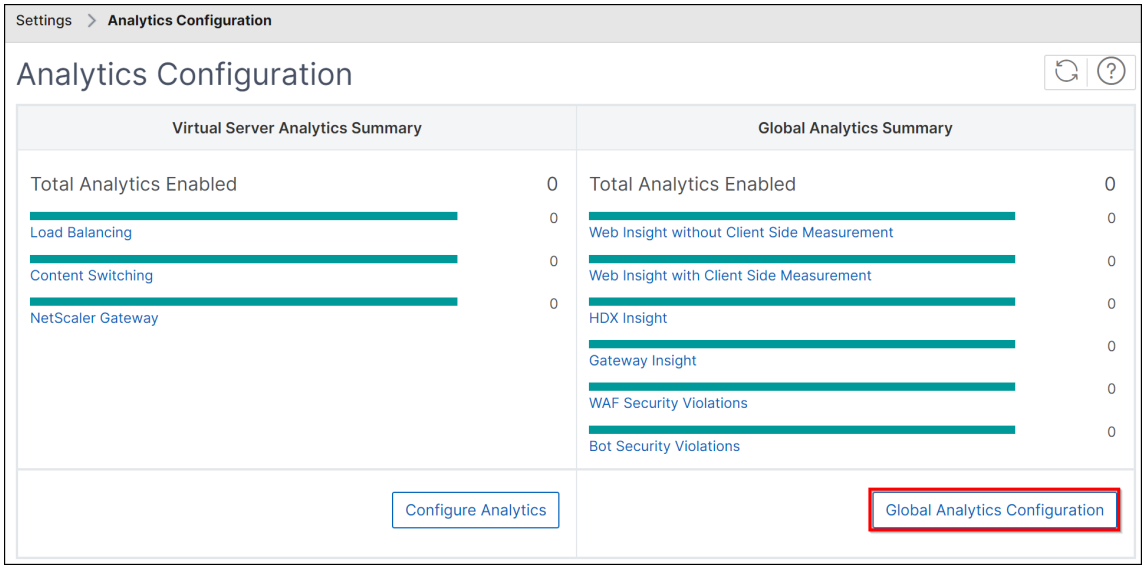
Custom policy

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:

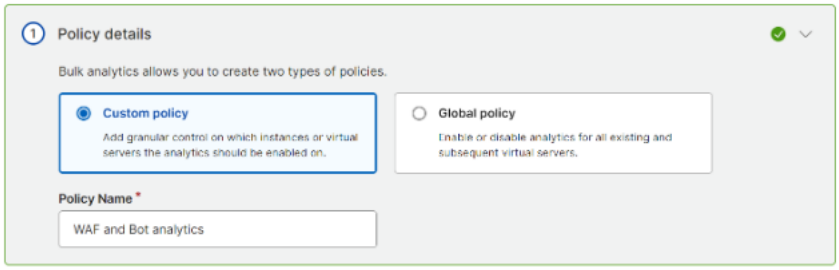
1. Under **Global Analytics Summary**, click **Global Analytics Configuration**.

© 1997–2025 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.



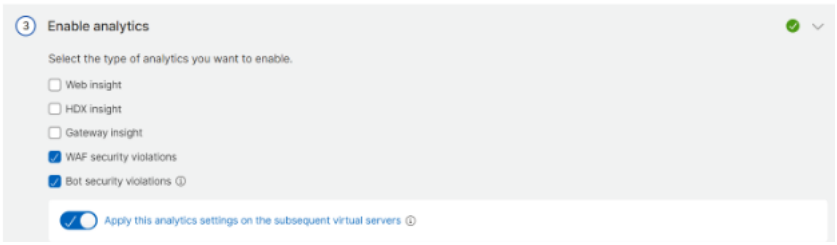
3. Under **Define Conditions**, create conditions by selecting the set of instance IPs or specific instances or virtual server name or both.



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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.

   > **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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

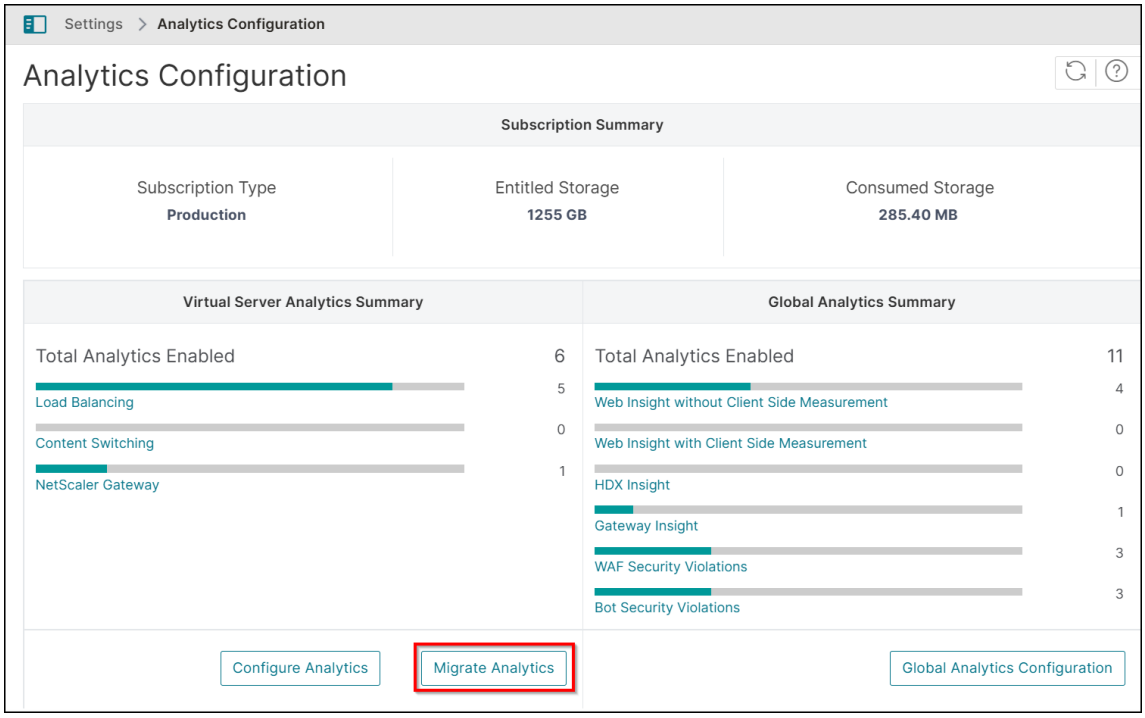
Starting from **14.1-40.x** build, when you enable analytics on virtual servers, the analytics are applied through profile-based configuration. Earlier, analytics was configured through an AppFlow policy. The profile-based configuration has the following benefits:

- Improved performance and flexibility
- Easier configuration and management

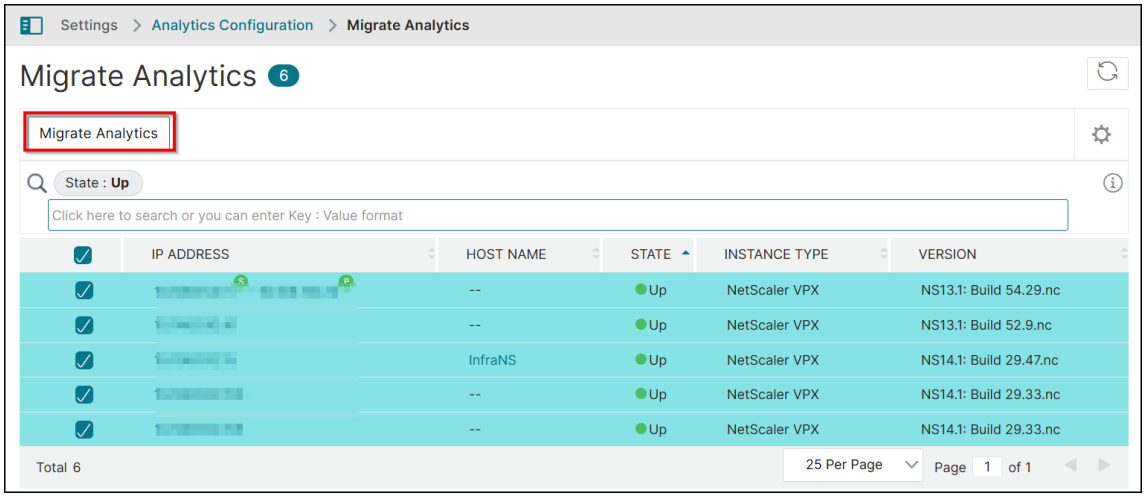
> **Note:**
>
> Enhancements related to analytics configurations are supported only through profile-based configuration. We recommend that you migrate all your existing virtual servers that are enabled for analytics to profile-based configuration.

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

© 1997–2025 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

January 16, 2024

NetScaler Console provides fine-grained, role-based access control (RBAC) with which you can grant

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 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:

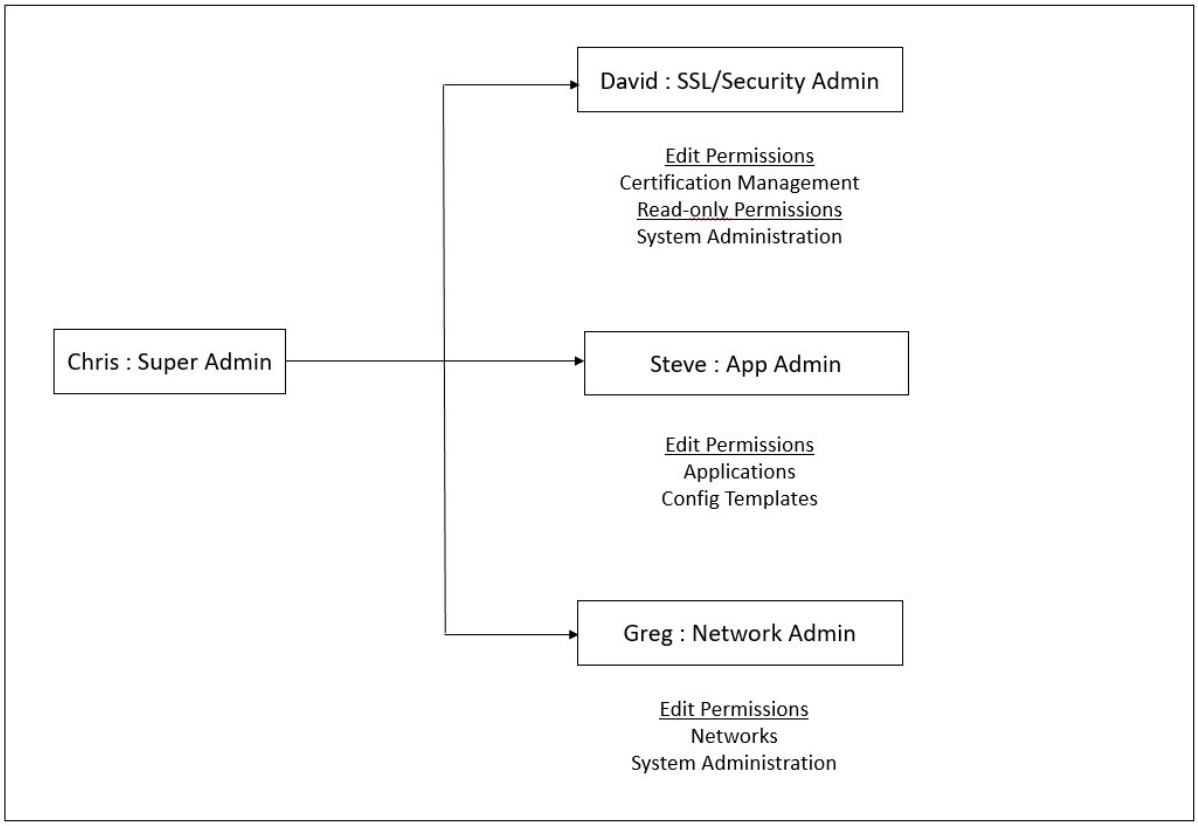
The following example illustrates how RBAC can be achieved in NetScaler Console.

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.

© 1997–2025 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.

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

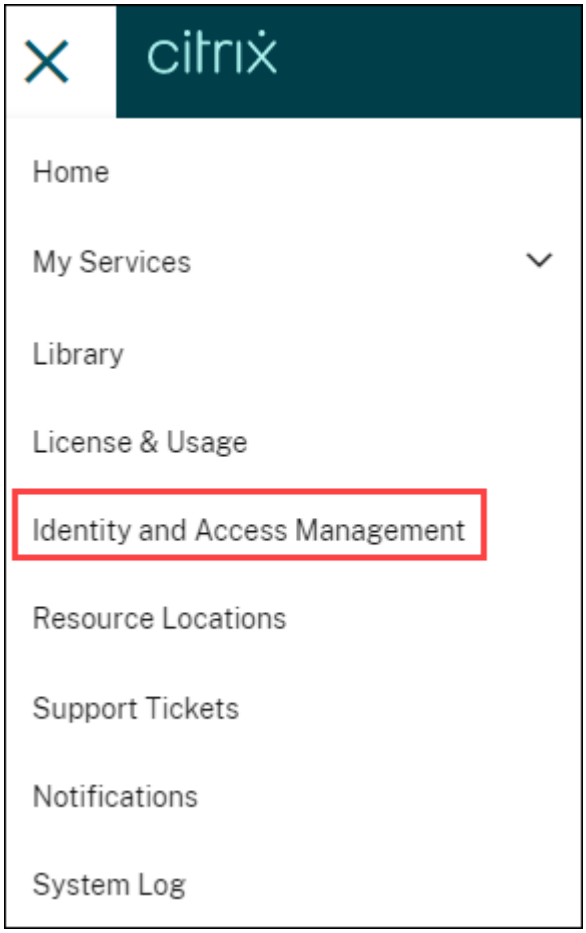
Therefore, in your role as Chris, the super admin, perform the following example tasks in NetScaler Console to configure access policies, roles, and user groups for David who is the security admin in your organization.

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**.



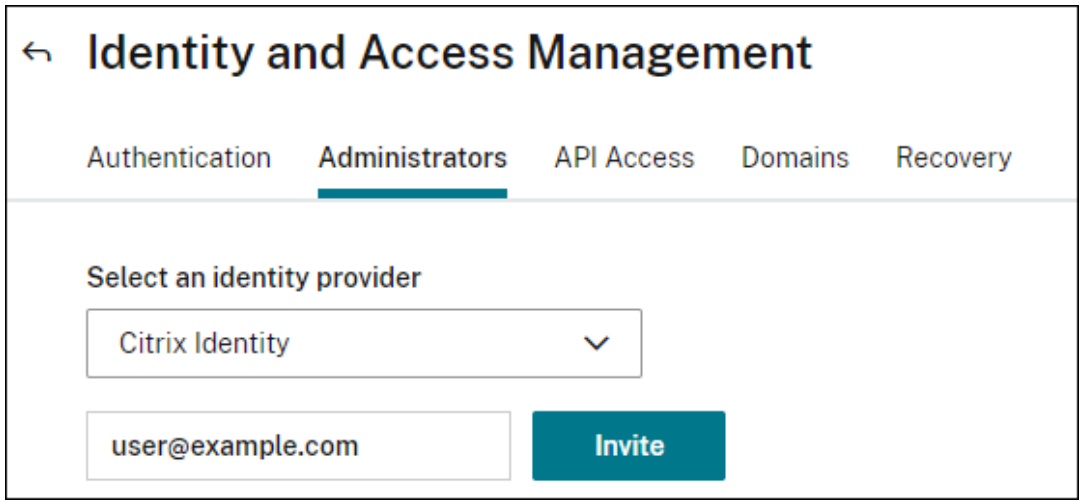
2. On the Identity and Access Management page, select the **Administrators** tab.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

This tab lists the users that are created in Citrix Cloud.

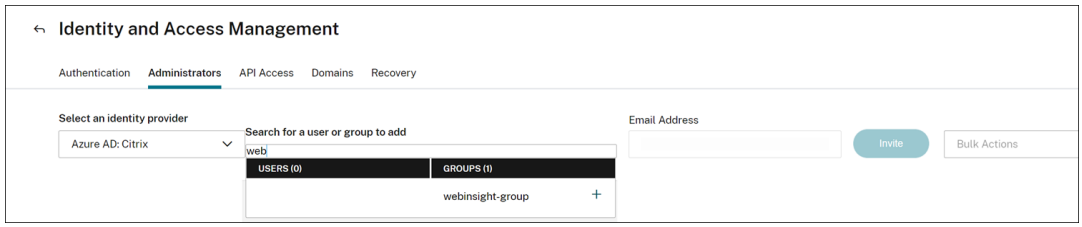
3. Select the identity provider from the list.

   - **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.

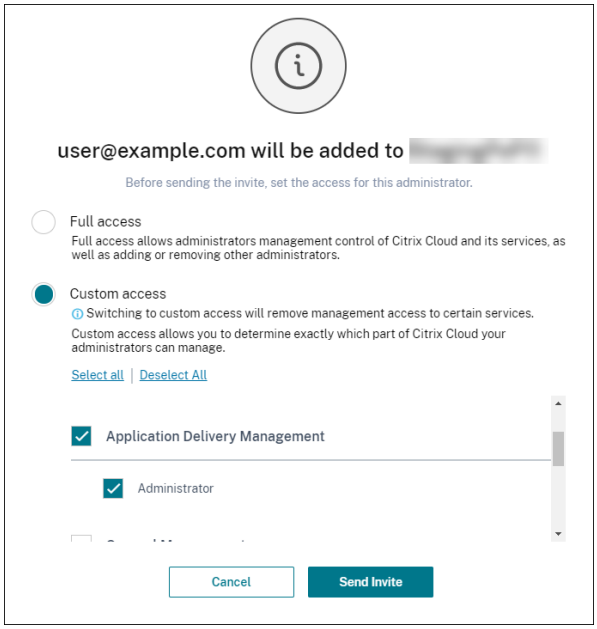
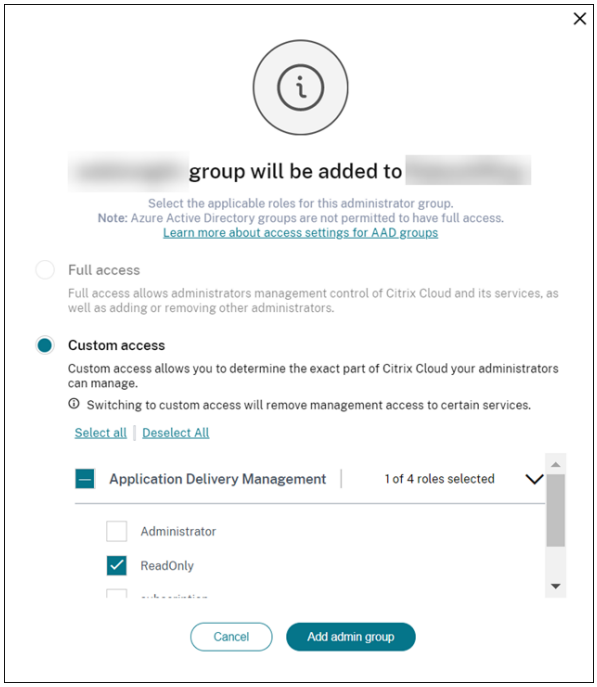
   - **Azure Active Directory (AD)**: This option appears only if your Azure AD is connected to Citrix Cloud, see Connect Azure Active Directory to Citrix Cloud. When you select this option to invite users or groups, you can specify only **Custom Access** for the selected user or group. The users can log 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.
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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Citrix Identity	Azure AD
	
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.
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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.
   - **Edit:** This option grants the full access to the user. The user can modify the feature and its functions.

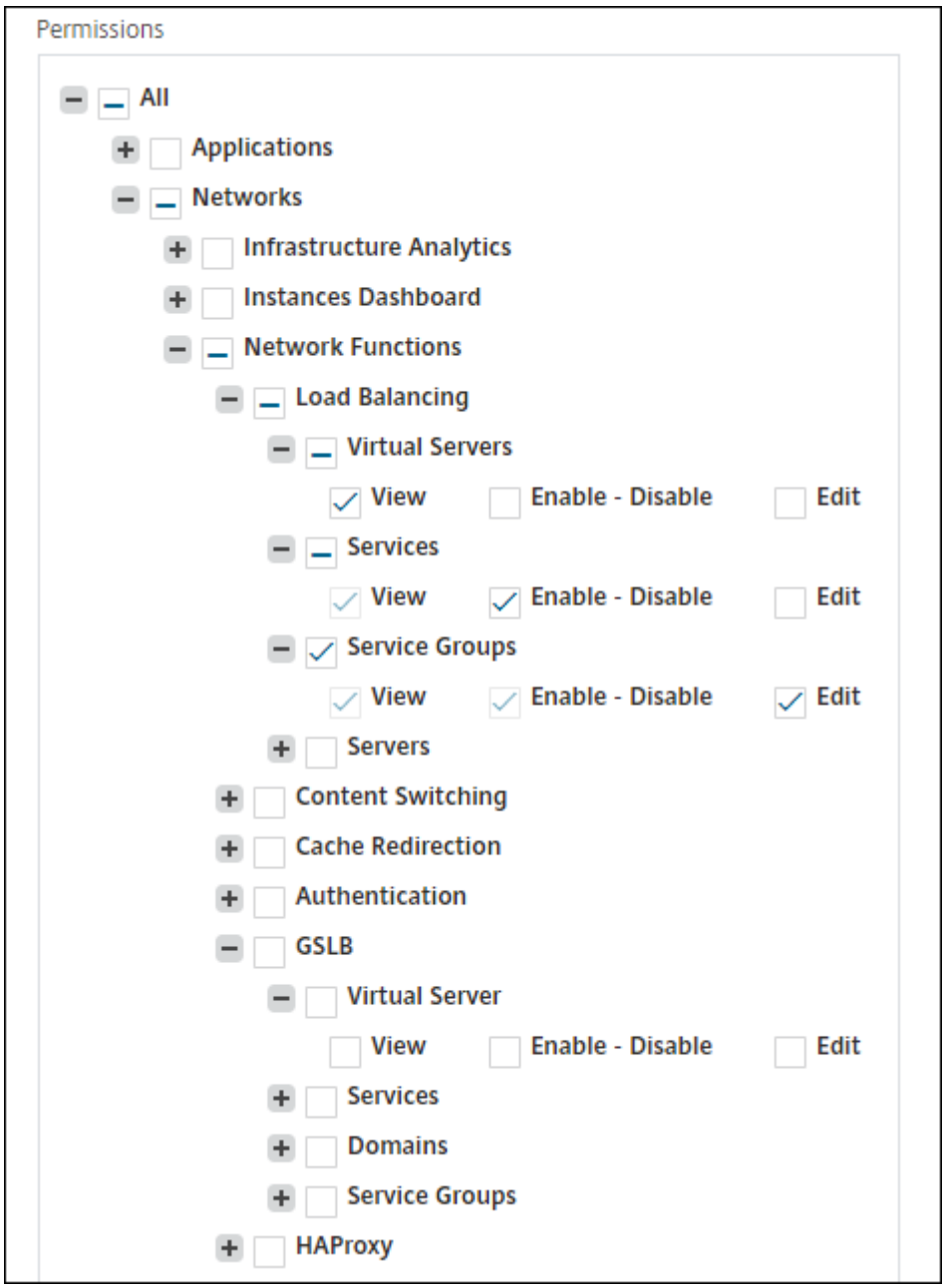
     If you grant the **Edit** permission, both **View** and **Enable-Disable** permissions are granted. You cannot deselect the auto-selected options.

   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:

© 1997–2025 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.

© 1997–2025 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.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.)

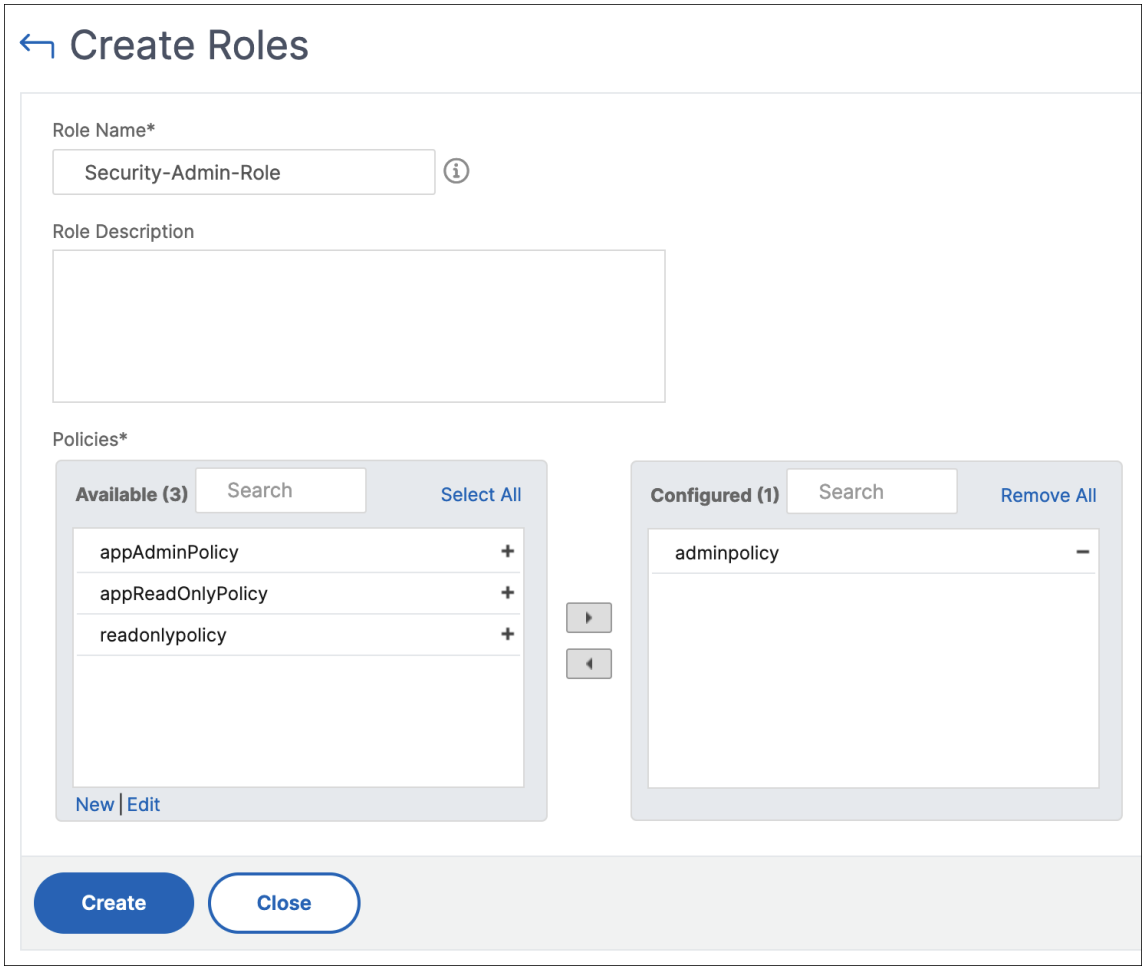
Though you cannot edit the predefined roles, you can create your own (user-defined) roles.

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.

   > **Note:**
   >
   > The policies are pre-fixed with a tenant ID (for example, `maasdocfour`) that is unique to all tenants.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



> **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**.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.

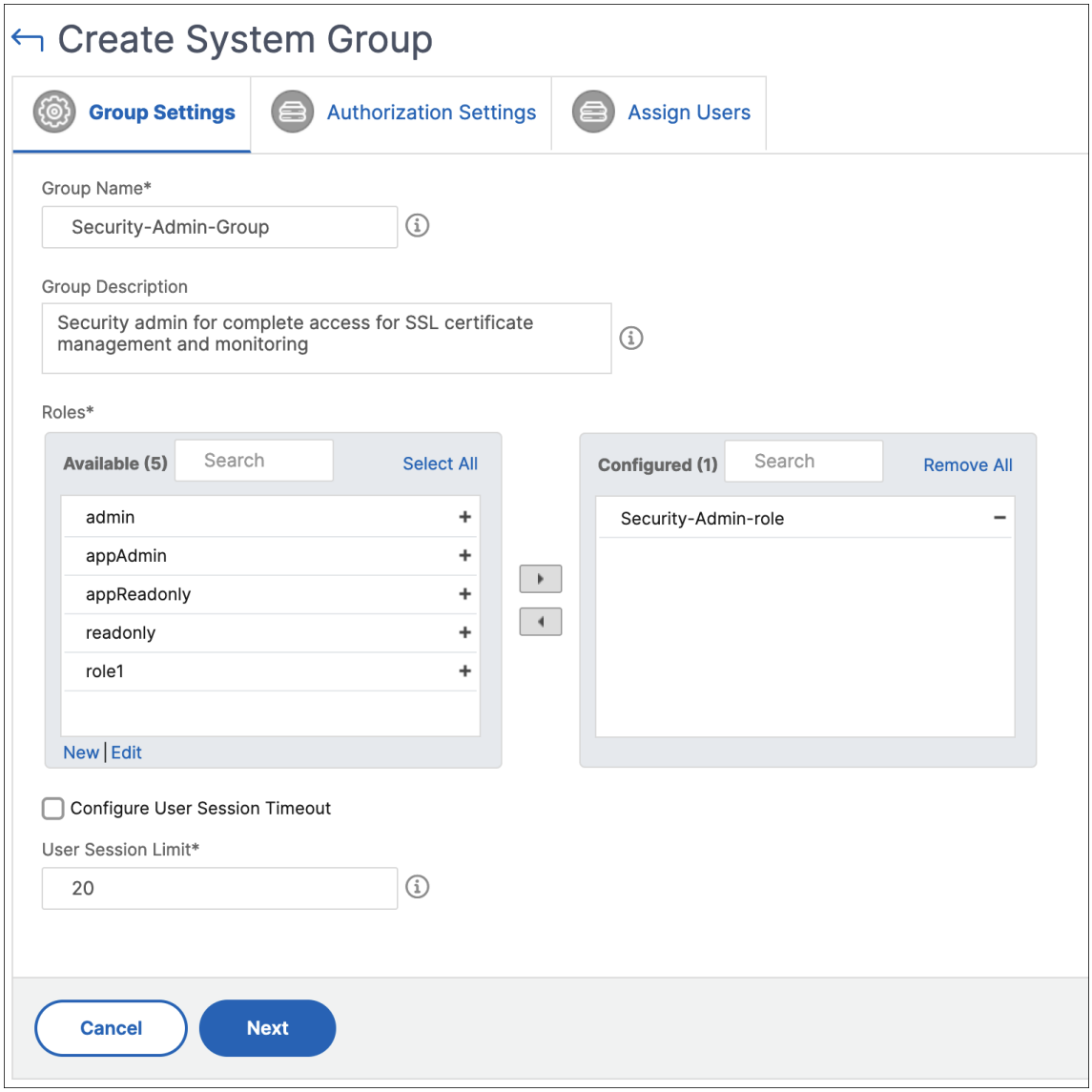
   The **Create System Group** page is displayed.
3. In the **Group Name** field, enter the name of the group.
4. In the **Group Description** field, type in a description of your group. Providing a good description helps you to understand the role and function of the group.
5. In the **Roles** section, 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.

   Alternatively, you can navigate to **Settings > Users & Roles > Users**, and create or modify users.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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**
   - **Config Packs**
   - **Domain Names**

   Select specific resources from the categories to which users can have access.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.

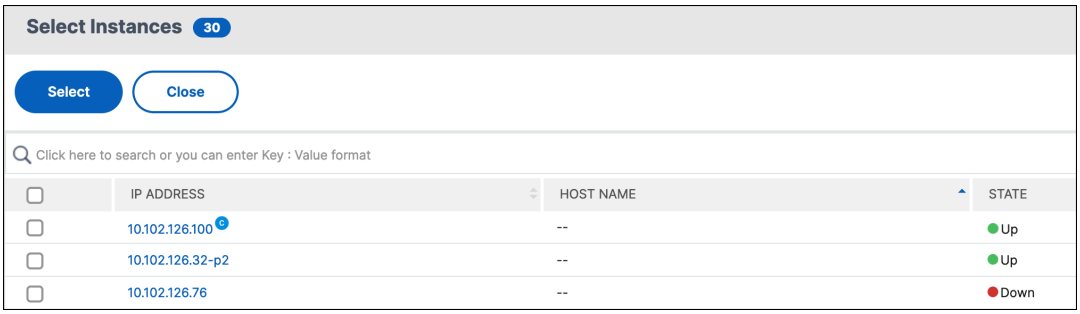
b) Select the required Autoscale groups from the list and click **OK**.

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**.

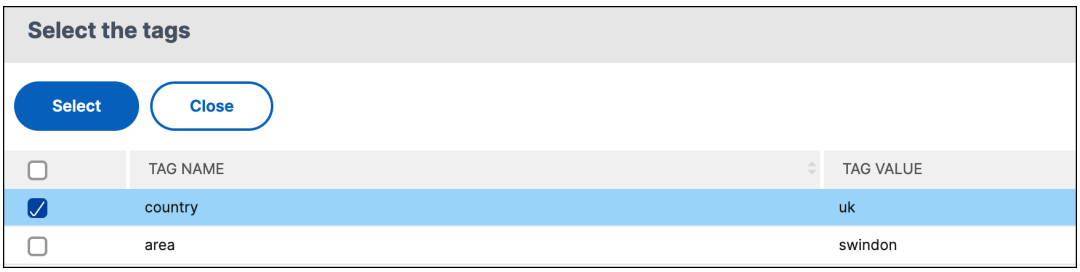


Tags:

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.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

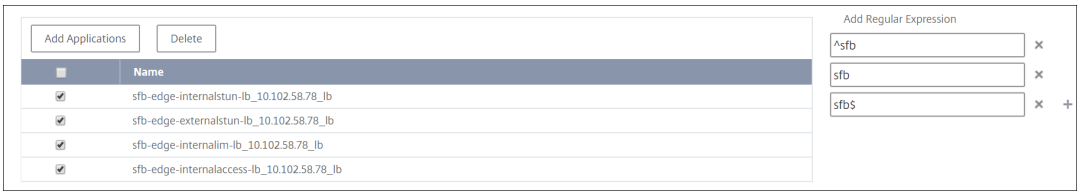
  > **Note:**
  >
  > Ensure you have selected only one entity type if you want to authorize bound entities.

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**.

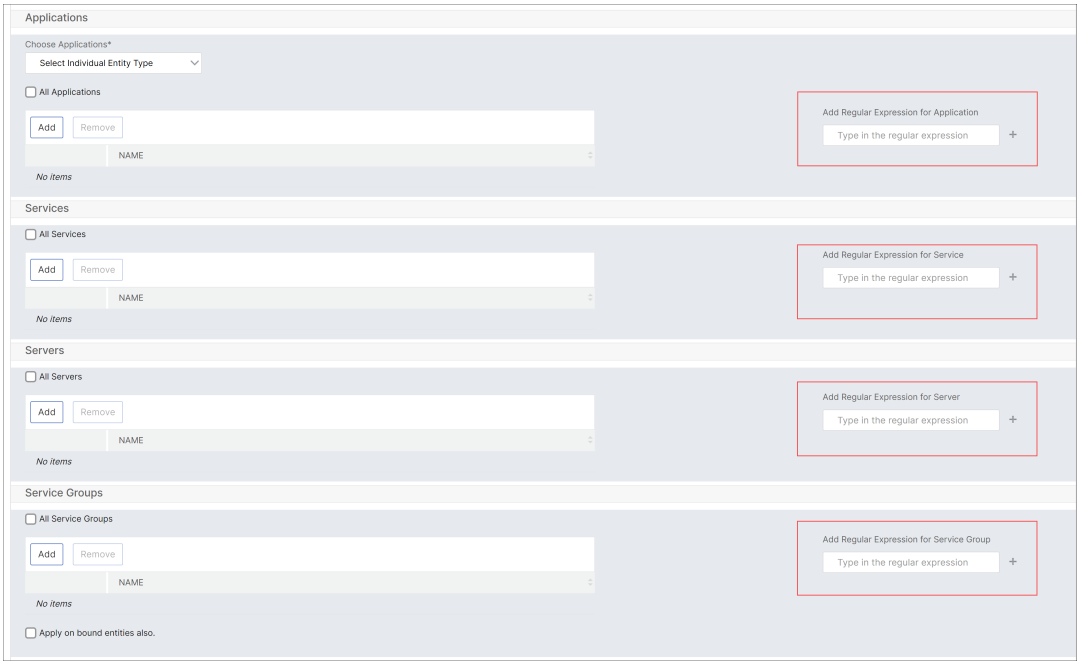
b) Specify the regular expression in the text box.

The following image explains how to use a regular expression to add an application when you select the **Specific Applications** option:



© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

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.

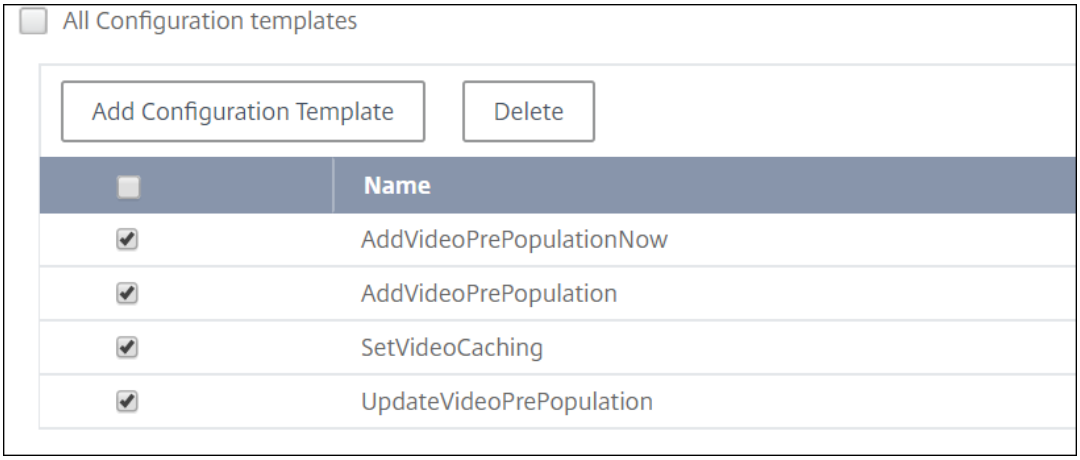
Configuration Templates:

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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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:

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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

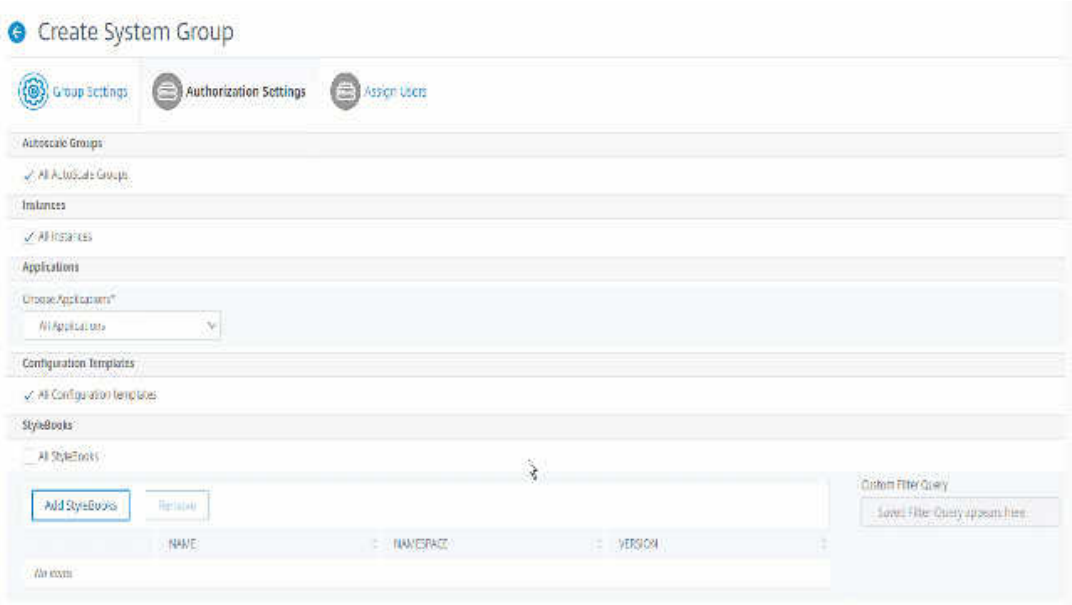
- StyleBook name is either `lb-mon` or `lb`.
- StyleBook namespace is `com.citrix.adc.stylebooks`.
- StyleBook version is `1.0`.

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**.



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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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:

If you want to select the specific domain name that a user can view or manage, perform the following steps:

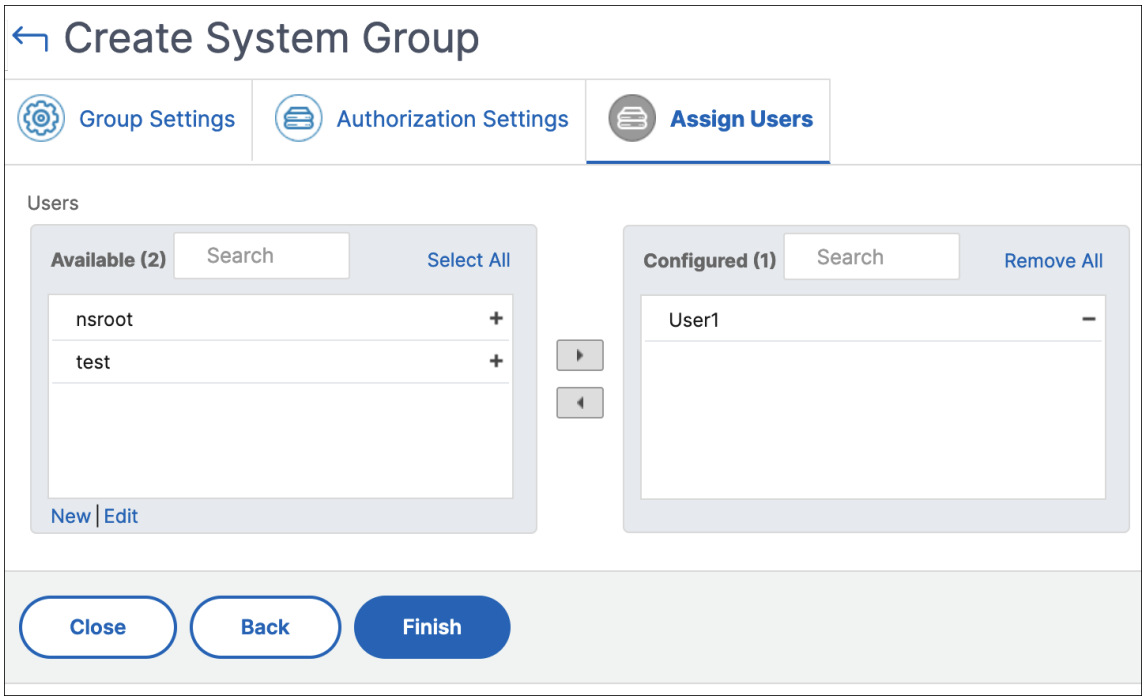
a) Clear the **All Domain Names** checkbox and click **Add Domain Name**.

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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

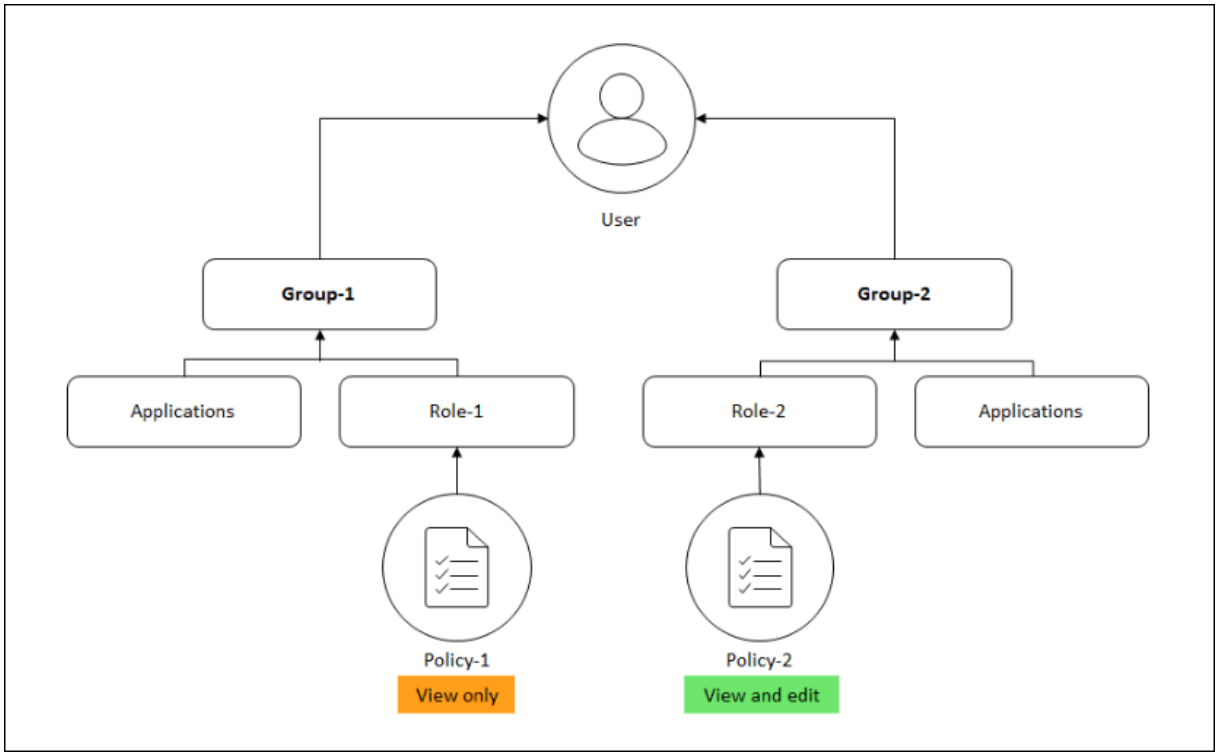
How user access changes based on the authorization scope

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.

- **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - 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.
  - 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

June 12, 2024

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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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**.

> **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

November 19, 2024

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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

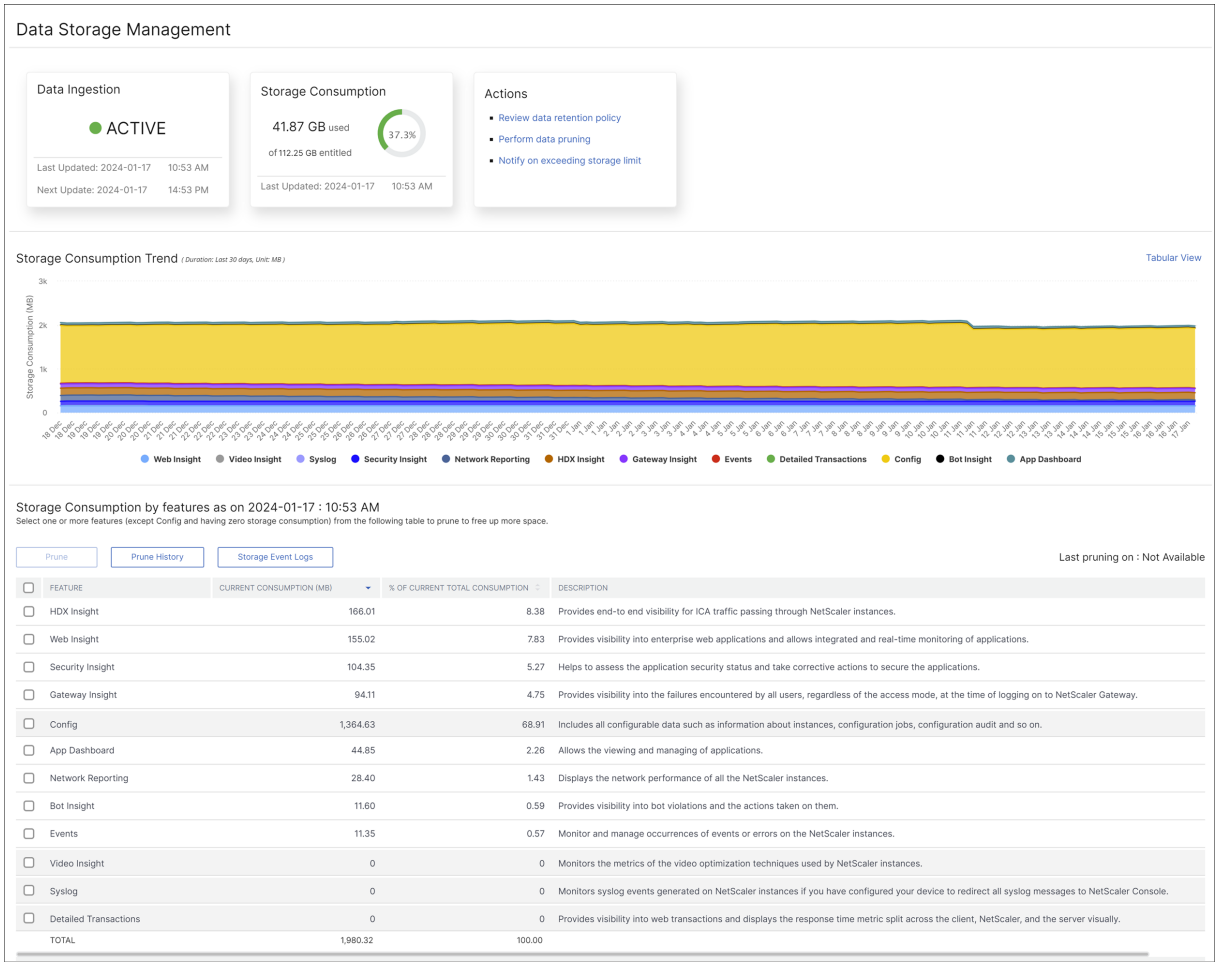
- Understand your data storage - This section helps you understand how you can use the dashboard to view information about your data storage.
- Manage your data storage - This section provides information on what actions you can take in the dashboard to manage your data storage.

Understand your data storage

November 19, 2024

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Total storage consumption
- Data Pruning status
- Storage consumption trends
- Storage consumption by features

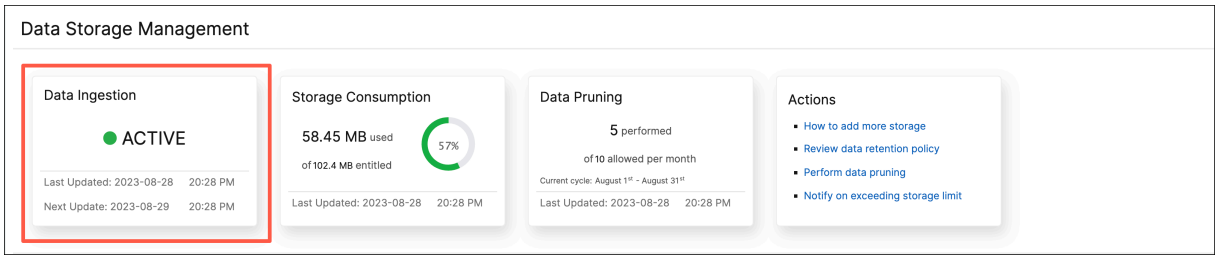
State of your data ingestion activity

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.

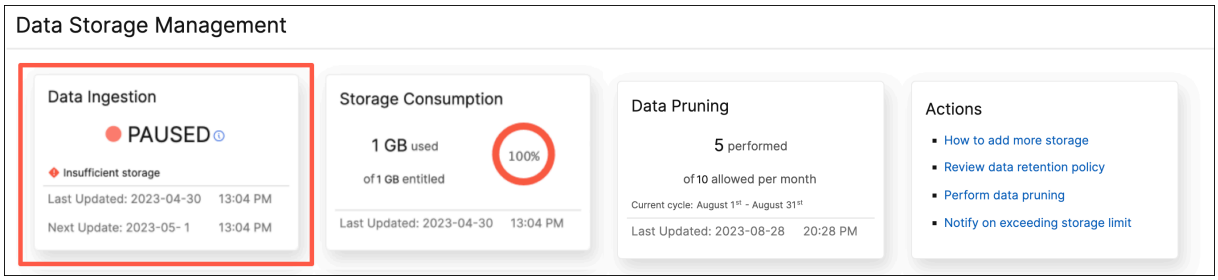
The data ingestion status indicates whether NetScaler Console is collecting statistics from NetScaler instances. The data ingestion activity continues as long as the consumed storage is within the entitled storage. When the consumption is more the entitled storage, the data ingestion is paused.

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

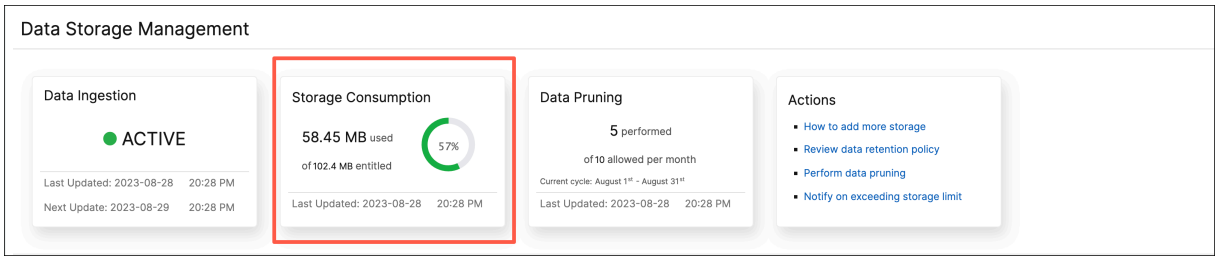
To resume your data ingestion activity, you can do either of the following actions:

- Add more data storage.
- Perform data pruning.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Total storage consumption

For a quick overview of your data storage, view the **Storage Consumption** tile.



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

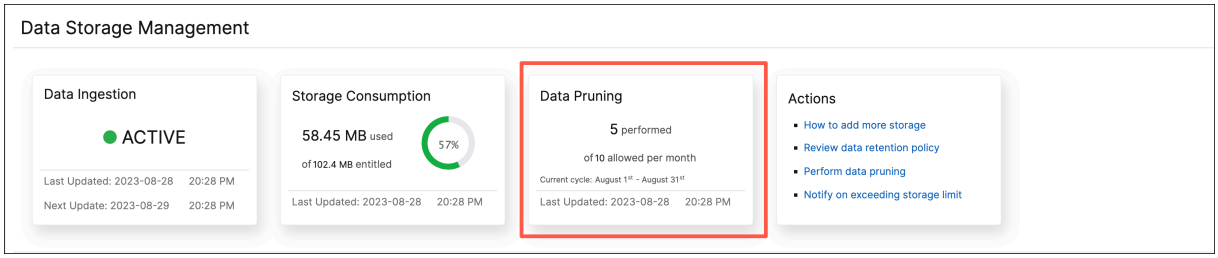
The consumed storage is the total storage used by all the features in the deployment. The following color coding criteria specify the amount of storage used by the features:

- **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.

© 1997–2025 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.

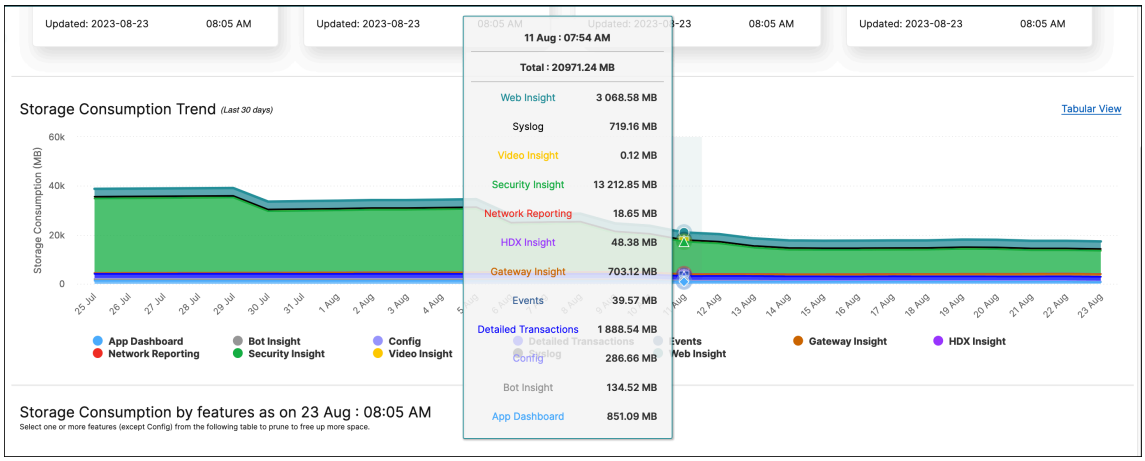
Storage consumption trends

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.



> **Note:**
>
> The **Graphical View** is the default view.

- **Tabular View** –Click **Tabular View** to display the data storage information in a table form.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



> **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.
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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

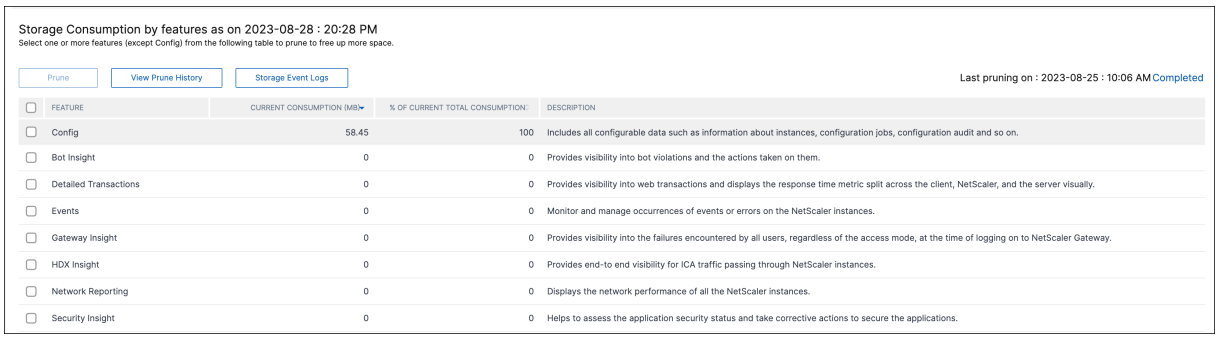
FEATURE	DESCRIPTION
App Dashboard	Allows the viewing and managing of applications.
Bot Insight	Provides visibility into bot violations and the actions taken on them.
Syslog	Monitors syslog events generated on NetScaler instances if you have configured your device to redirect all syslog messages to NetScaler 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
- 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.

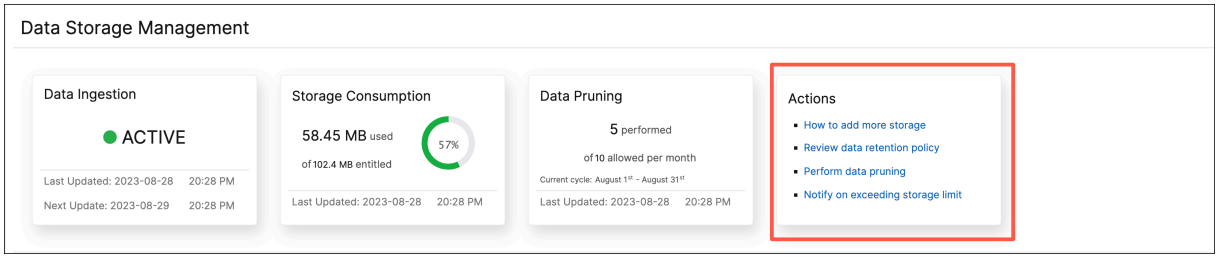
For information on pruning your data, prune history, and Storage Event logs, see Manage your data storage.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Manage your storage space

March 7, 2025

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.

Perform data pruning

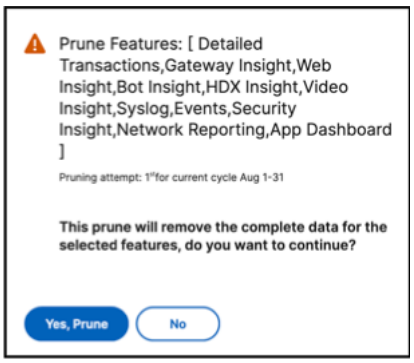
Prune your data to optimize storage resources and get more storage space. In addition to freeing up space, data pruning enhances data quality and accelerates processing times. We recommend you review and purge unnecessary data at regular intervals. This process makes sure that your resources are used 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**.

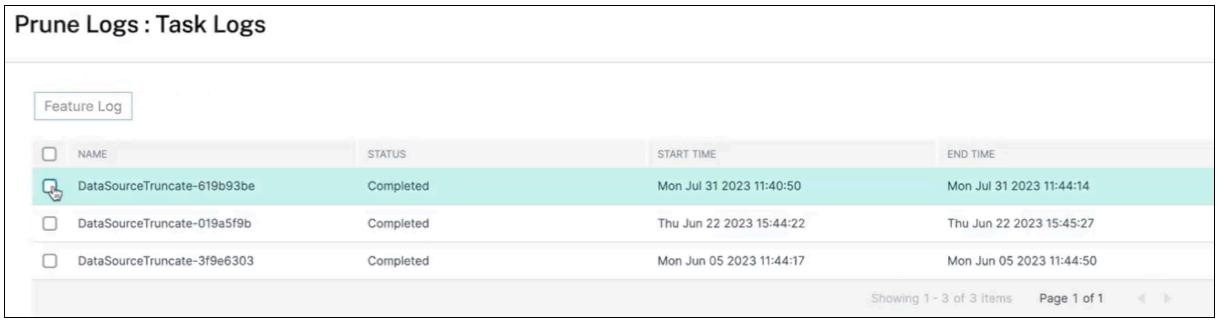
© 1997–2025 Citrix Systems, Inc. All rights reserved.



> **Note:**
>
> The pop-up window also displays information about your current pruning attempt.

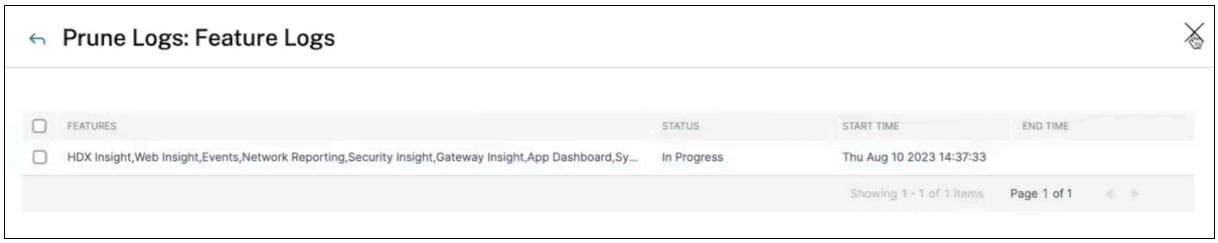
View prune history

Click **View Prune History** to get details on the all the prune activities that you did in NetScaler Console.



The **Prune Logs: Task Logs** page displays the list of all the prune tasks, including their respective statuses, start time, and end time.

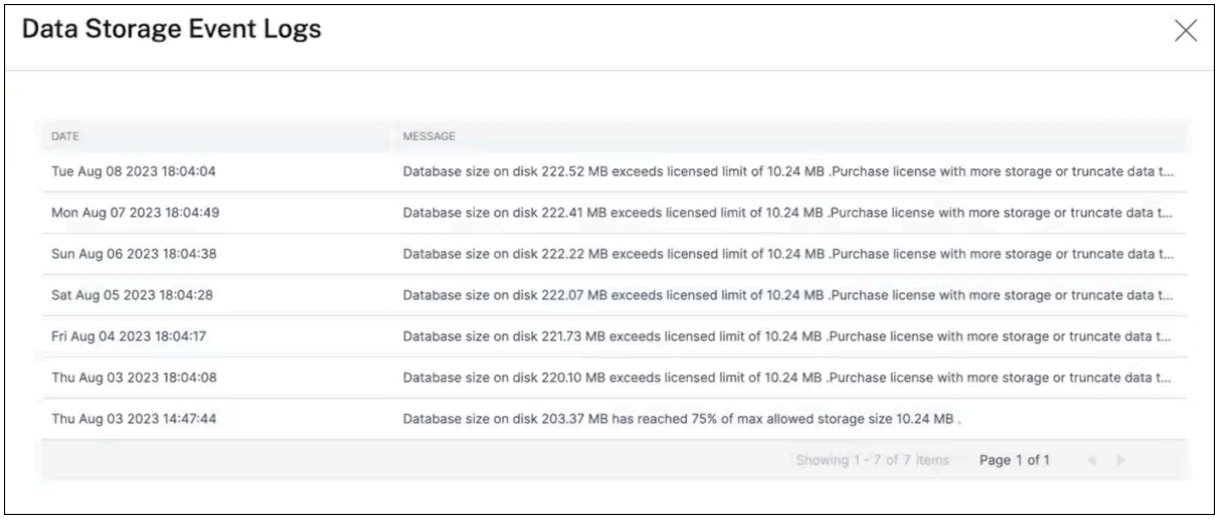
To understand which features were removed in each of the prune operations, select a task and click **Feature Log**.



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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

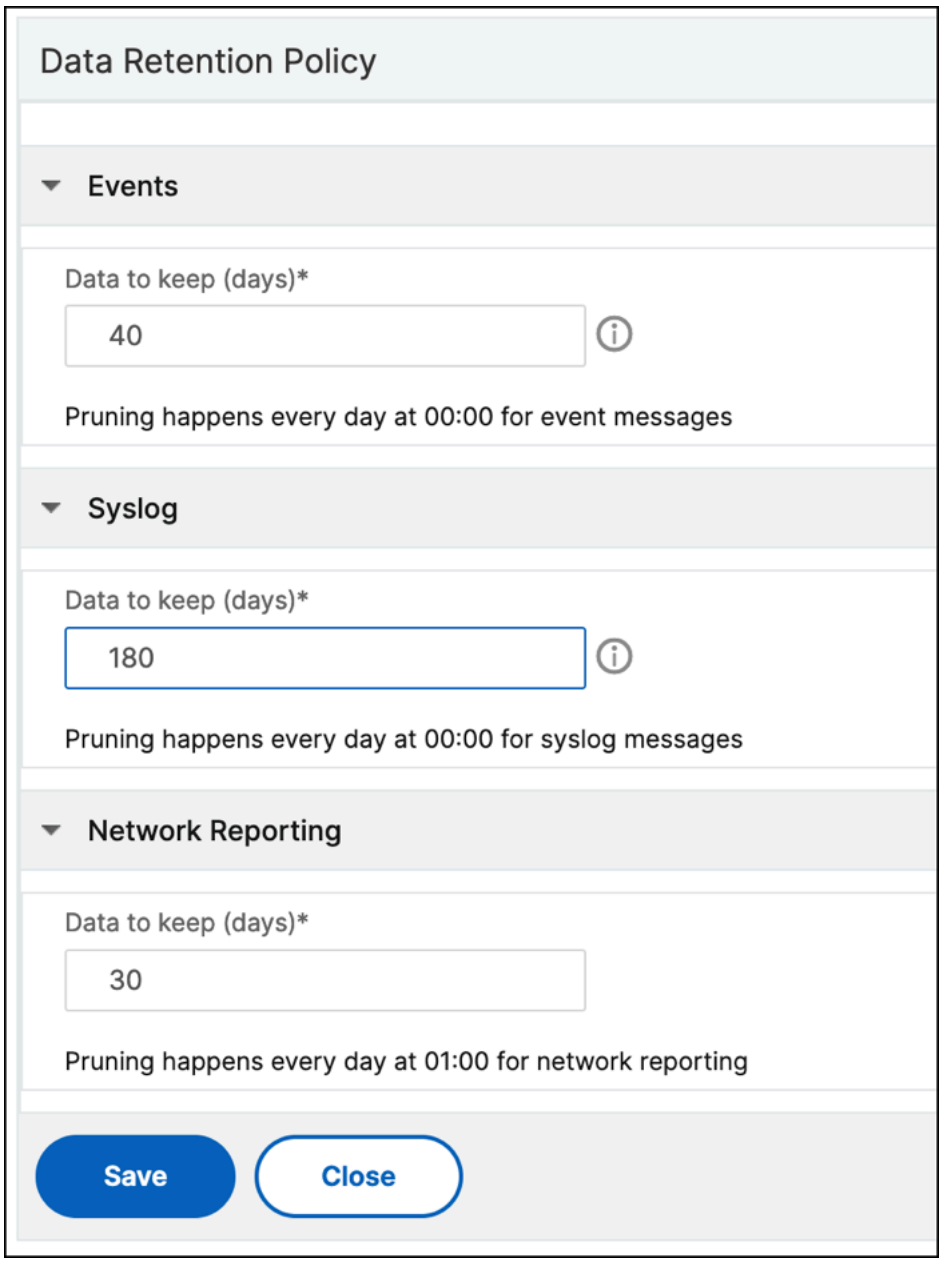
November 19, 2024

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 :

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.

© 1997–2025 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Configure and view system alarms

April 23, 2024

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.

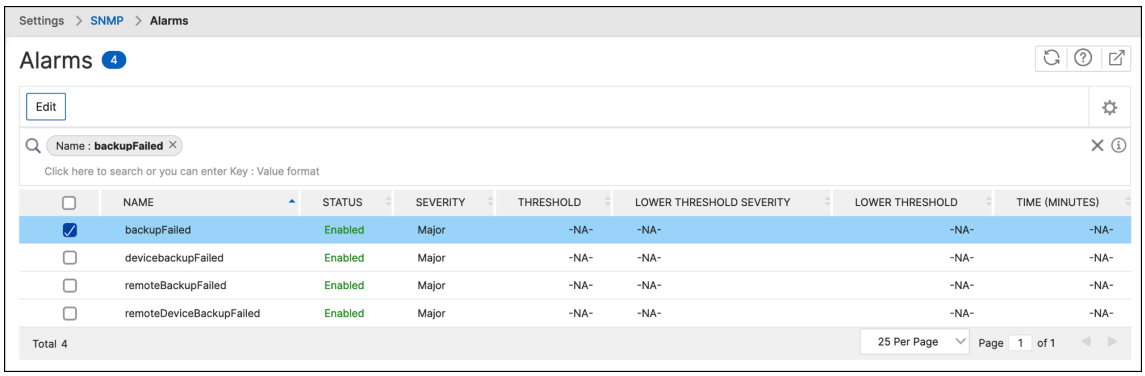
Configure an alarm

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.

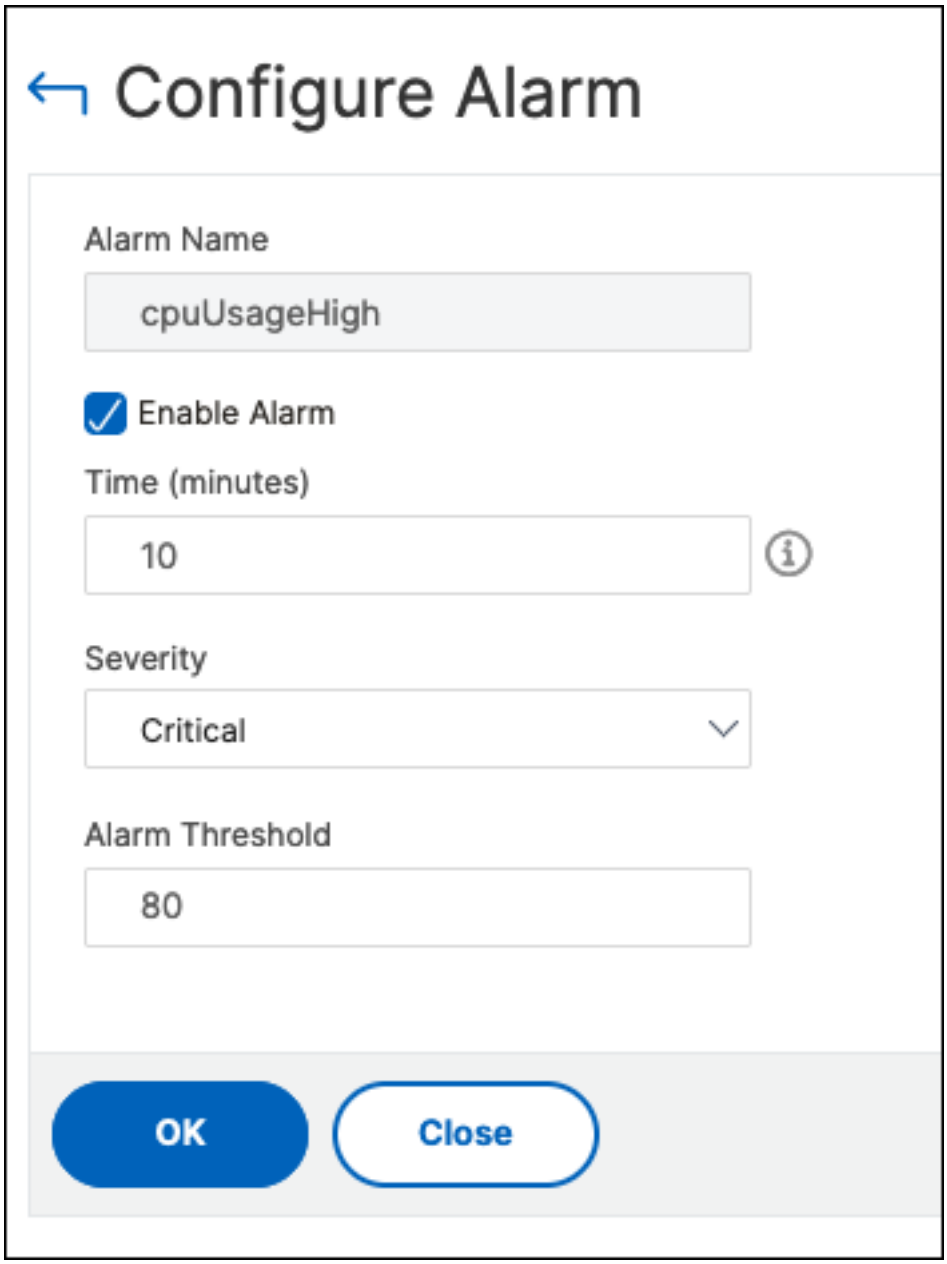
To configure and view a system alarm by using NetScaler Console:

1. Navigate to **Settings > SNMP**. Click **Alarms** in the upper-right corner.



© 1997–2025 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.

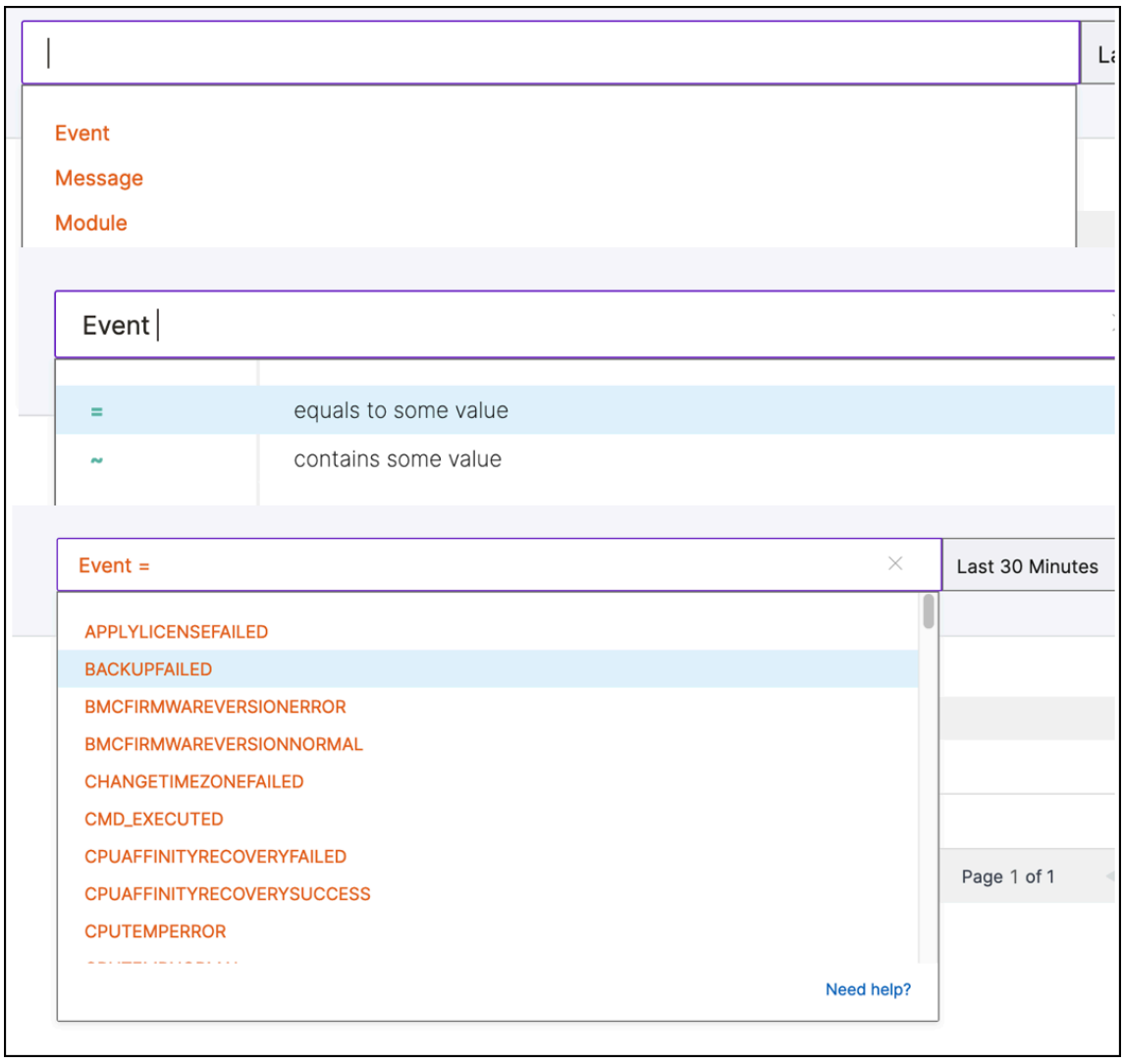
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

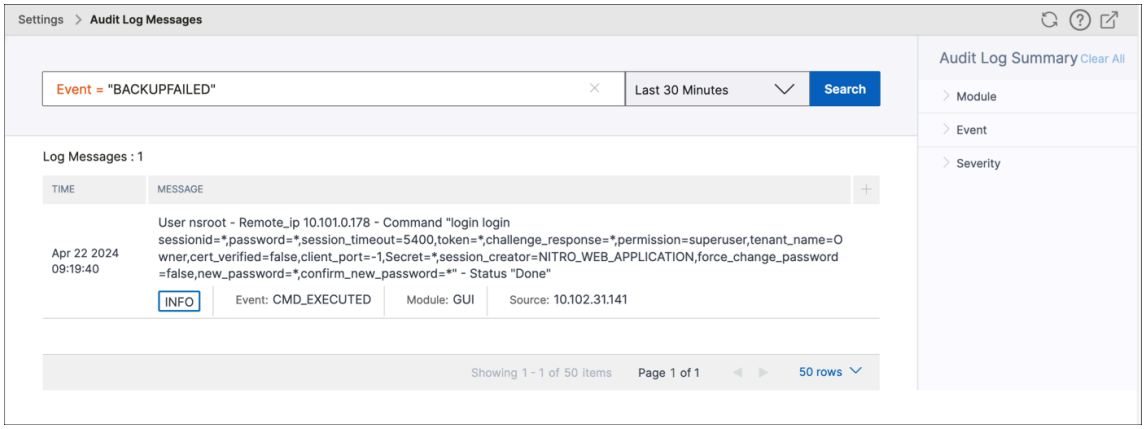
To view the event generated by alarm (for example, backupFailed):

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.

© 1997–2025 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.

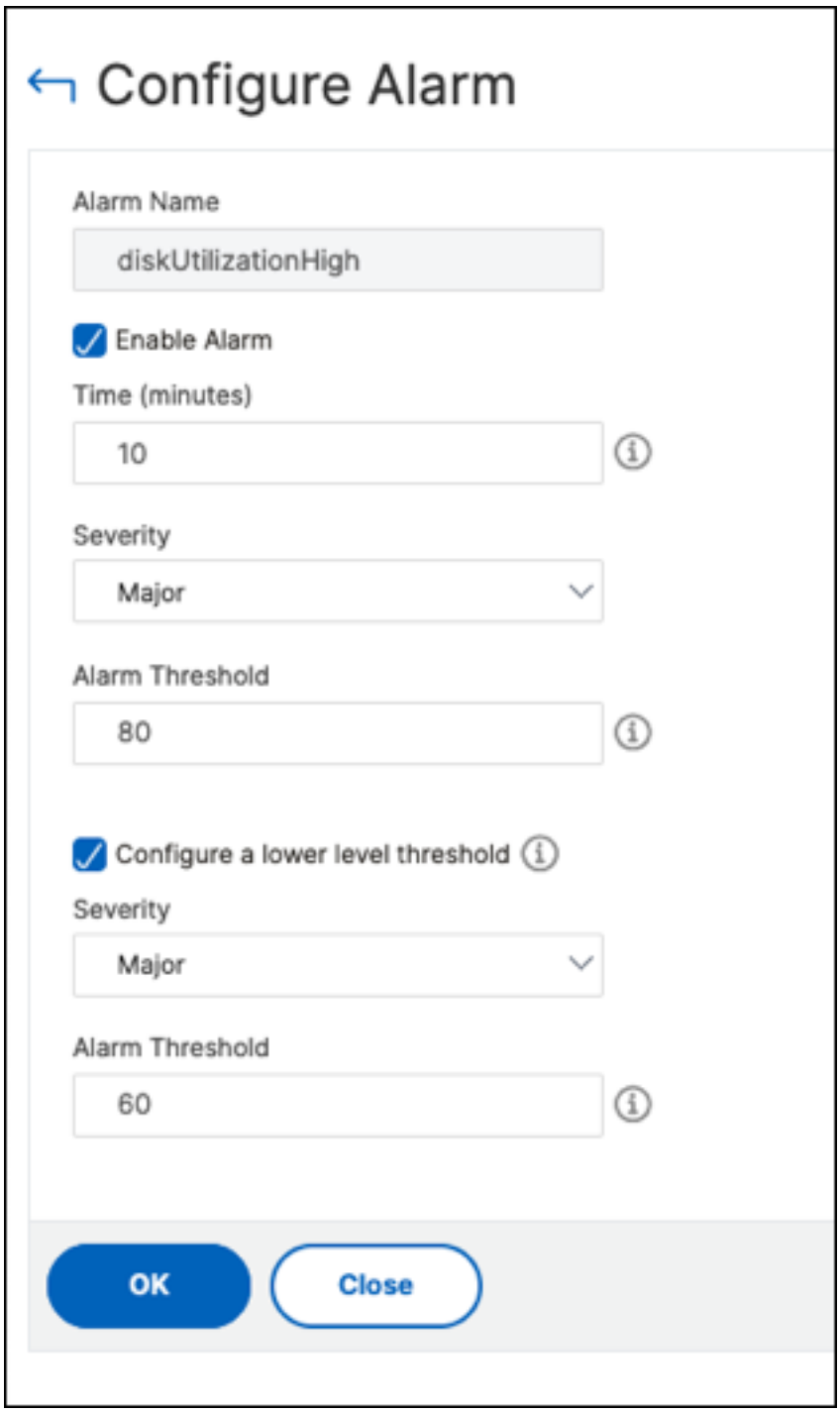
As an admin, when you receive alerts, you can choose to delete unnecessary data or allocate additional storage resources to prevent service disruptions or performance degradation.

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.

© 1997–2025 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%.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Observability Integration

June 25, 2024

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
- Configure NetScaler instances for the export of insights to Prometheus using the default schema.

Integration with Splunk

September 5, 2024

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

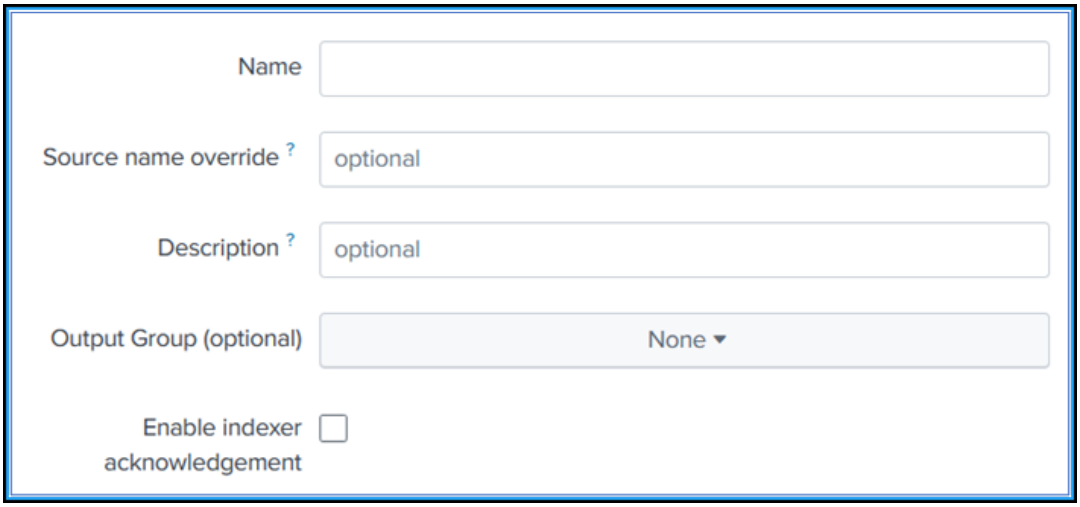
Setup the Splunk HTTP event collector endpoint and generate a token

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.

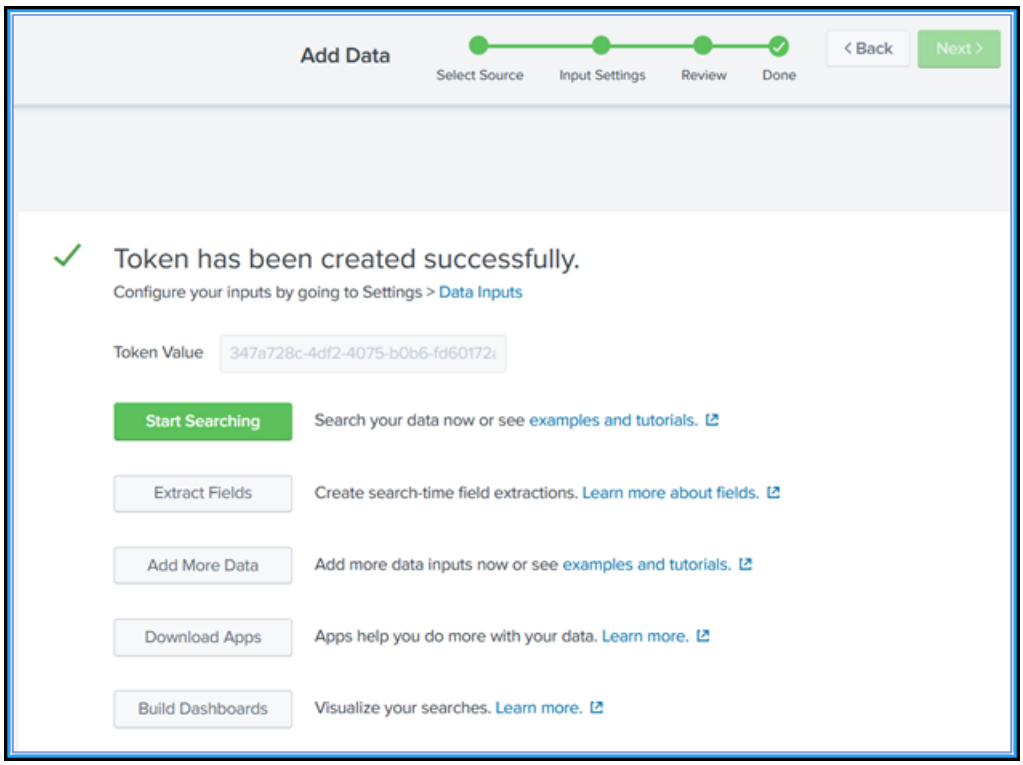
1. Log on to Splunk.
2. Navigate to **Settings > Data Inputs > HTTP event collector** and click **Add new**.
3. Specify the following parameters:
    a) **Name**: Specify a name of your choice.
    b) **Source name override (optional)**: If you set a value, it overrides the source value for HTTP event 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.



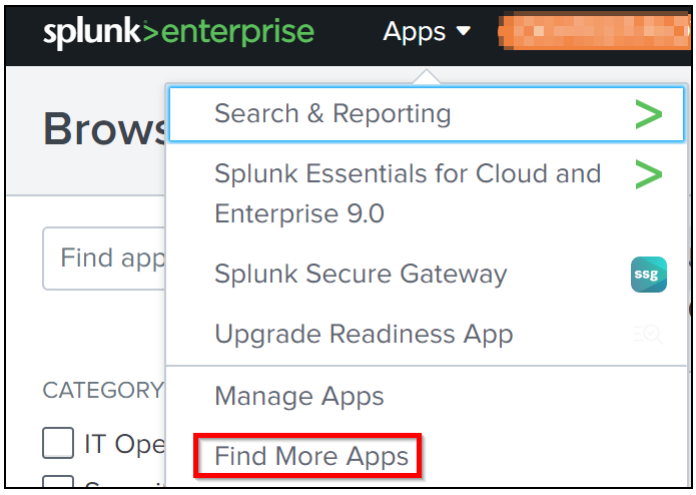
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Install the Splunk Common Information Model

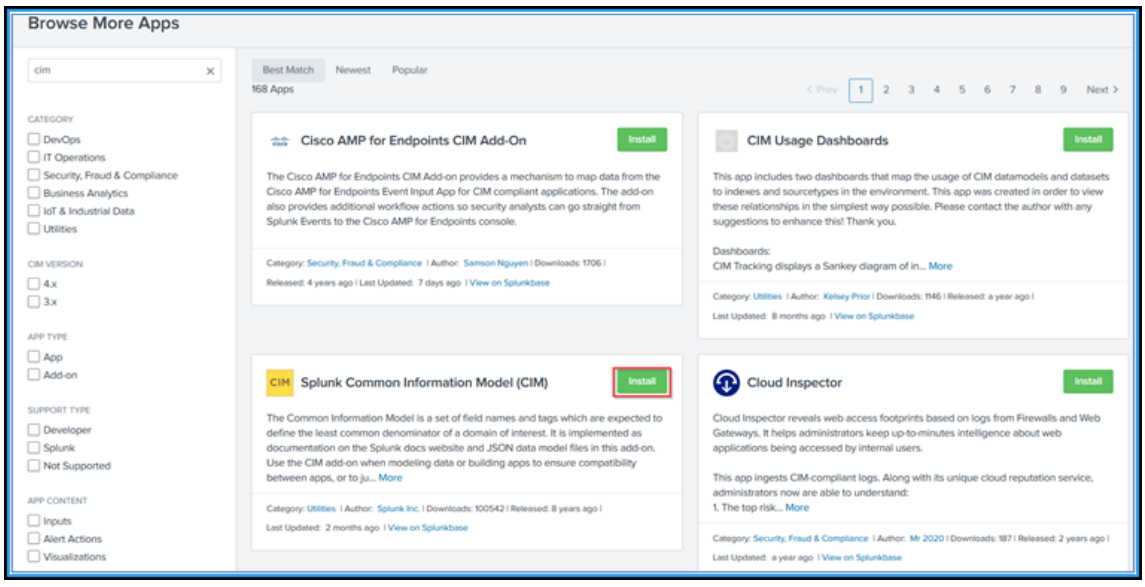
In Splunk, you must install the Splunk CIM add-on. This add-on ensures that the data received from NetScaler Console to normalize the ingested data and match a common standard using the same field names and event tags for equivalent events.

> **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**.



3. Type **CIM** in the search bar and press **Enter** to get the **Splunk Common Information Model (CIM)** add-on, and click **Install**.

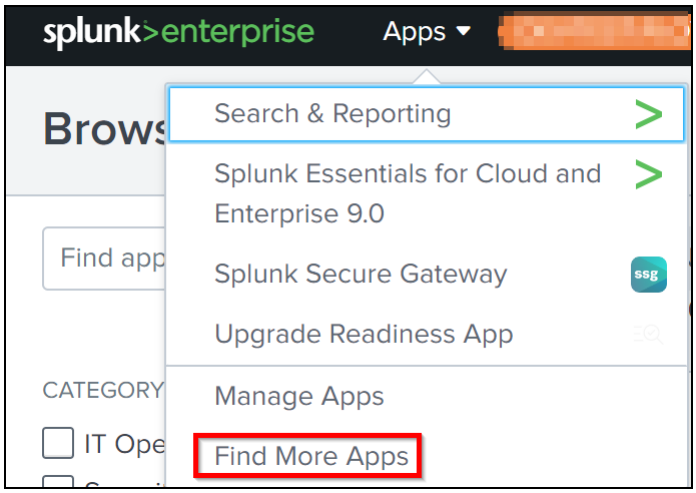


© 1997–2025 Citrix Systems, Inc. All rights reserved.

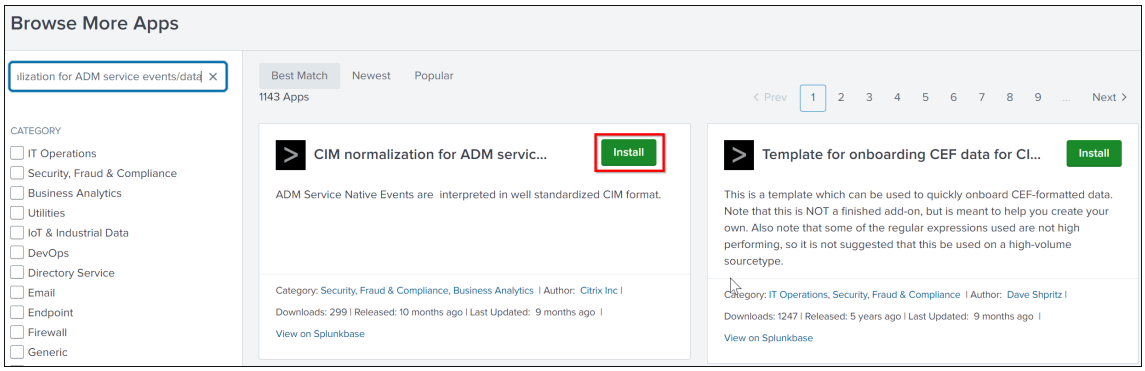
Install the CIM normalizer

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**.



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.

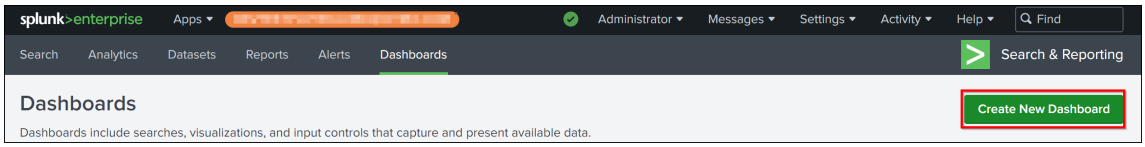
> **Note:**
>
> The following procedure to create a sample dashboard is applicable for both WAF and Bot, and SSL Certificate Insights. You must use the required `json` file.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

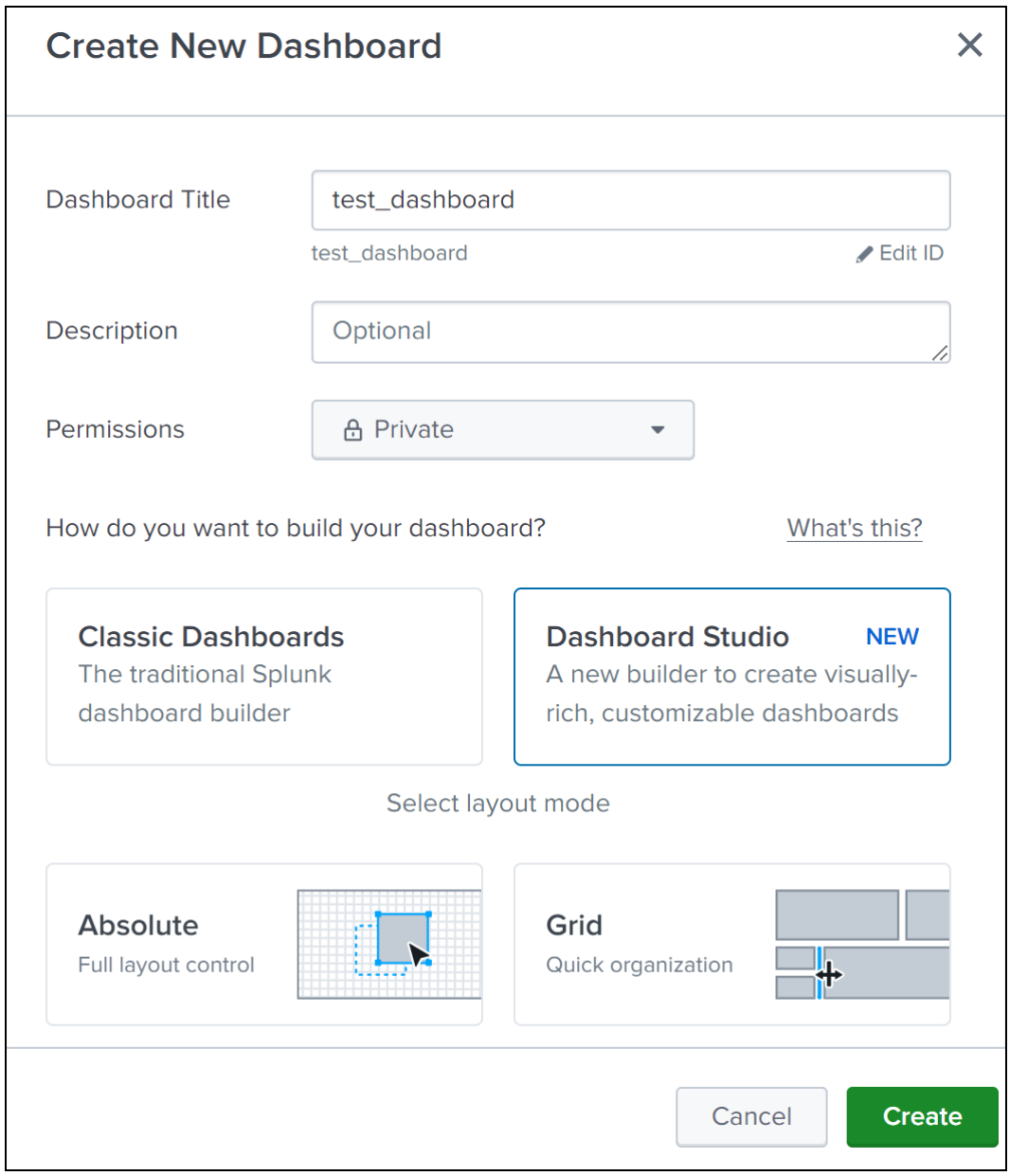
   b) **Description** - Optionally, you can provide a description for your reference.

   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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



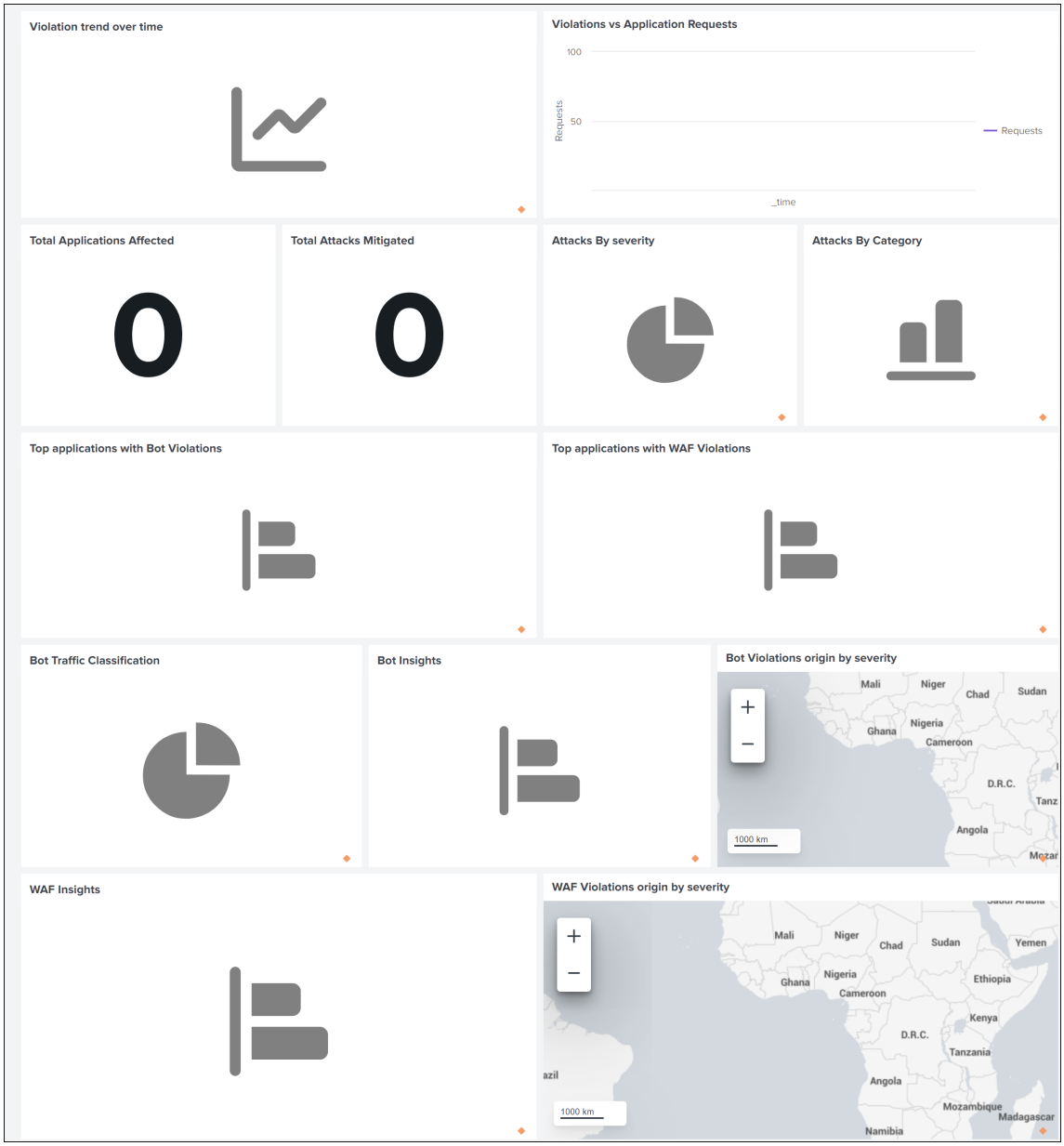
After you click **Create**, select the **Source** icon from the layout.



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.

© 1997–2025 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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 **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.
    - **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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> The data for the selected insights gets pushed to Splunk immediately after the violations are detected in NetScaler Console.

View dashboards in Splunk

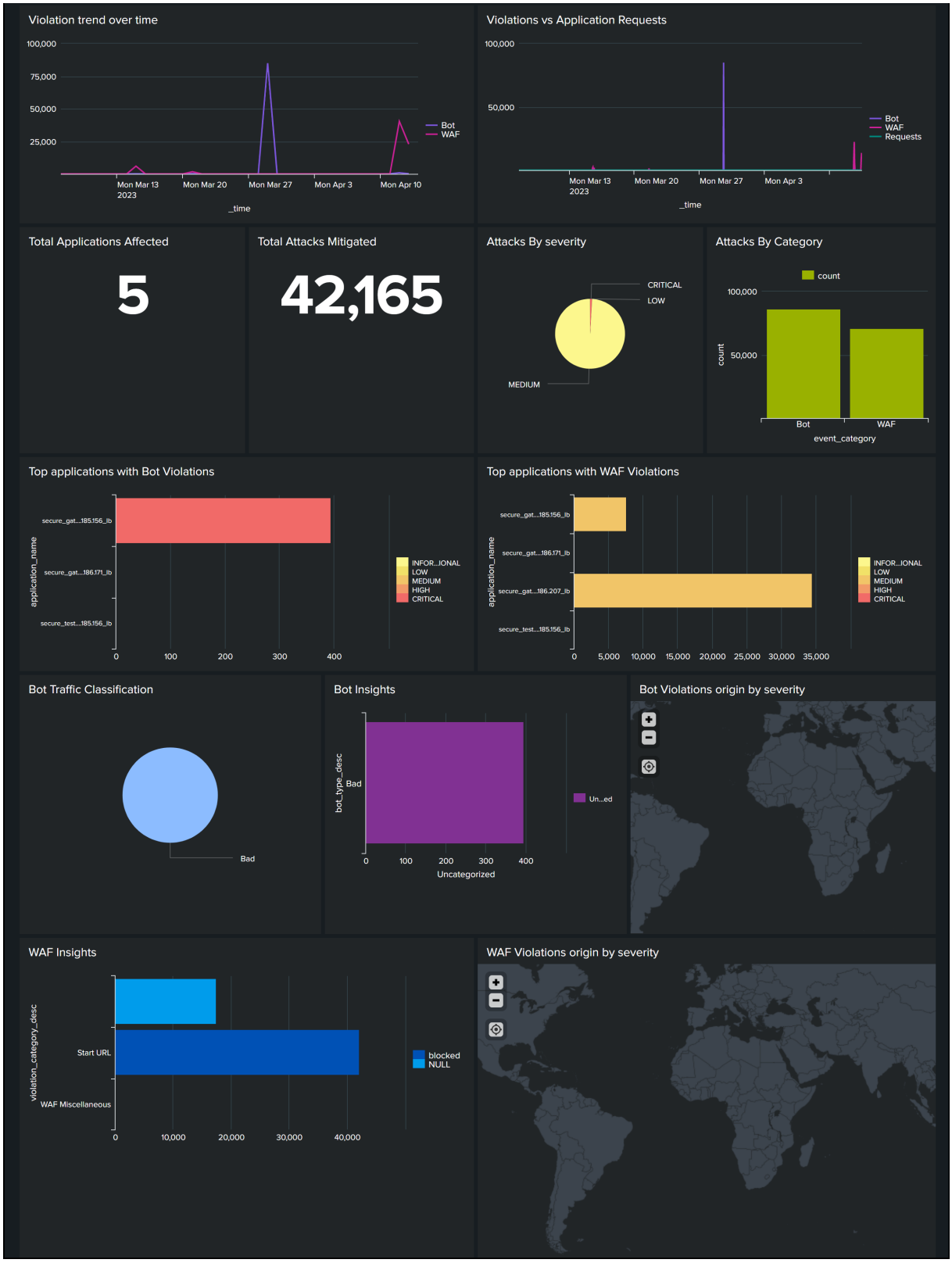
After you complete the configuration in NetScaler Console, the events appear in Splunk.

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.

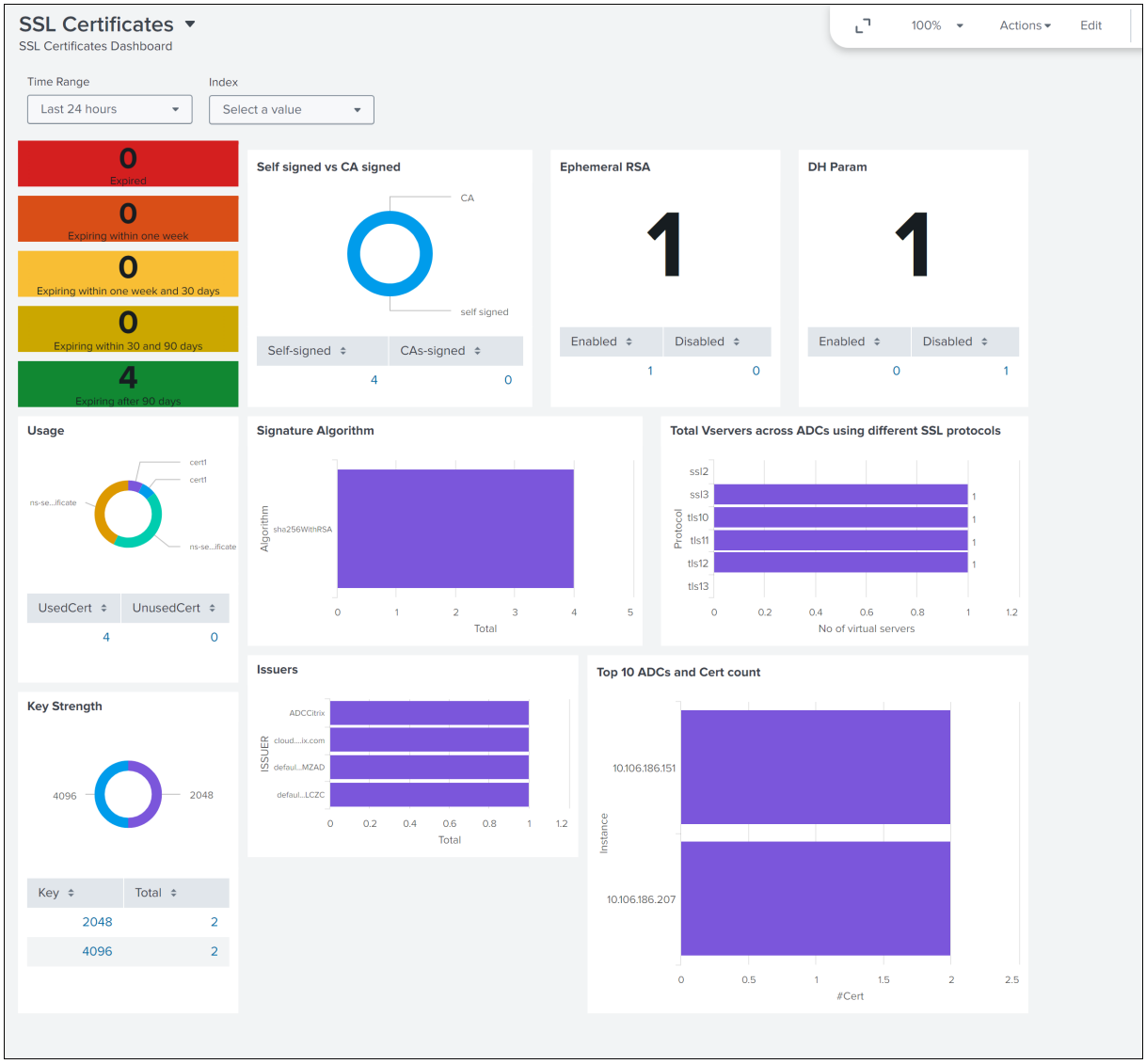
The following is an example for the updated WAF and Bot dashboard:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



The following dashboard is an example for the updated SSL Certificate Insights dashboard.

© 1997–2025 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Integration with New Relic

September 5, 2024

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

b) Select **NetScaler Console** as the **Source** and click **Next**.

c) Select **New Relic** and click **Configure**. In the **Configure Endpoint** page:

   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**.

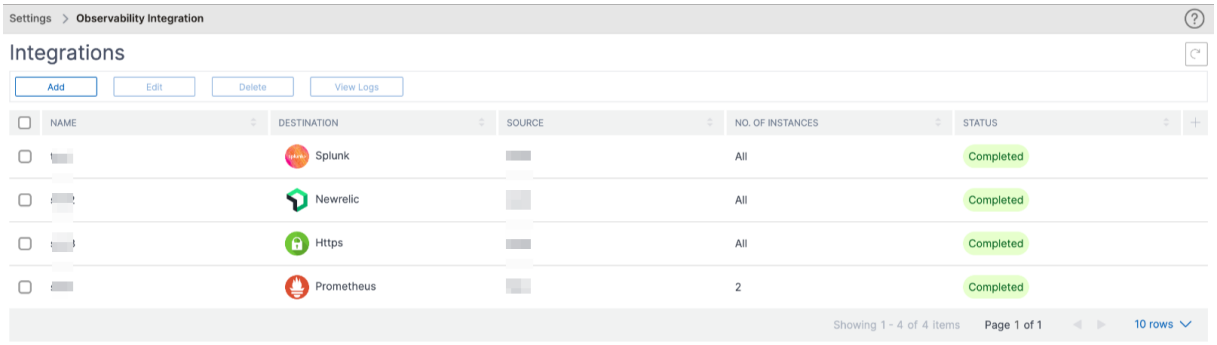
- **Select All Instances** - Exports data to New Relic from all the NetScaler instances.
- **Custom select** - Enables you to select the NetScaler instances from the list. If you select specific instances from the list, then the data is exported to New Relic only from the selected NetScaler instances.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



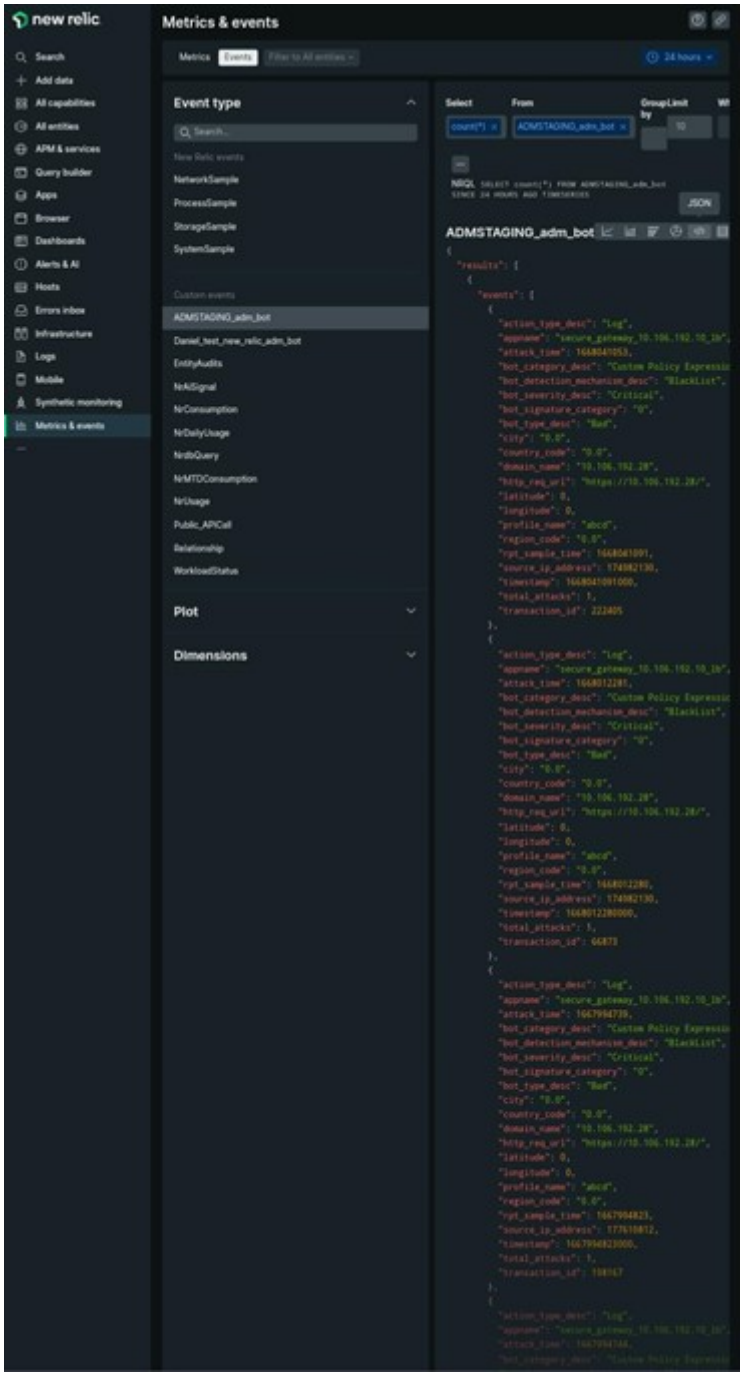
New Relic dashboard

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>.

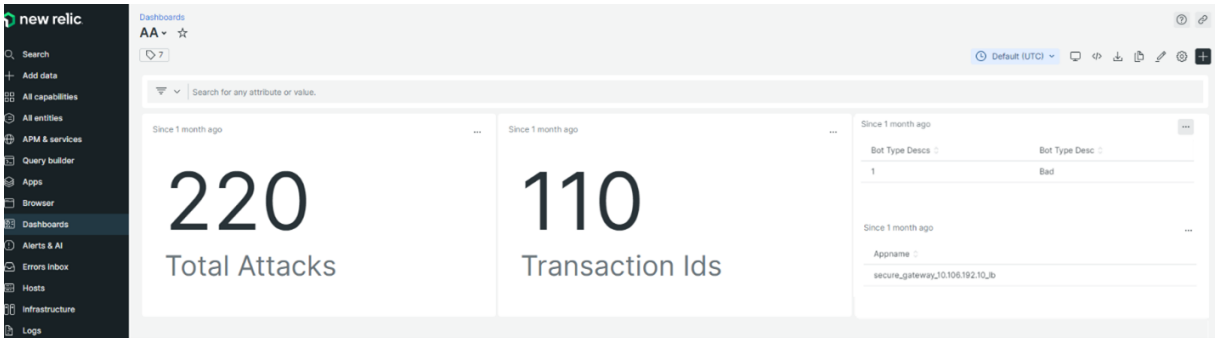
© 1997–2025 Citrix Systems, Inc. All rights reserved.



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:

© 1997–2025 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

September 8, 2025

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

For a successful integration, ensure that you have an active Azure subscription and then follow the procedure under each section:

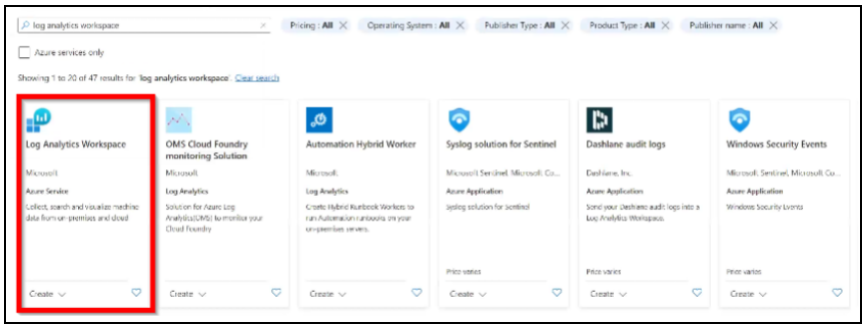
Configure the Log Analytics Workspace

A Log Analytics Workspace is required to store and analyze the collected data.

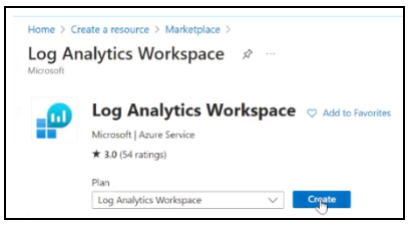
1. Login to Azure.
2. Click **Create a resource**.



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**.



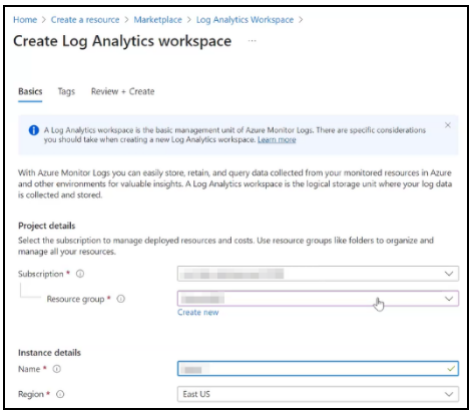
5. In the **Create Log Analytics workspace**:
   a) Select the active Subscription and the Resource group.

   > **Note:**
   >
   > You can also click **Create new** to add a resource group if you have the privilege.

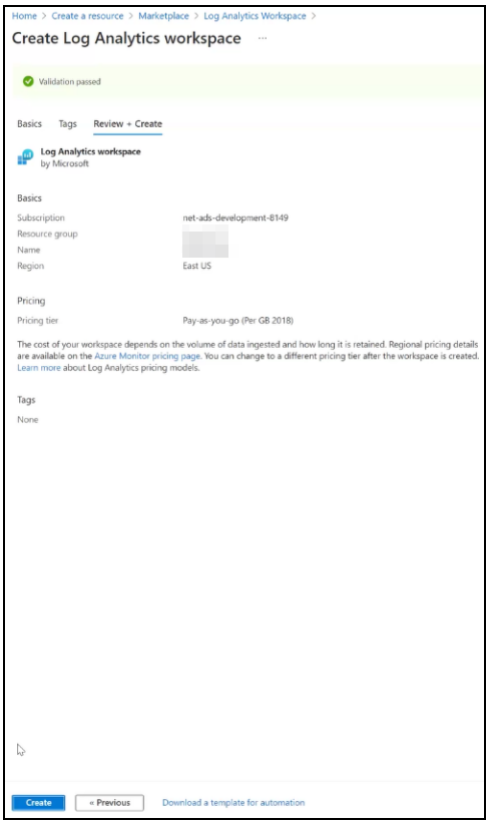
   b) Specify a name of your choice.
   c) Select your region from the list.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

d) Click **Review + Create**.



e) A validation passed message appears. Click **Create** to deploy the workspace.



f) You can see the deployment in progress message. After you see the deployment complete message, click **Go to resource**.



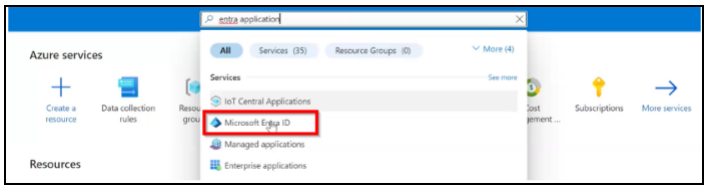
© 1997–2025 Citrix Systems, Inc. All rights reserved.

The workspace is successfully created.

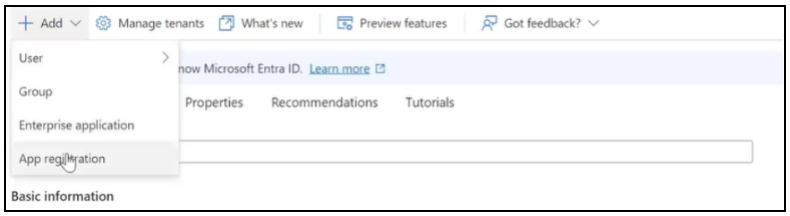
Create a Microsoft Entra application

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.

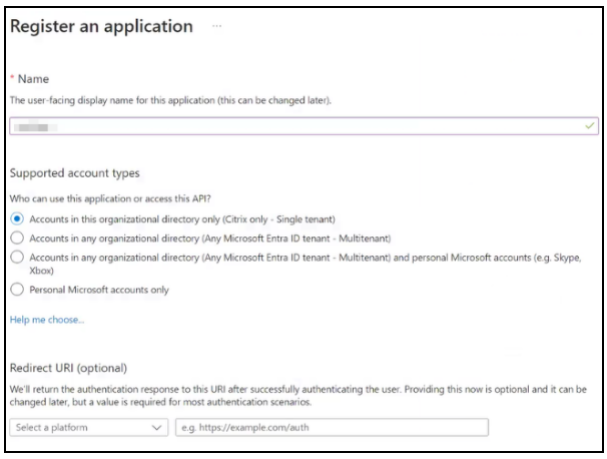
1. In your Azure portal, type the keyword in the search bar.
2. Click **Microsoft Entra ID**.



3. Click **Add** and select **App registration**.



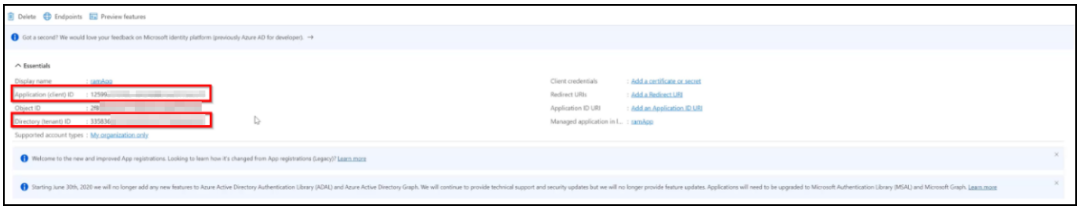
4. Specify a name for the app, select the default option under **Supported account types**, and then click **Register**.



5. After you register the application:

   a) Make a note of **Client ID** and **Tenant ID**.

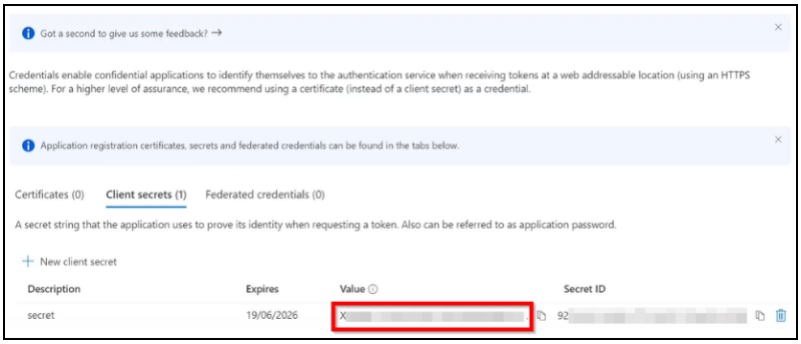
© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.



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

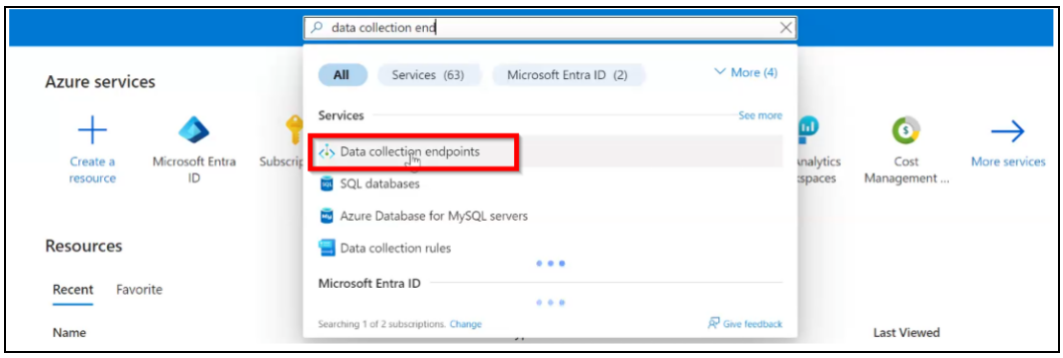
Microsoft Entra ID logs provide comprehensive information about users, applications, and networks accessing your Entra tenant. For more information, see Send data to Microsoft Sentinel using the Microsoft Entra ID data connector.

Configure data collection endpoint

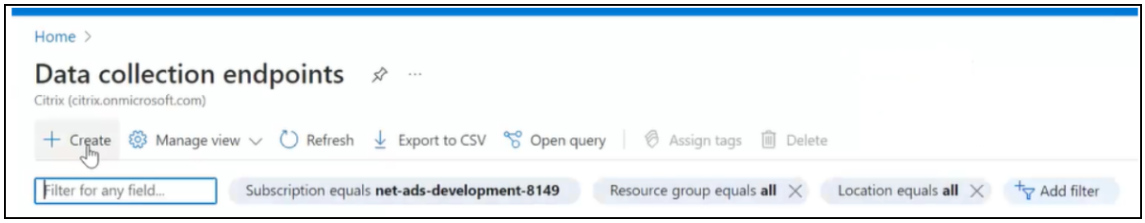
You must create a data collection endpoint to get the endpoint URL. This is required when you create a subscription in NetScaler Console.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.



3. In **Create data collection endpoint**:

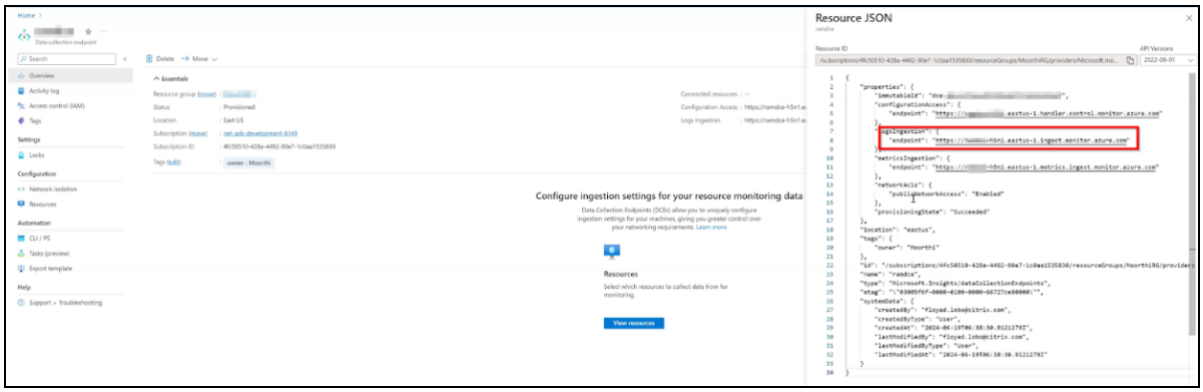
   a) Specify an endpoint name of your choice

   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.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

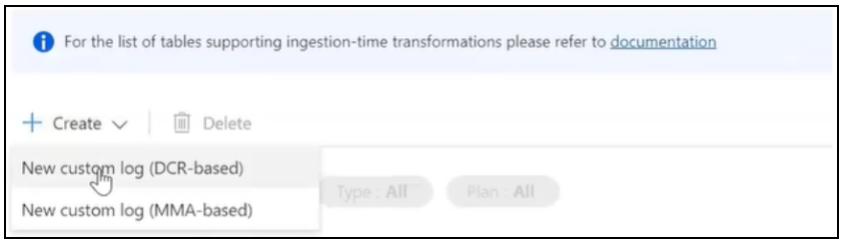
Create tables to export data

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

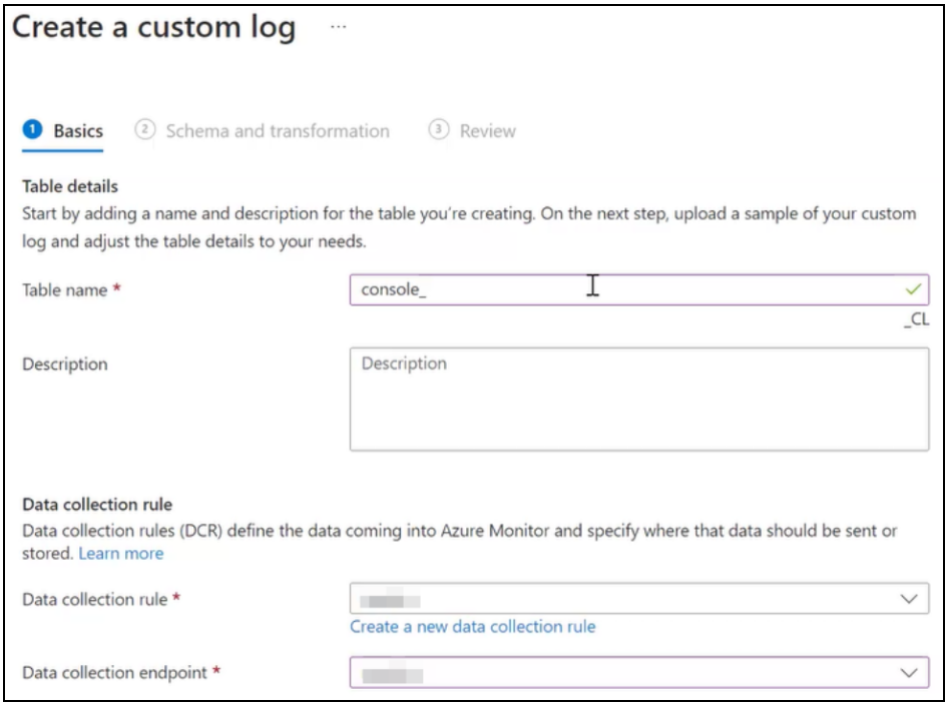
For each workspace, you can create a maximum of 10 tables. Beyond 10 tables, you must create another workspace.

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.

© 1997–2025 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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Insights	JSON	Table name to be used

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", "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", "	console_ns_sslvserver

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Insights	JSON	Table name to be used
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", "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, "	console_ns_ssl_certkey

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Insights	JSON	Table name to be used
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", "table_name": "ns_sslcertkey_binding"}	console_ns_sslcertkey_binding

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Insights	JSON	Table name to be used
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?field10=asfasd", "violation_name": "-NA-", "violation_value": "-NA-", "violation_location": 4, "violation_threat_index	console_af_threat_exporter_data_l2

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Insights	JSON	Table name to be used
Bot	{ "ip_address": "10.106.186.122", "ctnsappname": "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"}	console_af_bot_attack_details_l2

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Insights	JSON	Table name to be used
Gateway Insight (1)	{ "adc_ip_address": "10.106.186.141", "auth_server": "", "client_ip": 174766732, "epa_method_type": 0, "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"}	console_af_vpn_error_details
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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Insights	JSON	Table name to be used
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
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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Insights	JSON	Table name to be used
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:



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.

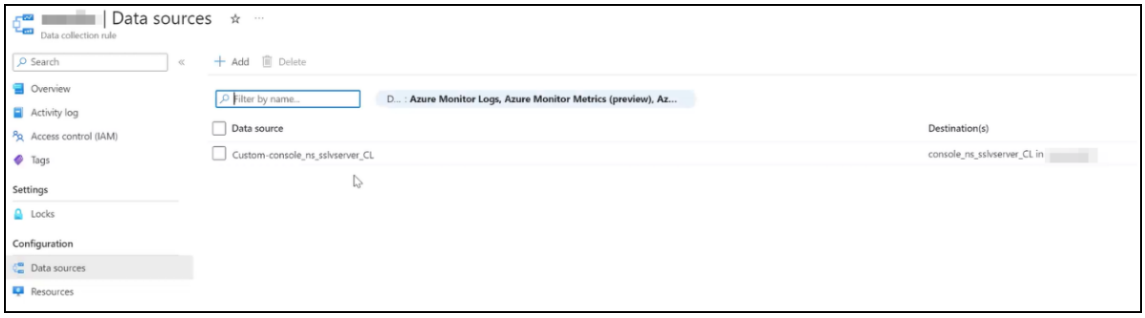
- **SSL** - `source | extend TimeGenerated = todatetime(poll_time)| project-rename sslvserver_id = id`
- **WAF** and **Bot** - `source | extend TimeGenerated = todatetime(rpt_sample_time )`
- **Gateway Insight** - `source | extend TimeGenerated = todatetime( rpt_sample_time)`



5. Click **Next** and click **Create** to complete.
6. Navigate to **Data collection rules**, click the DCR that you have created.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

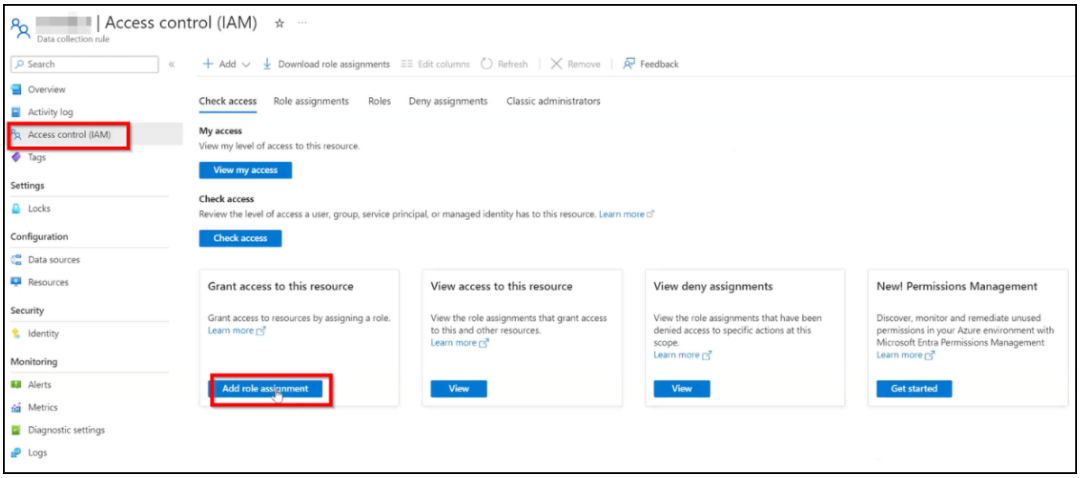
7. Under **Configuration**, click **Data sources** to view the created table.



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**.



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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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
- 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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

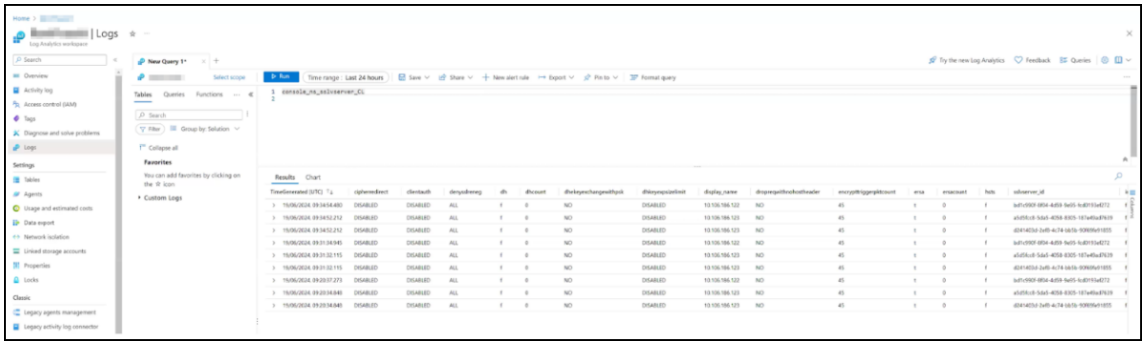
- **Select All Instances** - Exports data to Microsoft Sentinel from all the NetScaler instances.
- **Custom select** - Enables you to select the NetScaler instances from the list. If you select specific instances from the list, then the data is exported to Microsoft Sentinel only from the selected NetScaler 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.



Configure NetScaler instances for the export of insights to Prometheus using the default schema

June 11, 2024

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.

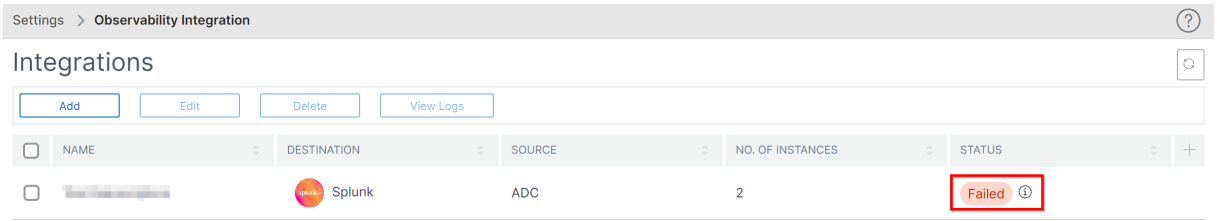
© 1997–2025 Citrix Systems, Inc. All rights reserved.

With the Observability Integration feature in NetScaler Console, you can configure the export of insights to Prometheus using the default schema.

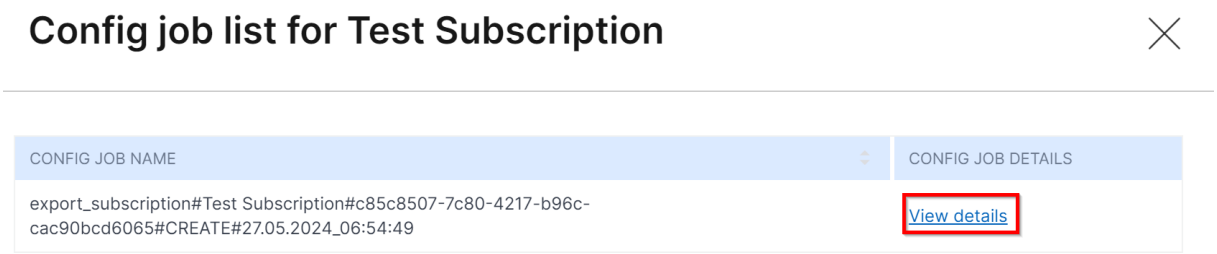
1. Navigate to **Settings > Observability Integration**.
2. In the **Integrations** page, click **Add**.
3. In the **Create Subscription** page, specify the following details:
    a) Specify a name of your choice in the **Subscription Name** field.
    b) Select **NetScaler** as the **Source** and click **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**.

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.

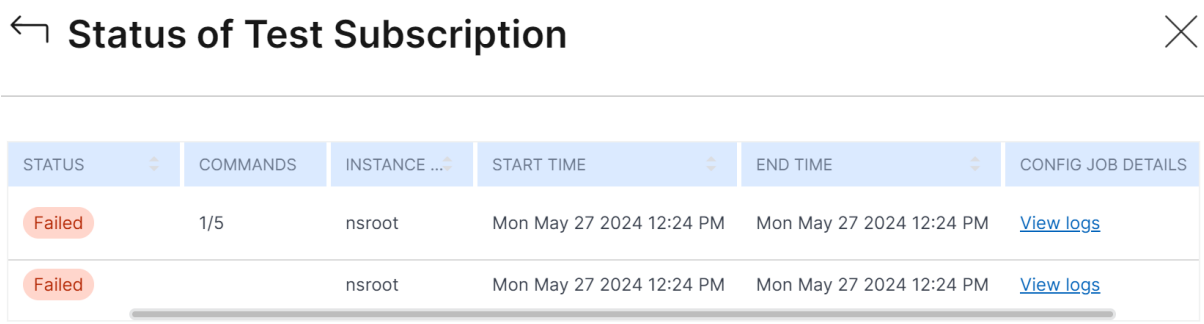


Click **View details** under **Config job details**.



Click **View logs** to view details of the issue.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Configure the export of NetScaler metrics and audit logs to Splunk

June 11, 2024

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

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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

d) Click **Next**.

e) Click **Add Insights** and select **NetScaler Metrics** and **NetScaler Audit Logs**, and then click **Add Selected**.

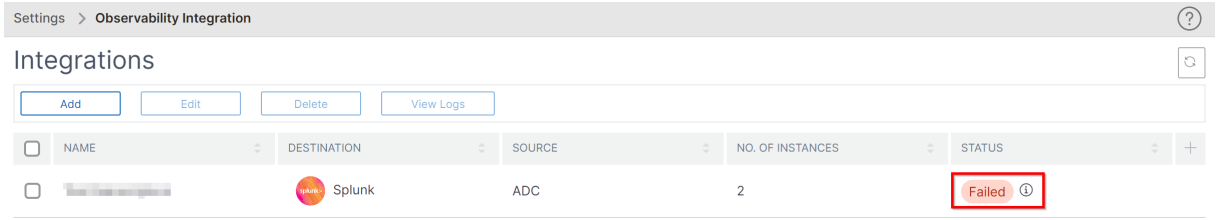
f) Click **Next**.

g) Click **Add Instances** and select the instances.

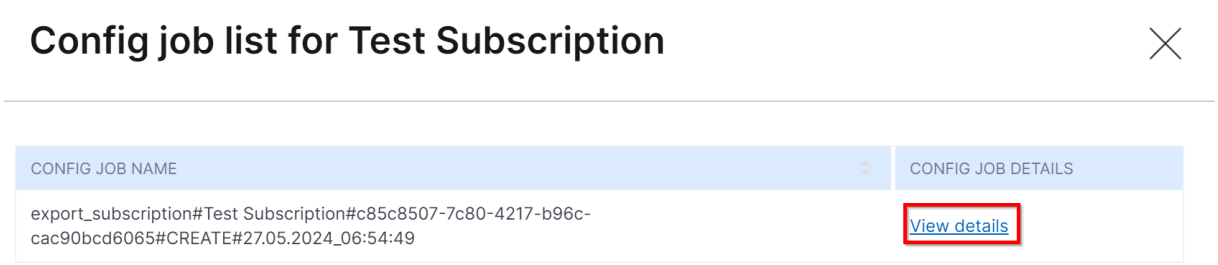
h) Click **Submit**.

View logs for failed configurations

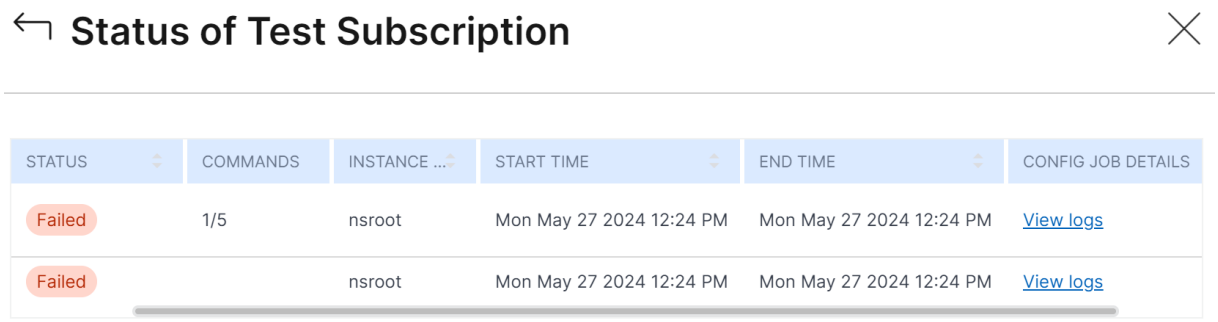
After you create a subscription, you can view the status of the created subscription at **Settings > Observability Integration**. If the status shows **Failed**, click to view details.



Click **View details** under **Config job details**.



Click **View logs** to view details of the issue.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Configuring Analytics settings

January 8, 2024

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.

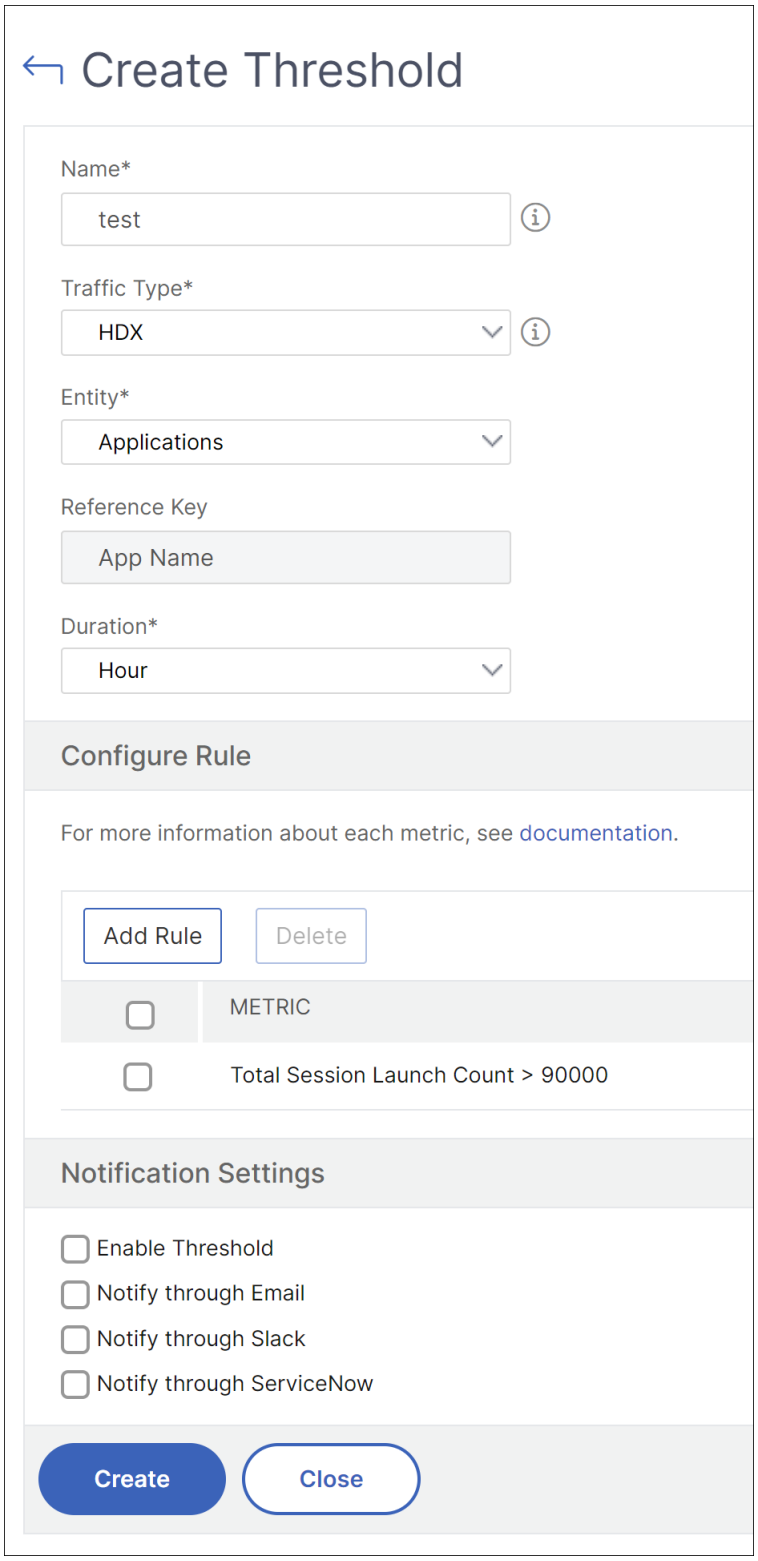
To create thresholds and alerts for analytics:

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.
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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Comparator** –Comparator to the selected metric (for example: <, >=).
- **Value** –Value for the metric to set the threshold, and invoke alerts.

6. Click **Create**.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Configure notifications

January 8, 2024

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.

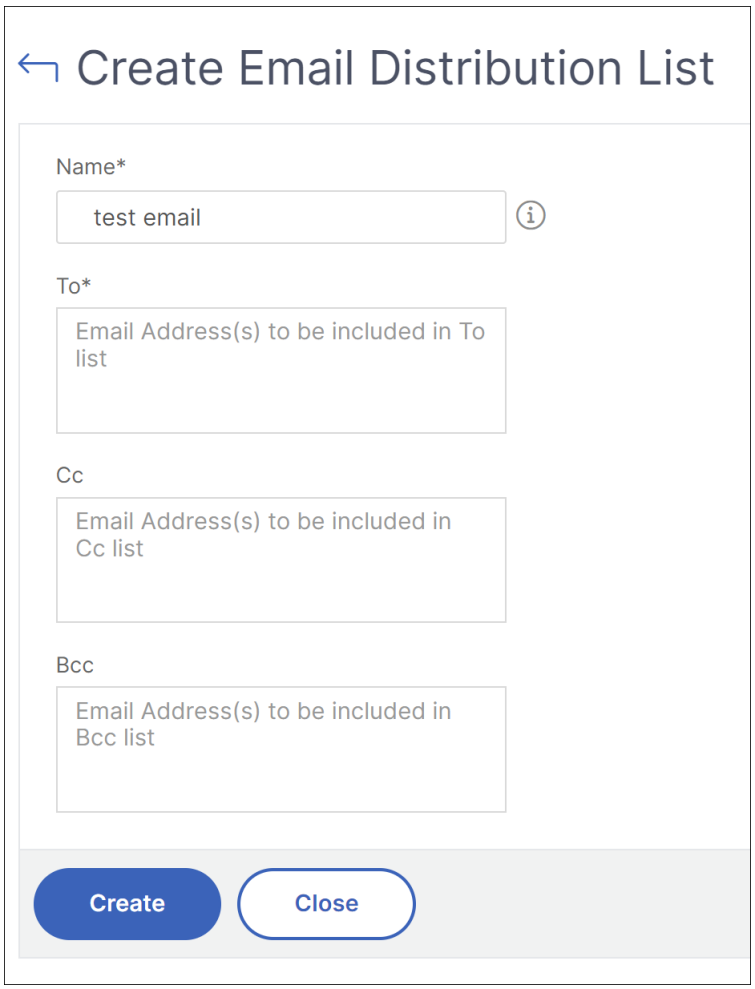
Create an email distribution list

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.

© 1997–2025 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.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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**.

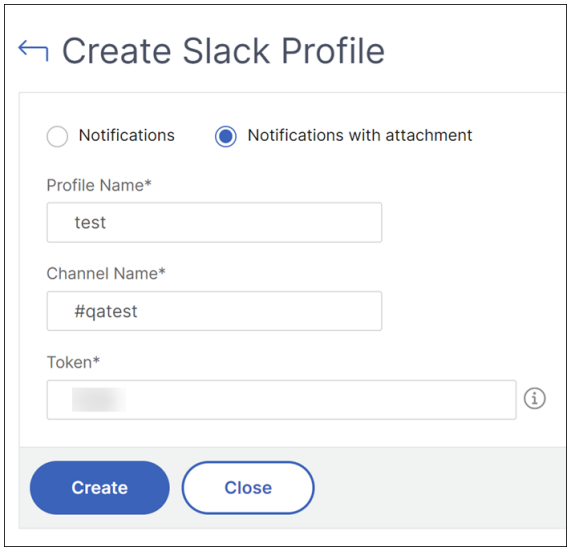
Repeat this procedure to create multiple SMS distribution lists. The **SMS** tab displays all the SMS distribution lists present in NetScaler Console.

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



4. Click **Create**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:

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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Export or schedule export reports

January 8, 2024

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.

In **Export Reports**, you can perform the following actions:

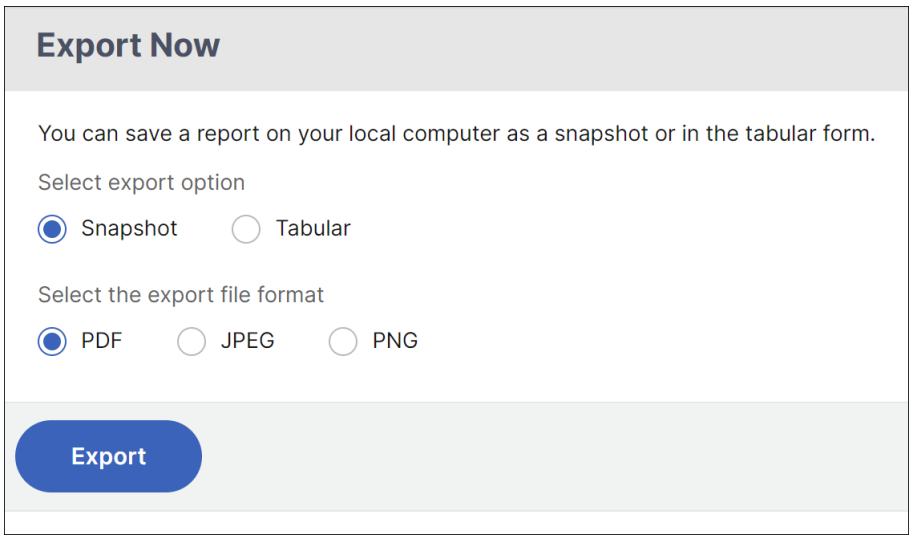
- Export a report to a local computer
- Schedule export reports
- View, edit, or delete the scheduled export reports

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.



4. Select the file format that you want to save the report on your local computer.
5. Click **Export**.

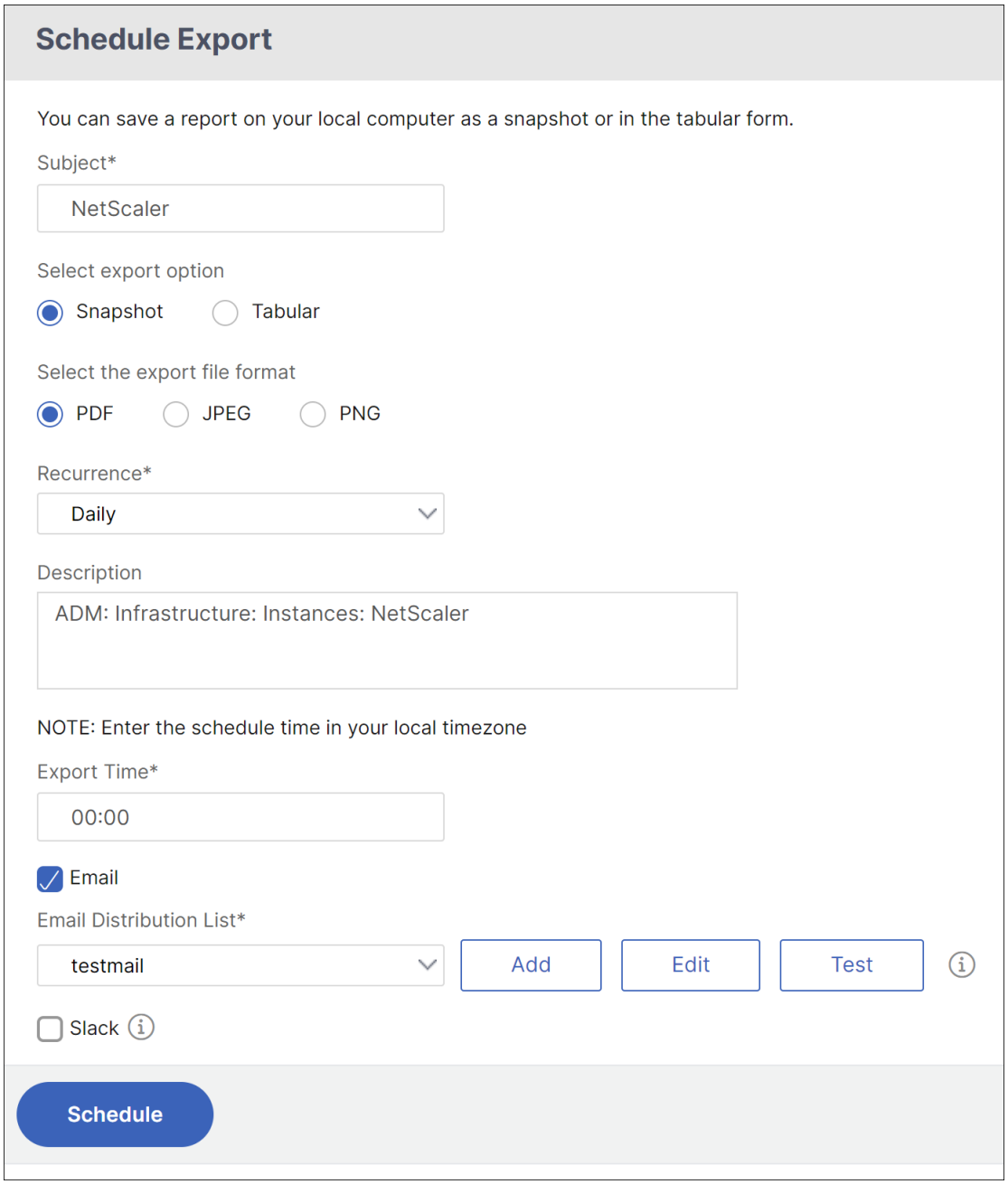
Schedule export report

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.

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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

3. Click **Schedule**.



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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Instance settings

January 30, 2025

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.
- **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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:

  1. Specify the IP address of the location.
  2. Specify the user name and the password of the external server to which you want to transfer the backup files.
  3. Specify the transfer protocol and the port number.
  4. Specify the directory path where the file must be stored.
  5. 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

Instance settings

January 30, 2025

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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.
- **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:
  1. Specify the IP address of the location.
  2. Specify the user name and the password of the external server to which you want to transfer the backup files.
  3. Specify the transfer protocol and the port number.
  4. Specify the directory path where the file must be stored.
  5. 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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

System configurations

January 8, 2024

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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Email subscriptions

January 8, 2024

NetScaler Console sends in email notifications to all the inactive and the new users.

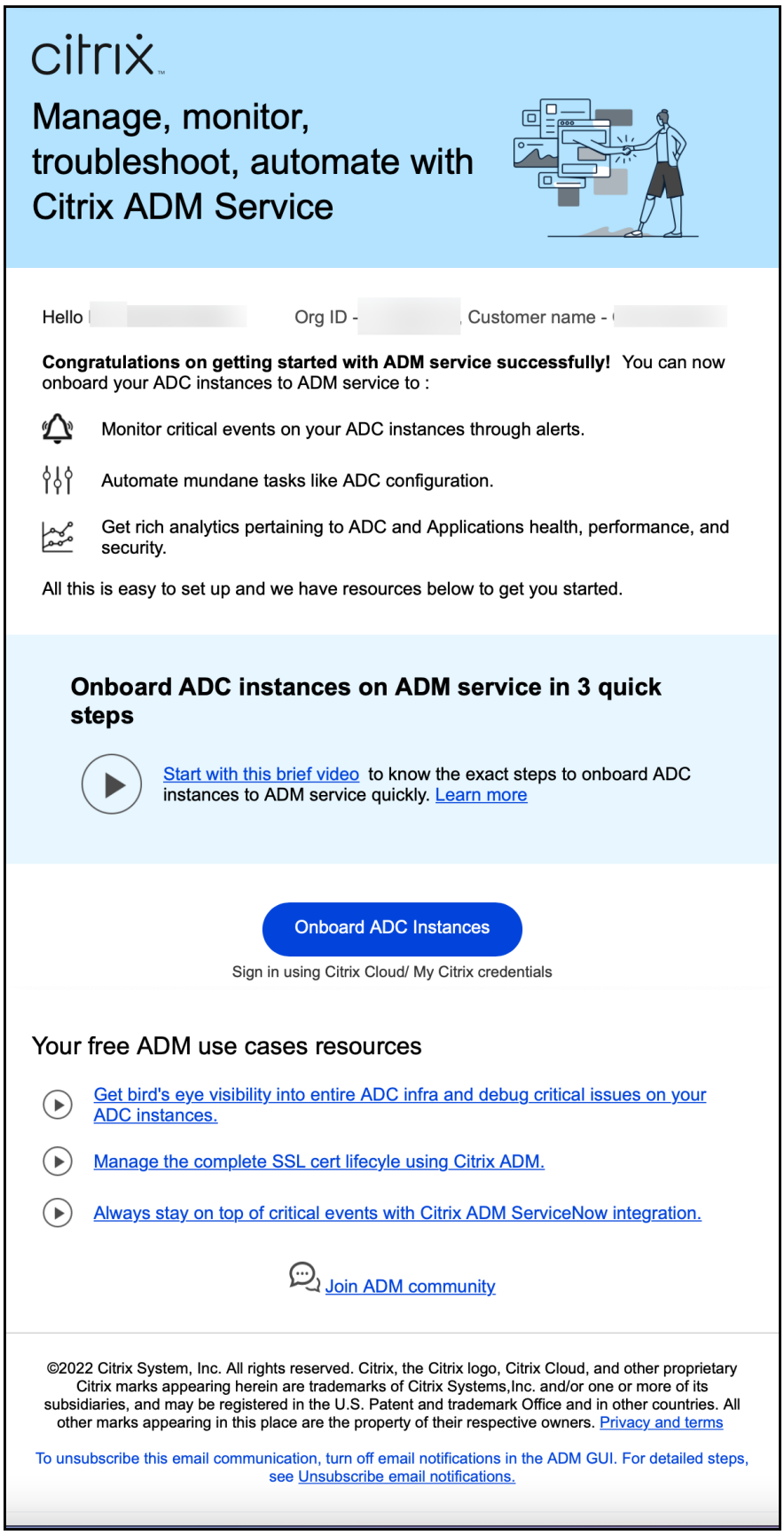
Inactive customers receive an email notification if:

- 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.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

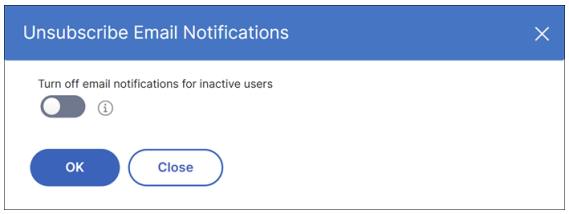


© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

June 6, 2024

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.
- **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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

February 27, 2024

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:

- Predefine certain conditions for the application events.
- Get notified for the following events through Slack, Email, PagerDuty, and ServiceNow:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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
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.

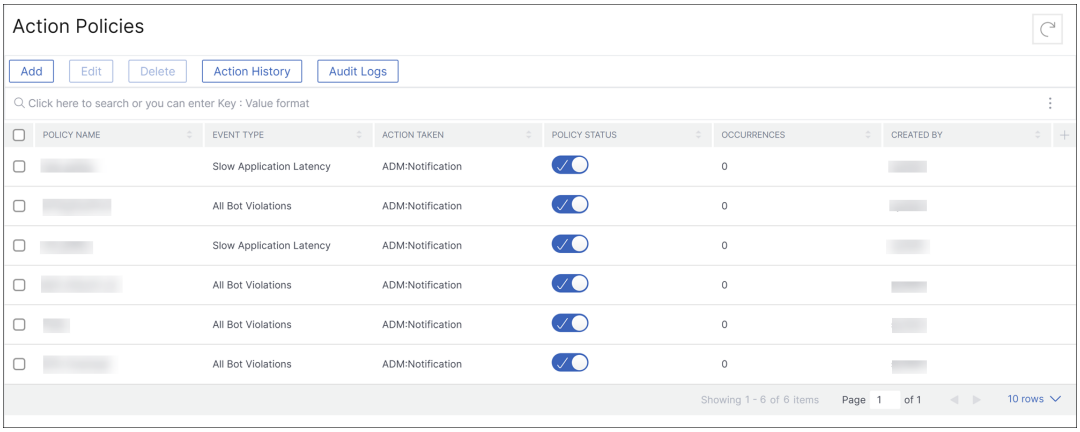
   f) **Notification Type** –Select the notification type Email, Slack, PagerDuty, or ServiceNow. Depending upon the notification type you select, the corresponding option (Distribution list, Slack Profile, PagerDuty Profile, or ServiceNow profile) appears. Select a profile from the list.

      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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.

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.

© 1997–2025 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 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.
	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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Violation name	Condition	Description
	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 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Violation name	Condition	Description
	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.
	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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Violation name	Condition	Description
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.
	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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Violation name	Condition	Description
	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 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Violation name	Condition	Description
	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.
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.

© 1997–2025 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.
	Application Name	Click **Select Applications** to select the applications that you want to get the violation notified.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Violation name	Condition	Description
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.



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,

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 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

January 8, 2024

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.

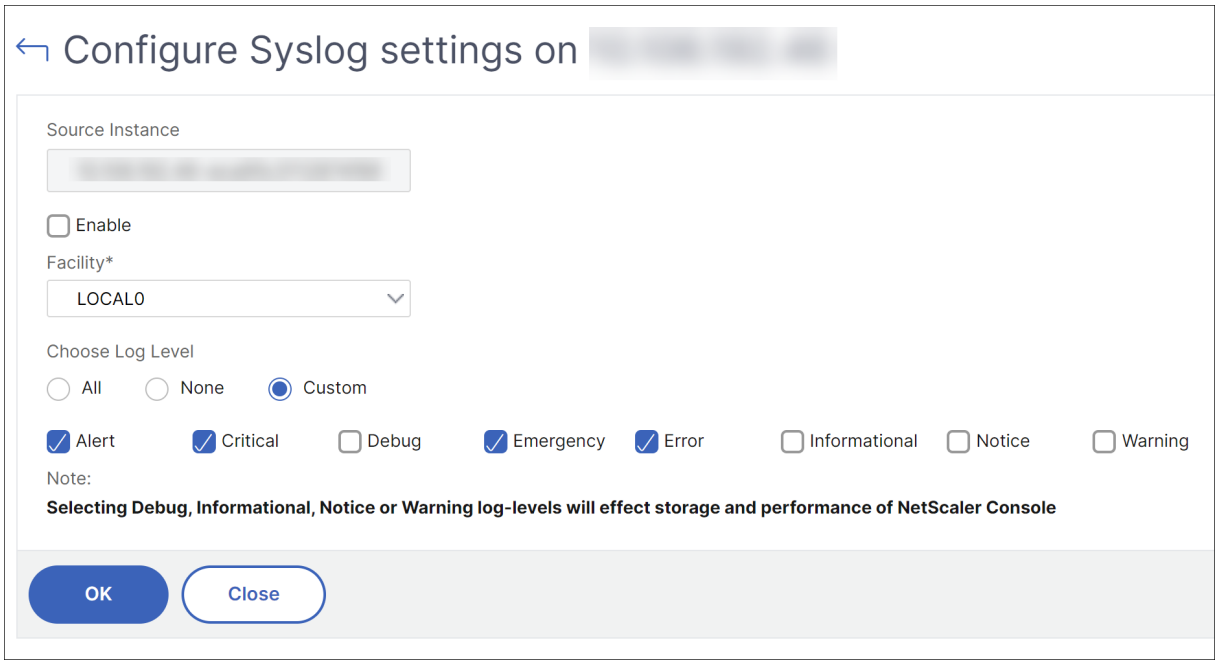
Configure NetScaler Console as a syslog server

Follow these steps to configure NetScaler Console as the syslog server:

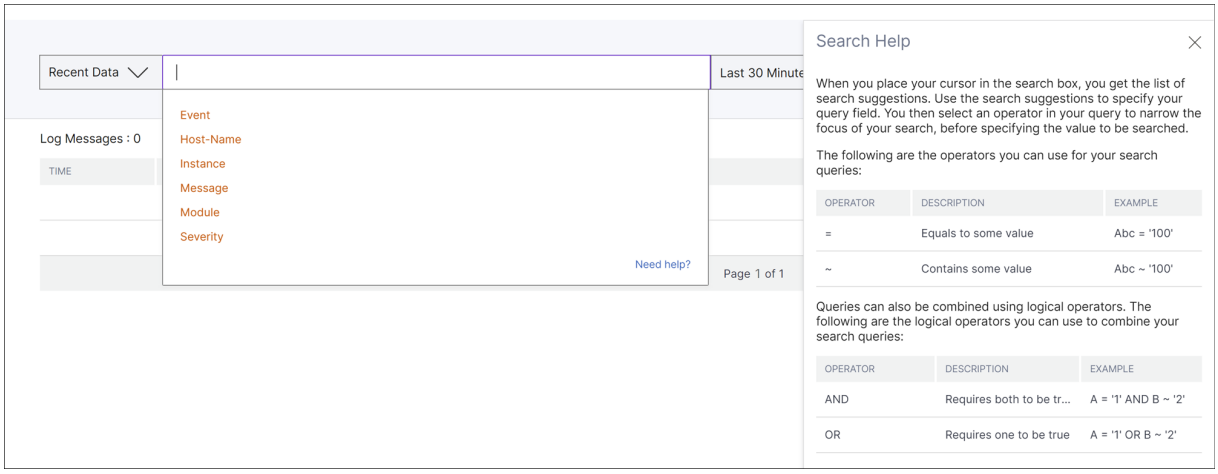
1. From the NetScaler Console GUI, navigate to **Infrastructure > Instances**.
2. Select the NetScaler instance from which you want the syslog messages to be collected and displayed in NetScaler Console.
3. In the **Select Action** list, select **Configure Syslog**.
4. Click **Enable**.
5. In the **Facility** drop-down list, select a local or user-level facility.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.



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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

Configure IP address management (IPAM)

April 15, 2025

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.
> - 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:

     ```
     1  https://<host name>
     ```

     Example: `https://myinfoblox.example.com`

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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
- 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **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.

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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
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**.
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**.

How-to articles

July 12, 2024

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

FAQs

May 8, 2024

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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`.

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`.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.