NetScaler Application Delivery Management 14.1

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

Contents

Release notes 12

Migrate NetScaler Console on-prem to Citrix Cloud 13

FAQs 22

Troubleshooting 26

All how to articles 28

Overview 33

Features and solutions 33

Architecture 36

How NetScaler Console discovers instances 37

Polling overview 39

NetScaler® telemetry program 47

Modes of telemetry collection 53

Diagnostics for troubleshooting telemetry collection and upload issues 57

Data governance 68

Licensing 70

Licensing 80

System requirements 82

Getting started 95

Enhanced Graphical User Interface 98

Deploy 106

Prerequisites for installing NetScaler Console 108

NetScaler Console on Citrix Hypervisor 109

NetScaler Console on Microsoft Hyper-V 112

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

NetScaler Console on VMware ESXi **118**

Automate deployment of NetScaler® agent on VMware ESXi **124**

NetScaler Console on Kubernetes cluster **136**

NetScaler Console on Linux KVM server **139**

NetScaler Console on Nutanix hypervisor (Acropolis) **145**

NetScaler Console on Azure Cloud **152**

NetScaler Console HA pair on Azure Cloud **154**

NetScaler Console on Amazon Web Services (AWS) **158**

Configure high availability deployment **159**

Configure disaster recovery for high availability **172**

Configure disaster recovery for standalone node **181**

Configure on-prem agents for multisite deployment **189**

Install a NetScaler® agent as a microservice on a Kubernetes cluster **198**

Upgrade agents **200**

Migrate NetScaler Console single-server deployment to a high availability deployment **202**

Migrate from NetScaler Insight Center to NetScaler Console **204**

Integrate NetScaler Console with Citrix Director **206**

Attach an extra disk to NetScaler Console **208**

NetScaler MPX™ disk encryption through NetScaler Console **220**

Behavior of NetScaler MPX™ HA pair after encryption **229**

Behavior of NetScaler MPX™ cluster after encryption **230**

NetScaler Console Cloud Connect **232**

Configure **238**

Add instances to NetScaler Console **239**

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

Add NetScaler VPX instances deployed in cloud to NetScaler Console **250**

Manage licensing and enable analytics on virtual servers **252**

Configure analytics on virtual servers **261**

Assign a net profile for the managed NetScaler instance **269**

Configure NTP server **270**

Configure system settings **271**

Integrate NetScaler Console with the ServiceNow instance **274**

Export or schedule export reports **280**

Upgrade **282**

Authentication **286**

Add LDAP authentication server **289**

Add RADIUS authentication server **291**

Add TACACS authentication server **293**

Users in NetScaler Console **295**

Extract an authentication server group **296**

Enable external authentication servers and fallback options **296**

Two factor authentication (2FA) support with LDAP, RADIUS, and TACACS **298**

Access Control **303**

Role-based access control **304**

Configure access policies **306**

Configure groups **309**

Configure roles **321**

Configure users **322**

Actionable tasks and recommendations **324**

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

A unified dashboard to view instance key metric details **335**

Create custom dashboards to view instance key metric details **345**

Applications **349**

Web Insight dashboard **351**

View the root cause for application latency **356**

Service Graph **360**

StyleBooks **363**

Application Security Dashboard **365**

Unified Security dashboard **368**

View application security violation details **379**

View API analytics **380**

Discover API endpoints **389**

Gateway Insight **390**

Troubleshoot Gateway Insight issues **409**

HDX™ Insight **413**

Enabling HDX™ Insight data collection **420**

Enable data collection for NetScaler Gateway appliances deployed in single-hop mode **434**

Enable data collection to monitor NetScalers deployed in transparent mode **436**

Enable data collection for NetScaler Gateway appliances deployed in double-hop mode **438**

Enable data collection to monitor NetScalers deployed in LAN user mode **443**

Create thresholds and configure alerts for HDX™ Insight **446**

Viewing HDX™ Insight reports and metrics **451**

Sessions **469**

Active Sessions **470**

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

Active Sessions **476**

Active Apps **476**

Active Sessions **479**

Active Apps **479**

Application View Reports and Metrics **496**

Sessions **497**

Active Sessions **499**

Desktop View Reports and Metrics **504**

Active Sessions **505**

Active Apps **505**

Active Sessions **508**

Active Apps **508**

User View Reports and Metrics **516**

Active Sessions **517**

Active Apps **517**

Active Sessions **519**

Active Apps **519**

Instance View Reports and Metrics **534**

License View Reports and Metrics **541**

Troubleshoot HDX™ Insight issues **542**

Infrastructure Analytics **555**

View instance details in Infrastructure Analytics **579**

View the capacity issues in a NetScaler instance **586**

Enhanced Infrastructure Analytics with new indicators **589**

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

Instance management **592**

Monitor globally distributed sites **595**

How to create tags and assign to instances **600**

How to search instances using values of tags and properties **603**

Centralized GeoIP DB Updates through NetScaler® Console **606**

Manage admin partitions of NetScaler instances **609**

Create a NetScaler high-availability pair **614**

Back up and restore NetScaler instances **618**

Force a failover to the secondary NetScaler instance **625**

Force a secondary NetScaler instance to stay secondary **627**

Create instance groups **628**

Provision NetScaler VPX instances on SDX using NetScaler Console **629**

Provision NetScaler VPX instances on VMware ESX **640**

Rediscover multiple NetScaler VPX instances **650**

Unmanage an instance **650**

Trace the route to an instance **651**

View NetScaler-owned IP addresses **652**

Replicate configurations from one NetScaler instance to another **657**

SSL certificate management **658**

Automated certificate renewal by using the ACME protocol **666**

Zero-touch certificate management **684**

Use the SSL Dashboard **687**

Set up notifications for SSL certificate expiry **694**

Update an installed certificate **696**

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

Install SSL certificates on a NetScaler instance **698**

Create a Certificate Signing Request (CSR) **700**

Link and unlink SSL certificates **703**

Configure an enterprise policy **703**

Poll SSL certificates from NetScaler instances **704**

Use the NetScaler Console certificate store to manage SSL certificates **706**

Manage database custom certificates and ciphers in a high-availability deployment **708**

Events **711**

Use events dashboard **711**

Set event age for events **713**

Schedule an event filter **714**

Set repeated email notifications for events **716**

Suppress events **717**

Create event rules **718**

Modify the reported severity of events that occur on NetScaler instances **733**

View events summary **734**

Display event severities and SNMP trap details **735**

View and export NetScaler syslog messages **738**

Suppress syslog messages **741**

Configure prune settings for instance events **744**

Network functions **745**

Generate reports for load balancing entities **746**

Export or schedule export of network functions reports **748**

Network reporting **750**

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

Configuration jobs **761**

Create a configuration job **763**

View audit reports **766**

Audit configuration changes across instances **771**

Get configuration advice on network configuration **779**

Poll configuration audit of NetScaler® instances **780**

Generate configuration audit diff for ConfigChange SNMP Traps **782**

Configuration audit **782**

Upgrade jobs **783**

Use jobs to upgrade NetScaler® instances **796**

Security Advisory **812**

Secure configuration recommendations **816**

CVE Detection **820**

File integrity monitoring **824**

Supported CVEs through Security Advisory **825**

Identify and remediate vulnerabilities for CVE-2025-12101 **828**

Identify and remediate vulnerabilities for CVE-2025-8424 **830**

Identify and remediate vulnerabilities for CVE-2025-7776 **832**

Identify and remediate vulnerabilities for CVE-2025-7775 **834**

Identify and remediate vulnerabilities for CVE-2025-6543 **836**

Identify and remediate vulnerabilities for CVE-2025-5349 **838**

Remediate vulnerabilities for CVE-2025-5777 **840**

Remediate vulnerabilities for CVE-2024-8535 **844**

Remediate vulnerabilities for CVE-2020-8300 **849**

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

Remediate vulnerabilities for CVE-2021-22927 and CVE-2021-22920 **861**

Identify and remediate vulnerabilities for CVE-2021-22956 **871**

Identify and remediate vulnerabilities for CVE-2022-27509 **878**

Unsupported CVEs in Security Advisory **880**

Upgrade Advisory (Preview) **880**

Orchestration **882**

OpenStack: Integrating NetScaler instances **883**

NSX Manager: manual provisioning of NetScaler instances **887**

NSX Manager: auto provisioning of NetScaler instances **904**

Manage the Kubernetes Ingress configuration in NetScaler Console **915**

Configure IP address management (IPAM) **918**

Configure an action policy to receive application event notifications **922**

Observability Integration **933**

Integration with Splunk **934**

Integration with New Relic **946**

Integration with Microsoft Sentinel **950**

Configure NetScaler® instances for the export of insights to Prometheus using the default schema **971**

Configure the export of NetScaler® metrics and audit logs to Splunk **972**

Access control lists **974**

Use NetScaler Console audit logs for managing and monitoring your infrastructure **979**

License Activation Service **982**

License management **991**

Minimum and maximum capacity for Flexed and Pooled licensing **1002**

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

Flexed capacity license **1009**

Configure license **1013**

Flexed license dashboard **1023**

Flexed license reporting **1025**

Transition to Flexed licensing **1029**

Scenarios for Flexed or Pooled license expiry and connectivity issues behavior **1033**

Configure NetScaler Console server as the Flexed or Pooled license server **1037**

NetScaler Pooled capacity **1040**

Configure NetScaler Pooled capacity **1048**

Upgrade a perpetual license in NetScaler VPX to NetScaler Pooled capacity **1058**

Upgrading a perpetual license in NetScaler MPX to NetScaler Pooled capacity **1064**

Upgrade a perpetual license in a NetScaler SDX to NetScaler Pooled capacity **1074**

NetScaler Pooled capacity on NetScaler instances in cluster mode **1077**

Check in and check out NetScaler VPX and NetScaler BLX licenses **1081**

NetScaler virtual CPU licensing **1091**

Expected behaviors when issues arise **1098**

Manage system settings **1100**

Configure system backup settings **1105**

Configure proxy server settings **1106**

Configure an NTP server **1110**

Upgrade NetScaler Console **1111**

How to reset the password for NetScaler Console **1113**

Configure a secondary NIC to access NetScaler Console **1121**

Configure a secondary NIC to access NetScaler® agent **1123**

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

Configure syslog purging interval **1126**

Configure system prune and event prune settings **1127**

Enable shell access for non-default users **1129**

Recover inaccessible NetScaler Console servers **1130**

Assign a host name to a NetScaler Console server **1135**

Back up and restore your NetScaler Console server **1136**

VM snapshots of NetScaler Console in high availability deployment **1140**

View auditing information **1141**

Configure SSL settings **1142**

Monitor CPU, memory, and disk usage **1143**

Configure notification settings **1144**

Generate a tech support file **1149**

Configure a cipher group **1151**

Create SNMP trap destination, manager community, and users **1152**

Configure and view system alarms **1153**

Create SNMP managers and users for NetScaler agent **1157**

Configure agent settings **1162**

Use Data Storage Management dashboard **1163**

Understand your data storage **1164**

Manage your storage space **1170**

Data retention policy **1173**

NetScaler Console as an API proxy server **1175**

FAQs **1181**

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

Release notes

December 11, 2025

The NetScaler Console 14.1 release notes describe the new features, enhancements to existing features, and the known issues in a build. The release notes document for the 14.1 release includes the following sections:

- **What's New**: The new features and enhancements to existing features released in a build.
- **Known Issues**: The issues that exist in a build, and their workarounds, wherever applicable.
- **Fixed Issues**: The issues addressed in a build.

> **Note:**
>
> These release notes do not document security related fixes. For a list of security related fixes and advisories, see the security bulletin. NetScaler Console Security Advisory supports identification and remediation of CVEs. For more information about the latest and existing supported CVEs, see Supported CVEs through Security Advisory.

To view the release notes document for a specific build of release 14.1, click the corresponding link in the following table. When the release notes are updated for a build, the published date is also updated. The release notes published date might not be the same as the build GA date.

Release notes for NetScaler Console on-prem software version 14.1	Published date
Build 14.1-60.54	Dec 11, 2025
Build 14.1-56.71	Dec 05, 2025
Build 14.1-51.83	Dec 05, 2025
Build 14.1-47.46	Jul 02, 2025
Build 14.1-43.50	Feb 27, 2025
Build 14.1-38.53	Dec 18, 2024
Build 14.1-34.43	Oct 28, 2024
Build 14.1-29.63	Aug 19, 2024
Build 14.1-25.56	Jul 09, 2024
Build 14.1-21.60	Apr 28, 2024
Build 14.1-17.38	Mar 18, 2024
Build 14.1-12.34	Dec 19, 2023

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

Release notes for NetScaler Console on-prem software version 14.1	Published date
Build 14.1-8.50	Oct 10, 2023
Build 14.1-4.42	Aug 07, 2023

Migrate NetScaler Console on-prem to Citrix Cloud

November 28, 2025

You can migrate **NetScaler ADM 13.0 64.35 or a later version** to Citrix Cloud. If your NetScaler ADM has 12.1 or an earlier version, you must first upgrade to **13.0 64.35 or a later version** and then migrate to Citrix Cloud. For more information, see the Upgrade section.

> **Note:**
>
> NetScaler® ADM service is now renamed to NetScaler Console service. Our product UI and documentation are currently undergoing updates to reflect these changes. During this time, you may come across the older and newer names being referenced interchangeably. We thank you for your understanding during this transition.

NetScaler Console service through Citrix Cloud™ enables you to get:

- Faster releases, approximately every two weeks with latest feature updates.
- Machine-learning based analytics for application security and bot, performance, and usage.
- Various other features that are currently supported only in NetScaler Console service, such as peak and lean period analytics, machine-learning based analytics for application security and bot, application CPU analytics, and many more.

For a successful migration, you must:

- Ensure to have internet connection in NetScaler Console on-prem for Citrix Cloud accessibility
- Configure the NetScaler agent
- Get the client and secret CSV file from Citrix Cloud
- Validate the NetScaler Console licensing
- Migrate using a script

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

After you migrate from NetScaler Console on-prem to NetScaler Console service, if you want to again continue with NetScaler Console on-prem, you can use the rollback script. For more information, see Roll back to NetScaler Console on-prem.

Configure the NetScaler agent

To enable communications between NetScaler instances and NetScaler Console service, you must configure an agent. NetScaler agents are, by default, automatically upgraded to latest build. You can also select a specific time for the agent upgrade. For more information, see Configuring agent upgrade settings.

- If your existing NetScaler Console on-prem (standalone or HA pair) has no agents configured, you must configure at least one agent for NetScaler Console service.
- If your existing NetScaler Console on-prem (standalone or HA pair) has configured with on-premises agents for multisite deployments, you must configure the same number of agents for NetScaler Console service.

For more information on configuring an agent, see the Getting Started section.

Get the client and secret CSV file from Citrix Cloud

After you configure the agent, get the client and secret CSV file from the Citrix Cloud page:

1. Log on to citrix.cloud.com
2. Click the **Home** icon and select **Identity and Access Management**
3. From the **API Access** tab, enter a secure client name and click **Create Client**.
4. ID and Secret is generated. Click **Download** and save the CSV file in the NetScaler Console on-prem.

   For example, save the CSV file to the /var directory.

Validate the NetScaler Console service licenses

You must obtain licenses for NetScaler service.

- The VIP licenses in NetScaler Console service must be more than or equal to the on-premises VIP licenses.

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

> **Note**
>
> If VIP licenses are lesser, then virtual servers are selected randomly and the VIP-level configuration for NetScaler Console service fails.

- If you use NetScaler Console on-prem deployment as a license server, reallocate your licenses to NetScaler Console service before migration. For more information, see How to reallocate a license file.
- If you are using the pooled licenses in NetScaler Console on-prem, you must obtain the pooled licenses for NetScaler Console service and then allocate licenses to the NetScaler instances. For more information, see Configure Pooled Licensing. The following supported NetScaler versions enable you to modify the license allocation from NetScaler Console:
  - NetScaler SDX: 13.0 74.11 or later versions.
  - NetScaler VPX and MPX: 13.0 47.24 or later versions, 12.1 58.14 or later versions, and 11.1 65.10 or later versions.

Migrate using a script

- Using the NetScaler Console 82.x build, you can select the feature and then migrate.
- For NetScaler Console 76.x or later builds, the migration scripts (`servicemigrationtool.py` and `config_collect_onprem.py`) are available as part of the build, available at `cd /mps/scripts`.
- For NetScaler Console earlier than 76.x builds, you must download the migration scripts and copy the scripts in NetScaler Console on-prem.

> Note
>
> Ensure that the NetScaler Console on-prem has internet connectivity during migration.

1. Using an SSH client, log on to the NetScaler Console on-prem.

> Note
>
> For a NetScaler Console HA pair, log on to the primary node.

2. Type **shell** and press **Enter** to switch to bash mode.
3. Copy the client ID and secret CSV file. For example, copy the file to the /var directory.

   After you copy the CSV file, you can validate if the CSV file is present.

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

```
bash-3.2# cd /var
bash-3.2# pwd
/var
bash-3.2# ls -ltr secureclient.csv
-rw-r--r--  1 root  nobody  102 Dec 11 19:09 secureclient.csv
bash-3.2#
```

> Note
>
> For a NetScaler Console HA pair, copy the CSV file in the primary node.

4. For NetScaler Console on-prem **13.0 82.xx version**, run the following commands to complete the migration:

   a) `cd /mps/scripts`

   b) `python servicemigrationtool.py <path of ClientID/Secret File in on-premises NetScaler Console VM>`

   For example, `python servicemigrationtool.py /var/secureclient.csv`

   After you run the migration script, the tool displays the following options:

```
------------------------------------------------------------
Checking For Pre-requisites before we start the Migration
------------------------------------------------------------

The no.of Agents in ADM Service are :1


VIP licenses available in ADM Service are: 2

No.of Vservers Licensed in ADM on-prem are: 72


All the vServers licensed in ADM on-prem will not be licensed in ADM Service since licenses available in service is less.
vServers will be licensed randomly. Do you want to continue ? [Y|N] y


User has started rerunning the migration.Providing the all options


------------------------------------------------------------------------------
Citrix ADM on-prem to ADM Service Configuration Migration.
The following menu enables you to select the components to migrate.
Type the number of the component that you want to migrate, and then press Enter.
For example, type 1 if you want to migrate Management and Monitoring(M&M).
------------------------------------------------------------------------------

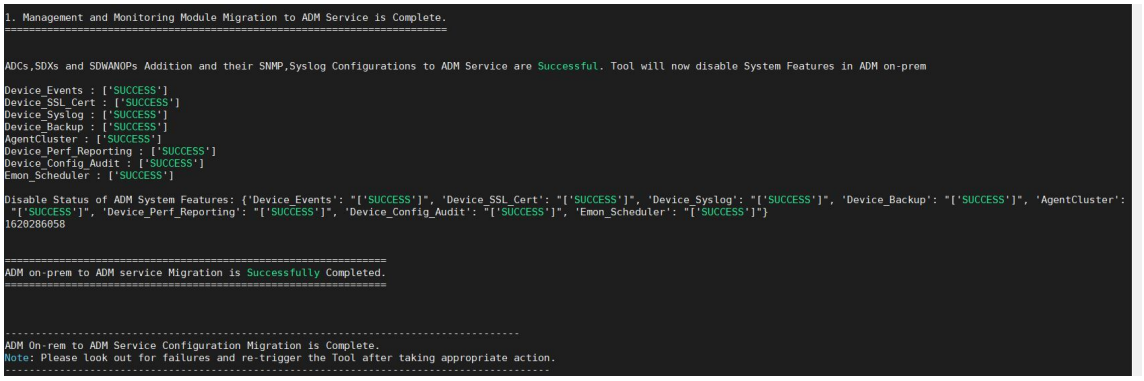
    1. Management and Monitoring(M&M).
    2. Analytics.
    3. Stylebooks.
    4. PooledLicensing.
    5. All.

Select an option from 1 to 5 [1]: 1
```

   Based on the choice you provide, only that feature gets migrated to NetScaler Console service.

   In the example, option 1 is selected. The tool completes the Management and Monitoring (M&M) migration and displays the following message:

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



The **Management and Monitoring (M&M)** feature includes:

- NetScaler Instances, tags, instance groups, profiles, custom apps, config jobs, SNMP, syslog configurations.
- Sites, IP blocks, network reporting, analytics thresholds, notification settings, data pruning settings.
- Config audit templates, polling intervals, event rules and settings.
- RBAC groups, roles, and policies

The **Analytics** feature includes:

- Appflow configuration per vserver from NetScaler instances.
- Appflow® configuration per SDWAN device.

> Note:
>
> - The Management and Monitoring (M&M) feature is automatically migrated, even if you select any other feature (2, 3, or 4).
> - You can specify only one feature at a time.
> - After you complete migrating any feature, if you want to migrate any other feature later, the feature that is already migrated is not shown in the list. For example, if you complete migrating the **Analytics** feature first, the next time you run the migration script, you can see only the **StyleBooks**, **Pooled Licensing**, and **All** options.
> - When you migrate pooled licensing, it migrates all types including vservers.

5. For NetScaler Console on-prem **13.0 76.xx version**, run the following commands to complete the migration:

   a) `cd /mps/scripts`

   b) `python servicemigrationtool.py <path of ClientID/Secret File in on-premises NetScaler Console VM>`

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

For example, `python servicemigrationtool.py /var/secureclient.csv`

6. For NetScaler Console on-prem earlier than 13.0 76.xx version:

   a) Download the migration script from the following location:
   `https://download.citrixnetworkapi.net/root/download/v1/public/software?product=admonprem&build=migrationtool&model=servicemigration.tgz`

   The downloaded file comprises two bundle scripts, `servicemigrationtool_27.py` and `config_collect_onprem_27.py`.

   b) Save the two scripts in NetScaler Console on-prem. For example, save in the /var directory

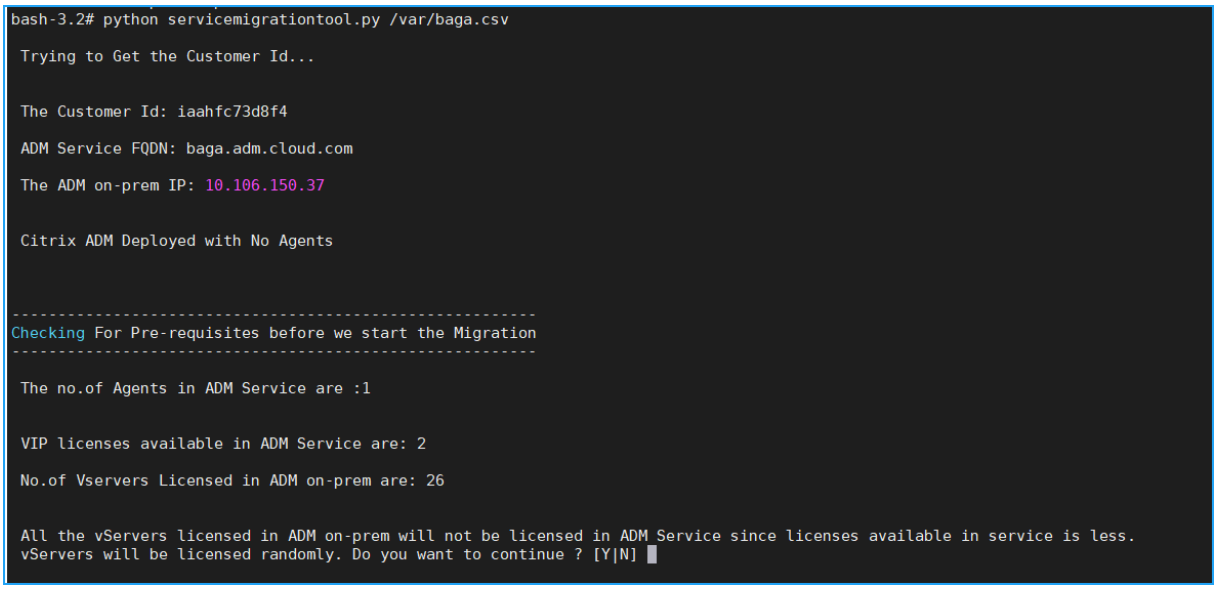
   c) Run the following commands to migrate:

      i. `cd /var`

      ii. `servicemigrationtool_27.py <path of ClientID/Secret File in NetScaler Console on-prem VM>`

      For example, `python servicemigrationtool_27.py /var/secureclient.csv`

After you run the script, it checks the prerequisites and then proceeds with the migration. The script first checks for the license availability. The following message is displayed only if you have lesser NetScaler Console service license than the on-premises license.



If you select **Y**, the migration continues by licensing the VIP randomly. If you select **N**, the script stops the migration.

If you have the unsupported NetScaler instance version for the pooled license server, the following message is displayed:

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

```
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Changing of PooledLicense Server will be effective for below SDX/ADC versions
--------------------------------------------------------------------------------
  For SDX Versions: 13.0 74.11 Onwards
  For ADC Versions: 13.0 47.24 and Onwards
                    12.1 58.14 and Onwards
                    11.1 65.10 and Onwards
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------

 The List of ADCs supported for Pooled License Server change are:
['10.106.150.73', '10.102.60.25']

 The List of SDXs supported for Pooled License Server change are:
[]

 The List of ADCs not supported for Pooled License Server change are:
[]

 The List of SDXs not supported for Pooled License Server chagne are:
['10.102.103.238']

 Migration will change the License Server to ADM Service Agent.
 Do you want to change License Server in all the supported Pooled ADCs/SDXs ? [Y|N] n

 Do you want to continue with rest of the migration ? [Y|N]
```

If you select **Y**, the migration process continues by changing the license server. If you select **N**, the script prompts if you want to proceed with rest of the migration. The script stops the migration if you select **N**.

Depending upon the on-premises configuration, the approximate time for the migration to complete is between a few minutes and a few hours. After the migration is complete, you see the following message:

```
--------------------------------------------------------------------------------
ADM OnPrem to ADM Service Configuration Migration is Complete.
Note: Please Look out for Failures and re-trigger the Tool after taking appropriate action.
--------------------------------------------------------------------------------
```

The migration is successful once all the NetScaler instances and their respective configurations are successfully moved to NetScaler Console service. After successful migration, the on-premises NetScaler Console stops processing the following instance events:

- SSL certificates
- Syslog messages
- Backup
- Agent cluster
- Performance reporting
- Configuration audit
- Emon scheduler

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

Roll back to NetScaler Console on-prem

If you want to roll back to NetScaler Console on-prem, ensure that the prerequisites are met.

Prerequisites

If your NetScaler Console on-prem (before migrating to NetScaler Console service) is:

- Used as a pooled license server, ensure you have the required pooled licenses in the NetScaler Console on-prem.
- Configured with NetScaler agents, ensure the agents are available in "UP"status.

Use the rollback script

> Note
>
> After rollback, the same configurations (before migration) in Analytics, SNMP, pooled licensing are again available in NetScaler Console on-prem. If you have made any changes to these configurations after migration, these changes are not reflected in NetScaler Console on-prem.

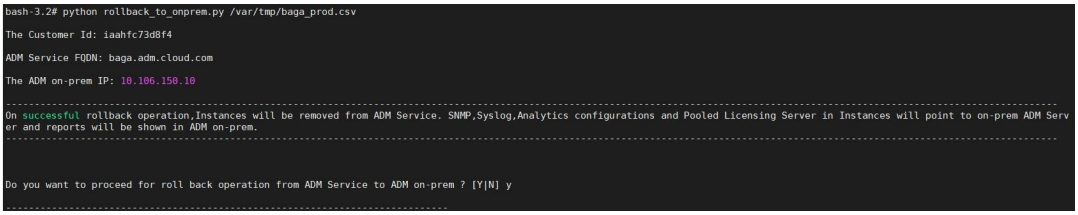
- For **NetScaler Console 82.xx or later** builds, the rollback script is available as part of the build and accessible at `/mps/scripts`.
- For **NetScaler Console earlier than 79.xx** builds, you can either upgrade to 82.x build and use the rollback script or you can download the rollback script and copy the script in NetScaler Console on-prem.

1. Using an SSH client, log on to the NetScaler Console on-prem.
2. Type shell and press Enter to switch to bash mode.
3. For NetScaler Console **13.0 82.xx** build, run the following commands to complete the rollback:
   a) cd /mps/scripts
   b) python rollback_to_onprem.py <path of ClientID/Secret File in NetScaler Console on-prem VM>

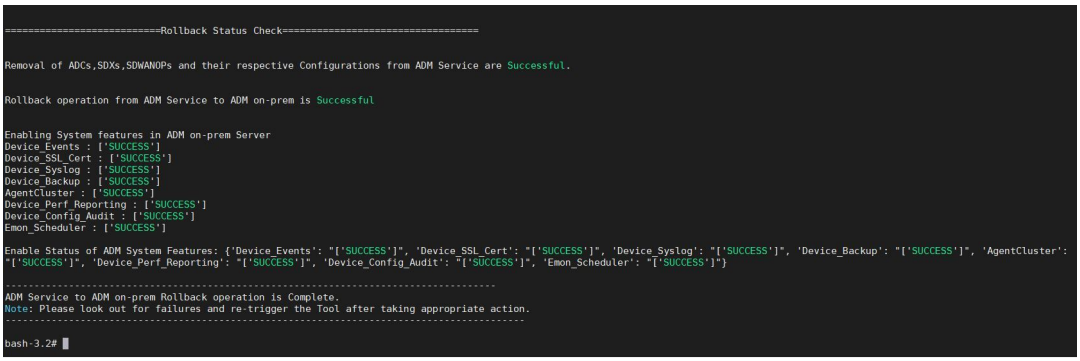
      For example, `python rollback_to_onprem.py /var/ secureclient.csv. csv`

      The tool initiates the rollback operation and a prompt asks if you want to proceed. Type **Y** to proceed.

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



You can see the following message after the rollback gets completed.



4. For NetScaler Console earlier than 82.xx build:

   a) Download the rollback script from the following location:

   `https://download.citrixnetworkapi.net/root/download/v1/public/software?product=admonprem&build=migrationtool&model=servicemigration.tgz`

   b) For NetScaler Console 79.xx and 76.xx builds, save the script in `/mps/scripts` and run the following commands to roll back:

      i. `cd /mps/scripts`

      ii. `python rollback_to_onprem.py < path of client/secret csv file in NetScaler Console on-prem>`

      For example, `python rollback_to_onprem.py /var/ secureclient.csv`

   c) For NetScaler Console earlier than 76.xx builds, save the script in NetScaler Console on-prem. For example, save it in the `/var` location and run the following commands to roll back:

      i. `cd /var`

      ii. `python rollback_to_onprem_27.py < path of client/secret csv file in NetScaler Console on-prem>`

      For example, `python rollback_to_onprem_27.py /var/secureclient.csv`

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

The tool initiates the rollback operation and a prompt asks if you want to proceed. Type **Y** to proceed.

FAQs

September 27, 2025

NetScaler Console service

Is NetScaler agent optional similar to on-premises NetScaler agent?

No. Agent is mandatory for NetScaler Console service and all communications between instances and NetScaler Console service happen through the agent. In NetScaler Console on-prem, agent is optional; however, you can configure an agent only for saving bandwidth consumption.

Why NetScaler Console service?

NetScaler Console service through Citrix Cloud provides the following benefits, without the need for new periodic builds:

- Cloud-based SaaS offering with easier onboarding and lesser cost of ownership than the on-premises NetScaler Console.
- Faster releases, approximately every two weeks with latest feature updates.
- Machine-learning based analytics for application security, performance, and usage.
- Various other features that are currently supported only in NetScaler Console service, such as peak and lean period analytics, machine-learning based application security analytics for WAF and bot, application CPU analytics, and many more.

What happens after migration if on-premises NetScaler Console is an HA pair?

All configurations are moved to Citrix Cloud. Configuring a disaster recovery node is not required.

What happens if the agent goes down for any reason?

You can expect a potential data loss until the agent is up and running. However, you can also configure NetScaler agents for multisite deployments to ensure continuity if there is an agent failover. For more information, see Configure agents for multisite deployment.

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

Is instance backup also migrated?

Backup is not included in migration.

Is historical data also migrated?

Historical data is not migrated. You can export the data from the NetScaler Console on-prem.

Are on-prem licenses also migrated?

No. The on-prem license file cannot be used for NetScaler Console service. You must obtain licenses for NetScaler Console service. For more information, see Licensing. If you are using pooled licenses in NetScaler Console on-prem, you must obtain pooled licenses for NetScaler Console service and then allocate licenses to instances.

What is not migrated from on-premises NetScaler Console?

The following features cannot be migrated to NetScaler Console service:

- **RBAC** –In NetScaler Console service, the user access is based on the invite from the administrator. NetScaler Console service users must have an account in Citrix Cloud. As a result, the NetScaler Console on-prem users are not migrated.
- **Export schedules** –Export schedules include details such as drill-down and schedules from various pages. All these detailed export schedules are not migrated.
- **SSL Certificates/Keys/CSRs** –NetScaler Console service can only display the NetScaler SSL certificates/Keys/CSRs. As a result, SSL certs/keys uploaded to on-premises NetScaler Console won't be migrated to NetScaler Console service.

On-premises NetScaler Console is integrated with Citrix Director. What happens to the integration?

Director integration with NetScaler Console is currently supported only in NetScaler Console on-prem.

After migration, is it again required to license the instance or to enable analytics?

You must ensure that the licenses in NetScaler Console service are more than or equal to the on-premises VIP licenses. If the licenses are already more than the on-premises NetScaler Console VIP, the virtual servers are automatically licensed. If not, the licenses are assigned randomly.

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

Migration tool

After running the migration script, error messages are displayed. What can be the issue?

A log file with failure reasons is displayed. You can take appropriate corrective actions and run the migration script again. In general, before you run the migration script, ensure to:

- Configure the NetScaler® agent
- Obtain the NetScaler Console service licenses
- Copy the correct path where you have stored the client and secure CSV file

The NetScaler instances have lower versions than the mentioned limitation for pooled licensing. What happens if the option 'Y'is selected to change the license server?

Change of license server happens only for the supported NetScaler MPX, VPX, and SDX versions.

What happens if the migration script has failed configuration regarding NetScaler instances?

The NetScaler instances continue to work on the NetScaler Console on-prem setup. You can take necessary action from the suggested failed reason and run the migration script again.

What happens if a few of the NetScaler instances fail to move to NetScaler Console service. Will rerunning the migration script help?

Yes. After you rerun the script, only the failed instances are migrated. Let's assume that two out of five instances have failed to move. After you have taken corrective actions and rerun the migration script, three instances that were moved successfully earlier show the "Device already exists"message. And the other two instances that failed earlier are migrated successfully.

Is there a log file to check the migration status?

Yes, a log file is generated in the `/var/mps/log/` directory. NetScaler Console with python3.7 has the log file as `servicemigrationtool.py.log` and NetScaler Console with python 2.7 has the log file as `servicemigrationtool_27.py.log`.

What happens if the session gets terminated while running the migration script?

You can rerun the migration script. In the new session, the already added instances from the last session display as "Device already exists", and the migration continues further.

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

What happens if NetScaler Console service has lesser licenses than the on-premises NetScaler Console and the migration script is initiated?

After the migration script is run, a suggestion appears, mentioning about the licenses are lesser and prompts to continue or stop. If you want to continue with lesser licenses, the virtual servers are licensed randomly from the available licenses.

What happens when on-premises NetScaler Console is migrated to the NetScaler Console service Express Account?

The NetScaler Console service Express Account has only two virtual server licenses, two StyleBook config packs, and two configuration jobs. If your NetScaler Console on-prem has more than these configurations and you initiate the migration with Express Account, the script can migrate only the mentioned configurations applicable for Express Account (two virtual server licenses, two StyleBook config packs, and two configuration jobs)

What happens if a Citrix Cloud invited user (other than Admin User who created Citrix Cloud account) tries to migrate NetScaler Console on-prem setup?

It is recommended that the administrator to run the migration script. An invited user does not have admin privileges (adminExceptSystem_group). As a result, groups, roles, and policies migration fail and the message "User doesn't have permission"is displayed.

As a solution, the administrator (who created the Citrix Cloud account) can change the group associated with invited user as "admin_group".

Rollback script

What happens if rollback script is used in NetScaler Console on-prem HA pair?

The NetScaler Console on-prem HA pair is restored with all configurations that were available before migration.

What happens to Disaster Recovery node after using the rollback script?

Disaster recovery node is also restored with all configurations before migration.

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

Troubleshooting

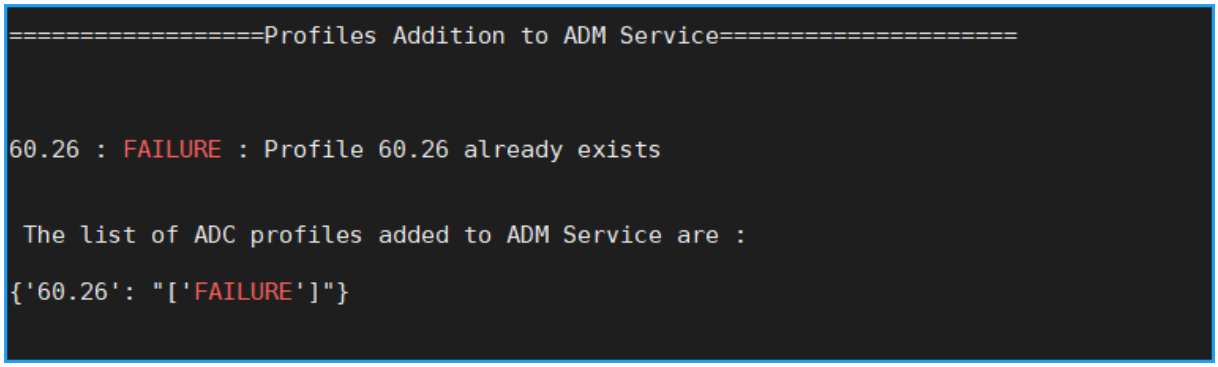
September 27, 2025

When you run the migration script for the first time, it checks for the prerequisites and proceeds with the migration. If all prerequisites are met, the migration completes without any errors. If any prerequisite fails, the script displays error messages with reasons. After fixing the errors, you must rerun the script again.

> Note
>
> If you see an error message that displays "already exists", it means that:
>
> - You might have run the migration script for more than one time and some configurations are already migrated to NetScaler Console service.
> - You might have manually created the same configuration in NetScaler Console service, before running the migration script.

Refer to some of the following error messages:

Manual profile added to NetScaler Console service



Workaround: If you have created admin profiles in NetScaler Console service before running the migration script, ensure to delete those profiles and rerun the migration script.

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

NetScaler device added to NetScaler Console service

```
==============ADC Device Addition================

10.106.150.53 : FAILURE : Error in contacting Citrix ADC, invalid credentials.
10.102.60.26 : FAILURE :Device with this IP address already exists.


The list of ADCs added to ADM Service are:


['10.102.60.26']
```

Workaround: In NetScaler Console, ensure the instance status and see if you can access the instance without any issues. If any issue persists, fix the issue, and rerun the migration script.

StyleBook custom templates import to NetScaler Console service

```
==============Stylebook custom templates Import to ADM Service====================


neustar.citrix.adc.stylebooks_5.0_appfw-signature : FAILURE : There is an existing StyleBook with same namespace, version and name.

neustar.citrix.adc.stylebooks_5.0_customer-template : FAILURE : There is an existing StyleBook with same namespace, version and name.

 Custom stylebooks import status is:{'neustar.citrix.adc.stylebooks_5.0_appfw-signature': 'FAILURE', 'neustar.citrix.adc.stylebooks_5.0_customer-template': 'FAILURE'}
==============Stylebook repository Addition to ADM Service=====================
```

Workaround: This error message is an example for the already migrated StyleBook. You can also see this error if you have manually created a StyleBook with the same name, version, and namespace, in NetScaler Console service before running the migration script.

Configuration Jobs added to NetScaler Console service

```
==============Config Jobs Addition to ADM Service====================


config_job2_show_ns_ip : FAILURE : Express user can have maximum 2 config jobs

ConfigJob1_show_ha_node : FAILURE : Express user can have maximum 2 config jobs

 The config jobs status is :
{'config_job2_show_ns_ip': 'FAILURE', 'ConfigJob1_show_ha_node': 'FAILURE'}
```

Workaround: This error occurs if you have subscribed to Express Account and have more than two configuration jobs. You must obtain a valid subscription to have all your configuration jobs to be migrated.

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

IP blocks added to NetScaler Console service

```
====================IP Blocks Addition in ADM Service=======================


ipblock1 : FAILURE : IP Block Name ipblock1 already exists

ipblock3 : FAILURE : IP Block Name ipblock3 already exists

test : FAILURE : IP Block Name test already exists
```

Workaround: Delete the IP block that is manually created in NetScaler Console service and rerun the migration script.

Network dashboard report addition status

```
================Network Dashboard Reports Addition to ADM Service=================


new456 : FAILURE : Dashboard new456 already exists

new123 : FAILURE : Dashboard new123 already exists

 The network dashoard reports addition status is:
{'new456': "['FAILURE']", 'new123': "['FAILURE']"}
```

Workaround: Delete the dashboard that is manually created in NetScaler Console service and rerun the migration script.

All how to articles

September 27, 2025

NetScaler Application Delivery Management (NetScaler Console) “How-to Articles”are simple, relevant, and easy to implement articles on the features of NetScaler Console. These articles contain information about some of the popular NetScaler Console features such as instance management, application management, StyleBooks, certificate management, and Analytics.

Click a feature name in the table below to view the list of how-to articles for that feature.

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

Topics				
Instance management	Event management	StyleBooks	Certificate management	NetScaler Console System
	Configuration management	Authentication	Analytics	Network functions

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 configure sites for Geomaps in NetScaler Console

How to force a failover to the secondary NetScaler instance by using NetScaler Console

How to force a secondary NetScaler instance to stay secondary by using NetScaler Console

How to back up and restore an instance using NetScaler Console

How to rediscover multiple NetScaler VPX instances

How to poll NetScaler instances and entities in NetScaler Console

How to unmanage an instance on NetScaler Console

How to trace the route to an instance from NetScaler Console

Configuration management

How to create a configuration job on NetScaler Console

How to use SCP (put) command in configuration jobs

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

How to reuse executed configuration jobs

How to upgrade NetScaler instances using NetScaler Console

How to use variables in configuration jobs on NetScaler Console

How to use configuration templates to create audit templates on NetScaler Console

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

How to create configuration jobs from corrective commands on NetScaler Console

How to replicate running and saved configuration commands from one NetScaler instance to another on NetScaler Console

How to use Record-and-Play to create configuration jobs

How to use configuration jobs to replicate configuration from one instance to multiple instances

How to use the master configuration template on NetScaler Console

How to poll configuration audit of NetScaler instances

How to reuse configuration audit templates in configuration jobs

How to import and export configuration templates

How to generate configuration audit diff for ConfigChange SNMP traps

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

How to poll SSL certificates from NetScaler Instances

StyleBooks

How to view different groups of StyleBooks

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 files to NetScaler Console

How to use API to create configurations to upload any file type

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

How to create a StyleBook to upload SSL certificate and certificate key files to NetScaler Console

How to use API to create configurations to upload cert and key files

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

Analytics

How to enable analytics on instances

How to configure adaptive thresholds

How to configure SLA management

How to configure database summarization for analytics

How to create thresholds and alerts using NetScaler Console

How to disable URL data collection for analytics from NetScaler Console

How to view the type of videos streamed and the data volume consumed from your network

How to view the peak data rate for a particular time frame

How to view the network efficiency

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

How to configure prune settings for instance events

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

Authentication

How to enable fallback and cascade external authentication servers

How to add RADIUS authentication servers

How to add LDAP authentication servers

How to add TACACS authentication servers

How to extract authentication server group in NetScaler Console

How to enable fallback local authentication

NetScaler Console system

How to upgrade NetScaler Console

How to reset the password for NetScaler Console

How to generate a tech support file for NetScaler Console

How to back up and restore your NetScaler Console server in a single server deployment

How to back up and restore a NetScaler Console configuration in an HA pair

How to enable shell access for non-default users in NetScaler Console

How to configure NTP server on NetScaler Console

How to configure SSL settings for NetScaler Console

How to configure syslog purging interval for NetScaler Console

How to view auditing information of NetScaler Console

How to configure system notification settings of NetScaler Console

How to monitor CPU, memory, and disk usage of NetScaler Console

How to configure a cipher group for NetScaler Console

How to create SNMP traps, managers, and users on NetScaler Console

How to assign a host name to a NetScaler Console server

How to configure system prune settings for NetScaler Console

How to configure system backup settings by using NetScaler Console

How to configure and view system alarms on NetScaler Console

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

Network functions

How to generate reports for load balancing entities

How to export or schedule export of network functions reports

Overview

September 27, 2025

> **Note:**
>
> Starting from 14.1 17.x build, NetScaler ADM is rebranded to NetScaler Console. For earlier builds, the product name is NetScaler ADM.

NetScaler Console is a centralized management solution that simplifies operations by providing administrators with enterprise-wide visibility and automating management jobs that need to be run across multiple instances. You can manage and monitor NetScaler products that include NetScaler MPX, NetScaler VPX, NetScaler SDX, NetScaler CPX and NetScaler Gateway. You can use NetScaler Console to manage, monitor, and troubleshoot the entire global application delivery infrastructure from a single, unified console.

NetScaler Console is a virtual appliance that runs on Citrix Hypervisor, VMware ESXi, and Linux KVM. NetScaler Console addresses the application visibility challenge by collecting the following detailed information about web-application and virtual-desktop traffic:

- user-session-level information
- Webpage performance data
- database information flowing through the NetScaler instances at your site and provides actionable reports.

NetScaler Console enables IT administrators to troubleshoot and proactively monitor customer issues in a matter of minutes.

Features and solutions

September 27, 2025

NetScaler Console provides the following features:

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

Application Analytics and Management

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 the systems up and running.

Application security analytics

The App Security Dashboard provides a holistic view of the security status of your applications. For example, it shows key security metrics such as security violations, signature violations, threat indexes. App Security dashboard also displays attack related information such as SYN attacks, small window attacks, and DNS flood attacks for the discovered NetScaler instances.

Networks

Instances

Enables you to manage the NetScaler and NetScaler Gateway instances.

Instance groups

Enables you to group your instances as follows:

- Static Group: Allow you to define a device group that you can use in different tasks such as, Configuration Jobs and so on.
- Private IP-block: Enables you to group your instances based on geographical locations.

Event management

When the IP address of a NetScaler instance is added to NetScaler Console, a NITRO call is sent by NetScaler Console 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.

Certificate management

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 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.

Configuration management

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

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

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.

Network reporting

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

Analytics

Web Insight

Provides visibility into enterprise web applications and allows IT administrators to monitor all web applications being served by the NetScaler by providing integrated and real-time monitoring of applications. Web Insight provides critical information such as user and server response time, enabling IT organizations to monitor and improve application performance.

HDX Insight

Provides end-to end visibility for ICA traffic passing through NetScaler. HDX Insight enables administrators to view real-time client and network latency metrics, historical reports, End-to-end performance data, and troubleshoot performance issues.

Gateway Insight

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.

SSL Insight

SSL Insight provides visibility into secure web transactions (HTTPS) and allows IT administrators to monitor all the secure web applications being served by the NetScaler by providing integrated and real-time and historic monitoring of secure web transactions.

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

TCP Insight

TCP Insight provides an easy and scalable solution for monitoring the metrics of the optimization techniques and congestion control strategies (or algorithms) used in NetScaler instances to avoid network congestion in data transmission.

Video Insight

The Video Insight feature provides an easy and scalable solution for monitoring the metrics of the video optimization techniques used by NetScaler instances to improve customer experience and operational efficiency.

Orchestration

Cloud Orchestration

Enables integration of NetScaler products with OpenStack cloud orchestration. NetScaler Console and OpenStack implement each other's APIs, enabling integration of the NetScaler instance's Load Balancing feature (LBaaS) with OpenStack cloud orchestration.

Orchestration

NetScaler Console supports SDN in the enterprise network by integrating with SDN controllers of different vendors. NetScaler Console supports both VMware NSX Manager and Cisco Application Policy Infrastructure Controller (APIC).

Architecture

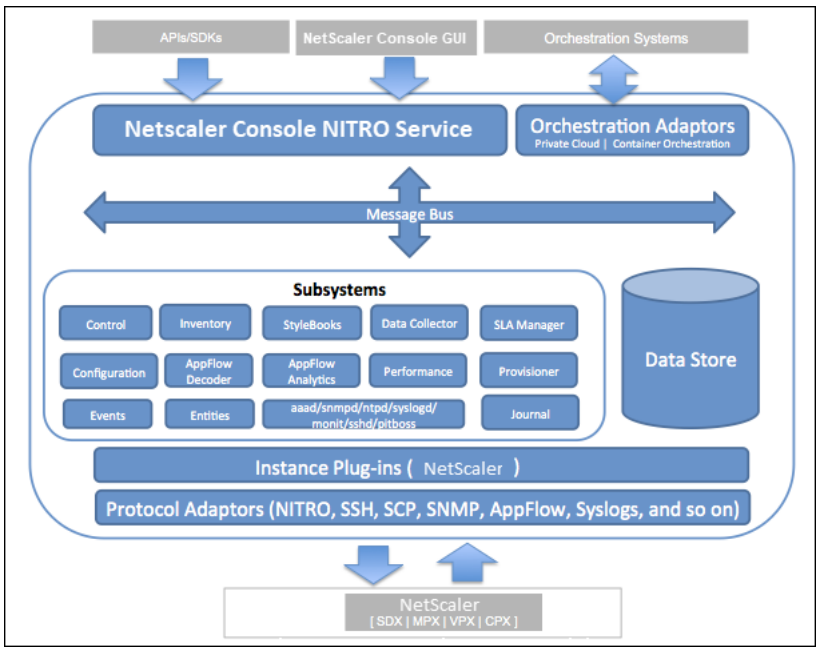
September 27, 2025

The NetScaler Console database is integrated with the server, and the server manages all the key processes, such as data collection, NITRO calls. In its data store, the server stores an inventory of instance details, such as host name, software version, running and saved configuration, certificate details, entities configured on the instance. A single server deployment is suitable if you want to process small amounts of traffic or store data for a limited time.

Currently, NetScaler Console supports two types of software deployments: single server and high availability.

The following image shows the different subsystems within NetScaler Console and how communication happens between the NetScaler Console server and managed instances.

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



The Service subsystem in NetScaler Console acts as a web server that handles HTTP requests and responses that are sent to subsystems within NetScaler Console from the GUI or API, using ports 80 and 443. These requests are sent to the subsystems over the message bus (message processing system) by using the IPC (inter-process communication) mechanism. A request is sent to the Control subsystem, which either processes the information or sends it to the appropriate subsystem. Each of the other subsystems—Inventory, StyleBooks, Data Collector, Configuration, AppFlow Decoder, AppFlow Analytics, Performance, Events, Entities, SLA Manager, Provisioner, and Journal—has a specific role.

Instance plug-ins are shared libraries that are unique to each instance type supported by NetScaler Console. Information is transferred between NetScaler Console and managed instances by using NITRO calls, or through the SNMP, Secure Shell (SSH), or Secure Copy (SCP) protocol. This information is then processed and stored in the internal database (data store).

How NetScaler Console discovers instances

September 27, 2025

Instances are NetScaler appliances or virtual appliances that you want to discover, manage, and monitor from NetScaler Console. To manage and monitor these instances, you must add them to the NetScaler Console server. You can add the following NetScaler appliances and virtual appliances to NetScaler Console:

- NetScaler instances
    - NetScaler MPX

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

- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler BLX

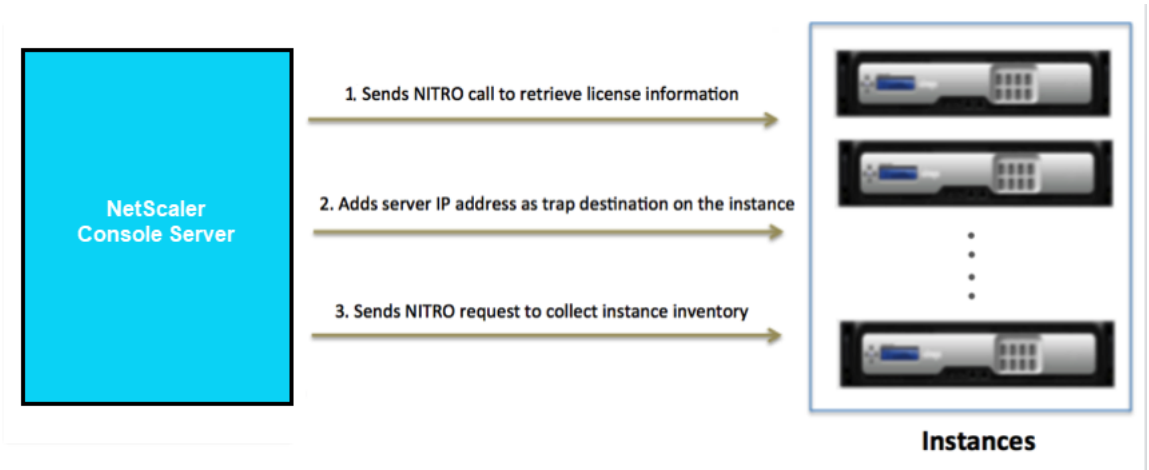
- NetScaler Gateway instances

You can add instances either while setting up the NetScaler Console server for the first time or later.

> **Note**
>
> NetScaler Console uses the NetScaler IP (NSIP) address of the NetScaler instances for communication. NetScaler Console can also discover NetScaler instances with a subnet IP (SNIP) address that has management access enabled on it. For information about the ports that must be open between the NetScaler instances and NetScaler Console, see Ports.
>
> If you want to add a NetScaler HA pair using SNIP, ensure to enable the Independent Network Configuration (INC) mode on the NetScaler HA pair. For more information to add instances, see Add instances.

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

The following diagram describes how NetScaler Console implicitly discovers and adds instances.



As shown in the diagram, the following steps are performed implicitly by NetScaler Console.

1. NetScaler Console uses the instance profile details to log on to the instance. Using a NetScaler NITRO call, NetScaler Console retrieves the license information of the instance. Based on the licensing information, it determines whether the instance is a NetScaler instance and the type of NetScaler platform (for example, NetScaler MPX, NetScaler VPX, NetScaler SDX, NetScaler BLX,

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

or NetScaler Gateway). On successful detection of the instance, it is added to the NetScaler Console database.

This step might fail if the instance profile does not include the correct credentials. For NetScaler MPX, NetScaler VPX, NetScaler SDX, NetScaler BLX, and NetScaler Gateway instances, this step might also fail if the licenses are not applied to the instance.

> **Note**
>
> Using HTTP, you can add all instances to NetScaler Console even if the licenses are not configured on the instances.

2. NetScaler Console adds its IP address to the list of trap destinations on the instance. This allows NetScaler Console to receive traps generated on the NetScaler instance.

   This step might fail if the number of trap destinations on the instance exceeds the maximum limit of trap destinations. The maximum limit on instances is 20.

3. NetScaler Console collects inventory from the instance by sending a NITRO request. It collects instance details such as host name, software version, running and saved configuration, certificate details, entities configured on the instance.

   This step might fail because of network or firewall issues.

   To learn to add instances to NetScaler Console, see Add instances.

Polling overview

September 27, 2025

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, and so on 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

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

- SSL certificate polling
- Entity polling

NetScaler Console uses protocols such as NITRO call, Secure Shell (SSH), and Secure Copy (SCP) to poll information from NetScaler instances.

How NetScaler Console polls managed instances and entities

NetScaler Console automatically polls at regular intervals by default. NetScaler Console also enables you to configure polling intervals for a few polling types and allows you to poll manually when required.

The following table describes the details of types of polling, polling interval, protocol used, and so on:

Polling type	Polling interval	Polled information	Protocol used	Polling interval configuration
Instance polling	Every 1 minute (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 calls and SSH	No
Performance data collection	Every 5 minutes (by default)	Network reporting information	NITRO call	No

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

Polling type	Polling interval	Polled information	Protocol used	Polling interval configuration
Instance backup polling	Every 12 hours (by default)	Backup file of the current state of the managed NetScaler instances	NITRO calls, SSH, and SCP.	Yes. Navigate to **Infrastructure > Instances > NetScaler**. Select the instance and from the **Select Action** list, click **Backup/Restore**.
Configuration audit polling	Every 10 hours (by default)	Configuration changes that occur on NetScaler instances (for example, running vs. saved configuration)	SSH, SCP, and NITRO call	Yes. Navigate to **Infrastructure > Configuration Audit**. On the Configuration Audit page, click **Settings** and configure the polling interval for Configuration Audit Polling.

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

Polling type	Polling interval	Polled information	Protocol used	Polling interval configuration
				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 Audit** and click **Poll Now**. The **Poll Now** page lets you to poll all or selected instances in the network.
SSL certificates polling	Every 24 hours (by default)	SSL certificates that are installed on NetScaler instances.	NITRO calls and SCP	Yes. Navigate to **Infrastructure > SSL Dashboard**. On the SSL Dashboard page, click **Settings** to configure the polling interval

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

Polling type	Polling interval	Polled information	Protocol used	Polling interval configuration
				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 to poll all or selected instances in the network.
Entity polling				
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.

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

Polling type	Polling interval	Polled information	Protocol used	Polling interval configuration
				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
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

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

> 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

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 30 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.

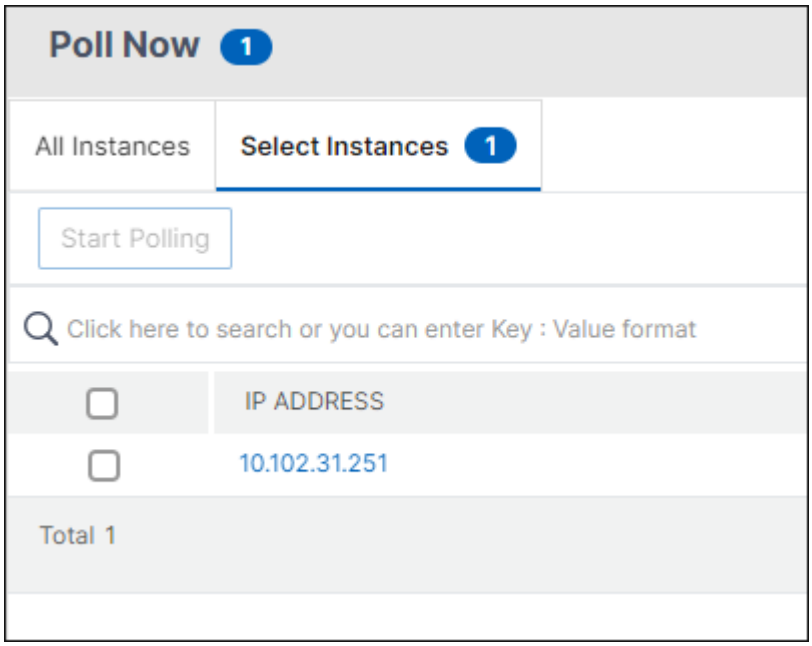
In NetScaler Console, there is a minimum polling interval period when automatic polling does not happen. If you add a new NetScaler instance, or if an entity is updated, NetScaler Console does not recognize the new instance or the updates made to an entity until the next polling happens. And, there is 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:

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

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 a particular instance. For example, you can use this option to know the latest status of a particular entity in an instance. In such a case, you need not poll the instance as a whole to know the status of 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 state 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 state is displayed on the GUI immediately.

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

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 **Infrasturcture > Network Functions > Load Balancing > Virtual Servers**.
2. Select the virtual server that shows the state as DOWN, and click **Poll Now**. The status of the virtual server now changes to UP.

NetScaler® telemetry program

September 27, 2025

Citrix collects basic license telemetry data and NetScaler deployment and feature usage telemetry data for its legitimate interests, including license compliance. You may automatically or manually upload the required license and feature usage data to remain compliant with the NetScaler telemetry program described here. NetScaler Console configuration and feature usage data is also collected to manage, measure, and improve Citrix products and services. If you are an existing NetScaler Console customer, you must ensure to be compliant with the NetScaler telemetry program. We highly recommend adding NetScaler instances to NetScaler Console to improve and simplify your NetScaler operations overall and support the enhancement of our products and services by sending NetScaler feature usage data. Learn more.

You can upload the required telemetry data using the following ways:

- **Automated collection mode** - This mode is enabled by default after you upgrade to **14.1 25.56 or later** / **13.1-53.22 or later** build. The automated mode creates an outbound connection to use the auto-enabled channel (endpoint URLs) and uploads the telemetry data automatically. You must only ensure that the endpoint URLs are reachable. Since the upload happens automatically, no action is required from your end unless the prerequisites fail. For more information, see Automated collection mode.

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

- **Manual collection mode** - This mode is enabled only if the automated mode is disabled. You must download the required telemetry data from the NetScaler telemetry home page in NetScaler Console on-prem and complete the first upload to NetScaler Console service within 30 days. The subsequent uploads must be done every 90 days to remain compliant. For more information, see Manual collection mode.

The recommendation is to use the automated telemetry mode and upload the required data automatically, but you can also choose to disable the automated mode and upload it manually. In both automated and manual modes, data upload is required to remain compliant with the NetScaler telemetry program. You may choose to disable the optional telemetry data from being included in the data upload, but the required license compliance and feature usage telemetry data must be provided in both the automated and manual modes.

To remain compliant, the number of days since the last successful upload must not be greater than 90 days.

As part of the NetScaler telemetry program, the following configurations were pushed to the managed NetScaler instances:

- AppFlow configuration: `enable ns feature AppFlow`
- Telemetry metrics profile configuration: `add analytics profile telemetry_metrics_profil -type timeseries -outputMode prometheus -metrics ENABLED -serveMode Pull -schemaFile "./telemetry_collect_ns_metrics_schema.json"-metricsExportFrequency 300`

> **Note:**
>
> For optimal telemetry collection, we recommend that you upgrade to the latest NetScaler Console build.

- Starting from **14.1-43.x** / **13.1-57.x** build, NetScaler Console removes the telemetry metrics profile configuration if it is present in your NetScaler instances. The removal of telemetry metrics profile configuration does not impact any existing features in your NetScaler instances.
- 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 following table provides details about the AppFlow® and Telemetry metrics profile configurations in the latest build and earlier builds:

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

Build	Configurations pushed as part of telemetry program	Telemetry mode	Action required
14.1-43.x / 13.1-57.x	No	Automated and manual	Configurations are not pushed to NetScaler instances and the telemetry metrics profile configuration is removed from NetScaler instances if it is present. If you are not using the NetScaler or NetScaler Console analytics features, you can use `disable ns feature AppFlow` to remove the AppFlow configuration.

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

Build	Configurations pushed as part of telemetry program	Telemetry mode	Action required
14.1-29.x / 13.1-55.x	No	Automated and manual	Configurations are not pushed as part of the NetScaler telemetry program. If these configurations are present in your NetScaler instances and you want to remove these configurations, run the `rm analytics profile telemetry_metrics_profile` command on NetScaler to remove the telemetry metrics profile configuration and use `disable ns feature AppFlow` to remove the AppFlow configuration.

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

Build	Configurations pushed as part of telemetry program	Telemetry mode	Action required
14.1-25.56 / 13.1-53.22	Yes. Both AppFlow and telemetry metrics profile configurations	Automated (with all prerequisites met)	Configurations are pushed as part of the NetScaler telemetry program, but not checked for every 24 hours. To remove these configurations, run the `rm analytics profile telemetry_metrics_profile` command on NetScaler to remove the telemetry metrics profile configuration and use `disable ns feature AppFlow` to remove the AppFlow configuration.

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

	Automated (with any prerequisites not met) or manual	NetScaler Console continues to check for these configurations every 24 hours and push it to NetScaler instances, if these configurations are missing. If you do not want the configurations to be pushed, you must be in the automated mode (with all prerequisites met) or upgrade to the latest build.

Notes:

- 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:

```
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:

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

Categories	Description	What do we use it for?	Required/Optional
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.	Required
NetScaler Console deployment and feature usage telemetry	Information about Console deployment and feature usage.	To manage, measure, and improve the service.	Optional

For more information about the list of optional and required telemetry parameters, see Data governance.

Citrix requires that you transition to the most recent NetScaler Console build (14.1 25.56 or later / 13.1–53.22 or later) within 3 months starting from **18th June 2024**. After upgrading to NetScaler Console 14.1 25.56 or later / 13.1–53.22 or later, one of the telemetry modes (automatic or manual) must be actively functioning. Unless you have elected manual reporting, you agree to adjust your firewalls as necessary to allow automatic telemetry reporting.

Points to note:

- You must ensure that you transition to the latest build (14.1–25.56 and later / 13.1–53.22 and later) by **18th September 2024**.
- If you opt for manual telemetry mode, the first upload must be completed within 30 days of your transition to the above build, but no later than 18th October 2024. Thereafter the manual telemetry upload must be done every 90 days for your NetScaler Console on-prem to be compliant with the NetScaler telemetry program.

Citrix may suspend or terminate your Citrix Support for non-compliance of these requirements without liability, in addition to any other remedies Citrix may have at law or equity. These requirements do not apply to the extent prohibited by law or regulation. For more information, see Citrix License Telemetry FAQ.

Modes of telemetry collection

October 10, 2025

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

Automated telemetry collection mode

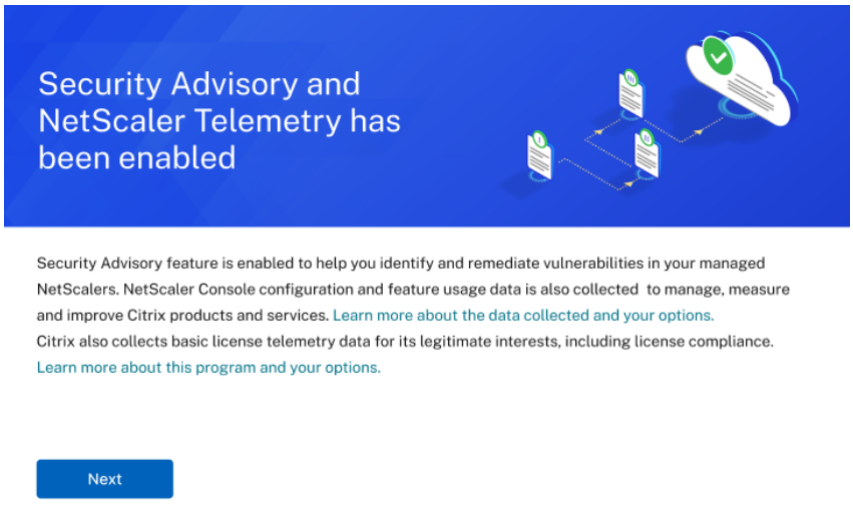
This mode is enabled by default after you upgrade to NetScaler Console on-prem 14.1 25.53 / 13.1-53.22 or later build.

Prerequisites for the automated telemetry collection mode:

- Ensure that you have an internet connection or have a proxy server configured in NetScaler Console on-prem for Citrix Cloud accessibility. For more information, see System Requirements.
- Ensure that the following endpoint URLs are reachable:
  - Download Service URL: `https://download.citrixnetworkapi.net`
  - Service URL: `https://adm.cloud.com` (required only in 14.1-43.x or earlier build).
  - Auto-enabled channel: `https://safehaven.adm.cloud.com`
- Ensure that the following port is open:

Port	Type	Details	Direct of communication
5140	UDP	Port to receive NetScaler Gateway telemetry data	NetScaler to NetScaler Console

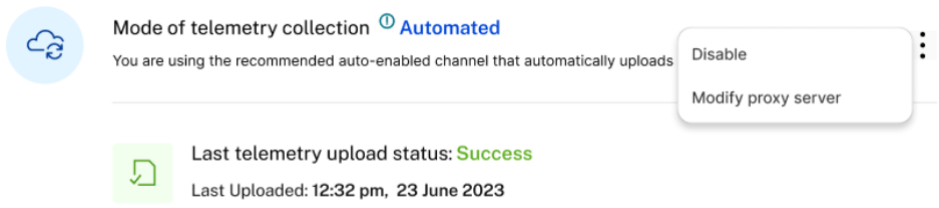
After you upgrade to 14.1-25.53 or 13.1-53.22 build and navigate to the **NetScaler Telemetry** page, click **Next** in the following pop-up window:



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

Manual telemetry collection mode

To use the manual telemetry collection mode, you must first disable **Security Advisory** and then click the vertical ellipse and select **Disable**.



In the pop-up window, click **I agree to upload the data manually** to disable the automated telemetry collection. The mode of telemetry collection is automatically changed to **Manual**. In the Manual telemetry mode, the new CVE updates are not available and you can only use the Security Advisory with the existing or the last updated CVEs.

After you opt for manual mode, you must download the telemetry and complete the first upload in NetScaler Console service within 30 days. The subsequent uploads are to be done every 90 days thereafter.

> **Note:**
>
> A maximum of 2 GB NetScaler Console disk space is utilized to save the 90 days of telemetry data.

From the **NetScaler Telemetry** homepage, click **Download Telemetry** to download the bundle (.tgz) file that comprises the required telemetry data.

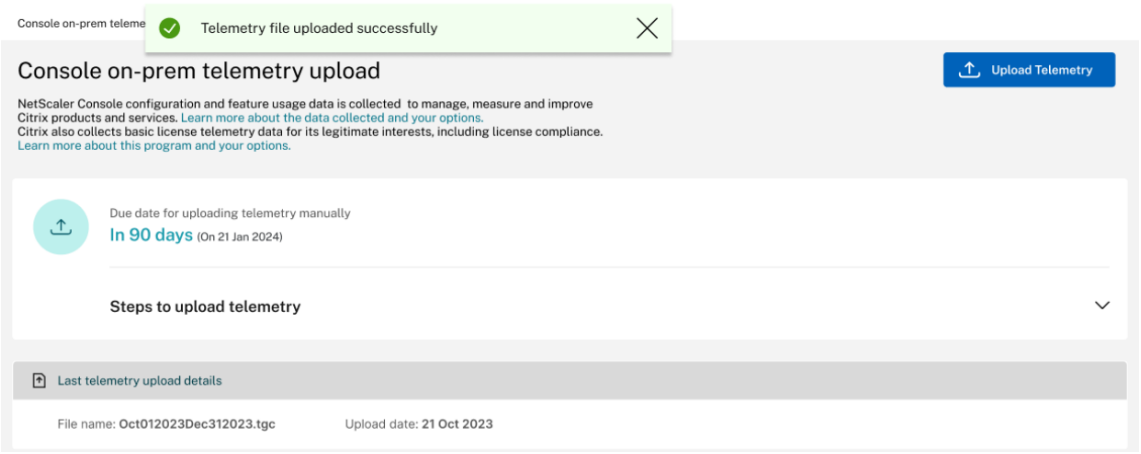


After you download the telemetry file, you must upload it to the NetScaler Console service. To upload in NetScaler Console service:

1. Log on to Citrix Cloud (citrix.cloud.com). If you do not have a Citrix Cloud account, sign up for a new account. For more information, see Create a Citrix Cloud account.
2. Select an account.
3. Under **NetScaler Console Service**, click **Manage**.
4. Set up a Console service account.
5. In NetScaler Console service, navigate to **Settings > Console on-prem telemetry upload**.
6. Click **Upload Telemetry** and select the downloaded (.tgz) file to complete the upload process.

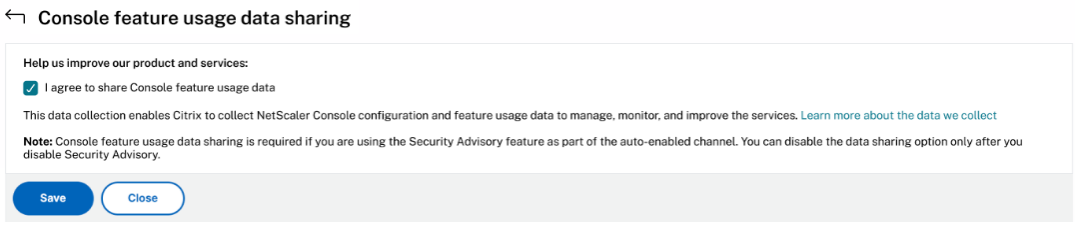
© 1997–2025 Citrix Systems, Inc. All rights reserved.

7. 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.
- You can disable uploading the optional telemetry data. To disable, 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.



- In your NetScaler Console on-prem, a reminder banner appears 7 days before the upload due date.

Notifications for telemetry uploads

By default, email notifications are enabled for telemetry uploads. The prerequisite to receive email notification is to configure an email distribution list. For more information, see Configure notification settings As an administrator, you receive email notifications for the following scenarios:

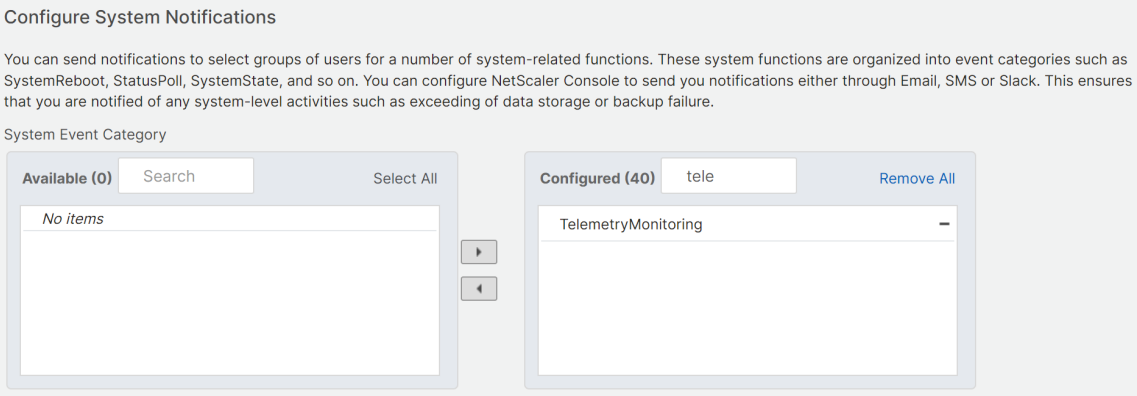
- **Upload failure through automated mode** - Email notification is received every 24 hours until the issue is resolved.

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

- **Upcoming deadline for manual upload** (only if enabled manual mode) - One email notification is received during the event and another email after the upload is complete.
- **Exceeded deadline for manual upload** (only if enabled manual mode) - One email notification is received during the event and another email after the upload is complete.

You can disable the email notification. To disable:

1. Navigate to **Settings > Administration > Configure Event Notification and Digest**.
2. In **Event Notification > Configure System Notifications**, search for **TelemetryMonitoring**, remove this notification, and click **Save**.



Diagnostics for troubleshooting telemetry collection and upload issues

October 13, 2025

Prior to release 14.1 build 56.x, the diagnostics helps to examine the outbound connectivity to these endpoint URLs and lets you know if they are in reachable status. NetScaler On-prem release 14.1 build 56.x and later provides enhanced diagnostics to identify and troubleshoot telemetry collection and upload issues at both collector level (Console) and device level (individual NetScaler instances).

Diagnostic behaviour from release 14.1 build 56.x onwards

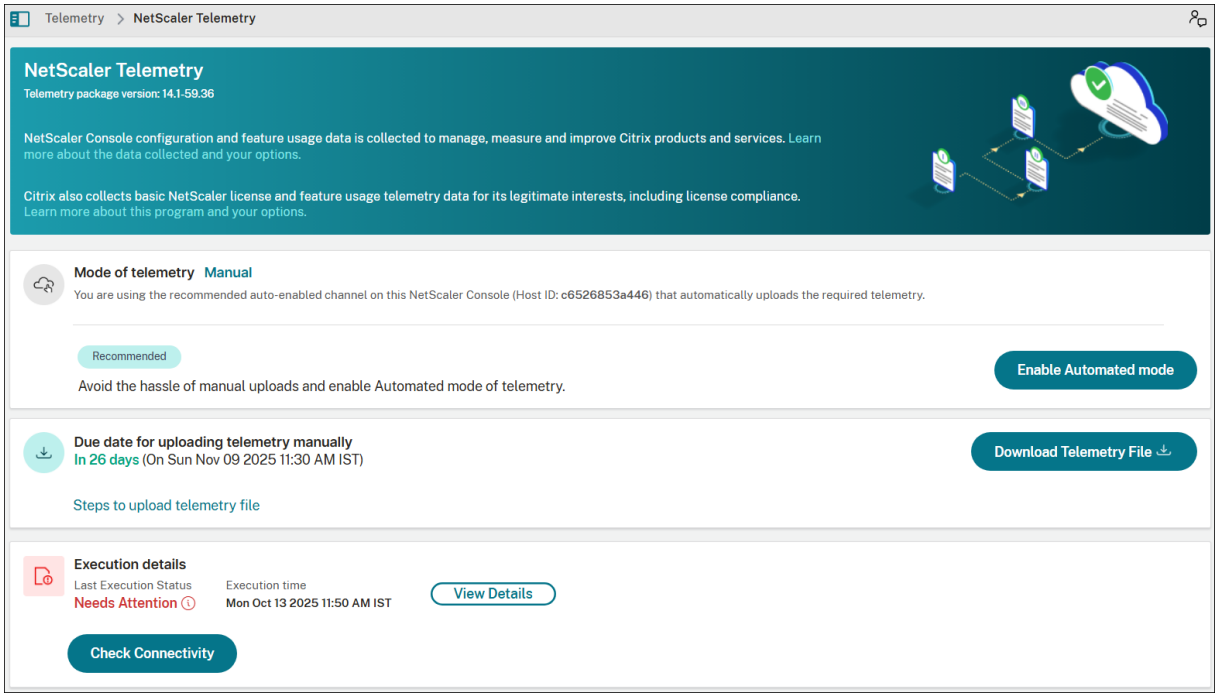
> Note:
>
> Starting from release 14.1 build 56.x,the telemetry diagnostics feature is enhanced to identify and troubleshoot telemetry collection and upload issues at both collector level (Console) and device level (individual NetScaler instances).

All managed NetScaler instances must send telemetry data to remain compliant. However, telemetry uploads and collection fails due to connectivity or configuration issues.

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

The Diagnostics capability on the NetScaler telemetry page of Console on-prem helps you quickly identify and troubleshoot issues at both levels:

- Collector level (Console): To check whether the data was successfully uploaded.
- Device level (individual NetScaler instances): To check whether the data was collected from NetScaler instances.



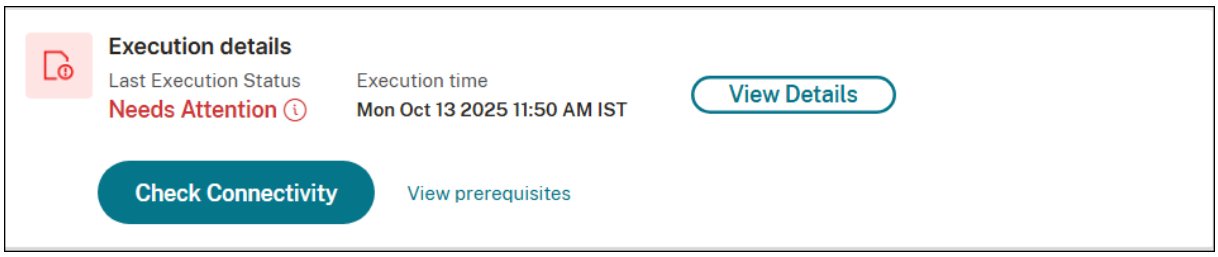
How it works

The following are the high-level steps involved in the diagnostics process:

- Automatic Run: Diagnostics run automatically every 24 hours.
- On-Demand Runs: Users can run diagnostics manually as needed, especially after attempting to fix an issue.
- Status Indicators: The results are displayed with clear statuses:
  - Success: No issues detected.
  - Needs Attention: One or more issues require user action.

> **Note:**
>
> Click **View Details** or on error-highlighted areas for in-depth error logs and mitigation steps.

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

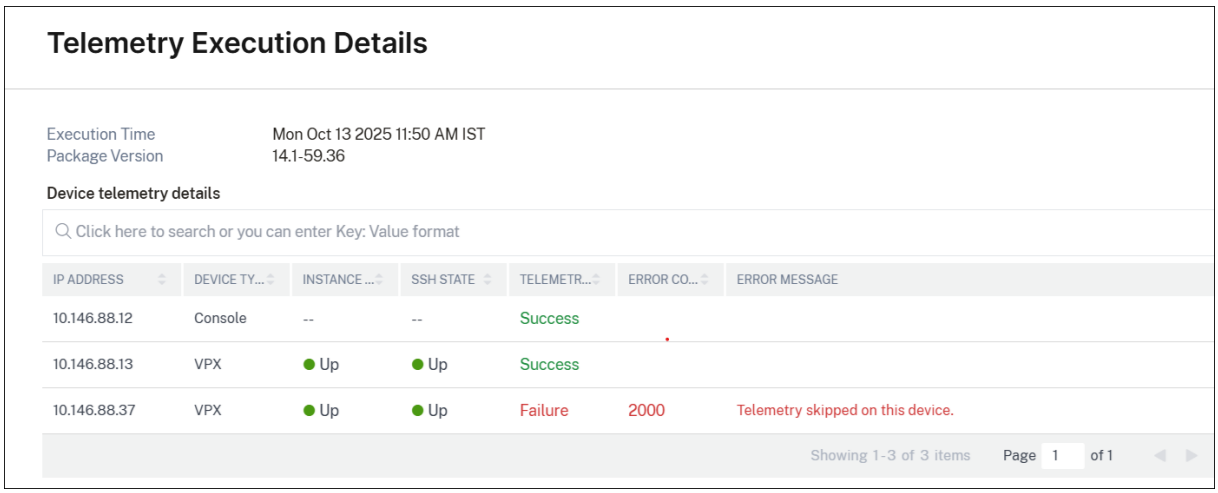


Collector level (Console) diagnostics

This section checks whether the NetScaler Console is successfully collecting data from managed devices and uploading it to the required destination.

Check Field	Description
Execution Time	Timestamp of the last telemetry collection from managed NetScaler instances.
Package Version	The check identifies which telemetry package version is installed on Console on-prem, ensuring the latest set of data is collected.
Evergreen Download Status	(Auto-mode only) Console on-prem checks every 24 hours for updated telemetry script packages from the download service URL. Hover over the information (i) icon to see the specific cause of failure. To get more details on the mitigation steps, click the Failure status.
Connectivity Status	(Auto-mode only) Confirms that required URLs are whitelisted and reachable. Connection issues, for example, proxy misconfiguration block Console from reaching these URLs. Hover over the information (i) icon to see the specific cause of unreachability. To get more details on the mitigation steps, click the **Unreachable status**. Download Service URL: Source for latest telemetry package downloads. Auto-enabled channel URL: Destination for uploading telemetry data.

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



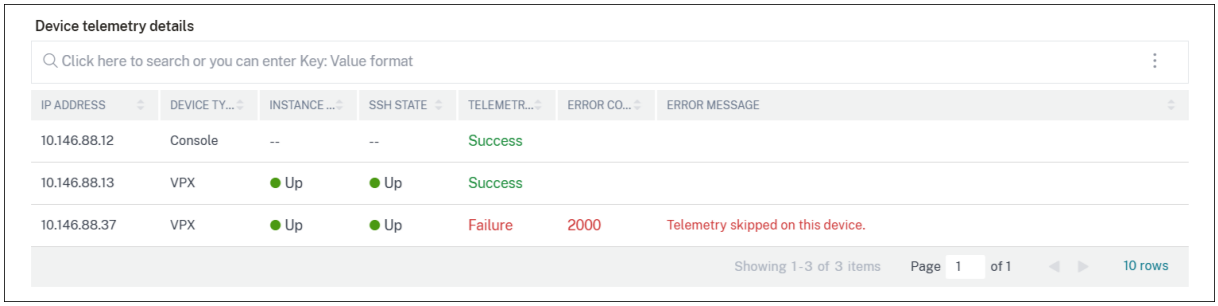
Device-Level (NetScaler) Diagnostics

The Console runs device-level diagnostics by pushing a telemetry collection script to each managed NetScaler instance, gathering the data, and preparing it for upload.

The Device Telemetry Details Table provides the results of this process, including:

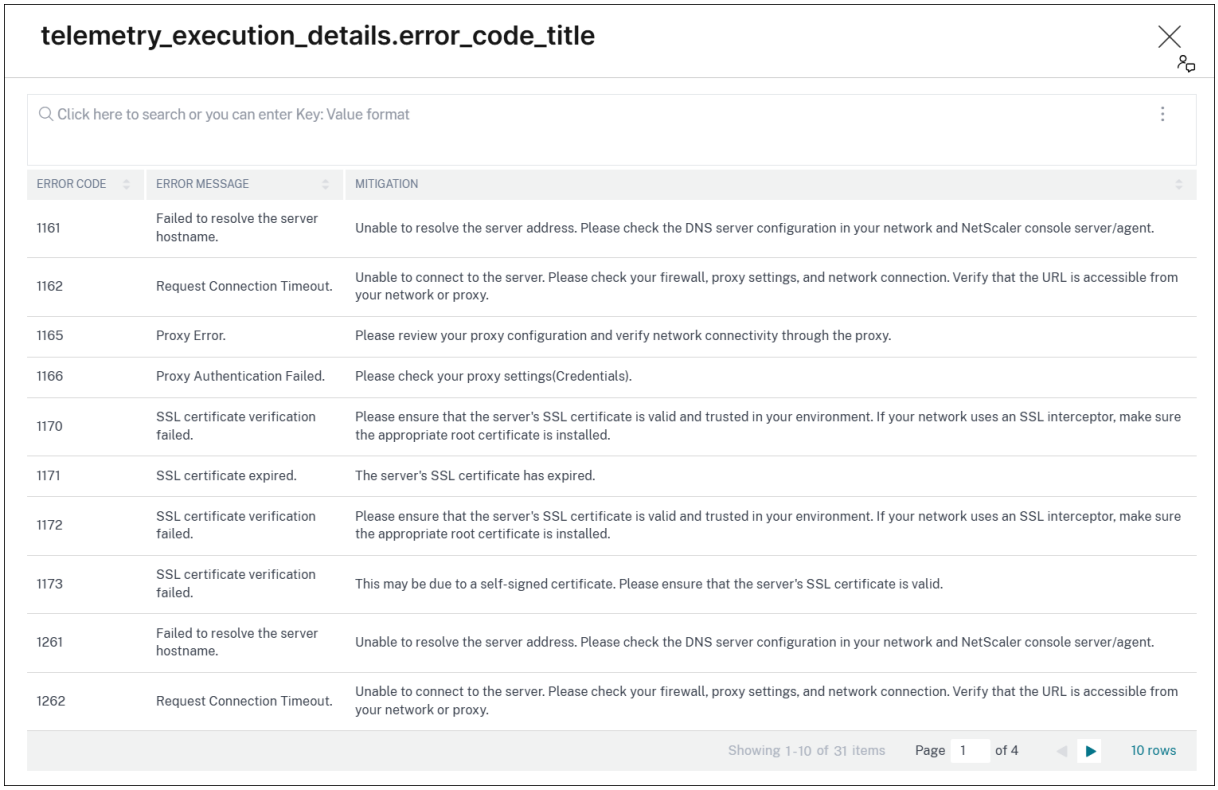
- Device details
- Telemetry Status
- Error codes and Error messages

For detailed error information and mitigation steps, click the red-highlighted error details.



Mitigation: Each error code is mapped to a recommended solution in the Mitigation Table. Follow the recommendation for fixing the issues.

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



Error Table Mapping

Error Code	Error Message	Customer Action
1161	Failed to resolve the server host name	Unable to resolve the server address. Please check the **DNS server configuration** in your network and NetScaler console server/agent.
1162	Unable to resolve the server address. Please check the **DNS server configuration** in your network and NetScaler console server/agent.	Unable to connect to the server. Please check your **firewall, proxy settings, and network connection**. Also, verify that the URL `download.citrixnetworkapi.net` is accessible from your network or through your proxy.

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

Error Code	Error Message	Customer Action
1165	Proxy Error	Please check your **proxy configuration** and ensure that network connectivity is working through the proxy.
1166	Proxy Authentication Failed	Please check your **proxy credentials** in the NetScaler console.
1170	SSL certificate verification failed.	If your network uses an **SSL interceptor**, make sure the appropriate **root certificate is installed** in the NetScaler console.
1171	SSL certificate expired	**SSL certificate expired**.
1172	SSL certificate verification failed.	If your network uses an **SSL interceptor**, make sure the appropriate **root certificate is installed** in the NetScaler console.
1173	SSL certificate verification failed.	This may be due to a **self-signed certificate**. If your network uses an **SSL interceptor**, make sure the appropriate **root certificate is installed** in the NetScaler console.
1261	Failed to resolve the server hostname	Unable to resolve the server address. Please check the **DNS server configuration** in your network and NetScaler console server/agent.

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

Error Code	Error Message	Customer Action
1262	Request Connection Timeout	Unable to connect to the server. Please check your **firewall, proxy settings, and network connection**. Verify that both URLs (`download.citrixnetworkapi.net`, `safehaven.adm.cloud.com`) are accessible from your network or through your proxy.
1265	Proxy Error	Please check your **proxy configuration** and ensure that network connectivity is working through the proxy.
1266	Proxy Authentication Failed.	Please check your **proxy credentials** in the NetScaler console.
1270	SSL certificate verification failed	If your network uses an **SSL interceptor**, make sure the appropriate **root certificate is installed** in the NetScaler console.
1271	SSL certificate expired.	The server's **SSL certificate has expired**.
1272	SSL certificate verification failed	If your network uses an **SSL interceptor**, make sure the appropriate **root certificate is installed** in the NetScaler console.
1273	SSL certificate verification failed	This may be due to a **self-signed certificate**. If your network uses an **SSL interceptor**, make sure the appropriate **root certificate is installed** in the NetScaler console.

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

Error Code	Error Message	Customer Action
1361	Failed to resolve the server hostname	Unable to resolve the server address. Please check the **DNS server configuration** in your network and NetScaler console server/agent.
1362	Request Connection Timeout.	Unable to connect to the server. Please check your **firewall, proxy settings, and network connection**. Verify that the URL `safehaven.adm.cloud.com` is accessible from your network or through your proxy.
1365	Proxy Error	Please check your **proxy configuration** and ensure that network connectivity is working through the proxy.
1366	Proxy Authentication Failed	Please check your **proxy credentials** in the NetScaler console.
1370	SSL certificate verification failed.	If your network uses an **SSL interceptor**, make sure the appropriate **root certificate is installed** in the NetScaler console.
1371	SSL certificate expired	The server's **SSL certificate has expired**.
1372	SSL certificate verification failed.	If your network uses an **SSL interceptor**, make sure the appropriate **root certificate is installed** in the NetScaler console.
1373	SSL certificate verification failed.	This may be due to a **self-signed certificate**. If your network uses an **SSL interceptor**, make sure the appropriate **root certificate is installed** in the NetScaler console.

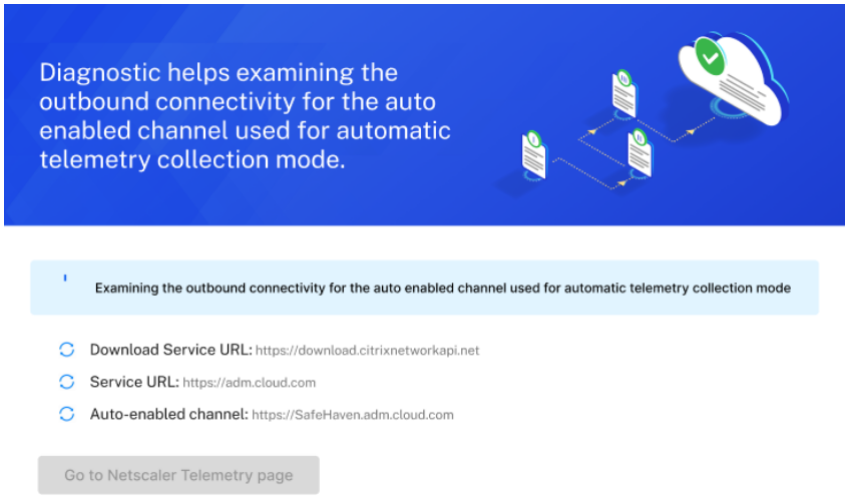
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Error Code	Error Message	Customer Action
2000	Telemetry skipped on this device.	This may be because this device is **managed by another NetScaler Console/Service/Agent**. Please ensure the other collector is sending telemetry data successfully.
2100	Instance state is down or not reachable.	Please ensure that the **instance is running and reachable**.
2250	SSH Authentication error	Please ensure that the **device profile is properly configured** in the NetScaler console for the device.
2251	SSH Connection timeout/refused.	The connection may be temporarily blocked by a firewall or network policy, or the device may be unreachable. Please **verify network connectivity** and ensure that the **SSH port is accessible**.
2252	Host key verification failed	Verify server identity with admin, then remove old key: `ssh-keygen -R <server_address>`.
2350	SSH Authentication error.	Please ensure that the **device profile is properly configured** in the NetScaler console for the device.
2351	SSH Failed to connect to device	The connection may be temporarily blocked by a firewall or network policy, or the device may be unreachable. Please **verify network connectivity** and ensure that the **SSH port is accessible**.

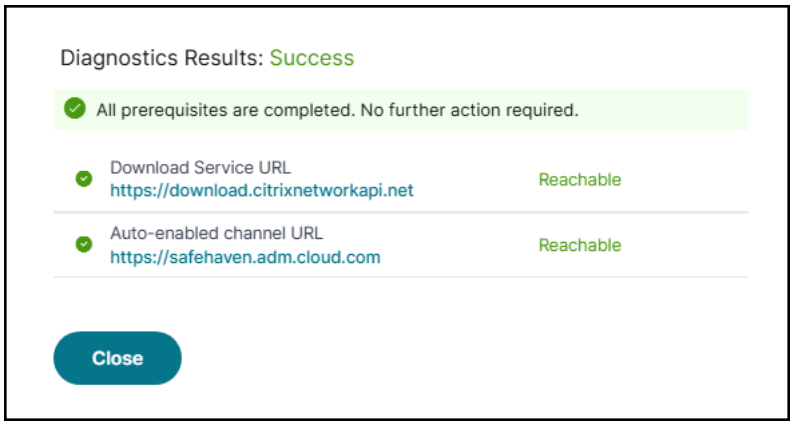
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Diagnostic behaviour before release 14.1 build 56.x

In release 14.1 build 51.x and earlier, the diagnostic helps to examine the outbound connectivity to these endpoint URLs and lets you know if they are in reachable status.

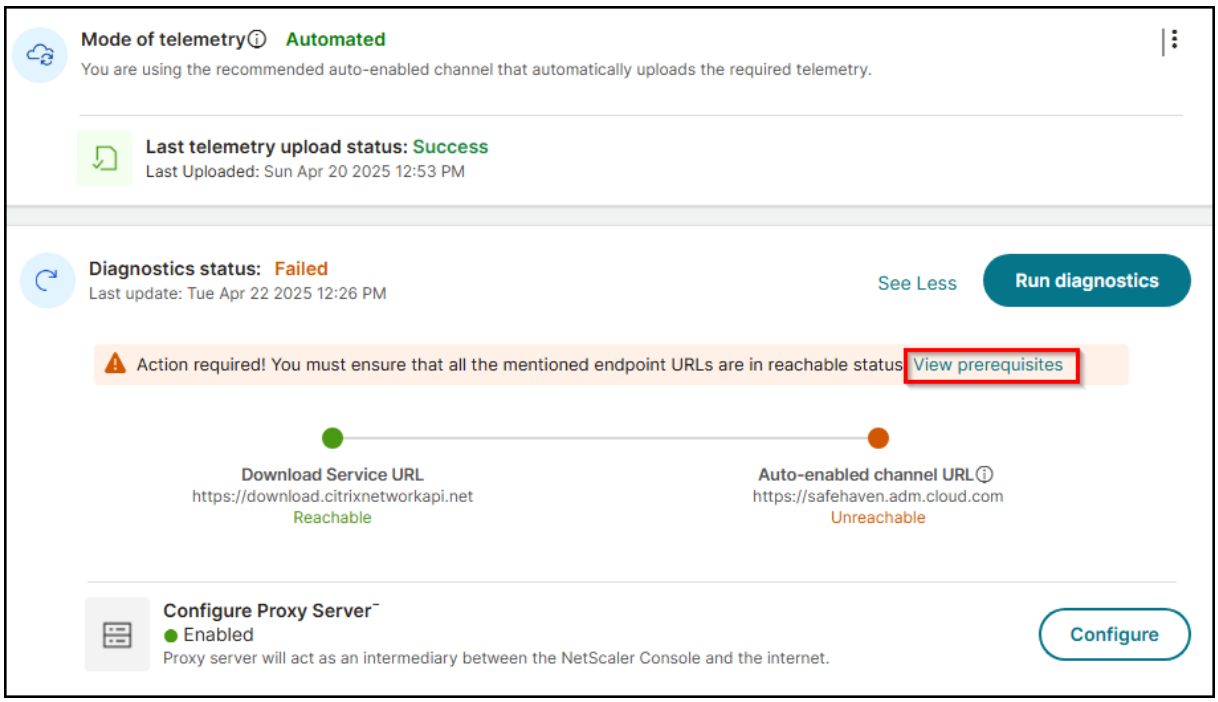


After you see the endpoint URLs in reachable status, click **Go to NetScaler® Telemetry** page.

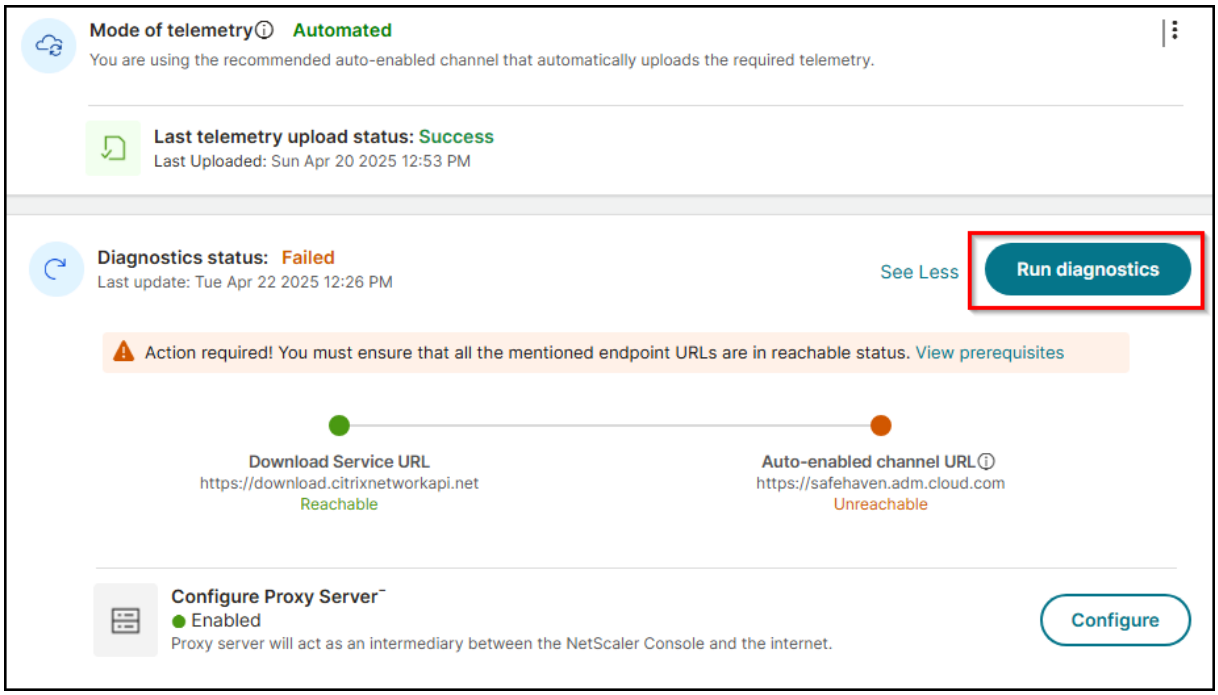


If any prerequisites fail, the diagnostic check displays the endpoints that are not reachable and you must ensure that the URLs reachable. Click **view pre-requisites** to view details.

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



You can run diagnosis by clicking **Run diagnosis** to confirm if the endpoint URLs are reachable.



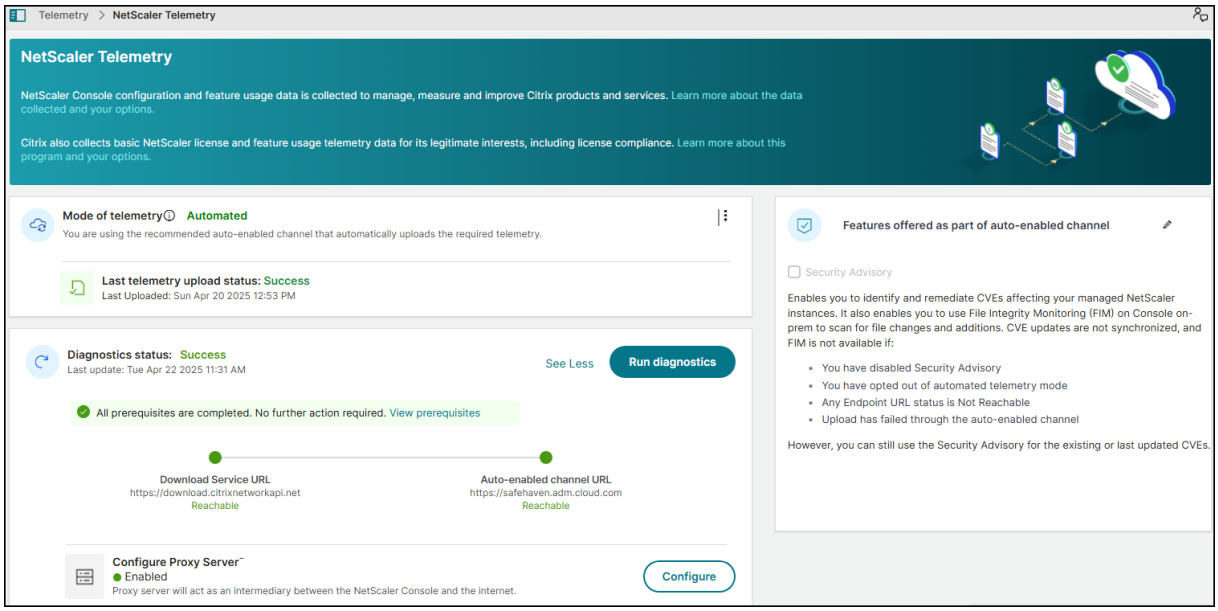
If no action is taken, your NetScaler Console on-prem might be non-compliant with the NetScaler telemetry program.

As part of the auto-enabled channel, you can use the **Security Advisory** feature with latest CVE updates in NetScaler Console on-prem. The Security Advisory feature enables you to identify the CVEs putting your NetScaler instances at risk and recommends remediations. You can view the latest CVE

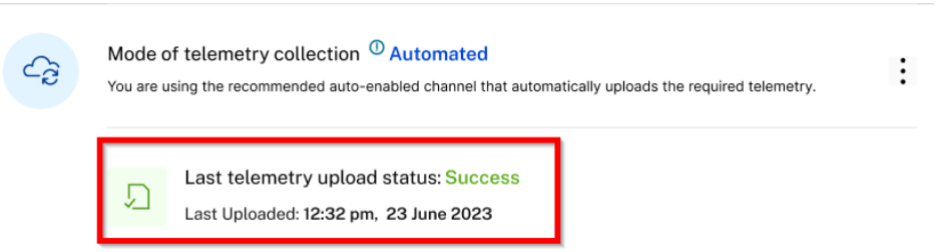
© 1997–2025 Citrix Systems, Inc. All rights reserved.

details that are impacting your NetScaler instances in Security Advisory. For more information, see Security Advisory.

> **Note:**
>
> You can also disable Security Advisory. If you disable **Security Advisory**, or opt-out of automated telemetry mode, or any prerequisites fail, the new CVE updates are not available and you can only use the Security Advisory with the existing or the last updated CVEs.



After the automated telemetry collection is enabled successfully, the first upload happens within 24 hours. The subsequent uploads happen every 24 hours automatically. The status changes to **Success** after the upload is complete.



If the upload fails, ensure that the endpoint URLs are reachable. If the status indicates reachable and still the upload fails, contact Customer Care.

Data governance

September 27, 2025

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

All existing NetScaler Console customers must be compliant with the NetScaler telemetry program by uploading the required telemetry data either through automated or manual mode. The NetScaler telemetry program is enabled starting from 14.1-25.53 and later / 13.1-53.22 and later build. For more information, see the NetScaler telemetry program.

Citrix collects basic license telemetry data and NetScaler® deployment and feature usage telemetry data for its legitimate interests, including license compliance. NetScaler Console configuration and feature usage data is also collected to manage, measure and improve Citrix products and services.

The automated telemetry collection mode enables you to use the **Security Advisory** feature in NetScaler Console on-prem that collects the optional telemetry parameters. You can disable the optional parameters, but not the required parameters.

Notes:

- After you upgrade to NetScaler Console **14.1-25.53 or later** / **13.1-53.22 or later** build, the following configuration is automatically pushed to your NetScaler instances through NetScaler Console. This configuration collects and stores the telemetry metrics in your NetScaler instances:

```
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
```

- If you are in manual mode or automated mode (with any prerequisite not met), NetScaler Console continues to check for the above configuration every 24 hours and push it to NetScaler instances, if this configuration is missing. If you do not want the configuration to be pushed, you must be in the automated mode (with all prerequisites met) or upgrade to the upcoming build (**14.1-29.x** or **13.1-55.x**).
- 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:

```
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, usernames, 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 teleme-

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

> try 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?	Required / Optional
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.	Required
NetScaler Console deployment and feature usage telemetry	Information about Console deployment and feature usage.	To manage, measure, and improve the service.	Optional

To disable the optional parameters:

1. In NetScaler Console on-prem, navigate to **NetScaler Telemetry** and disable **Security Advisory**.
2. Navigate to **Settings > Administration > Enable or disable the Console feature data sharing**, and clear the **I agree to share Console feature usage data** checkbox.

If your NetScaler Console is between 14.1-8.x and 14.1-21.x build, the data collection is enabled after you configure Cloud Connect and enable the Security Advisory feature. For more information, see Data governance for Cloud Connect

If your NetScaler Console is 14.1-4.x or lower version, you can create a Customer Identity on Citrix Cloud to send important statistics about NetScaler Console health, status, and other metrics from NetScaler Console on-prem deployment to Citrix Cloud account. Citrix collects statistics to understand the usage of NetScaler Console. For more information, see Data governance for Customer Identity.

Licensing

September 27, 2025

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

NetScaler Console requires a verified NetScaler license to manage and monitor the NetScaler instances, when the instances are discovered through the `https` protocol.

NetScaler Console supports the following license editions. Contact your NetScaler sales representative or partner to purchase a NetScaler Console license.

Express edition –You can manage and monitor any number of instances with the Express edition license. By default, the Express edition license is applied.

Advanced edition - It allows to manage the discovered applications and view analytics for the purchased virtual servers along with the free virtual servers.

Points to note:

- For build **13.1-9.x or earlier**, you can manage up to 30 discovered applications or virtual servers and view analytics. Beyond the 30 discovered applications or the 30 virtual servers, you must buy and apply an Advanced license. For example, if you buy 100 virtual server licenses, then you are entitled to you use up to 130 virtual server licenses.
- For build **13.1-12.x or later**, you can manage up to two discovered applications or virtual servers and view analytics. Beyond the two discovered applications or the two virtual servers, you must buy and apply an Advanced license. For example, if you buy 100 virtual server licenses, then you are entitled to you use up to 102 virtual server licenses.

Post upgrade to builds from 13.1-12.x until 14.1-17.x:

- All the Express default free virtual servers remain functional for 30 days. You can select the two virtual servers and apply the two default licenses within the 30 days period. If no user action is taken 30 days post upgrade, NetScaler Console randomly applies the license to two virtual servers and unlicenses the remaining virtual servers. You must buy and apply new Advanced licenses to enable these virtual servers.
- Post upgrade, the following are the changes in the NetScaler Console behavior:
    - NetScaler Console gives an additional 30 days to take the required action.
    - Within the 30-day period, the allocation of new virtual servers for the 30 express free virtual servers is blocked.
        - For example, if the number of available virtual server licenses before you upgraded to 12.x was 30 and only 20 licensed virtual servers were used, you are only allowed to use the 20 virtual servers and not allowed to license the remaining 10 virtual servers in the 30-day period.
    - However, within the 30-day period, as an administrator, you can still apply Advanced NetScaler Console licenses and allocate new virtual servers.

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

The following table provides the licensing details:

Features	Options	Express edition	Advance edition	NetScaler License
Applications	Application Dashboard	Up to two virtual servers.	Entitled for all purchased virtual server licenses and extra two virtual servers.	NetScaler Web App Firewall related information on App Dashboard needs Premium (or) Advanced with App Firewall license.
	Web Insight	Up to two virtual servers.	Entitled for all purchased virtual server licenses and extra two virtual servers.	NA
	Service Graph	Up to two virtual servers.	Entitled for all purchased virtual server licenses and extra two virtual servers.	NA
	Configuration > StyleBooks	Unlimited	Unlimited	NA
Security	Security Dashboard	Up to two virtual servers.	Entitled for all purchased virtual server licenses and extra two virtual servers.	NetScaler Web App Firewall related information on Security Dashboard needs Premium (or) Advanced with App Firewall license.
	Security Violations	Up to two virtual servers.	Entitled for all purchased virtual server licenses and extra two virtual servers.	Premium (or) Advanced with App Firewall license

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

Features	Options	Express edition	Advance edition	NetScaler License
	Users and endpoints	Up to two virtual servers.	Entitled for all purchased virtual server licenses and extra two virtual servers.	NA
Gateway	HDX Insight	Up to two virtual servers.	Entitled for all purchased virtual server licenses and extra two virtual servers.	Advanced (reporting < 1 hour) Premium (reporting = Unlimited)
	Gateway Insight	Up to two virtual servers.	Entitled for all purchased virtual server licenses and extra two virtual servers.	Advanced (reporting < 1 hour) Premium (reporting = Unlimited)
Infrastructure	Infrastructure Analytics	Unlimited	Unlimited	NA
	Instances	Unlimited	Unlimited	NA
	SSL Dashboard	Unlimited	Unlimited	NA
	Events	Unlimited	Unlimited	NA
	Network Functions	Unlimited	Unlimited	NA
	Network Reporting	Unlimited	Unlimited	NA
	Pooled licenses	Unlimited	Unlimited	NA
	Configuration > Configuration Jobs, Configuration Templates, and Configuration Advice	Unlimited	Unlimited	NA
	Upgrade Jobs	Unlimited	Unlimited	NA
	Orchestration	Unlimited	Unlimited	NA

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

Features	Options	Express edition	Advance edition	NetScaler License
Settings	RBAC and External Authentication (instance level)	Unlimited	Unlimited	NA
	RBAC and External Authentication	Unlimited	Unlimited	NA

*For Citrix Director integration with NetScaler Console support –Citrix Director must have a Premium license.

Licenses for more virtual servers are available in virtual server packs of 10. You can obtain a valid license and add the license on the NetScaler Console servers through the NetScaler Console GUI.

High Availability

The NetScaler Console server can contain VIP, CICO, and pooled capacity licenses. When the licenses are issued to a NetScaler Console server, the licenses are bound to the host ID of the server. Assigning licenses to a different NetScaler Console server is restricted.

If you configure a NetScaler Console high-availability pair as a license server, the primary and secondary servers must have the same license files. Therefore, in the NetScaler Console high-availability deployment, NetScaler Console supports assigning the same license files to both the servers.

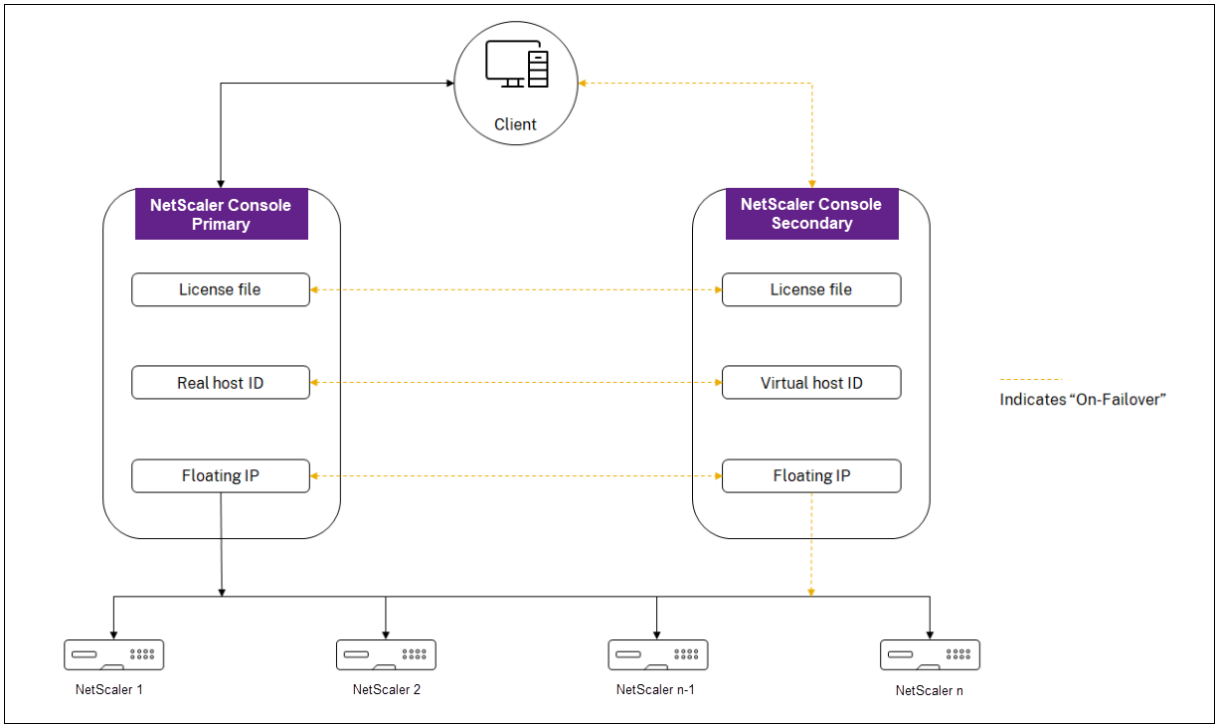
> **Note**
>
> - If you have installed NetScaler Console release 12.1-49.x or earlier, you get 30 days to maintain the licensing on the secondary node. After 30 days, you must contact Citrix to rehost the original license.
> - In release 12.1-50.x and later, the NetScaler Console license is automatically synchronized to the secondary node.
> - Pooled licenses are automatically synchronized to the secondary node in release 12.1-50.x and later.

How licenses are synchronized between NetScaler Console high-availability nodes?

Whenever a failover occurs, the secondary server assumes the role of the primary server. The real host ID of the primary server is configured as the virtual host ID of the new primary server. The license files recognize the new primary server using the virtual host ID.

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

- **Real Host ID** - This ID is generated from a MAC address of the NetScaler Console server. Each NetScaler Console standalone deployment has a unique host ID.
- **Virtual Host ID** - This ID is auto generated during HA deployment. The real host ID of a NetScaler Console primary server is used as the virtual Host ID of the secondary server. This ID is stored in the NetScaler Console database in an encrypted format and any modification to this ID is restricted. The virtual Host ID is preferred over the real Host ID.



Assume Node-1 is the primary server and Node-2 is the secondary server. The virtual host ID of Node-1 is synchronized with Node-2.

1. License files available in Node-1 are synchronized to Node-2.
2. Any new license files on Node-1 are synchronized to Node-2 periodically.
3. NetScaler Console ensures that the License Server is running only on Node-1 to avoid doubling of license capacity.
4. NetScaler instances check out licenses from Node-1 using the floating IP address.

Licenses are locked to NetScaler instances. To check out licenses from NetScaler Console HA, instances require the specific NetScalerNetScaler IP address. When you apply licenses on a primary server that will be in charge of licensing, it applies to all future licenses on that instance. You can delete licenses only from the server on which you have installed the licenses.

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

Orchestration

The Orchestration module is independent of licensing and is always available.

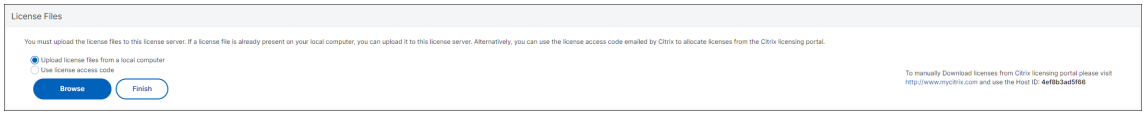
Upgrade the virtual server licenses

You can upgrade the licensing on NetScaler Console to monitor and manage more virtual servers hosted on NetScaler.

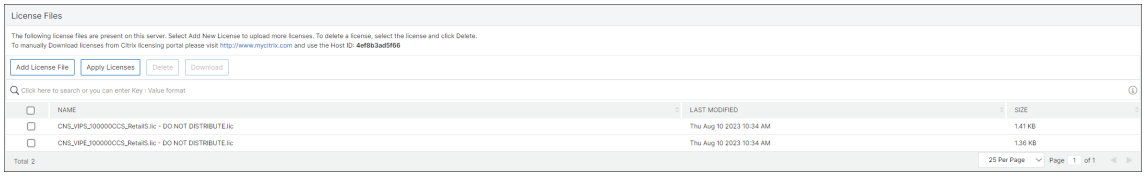
To upgrade your NetScaler licenses:

1. Log on to NetScaler Console using the administrator credentials.
2. Navigate to **Infrastructure > Pooled Licensing**.
3. Go to **License Files**, and select one of the following options:
   - **Upload license files from a local computer**. If a license is already present on your local computer, click **Browse** and select the license file (.lic) that you want to use to allocate your licenses. Click **Finish**.
   - **Use License Activation Code**. Citrix emails the license access code for the license that you purchased. Enter the license access code in the text box and then click **Get Licenses**.

   > **Note**
   >
   > If you select this option, NetScaler Console must be connected to the Internet, or a proxy server must be available.



4. You can add more licenses from the License Settings page at any time.



Verification

You can verify the licenses installed on NetScaler Console by navigating to **Settings > Licensing & Analytics Configuration**.



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

Manage virtual servers

You can select the virtual servers or third-party virtual servers you want to manage and monitor through NetScaler Console.

> **Points to note**
>
> - By default, NetScaler Console automatically licenses the virtual servers randomly after each virtual server poll cycle.
> - If the total number of virtual servers discovered in your NetScaler Console is lower than the number of installed virtual server licenses, NetScaler Console, by default, licenses all the virtual servers.

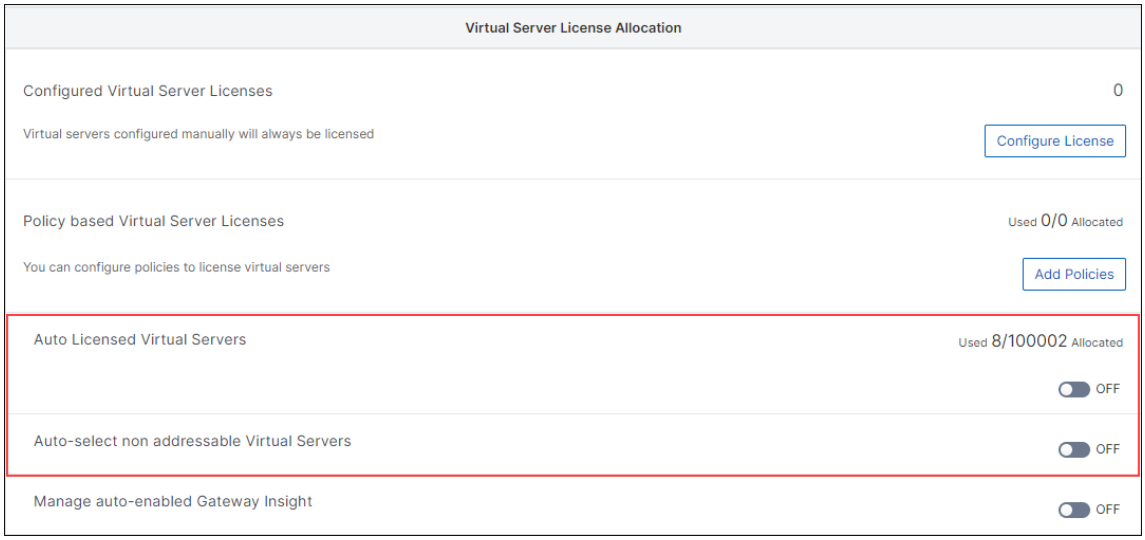
To select the virtual servers manually, or to restrict licensing to limited virtual servers, you have to first disable auto licensing the virtual servers, and then select the virtual servers you want to manage.

Disable auto-licensing virtual servers

1. Navigate to **Settings > Licensing & Analytics Configuration**.

   The dashboard displays the virtual server licenses available, the managed virtual servers along with the virtual server type, and license expiry information.

2. In **Virtual Server License Allocation**, disable **Auto Licensed Virtual Servers** and **Auto-select non addressable Virtual Servers**.



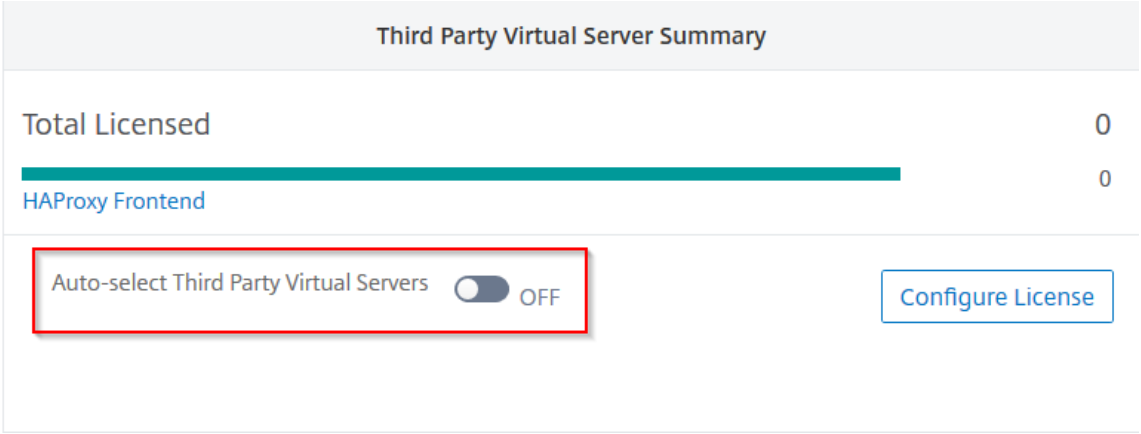
Select third-party virtual servers for licensing

1. Navigate to **Settings > Licensing & Analytics Configuration**.

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

The dashboard displays the virtual server licenses available, the managed virtual servers along with the virtual server type, and license expiry information.

2. In **Third Party Virtual Server Summary**, disable **Auto-select Third Party Virtual Servers**.



Apply virtual server licenses manually

You can manually apply licenses to an individual virtual server.

1. In **Virtual Server License Allocation**, select **Configure Licenses**.

   The **All Virtual Servers** page is displayed.
2. Filter unlicensed virtual servers using the property: `Licensed: No`.
3. Select the virtual server that you want to license.
4. Click **License**.

Configure policy based virtual server licensing

You can configure a policy to apply license to virtual servers. This policy controls the number of virtual servers that you want to auto-license. It also applies licenses to selected instances' virtual servers only.

Click **Edit Policies** and you can specify the following:

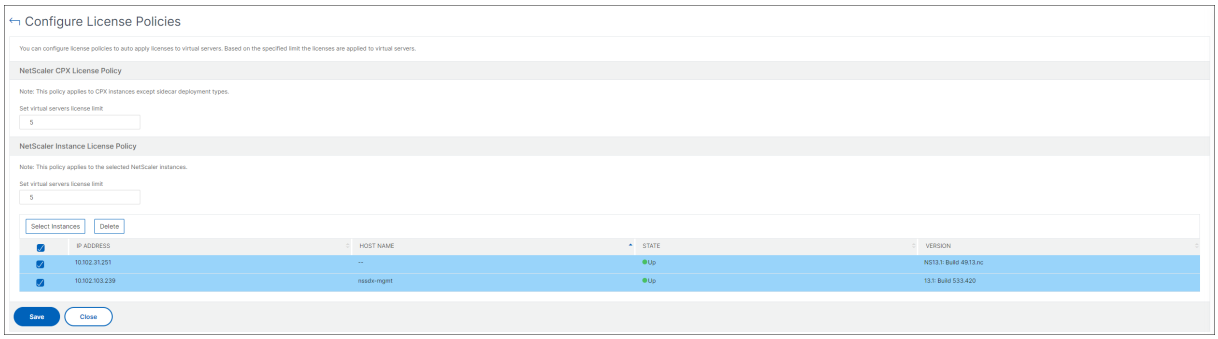
- Set virtual servers limit on CPX instances separately to apply licenses. NetScaler Console applies license to virtual servers on CPX instances up to a specified limit.

  > **Important**
  >
  > This limit applies to CPX instances except sidecar deployment types.
  >
  > To view CPX instances of sidecar deployment types, filter the virtual servers using the prop-

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

> erty: `License Type: Freely Managed.`

- Set virtual servers limit on selected NetScaler instances (MPX/VPX/BLX) to apply licenses. NetScaler Console applies licenses to virtual servers on NetScaler instances up to a specified limit.
- Select the priority NetScaler instances to apply virtual server licenses. Therefore, NetScaler Console can apply license to selected instances' virtual servers only.



View the licensed virtual servers

After the licenses are applied to the virtual servers, you can view the licensed virtual servers or third-party virtual servers.

1. Navigate to **Settings > Licensing & Analytics Configuration**.
2. Click the virtual server type in the **Total Licensed** section in the **Virtual Servers License Summary**.

Configure auto license support for non-addressable virtual servers

NetScaler Console, by default, does not automatically apply licenses to non-addressable virtual servers. For licensing non-addressable virtual servers, you must disable the auto-license option and manually select the non-addressable virtual servers. This increases your effort to manually select the non-addressable servers initially when you apply the licenses. You also need to manually select the new non-addressable virtual servers whenever they are added to your network.

NetScaler Console provides an option under **Virtual Server License Allocation**. If you enable the **Auto-select non addressable Virtual Servers** option, licenses are applied automatically to the non-addressable virtual servers.

> **Note**
>
> - NetScaler Console, by default, still does not automatically select non-addressable virtual

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

servers for licensing.

- Application analytics (App Dashboard) is the only analytics currently supported on licensed non-addressable virtual servers.

Licensing

March 19, 2025

Starting from **14.1-21.x** build, the concept of licensed VIPs is removed. An unlimited number of VIPs are now available in NetScaler Console on-prem. 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.

The following table provides the licensing details:

Features	Options	NetScaler License
Applications	Application Dashboard	NetScaler Web App Firewall related information on App Dashboard needs Premium (or) Advanced with App Firewall license.
	Web Insight	NA
	Service Graph	NA
	Configuration > StyleBooks	NA
Security	Security Dashboard	NetScaler Web App Firewall related information on Security Dashboard needs Premium (or) Advanced with App Firewall license.
	Security Violations	Premium (or) Advanced with App Firewall license
	Users and endpoints	NA
Gateway	HDX Insight	Advanced (reporting < 1 hour) Premium (reporting = Unlimited)

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

Features	Options	NetScaler License
	Gateway Insight	Advanced (reporting < 1 hour) Premium (reporting = Unlimited)
Infrastructure	Infrastructure Analytics	NA
	Instances	NA
	SSL Dashboard	NA
	Events	NA
	Network Functions	NA
	Network Reporting	NA
	Pooled licenses	NA
	Configuration > Configuration Jobs, Configuration Templates, and Configuration Advice	NA
	Upgrade Jobs	NA
	Orchestration	NA
Settings	RBAC and External Authentication (instance level)	NA
	RBAC and External Authentication	NA

*For Citrix Director integration with NetScaler Console support –Citrix Director must have a Premium license.

High Availability

The NetScaler Console server can contain VIP, CICO, and pooled capacity licenses. When the licenses are issued to a NetScaler Console server, the licenses are bound to the host ID of the server. Assigning licenses to a different NetScaler Console server is restricted.

If you configure a NetScaler Console high-availability pair as a license server, license files applied on primary get synchronized to secondary.

> **Note:**
>
> - In release 12.1-50.x and later, the NetScaler Console licenses are automatically synchro-

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

> nized from primary to the secondary node.

System requirements

December 10, 2025

Before you install NetScaler Console, you must understand the software requirements, browser requirements, port information, license information, and limitations.

Requirements for NetScaler Console

Component	Requirement
RAM	32 GB
Virtual CPU	8 CPUs **Note:** We recommend using solid-state drive (SSD) technology for NetScaler Console deployments.
Storage space	The default storage space required is 120 GB. The actual storage requirement depends on NetScaler Console sizing estimation. If your NetScaler Console storage requirement exceeds 120 GB, you to have to attach an additional disk. You can add only one additional disk. We recommend that you estimate storage and attach additional disks at the time of initial deployment. For more information, see How to Attach an Additional Disk to NetScaler Console.
Virtual network interfaces	1
Throughput	1 Gbps or 100 Mbps

Requirements for NetScaler Console on-prem agent

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

Component	Requirement
RAM	32 GB
Virtual CPU	8 CPUs
Storage space	30 GB
Virtual network interfaces	1
Throughput	1 Gbps

> **Note**
>
> AMD processor is supported in:
>
> - **NetScaler Console 13.1 build 4.43 or later**.
> - **NetScaler agent 13.1 build 17.42 or later**.

Minimum NetScaler version required for NetScaler Console features

> **Important**
>
> 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 Console 12.1 Build 50.39, then ensure you have installed NetScaler 12.1 Build 50.28/50.31 or earlier.

NetScaler Console Feature	NetScaler Software Version
StyleBooks	10.5 and later
OpenStack/CloudStack Support	11.0 and later, if a partition is required
	11.1 and later, if a partition on a shared virtual LAN is required
NSX Support	11.1 Build 47.14 and later (VPX)
Mesos/Marathon Support	10.5 and later
Backup/Restore	For NetScaler, 10.1 and later
	For NetScaler SDX, 11.0 and later
Monitoring/Reporting and Configuration using Jobs	10.1 and later
Analytics Features	

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

NetScaler Console Feature	NetScaler Software Version
Web Insight	10.5 and later
HDX Insight	10.1 and later
WAF Security Violations	11.0.65.31 and later
Gateway Insight	11.0.65.31 and later
Cache Insight	10.5 and later*
SSL Insight	12.0 and later

* Integrated Cache Metrics are not supported in NetScaler Console with NetScaler instances running version 11.0 build 66.x.

Requirements for NetScaler Console analytics

Minimum Citrix Virtual Apps and Desktops versions required for NetScaler Console features

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 Citrix Virtual Apps or Citrix Virtual Desktops and accessed through Citrix Workspace. However, this capability depends on the operating system on which 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

- Dell Wyse Windows based Thin Clients
- Dell Wyse Linux-based Thin Clients

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

- Dell Wyse ThinOS based Thin Clients
- 10ZiG Ubuntu-based Thin Clients
- IGEL UD3 W7+ (M340)
- IGEL UD3 W7 (M340C)

NetScaler instance license required for HDX insight

The data collected by NetScaler Console for HDX Insight depends on the version and licenses of the NetScaler instances being monitored. HDX Insight reports are displayed only for NetScaler Premium and Advanced appliances running release 10.5 and later.

NetScaler License/Duration	5 Minutes	1 Hour	1 Day	1 Week	1 Month
Standard	No	No	No	No	No
Advanced	Yes	Yes	No	No	No
Premium	Yes	Yes	Yes	Yes	Yes

Supported hypervisors

The following table lists the hypervisors supported by NetScaler Console:

Hypervisor	Versions
XenServer	7.1, 7.4, and 8.0
VMware ESX	6.0, 6.5, 6.7, 7.0, 8.0 (from 14.1-21.x and later), and 8.0.2b (from 14.1-25.x and later)
Microsoft Hyper-V	2012 R2, 2016, 2019, and 2022
Generic KVM	RHEL 7.4, RHEL 8.0, Ubuntu 16.04, and Ubuntu 18.04
Nutanix Hypervisor (AHV)	6.5.2 (from 14.1-38.x and later)

Supported operating systems and Workspace versions

The following table lists the operating systems supported by NetScaler Console, and the Citrix Workspace versions currently supported with each system:

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

Operating System	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

Supported browsers

The following table lists the web browsers supported by NetScaler Console:

Web Browser	Version
Microsoft Edge	79 and later
Google Chrome	51 and later
Safari	10 and later
Mozilla Firefox	52 and later

Supported ports

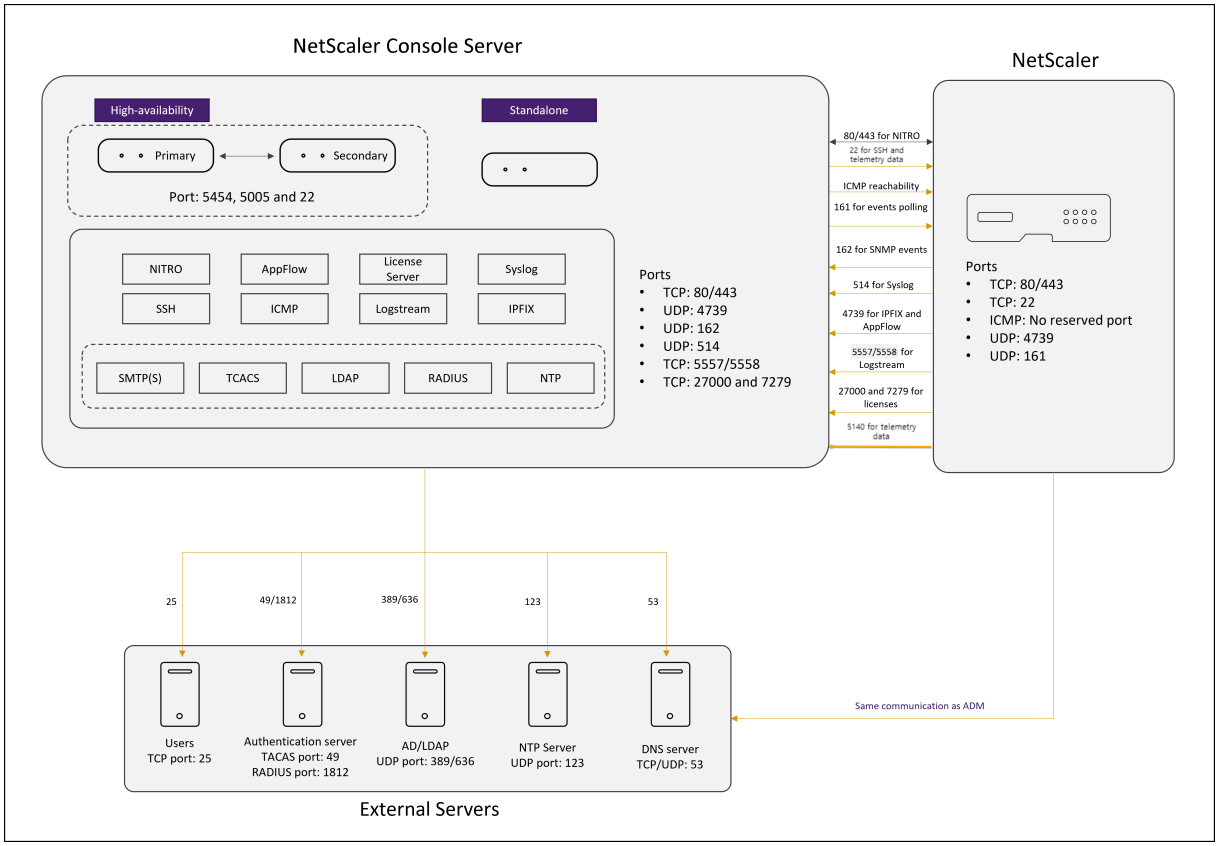
NetScaler Console uses the NetScaler IP (known as NSIP) address to communicate with NetScaler. You can use an agent as an intermediary between the NetScaler instance and NetScaler Console. To establish a communication with these servers, open the required ports.

- For AppFlow and log stream communication from NetScaler to NetScaler Console, Subnet IP address (known as SNIP) is used.
- For license related communication from NetScaler to NetScaler Console, NSIP address is used.
- If the SNIP address is enabled for management access and if NetScaler is added in NetScaler Console by using SNIP address, then SNIP address is used as the source IP address for events and Syslogs.

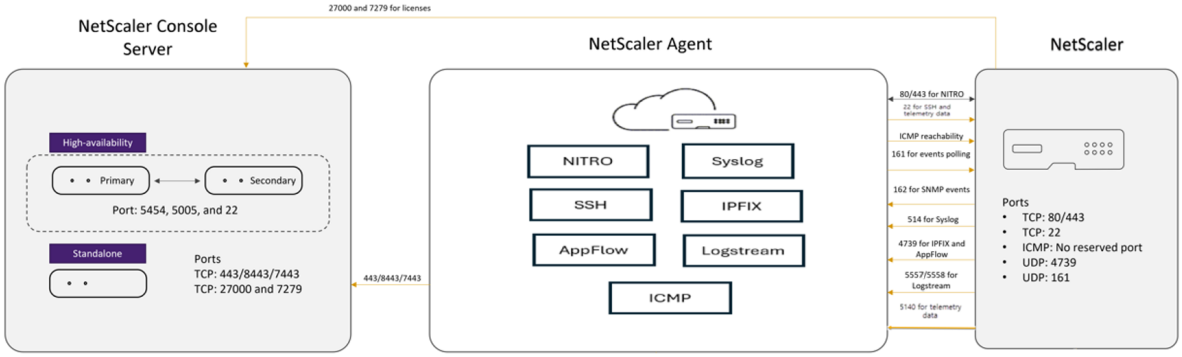
> **Note**
>
> If you have configured NetScalers in High Availability mode, NetScaler Console uses NSIP to communicate with NetScaler and the required ports remain the same.

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

Network port diagram for agentless deployment:

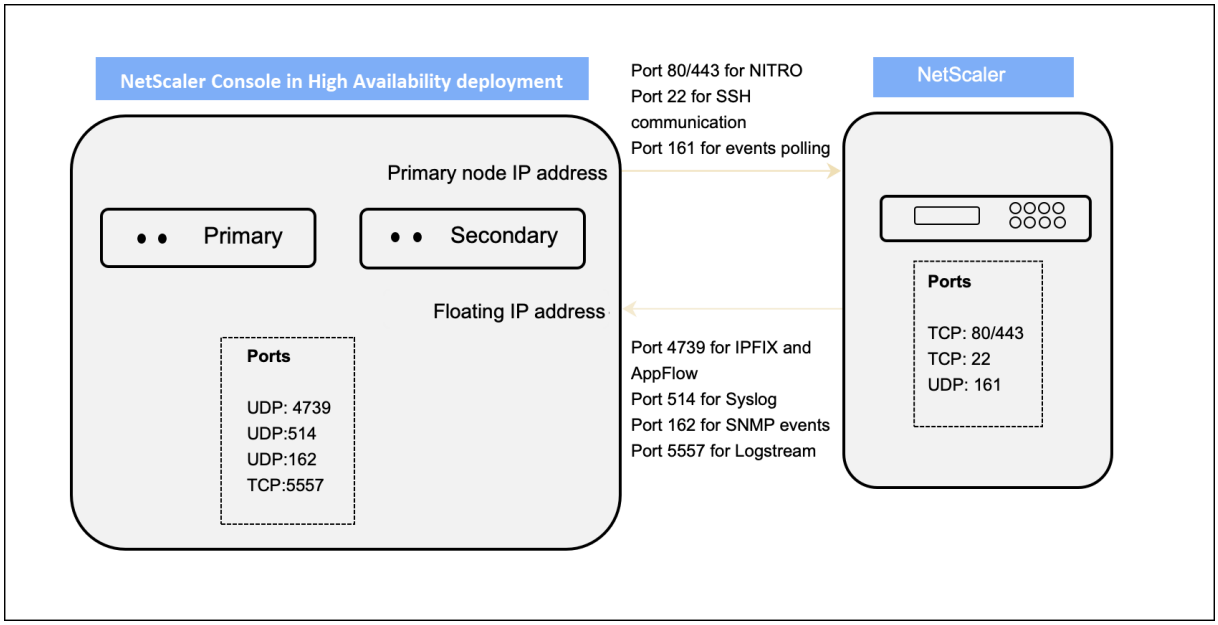


Network port diagram for the deployment that includes NetScaler® agent:



Network port diagram for the NetScaler Console High Availability deployment:

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



If two NetScaler Console servers are set up in high availability mode, when adding an instance:

- NetScaler Console communicates with NetScaler through the Primary IP address.
- NetScaler establishes connectivity with NetScaler Console through the NetScaler Console floating IP address. This implies that NetScaler directs all SNMP, Syslog, and Analytics traffic to the NetScaler Console floating IP address.

The following sections explain the required ports and their purpose:

- NetScaler Console server
- NetScaler agent
- NetScaler instance
- External servers

Ports for the NetScaler Console server

The following table explains the required ports that must be open on the NetScaler Console server.

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

Port	Type	Details	Direction of communication
80/443/5454/22	TCP	Default port for communication, and database synchronization in between NetScaler Console nodes in high availability mode. **Note:** This port is also used for NetScaler telemetry.	NetScaler Console primary node to NetScaler Console secondary node
443/8443/7443	TCP	Port for communication between NetScaler agent and NetScaler Console.	NetScaler agent initiates the communication with NetScaler Console. Then, NetScaler Console and agent interact with each other.
27000 and 7279	TCP	License ports for communication between NetScaler Console license server and NetScaler instance. These ports are also used for NetScaler pooled licenses.	NetScaler to NetScaler Console
5005	UDP	Port to exchange heartbeats between HA nodes.	NetScaler Console primary node to secondary node. NetScaler Console secondary node to primary node.
5140	UDP	Port to receive NetScaler Gateway telemetry data.	NetScaler to NetScaler Console

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

If the NetScaler Console and NetScaler instances do not use an agent for communication, open the following ports on the NetScaler Console server:

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
4739	UDP	For AppFlow communication from NetScaler instance to NetScaler Console.	NetScaler to NetScaler agent
162	UDP	To receive SNMP events from NetScaler instance to NetScaler Console.	NetScaler to NetScaler agent
514	UDP	To receive syslog messages 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 NetScaler Console.	NetScaler to NetScaler Console
5563	TCP	To receive NetScaler metrics (counters), system events, and Audit Log messages from NetScaler instance to NetScaler Console	NetScaler to NetScaler Console

Ports for the agent

The following table explains the required ports that must be open on the agent.

© 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
4739	UDP	For AppFlow communication from NetScaler instance to NetScaler Console.	NetScaler to NetScaler agent
162	UDP	To receive SNMP events from NetScaler instance to NetScaler Console.	NetScaler to NetScaler agent
514	UDP	To receive syslog messages 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 NetScaler Console.	NetScaler to NetScaler Console

Ports for NetScaler instances

The following 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. For NITRO communication between NetScaler Console servers in high availability mode.	NetScaler Console to NetScaler and NetScaler to NetScaler Console
22	TCP	For SSH communication from NetScaler Console to NetScaler instance. For synchronization between NetScaler Console servers deployed in high availability mode. And, this port is required for the SSH communication between the NetScaler Console agent and NetScaler.	NetScaler Console to NetScaler. Or, NetScaler agent to NetScaler.
No reserved port	ICMP	To detect network reachability between NetScaler Console and NetScaler instances, or the secondary NetScaler Console server deployed in high availability mode.	NetScaler Console to NetScaler
161	UDP	To poll events from NetScaler instances.	NetScaler Console to NetScaler

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

Ports for NetScaler built-in agent

The following table explains the required ports that must be open for a NetScaler built-in agent.

Port	Type	Details	Direction of communication
443	TCP	For all communication from NetScaler Console to NetScaler built-in agent	NetScaler Console to NetScaler built-in agent and NetScaler built-in agent to NetScaler Console

> **Note:**
>
> In NetScaler Console high-availability deployment, all communications from NetScaler Console use the primary node IP address.

Ports for external servers

The following table explains the required ports that must be open on external servers:

Port	Type	Details	Direction of communication
25	TCP	To send SMTP notifications from NetScaler Console to users.	NetScaler Console to users.
389/636	TCP	Default port for authentication protocol. For communication between NetScaler Console and LDAP external authentication server.	NetScaler Console to LDAP external authentication server
123	UDP	Default NTP server port for synchronizing with multiple time sources.	NetScaler Console to NTP server

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

Port	Type	Details	Direction of communication
1812	RADIUS	Default port for authentication protocol. For communication between NetScaler Console and RADIUS external authentication server.	NetScaler Console to RADIUS external authentication server
49	TACACS	Default port for authentication protocol. For communication between NetScaler Console and TACACS external authentication server.	NetScaler Console to TACACS external authentication server

Limitations

From NetScaler ADM 12.1 or later, the IPv6 format of IP addresses is supported. To configure IPv6, navigate to **Settings > Administration**, select **IP Address, Second NIC, Host Name and Proxy Server** under **Network Configurations**, enable **IPv6**, provide the IPv6 configuration details, and click **Save**.

The following table describes the supported and not supported list of features for IPv6:

IPv6 supported features	IPv6 not supported features
Management access for NetScaler ADM GUI	High availability floating IP
Management access for NetScaler	Syslogs received from ADCs that support IPv6
Registration and inventory	StyleBooks on ADCs that support IPv6
Network dashboard	Analytics
SSL dashboard	Pooled licensing
Config jobs	
Config audit	
Network functions	

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

IPv6 supported features	IPv6 not supported features
Network reporting	
Backup and restore of ADC instances	
SNMP events from NetScaler instances	

Getting started

September 27, 2025

This document walks you through how to get started with deploying and setting up NetScaler Console on-prem for the first time. This document is intended for network and application administrators who manage Citrix network devices (NetScaler and NetScaler Gateway). Follow the steps in this document irrespective of the type of device you plan to manage using NetScaler Console.

If you are an existing user of NetScaler Console, you are recommended to review the release notes, system requirements, and licensing details before upgrading your server to the latest release of NetScaler Console.

Step 1 - Review the system requirements

Before you begin deploying NetScaler Console in your data center, review the software requirements, browser requirements, port information, license information, and limitations.

- **License information**. You can add any number of instances and entities without a license. However, you can view analytics information for only two virtual servers without applying a license. To view analytics for more than two virtual servers, you must purchase appropriate licenses. Learn More.
- **Operating system and receiver requirements**. Review this information to make sure you have the correct receiver version for the supported operating systems. Learn More.
- **Browser requirements**. To access NetScaler Console GUI, you must make sure you have the required browser and the correct version. Learn More.
- **Ports**. Make sure that the required ports are open for NetScaler Console to communicate with NetScaler instances. Learn More.

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

- **NetScaler instance requirements**. Different NetScaler Console features are supported on different NetScaler software versions. Review this information to make sure you have upgraded your NetScaler instances to the correct version. Learn More.

Step 2 - Deploy NetScaler Console

To manage and monitor the applications and network infrastructure, you must first install NetScaler Console on one of the hypervisors. You can deploy NetScaler Console either as a single server or in a high availability mode. If you are using NetScaler Insight Center, you can migrate to NetScaler Console and avail of the management, monitoring, orchestration, and application management features in addition to the analytics features.

- **Single-server deployment**. In a NetScaler Console single server deployment, the database is integrated with the server and a single server processes all the traffic. You can deploy NetScaler Console with Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V, and Linux KVM. See:
  - NetScaler Console with Citrix Hypervisor
  - NetScaler Console with Microsoft Hyper-V
  - NetScaler Console with VMware ESXi
  - NetScaler Console with Linux KVM server
- **High availability deployment.** A high availability deployment (HA) of two NetScaler Console servers provides uninterrupted operations. In a high availability setup, both the NetScaler Console nodes must be deployed in active-passive mode, on the same subnet using the same software version and build, and must have the same configurations. With HA deployment the ability to configure the floating IP address on the NetScaler Console primary node eliminates the need of a separate NetScaler load balancer. To learn more, see Configure in high availability deployment.

Step 3 - Add instances to NetScaler Console

In NetScaler Console, you can discover, manage, and monitor all NetScaler instances that are deployed on-premises or on the cloud. You must add instances to the NetScaler Console server if you want to manage and monitor these instances. You can add the following instances to NetScaler Console:

- NetScaler
  - NetScaler MPX

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

- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler BLX
- NetScaler Gateway

When you add an instance to the NetScaler Console server, the server implicitly communicates with the instances and collects an inventory of these instances.

Learn More

Step 4 - Enable analytics on virtual servers

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.

Learn More

Step 5 - Configure NTP server on NetScaler Console

You have to configure a Network Time Protocol (NTP) server in NetScaler Console to synchronize its clock with the NTP server. Configuring an NTP server ensures that the NetScaler Console clock has the same date and time settings as the other servers on the network.

Learn More

Step 6 - Configure system settings for optimal NetScaler Console performance

Before you start using NetScaler Console to manage and monitor your instances and applications, it is recommended that you configure a few system settings that ensure optimal performance of your NetScaler Console server.

- **Configure system alarms**. 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.
- **Configure system notifications**. You can send notifications to select groups of users for various system-related functions. You can set up a notification server in NetScaler Console, and you can configure email and Short Message Service (SMS) gateway servers to send email and text notifications to users. This ensures that you are notified of any system-level activities such as user login or system restart.

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

- **Configure system prune settings**. To limit the amount of reporting data being stored in your NetScaler Console server's database, you can specify the interval for which you want NetScaler Console to retain network reporting data, events, audit logs, and task logs. By default, this data is pruned every 24 hours (at 00.00 hours).
- **Configure system backup settings**. NetScaler Console automatically backs up the system every day at 00:30 hours. By default, it saves three backup files. You might want to retain more number of backups of the system.
- **Configure instance backup settings**. If you back up the current state of a NetScaler instance, you can use the backup files to restore stability in case the instance becomes unstable. Doing so is especially important before performing an upgrade. By default, a backup is taken every 12 hours and three backup files are retained in the system.
- **Configure instance event prune settings**. To limit the amount of event messages data being stored in your NetScaler Console server's database, you can specify the interval for which you want NetScaler Console to retain network reporting data, events, audit logs, and task logs. By default, this data is pruned every 24 hours (at 00:00 hours).
- **Configure instance syslog purge settings**. To limit the amount of syslog data stored in the database, you can specify the interval at which you want to purge syslog data. You can specify the number of days after which the following syslog data will be deleted from NetScaler Console:
  - Generic Syslog data
  - AppFirewall data
  - NetScaler Gateway data.

  Learn More

What's next

After you have deployed and set up NetScaler Console, you can start managing and monitoring your instances and applications.

Managing NetScaler instances and applications. All NetScaler Console features are supported on NetScaler instances. You can start using any of the features.

Enhanced Graphical User Interface

September 27, 2025

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

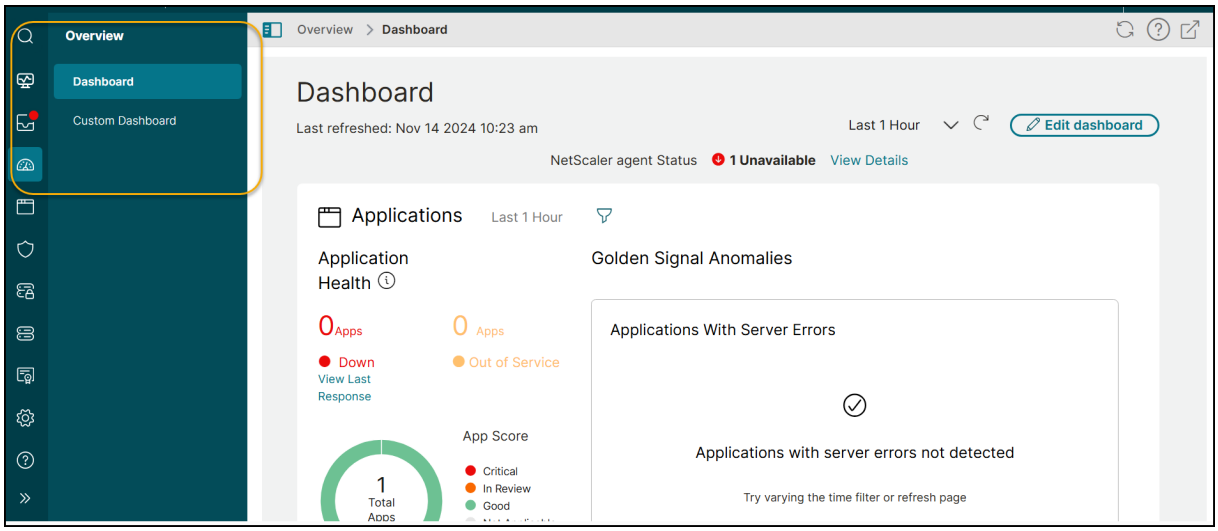
NetScaler Console Graphical User Interface (GUI) provides an enriching experience with several key features. These features provide:

- **Optimized screen space:** Users can show or hide the sidebar based on their preference.
- **Quick access to favorites:** Pin frequently used menu items for faster navigation.
- **Enhanced submenu visibility:** Hover over menu items to reveal submenus, offering a clearer view of all available options.
- **Improved submenu structure:** A consistent, three-level submenu system ensures seamless navigation across NetScaler Console, providing a uniform experience throughout.

This page walks you through the features of the NetScaler Console GUI providing an enriching user experience.

Hover-to-Display menu

Previously, the secondary-level submenu was displayed in a tree structure. NetScaler Console GUI provides a seamless navigation where the secondary menu appears on hover, revealing the submenu. This navigation elevates the viewing experience by displaying all submenu options without the need for scrolling.



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**

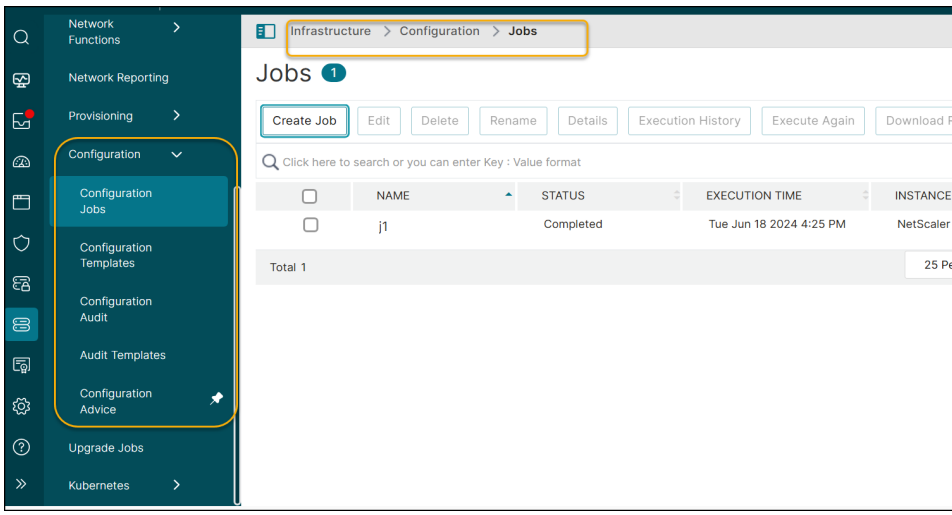
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Gateway > HDX™ Insight**

Updated submenu labels

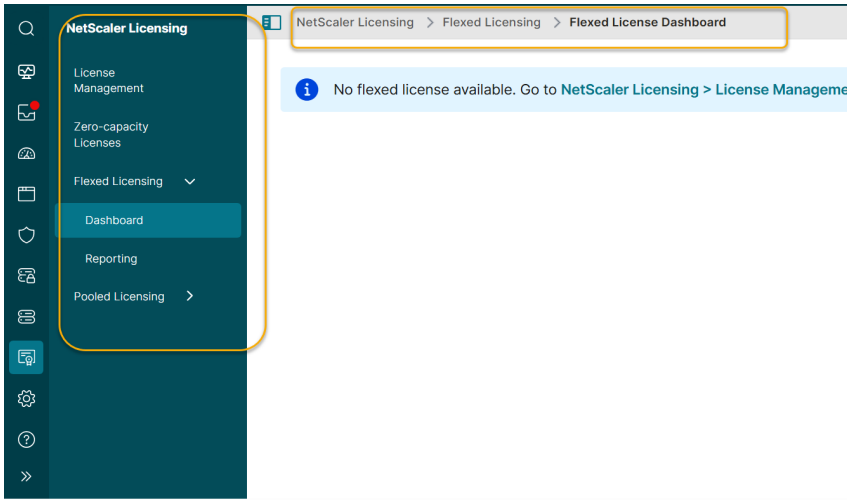
The names of some submenus are changed to align with this navigation approach. Screen navigation changes and submenu label updates are:

Infrastructure > Configuration



Previous screen navigation	Changed screen navigation	Is there a change in the submenu label?
Configuration > Configuration Jobs > Jobs	**Configuration > Configuration Jobs**	Yes
Configuration > Configuration Jobs > Configuration Templates	**Configuration > Configuration Templates**	No
Configuration > Configuration Audit > Overview	**Configuration > Configuration Audit**	Yes
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**

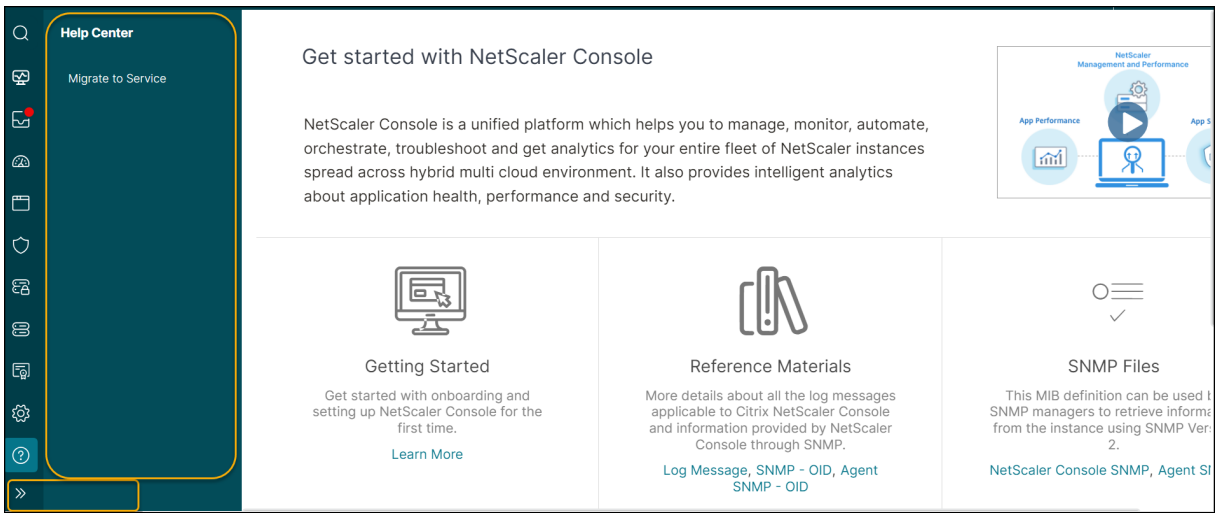
Collapsible menu

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

Expanded menu

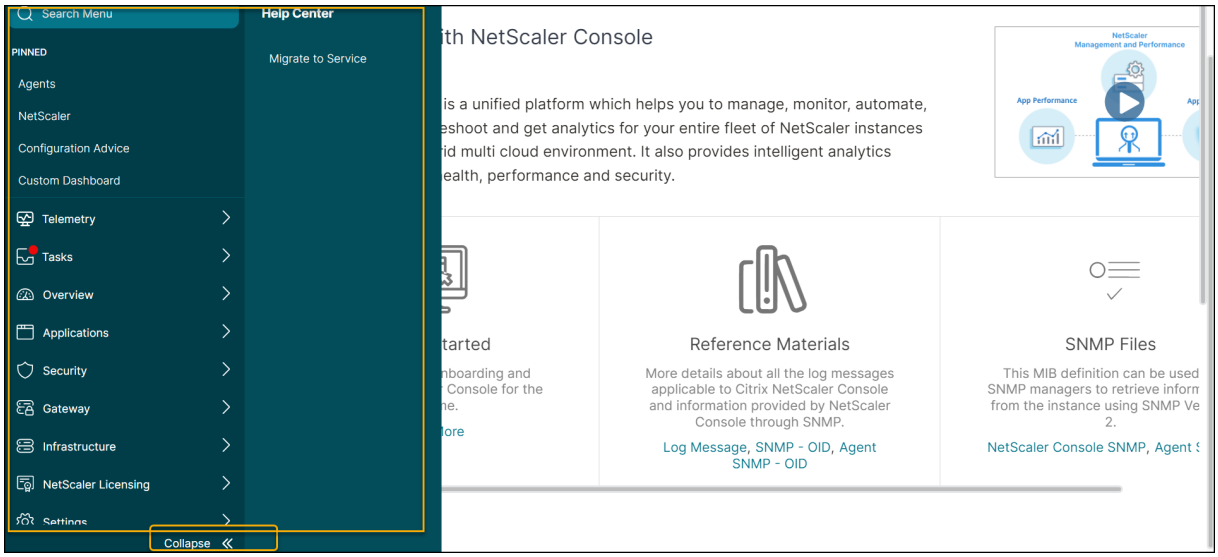
Click the icon » in the pane to expand the entire menu.

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



Collapsed menu

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

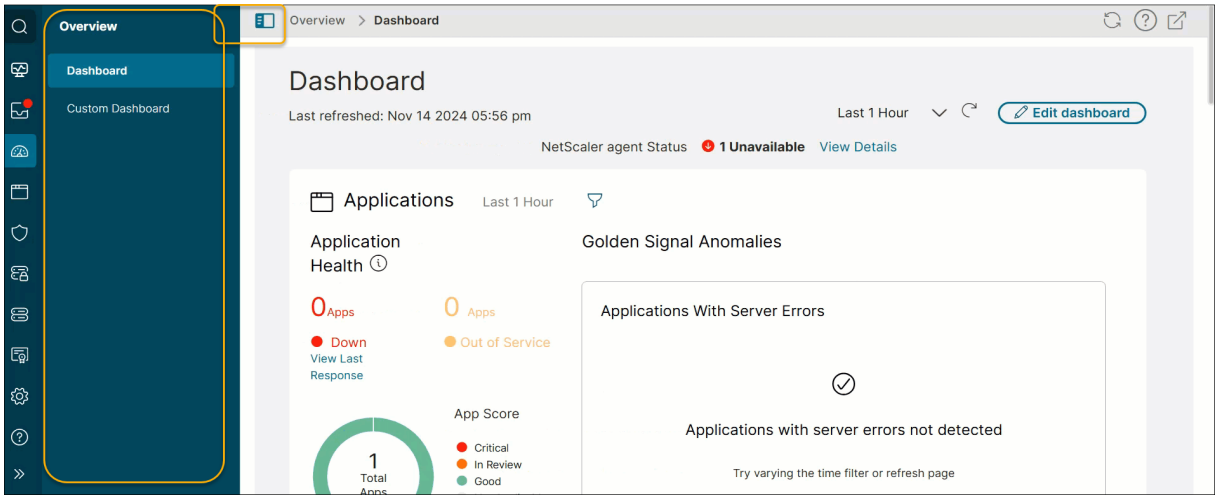


Sidebar Toggle

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

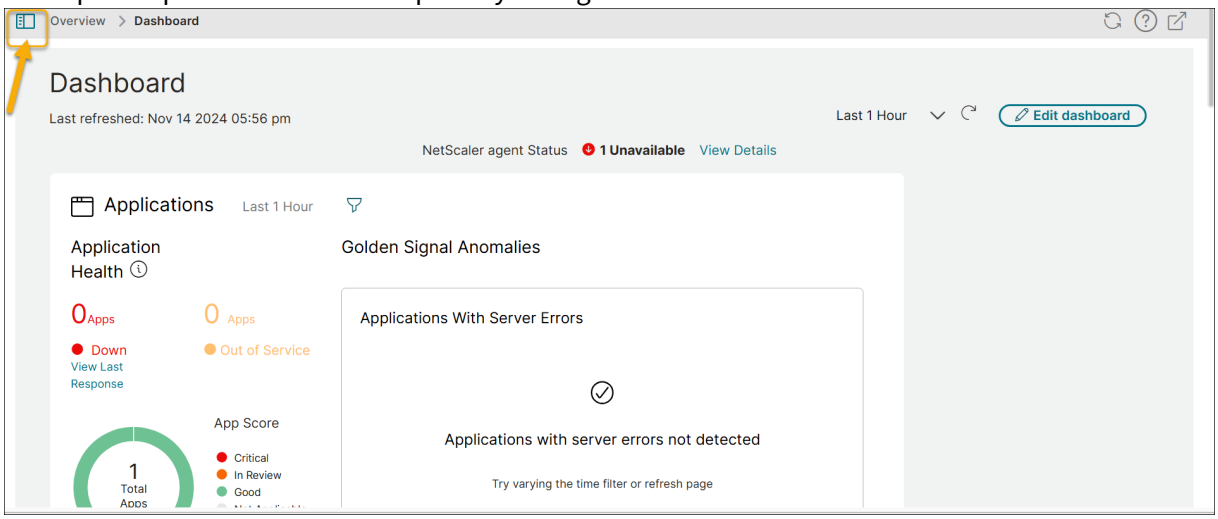
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Show sidebar



Hide sidebar

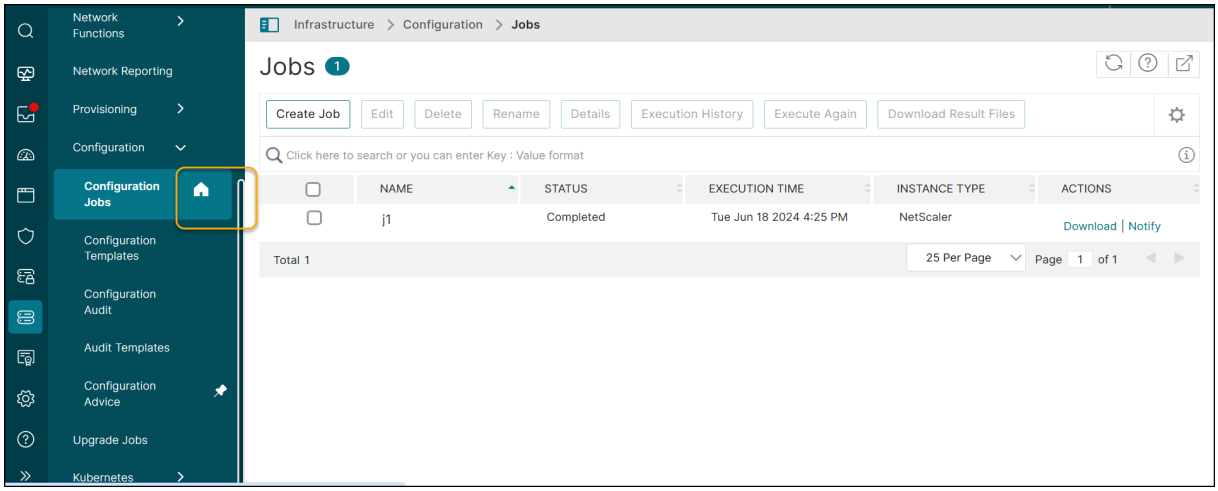
This option optimizes the screen space by hiding the sidebar.



Set as home screen

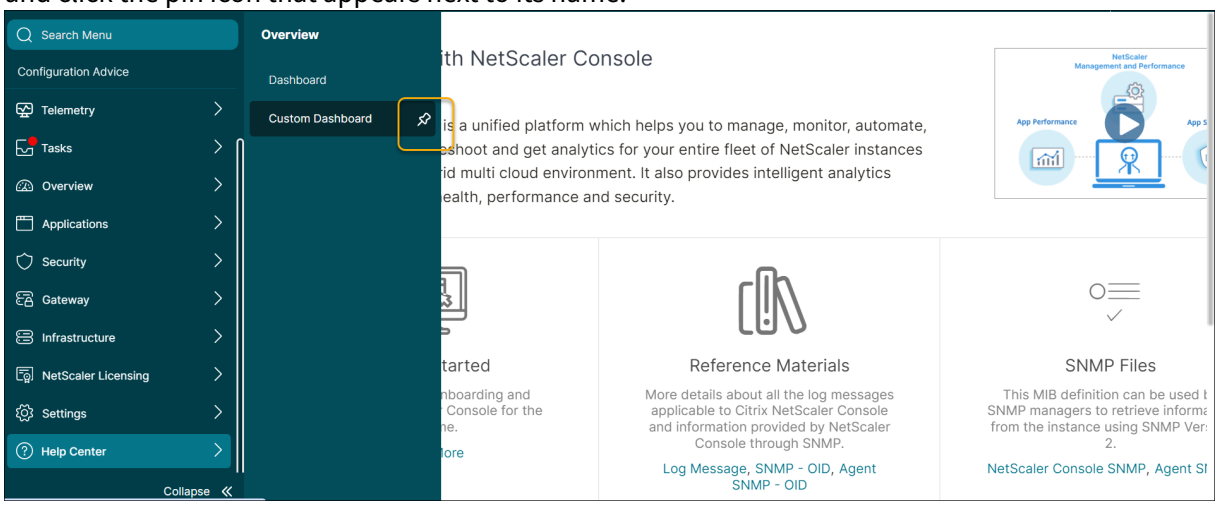
NetScaler Console GUI features an icon next to the name of a submenu that is displayed as a page.The home screen icon allows you to set your landing page. It only appears when you are on that specific page. To remove the page from the home page, simply click the icon again.

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



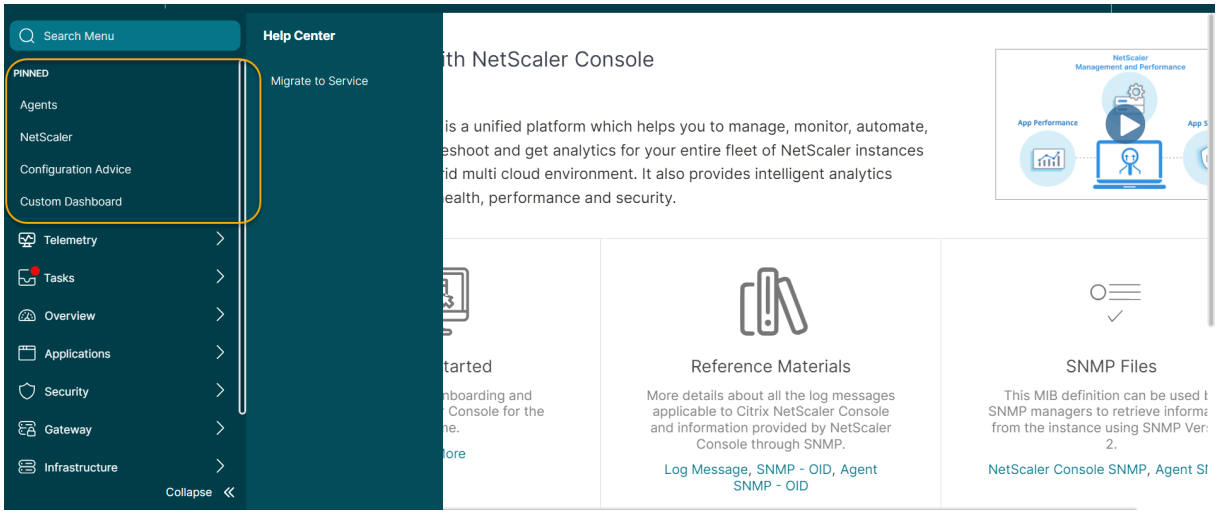
Pin favorite items

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.



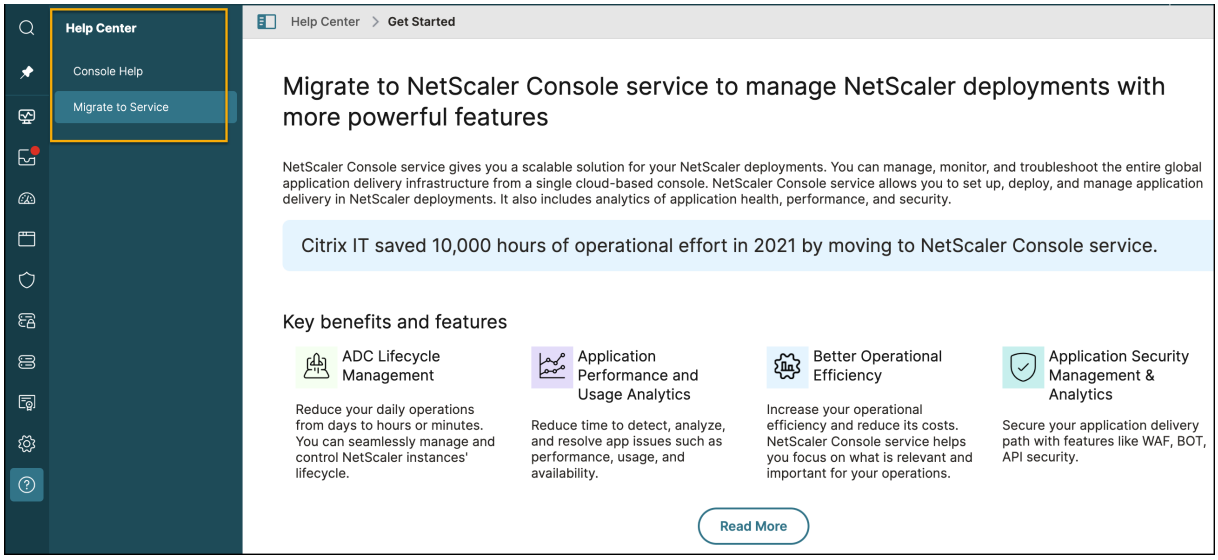
Pinned menus are displayed under **PINNED** in the sidebar, making them easily accessible.

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



Migrate to Service

The option to **Migrate to Service** is now available as a sub-menu to **Help Center**. Previously, this was available as an option in the navigation pane. This streamlines the available options under appropriate menu items.



Deploy

September 27, 2025

Before using NetScaler Console to manage and monitor your applications and network infrastructure, you must first install it on one of the hypervisors or on a Kubernetes cluster. If you deploy NetScaler

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

Console on a hypervisor, you can deploy it either as a single server or in a high-availability mode. High availability mode not is applicable on a Kubernetes cluster. If you are using NetScaler Insight Center, you can migrate to it NetScaler Console and avail of the management, monitoring, orchestration, and application management features in addition to the analytics features.

- **Single-server deployment**: For a standalone NetScaler Console deployed on a hypervisor, the database is integrated with the server and a single server processes all the traffic. You can deploy NetScaler Console with Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V, and Linux KVM. See:
  - NetScaler Console on Citrix Hypervisor
  - NetScaler Console on Microsoft Hyper-V
  - NetScaler Console on Azure
  - NetScaler Console on VMware ESXi
  - NetScaler Console on Linux KVM server
  - NetScaler Console on Nutanix hypervisor (Acropolis)
  - NetScaler Console on Kubernetes Cluster
- **High availability (HA) deployment**: An HA deployment of two NetScaler Console servers provides uninterrupted operations. In an HA setup, both the NetScaler Console nodes must be deployed in active-passive mode, on the same subnet using the same software version and build, and must have same configurations. With HA deployment the ability to configure the floating IP address on the NetScaler Console primary node eliminates the need for a separate NetScaler load balancer. See: Configure in high availability deployment.

  > **Note:**
  >
  > High availability is not applicable for NetScaler Console deployed on a Kubernetes cluster.

- **Lightweight deployment**: If you plan to use NetScaler Console only for Pooled or Flexed licensing, you can deploy with lower specifications. For more information, see Prerequisites.
- **Migrate from NetScaler Insight Center to NetScaler Console**: You can migrate your NetScaler Insight Center deployment to NetScaler Console without losing the existing configuration, settings, or data. With NetScaler Console you can not only view the various analytics generated by the NetScaler, but can also manage, monitor, and troubleshoot the entire global application delivery infrastructure from a single, unified console. See: Migrating from NetScaler Insight Center to NetScaler Console
- **Integrate NetScaler Console with Director**: Director integrates with NetScaler Console for network analysis and performance management. See: Integrate NetScaler Console with Director

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

Prerequisites for installing NetScaler Console

November 21, 2025

You can download and install NetScaler Console for Microsoft HyperV, VMware ESXi, Linux KVM, and Citrix Hypervisor™ platforms as a virtual appliance. Before you install NetScaler Console, you must understand the software requirements, browser requirements, port information, license information, and limitations on all these platforms.

For specific platform requirements and detailed steps to install NetScaler Console, see the following topics:

- NetScaler Console with Citrix Hypervisor
- NetScaler Console with Microsoft HyperV
- NetScaler Console with VMware ESXi
- NetScaler Console with Linux KVM server

General requirements for NetScaler Console

Component	Requirement
RAM	32 GB
Virtual CPU	8 CPUs
Storage space	Citrix recommends using Solid State Drive (SSD) technology for NetScaler Console deployments. The default storage space required is 120 GB. Actual storage requirement depends on NetScaler Console sizing estimation. If your NetScaler Console storage requirement exceeds 120 GB, you to have to attach an extra disk. Citrix recommends you to estimate storage and attach an extra disk at the time of initial deployment. You can add only one extra disk. For more information, see How to Attach an Additional Disk to NetScaler Console.
Virtual network interfaces	1

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

Component	Requirement
Throughput	1 Gbps

Lightweight NetScaler® Console only for Pooled or Flexed licensing

You can use NetScaler Console only for Pooled or Flexed licensing with lower specifications:

Component	Requirement
RAM	8 GB
Virtual CPU	4
Storage	120 GB

> **Note:**
>
> Citrix recommends you to host the NetScaler Console VHD on a local storage. When hosted on storage devices in a SAN, NetScaler Console might not work as expected. So, NetScaler Console deployment on SAN is not supported.

NetScaler Console on Citrix Hypervisor

September 27, 2025

To install NetScaler Console on Citrix Hypervisor (formerly known as XenServer), you need to first download the NetScaler Console .xva image file to your local computer. You need to use Citrix XenCenter to perform the NetScaler Console installation.

> **Note:**
>
> NetScaler Console does not support XenMotion.

Prerequisites

Before installing NetScaler Console, verify that the following requirements have been met:

- Citrix Hypervisor version 7.1 or later is installed on hardware that meets the minimum requirements.

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

- XenCenter is installed on a management workstation that meets the minimum requirements. You have to use XenCenter to install NetScaler Console on Citrix Hypervisor.
- You have downloaded the NetScaler Console .XVA image file.

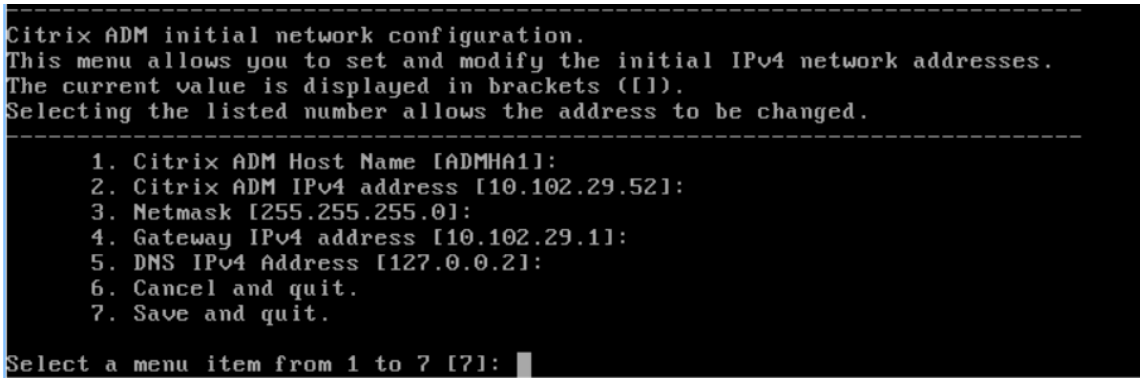
XenCenter® system requirements

XenCenter is a Windows client application. It cannot run on the same machine as the Citrix Hypervisor™ host. The following table describes the minimum system requirements.

Component	Requirement
Operating System	Windows 7, Windows Server 2003, or Windows 10
.NET framework	Version 2.0 or later
CPU	750 MHz (MHz), Recommended: 1 gigahertz (GHz) or faster
RAM	1 GB, Recommended: 2 GB
NIC	100 megabits per second (Mbps) or faster NIC

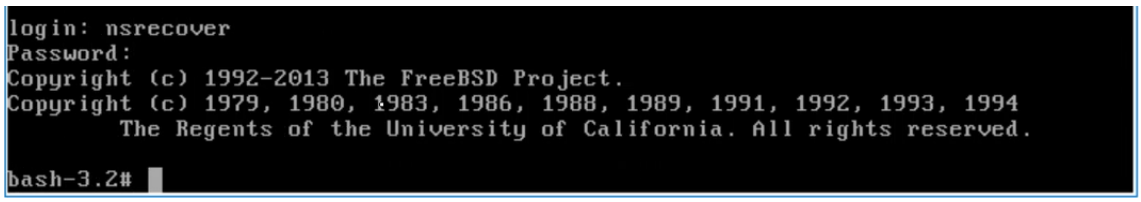
Install NetScaler® Application Delivery Management

1. Import the XVA image file to your Citrix Hypervisor, and from the **Console** tab configure the initial network configuration options.



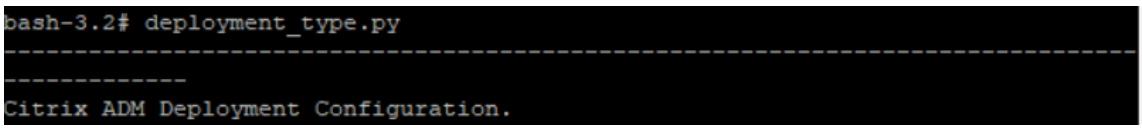
2. After specifying the required IP addresses, save the configuration settings.
3. When prompted, log on using nsrecover/nsroot credentials.

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



> **Note**
>
> After you log on, if you want to update the initial network configuration, type `networkconfig`, update the configuration, and save the configuration.

4. Run the deployment script by typing the command at the shell prompt: `/mps/deployment_type.py`



5. Select the deployment type as **NetScaler Console Server**. If you do not select any option, by default, it is deployed as a server.



6. Type **Yes** to deploy NetScaler Console as a standalone deployment.
7. Type **Yes** to restart the NetScaler Console server.

> **Note**
>
> After you install NetScaler Console, you can update the initial configuration settings later.

Verification

After the server is installed, you can access the GUI by typing the IP address of the NetScaler Console server in the web browser. The default administrator credentials to log on to the server are nsroot/nsroot.

The browser displays the NetScaler Console configuration utility.

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

NetScaler Console on Microsoft Hyper-V

September 27, 2025

To install NetScaler Console on Microsoft Hyper-V, you must first download the NetScaler Console image file to your local computer. Also, ensure that your system has the hardware virtualization extensions, and verify that the CPU virtualization extensions are available.

Prerequisites

Before installing the NetScaler Console virtual appliance, verify that the following requirements have been met:

- Microsoft Hyper-V version 6.2 or later is installed on hardware that meets the minimum requirements.
- Install Microsoft Hyper-V Manager on a management workstation that meets the minimum system requirements.
- You have downloaded the NetScaler Console image file.

Microsoft Hyper-V system requirements

Microsoft Hyper-V is a Windows client application. The following table describes the minimum system requirements.

Component	Requirement
Operating System	Windows Server 2012 R2
.NET framework	Version 2.0 or later
CPU	750 MHz (MHz), Recommended: 1 gigahertz (GHz) or faster
RAM	1 GB, Recommended: 2 GB
NIC	100 megabits per second (Mbps) or faster NIC

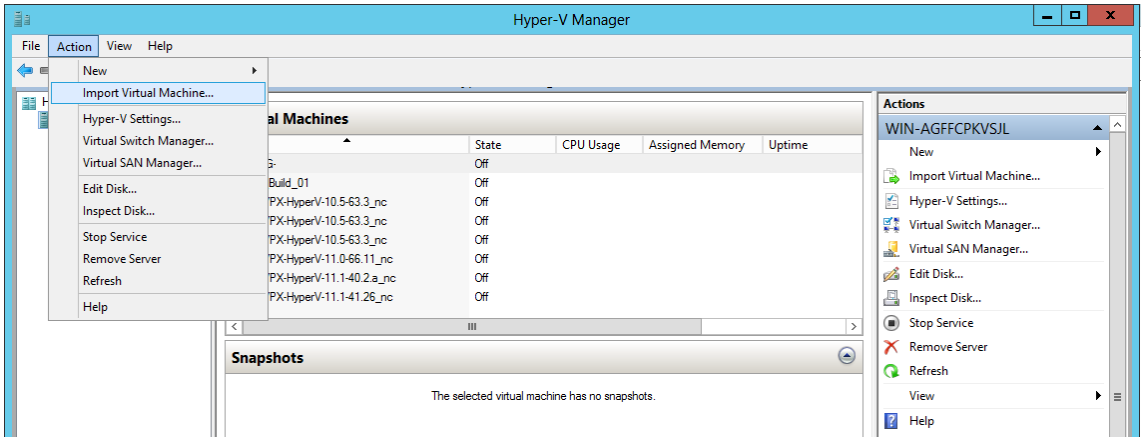
Installing NetScaler® Application Delivery Management

The number of NetScaler Console servers that you can install depends on the memory available on the Hyper-V server.

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

To install NetScaler Console:

1. Start the Hyper-V Manager client on your workstation.
2. On the **Action** menu, click **Import Virtual Machine**.



3. Import the Hyper-V image, and do the following:

   a) In the Import Virtual Machine dialog box, in **Locate Folder** section, browse to the folder in which you saved the NetScaler Console Hyper-V image, select the folder, and click **Next**.

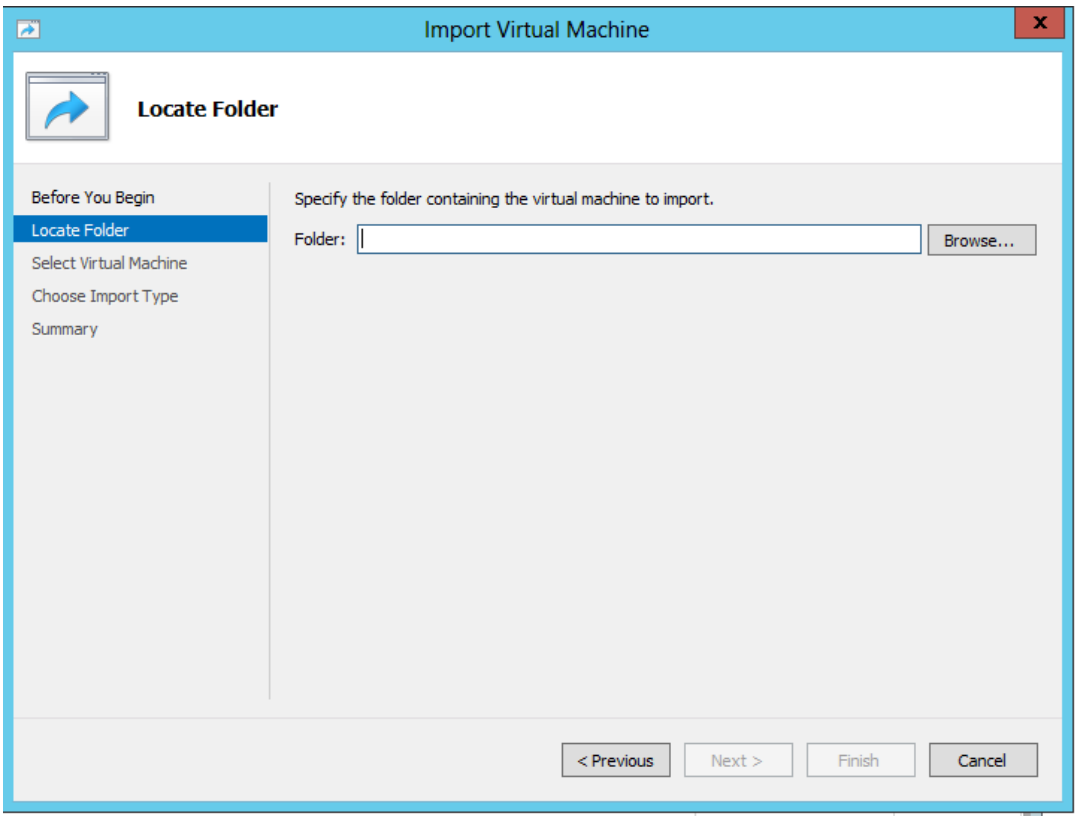
   b) In the Select virtual machine section, select the appropriate virtual machine name.

   c) In the **Choose Import Type** section, select Copy the virtual machine (create a new unique ID) option and click Next.

   d) In the **Choose Destination** section, you can specify the folders to store the virtual machine files.

   > **Note**
   >
   > By default the wizard imports the virtual machine files to default Hyper-V folders on your local host.

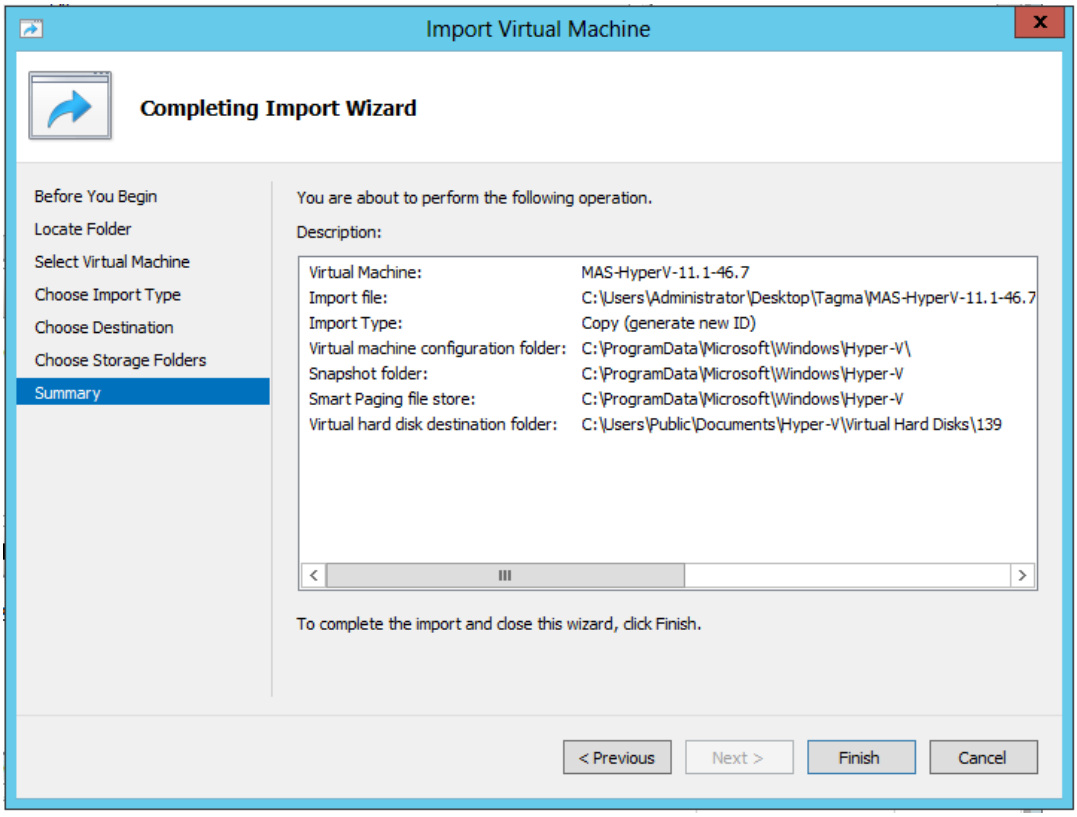
© 1997–2025 Citrix Systems, Inc. All rights reserved.



e) In the **Choose Storage Folders** section, you can select the location in which you want to store the virtual hard disks, and then click **Next**.

f) You can verify the Virtual Machine details in the summary pane, click **Finish**.

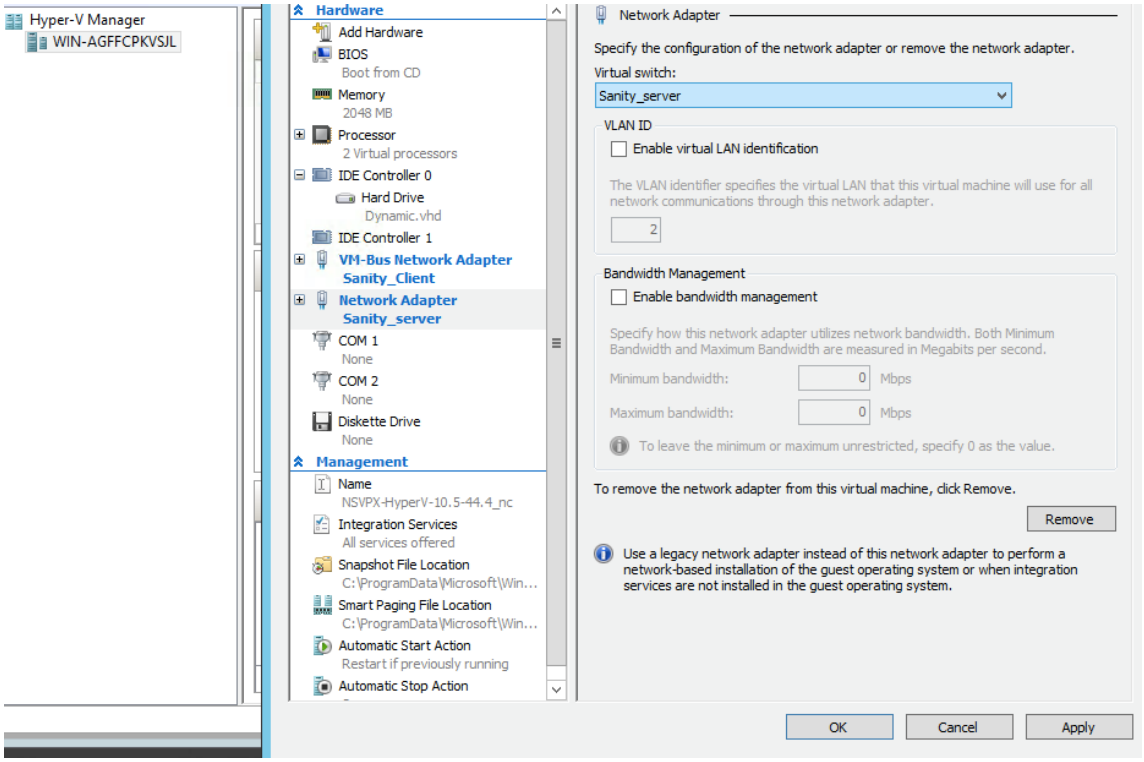
© 1997–2025 Citrix Systems, Inc. All rights reserved.



The NetScaler Console Hyper-V image is displayed in the right pane.

4. Right-click the NetScaler Console Hyper-V image, and then click **Settings**.
5. In the left pane of the dialog box that appears, navigate to **Hardware** > **VM_Bus Network Adaptor**, and in the right pane, from the Network list, select the appropriate network.

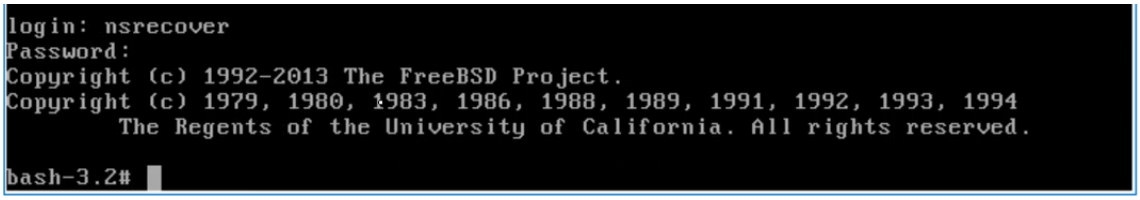
© 1997–2025 Citrix Systems, Inc. All rights reserved.



6. Click **Apply**, and then click **OK**.
7. Right-click the NetScaler Console Hyper-V image and click **Connect**.
8. On the Console window, click **Start** button.
9. Configure the initial network configuration options.



10. After specifying the required IP addresses, save the configuration settings.
11. When prompted, log on using nsrecover/nsroot credentials.



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

> **Note**
>
> After you log on, if you want to update the initial network configuration, type `networkconfig`, update the configuration, and save the configuration.

12. Run the deployment script by typing the command at the shell prompt:

```
deployment_type.py
```

```
bash-3.2# deployment_type.py
------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
```

13. Select the deployment type as **NetScaler Console Server**. If you do not select any option, by default, it is deployed as a server.

```
------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

14. Type **Yes** to deploy NetScaler Console as a standalone deployment.
15. Type **Yes** to restart the NetScaler Console server.

> **Note**
>
> After you install NetScaler Console, you can update the initial configuration settings later.

Verification

After the server is installed, you can access the GUI by typing the IP address of the NetScaler Console server in the address bar of your browser. The default administrator credentials to log on to the server are nsroot/nsroot.

The browser displays the NetScaler Console configuration utility.

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

NetScaler Console on VMware ESXi

September 27, 2025

This document describes how to install NetScaler Console virtual appliances on VMware ESXi, using the VMware vSphere client.

Prerequisites

Before you begin installing a virtual appliance, verify that the following requirements:

- Install a supported VMware ESXi version. For the list of supported versions, see Supported hypervisors.
- Install VMware Client on a management workstation that meets the minimum system requirements.
- Download the NetScaler Console setup files.

> Note
>
> - VMotion is supported only from **NetScaler Console 13.0 Build 47.22 or later**. You can schedule and automate migration of the NetScaler Console server deployed on an ESXi hypervisor, including vSphere high availability and vSphere DRS setups.
> - VMware Tools for NetScaler Console are delivered as part of the software build and they cannot be upgraded or modified separately.

To install NetScaler Console

Follow these steps to install a NetScaler Console virtual appliance on VMware ESXi.

> **Note**
>
> The steps and screen captures are based on VMware ESXi version 6.0. The GUI might differ in other ESXi versions. VMware ESXi version 7.0.1c build number 17325551 with VMXNET3 adapter is supported in **NetScaler Console 13.0 71.40 or later**. Refer to the VMware documentation for version-specific steps.

1. Start the VMware vSphere client on your workstation.
2. In the **IP address / Name** text box, type the IP address of the VMware ESXi server that you want to connect to.

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

3. In the **User Name** and **Password** text boxes, type the administrator credentials, and then click **Login**.
4. On the **File** menu, click **Deploy OVF Template**.
5. In the **Deploy OVF Template** dialog box, in **Deploy from a file or URL**, select the .ovf file, and click **Next**.

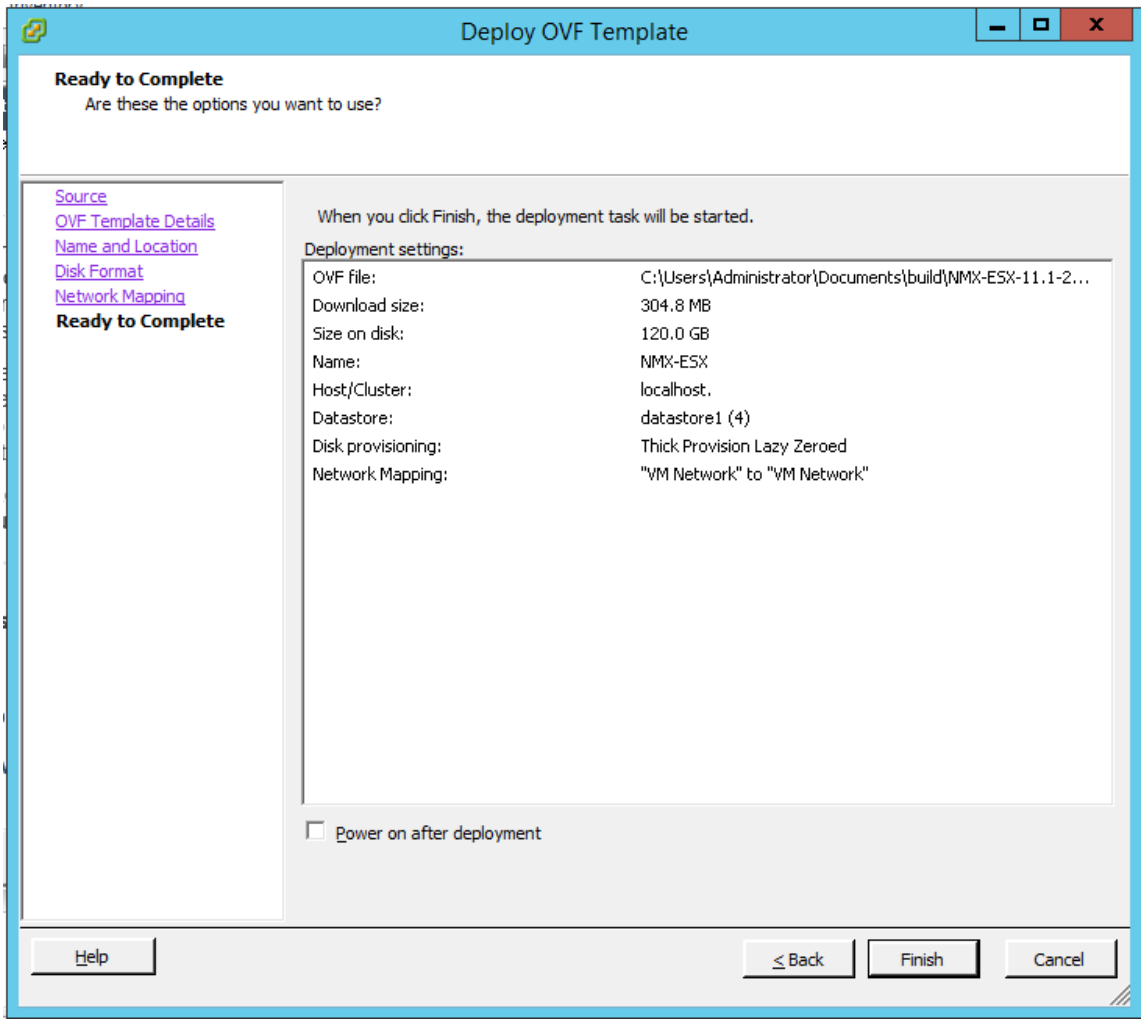
   > **Note**
   >
   > If a warning message appears with the following text: "The operating system identifier is not supported on the selected host, check to see if the VMware server supports the FreeBSD operating system."Click **Yes**.

6. On the **OVF Template Details** page, click **Next**.
7. Type a name for the NetScaler Console virtual appliance, and then click **Next**.
8. Specify the Disk Format by selecting either Thin provisioned format or Thick provisioned format.

   > **Note**
   >
   > We recommend you to select **Thick provisioned format**.

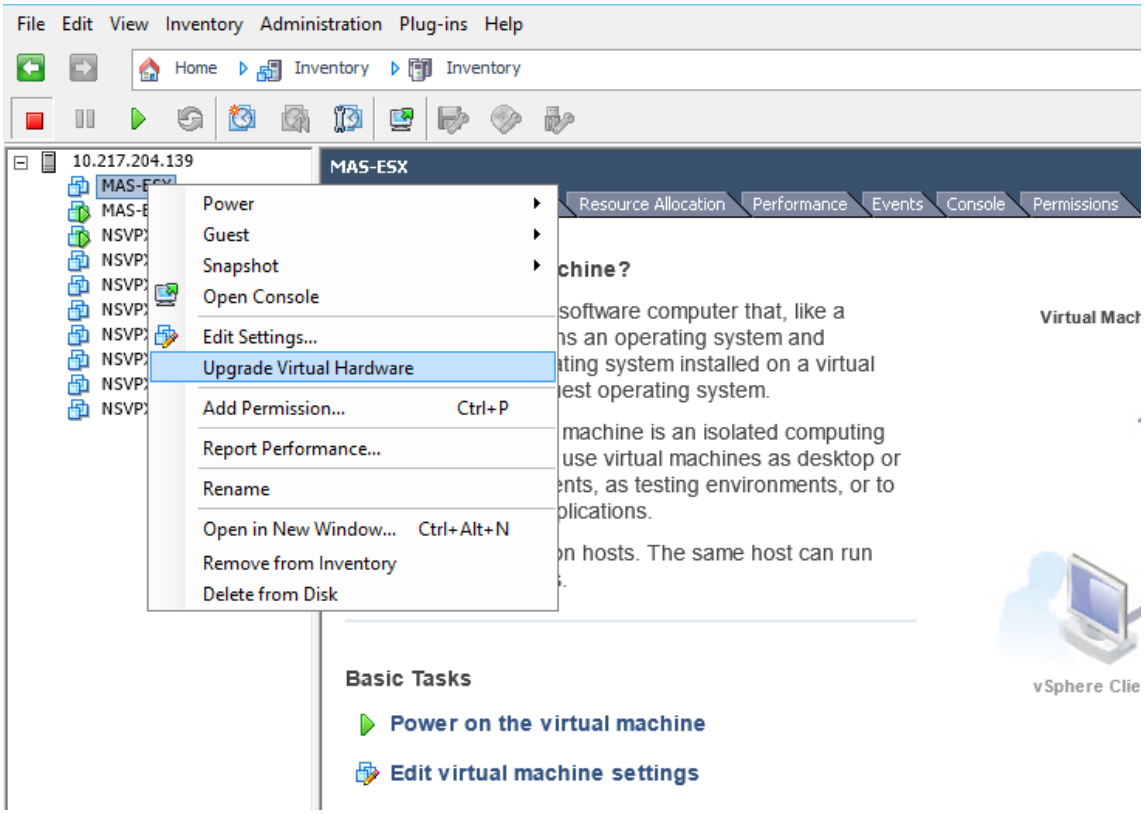
9. Click **Finish** to start the installation process.

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



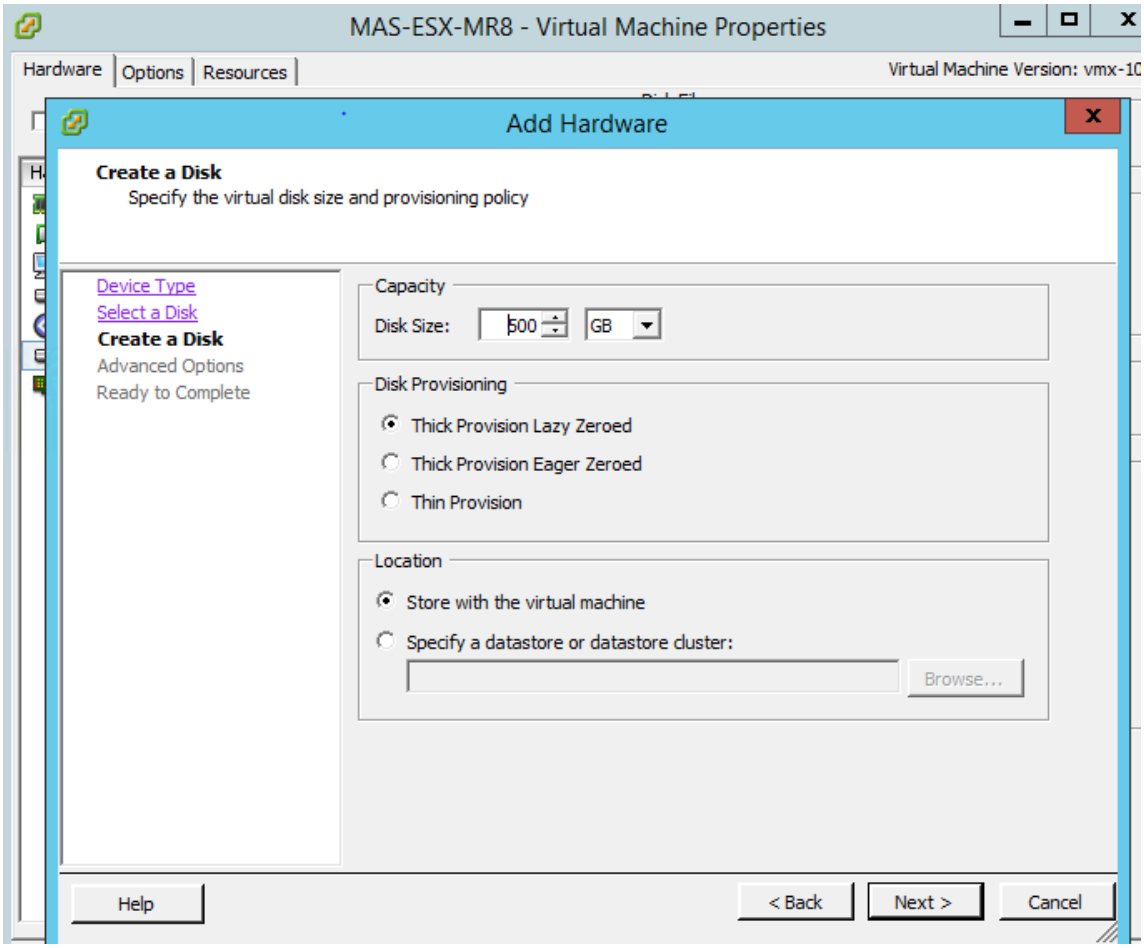
10. You are now ready to start the NetScaler Console virtual appliance.
11. In the navigation pane, select the virtual appliance that you installed. From the **Inventory** menu, right-click on the **Virtual Machine**, and then click **Upgrade Virtual Hardware**. In the **Confirm Virtual Machine** dialog box, click **Yes**.

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

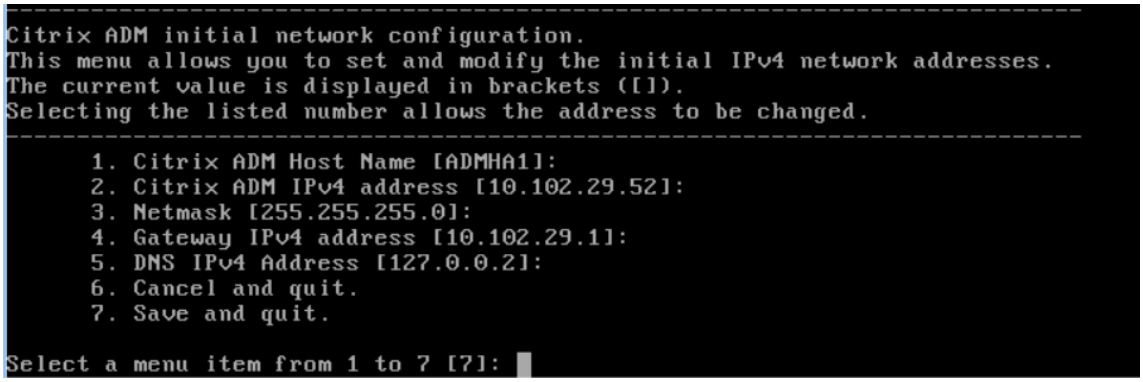


12. In the **Inventory** menu, click **Virtual Machine**, and then click **Edit Settings**.
13. In the **Virtual Machine Properties** dialog box, on the **Hardware** tab, click **Memory**, and then in the right pane specify the **Memory Size** as 32 GB.
14. Click **CPUs**, and then in the right pane, specify the CPUs as 8. Click **OK**.
15. Add an extra disk as per your requirement.

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

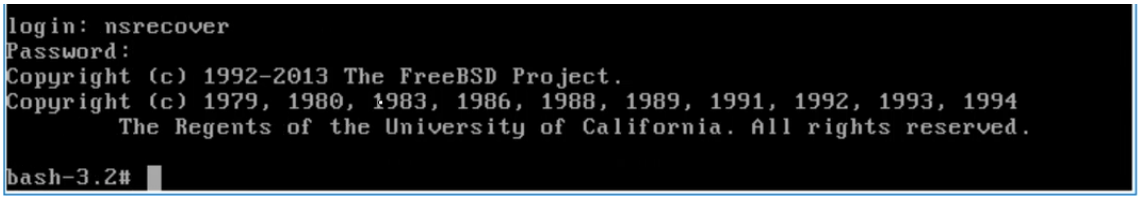


16. In the navigation pane, select the virtual appliance that you installed. From the **Inventory** menu, click **Virtual Machine**, click **Power**, and then click **Power On**.
17. Click the **Console** tab to display the NetScaler Console Initial Network Configuration options.



18. After specifying the required IP addresses, save the configuration settings.
19. When prompted, log on using nsrecover/nsroot credentials.

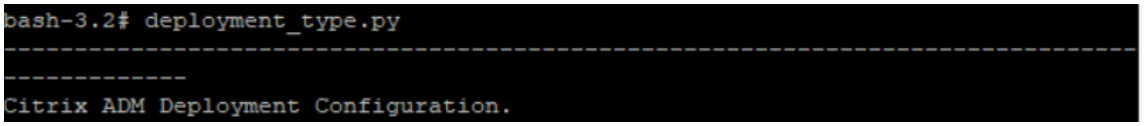
© 1997–2025 Citrix Systems, Inc. All rights reserved.



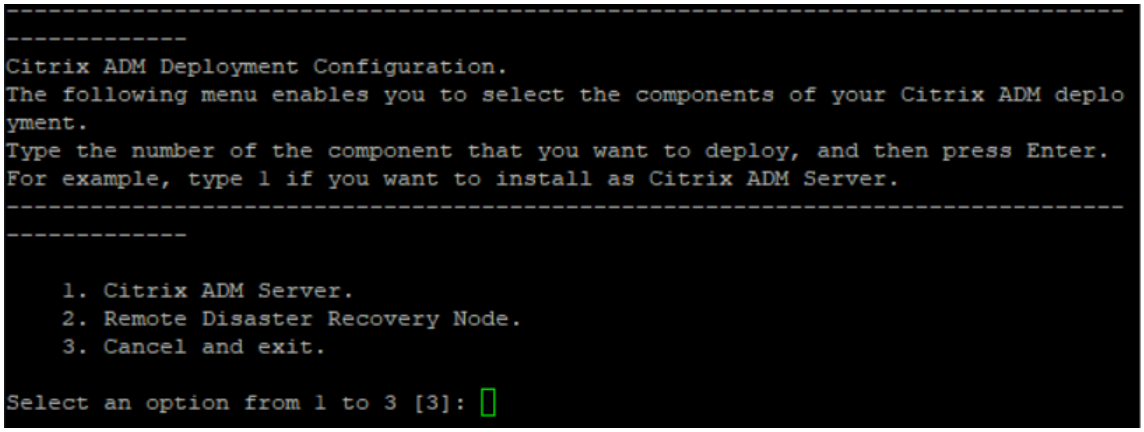
> **Note**
>
> After you log on, if you want to update the initial network configuration, type `networkconfig`, update the configuration, and save the configuration.

20. Run the deployment script by typing the command at the shell prompt:

```
1 deployment_type.py
```



21. Select the deployment type as **NetScaler Console Server**. If you do not select any option, by default, it is deployed as a server.



22. Type **Yes** to deploy NetScaler Console as a standalone deployment.
23. Type **Yes** to restart the NetScaler Console server.

> **Note**
>
> After you install NetScaler Console, you can update the initial configuration settings later.

Verification

After the server is installed, you can access the GUI by typing the IP address of the NetScaler Console server in the browser. The default administrator credentials to log on to the server are nsroot/nsroot.

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

The browser displays the NetScaler Console configuration utility.

> **Note**
>
> Typical NetScaler Console installation time is around 10 minutes on VMware ESXi but might take longer on some systems.

Automate deployment of NetScaler® agent on VMware ESXi

September 27, 2025

NetScaler Console allows you to automate the deployment of NetScaler agents on VMware ESXi.

As an admin, you can automate the following actions:

- Configure the NetScaler agent
- Register the NetScaler agent and change the default password of the agent.

Configure the NetScaler agent

To automate the configuration of the agent, add the values for the following parameters in the .ovf file:

1. `IPAddress`
2. `Netmask`
3. `Gateway`
4. `Nameserver`
5. `Hostname`

> **Note:**
>
> The .ovf file is available in the agent image file. To download the NetScaler agent file, go to https://www.citrix.com/downloads/citrix-application-management/. The naming pattern of the agent image file is as follows, **MASAGENT-ESX-releasenumber-buildnumber.zip**

Register the NetScaler agent and change the default password

> **Note:**
>
> Before registering and changing the default password, make sure that you have added the parameters specified in Configure the NetScaler agent.

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

To automate the registering of the NetScaler agent and the changing of the default password, add the values for the following parameters in the same .ovf file:

1. `NetScaler Console Server IP`
2. `NetScaler Console Username`
3. `NetScaler Console Password`
4. `Agent New Password`

Prerequisites

Before you begin installing a virtual appliance, make sure you:

- Install VMware vSphere 8.x on a management workstation that meets the minimum system requirements.
- Download the NetScaler Console setup files.

How to configure and register a NetScaler agent

1. Download and edit the .OVF file
2. Install NetScaler Console virtual appliance on VMware ESXi
3. Verify

Step 1: Download and edit the .OVF file

1. Extract the files from the **MASAGENT-ESX-releasenumber-buildnumber.zip** to the desired location. The following files are extracted:
   - .ovf file
   - .vmdk file
   - .ova file
   - .mf file
2. Open the .ovf file in any editor and add the following `<ProductSection>..</ProductSection>` sample code after the `</VirtualHardwareSection>` tag

```
<ProductSection>
<Info>Information about the installed software</Info>
<Product>Application Delivery management</Product>
<Vendor>Citrix</Vendor>

<Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
    string"
```

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

```
ovf:key="eth0.ip">
<Label>IPAddress</Label>
</Property>

<Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
    string"
ovf:key="eth0.netmask">
<Label>Netmask</Label>
</Property>

<Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
    string"
ovf:key="eth0.gateway">
<Label>Gateway</Label>
</Property>

<Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
    string"
ovf:key="eth0.nameserver">
<Label>Nameserver</Label>
</Property>

<Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
    string"
ovf:key="eth0.hostname">
<Label>Hostname</Label>
</Property>

<Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
    string"
ovf:key="eth0.ServerIP">
<Label>NetScaler Console Server IP</Label>
</Property>

<Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
    string"
ovf:key="eth0.ServerUname">
<Label>NetScaler Console Username</Label>
</Property>

<Property ovf:userConfigurable="true" ovf:password="true" ovf:
    value="VALUE"
ovf:type="string" ovf:key="eth0.ServerPassword">
<Label>NetScaler Console Password</Label>
</Property>

<Property ovf:userConfigurable="true" ovf:password="true" ovf:
    value="VALUE"
ovf:type="string" ovf:key="eth0.NewPassword">
<Label>Agent New Password</Label>
</Property>

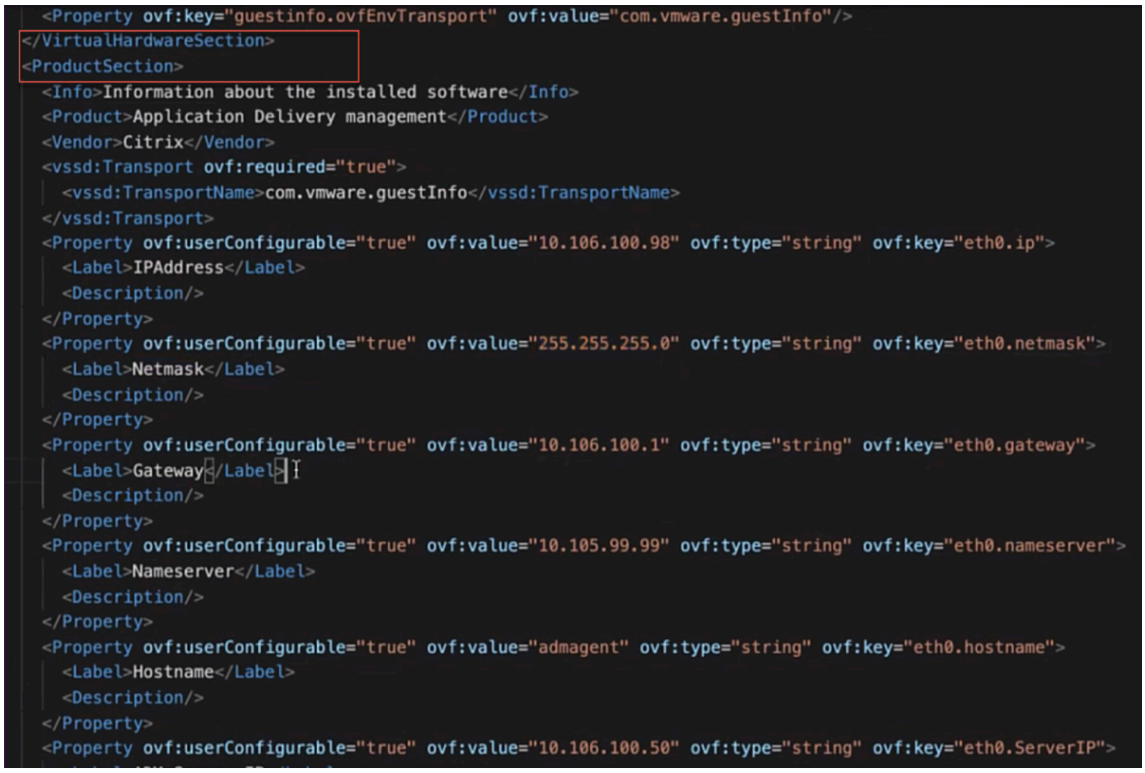
</ProductSection>
```

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

3. For the parameters which you want to configure, add their corresponding values in ovf:value=” VALUE”

   - To configure the NetScaler agent, add the values to the following parameters:
     - `IPAddress`
     - `Netmask`
     - `Gateway`
     - `Nameserver`
     - `Hostname`
   - To register and change the default password of the NetScaler agent, add the values to the following parameters:
     - `NetScaler Console Server IP`
     - `NetScaler Console Username`
     - `NetScaler Console Password`
     - `Agent New Password`

   > **Note:**
   >
   > - You must configure the NetScaler agent before you register and change the default password of the agent.
   > - If you do not register and change the default password in the .ovf file, perform these actions manually after the VM is deployed.

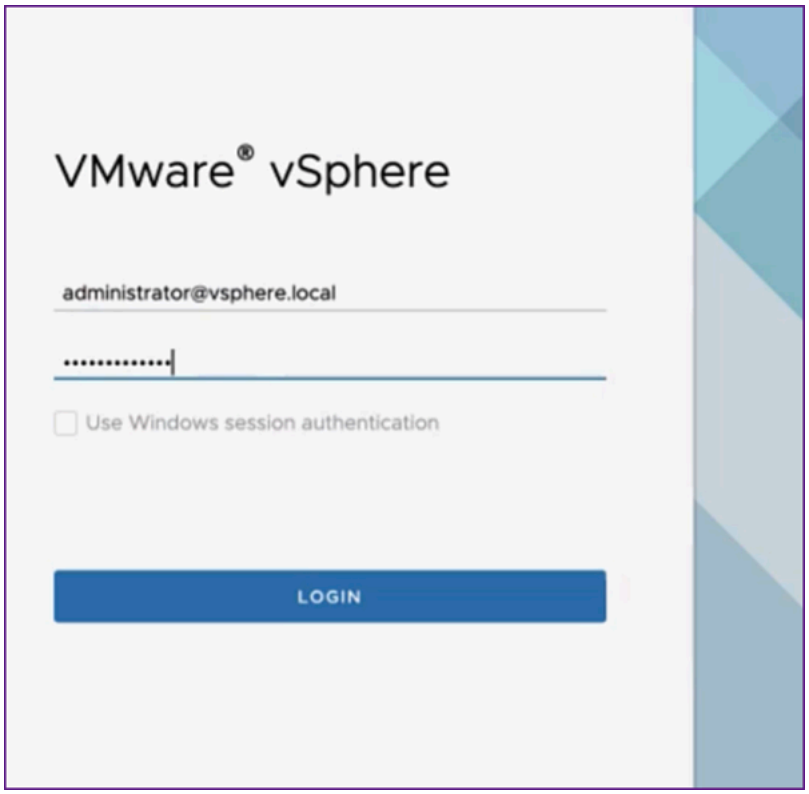


© 1997–2025 Citrix Systems, Inc. All rights reserved.

4. After adding the parameters and their values, save the .ovf file.

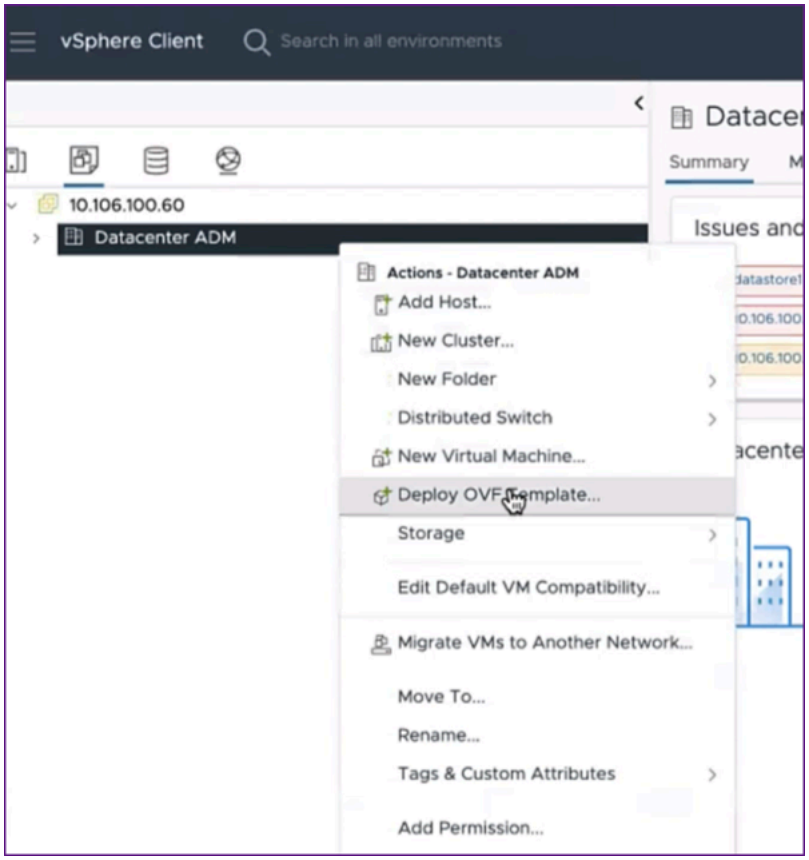
Step 2: Install NetScaler Console virtual appliance on VMware ESXi

1. Log in to the **VMWare vSphere Client** and type the administrator credentials. Click **Login**.



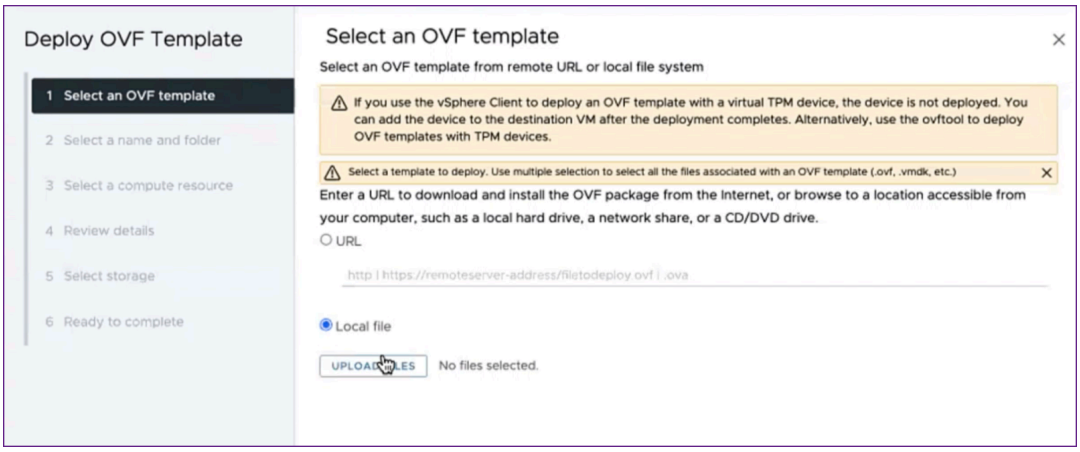
2. Select your ESXi server, and right-click to select **Deploy OVF Template**.

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



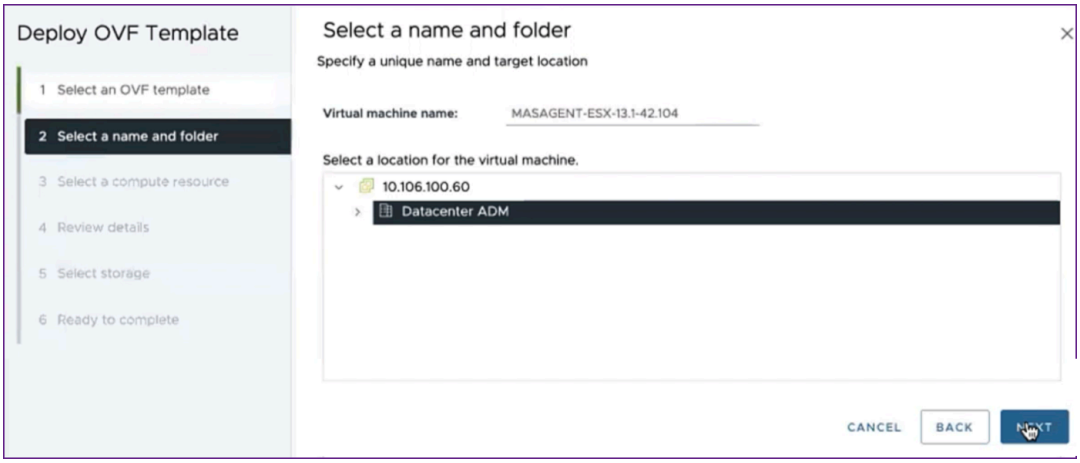
3. In the **Deploy OVF Template** page:

   a) **Select an OVF template**: Select **Local file** and navigate to where you have saved the edited .ovf file and the .vmdk file. Select the files and click **Open** to upload them. Click **Next**.

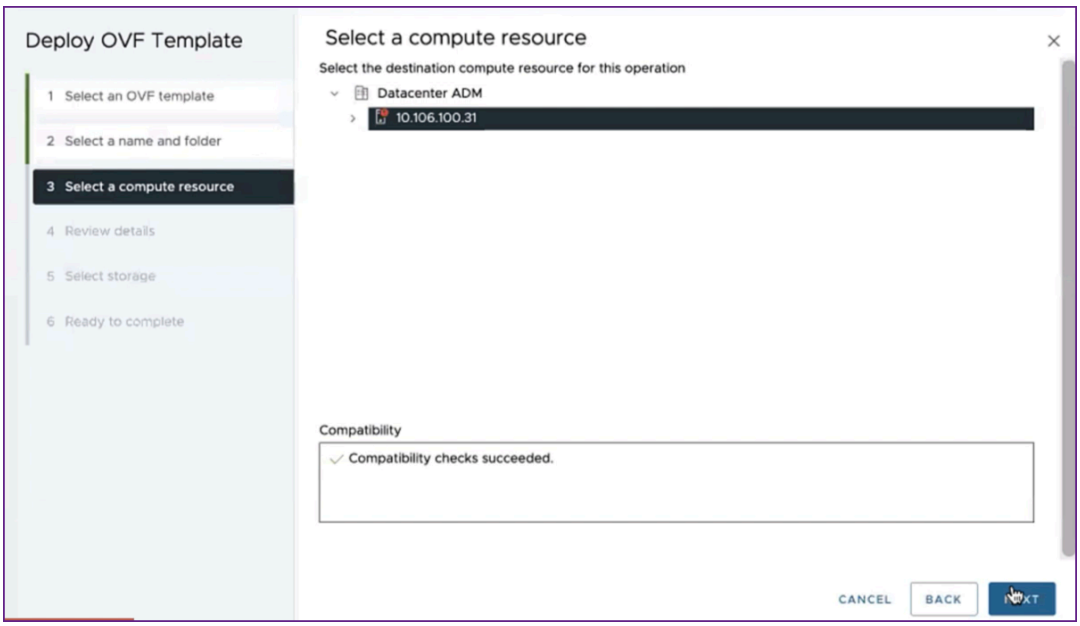


   b) **Select a name and folder**: Add a name for the virtual appliance and select the location on the ESXi where you want to deploy the virtual machine. Click **Next**.

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

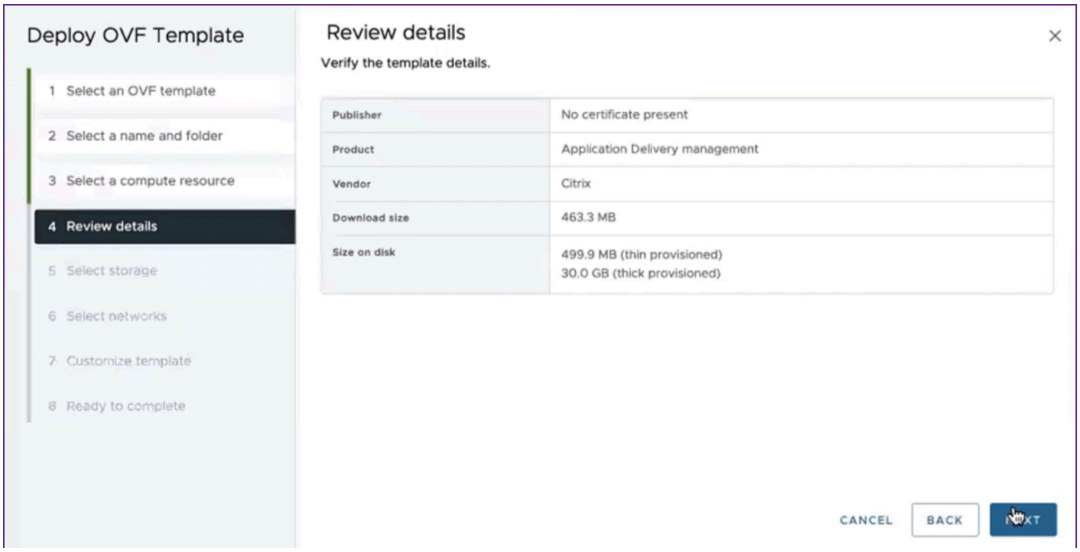


c) **Select a compute resource**: Select a resource on which to run the template after it is deployed. Click **Next**.

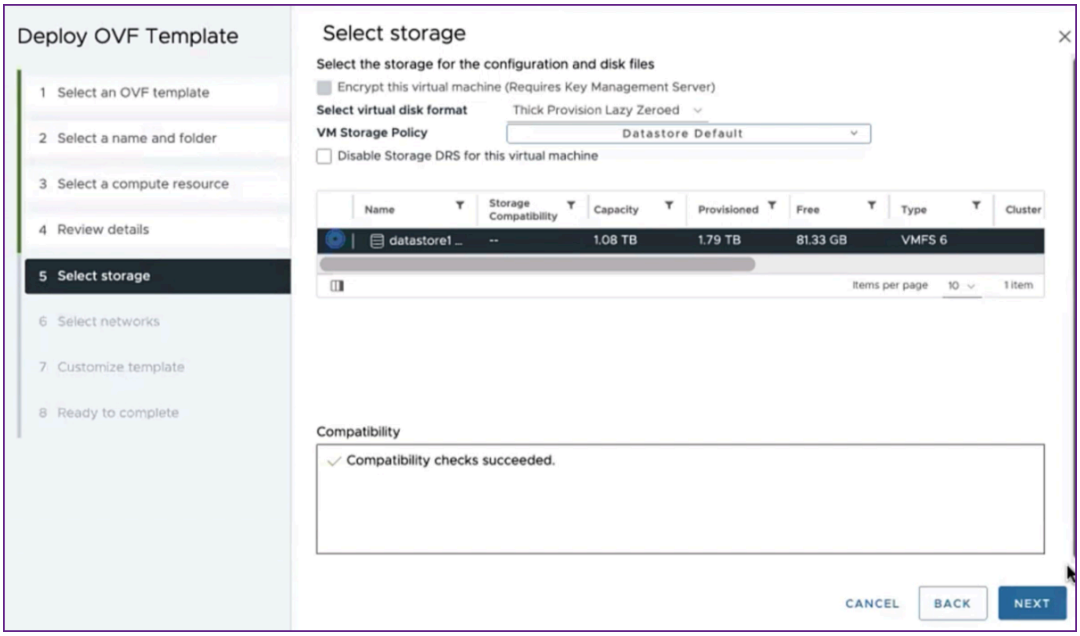


d) **Review details**: Verify the OVF template details. Click **Next**.

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

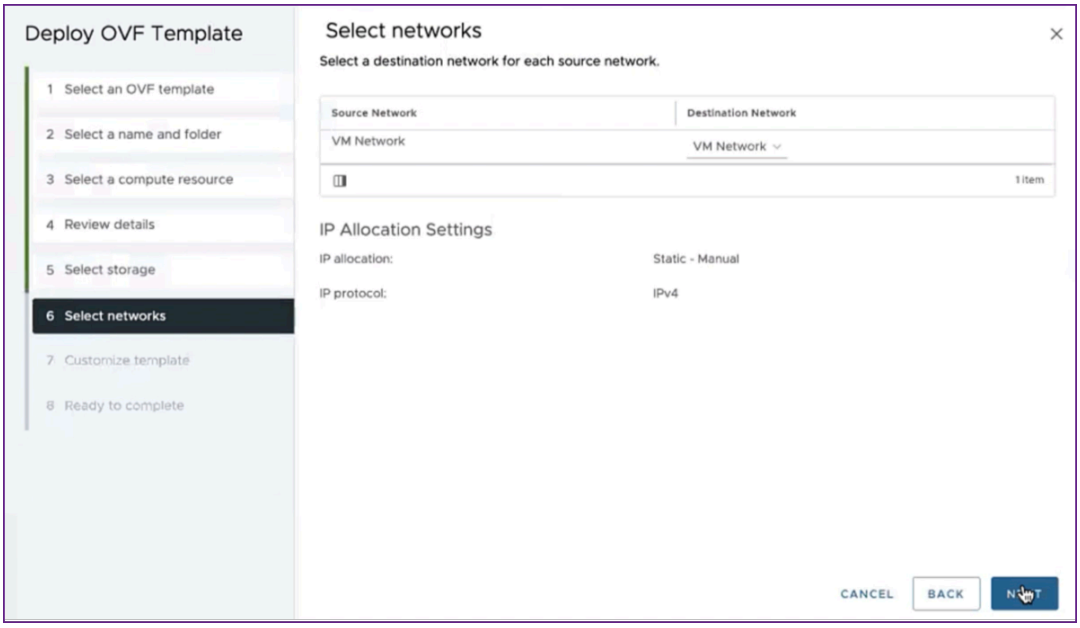


e) **Select storage**: Select a datastore to store the OVF template. Click **Next**.

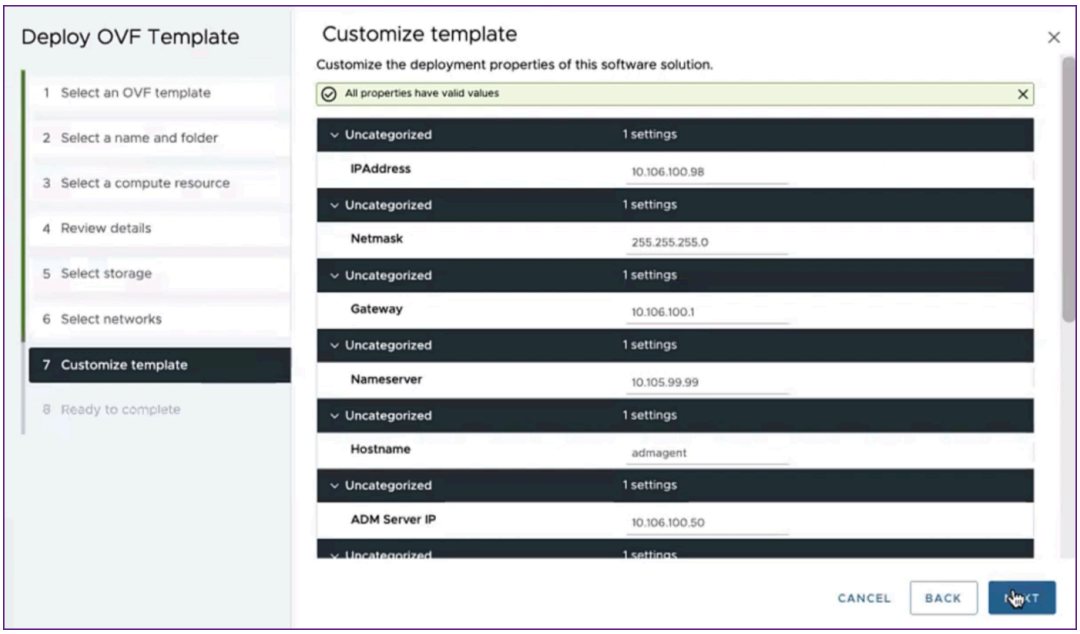


f) **Select networks**: Proceed with the default settings. Click **Next**.

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

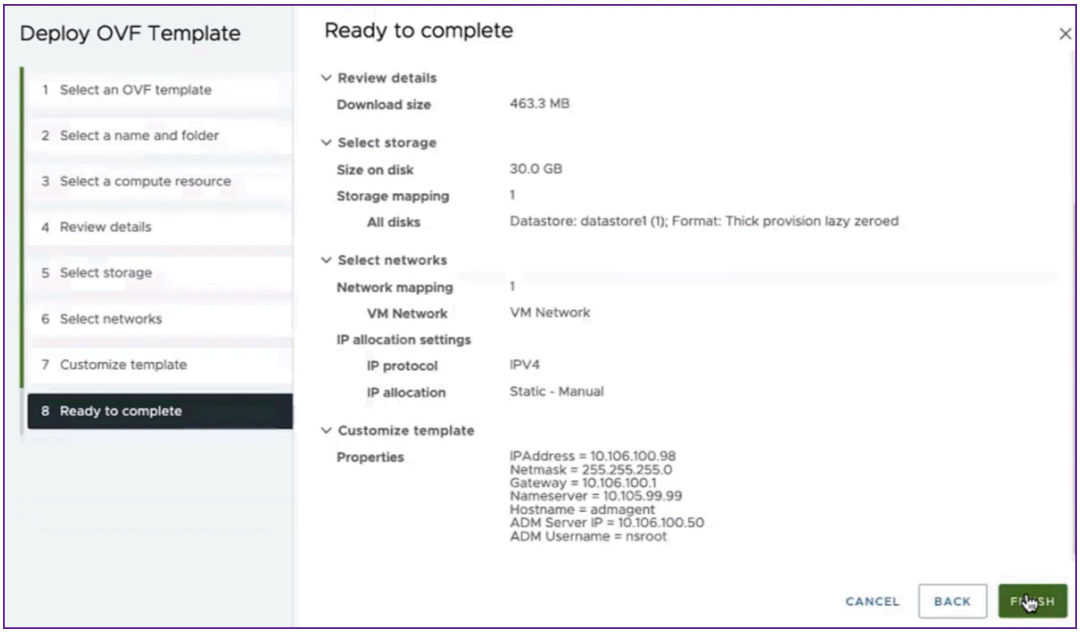


g) **Customize template**: Review all the properties of the OVF template. All the parameters and values you added in the .ovf file in the Download and edit the .OVF file section are displayed.

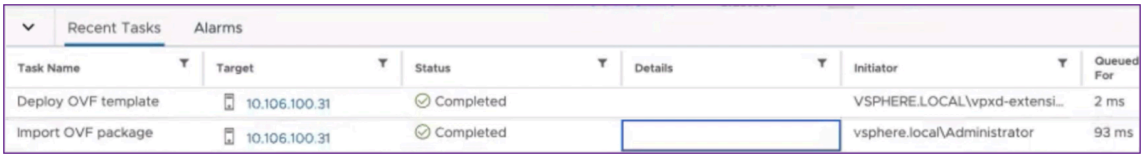


h) **Ready to complete**: To save the settings and start the deployment process, click **Finish**.

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



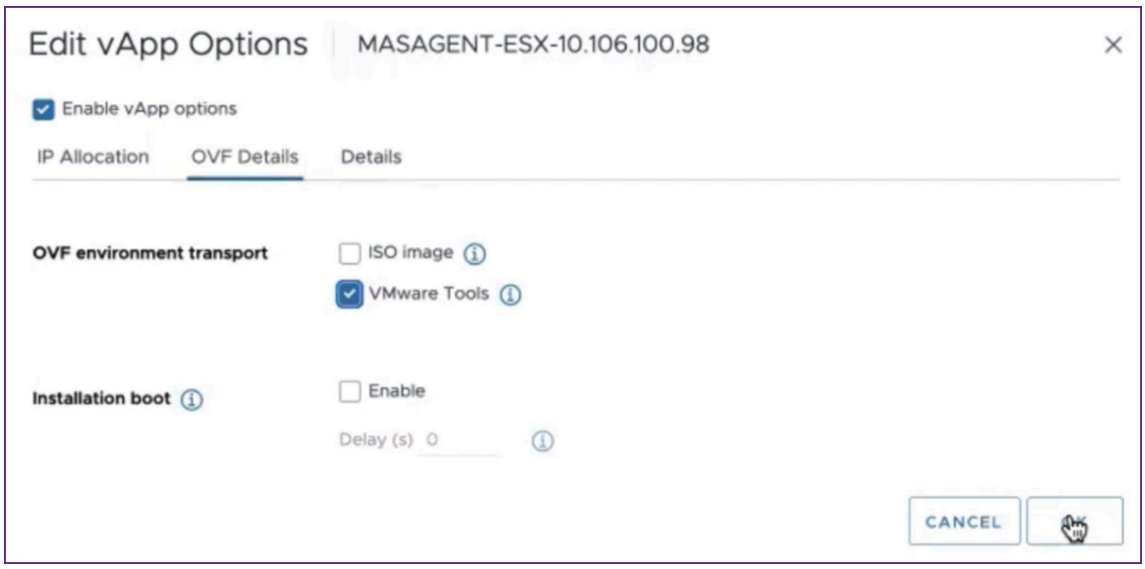
Wait for the deployment to complete. After the status of the **Deploy OVF template** operation is 100% complete, your agent is deployed.



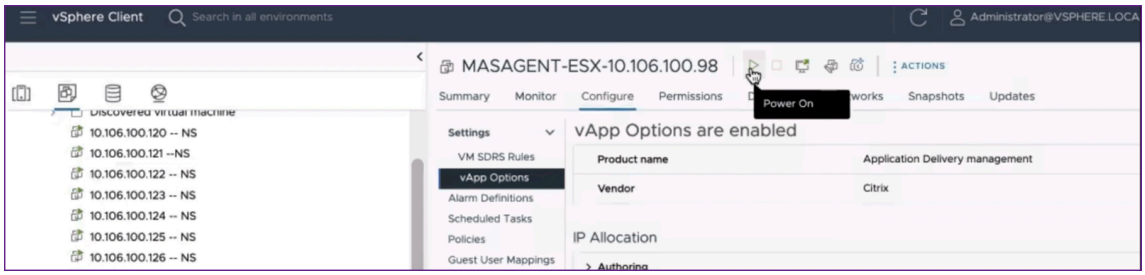
> **Important:**
>
> Do not power on the virtual appliance before you edit the settings.

4. Click the new virtual appliance that you installed and navigate to **Configure > Settings > vApp Options > Edit**.
5. In the **Edit vApp Options** window, navigate to **In OVF Details > OVF environment transport**, and select **VMware Tools**. Click **OK**.

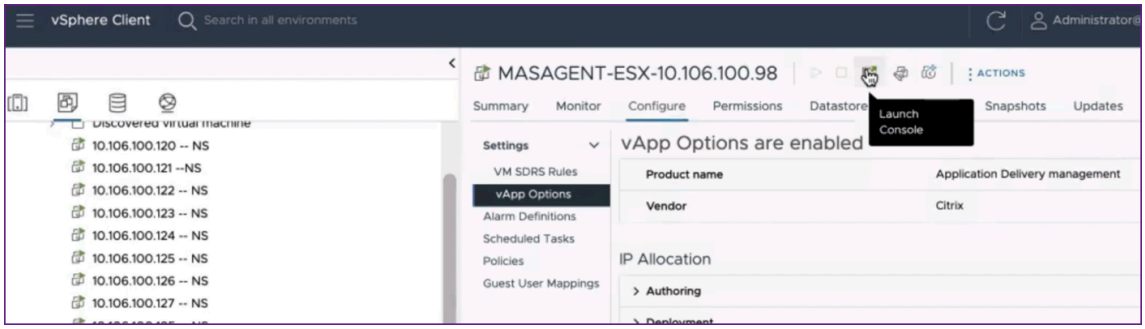
© 1997–2025 Citrix Systems, Inc. All rights reserved.



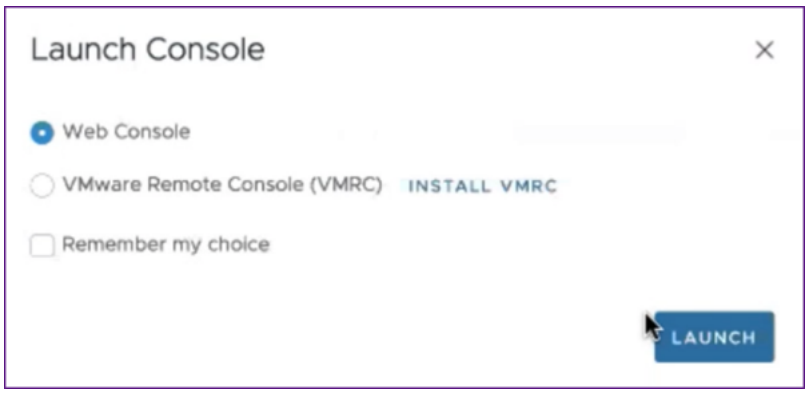
6. Right-click on the virtual machine and click **Power On**. As an alternative, you can select the virtual machine's **Summary** tab and click **Power On**.



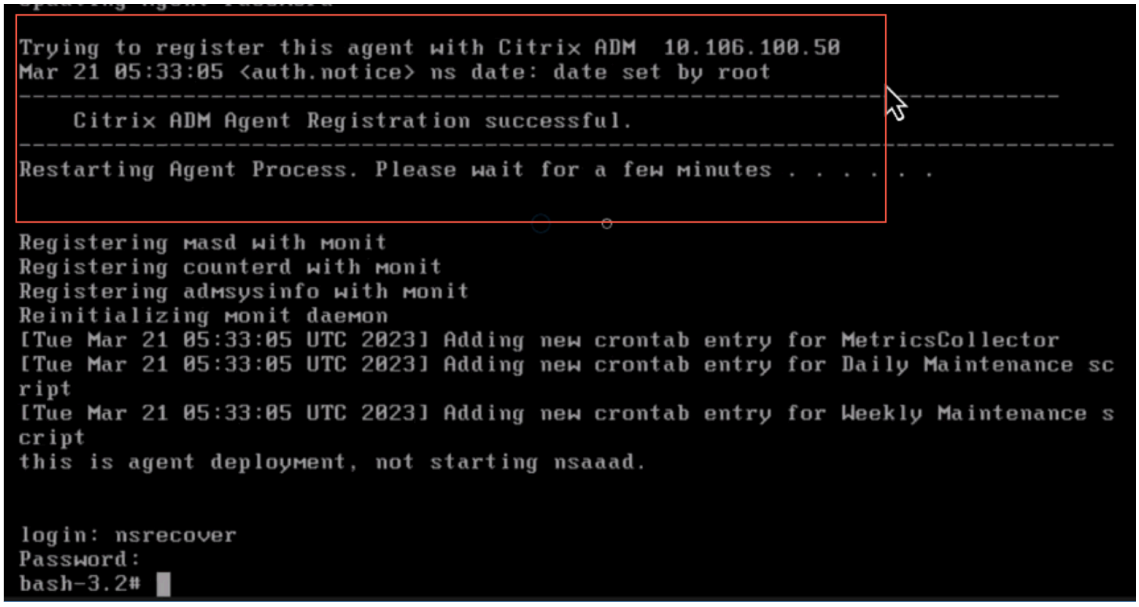
7. In the **Summary** tab, select **Launch Web Console**.
   In the **Launch Console** window, select **Web Console**. Click **Launch**.



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



8. In the console, a successful registration message is displayed after the NetScaler agent is registered to the NetScaler Console server. To verify that the NetScaler agent has been deployed and the default password has been changed, log in with the NetScaler agent user name and the new password.



Step 3: Verify

To verify that the NetScaler agent is deployed:

1. After the NetScaler agent is deployed, access the NetScaler Console GUI by typing the IP address of the NetScaler Console server in the browser.
2. Log in to the server with your credentials.
3. Navigate to **Infrastructure > Instances > Agents**.
   The newly deployed agent is displayed in the ESX Platform.

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

NetScaler Console on Kubernetes cluster

September 27, 2025

Before you install NetScaler Console virtual appliances on a Kubernetes cluster, read the prerequisites section.

Prerequisites

Ensure the following prerequisites are met before you install NetScaler Console.

Kubernetes cluster

- The Kubernetes cluster must be of the following version or above:
  - Server version v1.20
  - Client version v1.20

  Type the command `kubectl version` to check the version.
- The Helm application installed on the cluster must have the Client version v3.4.0 or above.

  Use the command `helm version` to check the version.
- Kubernetes cluster CNI (Container Network Interface) must be Calico version v3.21.1 or above.
- All the subordinate nodes in the cluster must have an NFS client installed on them. This is because the NetScaler Console application persists the data and configuration on volumes mounted on a Network File Server. To install an NFS client on an Ubuntu-based subordinate, type the following commands:

```
apt-get update
apt install nfs-common
```

- The NetScaler Console application needs 32 GB memory and 8 vCPUs across the cluster and 120 GB space on NFS.

NFS share

The NetScaler Console application needs persistent volumes to store data such as configuration, certificates, images, and others. For this purpose, NetScaler Console requires NFS mounts. The application requires two folders from the shared network mounts:

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

- One for storing files such as certificates, images, and others
- The other one for database

> Note
>
> It's recommended to have an NFS with an SSD.

These two folders can be different or the same. Both the folders must have 777 permissions. The first folder must have minimum 10 GB pace. The second folder's size depends upon the amount of data that needs to be persistent in the database. Minimum size is 100 GB.
For the production environment, we recommend having a production grade NFS solution.

NetScaler appliance

The NetScaler appliance is required as the ingress device. NetScaler makes the required application services available outside the Kubernetes
cluster. The NetScaler appliance must be outside the Kubernetes cluster, and the worker nodes must be reachable from the NetScaler. Perform the following steps:

- Configure a SNIP on the NetScaler. NetScaler uses this SNIP to reach the worker nodes of the Kubernetes cluster.
- Identify a free IP address to be used as virtual server IP address to make the required application services available outside the Kubernetes cluster.

Install NetScaler Console on Kubernetes cluster

Follow these steps to install a NetScaler Console appliance on a Kubernetes cluster:

1. Go to the NetScaler site and download the file for the NetScaler Console Helm Chart for Kubernetes.
2. Extract the downloaded Helm Chart tarball into the /var directory of the main node of the Kubernetes cluster.
3. Open the `values.yaml` file under the `/var/citrixadm` directory.
4. Enter a password for the database in the `dbpasswd` field in the file.
5. Change the following values. The NetScaler Console application uses these values to configure the NetScaler appliance so that the services are exposed to the external world:
    - `ingressIP`: a Virtual IP configured in the NetScaler for accessing the application.
    - `applicationID`: a unique ID to distinguish the ingress configuration from the rest of the configuration on the NetScaler appliance.

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

- `ingressADCIP`: NetScaler IP address (NSIP), which is used as an ingress for the NetScaler Console application.
- `ingressADCUsername`: a user name to access the NetScaler appliance. This user must have write privileges.
- `ingressADCPassword`: Password for the user name.

```
# ingressIP is the Virtual IP configured in the Citrix ADC for accessing the application
ingressIP: "xx.xx.xx.xx"

# coreDumpFilePath is the directory on slave nodes of the cluster which will be used to store core dumps files in case
application runs into faulty state
# this setting is optional
# Admin needs to create this directory on each of the slave nodes and then run the command: "echo <coreDumpFilePath_value>/
core.%h.%e.%p > /proc/sys/kernel/core_pattern"
coreDumpFilePath: "/var/mps/cores"

# applicationID is the identifier for ingress configuration
applicationID: "citrixadm"

# ingressADCIP is the NSIP of the northbound ADC used to expose the ADM application to the outside world
ingressADCIP: "xx.xx.xx.xx"

# ingressADCUsername is the username of the northbound ADC
ingressADCUsername: "nsroot"

# ingressADCUsername is the password for above username
ingressADCPassword: "nsroot"
```

6. Change the following values in the **storage** section. These values specify the persistence required to store files required by the NetScaler Console application.
   - `nfsServer`: Host name or IP address of the NFS server
   - `path`: mount the path for the folder to store application files.
   - `size`: at least 10 GB.

   > Note
   >
   > The unit for this value is Gi. For example, 10Gi, 20Gi.

7. Go to **storage** section under `pg-datastore` and change the following values. These values specify the persistence used for creating a database.
   - `nsfServer`: Host name or IP address of the NFS server.
   - `size`: mount a path for the folder used for the datastore.
   - `path`: at least 100 GB.

   > Note
   >
   > The unit for this value is Gi. For example, 100Gi, 200Gi.

8. Go to the /var/citrix directory in the main node and run the following command to install a NetScaler Console application:
   `helm install -n citrixadm --namespace <name> ./citrixadm`

   > Note

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

> This helm command is not supported in helm version 3.x.

This command also installs the required pods in your cluster. Namespace argument is optional. If namespace is not provided, Helm installs NetScaler Console in the default namespace. For ease of management, install NetScaler Console under a separate namespace.

9. Open your browser and type `http://< virtual server IP address >` and log in to the NetScaler Console using `nsroot`/`nsroot` as credentials. For secure access type `https://< virtual server IP address >`.

> Note
>
> During deployment, the NetScaler Console application creates tables in the datastore, which can take a while. Depending upon the resources allocated by Kubernetes to various pods of the NetScaler Console application, it can take 5- 15 mins for the service to come up.

NetScaler Console on Linux KVM server

September 27, 2025

Virtualization platforms on which the NetScaler Console can be provisioned include Linux-KVM.

Before you install NetScaler Console on Linux-KVM, make sure that your system has the hardware virtualization extensions, and verify that the CPU virtualization extensions are available. Verify that `virsh` (a command-line tool for managing virtual machines) is available on the hypervisor.

Use your administrator credentials to log on to Citrix.com website, access the latest NetScaler Console setup files, and download them onto your computer. Then, install the NetScaler Console on your Linux-KVM platform and configure it for your network.

Prerequisites

Before installing the NetScaler Console virtual appliance, verify that Linux-KVM version 3.6.11-4 and later is installed on hardware that meets the minimum requirements.

Hardware requirements

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

Component	Requirement
CPU	A 64-bit x86 processor with the hardware virtualization features that are included in the Intel VT-X processor. Provide at least 2 CPU cores to host Linux-KVM. **Note** To test whether your CPU supports Linux host, enter the following command at the host Linux shell prompt: `*. egrep'^flags.\* ( vmx | svm )' /proc/cpuinfo*`. If the BIOS settings for the extension are disabled, you must enable them in BIOS. There is no specific recommendation for processor speed, but higher the speed, the better is the performance of the NetScaler Console.
Memory (RAM)	Minimum 4 GB for the host Linux kernel. Add additional memory as required by the VMs.
Hard Disk	Calculate the space for Host Linux kernel and VM requirements. A single NetScaler Console VM requires 120 GB of disk space.

> **Note**
>
> The memory and hard disk requirements specified are for deploying NetScaler Console on the OpenStack platform, considering that there are no other virtual machines running on the host. The hardware requirements for OpenStack depend on the number of virtual machines running on it.

Software requirements

We recommend newer kernels, such as the 64-bit version of the 3.6.11-4 kernel or later.

Network requirements NetScaler Console supports only one virtIO para-virtualized network interface. Ensure to connect this interface to the management network of the Linux-KVM host, so that the NetScaler Console and Linux-KVM can communicate.

Download NetScaler Console setup files

To download the NetScaler Console setup files from `www.citrix.com`:

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

1. Open a web browser and type www.citrix.com in the address bar.
2. Hover over the **Sign In** option and click **My Account**, enter your Citrix credentials, and then again click **Sign In**.
3. Navigate to **Downloads** section.
4. From the **Downloads** list, select **NetScaler® Application Delivery Management**.
5. On the **NetScaler Application Delivery Management** page, select the release. For example, select **Release 13.0**.
6. Click **Product Software** to expand it, and click the latest build. For example, select **NetScaler MAS Release (Feature Phase) 13.0 Build 36.27**.

   The selected build page is displayed.
7. On the **Jump to Download** list, select **NetScaler MAS image for KVM, 13.0 Build xx.xx**
8. Click **Download File**, accept the EULA, and download the compressed image file to any folder on your local machine.

Install the NetScaler Application Delivery Management on Linux-KVM

1. Using SSH, log on to the KVM host.
2. At the CLI prompt, by using any of the file transfer programs, copy the image to a folder on the server.
3. Navigate to the directory where you have saved the downloaded image.
4. Perform these at the command line:

   a) List the files in the directory verify the presence of the image file.

   b) Use the tar command to untar the NetScaler Application Delivery Management image file. The unzipped package contains the following components:

      i. A domain XML file that specifies the NetScaler Console attributes

      ii. A text file that specifies the check sum of the domain disk image

      iii. A domain disk image

```
tar -xvfz MAS-KVM.tgz
MAS-KVM.xml
MAS-KVM.qcow2
checksum.txt
```

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

```
root@ubuntu:~/mas-build#
root@ubuntu:~/mas-build# tar xvfz MAS-KVM-11.1-50.10.tgz
MAS-KVM.xml
checksum.txt
MAS-KVM-11.1-50.10.qcow2
root@ubuntu:~/mas-build#
```

iv. Create a copy of MAS-KVM.xml as MAS1-KVM.xml, as a back-up option. Open the MAS1-KVM.xml file by using the vi editor.

v. Edit MAS1-KVM.xml for the following networking attributes:

A. `name` - Specify the name.

B. `mac` - Specify the MAC address.

C. `source file` - Specify the absolute disk-image source path. The file path has to be absolute.

> **Note**
>
> The domain name and the MAC address must be unique.

D. `mode` - Specify the mode.

E. `model type` - Set to virtIO.

F. `source dev` - Specify the interface.

```
1  <name> MAS1-KVM</name>
2  <mac address='52:54:00:29:74:b3'/>
3  <source file='/var/ MAS-KVM.qcow2'/>
4  <source dev='eth0' mode='bridge'/>
5  <model type='virtio'/>
```

vi. Define the VM attributes in the MAS1-KVM.xml file by using the following command: `virsh define \<FileName\>.xml`

```
1  virsh define MAS-KVM.xml
2  Domain MAS defined from MAS-KVM.xml
```

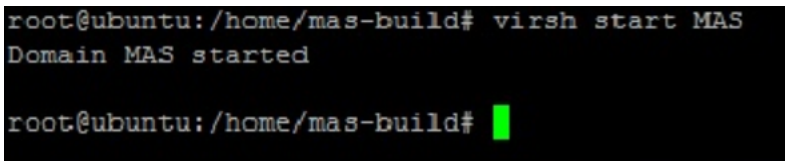
```
root@ubuntu:~/mas-build# virsh define MAS-KVM.xml
Domain MAS defined from MAS-KVM.xml

root@ubuntu:~/mas-build#
```

vii. Start the NetScaler Console by entering the following command: `virsh start \[\<DomainName\> | \<DomainUUID\>\]`

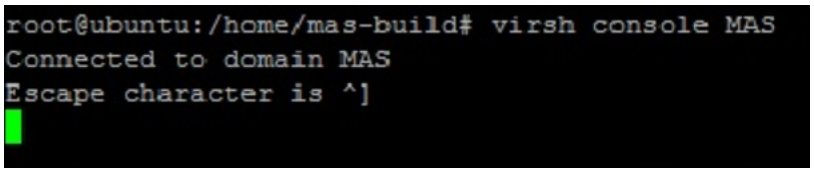
```
1  virsh start MAS
2  Domain MAS started
```

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



viii. You can connect to the NetScaler Console virtual machine by using the following command: `virsh console \<DomainName\>`

```
virsh console MAS
Connected to domain MAS
Escape character is ^]
```



Configure the NetScaler Application Delivery Management

> **Note**
>
> On some Linux KVM hosts, FreeBSD guests fail to restart properly if they have more than one CPU. When The NetScaler Console virtual appliance is restarted, the NetScaler Console CLI and GUI become unresponsive. For details, see https://bugs.launchpad.net/qemu/+bug/1329956
>
> To avoid the NetScaler Console CLI and GUI from becoming unresponsive when the NetScaler Console virtual appliance is restarted, shut down all the virtual machines on the KVM host, and perform the following on the KVM host:
>
> 1. Remove the kvm_intel module using the following command:
>   `rmmod kvm\\_intel`
> 2. Disable **APICv** and reload kvm_intel module using the following command:
>   `modprobe kvm\\_intel enable\\_apicv=N`
> 3. Start the virtual machines on the KVM host.

After installing the NetScaler Console, allow about 10 minutes for the services to become available, and then log on to the NetScaler Console.

1. At the command line, use the default system administrator credentials to log on to the system:
   - User name: `nsroot`
   - Password: `nsroot`

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

> **Note**
>
> After logging on for the first time, change the administrative password. Then, configure the MAS to function in your network. You can change the password from the NetScaler Console user interface. From the NetScaler Console home page, navigate to **Settings > User Administration > Users**. Select the user and click **Edit**, and then update the password in the Password field.

2. At the prompt, type: *shell*
3. Type **networkconfig** to enter the NetScaler Console initial network configuration menu. Configure the management IP address.
4. To complete the initial network configuration of NetScaler Console, follow the prompts. The console displays the NetScaler Console initial network configuration options for setting the following parameters for the NetScaler Console. The host name is populated by default.

    a) Enter **2** to update NetScaler Console IPv4 address - management IP address at which you access a NetScaler Console

    b) Enter **3** to update Netmask - subnet mask associated with the Management IP address

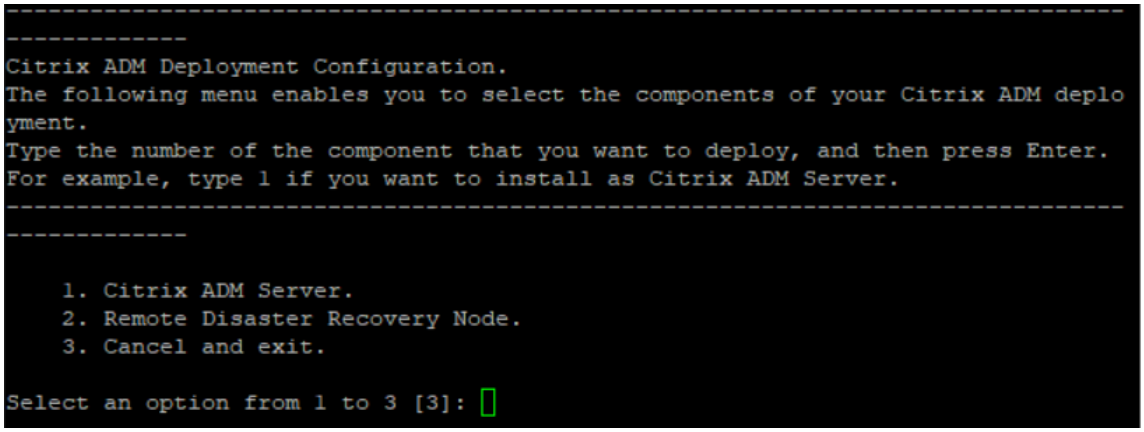
    c) Enter **4** to update Gateway IPv4 address - default gateway IP address for the subnet of the Management IP address of the NetScaler Console

    d) Enter **7** to save and quit - saves your configuration changes and exits the system.

5. Run the deployment script by typing the command at the shell prompt: `deployment_type.py`
6. In the deployment screen that appears, select the deployment type as **NetScaler Console server**.

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



7. Type **Yes** to deploy NetScaler Console as a standalone deployment.
8. Type **Yes** to restart the NetScaler Console server.
9. After NetScaler Console server restarts, log on to NetScaler Console by using the default administrator credentials as nsroot/nsroot through the command line or the GUI.

   You can later access the NetScaler Console by typing the IP address of the NetScaler Console server in the address bar of your browser. The default administrator credentials to log on to the server are *nsroot/nsroot*.

NetScaler Console on Nutanix hypervisor (Acropolis)

September 27, 2025

> **Note:**
>
> This feature is available in release 14.1-38.xx and later.

You can use the KVM software image to configure the NetScaler® Console server on Nutanix hypervisor. Before you begin, ensure that you have configured Nutanix Prism to create a VM for NetScaler Console.

Hardware requirements

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

Component	Requirement
CPU	A 64-bit x86 processor with the hardware virtualization features that are included in the Intel VT-X processor. Provide at least 8 CPU cores to host Linux-KVM.
Memory (RAM)	Minimum 4 GB for the host Linux kernel. Add additional memory as required by the VMs.
Hard Disk	Calculate the space for Host Linux kernel and VM requirements. A single NetScaler Console VM requires 120 GB of disk space.

Download the NetScaler Console setup file

To download the NetScaler Console setup file:

1. Log on to www.citrix.com/downloads page.
2. Select **NetScaler Console** from the product list.
3. Under **Release 14.1**, select the 14.1-38.x or later build.

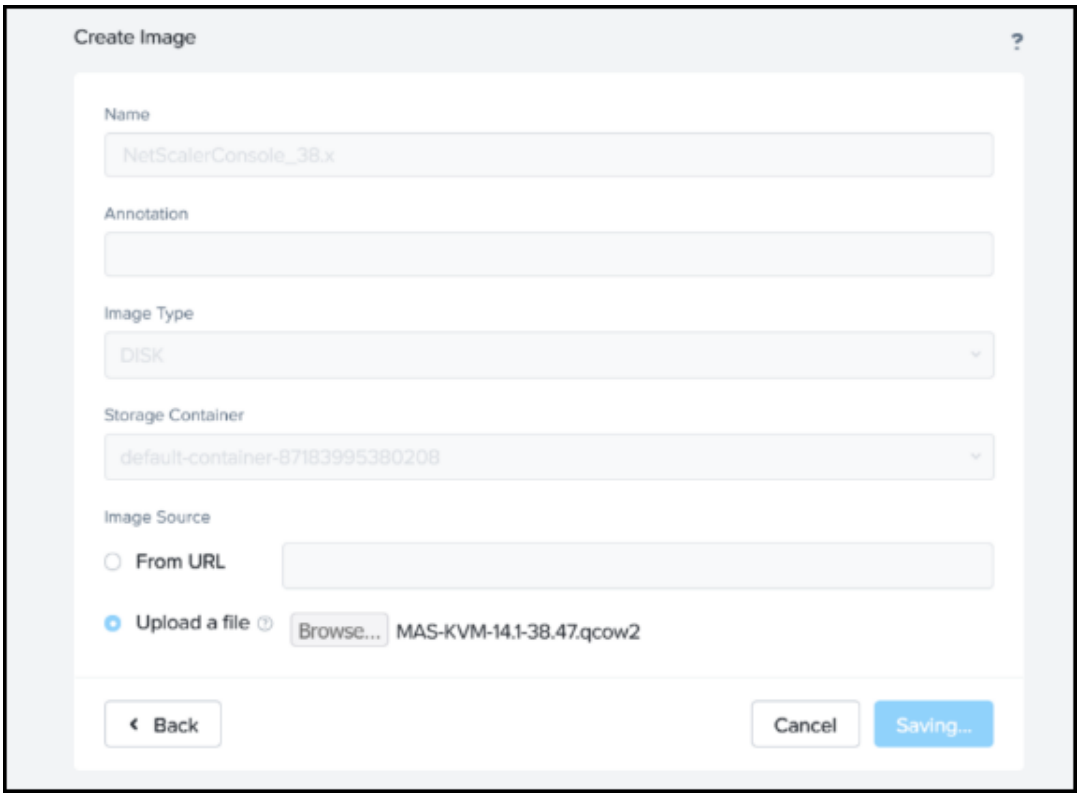
   The selected build page is displayed.
4. On the **Jump to Download** list, select **Citrix ADM image for KVM, 14.1 Build xx.xx**
5. Click **Download File**, accept the EULA, and download the compressed image file to any folder on your local machine.

Configure NetScaler Console on Nutanix hypervisor

1. Unpack the `.tgz` file.
2. Log on to Nutanix Prism.
3. Navigate to **Settings** and choose **Image Configuration**.
   a) Specify an image name.
   b) Select **DISK** as the image type.
   c) Select a storage container.
   d) In **Image Source**, select Upload a file, and upload the file with `.qcow2` extension.

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

e) Click **Save**.



After you upload and save, the image and its status is shown:



4. Navigate to VM and click **Create VM**.
5. On the **Create VM** page, remove the **CD ROM Drive**.
6. Add a new disk.

   a) Select **DISK** from the **Type** list.

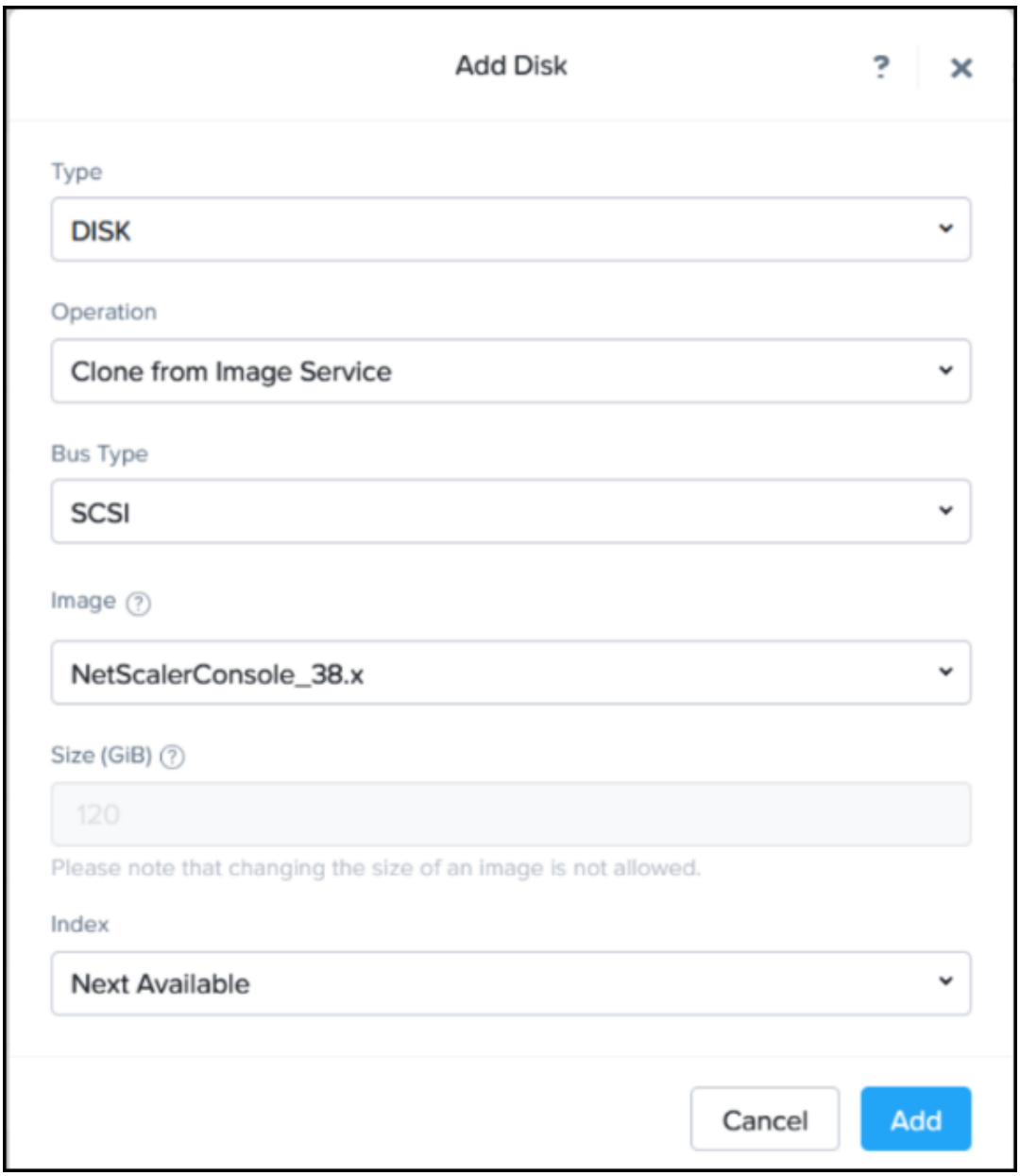
   b) Select **Clone from Image Service** from the **Operation** list.

   c) Select **SCSI** from the **Bus Type** list.

   d) Select the NetScaler Console image from the list.

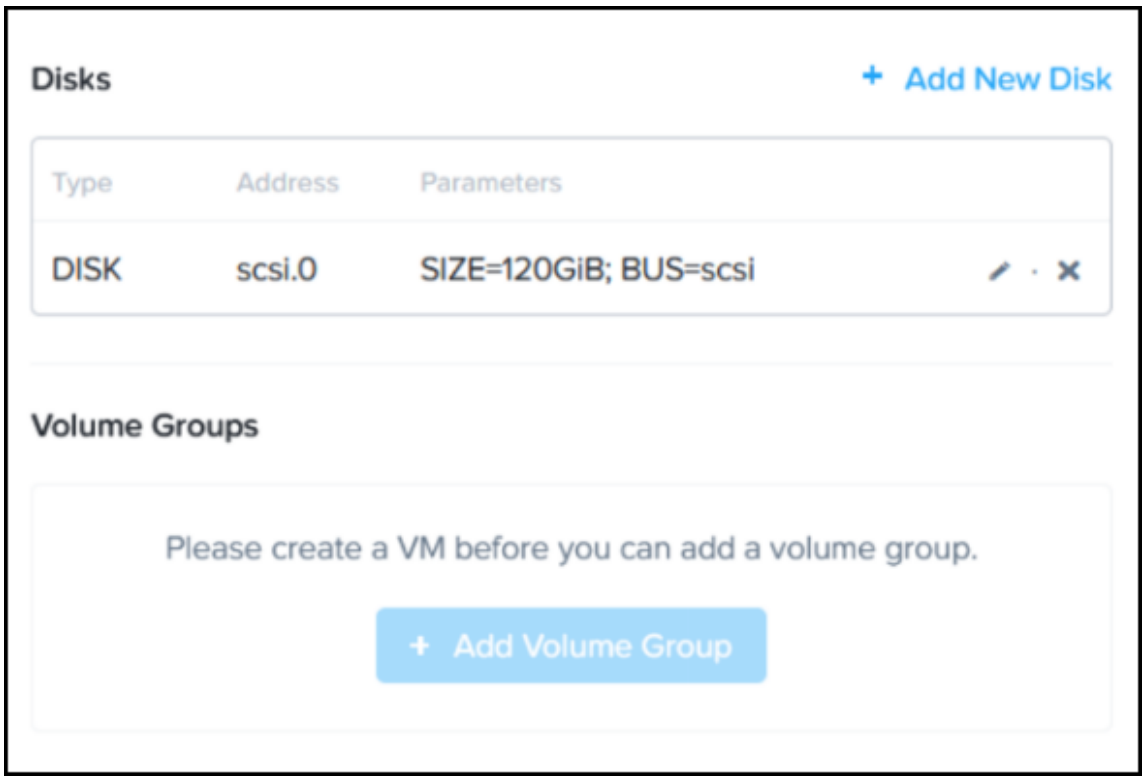
   e) Click **Add**.

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

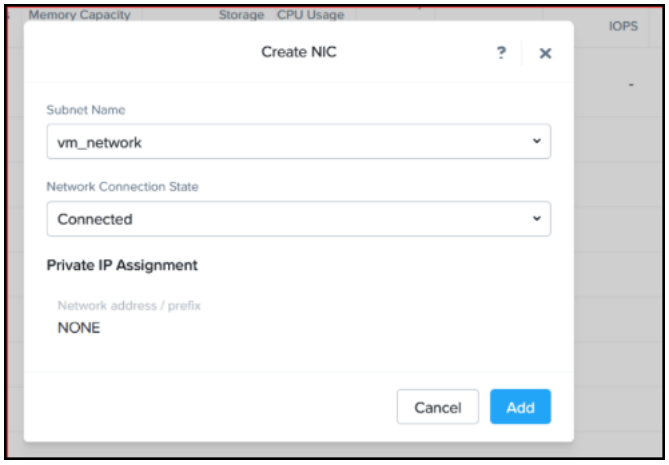


The disk is added.

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

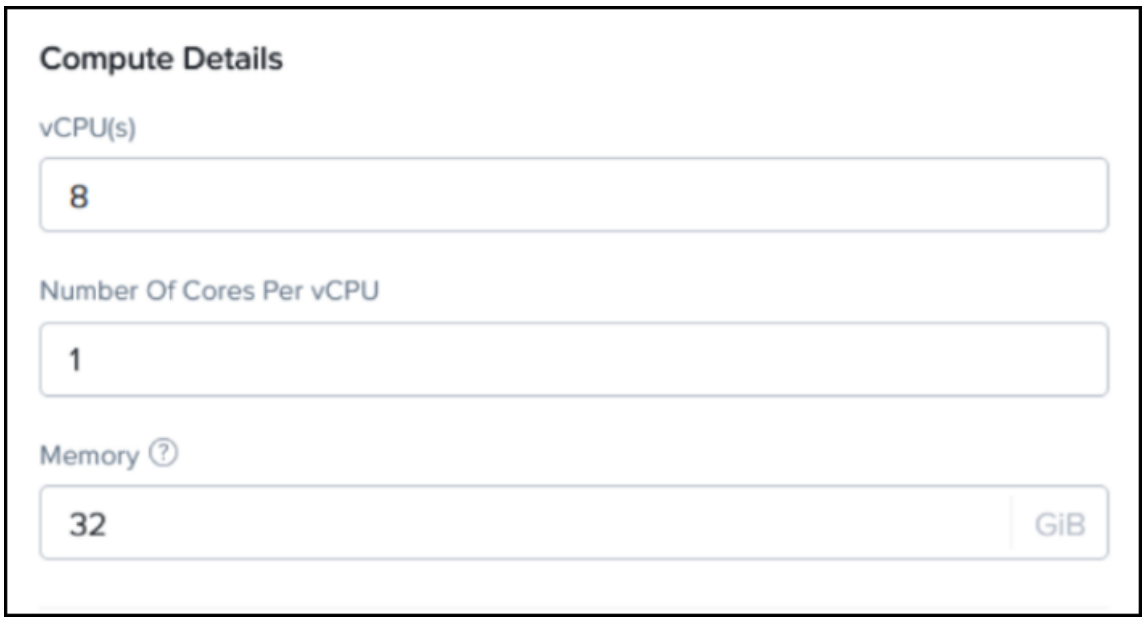


7. Add the following NIC details to the VM:



8. Click **Save**.
9. Specify the Compute details. Use the default values for NetScaler Console and NetScaler agent.

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



10. Click **Save**.

    After the VM is listed and shows as powered off, you must add the serial port to boot the VM.

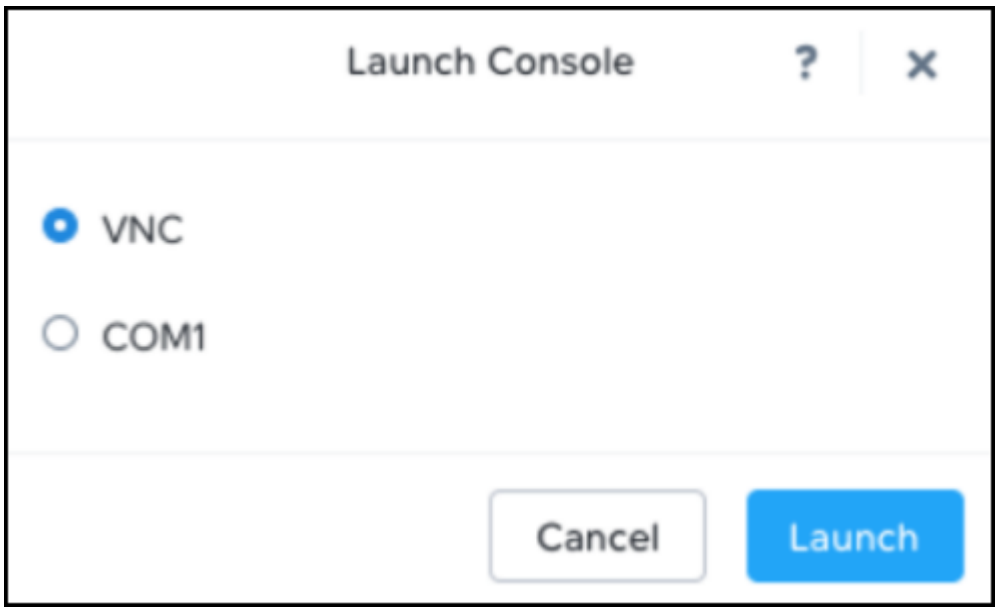
11. SSH into the Controller VM (CVM) using the user name and the password you set for that account. You can find a list of CVM IP addresses in the Hardware section of the Prism Element console.
12. Enter **ACLI**.
13. Use the following command to create the serial port. Type the name of the VPX appliance in `vmname`

    ```
    vm.serial_port_create <vmname> type=kServer index=0
    ```

Network configuration

1. Power on the VM.
2. Launch the VNC console.

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



3. After the VM boots, log in using the default credentials (**nsrecover**/**nsroot**).
4. At the prompt, type: *shell*
5. Type **networkconfig** to enter the NetScaler Console initial network configuration menu. Configure the management IP address.
6. To complete the initial network configuration of NetScaler Console, follow the prompts. The console displays the NetScaler Console initial network configuration options for setting the following parameters. The host name is populated by default.

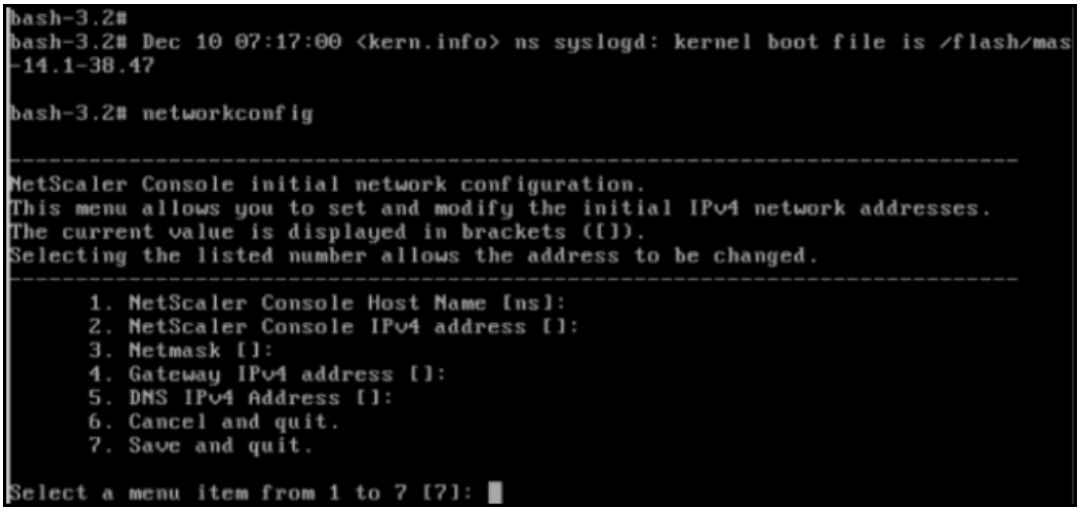
    a) Enter **2** to update NetScaler Console IPv4 address - management IP address to access NetScaler Console.

    b) Enter **3** to update Netmask - subnet mask associated with the Management IP address.

    c) Enter **4** to update Gateway IPv4 address - default gateway IP address for the subnet of the Management IP address of the NetScaler Console.

    d) Enter **7** to save and quit - saves your configuration changes and exits the system.

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



You can access the NetScaler Console by typing the IP address of the NetScaler Console server in the address bar of your browser. The default administrator credentials to log on to the server are *nsroot/nsroot*.

NetScaler Console on Azure Cloud

October 10, 2025

Starting from 14.1-43.x, NetScaler Console offers more deployment options where NetScaler Console can be deployed as a Virtual Machine (VM) on Azure through the Azure Government Marketplace. NetScaler Console service is not a feasible option for customers whose cloud deployments are air-gapped and lack internet connectivity. NetScaler Console deployed as a VM on Azure enables you to efficiently manage and monitor your NetScaler VPX instances using NetScaler Console within the Azure deployments.

> **Note:**
>
> NetScaler Console on Azure Cloud is available only on the Azure Government Marketplace.

Prerequisites

Before you configure, ensure that you have access to Azure Cloud and Resource Group.

> **Note:**
>
> We recommend that you create a resource group, network security group, virtual network, and other required entities before you provision NetScaler Console.

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

Configure NetScaler Console

In Azure Cloud:

1. Go to Marketplace, search for NetScaler Console, and then click **Select**.

   After you select the image, you will be redirected to the **Create Virtual Machine** workflow.

2. Specify the following:

   a) **Resource Group** - Select a resource group from the list.

   b) **Virtual Machine Name** - A name of your choice.

   c) **Region** - Select a region from the list.

   d) **Image** - Populated automatically since you have selected it from the Marketplace.

   e) Select the VM size from the list (8vcpu, 32 GB RAM is recommended).

   f) **Authentication Type** - Select SSH public key.

   > **Note:**
   >
   > Password option is not supported.

   g) **Username** - Change the name as `nsroot`. The default user name to access NetScaler Console is `nsroot`.

   h) **SSH public key source** - You can use an existing key pair or create a new key pair.

   i) **Public Inbound Ports** - Select **None**.

   j) Click **Review + Create**.

   The VM summary is displayed. Validate everything and then click **Create**.

   k) The VM deployment shows that the status is in progress. After the deployment is complete, click **Go to Resource**.

   The information about the VM is displayed and you can view the public and private IPs of the VM under **Networking**. You can log in (`nsroot`/`nsroot`) using the public IP through a browser.

   > **Note:**
   >
   > If you want to use the private IP address, ensure that you have an Azure Virtual Desktop running in the same Azure Cloud Network to access NetScaler Console through the private IP address.

   l) Validate if the NetScaler Console process is up and running by logging into the virtual machine using SSH with user name `nsrecover` and password `nsroot`.

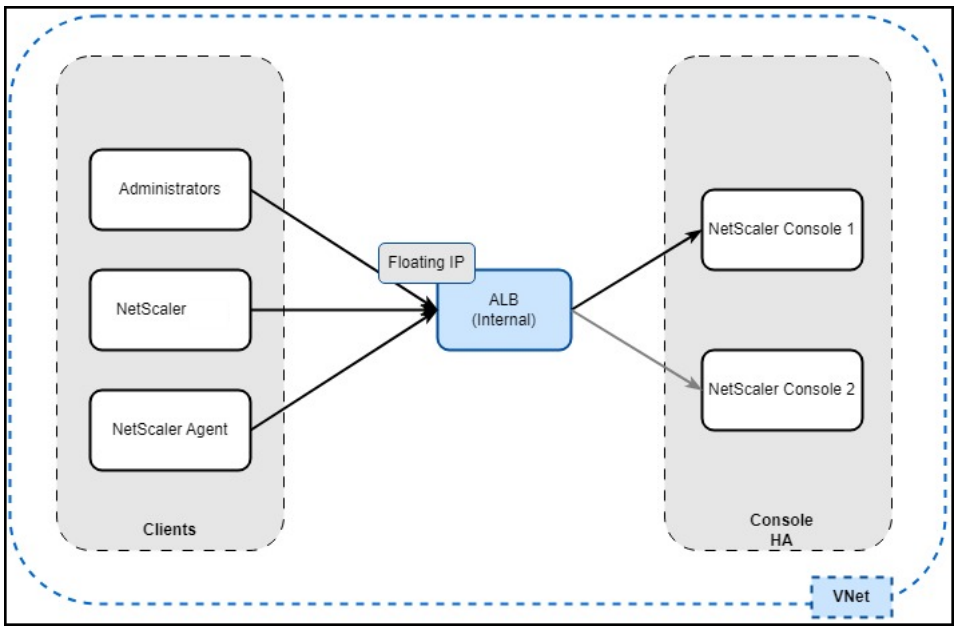
© 1997–2025 Citrix Systems, Inc. All rights reserved.

m) Once the backend processes are up and running, you can log in to the NetScaler Console GUI using the `nsroot` password. On first login, the system prompts you to change the default password.

NetScaler Console HA pair on Azure Cloud

December 22, 2025

In Azure, high availability for NetScaler Console is achieved using an Azure Load Balancer (ALB). ALB monitors instances by sending health probes to both the primary and secondary nodes. The primary instance responds with `200 OK`, while the secondary instance does not respond. Based on these responses, ALB sends traffic exclusively to the primary instance. In the event of a failover, the new primary begins responding with `200 OK`, and ALB automatically sends traffic to it.



Prerequisites

Ensure that:

- You have access to Azure Cloud and Resource Group.

> **Note:**
>
> We recommend that you create a resource group, network security group, virtual network, and other required entities before you provision NetScaler Console.

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

- You create two standalone NetScaler Console instances on Azure Cloud.
- The required ports are open for communication. For more information, see System Requirements.

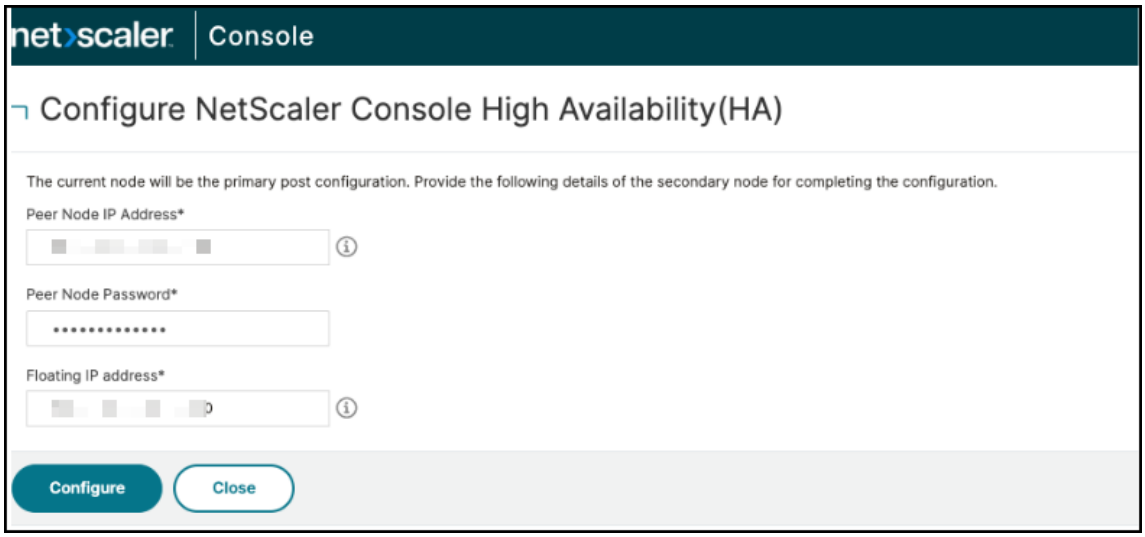
Configure NetScaler Console HA pair

After you configure two standalone NetScaler Console instances:

1. Login to one of the NetScaler Console GUI.
2. Navigate to **Settings > High Availability Settings**.

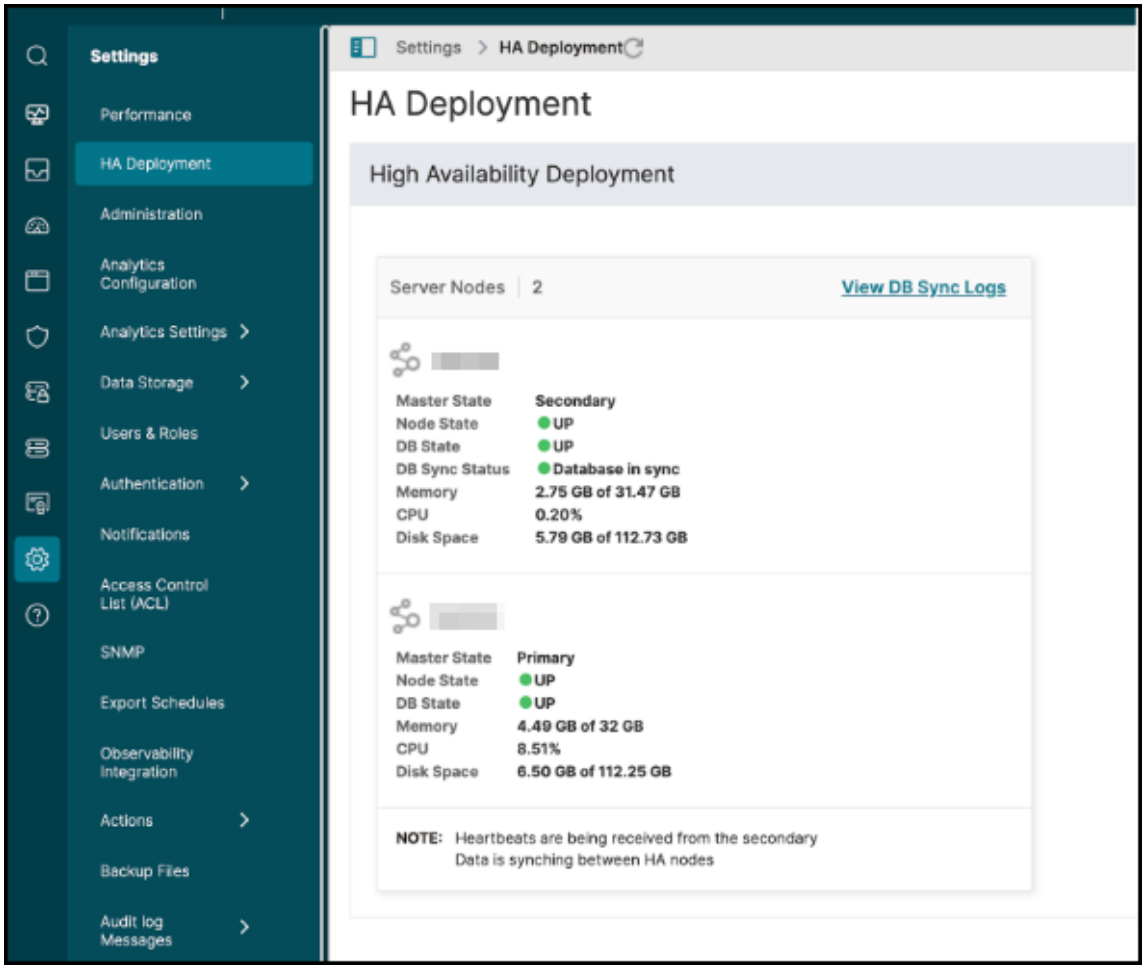
   > **Note:**
   >
   > - For configuring an HA pair, you must provide the private IP address of the other NetScaler Console.
   > - Floating IP can be any available IP from the Azure VNet (Virtual Network).

3. Click **Configure NetScaler Console High Availability (HA)**, and provide the secondary node details, floating IP address, and click **Configure**.



4. In the confirmation window, click **Yes**. NetScaler Console instances reboot to form a HA pair.
5. After the HA pair configuration is complete, login to the primary NetScaler Console and navigate to **Settings > HA Deployment** to validate the primary and secondary nodes.

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



The next step is to configure the floating IP address as the frontend IP of Azure load balancer in Azure Cloud. In Azure Cloud portal, search for load balancer, and select **Load Balancers** in the results, and click **Create**:

1. In **Basics**, create an Azure Load Balancer (ALB) in the same Resource Group and Region where the Console VMs are configured.

    a) Select SKU: **Standard**, Type: **Internal**, and Tier: **Regional** under **Instance details**.

2. In **Frontend IP Configuration**, add a frontend IP with the floating IP configured for the Console HA pair.
3. In **Backend pools**, add the IP address of the two Console instances.
4. **Load balancing rules**: Configure the following rules with Protocol, Port, Backend Port, Health Probe, and floating IP enabled:

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

Rule name	Protocol	Port	Backend port	Floating IP
Rule-80	TCP	80	80	Yes
Rule-443	TCP	443	443	Yes
Rule-5454	TCP	5454	5454	Yes
Rule-22	TCP	22	22	Yes
Rule-8443	TCP	8443	8443	Yes
Rule-7443	TCP	7443	7443	Yes
Rule-27000	TCP	27000	27000	Yes
Rule-7279	TCP	7279	7279	Yes
Rule-5563	TCP	5563	5563	Yes
Rule-4739	UDP	4739	4739	Yes
Rule-5140	UDP	5140	5140	Yes
Rule-162	UDP	162	162	Yes
Rule-514	UDP	514	514	Yes
Rule-5557	UDP	5557	5557	Yes
Rule-5558	UDP	5558	5558	Yes

5. **Health Probe**: Create an HTTP health check with all the required ports listed in Step 4. This health probe enables the primary Console as Active and secondary Console as Passive. For example:

   a) Port: 443

   b) URL: /`mas_health`

   c) Expected Response Code: 200

   For more information to create a load balancer, see Create load balancer in Azure documentation.

   After you configure the load balancer, you can use the frontend IP address of ALB to access NetScaler Console.

   > **Note:**
   >
   > Ensure that you have an Azure Virtual Desktop running in the same Azure network to access NetScaler Console through frontend IP address.

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

NetScaler Console on Amazon Web Services (AWS)

September 27, 2025

Starting from **14.1-47.x**, you can deploy NetScaler Console by using an AMI on AWS Marketplace in **AWS GovCloud**.

Prerequisites

To launch a NetScaler Console AMI within an AWS Virtual Private Cloud (VPC) by using the Amazon GUI, you need:

- An AWS account
- An AWS virtual private cloud (VPC)
- To ensure that the required ports, such as 22, 80, and 443 are open when you create a security group in AWS. For more information, see System Requirements.

Configure NetScaler Console

1. Log on to the AWS marketplace by using your AWS credentials.
2. Search for AMI and select **AMIs**.
3. In the search box, type NetScaler Console, select NetScaler Console, and click **Launch instance from AMI**.
4. Under **Instance Type**, select 8 vCPU and 32 GB memory option from the list.

   > **Note:**
   >
   > By default, the NetScaler Console AMI is 500 GB.

5. Under **Key Pair (login)**, select an existing key pair or create a new key pair.
6. Under **Network settings**, click **Edit** and:
   a) Select the VPC from the list.
   b) Select or create a new subnet.
   c) Enable **Auto-assign public IP** to launch NetScaler Console using a public IP address.
   d) Select or create a security group.

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

> **Note:**
>
> Ensure that the required ports such as port 22, 443, and 80 are open. For more information, see System Requirements.

e) Click **Launch instance**. An instance ID is created.

7. Click the instance ID.

   You might have to wait for the **Status check** to show passed (green check mark).

8. After the security checks are passed, click the instance ID to view the details.

   Use the IP address to launch the NetScaler Console GUI. If you want to use a private IP address, ensure that you have a VDI in AWS.

   The following table describes the AWS login process through SSH, GUI, and serial console (a console that can be accessed from AWS):

	SSH		Serial Console	GUI		
	nsroot	**nsrecover**	**nsroot**	**nsrecover**	**nsroot**	**Custom user**
Password	Allowed (Default password is `nsroot`)	Allowed (Default password is `nsroot`)	Not allowed	Allowed (Default password is `nsroot`)	Allowed (Default password is `nsroot`)	Allowed (User-defined password)
Public key	Allowed	n/a	n/a	n/a	n/a	n/a

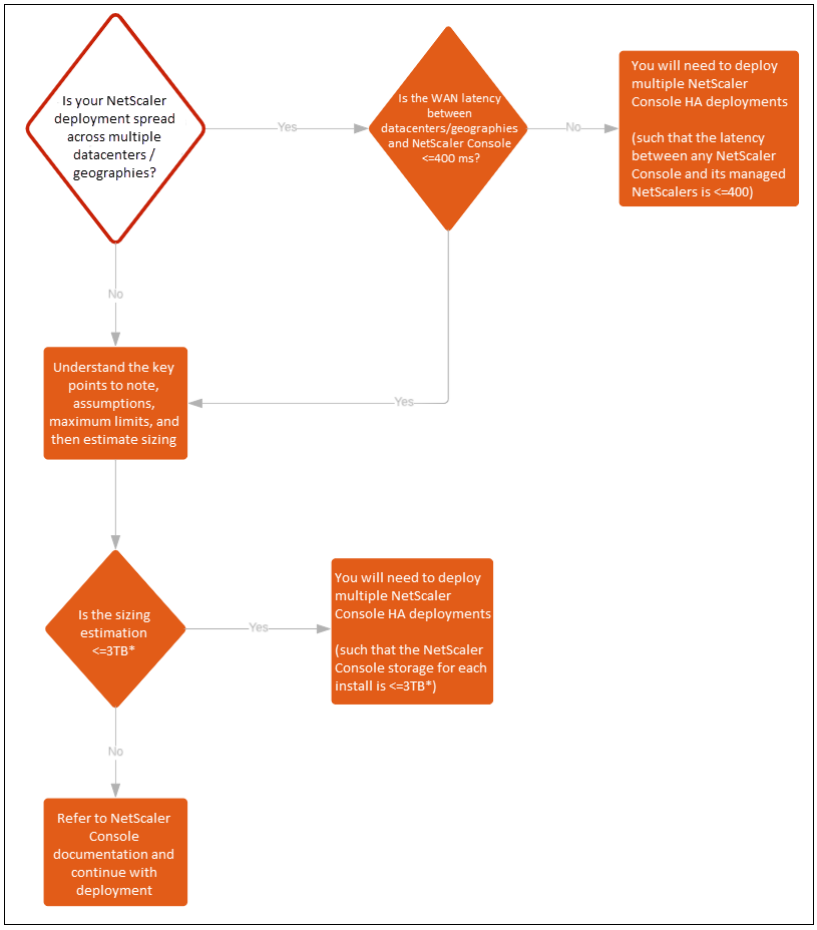
Configure high availability deployment

September 27, 2025

High Availability (HA) refers to a system that is always available to a user without any interruption to the services. High availability setup is crucial during system downtime, network or application failures, and is a key requirement to any enterprise. A high availability deployment of two NetScaler Console nodes in active-passive mode with same configurations provides uninterrupted operations.

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

Deployment scenario



> **Note**
>
> The validated maximum storage limit for a single NetScaler Console HA deployment is 3 TB. For more information, see the deployment guide.
>
> **Important**
>
> **To access NetScaler Console 12.1 build 48.18 or later versions using HTTPS:**
>
> If you have configured a NetScaler instance to load balance NetScaler Console in a high availability mode, first remove the NetScaler instance. Then, configure a floating IP address to access NetScaler Console in high availability mode.

The following are the benefits of high availability deployment in NetScaler Console:

- An improved mechanism to monitor heartbeats between the primary and secondary node.
- Provides physical streaming replication of database instead of a logical bi-directional replication.

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

- Ability to configure the floating IP address on the primary node to eliminate the need of separate NetScaler load balancer.
- Provides easy access to the NetScaler Console user interface using the floating IP address.
- NetScaler Console user interface is provided only on the primary node. By using the primary node, you can eliminate the risk of accessing and making changes to the secondary node.
- Configuring the floating IP address handles the failover situation and reconfiguring the instances is not required.
- Provides built in ability to detect and handle split-brain situation.

The following table describes the terms used in high availability deployment.

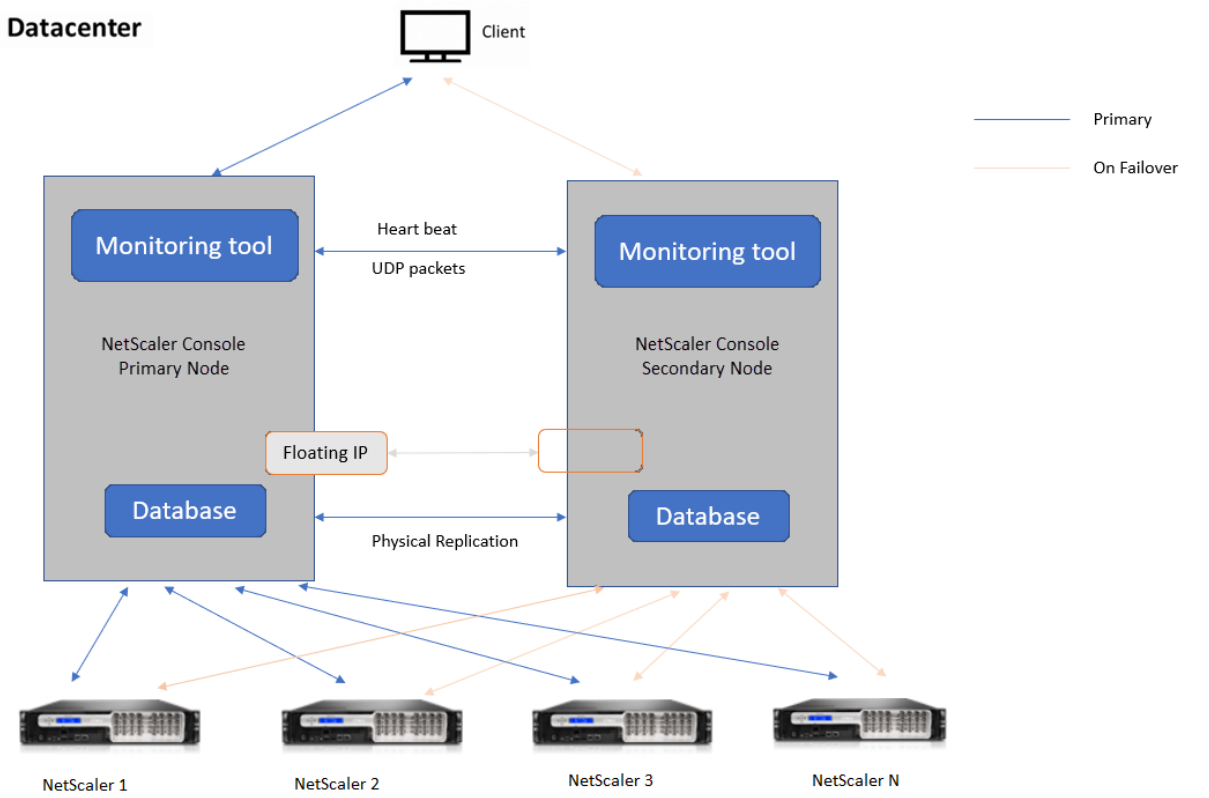
Terms	Description
Primary node	First node registered in the high availability deployment.
Secondary node	Second node registered in the high availability deployment.
Heartbeat	A mechanism used to exchange messages between primary and secondary node in the high availability setup. The messages determine status and health of the application on each individual node.
Floating IP address	A floating IP is an IP address that can be instantly moved from one node to another in the same subnet. Internally it is set up as an alias on the network interface of the primary node. If there is a failover, the floating IP address is seamlessly moved from the old primary to the new one. It is useful in high availability setup because it allows clients to communicate with the high availability nodes using a single IP address.

> **Note:**
>
> For more information on port and protocol details, see Ports.

Components of high availability architecture

The following figure displays the architecture of two NetScaler Console nodes deployed in high availability mode.

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



In high availability deployment, one NetScaler Console node is configured as the primary node (MAS 1) and the other as the secondary node (MAS 2). If the primary node goes down due to any reason, the secondary node takes over as the new primary node.

Monitoring tool

Monitoring tool is an internal process used to monitor, alert, and handle failover situations. The tool is active and running on each node in high availability. It is responsible for starting subsystems, initiating database on both the nodes, deciding on the primary, or secondary node if there is a failover, and so on.

Primary node

The primary node accepts connections and manages the instances. All processes such as AppFlow, SNMP, LogStream, syslog, and so on is managed by the primary node. The NetScaler Console user interface access is available on primary node. The floating IP address is configured on the primary node.

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

Secondary node

The secondary node listens to the heartbeat messages sent from the primary node. Database on the secondary node is in read-replica mode only. None of the processes are active in the secondary node and the NetScaler Console user interface is not accessible on the secondary node.

Physical streaming replication

The primary and secondary nodes synchronize through heartbeat mechanism. With the physical streaming replication of database, the secondary node starts in read-replica mode. The secondary node listens to the heartbeat messages received from the primary node. If the secondary node does not receive any heartbeats for a time period of 180 seconds, the primary node is considered to be down. Then, the secondary node takes over as the primary node.

Heartbeat messages

Heartbeat messages are User Datagram Packets (UDP) that are sent and received between primary and secondary node. It monitors all subsystems of NetScaler Console and database to exchange information about the node state, health, processes, and so on. The information is shared between the high availability nodes every second. Notifications are sent as alerts to the administrator if there is a failover or break up of high availability states.

Floating IP address

The floating IP address is associated with the primary node in the high availability setup. It is an alias given to the primary node IP address, that the client can use to connect to NetScaler Console in the primary node. Since the floating IP address is configured on the primary node, the instance reconfiguration is not required in case of failover. The instances reconnect to the same IP address to reach the new primary.

Key points to note

- In a high availability setup, both the NetScaler Console nodes are deployed in active-passive mode. They must be on the same subnets using the same software version and build, and have same configurations.
- Floating IP address:
    - Floating IP address is configured on the primary node.

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

- Instances need not be reconfigured if there is a failover.
- You can access a high availability node from the user interface, either by using the primary node IP or floating IP address.

  > **Note:**
  >
  > We recommend you to use the floating IP address to access the user interface.

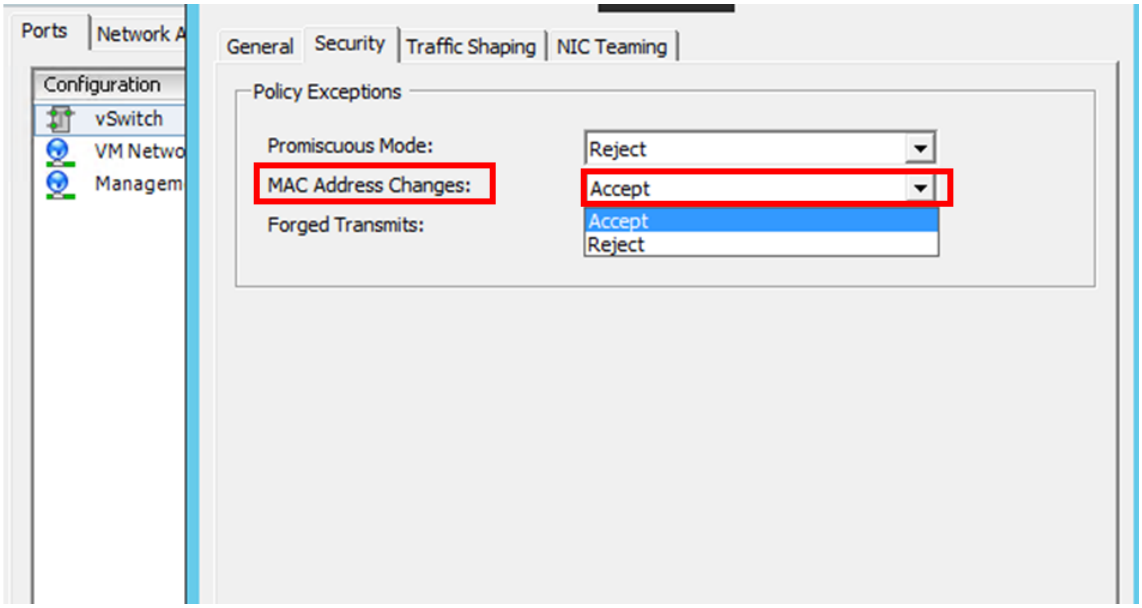
- Database:
  - In a high availability setup, all configuration files are synchronized automatically from the primary node to the secondary node at an interval of one minute.
  - Database synchronization happens instantly by physical replication of database.
  - Database on secondary node is in read-replica mode.
- NetScaler Console upgrade:
  - Internal processes implicitly upgrade NetScaler Console from the earlier versions.

    > **Note:**
    >
    > After the upgrade is successful, you must configure the floating IP address.

- UDP default port 5005 is available on both the nodes for heartbeats to be sent and for messages to be received.
- MAC address
  The setting for the "MAC Address Changes"option in a hypervisor affects the traffic that a virtual machine receives. Allow MAC address changes to be enabled on the virtual switch so that the floating IP address moves seamlessly to the new primary node after failover.
  For example, when deploying NetScaler Console on a high availability on VMware ESXi, ensure you accept changes to MAC address. ESXi now allows requests to change the active MAC address to other than the initial MAC address.

  > **Note:**
  >
  > For NetScaler Console deployed on ESXI version 6.7, you can set the **MAC Address Changes** option to **Reject** also. After failover, the traffic flows to new primary node seamlessly irrespective of the **MAC Address Changes** setting. Therefore, accept changes to MAC address is not mandatory.
  >
  > If the NetScaler Console is deployed on the ESXI version lower than 6.7, ensure the **MAC Address Changes** option is set to **Accept** only.

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



Prerequisites

Before you set up high availability for NetScaler Console nodes, note the following prerequisites:

- The NetScaler Console high availability deployment is supported from NetScaler Console version 12.0 build 51.24.
- Download the NetScaler Console image file (.xva) from the NetScaler site: https://www.citrix.com/downloads/

We recommend you to set CPU priority (in virtual machine properties) at the highest level to improve scheduling behavior and network latency.

The following table lists the minimum requirements for the virtual computing resources:

Component	Requirement
RAM	**32 GB**
Virtual CPU	**8 CPUs**

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

Component	Requirement
Storage Space	We recommend you to use solid-state drive (SSD) technology for NetScaler Console deployments. The default value is 120 GB. Actual storage requirement depends on NetScaler Console sizing estimation. If your NetScaler Console storage requirement exceeds 120 GB, you have to attach an additional disk. **Note:** You can add only one additional disk. We recommend you to estimate storage and attach additional disk at the time of initial deployment. For more information, see How to Attach an Additional Disk to NetScaler Console.
Virtual network interfaces	1
Throughput	1 Gbps or 100 Mbps
Hypervisor	**Versions**
Citrix Hypervisor	6.2 and 6.5
VMware ESXi	5.5 and 6.0
Microsoft Hyper-V	2012 R2
Linux KVM	Ubuntu and Fedora

To set up NetScaler Console in high availability mode

Starting from version 14.1 build 17.x, you can deploy a high availability setup directly from NetScaler Console GUI of the primary node.

1. Register the first server (primary node).
2. Register the second server (secondary node).
3. Deploy high availability setup in the primary node GUI.

Register the first server (primary node)

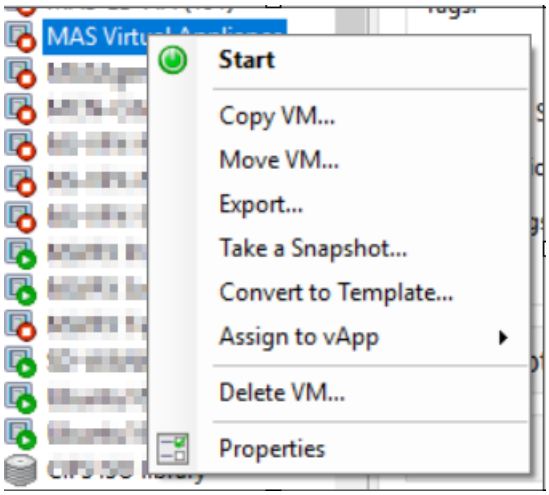
To register the primary node:

1. Use the .xva image file downloaded from the NetScaler site and import it in to your hypervisor.

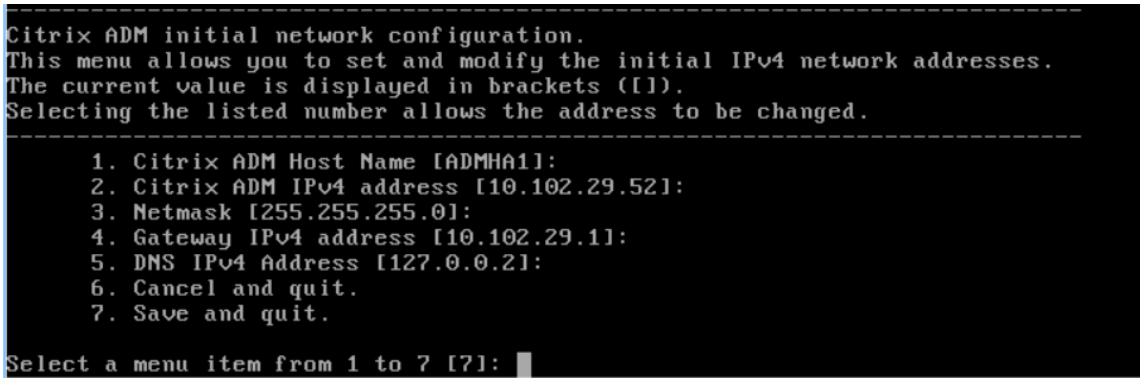
© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> It might take a few minutes for the .xva image file to import and get started. You can see the status on the bottom of the screen.
>
>
>

2. After the import is successful, right-click and click **Start**.



3. From the **Console** tab, configure NetScaler Console with the initial network configurations.



4. After the initial network configuration is complete, the system prompts for login. Log on using following credentials –*nsrecover/nsroot*.

> **Note:**
>
> After you log on, if you want to update the initial network configuration, type `networkconfig`, update the configuration, and save the configuration.

Register the second server (secondary node)

1. Use the **.xva** image file downloaded from the NetScaler site and import it in to your hypervisor.

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

2. From the **Console** tab, configure NetScaler Console with the initial network configurations as displayed in the following image.
3. After the initial network configuration is completed, the system prompts for login. Log on using following credentials –*nsrecover/nsroot*.

> **Notes:**
>
> - After you log on, if you want to update the initial network configuration, type `networkconfig`, update the configuration, and save the configuration.
> - The system will show error messages if there are any issues in the configuration.
> - The system reboots and takes a few minutes for the configurations to take effect.

Deploy high availability setup from the primary node GUI

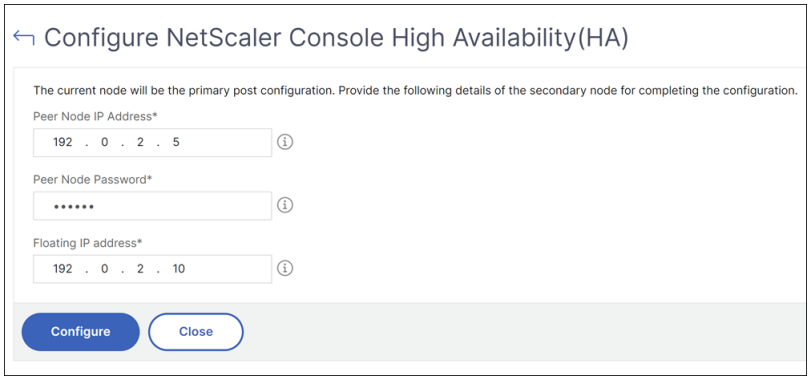
After registering both primary and secondary nodes, log in to the primary node GUI to set up the high availability pair.

> Note:
>
> - Before deploying the nodes into a high availability pair, ensure that the secondary node is completed with a reboot, after the initial network configuration.

To deploy a high availability pair from the primary node, follow these steps:

1. Log in to the primary node GUI.
2. Navigate to **Settings > Administration > High Availability Settings > Configure NetScaler Console High Availability (HA)**.
3. On the **Configure NetScaler Console High Availability (HA) page**, enter the following details for the secondary node:
    - Peer Node IP Address
    - Peer Node Password
    - Floating IP address
4. Click Configure.
5. On the **Confirm** page, click **Yes**.

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



Both primary and secondary nodes are rebooted to form a high availability pair, typically taking approximately 10 minutes.

> Notes:
>
> - You can now start using the **Floating IP address**.
> - A floating IP address is mandatory for high availability deployment of nodes.
> - After the high availability deployment is complete, use the floating IP address to access the NetScaler Console user interface.

6. Navigate to **Settings > Deployment** to validate the deployment.

> Note:
>
> The secondary node might take around 10 minutes to come up. Until then, the secondary node status is shown as **Down**.

For more information, see the Frequently Asked Questions.

Disable high availability

You can disable high availability on a NetScaler Console high availability pair and convert the nodes to standalone NetScaler Console servers.

> **Note:**
>
> Disable high availability from the primary node.

To disable the high availability:

1. In a web browser, enter the IP address of the NetScaler Console server primary node.
2. In the **User Name** and **Password** fields, enter the administrator credentials.
3. On the **System** tab, navigate to **Deployment** and click **Break HA**.

   A dialogue box is displayed. Click **Yes** to break the high availability deployment.

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

Redeploy high availability

After you disable the high availability to a standalone deployment, you can redeploy it to high availability mode again. Redeploying high availability is similar to the first time deployment of high availability. For more details see Deploy high availability setup from the primary node GUI.

> **Note:**
>
> After disabling NetScaler® Console high availability, use only one console node as the standalone license server. The second node must be reprovisioned.

High availability failover scenarios

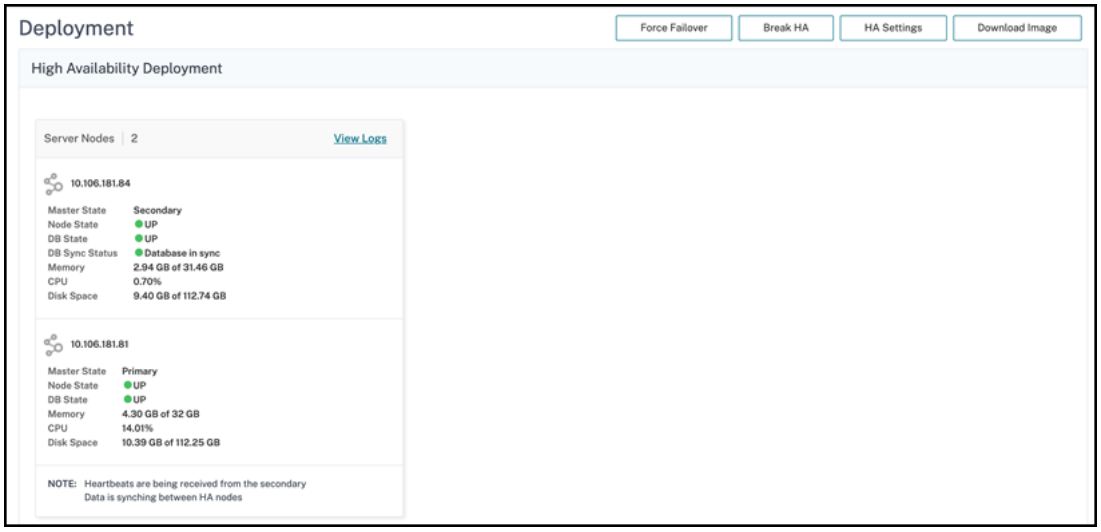
A failover occurs if one of the following conditions is encountered:

- **Node failure**: Primary node goes down, no heartbeat is detected from primary node for 180 seconds.
- **Application health failure**: Primary node is up and running but one of the NetScaler Console processes is down.

View Database Synchronization Log messages

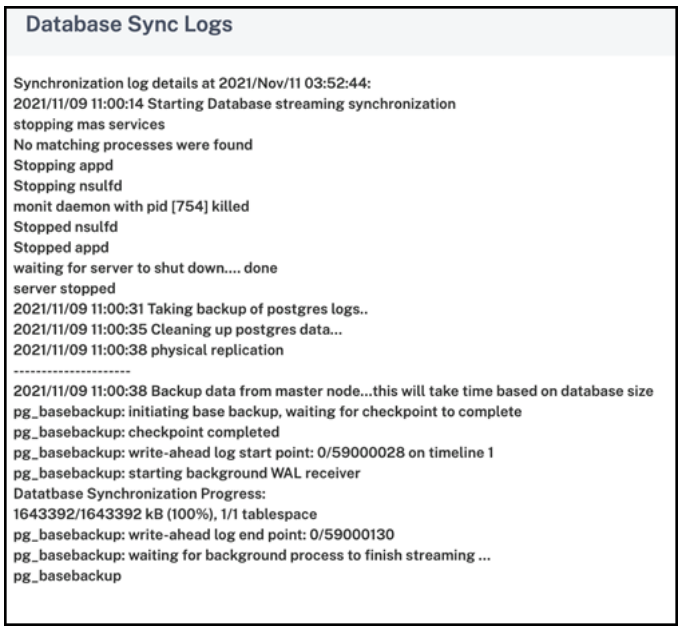
In the NetScaler Console HA pair, the configuration files are synchronized automatically from the primary node to the secondary node and the physical streaming replication of database happens.

However, if there is a streaming replication error, the **Sync Database** button appears. You can click the **Sync Database** button to start the database synchronization process.



To view the progress of the database synchronization, click **View Logs**. The **Database Sync Logs** message appears and you can view the details of the synchronization progress real-time.

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



Split-brain scenario

When there is no communication between both the nodes due to downtime in network link, then:

- Primary node continues to operate as primary
- Secondary node takes over as primary because of the failure to receive heartbeats
- Both the nodes would run their individual database instances

For example, in an enterprise two NetScaler Console nodes have been deployed as primary and secondary. Due to a possible network link downtime, the communication between the two NetScaler Console nodes breaks completely. Since there is no heartbeat exchange for over 180 seconds, both the nodes consider themselves to be the primary node. Both nodes act as active nodes and run their own instances of database.

From NetScaler Console 12.1 or later release, this split-brain situation is handled gracefully after the network link and heartbeat is restored. High availability synchronization is restored automatically. The recovery time depends on the data and speed of the link between the nodes.

> **Note:**
>
> During the split-brain condition, changes that occurred on the old primary node is reset with the new primary when it is rejoined in high availability. The changes that happened on new primary node during split-brain remains intact.

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

Licensing

The NetScaler Console server can contain VIP, CICO, and pooled capacity licenses. When the licenses are issued to a NetScaler Console server, the licenses are bound to the server host ID. Assigning licenses to a different NetScaler Console server is restricted.

If you configure a NetScaler Console high-availability pair as a license server, license files applied on primary get synchronized to secondary.

> **Note:**
>
> - In release 12.1-50.x and later, the NetScaler Console licenses are automatically synchronized from primary to the secondary node.

Configure disaster recovery for high availability

September 27, 2025

Disaster is a sudden disruption of business functions caused by natural calamities or human caused events. Disasters affect data center operations, after which resources and the data lost at the disaster site must be fully rebuilt and restored. The loss of data or downtime in the data center is critical and collapses the business continuity.

The NetScaler Console disaster recovery (DR) feature provides full system backup and recovery capabilities for NetScaler Console deployed in high availability mode. At the time of recovery, certificates, configuration files, and a complete backup of the database is available in the recovery site.

The following table describes the terms used while configuring disaster recovery in NetScaler Console.

Terms	Description
Primary site (Data center A)	The primary site has NetScaler Console nodes deployed in high availability mode.
Recovery site (Data center B)	The recovery site has a disaster recovery node deployed in standalone mode. This node is in read-only mode and is not operational until the primary site is down.

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

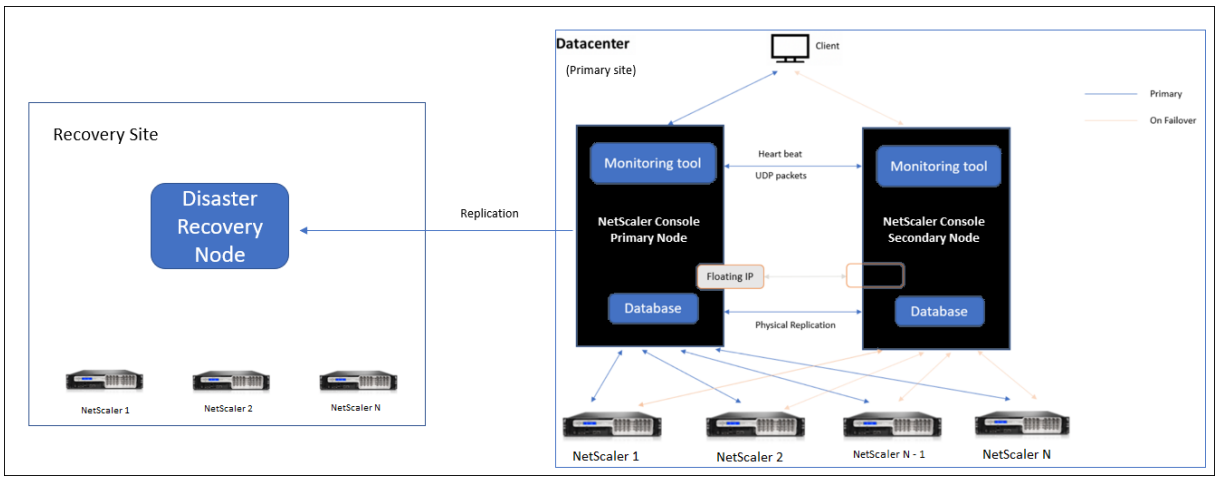
Terms	Description
Disaster recovery node	The recovery node is a standalone node deployed in the recovery site. This node is made operational (to the new primary) in case a disaster occurs at the primary site and it is nonfunctional.

> **Note**
>
> The primary site and DR site communicate with each other through ports 5454 and 22, and these ports are enabled by default.
>
> For more information on port and protocol details, see Ports.

Disaster recovery workflow

The following image shows the disaster recovery workflow, the initial setup before disaster, and the workflow after the disaster.

Initial setup before disaster



The image shows the disaster recovery setup before disaster.

The primary site has NetScaler Console nodes deployed in the high availability mode. To learn more, see High availability deployment

The recovery site has a standalone NetScaler Console disaster recovery node deployed remotely. The disaster recovery node is in read-only mode and receives data from the primary node to create data backup. NetScaler instances in the recovery site are also discovered but, they do not have any traffic

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

flowing through them. During the backup process, all data, files, and configurations are replicated on the disaster recovery node from the primary node.

Prerequisites

Before you set up the disaster recovery node, note the following the prerequisites:

- To enable disaster recovery settings, the primary site must have NetScaler Console nodes configured in high availability mode.
- The NetScaler Console HA pair (in primary site) and the standalone node (in DR site) must have same software version, build, and configurations.

We recommend that you set CPU priority (in virtual machine properties) at the highest level to improve scheduling behavior and network latency.

The following table lists the minimum requirements to configure the Disaster Recovery node:

Component	Requirement
RAM	32 GB
Virtual CPU	8 CPUs
Storage Space	We recommend using solid-state drive (SSD) technology for NetScaler Console deployments. The default value is 120 GB. Actual storage requirement depends on NetScaler Console sizing estimation. If your NetScaler Console storage requirement exceeds 120 GB, you have to attach an extra disk. **Note** You can add only one more disk. We recommend you to estimate storage and attach more disk at the time of initial deployment. For more information, see How to Attach an Additional Disk to NetScaler Console.
Virtual network interfaces	1
Throughput	1 Gbps or 100 Mbps
Hypervisor	**Versions**
Citrix Hypervisor	6.2 and 6.5
VMware ESXi	5.5 and 6.0
Microsoft Hyper-V	2012 R2

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

Component	Requirement
Linux KVM	Ubuntu and Fedora

First time disaster recovery setup

- Deploy NetScaler Console in high availability mode
- Deploy and register the NetScaler Console disaster recovery node
- Enable and disable disaster recovery settings from the user interface

Deploy NetScaler Console in high availability mode

To set up the disaster recovery settings, ensure that NetScaler Console is deployed in high availability mode. For information on deploying the NetScaler Console in high availability, see High availability deployment

> **Note**
>
> - NetScaler Console deployed in high availability mode must be upgraded to NetScaler Console release version 13.1.
> - **Floating IP address is mandatory** to register disaster recovery node with the primary node.

Deploy and register the NetScaler Console disaster recovery node using DR console

To register the NetScaler Console disaster recovery node:

1. Download the `.xva` image file from the NetScaler site and import it into your hypervisor.
2. From the **Console** tab, configure NetScaler Console with the initial network configurations.

   > **Note**
   >
   > The disaster recovery node can be on a different subnet.

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

```
--------------------------------------------------------------------------------
Citrix ADM 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 Host Name [DR]:
      2. Citrix ADM IPv4 address [10.102.29.53]:
      3. Netmask [255.255.255.0]:
      4. Gateway IPv4 address [10.102.29.1]:
      5. DNS IPv4 Address [127.0.0.2]:
      6. Cancel and quit.
      7. Save and quit.

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

3. After the initial network configuration is complete, the system prompts for login. Log on using the following credentials –`nsrecover`/`nsroot`.

> **Important**
>
> Do not change the DR node credentials (`nsrecover`/`nsroot`) during registration. You can change the DR node credentials after you register DR node successfully.

4. To deploy the disaster recovery node, type **/mps/deployment_type.py** and press enter. The NetScaler Console deployment configuration menu is displayed.

```
bash-3.2# /mps/deployment_type.py
--------------------------------------------------------------------------------
------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
--------------------------------------------------------------------------------
------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

5. Select **2** to register disaster recovery node.

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

```
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 2
Selected Option      2. Remote Disaster Recovery Node.
```

6. The console prompts for floating IP address of the high availability node and password.
7. Enter the floating IP address and password to register the disaster recovery node to the primary node.

```
------------------------------------------------------------------------------
    Backup node Configuration.

    Specify the IP address and the password of the Citrix ADM server.
    Type 0 anytime to cancel and quit.
    ------------------------------------------------------------------------
    Enter Citrix ADM Floating IP Address:10.102.29.97
    Enter password for Citrix ADM:
```

The disaster recovery node is now registered successfully.

```
Stopping appd
Stopping nsulfd
Stopped nsulfd
Stopped appd
waiting for server to shut down.... done
server stopped
------------------------------------------------------------------------
    Backup node Registration successful.
```

> **Note**
>
> - The disaster recovery node does not have a GUI.
> - After registration is successful, the default administrator credentials to log on to the server are `nsroot`/`nsroot`.

8. If you want to change the DR node password, run the following script:

```
1 /mps/change_freebsd_password.sh <username> <password>
```

Example:

```
1 /mps/change_freebsd_password.sh nsroot new_password
```

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

Deploy the disaster recovery node using NetScaler Console GUI

After the disaster recovery node is registered successfully using DR console, deploy the DR node from the NetScaler Console GUI. This step enables the disaster recovery settings from the NetScaler Console primary site.

1. Navigate to **System > System Administration > Disaster Recovery Settings.**
2. On the **Disaster Recovery** page, select **Deploy DR Node**.
3. A confirmation dialogue box is displayed. Click **Yes** to continue.

   > **Note**
   >
   > The time taken for system backup depends on the data size and the WAN link speed.

After you deploy the DR node successfully in the NetScaler Console GUI, you can monitor database state, memory, CPU, and disk usage of the DR node.

To disable the disaster recovery settings, select **Remove DR Node**. A confirmation dialogue box is displayed. Click **Yes** to continue.

To enable the DR node again, reconfigure the DR node for your high availability pair:

1. Log on to the DR node using a hypervisor or an SSH console.
2. Configure the DR node by following the procedure available at Deploy and register the NetScaler Console disaster recovery node using DR console.
3. Deploy the disaster recovery node using NetScaler Console GUI.

For more information, see the FAQs.

> **Important**
>
> - It is the responsibility of the administrator to detect that a disaster has occurred on the primary site.
> - The disaster recovery workflow is manually initiated by the administrator after the primary site goes down.
> - An administrator must manually initiate the process by running a recovery script on the disaster recovery node at the recovery site.
> - If you upgrade the HA pair in primary site, you must also manually upgrade the standalone node in the DR site.

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

Workflow after the disaster

When the primary site goes down after a disaster, the disaster recovery workflow must be initiated as follows:

1. The administrator identifies that a disaster has struck the primary site and it is not operational.
2. The administrator initiates the recovery process.
3. The administrator must manually run one of the following recovery scripts on the disaster recovery node based on your requirement(at the recovery site):

    - Configure SNMP, Syslog, and Analytics on the DR node:

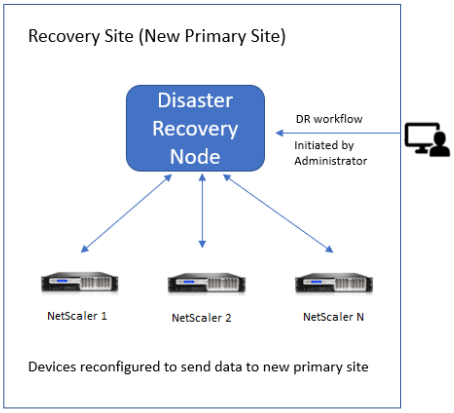
    ```
    /mps/scripts/pgsql/pgsql\_restore\_remote\_backup.sh
    ```

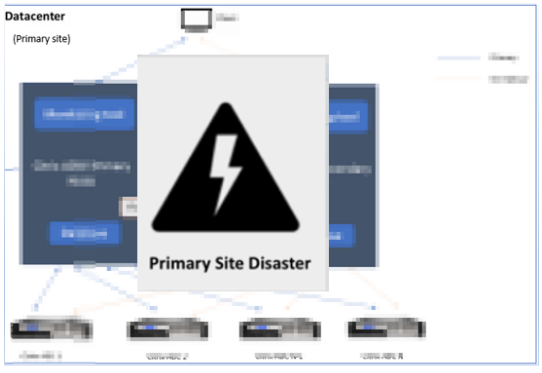
    - Configure the DR node as a license server also:

    ```
    /mps/scripts/pgsql/pgsql\_restore\_remote\_backup.sh -
       reconfig-ls <IP-address-of-the-primary-site>
    ```

4. Internally, NetScaler instances are automatically reconfigured to send the data to the disaster recovery node that has now become the new primary site.

    The following image shows that the disaster recovery workflow after the primary site is struck with a disaster.





> **Note:**
>
> After you initiate the script at the DR site, the DR site now becomes the new primary site. You can also access the DR user interface.

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

Post disaster recovery

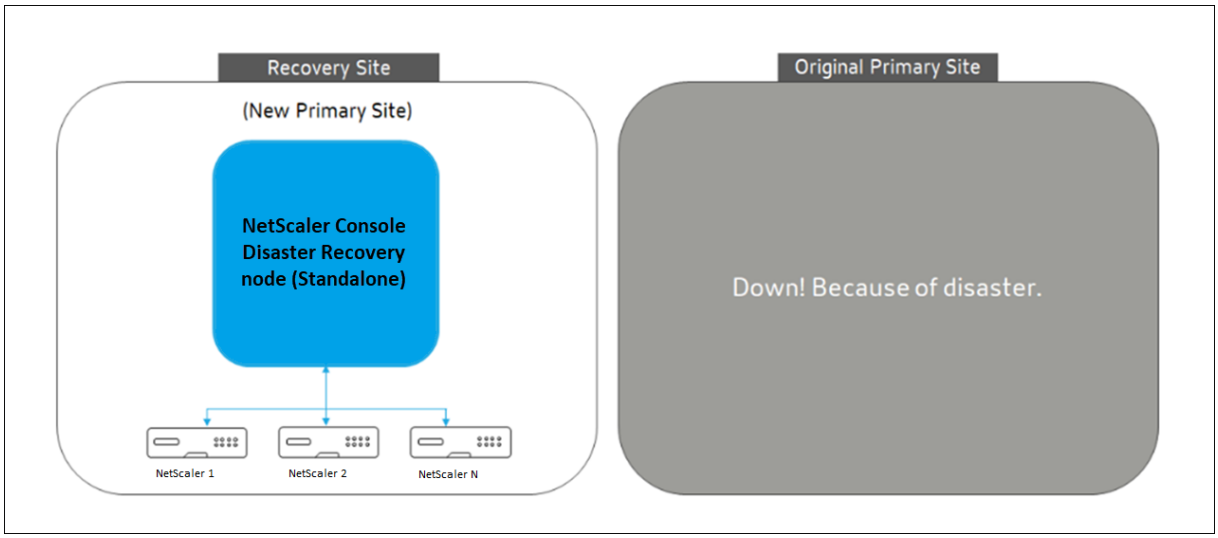
After the disaster has occurred and the administrator initiates the recovery script, the DR site now becomes the new primary site.

If you want to revert the configurations to the original site later, see Revert configurations to the original primary site.

> **Important**
>
> - If you have installed NetScaler Console 12.1.49.x or earlier releases, you get a grace period of 30 days to contact Citrix to rehost the original license on the NetScaler Console (at the DR site).
> - For 12.1.50.x or later releases, the NetScaler Console license is automatically synchronized to the DR site (Not a requirement to contact Citrix for the license).
> - If you have applied pooled licenses for the instances, NetScaler instances with version **11.1 65.x or later**, **12.1 58.x or later**, **13.0 47.x or later**, and NetScaler SDX **13.0 76.x or later** have the support for auto-license server update in the DR site. All other versions, you must manually reconfigure the instances to the DR site.

Revert configurations to the original primary site

Post disaster the configured disaster recovery (DR) node becomes the new primary site and the client traffic flows through this node.



For more information, see Workflow after the disaster.

When your original primary site is free from disaster and you decide to move all operations to the primary site, reconfigure the original primary site to match the configurations from the DR node.

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

Before you begin, ensure both primary site and DR site are active.

To revert the changes to the original primary site from the DR site, perform the following steps:

1. Log in to the original primary site and run the following command:

```
nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-password> -L <primary-node-password> &
```

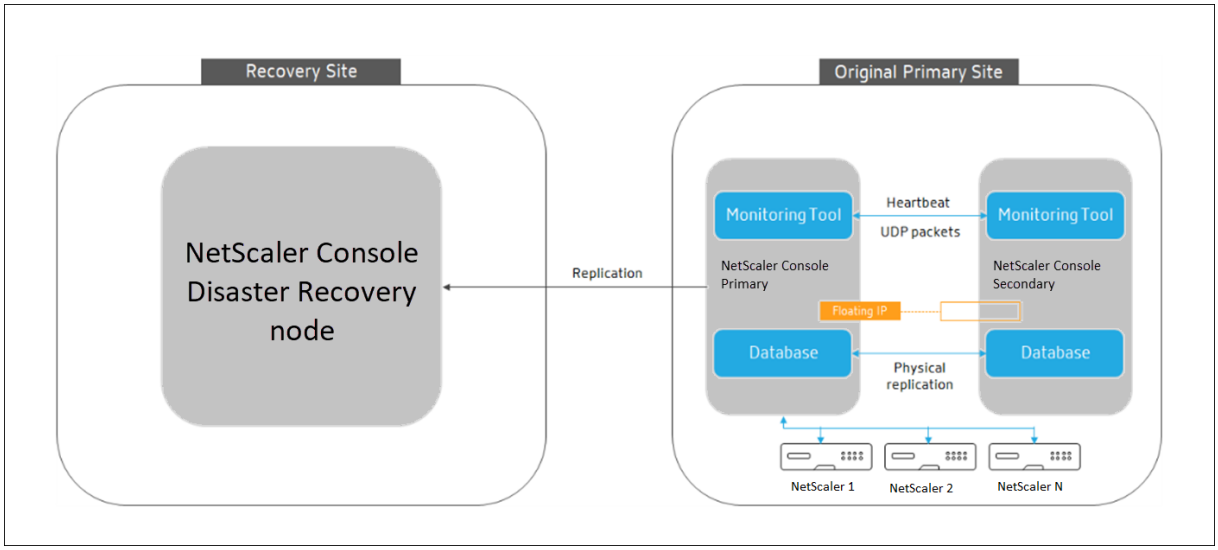
   This command configures only Syslog, SNMP, and Analytics to the primary site.

   If you want to configure the primary site as a pooled license server for NetScaler instances, run the following command:

```
nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-password> -L <primary-node-password>  -O yes &
```

   The `-O` command fetches the DR site IP address and reconfigures the primary site as pooled license server.

2. Reconfigure the DR site. See, Deploy disaster recovery setup.



After you successfully revert the configurations from the DR site to the original primary site, the client traffic flows through the NetScaler Console primary node.

Configure disaster recovery for standalone node

September 27, 2025

You can also configure a disaster recovery for NetScaler Console deployed in standalone mode.

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

The following table describes the terms used while configuring disaster recovery in NetScaler Console.

Terms	Description
Primary site (Data center A)	The primary site has NetScaler Console node deployed in standalone mode.
Recovery site (Data center B)	The recovery site has a disaster recovery node deployed in standalone mode. This node is in read-only mode and is not operational until the primary site is down.
Disaster recovery node	The recovery node is a standalone node deployed in the recovery site. This node is made operational (to the new primary) in case a disaster occurs at the primary site and it is nonfunctional.

> **Note**
>
> The primary site and DR site communicate with each other through ports 5454 and 22, and these ports are enabled by default.
>
> For more information on port and protocol details, see Ports.

Disaster recovery workflow

The primary site has NetScaler Console node deployed in the standalone mode.

The recovery site has a disaster recovery node deployed remotely. The disaster recovery node is in read-only mode and receives data from the primary node to create data backup. NetScaler instances in the recovery site are also discovered but, they do not have any traffic flowing through them. During the backup process, all data, files, and configurations are replicated on the disaster recovery node from the primary node.

Prerequisites

Before you set up the disaster recovery node, note the following the prerequisites:

- To enable disaster recovery settings, the primary site must have NetScaler Console configured in standalone mode.
- The standalone NetScaler Console (in primary site) and the disaster recovery node (in DR site) must have same software version, build, and configurations.

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

We recommend that you set CPU priority (in virtual machine properties) at the highest level to improve scheduling behavior and network latency.

The following table lists the minimum requirements to configure the Disaster Recovery node:

Component	Requirement
RAM	32 GB
Virtual CPU	8 CPUs
Storage Space	We recommend using solid-state drive (SSD) technology for NetScaler Console deployments. The default value is 120 GB. Actual storage requirement depends on NetScaler Console sizing estimation. If your NetScaler Console storage requirement exceeds 120 GB, you have to attach an extra disk. **Note** You can add only one more disk. We recommend you to estimate storage and attach more disk at the time of initial deployment. For more information, see How to Attach an Additional Disk to NetScaler Console.
Virtual network interfaces	1
Throughput	1 Gbps or 100 Mbps
Hypervisor	**Versions**
Citrix Hypervisor	6.2 and 6.5
VMware ESXi	5.5 and 6.0
Microsoft Hyper-V	2012 R2
Linux KVM	Ubuntu and Fedora

First time disaster recovery setup

- Deploy NetScaler Console
- Deploy and register the NetScaler Console disaster recovery node
- Enable and disable disaster recovery settings from the user interface

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

Deploy NetScaler Console

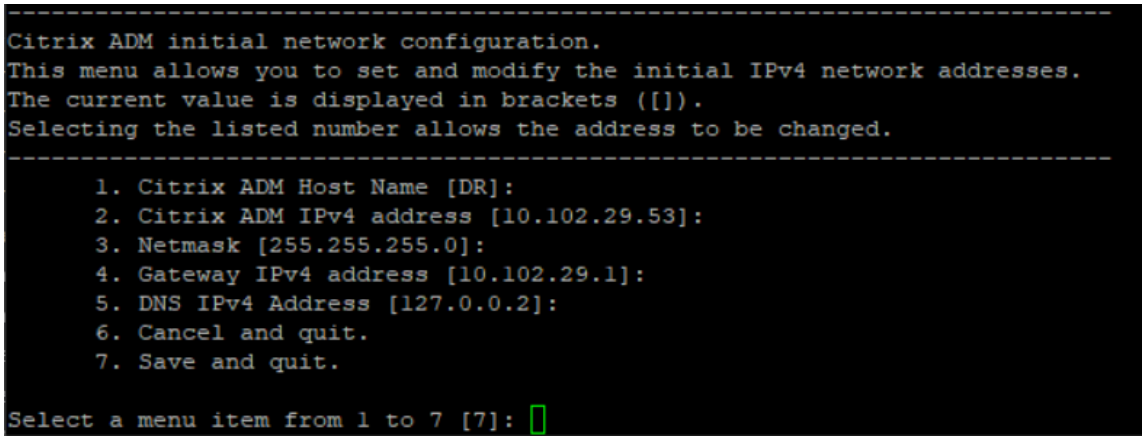
To set up the disaster recovery settings, ensure that NetScaler Console is deployed in standalone mode. For more information, see single-server deployment.

Deploy and register the NetScaler Console disaster recovery node using DR console

To register the NetScaler Console disaster recovery node:

1. Download the `.xva` image file from the NetScaler site and import it into your hypervisor.
2. From the **Console** tab, configure NetScaler Console with the initial network configurations.

   > **Note**
   >
   > The disaster recovery node can be on a different subnet.

3. After the initial network configuration is complete, the system prompts for login. Log on using the following credentials –`nsrecover`/`nsroot`.

   > **Important**
   >
   > Do not change the DR node credentials (`nsrecover`/`nsroot`) during registration. You can change the DR node credentials after you register DR node successfully.

4. To deploy the disaster recovery node, type **/mps/deployment_type.py** and press enter. The NetScaler Console deployment configuration menu is displayed.

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

```
bash-3.2# /mps/deployment_type.py
------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

5. Select **2** to register disaster recovery node.

```
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 2
Selected Option      2. Remote Disaster Recovery Node.
```

6. The console prompts for the standalone node IP address and password.
7. Enter the standalone node IP address and password to register the disaster recovery node.

   The disaster recovery node is now registered successfully.

```
Stopping appd
Stopping nsulfd
Stopped nsulfd
Stopped appd
waiting for server to shut down.... done
server stopped
------------------------------------------------------------------------
    Backup node Registration successful.
```

> **Note**
>
> - The disaster recovery node does not have a GUI.
> - After registration is successful, the default administrator credentials to log on to the server are `nsroot`/`nsroot`.

8. If you want to change the DR node password, run the following script:

```
1 /mps/change_freebsd_password.sh <username> <password>
```

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

Example:

```
/mps/change_freebsd_password.sh nsroot new_password
```

Deploy the disaster recovery node using NetScaler Console GUI

After the disaster recovery node is registered successfully using DR console, deploy the DR node from the NetScaler Console GUI. This step enables the disaster recovery settings from the NetScaler Console primary site.

1. Navigate to **System > System Administration > Disaster Recovery Settings.**
2. On the **Disaster Recovery** page, select **Deploy DR Node**.
3. A confirmation dialogue box is displayed. Click **Yes** to continue.

> **Note**
>
> The time taken for system backup depends on the data size and the WAN link speed.

After you deploy the DR node successfully in the NetScaler Console GUI, you can monitor database state, memory, CPU, and disk usage of the DR node.

To disable the disaster recovery settings, select **Remove DR Node**. A confirmation dialogue box is displayed. Click **Yes** to continue.

To enable the DR node again, reconfigure the DR node for your high availability pair:

1. Log on to the DR node using a hypervisor or an SSH console.
2. Configure the DR node, by following the procedure available at Deploy and register the NetScaler Console disaster recovery node using DR console.
3. Deploy the disaster recovery node using NetScaler Console GUI.

For more information, see the FAQs.

> **Important**
>
> - It is the responsibility of the administrator to detect that a disaster has occurred on the primary site.
> - The disaster recovery workflow is manually initiated by the administrator after the primary site goes down.
> - An administrator must manually initiate the process by running a recovery script on the disaster recovery node at the recovery site.
> - If you upgrade the standalone node in primary site, you must also manually upgrade the

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

> standalone node in the DR site.

Workflow after the disaster

When the primary site goes down after a disaster, the disaster recovery workflow must be initiated as follows:

1. The administrator identifies that a disaster has struck the primary site and it is not operational.
2. The administrator initiates the recovery process.
3. The administrator must manually run one of the following recovery scripts on the disaster recovery node based on your requirement(at the recovery site):
   - Cofigure SNMP, Syslog, and Analytics on the DR node:

     ```
     /mps/scripts/pgsql/pgsql\_restore\_remote\_backup.sh
     ```

   - Configure the DR node as a license server also:

     ```
     /mps/scripts/pgsql/pgsql\_restore\_remote\_backup.sh -
        reconfig-ls <IP-address-of-the-primary-site>
     ```

4. Internally, NetScaler instances are automatically reconfigured to send the data to the disaster recovery node that has now become the new primary site.

   > **Note:**
   >
   > After you initiate the script at the DR site, the DR site now becomes the new primary site. You can also access the DR user interface.

Post disaster recovery

After the disaster has occurred and the administrator initiates the recovery script, the DR site now becomes the new primary site.

If you want to revert the configurations to the original site later, see Revert configurations to the original primary site.

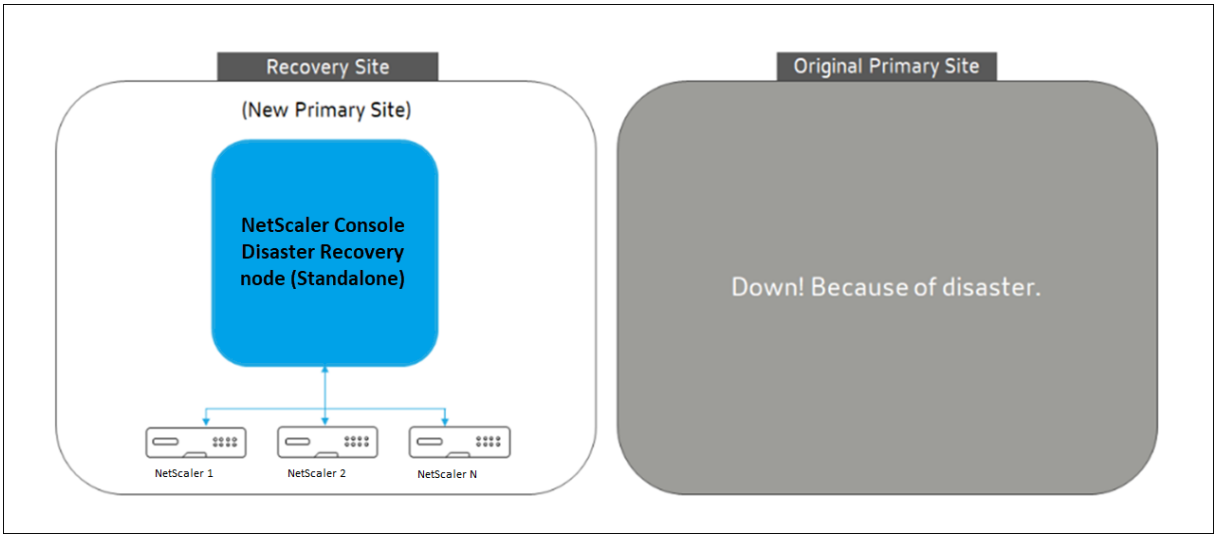
> **Important**
>
> - If you have installed NetScaler Console 12.1.49.x or earlier releases, you get a grace period of 30 days to contact Citrix to rehost the original license on the NetScaler Console (at the DR site).
> - For 12.1.50.x or later releases, the NetScaler Console license is automatically synchronized to the DR site (Not a requirement to contact Citrix for the license).

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

> - If you have applied pooled licenses for the instances, NetScaler instances with version **11.1 65.x or later**, **12.1 58.x or later**, **13.0 47.x or later**, and NetScaler SDX **13.0 76.x or later** have the support for auto-license server update in the DR site. All other versions, you must manually reconfigure the instances to the DR site.

Revert configurations to the original primary site

Post disaster the configured disaster recovery (DR) node becomes the new primary site and the client traffic flows through this node.



For more information, see Workflow after the disaster.

When your original primary site is free from disaster and you decide to move all operations to the primary site, reconfigure the original primary site to match the configurations from the DR node.

Before you begin, ensure both primary site and DR site are active.

To revert the changes to the original primary site from the DR site, perform the following steps:

1. Log in to the original primary site and run the following command:

```
nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-password> -L <primary-node-password> &
```

   This command configures only Syslog, SNMP, and Analytics to the primary site.

   If you want to configure the primary site as a pooled license server for NetScaler instances, run the following command:

```
nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-password> -L <primary-node-password>  -O yes &
```

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

The −O command fetches the DR site IP address and reconfigures the primary site as pooled license server.

2. Reconfigure the DR site. See, Deploy disaster recovery setup.

After you successfully revert the configurations from the DR site to the original primary site, the client traffic flows through the NetScaler Console primary node.

Configure on-prem agents for multisite deployment

September 27, 2025

In the earlier versions of NetScaler Console, NetScaler instances deployed in remote data centers can be managed and monitored from NetScaler Console running in a primary data center. NetScaler instances sent data directly to the primary NetScaler Console that resulted in consumption of WAN bandwidth. Also, processing of analytics data utilizes CPU and memory resources of the primary NetScaler Console.

You can have data centers located across the globe. Agents play a vital role in the following scenarios:

- To install agents in remote data centers so that there is reduction in WAN bandwidth consumption.
- To limit the number of instances directly sending traffic to primary NetScaler Console for data processing.

> **Note**
>
> - Installing agents for instances in remote data center is recommended but not mandatory. If necessary, users can directly add NetScaler instances to primary NetScaler Console.
> - If you have installed agents for one or more remote data centers, then the communication between the agents and the primary site is through floating IP address. For more information, see port.
> - You can install agents and apply pooled licenses to the instances at one or more remote data centers. In this scenario, the communication between the primary site and one or more remote data centers is through the floating IP address.
> - NetScaler Console on-premises agent doesn't support pooled licensing.

From NetScaler Console 12.1 or later, instances can be configured with agents to communicate with the primary NetScaler Console located in a different data center.

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

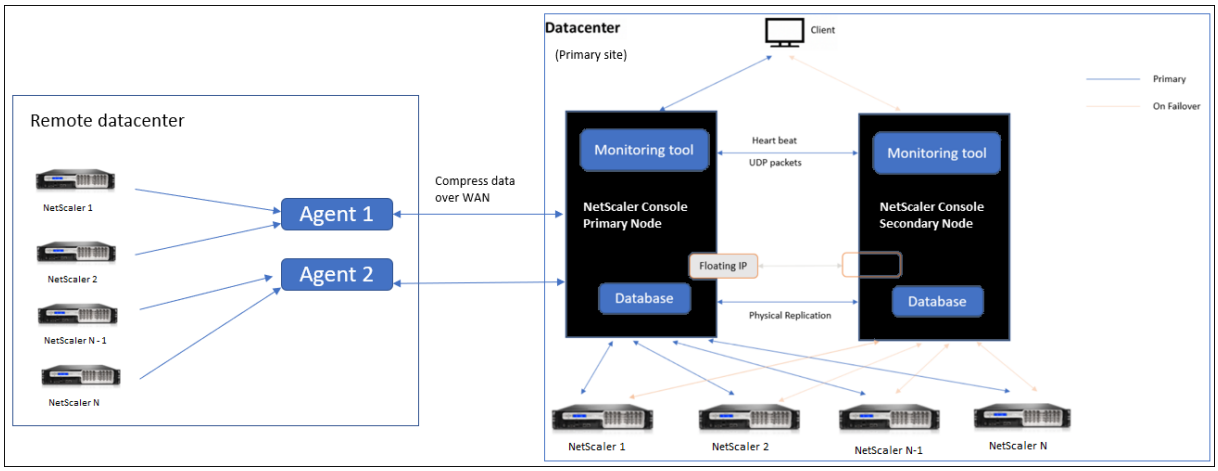
Agents work as an intermediary between the primary NetScaler Console and the discovered instances across different data centers. Following are the benefits of installing agents:

- The instances are configured to agents so that the unprocessed data is sent directly to agents instead of primary NetScaler Console. Agents do the first level of data processing and send the processed data in compressed format to the primary NetScaler Console for storage.
- Agents and instances are co-located in the same data center 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 is switched to another available agent in the same site.

> **Note**
>
> The number of agents to be installed per site depends on the traffic being processed.

Architecture

The following figure shows NetScaler instances in two data centers and NetScaler Console high availability deployment using multisite agent-based architecture.



The primary site has the NetScaler Console nodes deployed in a high availability configuration. The NetScaler instances in the primary site are directly registered with the NetScaler Console.

In the secondary site, agents are deployed and registered with the NetScaler Console server in the primary site. These agents work in a cluster to handle continuous flow of traffic in case an agent failover occurs. The NetScaler instances in the secondary site are registered with the primary NetScaler Console server through agents located within that site. The instances send data directly to agents instead of primary NetScaler Console. The agents process the data received from the instances and send it to the primary NetScaler Console in a compressed format. Agents communicate with the NetScaler Console server over a secure channel and the data sent over the channel is compressed for bandwidth efficiency.

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

Get started

- Install the agent in a data center
  - Register the agent
  - Attach the agent to a site
- Add NetScaler instances
  - Add new instance
  - Update an existing instance

Install the agent in a data center

You can install and configure the agent, to enable communication between the primary NetScaler Console and the managed NetScaler instances in another data center.

You can install an agent on the following hypervisors in your enterprise data center:

- Citrix Hypervisor™
- VMware ESXi
- Microsoft Hyper-V
- Linux KVM Server

> **Note**
>
> On-prem agents for multisite deployment are supported only with NetScaler Console high availability deployment.

Before you begin installing the agent, ensure you have the required virtual computing resources that the hypervisor must provide for each agent.

Component	Requirement
RAM	32 GB
Virtual CPU	8 CPUs
Storage space	30 GB
Virtual Network Interfaces	1
Throughput	1 Gbps

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

Ports

For communication purposes, the following ports must be open between the agent and NetScaler Console on-prem server.

Type	Port	Details	Direction of communication
TCP	8443, 7443, 443	For outbound and inbound communication between agent and the NetScaler Console on-prem server.	NetScaler agent to NetScaler Console

The following ports must be open between the agent and NetScaler Instances.

Type	Port	Details	Direction of communication
TCP	80	For NITRO communication between agent and NetScaler instance.	NetScaler Console to NetScaler and NetScaler to NetScaler Console
TCP	22	For SSH communication between agent and NetScaler instance. For synchronization between NetScaler Console servers deployed in high availability mode.	NetScaler Console to NetScaler and NetScaler agent to NetScaler
UDP	4739	For AppFlow communication between agent and NetScaler instance.	NetScaler to NetScaler Console

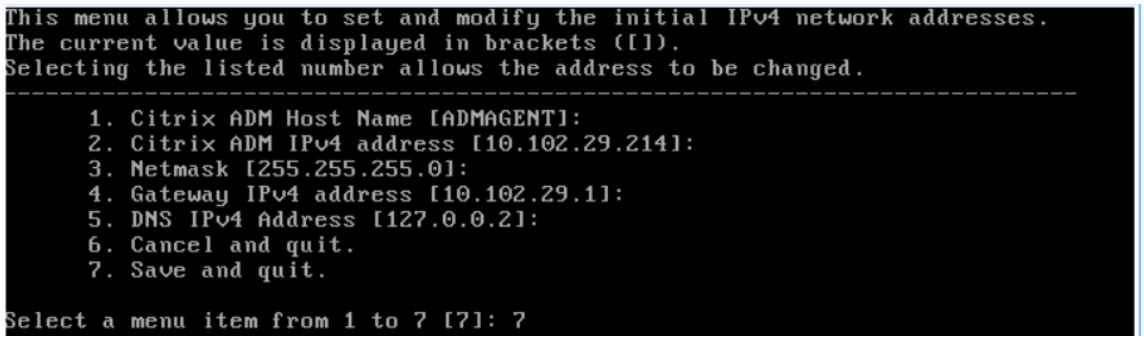
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Type	Port	Details	Direction of communication
ICMP	No reserved port	To detect network reachability between NetScaler Console and NetScaler instances, or the secondary NetScaler Console server deployed in high availability mode.	
UDP	161, 162	To receive SNMP events from NetScaler instance to agent.	Port 161 - NetScaler Console to NetScaler Port 162 - NetScaler to NetScaler Console
UDP	514	To receive syslog messages from NetScaler instance to agent.	NetScaler to NetScaler Console
TCP	5557	For Logstream communication between agent and NetScaler instances.	NetScaler to NetScaler Console

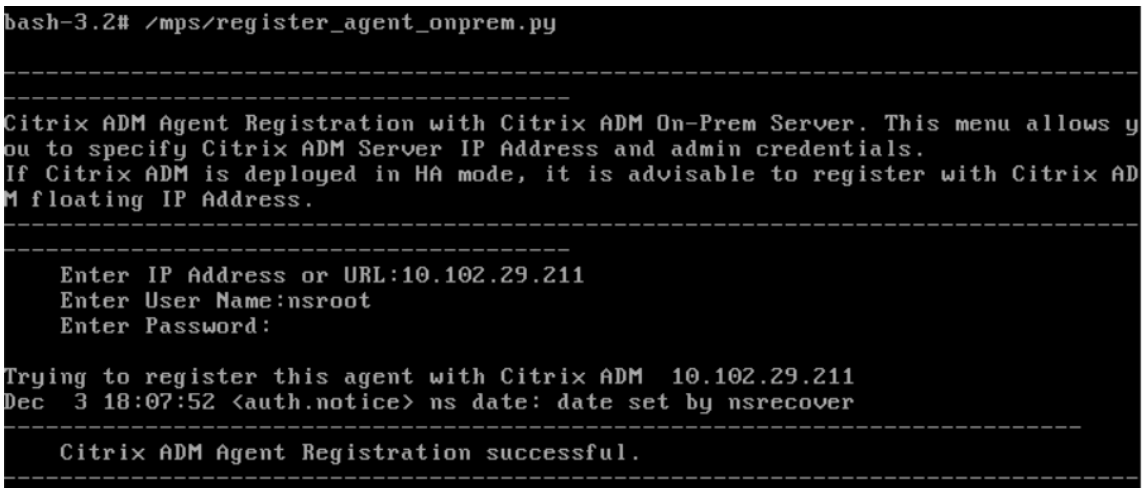
Register the agent

1. Use the agent image file downloaded from the NetScaler site and import it in to your hypervisor. The naming pattern of the agent image file is as follows, **MASAGENT-<HYPERVISOR>-<Version.no>.** For example: **MASAGENT-XEN-13.0-xy.xva**
2. From the **Console** tab, configure NetScaler Console with the initial network configurations.
3. Enter the NetScaler Console host name, IPv4 address, and gateway IPv4 address. Select option 7 to save and quit the configuration.

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



4. After the registration is successful, the console prompts to log on. Use *nsrecover/nsroot* as the credentials.
5. To register the agent, enter **/mps/register_agent_onprem.py**. The NetScaler agent registration credentials are displayed as shown in the following image.
6. Enter the NetScaler Console floating IP address and the user credentials.



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

After the agent restarts, access the NetScaler Console GUI, from the main menu go to the **Infrastructure > Instances > Agents** page to verify the status of the agent. The newly added agent is displayed in **Up** state.

> **Note**
>
> The NetScaler Console displays the version of the agent and also checks if the agent is on the latest version. The download icon signifies that the agent is not on the latest version and needs to be upgraded. We recommend you upgrade the agent version to the NetScaler Console version.

Attach an agent to a site

1. Select the agent and click **Attach Site.**

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

2. In the **Attach site** page, select a site from the list, or create a site using the plus (+) button.
3. Click **Save.**

> **Note**
>
> - By default, all newly registered agents are added to the default data center.
> - It is important to associate the agent with the correct site. In the event of an agent failure, the NetScaler instances assigned to it are automatically switched to other functioning agents in the same site.

Agent actions

You can apply various actions to an agent under **Infrastructure > Agents > Select Actions**.

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 default 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 NetScaler agent. You can download this file and send it to Citrix technical support for investigation and troubleshooting.

Add NetScaler instances

Instances are NetScaler appliances or virtual appliances that you want to discover, manage, and monitor from NetScaler Console through agents. You can add the following NetScaler appliances and virtual appliances to NetScaler Console or agents:

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler Gateway
- Citrix SSL Forward Proxy

For more information, see Add instances to NetScaler Console.

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

Attach an existing instance to the agent

If an instance is already added to the primary NetScaler Console, you can attach it to an agent by editing an agent.

1. Navigate to **Infrastructure > Instances** and select the instance type. For example, NetScaler.
2. Click **Edit** to edit an existing instance.
3. Click to select the agent.
4. From the **Agent** page, select the agent with which you want to associate the instance and then click **OK**.

   > **Note**
   >
   > Ensure to select the **Site** with which you want to associate the instance.

Access the GUI of an instance to validate events

After the instances are added and agent is configured, access the GUI of an instance to check if the trap destination is configured.

In NetScaler Console, navigate to **Infrastructure > Instances**. Under **Instances**, select the type of instance you want to access (for example, NetScaler VPX), and then click the IP address of a specific instance.

The GUI of the selected instance is displayed in a pop-up window.

By default, the agent is configured as the trap destination on the instance. To confirm, log on to the GUI of the instance and check the trap destinations.

> **Important**
>
> Adding an agent for NetScaler instances in remote data centers is recommended but not mandatory.
>
> In case you want to add the instance directly to the primary MAS, do not select **an agent** while adding instances.

NetScaler 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.

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

> **Important**
>
> - Ensure the **Agent Failover** feature is enabled on your account. To enable this feature, see Enable or disable NetScaler Console features.
> - If an agent is running a script, ensure that script is present on all the agents in the site. Therefore, the changed agent can run the script after agent failover.

To attach a site to an agent in the NetScaler Console GUI, see Attach an agent to a site.

To achieve an agent failover, select NetScaler agents one by one and attach to the same site.

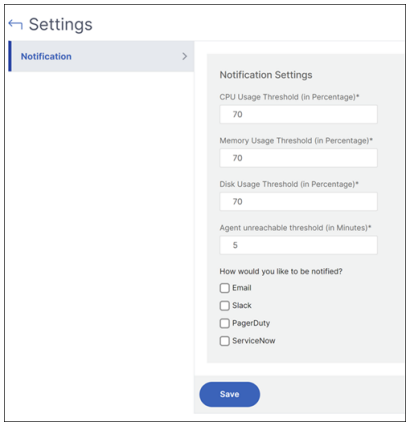
For example, two agents 10.106.1xx.2x and 10.106.1xx.3x are attached and operational in the Bangalore site. If one agent becomes inactive, NetScaler Console detects it and displays the state as down.

When a NetScaler agent becomes inactive (Down state) in a site, NetScaler Console waits for five 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.

NetScaler Console triggers instance redistribution every 30 minutes to balance the load among active agents in the site.

Configure agent unreachable threshold and notification

If an agent is down or not reachable for a certain duration, you can get notification on the agent status through email, slack, PagerDuty, and ServiceNow. In **Infrastructure > Instances > Agents**, click **Settings**, specify the duration between 5 minutes and 60 minutes, and select the notification method that you want to get notified.



Secure communication between NetScaler® Console agents and NetScaler Console

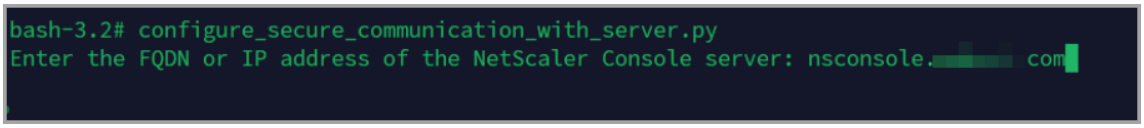
A secure communication between NetScaler Console agents and NetScaler Console is available for versions 14.1-34.x or later. You can enable this secure communication by verifying the Console server

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

SSL certificate. Previously, communication between NetScaler Console agents and the NetScaler Console on-prem server was not verifying the Console server SSL certificate, leading to potential security vulnerabilities.

To enable this secure communication:

1. Ensure that the Netscaler Console has SSL certificates configured.
2. Login to the NetScaler Console agent.
3. Place the CA root certificate at **/mpsconfig/console_onprem_cacert**. This is used to validate the server certificate. The name of the CA root certificate must be **cacert.pem**.
4. Configure the secure communication by running the following command. **Configure_secure_communication_with_server.py**
5. This prompts for FQDN(Fully Qualified Domain Name) or IP address of the Netscaler Console server.
6. Enter the FQDN or IP address to finish executing the script.



7. The script verifies the server certificate presented by an FQDN or IP address, using the provided CA root certificate. Secure communication is enabled if the certificate validation passes.
8. This script can be invoked either before or after the agent is registered with the NetScaler Console.

> **NOTE:**
>
> This is applicable for VM based agents only.

Install a NetScaler® agent as a microservice on a Kubernetes cluster

December 1, 2025

Deploying a NetScaler agent as a microservice is useful for managing your NetScaler CPX. The procedures available in this document are applicable only if the NetScaler Console and Kubernetes cluster are configured on a different network. In this scenario, you can configure an agent as a microservice, where the Kubernetes cluster is hosted.

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

> **Note:**
>
> - You can also configure an on-prem agent and register the agent on the network, where the Kubernetes cluster is hosted.
> - Starting from NetScaler Console release 14.1 build 60.x, NetScaler Console supports the use of containerized console agent for streamlined connectivity and monitoring of managed instances on Kubernetes or OpenShift platforms.

Get started

1. In NetScaler Console, navigate to **Infrastructure > Instances > Agents**.
2. From the **Select Action** list, select the **Download Agent Microservice** option.
3. In the **Download Agent Microservice** page, specify the following parameters:
   a) **Application ID** –A string id to define the service for the agent in the Kubernetes cluster and distinguish this agent from other agents in the same cluster.
   b) **Password** –Specify a password for CPX to use this password to onboard CPX to NetScaler Console through the agent.
   c) **Confirm Password** –Specify the same password for confirmation.

      > Note
      >
      > You must not use the default password (`nsroot`).

   d) Click **Download Yaml File**.

Install NetScaler agent in Kubernetes cluster

In the Kubernetes main 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.

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

```
root@[redacted]:/# kubectl create -f testing.yaml
deployment.apps/testing created
service/testing created
secret/testing created
configmap/testing created
root@[redacted]:/#
```

In NetScaler Console, navigate to **Infrastructure > Instances > Agents** to see the agent status.

After you configure the agent, you can add the NetScaler CPX instances and view analytics in service graph. For more information, see:

- Adding NetScaler CPX Instances to NetScaler Console.
- Setting up service graph.

Upgrade agents

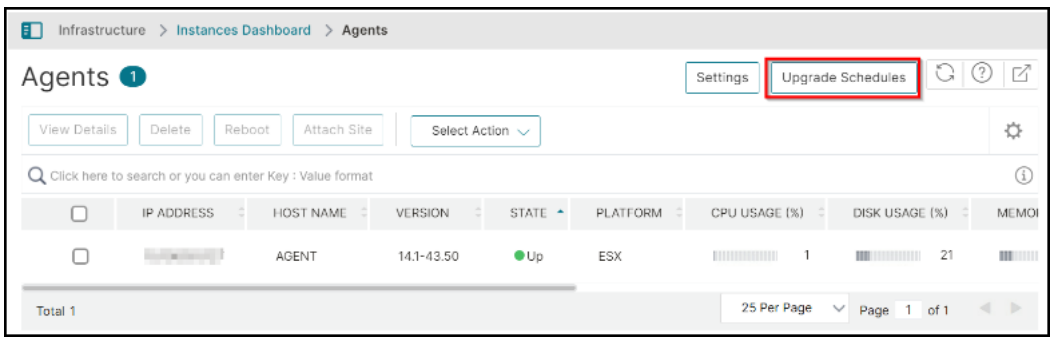
December 22, 2025

> **Note:**
>
> Ensure that the agent version is 14.1-38.x or later.

Starting 14.1–43.50, you can upgrade NetScaler agents (14.1-38.x or later) through the NetScaler Console GUI. This enhancement eliminates the manual upgrade workflow for each agent and enables you to upgrade all agents in a single workflow or schedule upgrades for a later time.

Upgrade workflow

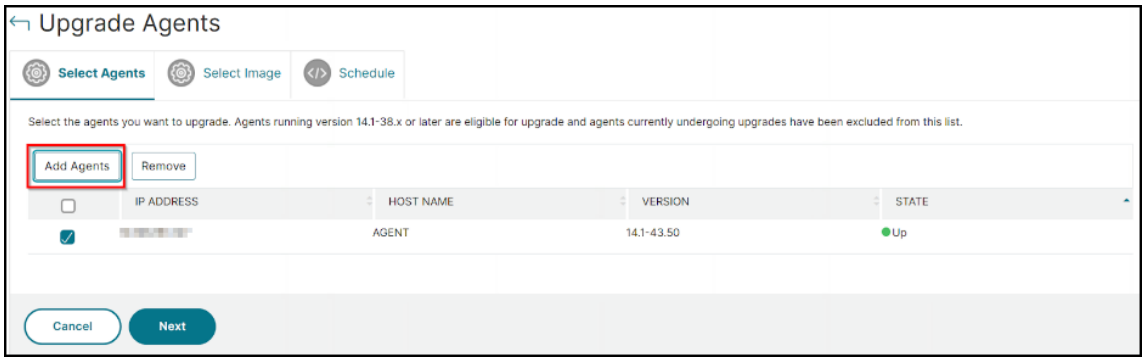
1. Navigate to **Infrastructure > Instances > Agents**.
2. Click **Upgrade Schedules**.



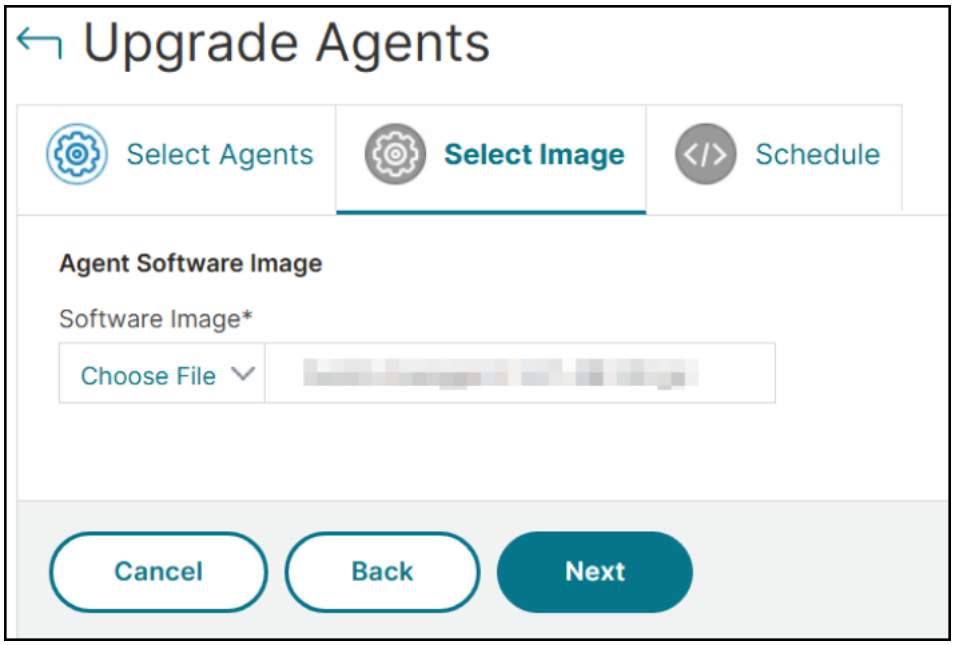
© 1997–2025 Citrix Systems, Inc. All rights reserved.

3. In the **Upgrade Schedules** page, click **Add**.
4. Click **Add Agents**, select the agents from the list that you want to upgrade, and click **Next**.

> **Note:**
>
> Agents that are running build 14.1-38.x or later only are displayed.

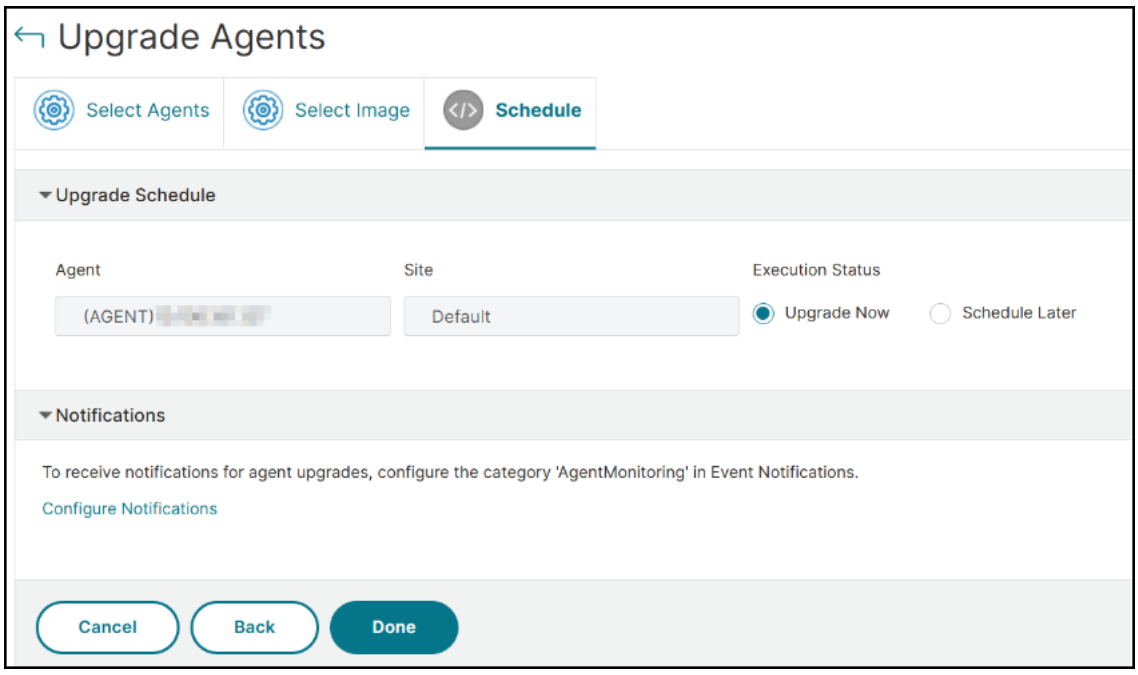


5. In the **Select Image** tab, select an image (.tgz) from local or appliance. You can upload the image from your local computer or the appliance. When you select **Appliance**, the NetScaler Console GUI displays the images that are present in `/var/mps/mas_agent_images`. Select an image from the list.

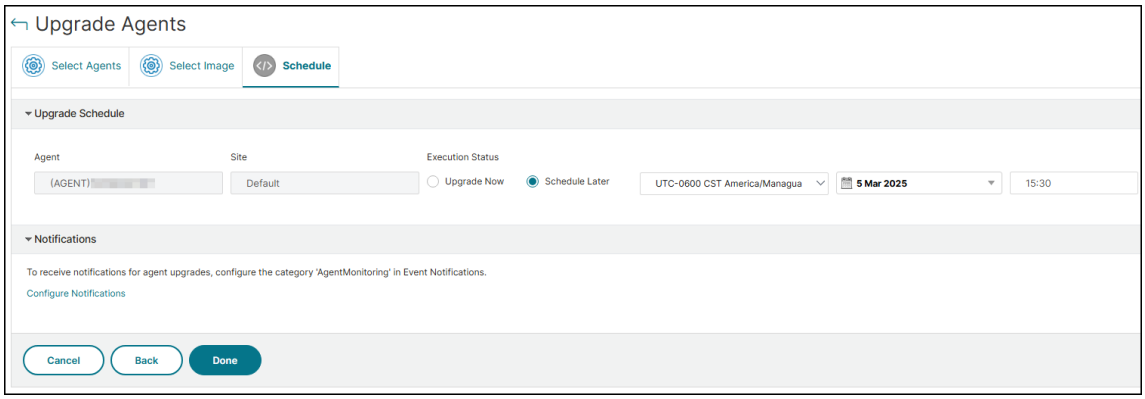


6. After selecting the image, click **Next**.
7. Under **Upgrade Schedule**, select **Upgrade Now** to upgrade immediately.

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



If you want to schedule an upgrade, select **Schedule Later** and then provide details by selecting the time zone, date, and time (24 hours format).



8. If you want to get notified for the upgrade workflow, click **Configure Notifications** under **Notifications**, select the category `AgentMonitoring`, and select the communication options (Email, SMS, Slack, PagerDuty, and ServiceNow) that you want to get notified.
9. Click **Done**.

Migrate NetScaler Console single-server deployment to a high availability deployment

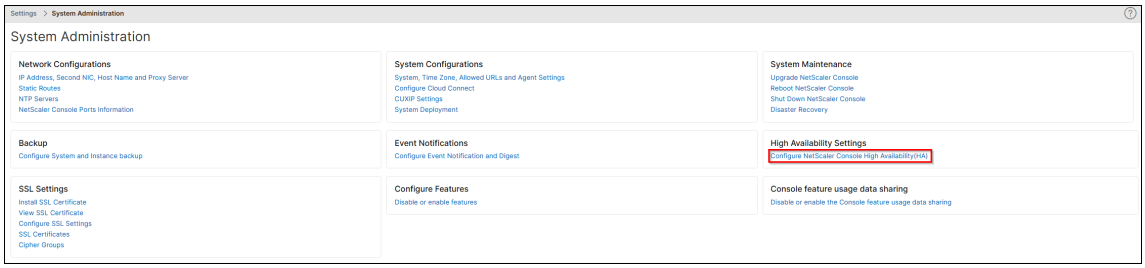
September 27, 2025

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

You can upgrade your NetScaler Console single server to a high availability deployment of two NetScaler Console servers. A high availability pair of NetScaler Console servers is in active-passive mode, and both the servers have the same configuration. In this type of active-passive deployment, one NetScaler Console server is configured as the primary node and the other as the secondary node. If for any reason, the primary node goes down, the secondary node takes over. For more information, see Configure high availability deployment.

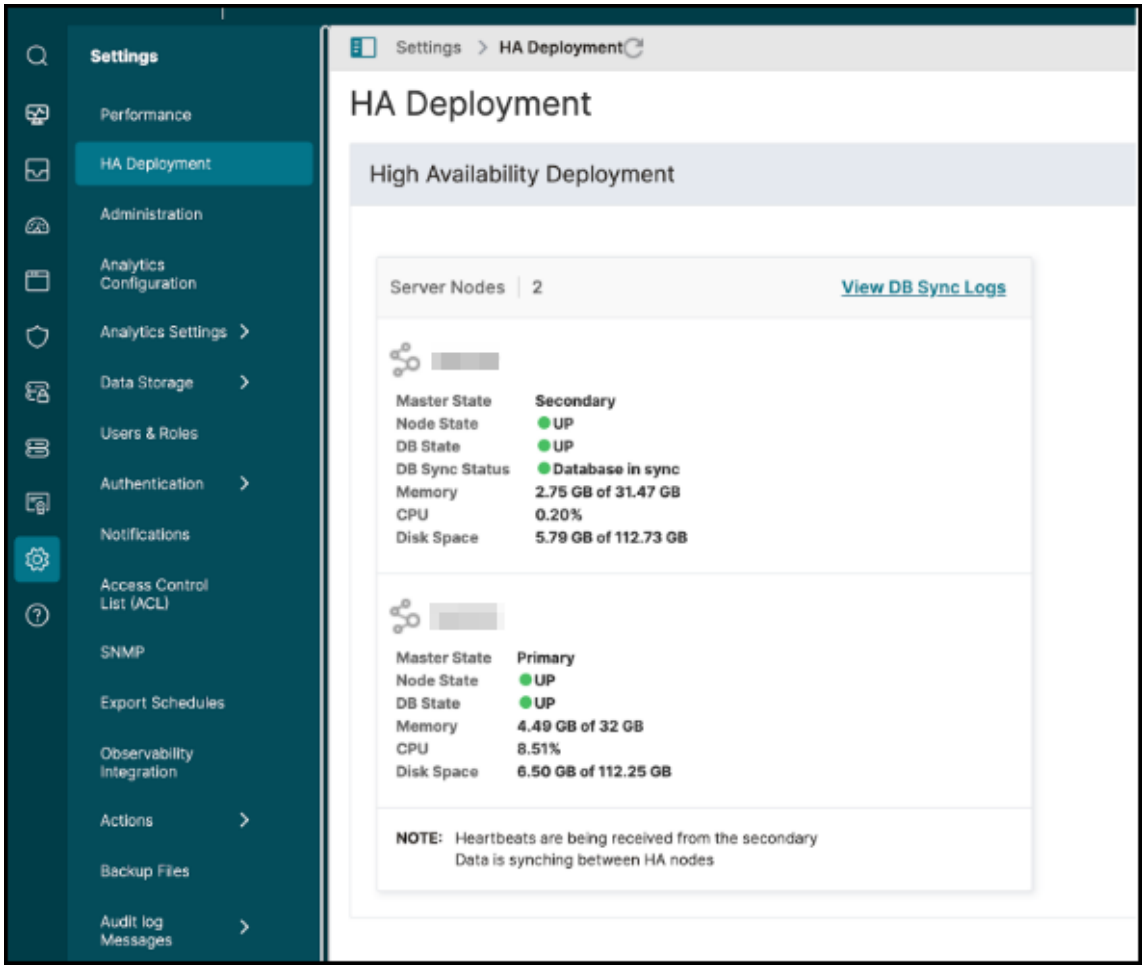
To migrate a NetScaler Console single server to a high availability pair, you must:

1. Log on to the single NetScaler Console server.
2. Navigate to **Settings > Administration** and click **Configure NetScaler® Console High Availability (HA)** under **High Availability Settings**.



3. In the **Configure NetScaler Console High Availability (HA)** page:
   a) Provide a secondary NetScaler Console server IP address.
   b) Specify the secondary node password.
   c) Specify the floating IP address.
   d) Click **Configure**.
4. In the confirmation window, click **Yes**. NetScaler Console instances reboot to form a HA pair.
5. After the HA pair configuration is complete, login to the primary NetScaler Console and navigate to **Settings > HA Deployment** to validate the primary and secondary nodes.

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



Migrate from NetScaler Insight Center to NetScaler Console

September 27, 2025

You can now migrate your NetScaler Insight Center deployment to NetScaler Console without losing the existing configuration, settings, or data. With NetScaler Console you can not only view the various analytics generated by the NetScaler instances associated with an application, but can also manage, monitor, and troubleshoot the entire global application delivery infrastructure from a single, unified console.

> **Note**
>
> Migration is currently supported only on NetScaler® Insight Center Standalone instances.

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

Prerequisites

Before migrating the NetScaler Insight Center virtual appliance to NetScaler Console, verify that the following requirements have been met:

- NetScaler Insight Center 11.1 Build 47.14 or later is installed.
- You have downloaded the NetScaler Console 12.0 build 57.24 .tgz image file.

  > **Note**
  >
  > You must install NetScaler Console 12.0 build 57.24 and then upgrade to the latest NetScaler Console 13.1 build. For more information, see Upgrade.

- You have downloaded the NetScaler Console 13.1 latest build .tgz image file.

Hardware requirement

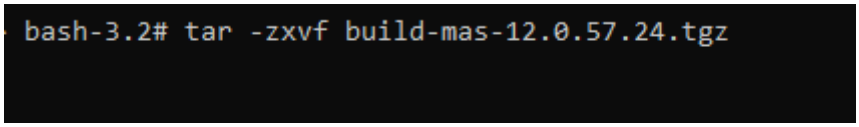
Component	Requirement
RAM	32 GB
Virtual CPU	8 CPUs
Storage space	120 GB **Note** We recommend that you use **500 GB** for better performance. Also, Citrix recommends using solid-state drive (SSD) technology for NetScaler Console deployments.
Virtual Network Interfaces	1
Throughput	1 Gbps or 100 Mbps
Hypervisor Requirements	
Citrix Hypervisor	6.2, 6.5
VMware ESX	5.5, 6.0
Microsoft Hyper-V	2012 R2
Linux - KVM	Ubuntu, Fedora

Installation procedure

To migrate NetScaler Insight Center to NetScaler Console:

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

1. Log on to the shell prompt of NetScaler Insight Center.
2. Download the NetScaler Console 12.0 build 57.24 to the */var/mps/mps_images* folder.
3. Untar the TGZ file by using the **tar -zxvf build-mas-12.0-57.24.tgz** command.



4. Install NetScaler Console by using the **./installmas** command.



5. After installing NetScaler Console 12.0 build 57.24, you need to upgrade to the latest NetScaler Console 13.1 build by performing the above steps.

After the migration, all the NetScaler instances that were discovered in the NetScaler Insight Center inventory appear in the **Infrasturcture > Instances** section of NetScaler Console. However, for the first time you need to manually poll the virtual servers hosted in the discovered appliances.

> **Note**
>
> In NetScaler Console, by default, there is no licensing cost to manage and monitor two virtual servers created within the discovered NetScaler instances. To monitor and manage more than two virtual servers, install the required NetScaler Console licenses. For more details, see NetScaler Console Licensing.

Integrate NetScaler Console with Citrix Director

September 27, 2025

Director integrates with NetScaler Console for network analysis and performance management.

- Network analysis obtains HDX Insight reports from NetScaler Console and provides an application and desktop view of the network. With this feature, Director provides an advanced analytics view of ICA traffic in your deployment.
- Performance management provides historical retention and trend reporting. With historical retention of data versus the real-time assessment, you can create Trend reports, including capacity and health trending.

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

After you integrate NetScaler Console with Director, HDX Insight reports provide you with the following information in Director:

- The Network tab in the Trends page shows latency and bandwidth effects for applications, desktops, and users across your deployment.
- The User Details page shows latency and bandwidth information specific to a particular user session.

Prerequisites

Hardware requirements for HDX Insight to NetScaler Console Migration

Component	Requirement
RAM	32 GB
Virtual CPU	8
Storage Space	500 GB. We recommend using solid-state drive (SSD) technology for NetScaler Console deployments.
Virtual Network Interfaces	1
Throughput	1 Gbps or 100 Mbps

Minimal requirements

Before you configure the network integration, ensure that you create an RBAC user with HDX™ Insights access.

Software requirements

Before migrating to the NetScaler Console virtual appliance, verify that the following requirements have been met:

- Director version 1811 is installed
- NetScaler HDX Insight version 10.1 or later is installed
- HDX Insight and NetScaler Console support Citrix VDA version 7.0 and later
- Citrix Workspace is supported on Citrix Virtual Apps and Desktops version 7.0 and later

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

- Ensure that MAC Citrix Workspace for Mac version 11.8 and later, and Windows Citrix Workspace for Windows 14.0 and later are available to display accurate ICA RTT metrics
- NetScaler Console version 11.0 and later is installed. For more information on how to install NetScaler Console, see Deploy NetScaler Console.

Limitations

- The availability of this feature depends on your organization's license and your administrator permissions.
- ICA session Round Trip Time (RTT) shows data correctly for Citrix Workspace for Windows 3.4 or later and for Citrix Workspace for Mac 11.8 or later. For earlier versions of these Workspaces, the data does not display correctly.
- In the Trends view, HDX connection logon data is not collected for VDAs earlier than version 7. For earlier VDAs, the chart data is displayed as 0.
- For deployments that already have an external hard disk with storage space less than 500 GB, you cannot add another hard disk.

> **Note**
>
> - For more information on Director and for steps to integrate NetScaler Console with Director, see https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/director/install-and-configure/hdx-insight.html.
> - For more information on HDX Insight, see http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-11/director/hdx-insight.html.

Attach an extra disk to NetScaler Console

September 27, 2025

NetScaler Console storage requirement is determined based on your NetScaler Console sizing estimation. By default, NetScaler Console provides you a storage capacity of 120 GB. If you need more than 120 GB for storing your data, you can attach an extra disk.

> **Note:**
>
> - Estimate storage requirements and attach an extra disk to the server.
> - For a NetScaler Console single-server deployment, you can attach only one disk to the

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

> server in addition to the default disk.
>
> - For a NetScaler Console high availability deployment, you must attach an extra disk to each node. The size of both disks must be the same.
> - If there is an existing external disk of lower capacity, you must remove the disk before attaching a new disk.
> - We recommend using solid-state drive (SSD) technology for NetScaler Console deployments.

This document explains the following scenarios about attaching an extra, new disk, creating partitions, and resizing the additional disks:

1. Attach an extra disk in a standalone NetScaler Console
2. Launch the disk partition tool
3. Create partitions in the new additional disk
4. Resize the partitions in the existing additional disk
5. Remove the partitions in the additional disk

Attach an extra disk in a standalone NetScaler Console

1. Shut down the NetScaler Console virtual machine.
2. In the hypervisor, attach an extra disk of the required disk size to the NetScaler Console virtual machine.

   The newly attached larger disk stores the database data and NetScaler Console log files. The existing default disk of 120 gigabytes is now used to store the core files, operating system log files, and so on.
3. Start the NetScaler Console virtual machine.

Launch the disk partition tool

NetScaler Console now provides **NetScaler Console disk partition tool**, a new command line tool.

1. Using the tool, you can create partitions in the newly added extra disk.
2. You can also resize the existing extra disks using the tool. But the existing external disk must not be greater than 2 terabytes.

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

> **Note:**
>
> - Resizing existing disks beyond 2 terabytes might cause data loss. This is because of a known limitation on the platform.
> - To create a storage capacity greater than 2 terabytes, you must remove the existing partitions and create partitions using this new tool.

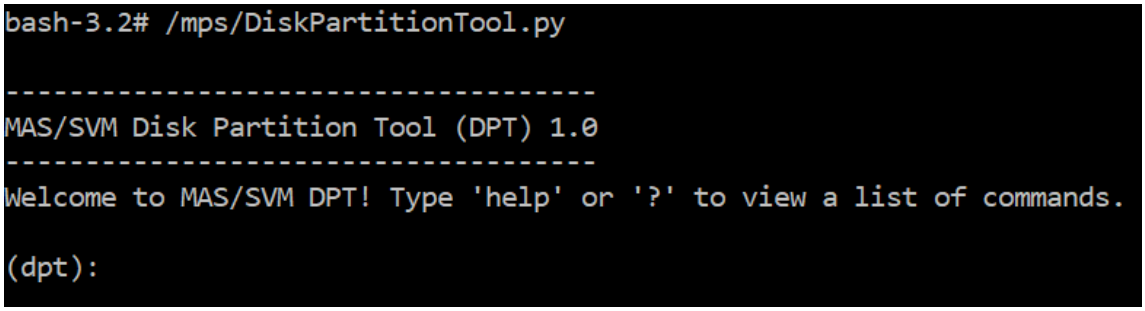
3. Using this new tool, you can do any partition action on the disk explicitly. The tool provides you with clear visibility and control over the disk and the associated data.

> **Note:**
>
> You can only use this tool on the additional disk that you have attached to the NetScaler Console server. You cannot create partitions in the primary (default) disk using this tool.

To launch the disk partition tool:

1. Open an SSH connection to the NetScaler Console by using an SSH client, such as PuTTY.
2. Log on to the NetScaler Console by using the `nsrecover`/`nsroot` credentials.
3. Switch to the shell prompt and type:

```
1 /mps/DiskPartitionTool.py
```



> **Note:**
>
> For NetScaler Console in high availability deployment, you must launch the tool in both nodes and create or resize partitions after attaching disks to the respective virtual machines.

Create partitions in the new additional disk

The **create** command is used to create partitions whenever a new secondary disk is added. You can also use this command to create partitions on an existing secondary disk after the existing partitions are deleted using the “remove”command.

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

```
(dpt): ?create
Creates a new partition on the attached disk. A swap partition of size 32GB is also created automatically.

The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

> **Note:**
>
> There is no 2 terabytes size limitation while creating partitions with the disk partition tool. The tool can create partitions larger than 2 terabytes. When you partition the disk, a swap partition of size 32 GB is automatically added. The primary partition then uses all the remaining space on the disk.

Once the command is run, a GUID partition table (GPT) partition scheme is created. Also a 32 GB swap partition and data partition are created to use rest of the space. A new file system is then created on the primary partition.

> **Note:**
>
> This process can take a few seconds, and you must not interrupt the process.

```
(dpt): create

The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to continue (Y/N): y
```

```
Creating GPT partition scheme...
da1 created

Creating partition 1 using (456287933) blocks. Leaving aside 32G for swap...
da1p1 added

Creating partition 2 for swap using remaining 32G...
da1p2 added

Formatting the new partition. This may take some time (~20 seconds). Please be patient and don't interrup the process...
```

Once the create command completes, the virtual machine is automatically restarted for the new partition to get mounted.

```
Create Done.
VM has to be rebooted for the new partition to be used.
Rebooting VM now...

*** FINAL System shutdown message from nsroot@ns-mgmt-system ***

System going down IMMEDIATELY
```

After the restart, the new partition is mounted at /var/mps.

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

```
bash-3.2# df -k
Filesystem  1024-blocks     Used     Avail Capacity  Mounted on
/dev/md0         456046   374346     72580    84%    /
devfs                 1        1         0   100%    /dev
procfs                4        4         0   100%    /proc
fdescfs               1        1         0   100%    /dev/fd
/dev/da0s1a     1623950   284466   1209568    19%    /flash
/dev/da0s1e   116073918 2812298 103975708     3%    /var
/dev/da1p1    495168802   43854 455511444     0%    /var/mps
```

The swap partition added shows up as swap space in the output of the “create”command.

```
CPU:  0.0% user,  0.0% nice,  0.0% system,  0.7% interrupt, 99.3% idle
Mem: 89M Active, 21M Inact, 123M Wired, 16M Cache, 74M Buf, 6965M Free
Swap: 37G Total, 37G Free
```

> **Note:**
>
> The tool restarts the virtual machine after the partition is created.

Resize the partitions in the existing additional disk

You can use the **resize** command to resize the attached (secondary) disk. You can resize a disk that has a `master boot record` (`MBR`) or GPT scheme. The size of the disk must be less than 2 terabytes in size.

> **Note:**
>
> - The `resize` command is designed to function without losing any existing data. But we recommend that you back up critical data in this disk to external storage before resizing. Data backup is helpful in cases where the disk data can get corrupted during the resize operation.
> - Make sure you increase the disk space in increments of 100 GB of space while resizing the partitions. An incremental increase of this kind ensures that you won’t have to resize more frequently.

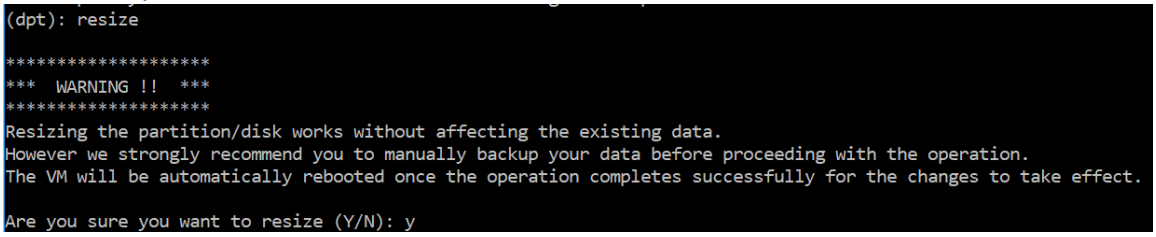
```
(dpt): ?resize
Resizes existing partition on attached disk to utilize all space available. Pre-conditions are:
1. Secondary disk exists and capcity of disk < 2TB
2. A single partition exists on secondary disk and there is atleast 100GB to gain by resizing

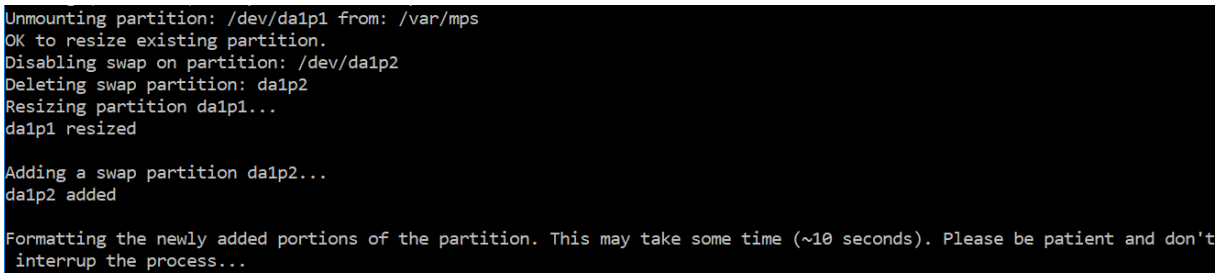
********************
***  WARNING !!  ***
********************
Resizing the partition/disk works without affecting the existing data.
However we strongly recommend you to manually backup your data before proceeding with the operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

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

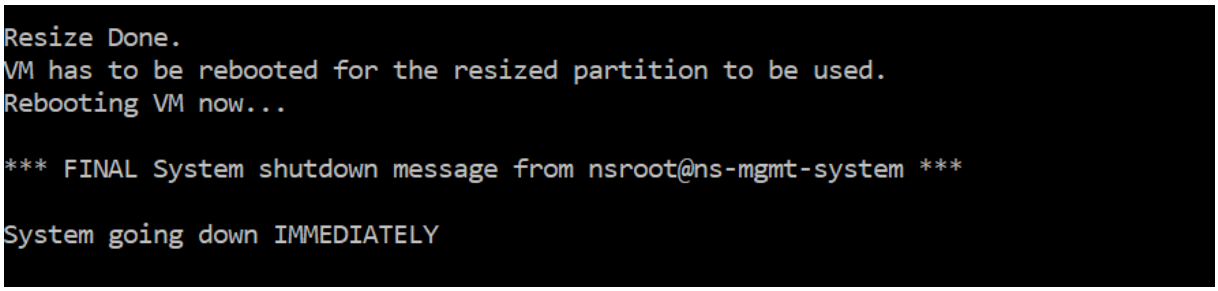
The `resize` command checks for all preconditions and proceeds if all preconditions are met and after you have given consent to resizing. It stops the processes accessing the disk, which includes the NetScaler Console subsystems, PostgreSQL DB processes, and the NetScaler Console monitor process. Once the processes are stopped, the disk is unmounted to prepare it for resizing. The resizing is done by extending the partition to occupy the complete available space and then growing the file system. If a swap partition exists on the disk, it is deleted and recreated at the end of the disk after resizing. The swap partition is discussed in the **Create** command section of the document.

> **Note:**
>
> The "growing file system"process can take some to complete and take care that you do not interrupt the process while it is in progress. The tool restarts the virtual machine after you have resized the partition.





All the intermediate steps in the resize process (stopping applications, resizing disk, growing filesystem) are shown on the console. Once the process completes, the following message is seen.



After rebooting, the increase in size can be observed using the `df` command. Here's the before and after details when you increase the size:

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

```
bash-3.2# df -k
Filesystem  1024-blocks    Used     Avail Capacity  Mounted on
/dev/md0         456046  374864     72062    84%    /
devfs                 1       1         0   100%    /dev
procfs                4       4         0   100%    /proc
fdescfs               1       1         0   100%    /dev/fd
/dev/da0s1a     1623950  284468   1209566    19%    /flash
/dev/da0s1e   116073918 1662048 105125958     2%    /var
/dev/da1s1a   152329216 3082226 137060654     2%    /var/mps
```

```
bash-3.2# df -k
Filesystem  1024-blocks    Used     Avail Capacity  Mounted on
/dev/md0         456046  374838     72088    84%    /
devfs                 1       1         0   100%    /dev
procfs                4       4         0   100%    /proc
fdescfs               1       1         0   100%    /dev/fd
/dev/da0s1a     1623950  284468   1209566    19%    /flash
/dev/da0s1e   116073918 1666800 105121206     2%    /var
/dev/da1s1a   304651668 3137954 277141582     1%    /var/mps
```

Remove the partitions in the additional disk

An existing partition on the secondary disk can be resized up to 2 terabytes. This issue is because of a known limitation on the partition. If you want a disk larger than 2 terabytes, either attach a new disk and partition it by using the disk partition tool. You can also remove the existing partition by using the `remove` command, and then create a partition.

> **Note:**
>
> Removing the existing partition deletes all existing data. So, any critical data must be backed up to external storage before using this command.

```
(dpt): ?remove
Removes existing partition from attached disk.

********************
***  WARNING !!  ***
********************
All data on the partition/disk will be PERMANENTLY ERASED as a result of this operation.
Backup the data before proceeding with this operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

Running the “remove”command asks you for confirmation and once confirmed, it stops all processes (such as NetScaler Console subsystems, PostgreSQL processes, and NetScaler Console monitors) using the secondary disk. If a swap partition exists and swap is enabled on the partition, then the swap is disabled.

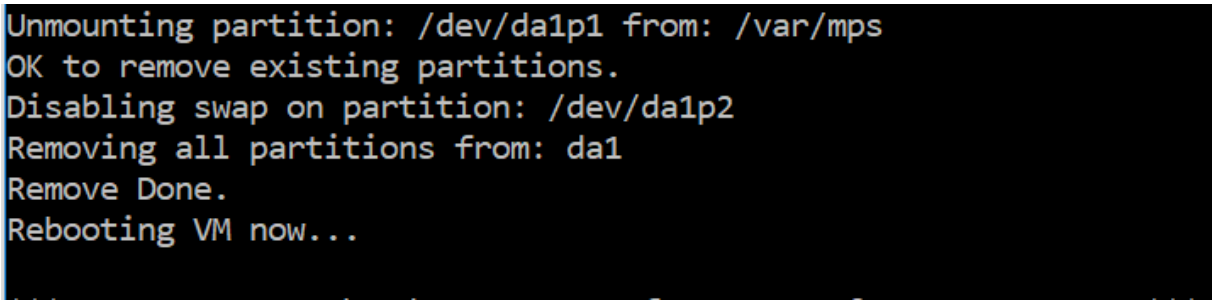
```
(dpt): remove

********************
***  WARNING !!  ***
********************
All data on the partition/disk will be PERMANENTLY ERASED as a result of this operation.
Backup the data before proceeding with this operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to continue (Y/N): y
```

When you type “y,”the command unmounts the disk and removes all partitions on the disk.

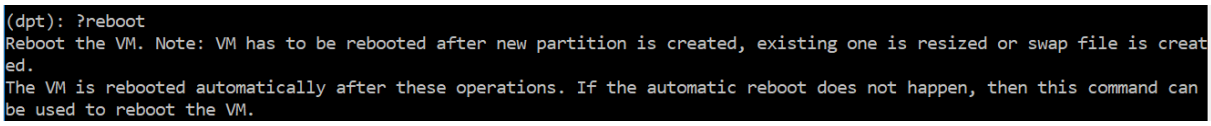
© 1997–2025 Citrix Systems, Inc. All rights reserved.



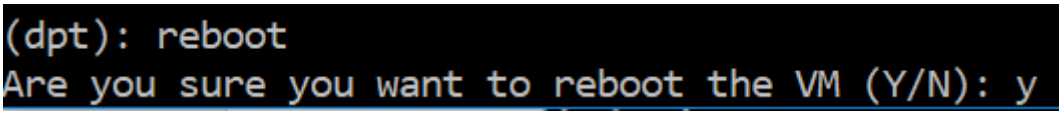
> **Note:**
>
> The tool restarts the virtual machine after you have removed the partition.

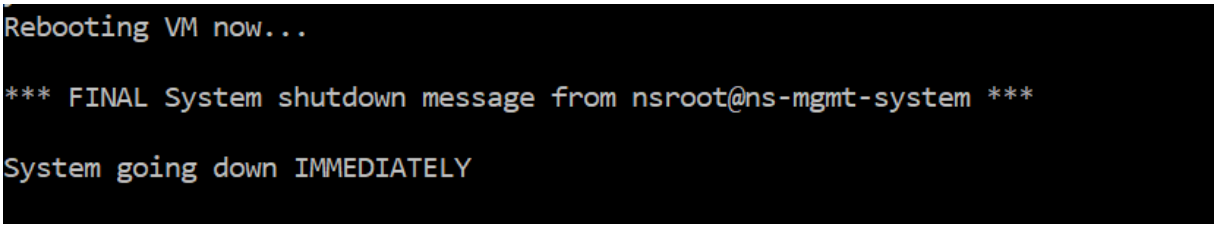
Restart the virtual machine

When a partition is created or resized, or when a swap file is created, restart the virtual machine. The changes take effect only after restarting. For this purpose, a **reboot** command is provided in the tool.



You are prompted for confirmation and after confirmation, all processes (such as NetScaler Console subsystems, PostgreSQL processes, and NetScaler Console monitors) are stopped. The virtual machine is then restarted.





Create a backup file of the disk data

> **Note:**
>
> Creating a backup file requires disk space. Make sure there is sufficient disk space (50% or more) before the backup commands are run.

To back up the NetScaler Console data before resizing or removing the partitions:

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

1. Stop NetScaler Console.

```
/mps/masd stop
```

2. Stop PostgreSQL.

```
su -l mpspostgres /mps/scripts/pgsql/stoppgsql_smart.sh
```

3. Stop NetScaler Console Monitor.

```
/mps/scripts/stop_mas_monit.sh
```

4. Create a tarball.

```
cd /var
tar cvfz /var/mps/mps_backup.tgz mps
```

> **Note:**
>
> The operation takes time depending on the size of the data to be backed up.

5. Generate a checksum.

```
md5 /var/mps/mps_backup.tgz > /var/mps/mps_backup_checksum
```

6. Copy the tarball and checksum files to a remote server.
7. Validate the correctness of the copied tarball. Generate a checksum of the transferred file and compare with the source checksum.
8. Remove the tarball from the NetScaler Console virtual machine.

```
cd /var/mps/
rm mps_backup.tgz  mps_backup_checksum
```

Additional commands

In addition to the commands listed earlier, you can also use the following commands in the tool:

Help command:

To list the supported commands, type **help** or **?** and press enter. To get further help on each of the commands press **help** or **?** followed by the command name and press the **Enter** key.

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

```
(dpt): help

DPT Commands
------------
create  create_swapfile  exit  help  info  reboot  remove  resize

(dpt):
```

Info command:

The **info** command provides information about the attached secondary disk if the disk exists. The command provides the device name, the partition scheme, size in human-readable form, and the number of disk blocks. The scheme can be MBR or GPT. An MBR scheme means that the disk was partitioned using an earlier version of NetScaler Console version. The MBR/GPT based partition can be resized but not beyond 2 terabytes. The GPT partition scheme means that the disk was partitioned using NetScaler Console 12.1 or later.

> **Note:**
>
> A GPT partition can be greater than 2 terabytes but when it is created. But you cannot resize the disk to a size greater than 2 terabytes after creating a disk with a smaller size. This issue is a known limitation of the platform.

```
(dpt): ?info
Provides information about attached disk (if found).
(dpt): info
--------------
Disk: da1
Scheme: MBR
Size: (150G)
Blocks: 314572737
--------------
(dpt):
```

Create_swapfile command:

The default swap partition on the primary disk of NetScaler Console is 4 GB and so, the default swap space is 4 GB. For the default memory configuration of NetScaler Console which is 2 GB, this swap space is sufficient. However, when you run NetScaler Console with a higher memory configuration, you need to have more swap space allocated on the disk.

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

> **Note:**
>
> Swap partition is usually a dedicated partition that is created on a hard disk drive (HDD) during the installation of the operating system. Such a partition is also referred to as a swap space. A swap partition is used for virtual memory that simulates the additional main memory.

Secondary disks that were added in the earlier versions of NetScaler Console do not have a swap partition created by default. The "create_swapfile"command is meant for secondary disks created using older NetScaler Console versions which don't have a swap partition. The command checks for the following:

- Presence of a secondary disk
- Disk being mounted
- Size of the disk (at least 500 GB)
- The existence of the swap file

The `create_swapfile` command is useful only when the memory is greater or equal to 16 GB and not when memory is low. So, this command also checks for memory before proceeding with swap file creation.

```
(dpt): ?create_swapfile
Creates a 32GB swap file on the secondary disk. Pre-conditions are:
1. Secondary disk exists
2. Secondary disk is partitioned and mounted
3. Capacity of disk >= 500GB
4. Swap file is not already found
5. RAM size >= 16GB

Creating swapfile is a time consuming operation and can take ~5 minutes to complete. Once started the operation should n
ot be interrupted.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

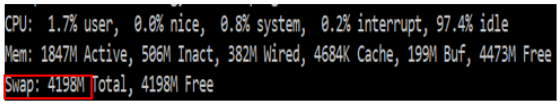
If all the conditions are met, and the user consents to continue, a 32 GB swap file is created on the secondary disk. The swap file creation process takes a few minutes to complete and take care that you do not interrupt the process while in progress. After successful completion, a restart is done for the swap file to take effect.

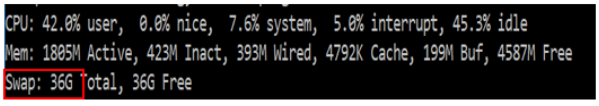
```
Creating swapfile. This may take some time (~5 mins). Please be patient and don't interrupt the process...
32768+0 records in
32768+0 records out
34359738368 bytes transferred in 724.061475 secs (47454173 bytes/sec)

Changing permissions for created swapfile...

Create (swapfile) Done.
VM has to be rebooted for the newly created swapfile to take effect.
```

After reboot, the increase in swap can be observed using the top command.





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

Exit command:

To exit from the tool, type exit and press the **Enter** key.

```
(dpt): exit
bash-3.2#
```

Attach additional disks to NetScaler Console deployed in high availability

Consider you have configured a pair of NetScaler Console servers in a high availability set up without any secondary disks. Also, consider you have added 2 or more NetScaler instances, checked and ensured all processes are running. You might want to add secondary disks to the virtual machines in this setup. In a high availability set up, you must add additional disks to both nodes as detailed in this task:

1. Shut down the secondary node.
2. Add a disk through the hypervisor.

   > **Note:**
   >
   > Make sure not to extend the secondary node main disk.

3. Start the secondary node.
4. Run the partition tool on the secondary node.
5. After the disk is added, the secondary node restarts.
6. Shut down the secondary node after it restarts.
7. Shut down the primary node.
8. Add a disk through the hypervisor.

   > **Note:**
   >
   > Make sure not to extend the primary node main disk.

9. Start the primary node.
10. Run the partition tool on the primary node.
11. After the disk is added, the primary node restarts.
12. After the primary node is up and running, start the secondary node.
13. Make sure that the secondary node is up and running and the databases have synchronized.

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

14. Confirm that all data still exists.

To increase the capacity of RAM on both the nodes:

1. Shutdown Console_Secondary and increase the RAM size as required. Don't restart the node.
2. Shutdown Console_Primary and increase the RAM size as required.

   Make sure that you increase the RAM size equally on both nodes. For example, if you increase the RAM size on the primary node to 16 GB, do the same on the secondary node as well.
3. Restart the Console_Primary.
4. After the Console_Primary reboots, check if it is the primary node.
5. Start the Console_Secondary node. After it restarts, make sure that it has come up as secondary and the DB sync is working.
6. Confirm that all data still exists.

   > **Note:**
   >
   > After you add the secondary disk, the primary node takes some time to come up. Also, the entire process of adding secondary disks to both nodes and increasing RAM capacity requires both nodes to be down for some time. Consider this downtime while planning this maintenance activity.

NetScaler MPX™ disk encryption through NetScaler Console

October 17, 2025

> **Notes:**
>
> - Disk encryption is supported only on NetScaler MPX 9100 instances.
> - Disk encryption for NetScaler MPX 9100 instances can be enabled only in standalone NetScaler Console.
> - Starting from release 14.1-56.x, disk encryption is supported on NetScaler MPX 9100, 16000, and MPX 15000-50G instances manufactured after May 20, 2025.

Disk encryption is essential for securing sensitive data stored on a storage disk. It ensures that even if the physical storage device is compromised, the data remains inaccessible. For NetScaler MPX, disk encryption provides an additional layer of security, especially for critical directories such as `/var/core`, `/var/crash`, `/var/log`, `/var/nslog`, `/flash/nsconfig`, `/var/nstrace`, and `/var/temp`.

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

Some of the benefits of disk encryption are:

- **Data Protection at Rest**: Prevents unauthorized access to sensitive data when the system is powered off.
- **Compliance**: Helps meet regulatory and compliance requirements for data security.
- **Mitigation of Physical Theft Risks**: Ensures that the sensitive and proprietary data on stolen or misplaced storage devices cannot be accessed.
- **Secure Boot Process**: Requires authenticated credentials during boot-up, ensuring only authorized users can access the system.
- **Enhanced Security for Critical Data**: Protects logs, configurations, and crash data from unauthorized access.

The disk encryption on NetScaler MPX 9100 is supported only in build 14.1-47.x shipped after **May 20, 2025** and can be enabled through NetScaler Console running build 14.1-47.x. The disk encryption of each NetScaler MPX instance requires a key that is managed by the Hardware Security Module (HSM) server, which is the Thales CipherTrust Manager. NetScaler MPX instances use NetScaler Console to fetch the key from the HSM server.

The disk encryption on NetScaler MPX 9100, 16000,and MPX 15000-50G is supported only in build 14.1-56.x shipped before **May 20, 2025** and can be enabled through NetScaler Console running build 14.1-56.x. To enable the feature, see Instance disk encryption through NetScaler Console.

> **Note:**
>
> NetScaler Console supports Thales CipherTrust Manager as the HSM server.

For successful encryption, you must add the NetScaler MPX instance serial number in the HSM server. After adding the NetScaler MPX instance serial number, NetScaler Console fetches the key using the instance serial number from the HSM server.

After the disk encryption is complete:

- If the NetScaler MPX instance disk is removed, the data is not accessible.
- If you reboot the NetScaler MPX instance, the reboot is successful only after NetScaler Console authenticates the NetScaler MPX instance using its serial number from the HSM server.

Prerequisites

Ensure that:

- For 9100, the NetScaler MPX instances are running build 14.1-47.x and are managed on NetScaler Console on-premises running build 14.1-47.x.

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

> **Note:**
>
> Disk Encryption is not supported on NetScaler Console service.

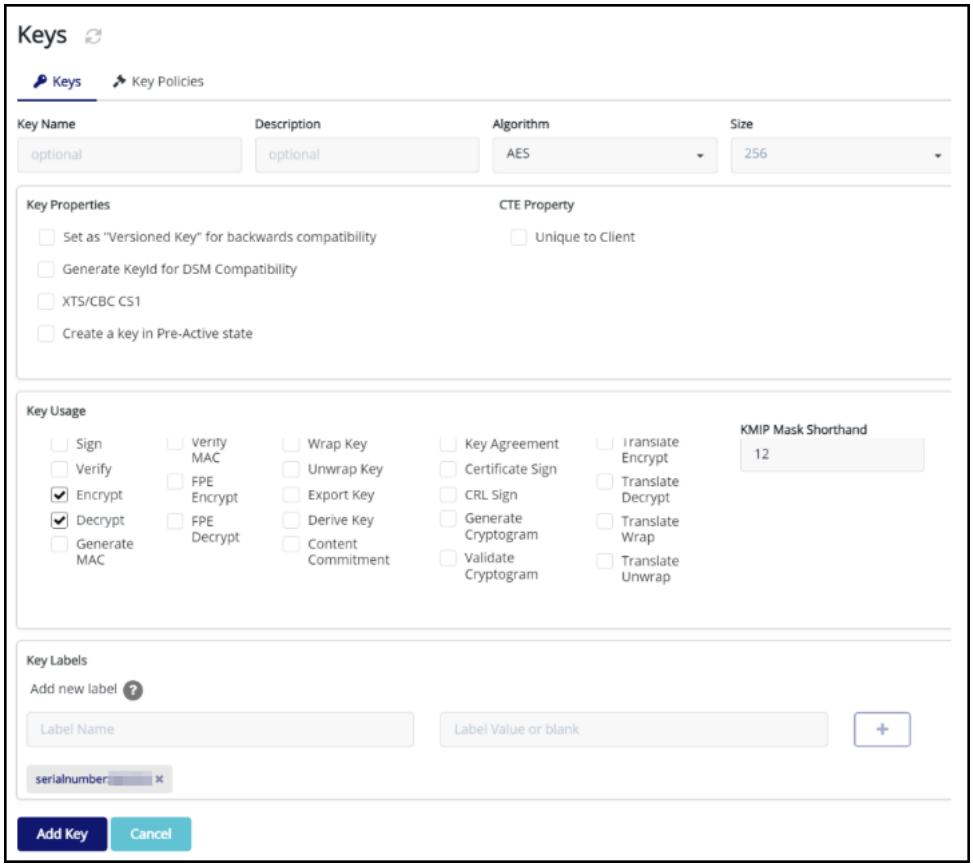
- You have added the NetScaler MPX instance serial number in the HSM (Thales CipherTrust Manager) server for NetScaler Console to share the key after authenticating the instance using its serial number.
- The NetScaler MPX instance is backed up through NetScaler Console. For more information, see Backup and restore NetScaler instances.
- For MPX 16000 and MPX 15000-50G, NetScaler Console on-premises is on release 14.1 build 56.x.

Add the instance serial number in the HSM (Thales CipherTrust Manager) server

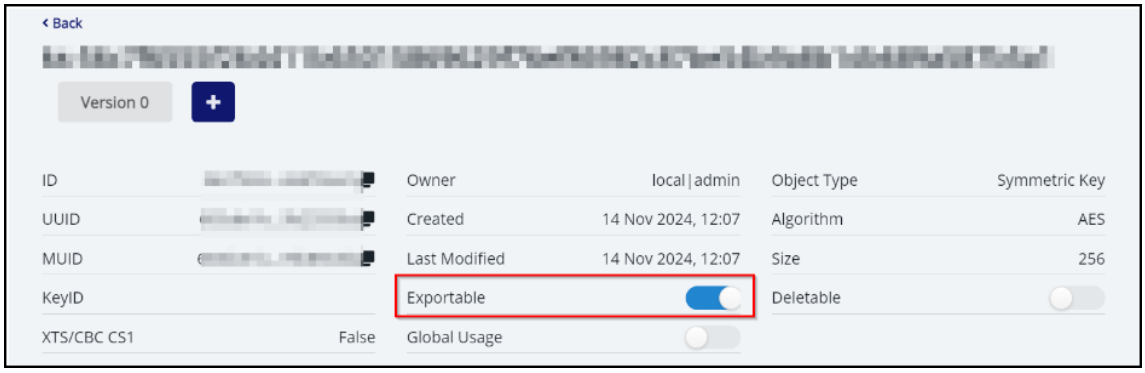
Before you encrypt the NetScaler MPX instance, you must add the NetScaler MPX instance serial number in the HSM server.

1. Log on to the Thales CipherTrust Manager server.
2. In the left pane, select **Keys** and click **Add Key**.
3. Under **Key Labels**, add a label with the name `serialnumber`, specify the instance serial number in the **Label Value** text box, click the **+** button to add the key details, and then click **Add Key**.

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



4. In the key details page, you must enable the Exportable toggle for this key.



Notes:

- The maximum supported key size is 511 bytes. For example: AES-128 and AES-256 are supported. RSA keys between 512 and 4096 are not supported.
- We recommend that you use only the supported key size. NetScaler® instance fails if you configure an unsupported key size.
- Ensure that you specify the correct serial number. If there is a mismatch in the serial number, the encryption process does not start.

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

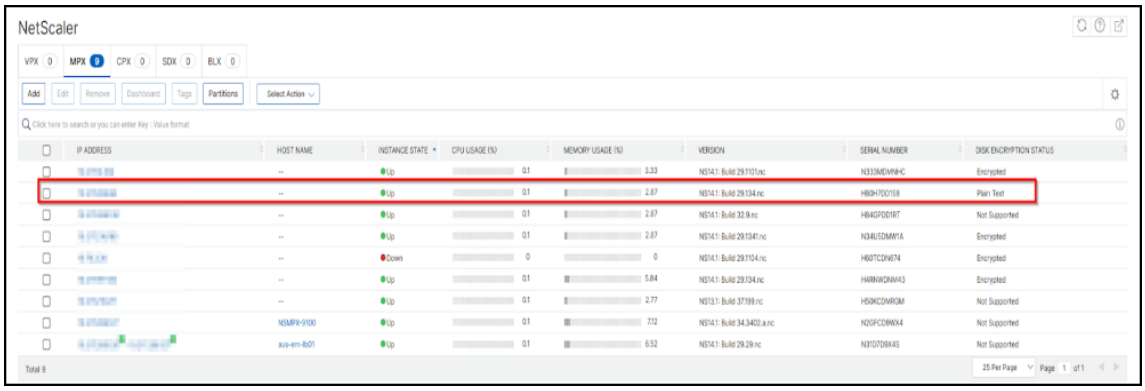
> - We recommend that you copy the instance serial number from NetScaler Console. In the NetScaler Console GUI, navigate to **Infrastructure > Instance > MPX**, select the NetScaler MPX instance, and from the **Select Action** list, click **Get Serial Number**.

Instance disk encryption through NetScaler Console

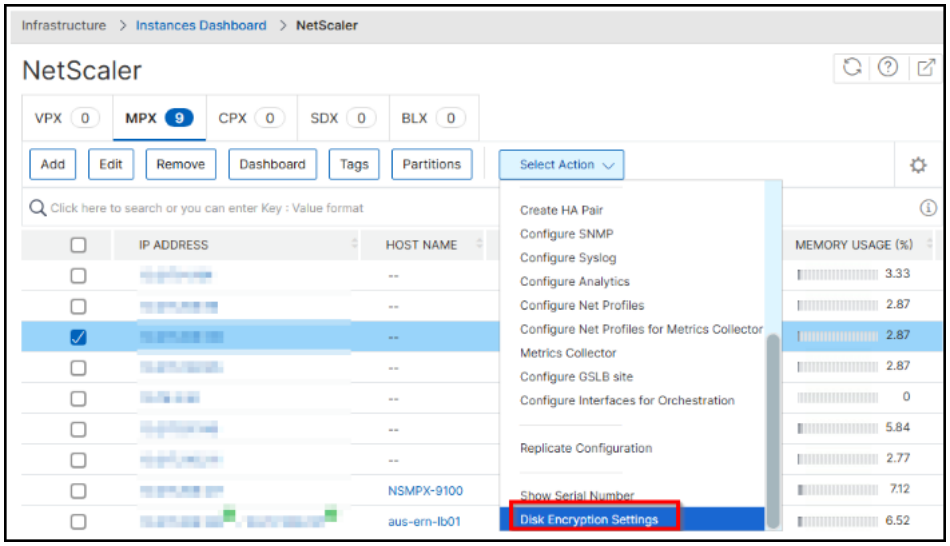
Before you begin the disk encryption, ensure that you take the MPX instance backup through NetScaler Console. For more information, see Configure instance backup.

After you take the backup:

1. Navigate to **Infrastructure > Instances > NetScaler**.
2. In the **NetScaler MPX** tab, you can see the managed instances details. The instance that you want to encrypt displays **Plain Text** under **Disk Encryption Status**.



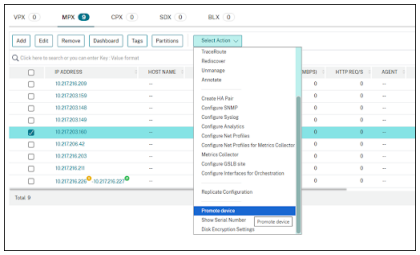
3. From the **Select Action** list, click **Disk Encryption Settings**.



4. From the **Select Action** list and click **Promote device** .

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

> **Note:**
>
> Selecting the **Promote device** option is mandatory to activate the Disk Encryption feature specifically for MPX appliances manufactured before May 20, 2025. Allow approximately 30 minutes for the MPX appliance to complete its conversion into a disk encryption-enabled device.



5. In the **Disk Encryption Settings** page:

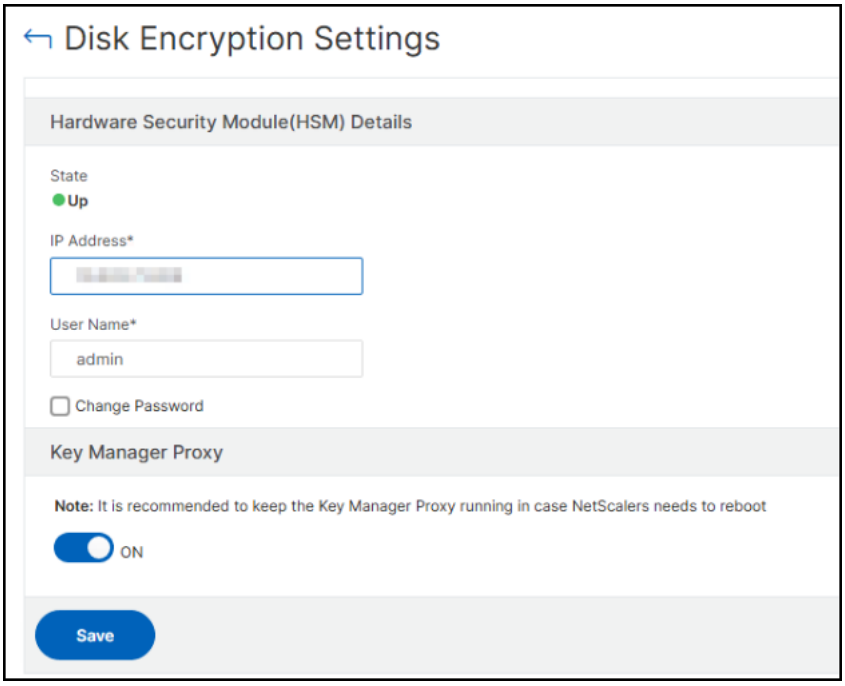
   a) Specify the IP address, user name, and password of the HSM server from where NetScaler Console can fetch the encryption key by using the serial number.

   b) Enable the **Key Manager Proxy**. You must enable this option to continue with the disk encryption process.

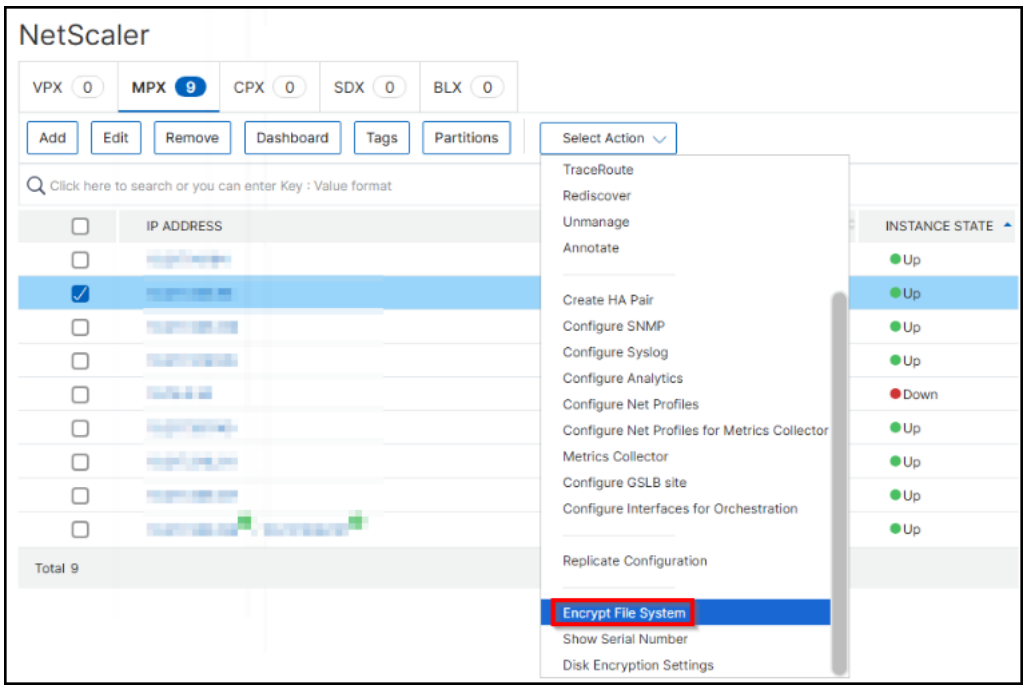
   > **Note:**
   >
   > Ensure that the **Key Manager Proxy** is always enabled even after the encryption is complete. If you disable this option, the encrypted instance will not reboot successfully for scenarios, such as after you upgrade the instance or force a reboot of the instance.

   c) Click **Save**.

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



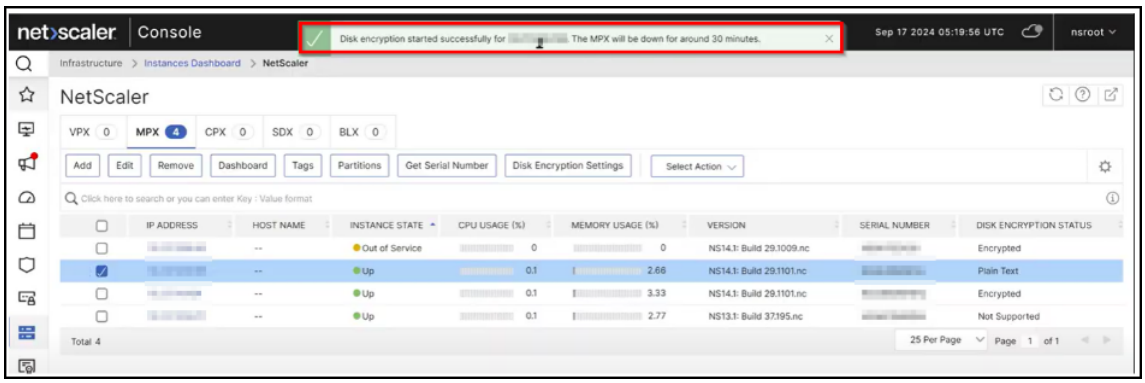
6. Select the instance and from the **Select Action** list, click **Encrypt File System**.



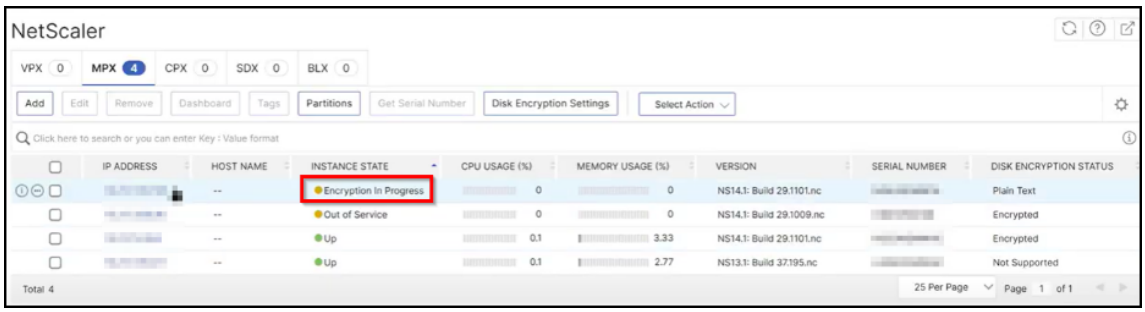
A confirmation window appears. Click **Yes** to proceed.

7. A confirmation message appears in NetScaler Console stating that the encryption is started and the instance will be in **Down** status for approximately 30 minutes.

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



The instance state appears as **Encryption in progress**.



Validation after encryption

The instance encryption is completed in approximately 30 minutes. After the encryption is complete:

- You can log on to the NetScaler MPX instance using an SSH client and then validate if the encryption is successful by using the following command:

  ```
  show filesystemencryption
  ```

Before encryption

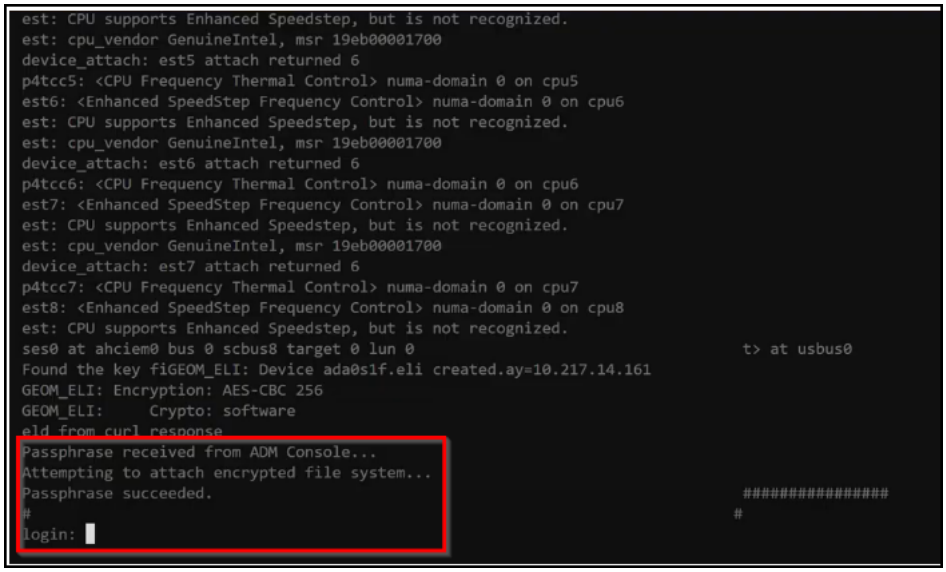
```
Done
> show version
        NetScaler NS14.1: Build 29.134.nc, Date: Nov  5 2024, 23:55:14   (64-bit)
Done
> show filesystemencryption
        File System Encyption: Supported        File System State: Not Encrypted
Done
```

After encryption

```
> show filesys
        File
Done
```

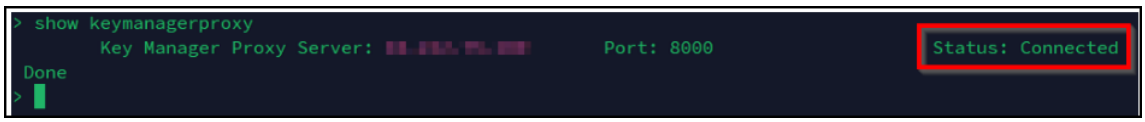
- You can reboot your NetScaler MPX instance and validate if the reboot is completed after the encryption as shown in the following example:

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



- You can use the following command to validate if **Key Manager Proxy** is successfully configured and is accessible from NetScaler:

  ```
  show keymanagerproxy
  ```



> **Note:**
>
> After the encryption, NetScaler Console uses `mpx_disk_encryption_default_profile` to access the NetScaler MPX instance. The `mpx_disk_encryption_default_profile` has the default credentials (`nsroot`/`nsroot`).



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

Restore NetScaler MPX instance after encryption

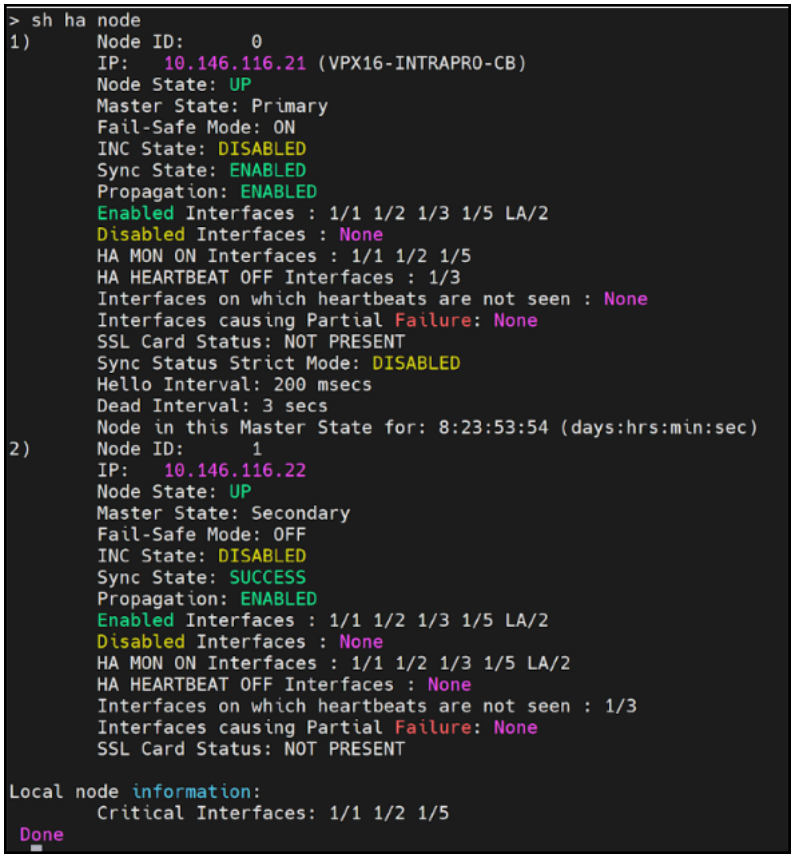
If you have changed the default password (nsroot) before taking the backup, ensure that the profile that is used during the backup is available in NetScaler Console after encryption.

Behavior of NetScaler MPX™ HA pair after encryption

September 27, 2025

Both primary and secondary nodes must have the same encryption status. If there is any mismatch between the primary and secondary node encryption status, the synchronization between the two nodes is disabled. Log on to the primary NetScaler® MPX instance using an SSH client and use the following command to validate if both nodes show the same encryption status:

`sh ha node`



If the encryption status of the two nodes is different:

- The following output appears when there is a disk encryption mismatch:

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

```
> sh ha node
1)      Node ID:      0
        IP:  10.217.216.223
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: AUTO DISABLED (Disk Encryption Mismatch)
        Propagation: AUTO DISABLED (Disk Encryption Mismatch)
        Enabled Interfaces : 0/1 25/8 25/7 25/6 25/5 25/4 25/3 25/2 25/1
        Disabled Interfaces : None
        HA MON ON Interfaces : 0/1
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 25/8 25/7 25/6 25/5 25/4 25/3 25/2 25/1
        Interfaces causing Partial Failure: None
        SSL Card Status: UP
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:0:11:52 (days:hrs:min:sec)
2)      Node ID:      1
        IP:   10.146.116.21
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: AUTO DISABLED (Disk Encryption Mismatch)
        Propagation: AUTO DISABLED (Disk Encryption Mismatch)
        Enabled Interfaces : UNKNOWN
        Disabled Interfaces : UNKNOWN
        HA MON ON Interfaces : UNKNOWN
        HA HEARTBEAT OFF Interfaces : UNKNOWN
        Interfaces on which heartbeats are not seen : UNKNOWN
        Interfaces causing Partial Failure: UNKNOWN
        SSL Card Status: UNKNOWN

Local node information:
        Critical Interfaces: 0/1
 Done
>
```

- A disk encryption mismatch error appears for enable HA sync, enable HA prop, and force HA sync:
  - `set ha node -haprop enabled`

    ```
    > set ha node -haprop enabled
    ERROR: Disk Encryption mismatch between HA Nodes. [Prop and sync not allowed]
    ```

  - `set ha node -hasync enabled`

    ```
    > set ha node -hasync enabled
    ERROR: Disk Encryption mismatch between HA Nodes. [Prop and sync not allowed]
    ```

  - `force ha sync`

    ```
    > force ha sync
    ERROR: Disk Encryption mismatch between HA Nodes.
    ```

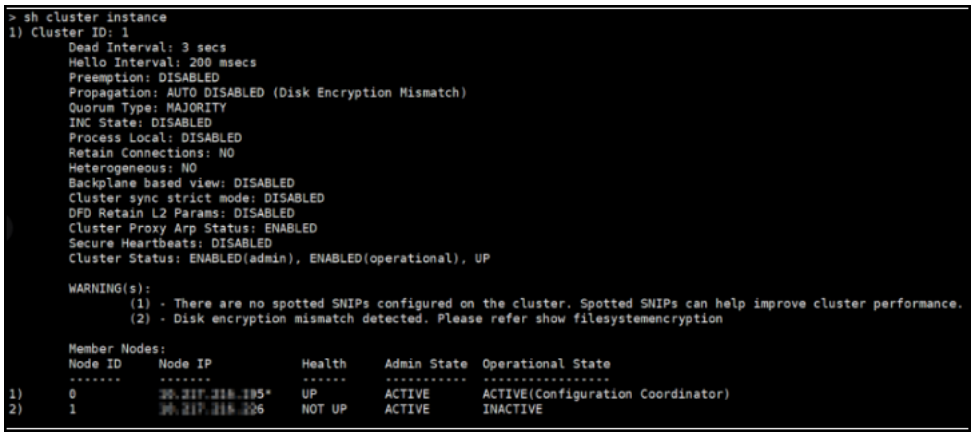
Behavior of NetScaler MPX™ cluster after encryption

September 27, 2025

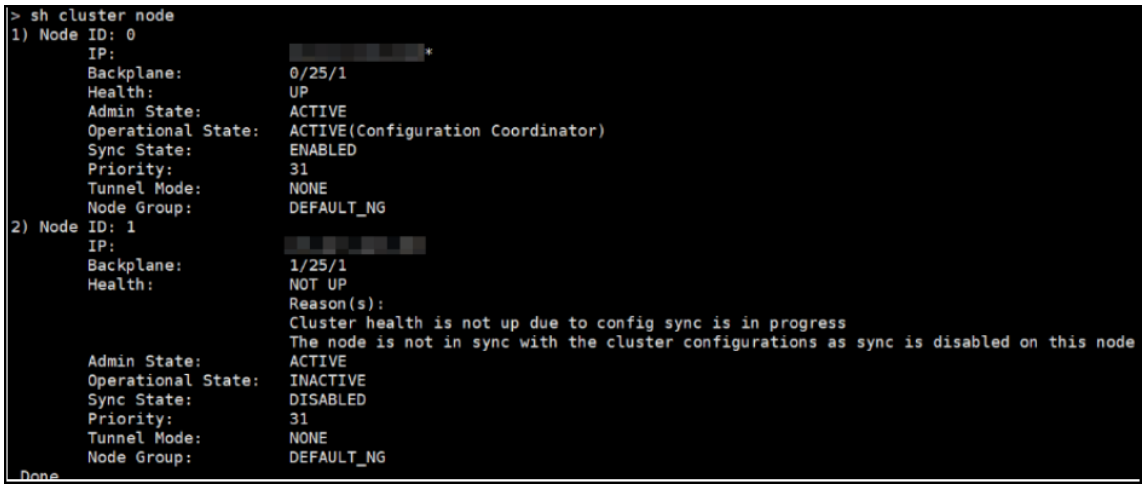
© 1997–2025 Citrix Systems, Inc. All rights reserved.

For a successful cluster formation, all nodes must have the same encryption status. If there is a mismatch in any node encryption status:

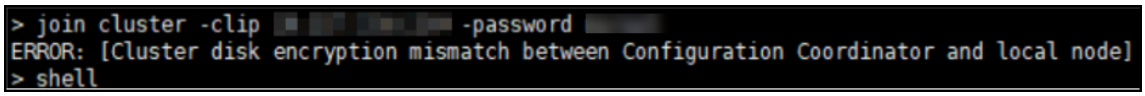
- The mismatched node health status is shown as **NOT UP** and the node does not serve traffic.



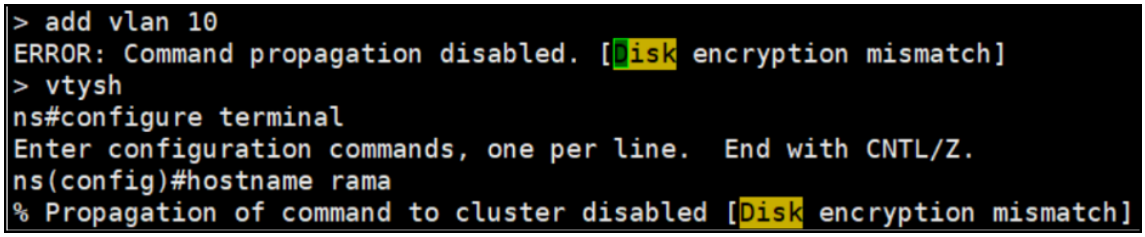
- The mismatched node synchronization in the cluster is disabled.



- Node cannot be added to the cluster. The join command failure message appears:



- The cluster command propagation is disabled.



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

NetScaler Console Cloud Connect

September 27, 2025

You can use the NetScaler Console Cloud Connect feature to establish a connection between NetScaler Console on-prem and NetScaler Console service. Starting from 14.1 25.x build, telemetry data is not collected through Cloud Connect. The telemetry data is now collected using the auto-enabled channel as part of NetScaler telemetry program.

You can configure Cloud Connect to use the following feature in NetScaler Console on-prem:

ServiceNow Integration - This integration uses Citrix ITSM connector to communicate between NetScaler Console and the ServiceNow instance. The ServiceNow integration with NetScaler Console uses the ITSM Adapter service for token based authentication. For more information, see [ServiceNow docs link]

The following table provides the feature availability through Cloud Connect in different NetScaler® Console on-prem builds:

Build	Feature available in Cloud Connect	Action required	Data collection through Cloud Connect
14.1-25.x and later	ServiceNow Integration	Configure Cloud Connect and enable ServiceNow Integration.	No
Between 14.1-8.x and 14.1-21.x	Security Advisory and ServiceNow Integration	Configure Cloud Connect and enable feature	Yes. After configuring Cloud Connect. For more information, see Data governance for Cloud Connect
14.1-4.x or earlier	NA	NA	NA

Notes:

- You do not need to add or migrate the NetScaler instances to NetScaler Console service.
- Cloud Connect requires you to connect to NetScaler Console service by setting up a NetScaler Console service account (if not created already).

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

Prerequisites

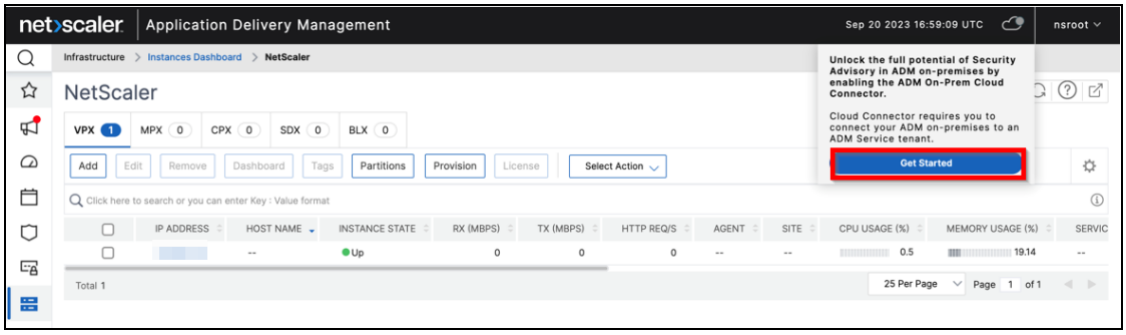
Before you configure Cloud Connect, ensure that you have the following prerequisites:

- Ensure to have internet connection or have a proxy server configured in NetScaler Console on-prem for Citrix Cloud accessibility.
- Ensure that the following endpoint urls are allowed access:
  - Download Service: `https://download.citrixnetworkapi.net`
  - Trust Service: `*.citrixnetworkapi.net`
  - Service URLs
    - `*.agent.adm.cloud.com`
    - `*.adm.cloud.com`
    - `adm.cloud.com`
  - Citrix Cloud™ connectivity:
    - `Citrix.cloud.com`
    - `Accounts.cloud.com`
- Ensure you disable the pop-up blocker in the browser from where you access the NetScaler Console on-prem GUI.

Configure Cloud Connect

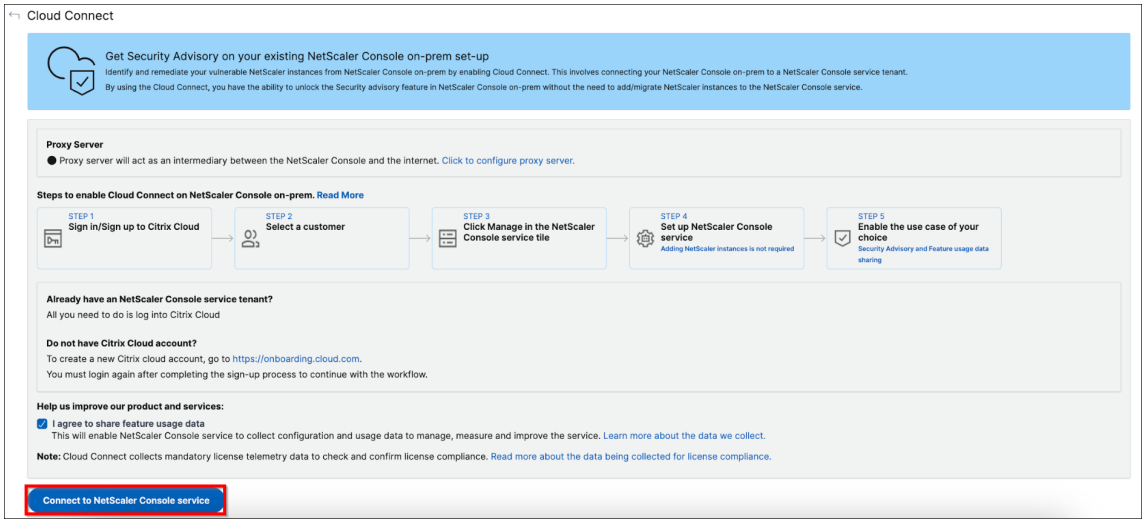
Workflow 1 –If you are a new user without a Citrix Cloud account and NetScaler Console service tenant

1. In NetScaler Console, click the **Cloud** icon > **Get Started**.



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

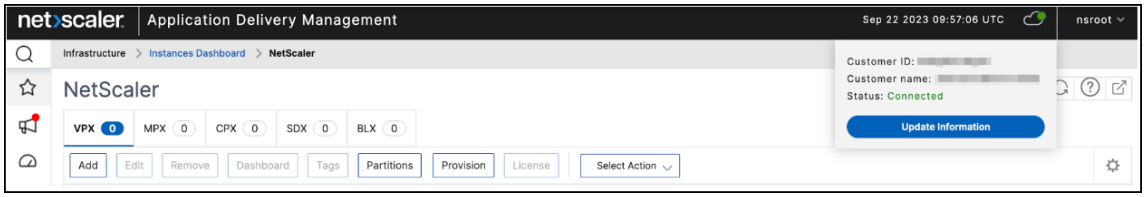
2. Follow the procedure in this document to create a Citrix Cloud account.
3. After you create a Citrix Cloud account, you must again login by clicking **Connect to NetScaler Console service** in NetScaler Console on-prem. Upon successful login, the page redirects to the NetScaler Console service tenant creation steps.



4. Select a region that suits your business needs and click **Done**.
5. Select a role and finish the setup.

   It might take a few minutes for the configuration to complete. In NetScaler Console on-prem, you can see the **Cloud Connect enablement is in progress** screen. You can either click **Refresh** and wait until you get the updated configuration page or click **Cancel** to skip this screen and check later for the updated configuration page.
6. The Cloud Connect configuration is complete. You can proceed further to enable ServiceNow Integration from the Cloud Connect configuration page.
7. Select **ServiceNow Integration using Cloud Connect** and click **Save**.

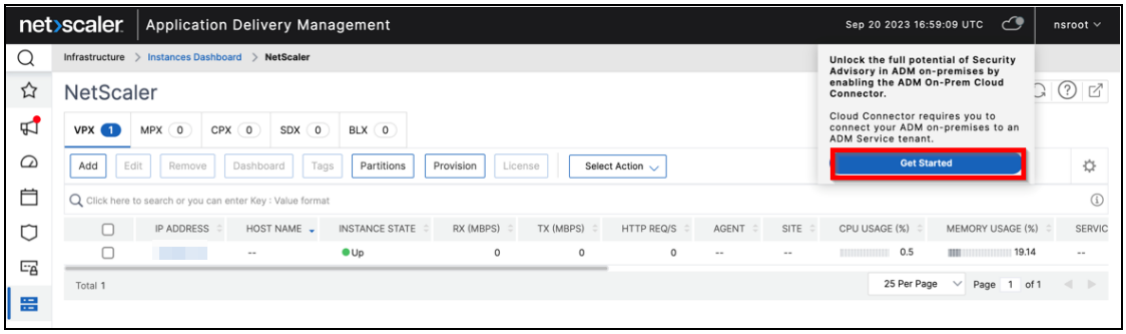
   You can see the status as connected.



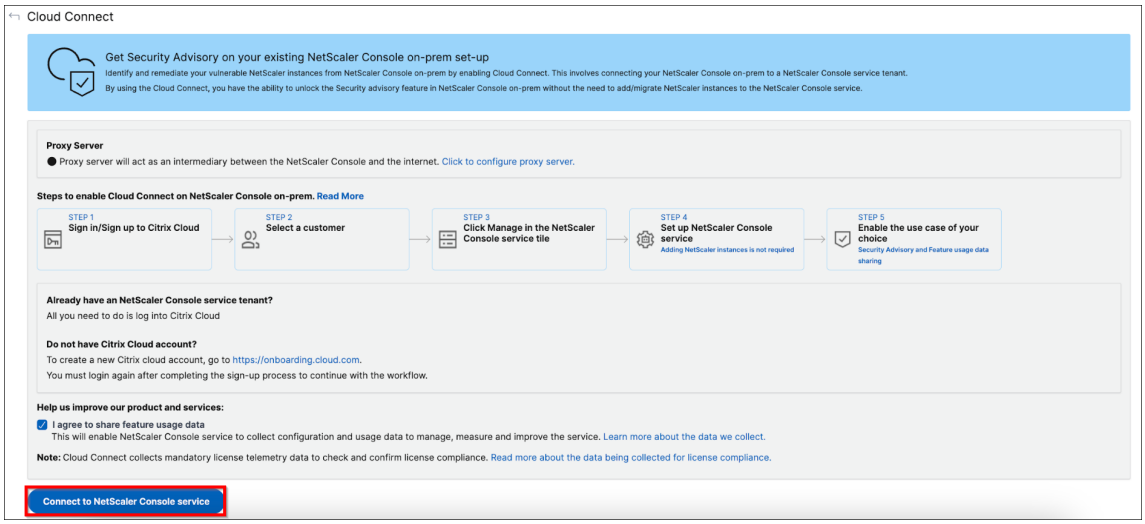
Workflow 2 –If you have a Citrix Cloud account but do not have a NetScaler Console service tenant

1. In NetScaler Console, click the **Cloud** icon > **Get Started**.

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



2. Click **Connect to NetScaler Console service**.

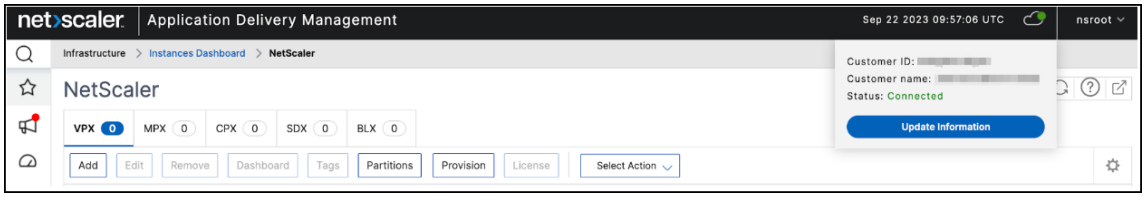


3. You will be redirected to a new tab. Sign into Citrix Cloud.
4. Once you get the login successful message, the page redirects to the NetScaler Console onboarding steps.
5. Select a region that suits your business needs and click Done.
6. Select a role and finish the setup.

   It might take a few minutes for the configuration to complete. In NetScaler Console on-prem, you can see the **Cloud Connect enablement is in progress** screen. You can either click **Refresh** and wait until you get the updated configuration page or click **Cancel** to skip this screen and check later for the updated configuration page.
7. The Cloud Connect configuration is complete. You can proceed further to enable ServiceNow Integration from the Cloud Connect configuration page.
8. Select **ServiceNow Integration using Cloud Connect** and click **Save**.

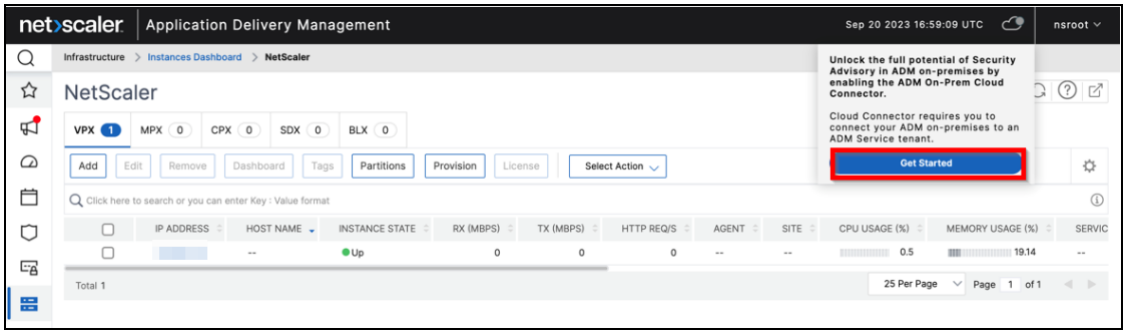
   You can see the status as connected.

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

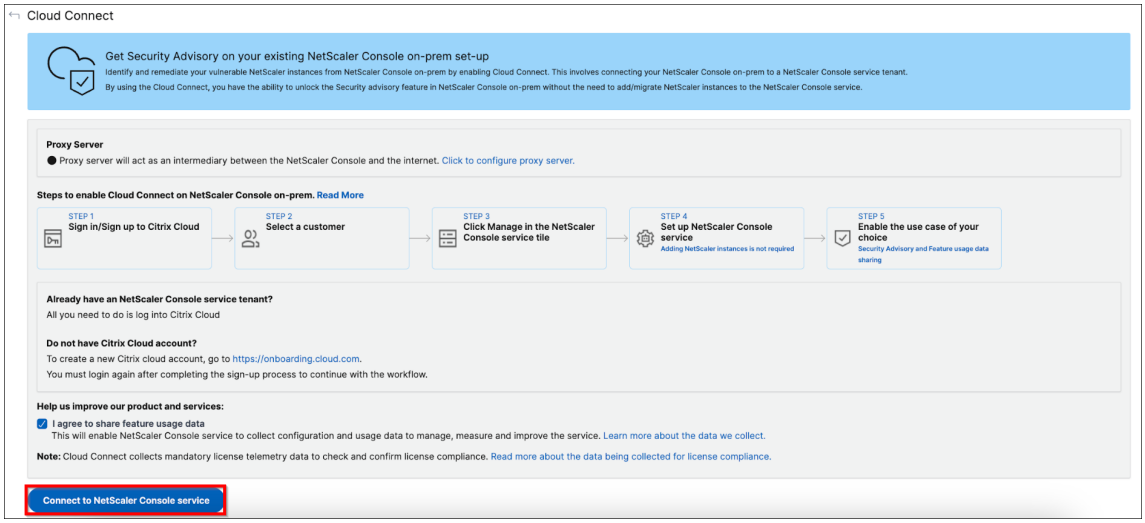


Workflow 3 - If you are an existing user with both Citrix Cloud account and NetScaler Console service tenant

1. In NetScaler Console, click the **Cloud** icon > **Get Started**.



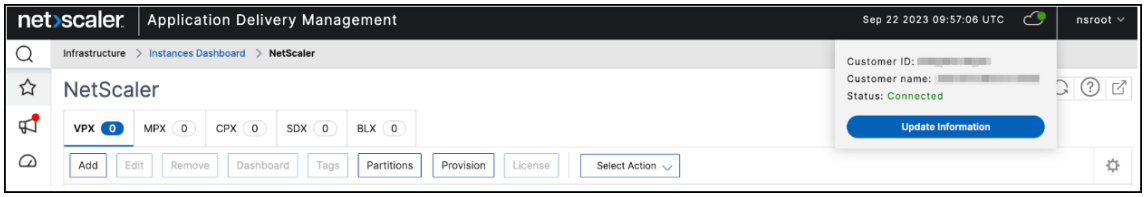
2. Click **Connect to NetScaler Console service**.



3. You will be redirected to a new tab. Sign into Citrix Cloud and select a tenant. After you select the tenant, you get a login successful message.
4. The Cloud Connect configuration is complete. You can proceed further to enable ServiceNow Integration from the Cloud Connect configuration page.
5. Select **ServiceNow Integration using Cloud Connect** and click **Save**.

   You can see the status as connected.

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



Other options

After you enable Cloud Connect, you can use the following options:

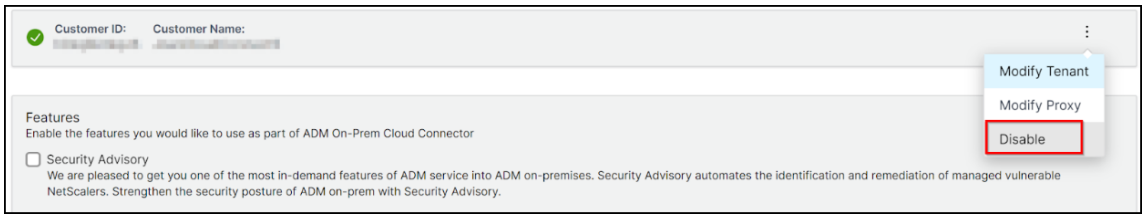
- **Modify Tenant** - Enables you to change the existing tenant. When you click **Modify Tenant**, you will be redirected to a new tab and you must sign into Citrix Cloud. After successful login, you can select a different tenant.
- **Modify Proxy** - Enables you to configure the proxy settings in NetScaler Console on-prem. This is required when NetScaler Console does not have direct access to the internet through the management network. Click **Modify Proxy** from the list, update details, and then click **Save**.



- **Disable** - Disables the Cloud Connect feature. If you choose to disable, the data metric collection is disabled and you cannot use the full version of the Security Advisory.

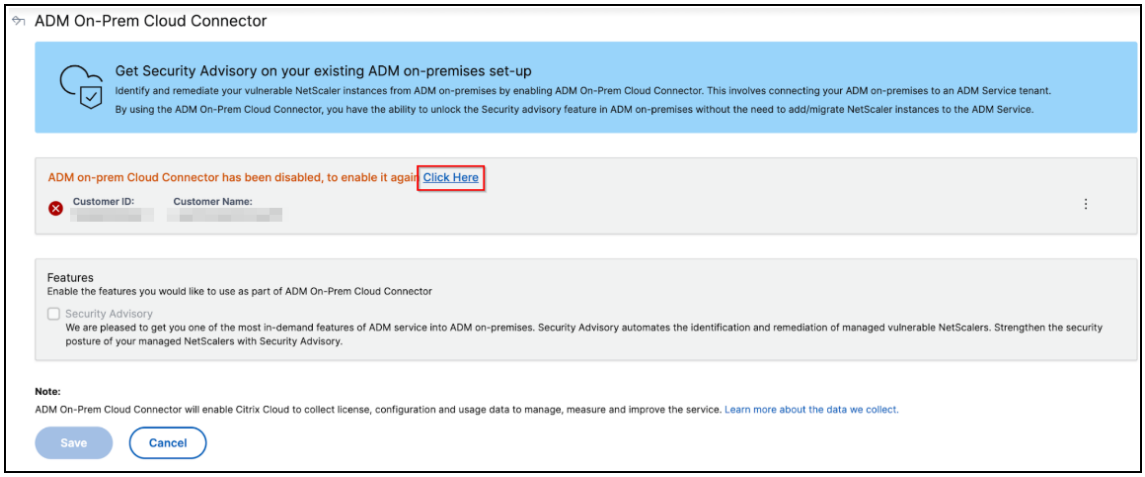
© 1997–2025 Citrix Systems, Inc. All rights reserved.

To disable, click **Disable** from the list.



A confirmation message is displayed. Click **Yes** to disable.

You can again enable Cloud Connect later without any additional steps.



Disable Security Advisory

From the Cloud Connect configuration page, you can also clear the **Security Advisory** check box to disable the Security Advisory feature. The data metrics are still collected.

Configure

September 27, 2025

You can access a NetScaler Console server only by using the GUI. You have to access the GUI to add instances, manage, and monitor your instances and apps, view analytics, and configure the NetScaler Console server.

Your workstation must have a supported web browser to access the configuration utility and Dashboard.

The following browsers are supported.

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

Web Browser	Version
Internet Explorer	11.0 and later
Google Chrome	Chrome 19 and later
Safari	Safari 5.1.1 and later
Mozilla Firefox	Firefox 3.6.25 and later

To access the NetScaler Console GUI:

Log on to NetScaler Console using the administrator credentials.

After you log on to NetScaler Console, you have to do the following to get started:

- Add instances to NetScaler Console. You must add instances to the NetScaler Console server if you want to manage and monitor these instances.
- Enable analytics on virtual servers. 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.
- Configure NTP server on NetScaler Console. You have to configure a Network Time Protocol (NTP) server in NetScaler Console to synchronize its clock with the NTP server.
- Configure system settings for optimal NetScaler Console performance. Before you start using NetScaler Console to manage and monitor your instances and applications, it is recommended that you configure a few system settings that ensure optimal performance of your NetScaler Console server.

Add instances to NetScaler Console

September 27, 2025

Instances are NetScaler appliances or virtual appliances that you want to discover, manage, and monitor from NetScaler Console. You must add instances to the NetScaler Console server if you want to manage and monitor these instances. You can add the following NetScaler appliances and virtual appliances to NetScaler Console:

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX

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

- NetScaler CPX
- NetScaler BLX
- NetScaler Gateway

You can add instances either while setting up the NetScaler Console server for the first time or later. You must then specify an instance profile that NetScaler Console can use to access the instance.

> **Note:**
>
> - NetScaler Console uses the NetScaler IP (NSIP) address of the NetScaler instances for communication. For information about the ports that must be open between the NetScaler instances and NetScaler Console, see Ports.
> - To learn how NetScaler Console discovers instances, see Discover instances.

How to create a NetScaler profile

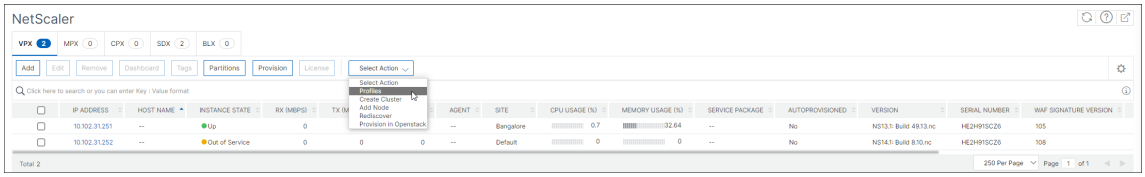
The NetScaler profile includes the credentials, ports, and authentication types for adding instances to NetScaler Console. For each instance type, a default profile is available. For example, the `nsroot` is the default profile for NetScaler instances. The default profile is defined by using the default 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**.



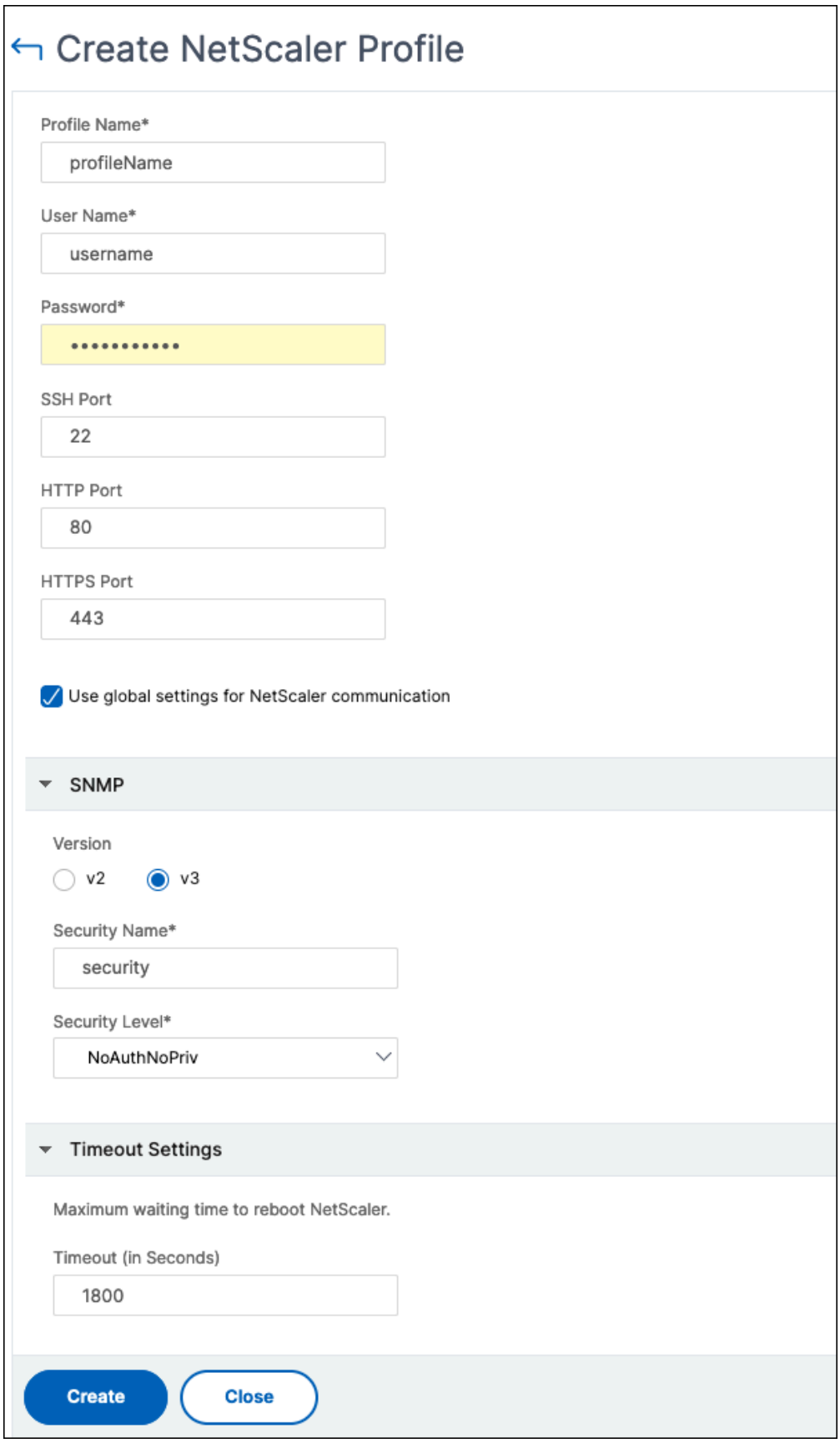
4. On the **Admin Profiles** page, select **Add**.

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



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.

Add NetScaler instances to NetScaler Console

You can add instances either while setting up the NetScaler Console server for the first time or later.

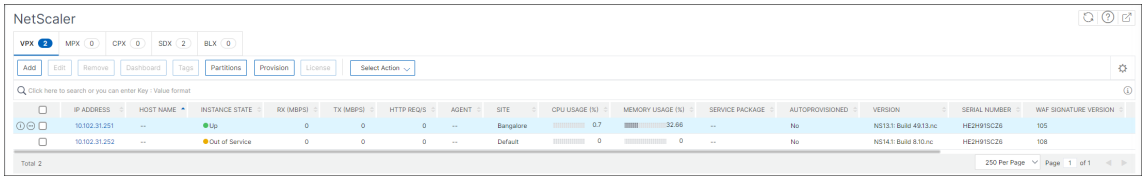
To add instances, you must specify either the host name or IP address of each NetScaler instance, or a range of IP addresses.

> **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 is represented by the cluster IP address only.
> - For NetScaler instances set up as an HA pair, when you add one instance, the other instance in the pair is automatically added.

When you add an instance from a remote data that is configured with an agent, the traffic source is through the agent.

To add an instance to NetScaler Console:

1. Log on to NetScaler Console with administrator credentials.
2. Navigate to **Infrastructure > Instances > NetScaler**. Select the type of instance that you want to add (for example, NetScaler VPX) and click **Add**.



3. Select one of the following options:
   - **Enter Device IP address** - For NetScaler instances, specify 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)

       If you want to discover a NetScaler HA pair using SNIP, ensure the Independent Network Configuration (INC) mode is enabled. And, specify the SNIP addresses in the following format:

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

```
<SNIP of primary instance>#<SNIP of secondary instance>
```

- **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. From **Profile Name**, select the appropriate instance profile, or create a profile by clicking the + icon.
5. From **Site**, select the location where you want to add the instance, or create a location by clicking the **+** icon.
6. Click **OK** to start the process of adding instances to NetScaler Console.

> **Note:**
>
> If you want to rediscover an instance, navigate to **Infrastructure > Instances > NetScaler**. Select the instance type (for example, VPX) and select the instance you want to rediscover, and then from the **Select Action** list, click **Rediscover**.

Add NetScaler CPX instances to NetScaler Console

NetScaler Console has been enhanced to provide support to the improvements that have been accomplished in CPX functionalities. NetScaler CPX instance is now added in NetScaler Console by providing an IP address for the CPX along with a device profile. The process of addition of a CPX instance is now similar to how other NetScaler types such as VPX or MPX is added in NetScaler Console. Also, the registration of CPX in NetScaler Console has been enhanced. When a CPX starts, NetScaler Console automatically discovers and registers the CPX instance. A CPX instance is no longer discovered through the Docker host.

1. Navigate to **Infrastructure > Instances > NetScaler** and click **CPX**.
2. Click **Add** to add new CPX instances in NetScaler Console.
3. The **Add NetScaler CPX** page opens. Enter the values for the following parameters:

    a) You can add CPX instances by providing either the reachable IP address of the CPX instance or the IP address of the Docker container where the CPX instance is hosted.

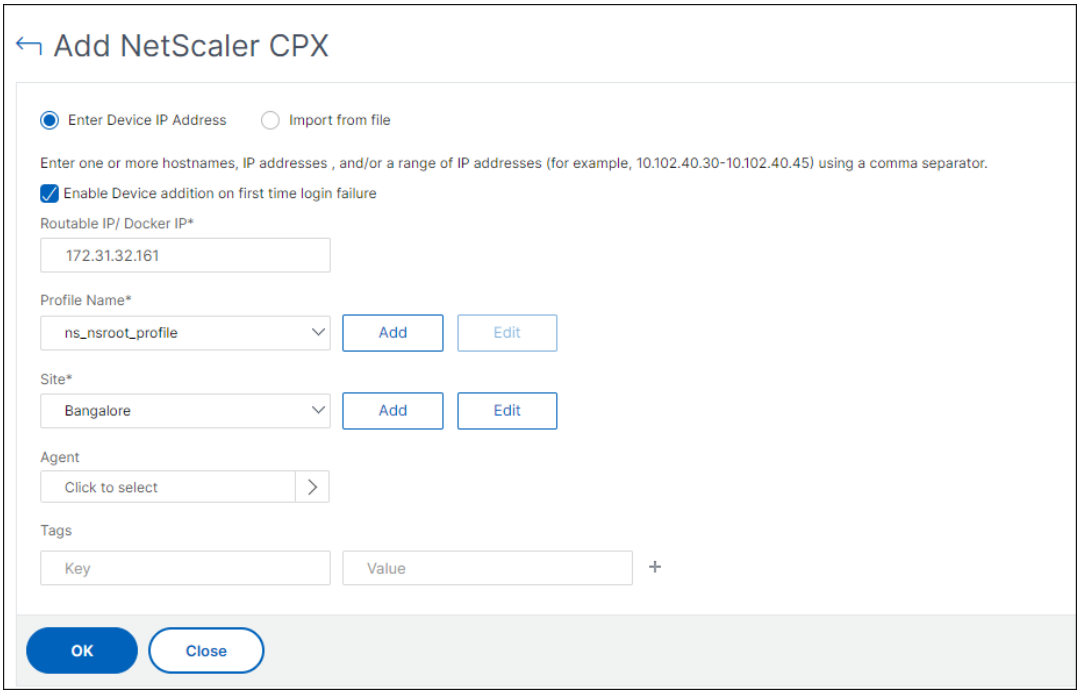
    b) Select the profile of the CPX instance.

    c) Select the site where the instances are to be deployed.

    d) Select the agent.

    e) As an option, you can enter the key-value pair to the instance. Adding a key-value pair makes it easy for you to search for the instance later.

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



> **Note:**
>
> For NetScaler CPX instances, you must specify the **HTTP, HTTPS, SSH**, and **SNMP** port details of the host while creating the CPX instance profile. You can also specify the range of ports that were published by the host in the **Start Port** and **Number of ports** field.

4. Click **OK**.

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. Select the **Standalone** option from the **Instance Type** list.
4. In the **IP address** field, specify the IP address of the BLX instance.
5. In the **Host IP address** field, specify the IP address of the Linux server where the BLX instance is hosted.
6. In the **Profile Name** list, select the appropriate profile for a BLX instance, or create a profile.

   To create a profile, click **Add**.

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

> **Important:**
>
> Make sure that you have specified the correct host user name and password of the Linux server in the profile.

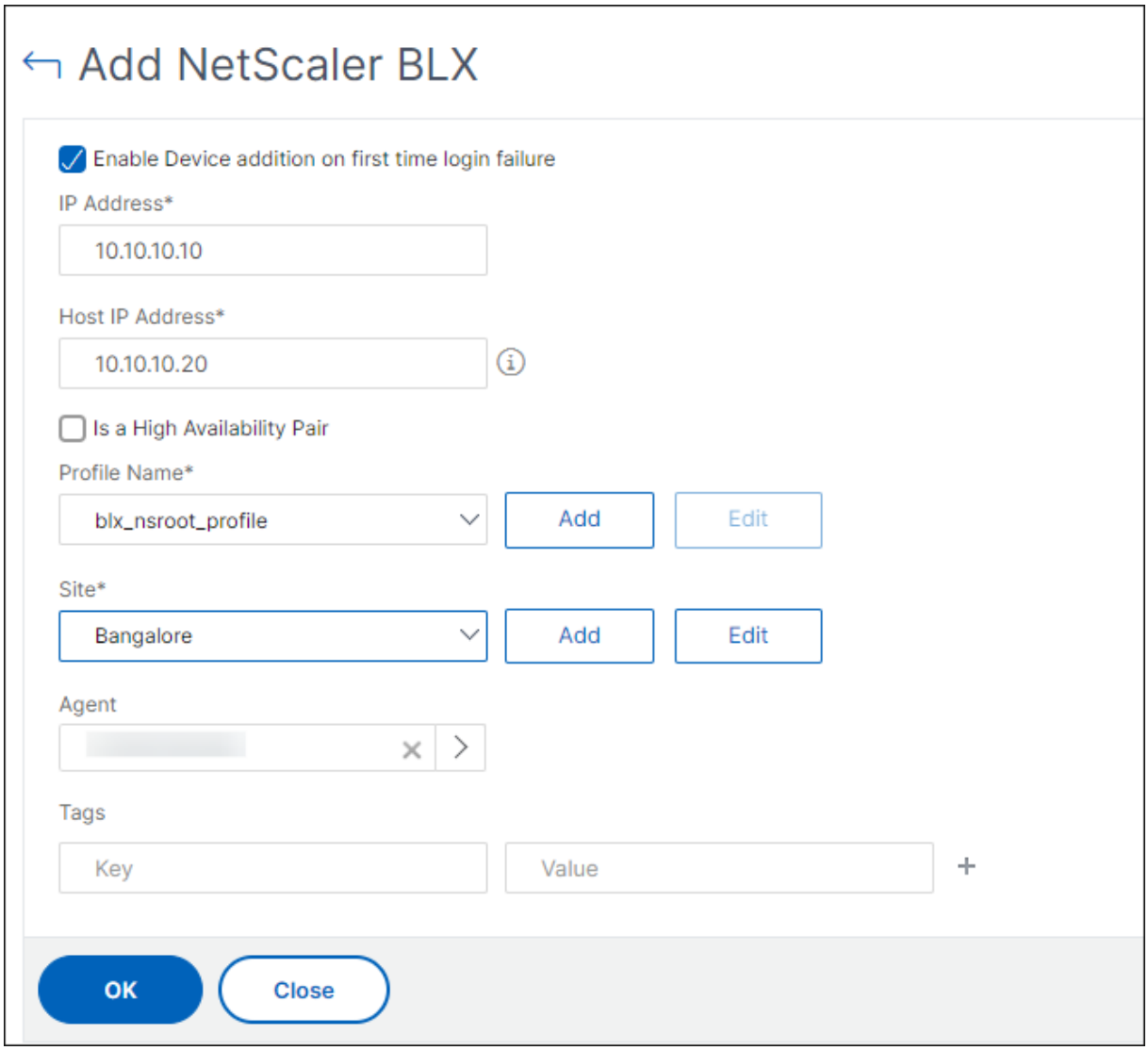
7. In the **Site** list, select the site where you want to add an instance.

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

8. In the **Agent** list, select the NetScaler 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.

9. Click **OK**.



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

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 instance.

1. In the **BLX** tab, click **Add**.
2. Select the **High Availability** option from the **Instance Type** list.
3. In the **IP address** field, specify the IP address of the BLX instance.
4. In the **Host IP address** field, specify the IP address of the Linux server where the BLX instance is hosted.
5. In the **Peer IP address** field, specify the IP address of the peer BLX instance.
6. In the **Peer Host IP address** field, specify the IP address of the Linux server where the peer 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**.

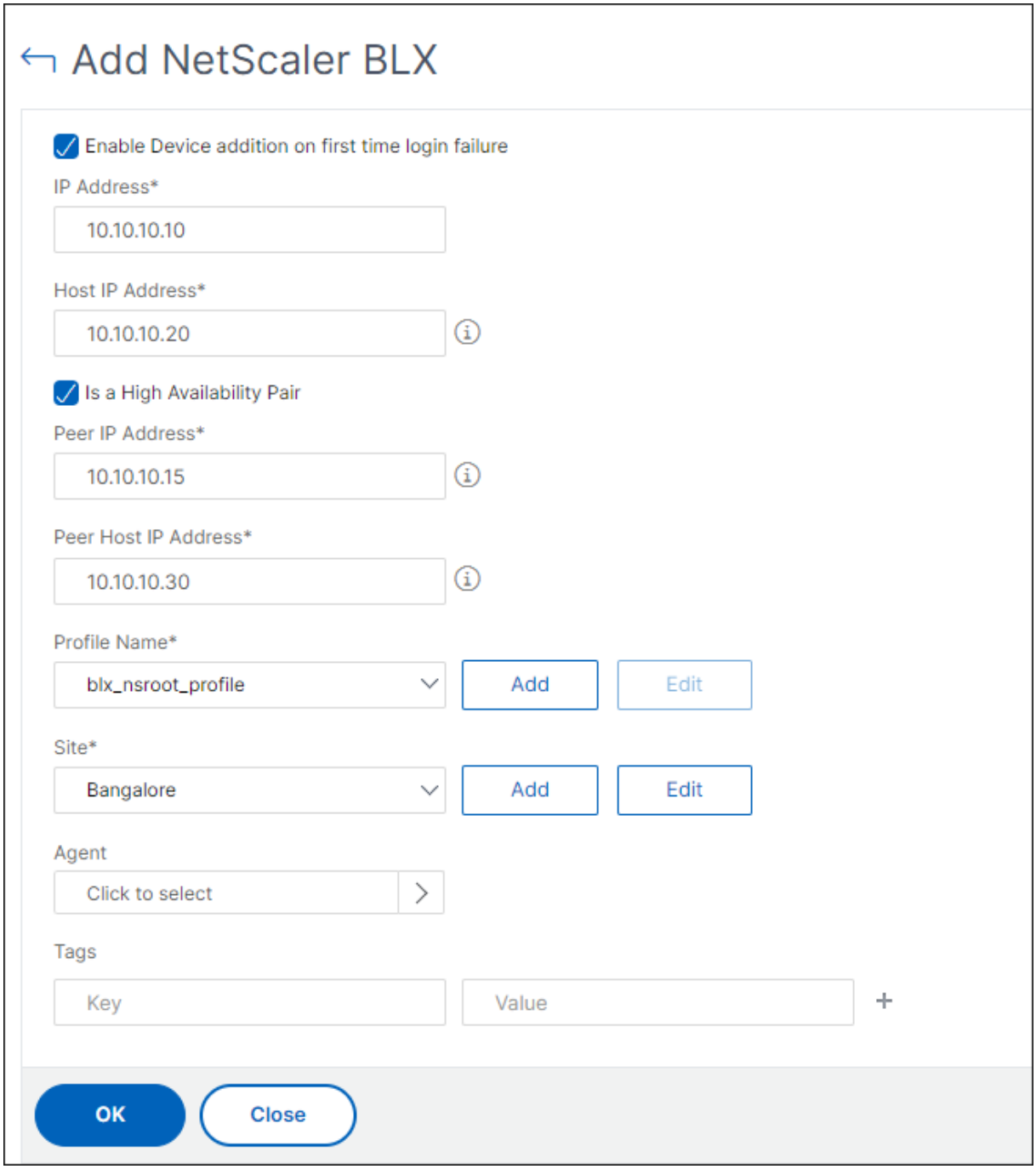
   > **Important:**
   >
   > Make sure to specify the correct host user name and password of the Linux server in the profile.

8. In the **Site** list, select the site where you want to add an instance.

   If you want to add a site, click **Add**.
9. In the **Agent** list, select the NetScaler agent to which you want to associate the instance.

   If there is only one agent configured on your NetScaler Console, that agent is selected by default.
10. Click **OK**.

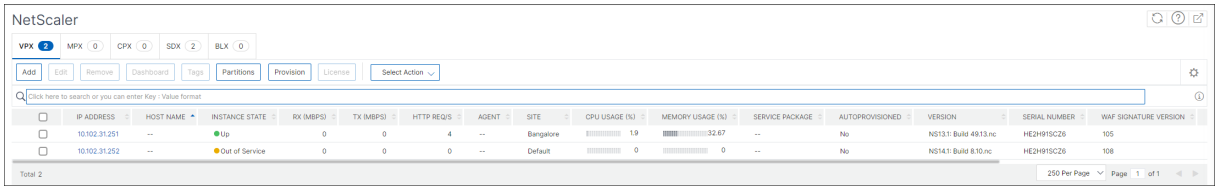
© 1997–2025 Citrix Systems, Inc. All rights reserved.



Access an instance GUI from the NetScaler Console

1. Navigate to **Infrastructure > Instances** > **NetScaler**.
2. Select the type of instance that 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.



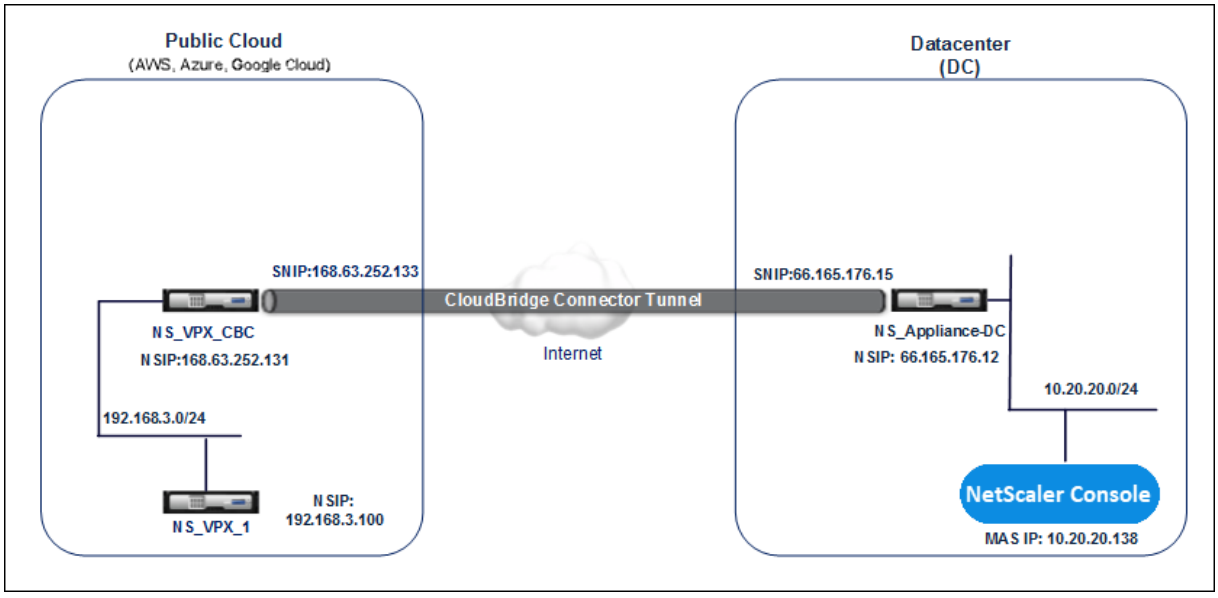
The GUI of the selected instance appears in a pop-up window.

Add NetScaler VPX instances deployed in cloud to NetScaler Console

September 27, 2025

You can use NetScaler Console to manage and monitor the NetScaler VPX instances deployed on a public cloud such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud. You need to establish Layer 3 connectivity between NetScaler Console and the NetScaler VPX instances deployed on the public cloud. To establish the Layer 3 connectivity, you can use solutions such as Direct Connect to AWS, VPN in Azure, or third-party connectors such as Equinix and so on.

The following sample topology uses Citrix CloudBridge Connector for Layer 3 connectivity between NetScaler Console and the NetScaler VPX instances deployed in the cloud.

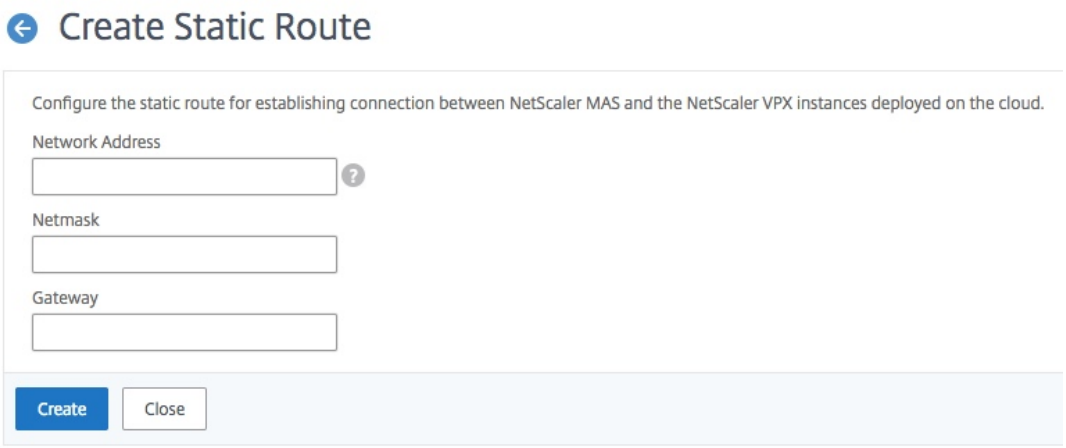


A Citrix CloudBridge Connector tunnel is set up between NetScaler appliance NS_Appliance-DC, in a data center DC, and NetScaler virtual appliance (VPX) NS_VPX_CBC in the public cloud. NS_Appliance-DC and NS_VPX_CBC enable the communication between NetScaler Console and the NetScaler VPX instance, NS_VPX_1, deployed in the public cloud. After the communication is established, you can discover NS_VPX_1 in NetScaler Console.

To configure this topology:

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

1. Install, configure, and start a NetScaler VPX instance in the public cloud.
   - For instructions, see Install NetScaler VPX on AWS.
   - For instructions, see Install NetScaler VPX on Microsoft Azure.
   - For instructions, see Install NetScaler VPX on Google Cloud.
2. Deploy and configure a NetScaler physical appliance, or provision and configure a NetScaler virtual appliance (VPX) on a virtualization platform in the data center.
   - For instructions, see Install a NetScaler VPX instance on Citrix Hypervisor.
   - For instructions, see Install Citrix virtual appliances on VMware ESXi.
   - For instructions, see Install NetScaler virtual appliances on Microsoft Hyper-V.
3. Configure the Citrix CloudBridge Connector between the data center and the public cloud. For instructions, see Configuring Citrix CloudBridge Connector.
4. Configure the static route for establishing connection between NetScaler Console and the NetScaler VPX instances deployed on the cloud, as follows:
   a) Log on to NetScaler Console.
   b) Navigate to **System > Static Routes** and click **Add**.



   c) In the **Network Address** field, enter the address of the network that you want to establish a static route from NetScaler Console through the connector.
   d) In the **Netmask** field, enter the netmask for the network.
   e) In the **Gateway** field, enter the address of the gateway.
5. Add the NetScaler VPX cloud instances to the NetScaler Console by specifying the range of IP addresses of NetScaler VPX instances in the public cloud. For detailed instructions, Add Instances to NetScaler Console.

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

Manage licensing and enable analytics on virtual servers

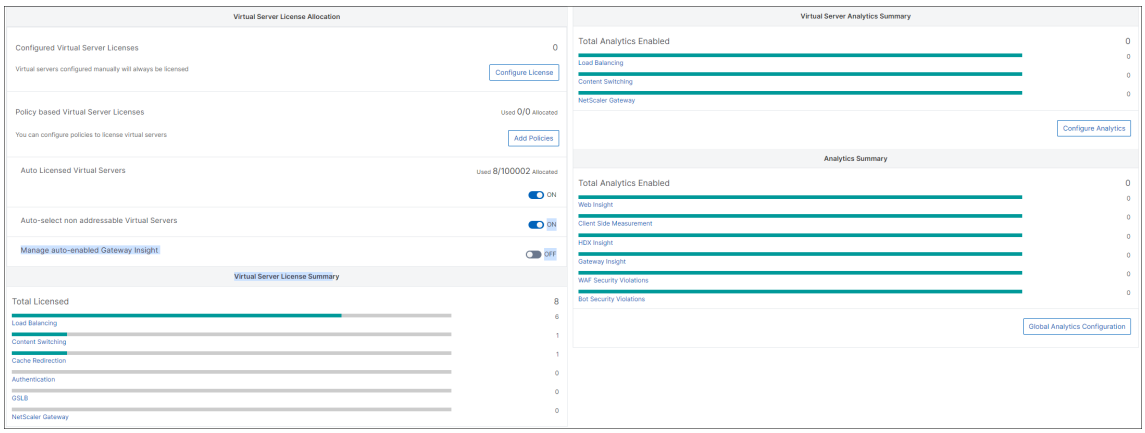
September 27, 2025

> **Note**
>
> - By default, the **Auto Licensed Virtual Servers** option is enabled. You must ensure to have sufficient licenses to license the virtual servers. If you have limited licenses and want to license only the selective virtual servers based on your requirement, disable the **Auto Licensed Virtual Servers** option. Navigate to **Settings > Licensing & Analytics Configuration** and disable the **Auto Licensed Virtual Servers** option under **Virtual Server License Allocation**.

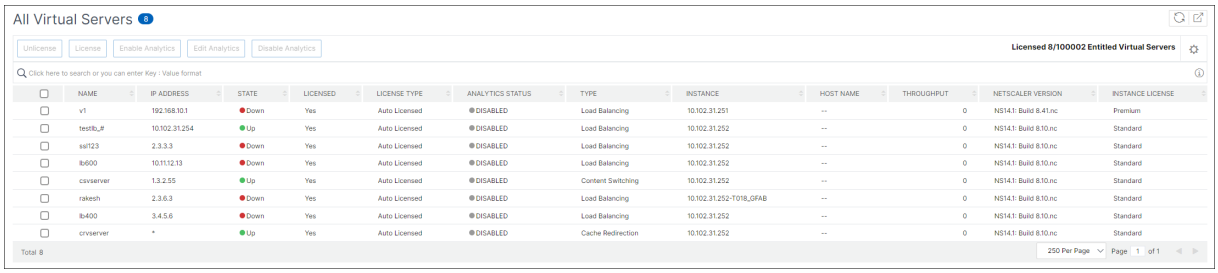
The process of enabling analytics is simplified. You can license the virtual server and enable analytics in a single workflow.

Navigate to **Settings > Licensing & Analytics Configuration** to:

- View the **Virtual Server Licence Summary**
- View the **Virtual Server Analytics Summary**



When you click **Configure License** or **Configure Analytics**, the **All Virtual Servers** page is displayed.



On the **All Virtual Servers** page, you can:

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

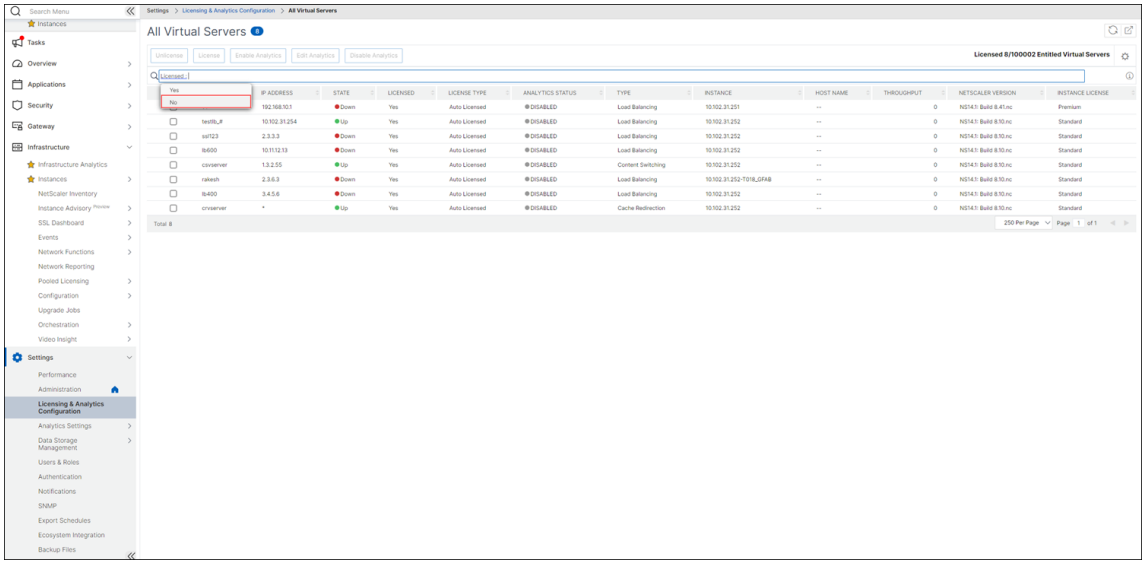
- Apply license for unlicensed virtual servers
- Remove license for licensed virtual servers
- Enable analytics on licensed virtual servers
- Edit analytics
- Disable analytics

> **Note**
>
> The supported virtual servers to enable analytics are Load Balancing, Content Switching, and NetScaler Gateway.

Manage licensing on virtual servers

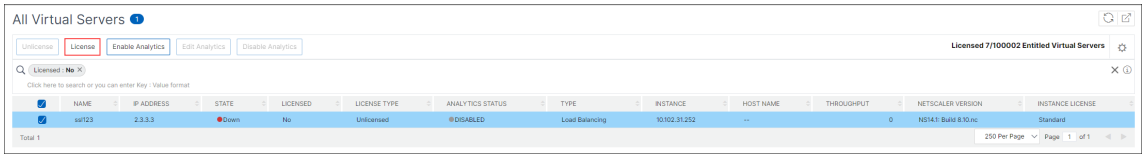
To license the virtual servers, from the **All Virtual Servers** page:

1. Click the search bar, select **Licensed**, and select **No**.



   The filter is now applied and only the unlicensed virtual servers are displayed.

2. Select the virtual servers and then click **License**.



To unlicense the virtual servers, from the **All Virtual Servers** page:

1. Click the search bar, select **Licensed**, and select **Yes**.
2. Select the virtual servers and click **Unlicense**.

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

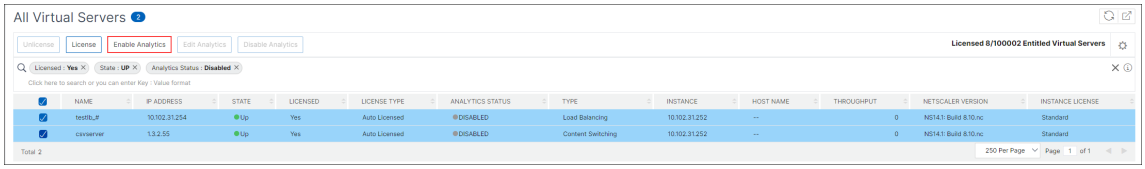
Enable analytics

The following are the prerequisites to enable analytics for virtual servers:

- Ensure that virtual servers are **licensed**
- Ensure that analytics status is **Disabled**
- Ensure that virtual servers are in **UP** status

You can filter the results to identify the virtual servers that are mentioned in the prerequisites.

1. Click the search bar and select **State** and then select **UP**.
2. Click the search bar and select **Licensed**, and then select **Yes**.
3. Click the search bar and select **Analytics Status**, and then select **Disabled**.
4. After applying the filters, select the virtual servers, and then click **Enable Analytics**.



> **Note**
>
> Alternatively, you can enable analytics for a particular instance:
>
> a) Navigate to **Infrastructure > Instances > NetScaler** and then select the instance type. For example, VPX.
>
> b) Select the instance and from **Select Action** list, select **Configure Analytics**
>
> c) On the Configure Analytics on Virtual Servers page, select the Virtual Server and click **Enable Analytics**.

5. On the **Enable Analytics** window:

   a) Select the insight types (Web Insight or WAF Security Violations)

   b) 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.

   c) Under **Instance level options**:

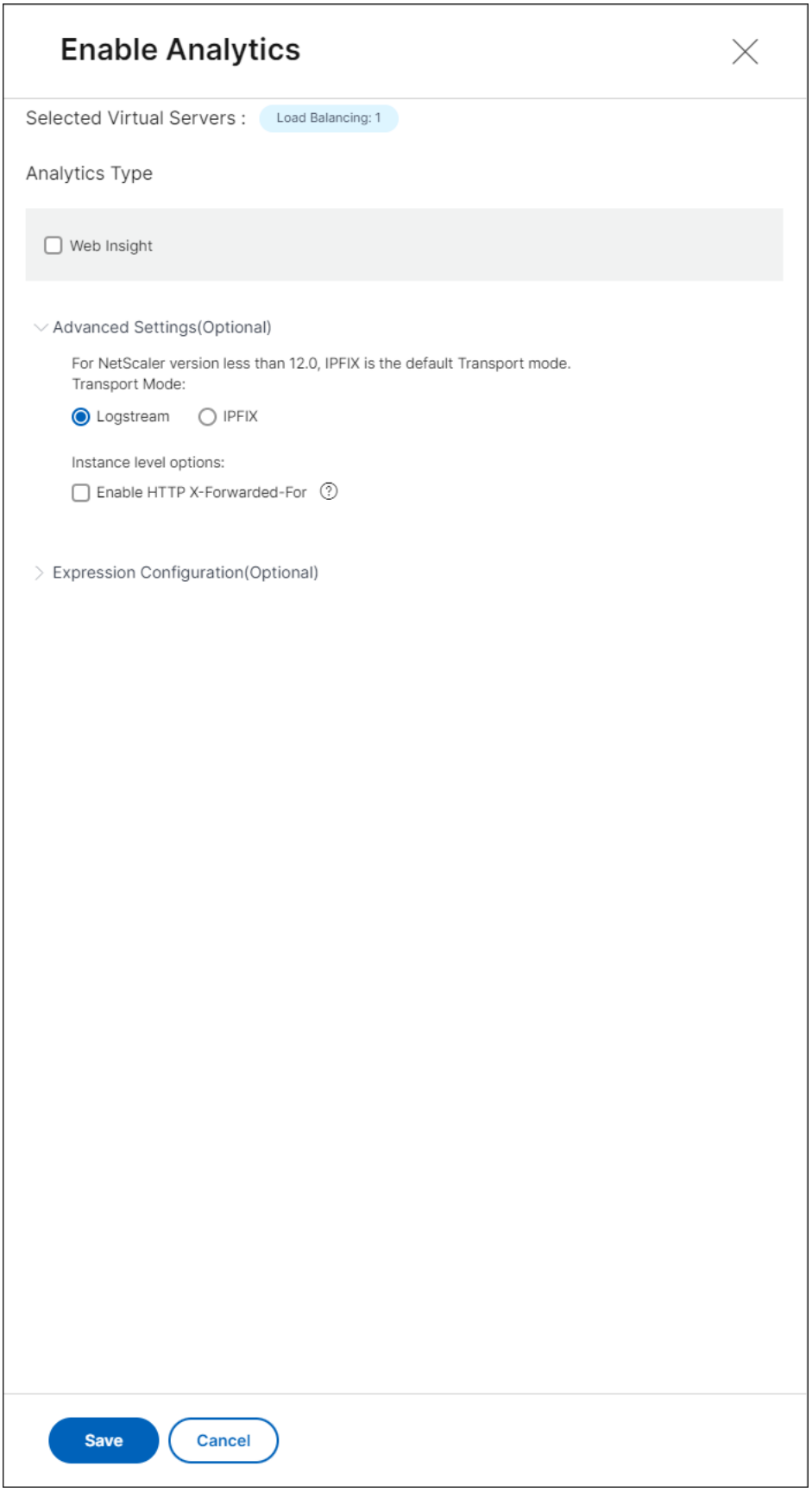
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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.
- **NetScaler Gateway** - Select this option to view analytics for NetScaler Gateway.

d) The Expression is true by default

e) Click **OK**

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



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

> **Note**
>
> - If you select virtual servers that are not licensed, then NetScaler Console first licenses those virtual servers and then enables analytics
> - For admin partitions, only **Web Insight** is supported
> - For virtual servers such as Cache Redirection, Authentication, and GSLB, you cannot enable analytics. An error message is displayed.

After you click **OK**, NetScaler Console processes to enable analytics on the selected virtual servers.

> **Note**
>
> NetScaler Console uses NetScaler SNIP for Logstream and NSIP for IPFIX. If there is a firewall enabled between NetScaler agent and NetScaler instance, ensure you open the following port to enable NetScaler Console to collect AppFlow traffic:

Transport Mode	Source IP	Type	Port
IPFIX	NSIP	UDP	4739
Logstream	SNIP	TCP	5557

Edit analytics

To edit analytics on the virtual servers:

1. Select the virtual servers

   > Note
   >
   > Alternatively, you can also edit analytics for a particular instance:
   >
   > a) Navigate to **Infrastructure > Instances > NetScaler** and then select the instance type. For example, VPX.
   >
   > b) Select the instance and click **Edit Analytics**.

2. Click **Edit 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:

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

1. Select the virtual servers
2. Click **Disable Analytics**

NetScaler Console disables the analytics on the selected virtual servers

The following table describes the features of NetScaler Console that supports IPFIX and Logstream as the transport mode:

Feature	IPFIX	Logstream
Web Insight	•	•
WAF Security Violations	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	Not supported	•
CR Insight	•	•
IP Reputation	•	•
AppFirewall	•	•
Client Side Measurement	•	•
Syslog/Auditlog	•	•

Configure analytics globally

Apart from the existing process to enable analytics, you can also use a single-pane workflow to configure analytics on:

- All the existing licensed virtual servers
- The subsequent licensed virtual servers

After configuration, this feature eliminates the necessity to manually enable analytics on the existing and subsequent virtual servers.

Points to note:

Before you configure analytics, you must understand the following behaviors of NetScaler Console:

- When you configure this feature for the first time, you must ensure that the prerequisites mentioned in this document are met.

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

- Modify the analytics settings later.

  Consider that you have configured the analytics settings for the first time by selecting Web Insight, HDX™ Insight, and Gateway Insight. If you want to modify the analytics settings later and deselect Gateway Insight, the changes do not impact the virtual servers that are already enabled with analytics.

- The virtual servers that are already enabled with analytics.

  Consider that you have 10 licensed virtual servers and two of them are already enabled with analytics. In this scenario, this feature enables analytics only for the remaining eight virtual servers.

- The virtual servers that are manually disabled with analytics.

  Consider that you have 10 licensed virtual servers and you have manually disabled analytics for two virtual servers. In this scenario, this feature enables analytics only for the remaining eight virtual servers and skips the virtual servers that are manually disabled with analytics.

- **Bot Security Violations** and **WAF Security Violations** options are supported only in premium licensed virtual servers. If the virtual servers are not premium licensed, then **Bot Security Violations** and **WAF Security Violations** are not enabled.

Prerequisites

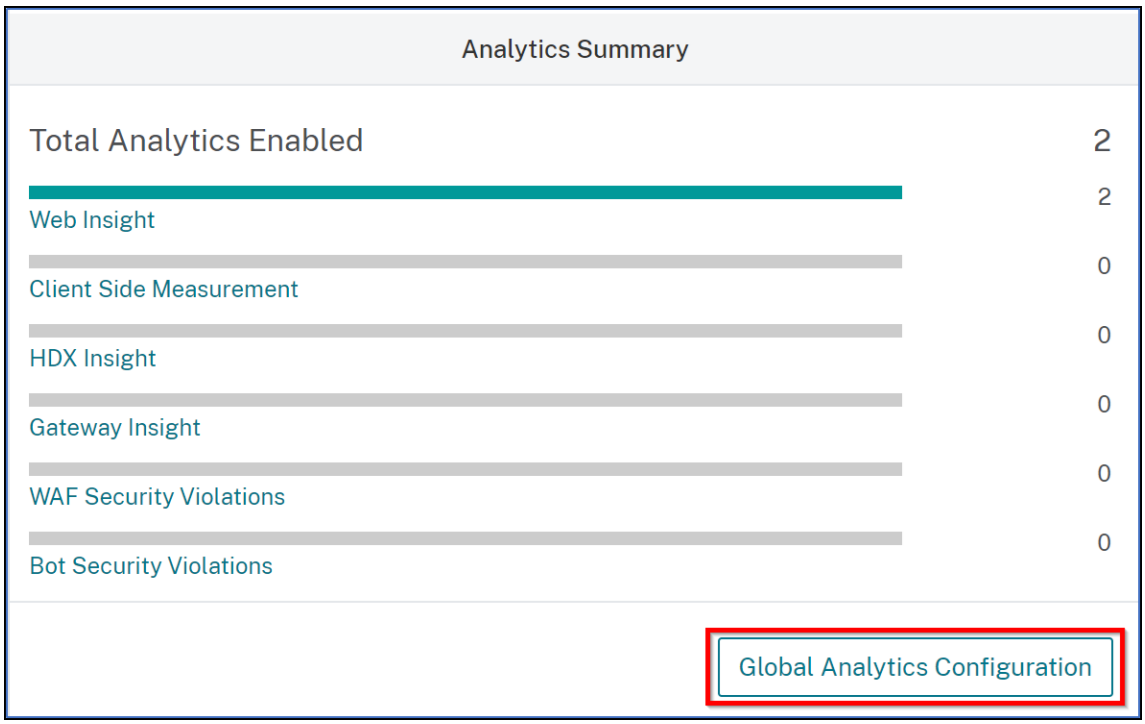
Ensure that:

- All existing virtual servers are licensed.
- Auto-licensed option is enabled to license all the subsequent virtual servers. Navigate to **Settings > Licensing & Analytics Config** and under **Virtual Server License Allocation**, turn on the **Auto Licensed Virtual Servers** option.

Enable analytics

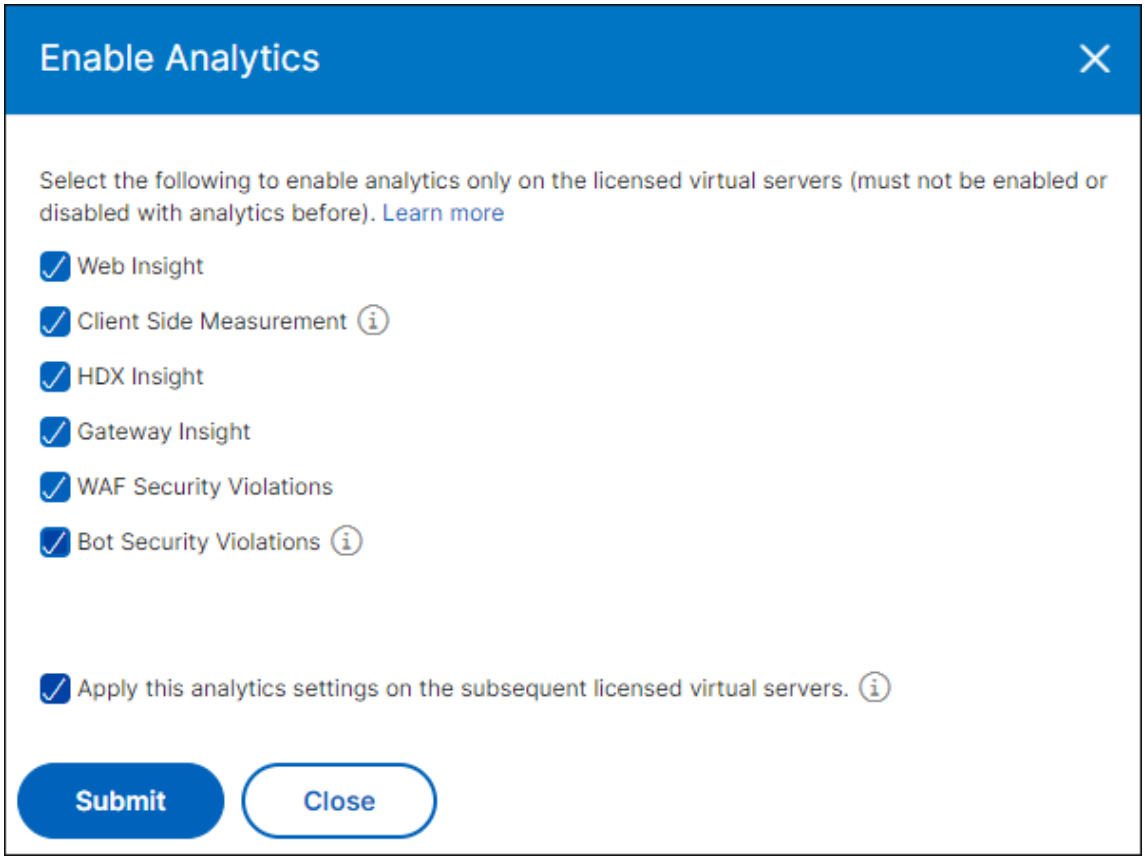
1. Navigate to **Settings > Licensing & Analytics Config**.
2. Under **Analytics Summary**, click **Global Analytics Configuration**.

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



3. Select the analytics features that you want to enable analytics on the virtual servers.
4. To enable analytics on the subsequent virtual servers, select the **Apply this analytics settings on the subsequent licensed virtual servers** check box.
5. Click **Submit**.

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



Configure analytics on virtual servers

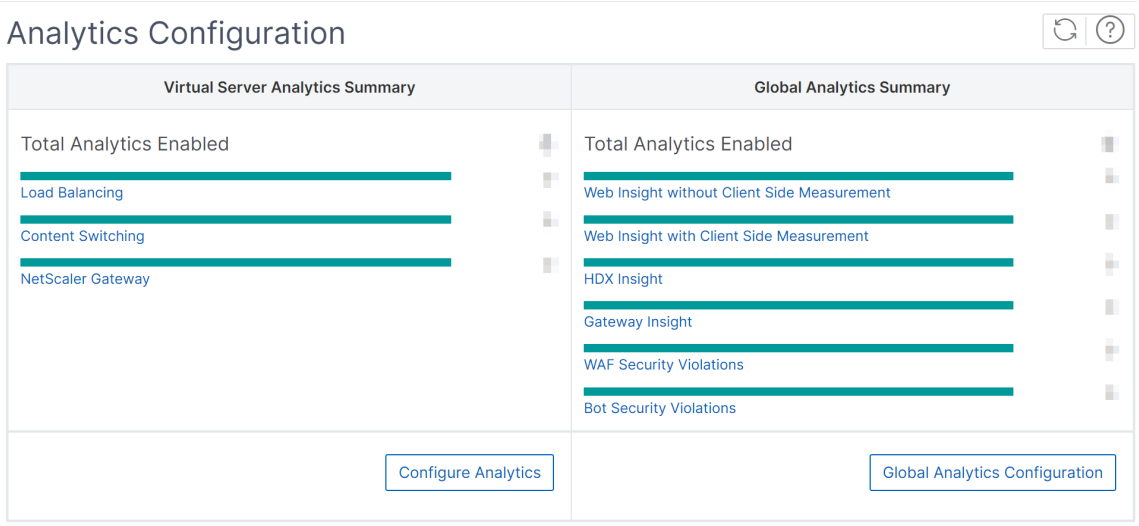
September 27, 2025

The prerequisite to enable analytics is that the virtual servers must be licensed. If you use a flexed license, all the existing 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 existing virtual servers.
- **Global Analytics Summary** - Enables you to configure analytics on both existing and subsequent virtual servers.

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



Configure analytics on the existing virtual servers

> **Note:**
>
> Ensure that the virtual servers you want to enable analytics are in **UP** status.

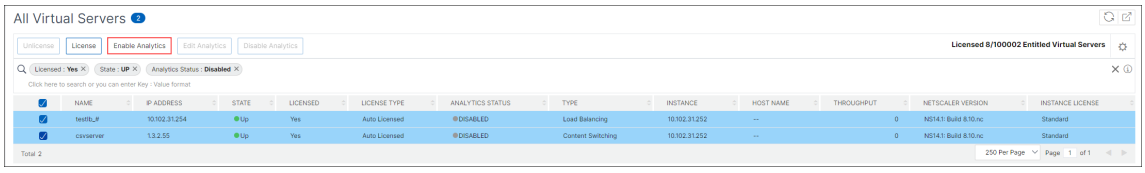
1. Under **Virtual Server Analytics Summary**, click **Configure Analytics**.

   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 Analytics**.



> **Note**
>
> Alternatively, you can enable analytics for an instance:
>
> a) Navigate to **Infrastructure > Instances > NetScaler** and then select the instance type. For example, VPX.

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

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 Analytics**.

3. On the **Enable Analytics** window:

   a) Select the insight types.

   b) 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.

   c) Under **Instance level options**:

   - **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.

   d) The Expression is true by default.

   e) Click **OK**.

   > **Note:**
   >
   > - For admin partitions, only **Web Insight** is supported.
   > - For virtual servers such as Cache Redirection, Authentication, and GSLB, you cannot enable analytics. An error message is displayed.

After you click **OK**, NetScaler Console processes to enable analytics on the selected virtual servers.

> **Note**
>
> NetScaler Console uses NetScaler SNIP for Logstream and NSIP for IPFIX. If there is a firewall enabled between NetScaler agent and NetScaler instance, ensure you open the following port to enable NetScaler Console to collect AppFlow traffic:

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

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 Analytics**.

2. Click **Edit Analytics**
3. Edit the parameters that you want to apply on the **Edit Analytics Configuration** window.
4. Click **OK**.

Disable analytics

To disable analytics on the selected virtual servers:

1. Select the virtual servers.
2. Click **Disable Analytics**.

NetScaler Console disables the analytics on the selected virtual servers.

The following table describes the features of NetScaler Console that supports IPFIX and Logstream as the transport mode:

Feature	IPFIX	Logstream
Web Insight	•	•
WAF Security Violations	•	•
Gateway Insight	•	•

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

Feature	IPFIX	Logstream
HDX Insight	•	•
SSL Insight	Not supported	•
CR Insight	•	•
IP Reputation	•	•
AppFirewall	•	•
Client Side Measurement	•	•
Syslog/Auditlog	•	•

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.

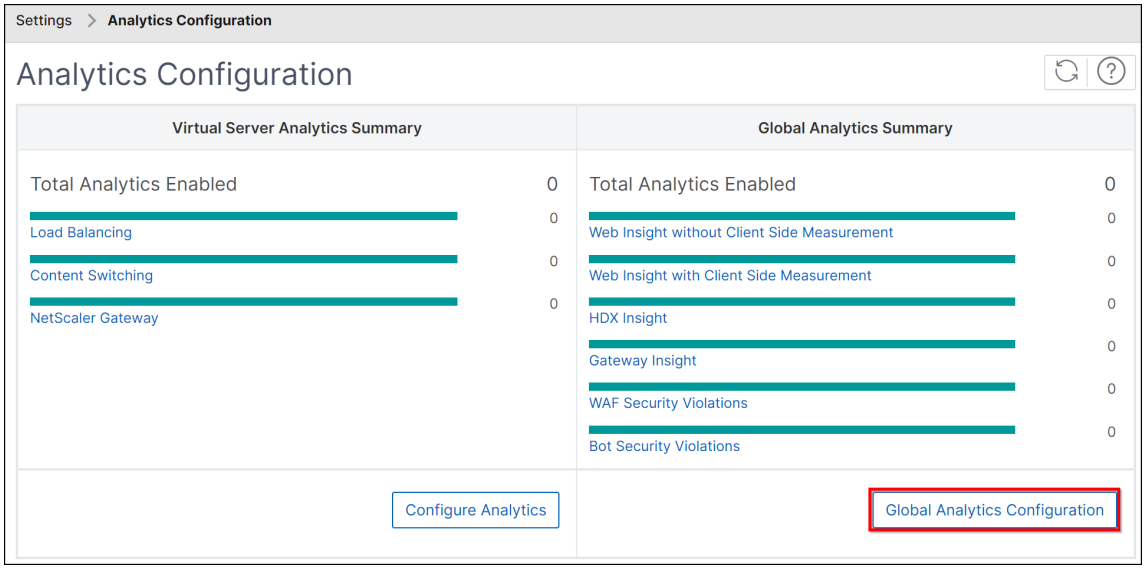
Custom policy

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:

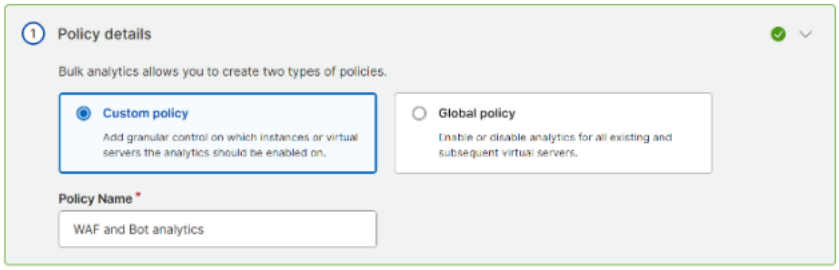
1. Under **Global Analytics Summary**, click **Global Analytics Configuration**.

© 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.



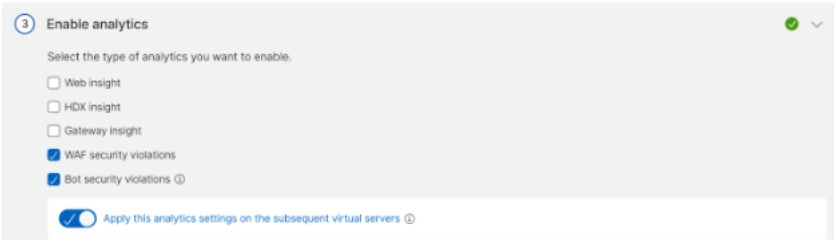
3. Under **Define Conditions**, create conditions by selecting the set of instance IPs or specific instances or virtual server name or both.



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 des-

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

elect **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

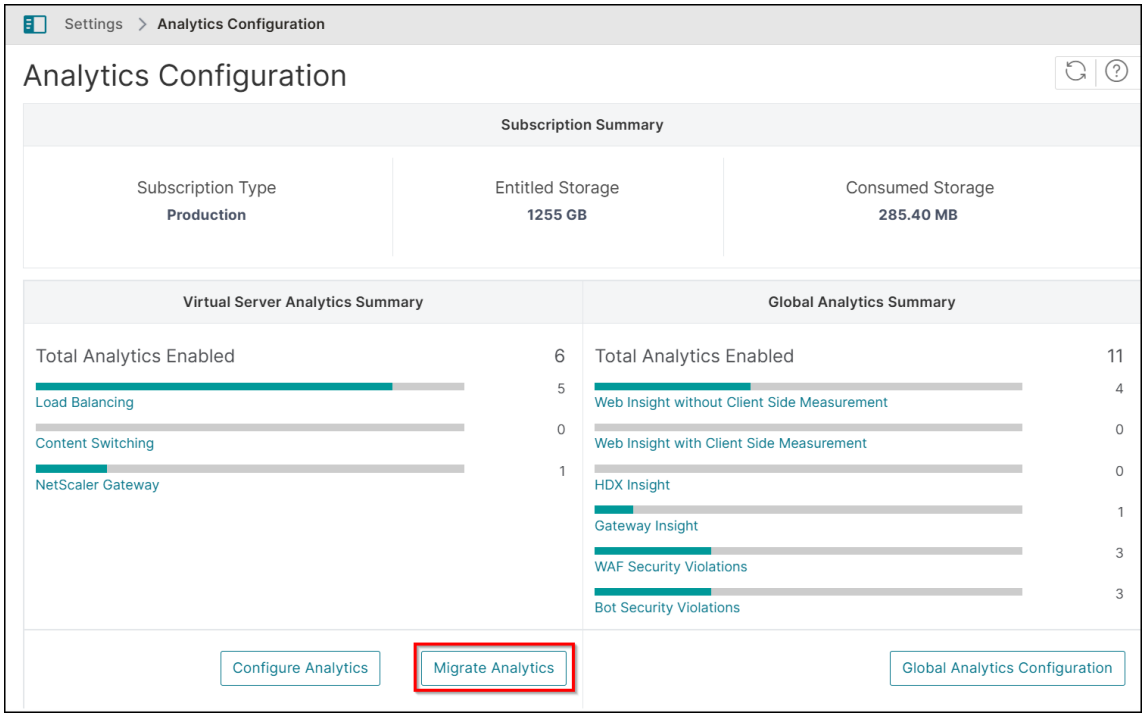
Starting from **14.1-43.x** build, when you enable analytics on virtual servers, the analytics are applied through profile-based configuration. Earlier, analytics was configured through an AppFlow policy. The profile-based configuration has the following benefits:

- Improved performance and flexibility
- Easier configuration and management

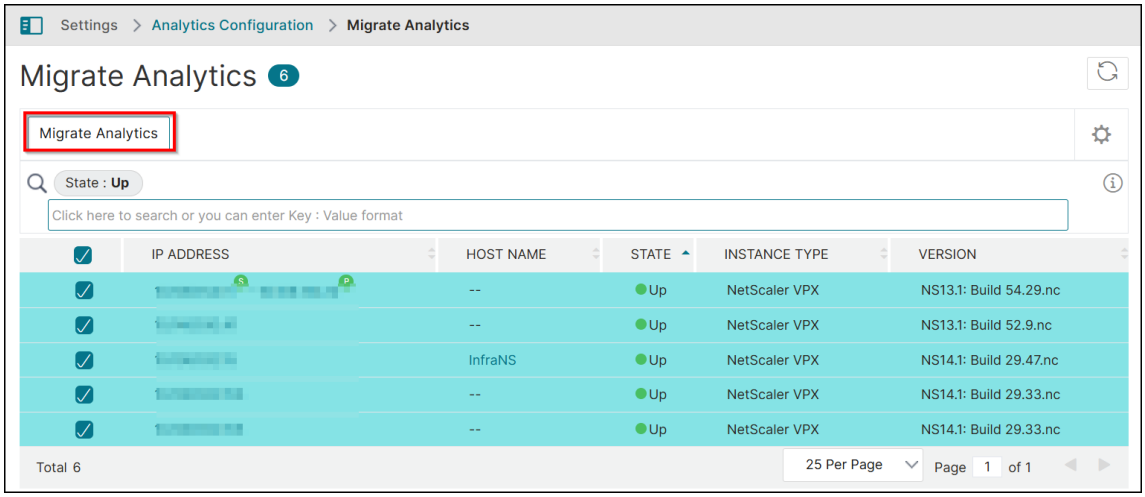
> **Note:**
>
> Enhancements related to analytics configurations are supported only through profile-based configuration. We recommend that you migrate all your existing virtual servers that are enabled for analytics to profile-based configuration.

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.

Assign a net profile for the managed NetScaler instance

August 12, 2024

When you enable analytics or metrics collector for the virtual servers in NetScaler Console, the

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

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 than the SNIP. For more information about net profile, see Use a specified source IP for back-end communication.

You can assign a net profile to a NetScaler instance through NetScaler Console for exporting AppFlow data from NetScaler to NetScaler Console.

Prerequisites

Ensure that:

- The NetScaler instance version is **13.0-48.4 or later**.
- Net profile is configured in NetScaler instances.

To assign a net profile in NetScaler Console:

1. Navigate to **Infrastructure > Instances > NetScaler**.
2. Select the instance, and from the **Select Action** list:
    - Click **Configure Net Profiles** to assign a net profile for AppFlow.
    - Click **Configure Net Profiles for Metrics Collector** to assign a net profile for metrics collector.
3. Select a net profile from the list and click **Apply**.

> **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.

Configure NTP server

September 27, 2025

You can configure a Network Time Protocol (NTP) server in NetScaler Console to synchronize its clock with the NTP server. Configuring an NTP server ensures that the NetScaler Console clock has the same date and time settings as the other servers on the network.

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

To configure an NTP server on NetScaler Console:

1. From the NetScaler Console GUI, navigate to **Settings > Administration**. In the **System Administration** page, under **Network Configurations**, click **NTP Servers**. Then click **Add**.
2. On the **Create NTP Server** page, enter the following details:
    - **Server Name/IP Address** –Enter the domain name or IP address of the NTP server. The name or IP address cannot be changed after you have added the NTP server.
    - **Minimum Poll Interval** –Specify the minimum value for the interval between transmitted NTP messages, in seconds as a power of 2. For example, if you want the minimum poll interval to be 64 seconds, which can be expressed as 2^6, enter 6
    - **Maximum Poll Interval** –Specify the maximum value for the interval between transmitted NTP messages, in seconds as a power of 2. For example, if you want the maximum poll interval to be 256 seconds, which can be expressed as 2^8, enter 8.
    - **Key Identifier** - Enter the key identifier that can be used for symmetric key authentication with the NTP server. Do not add a key identifier if you choose to select Autokey. To find the key identifier, see your NTP server's documentation.
    - **Autokey** - Select **Autokey** if you want to use public key authentication with the NTP server. Do not select if you want to add a key identifier.
    - **Preferred** –Select this option if you want to specify this NTP server as the preferred server for clock synchronization. This applies only if more than one server is configured.
3. Click **Create**.

To enable NTP synchronization on NetScaler Console:

1. Navigate to the **NTP Servers** home page.
2. Click **NTP Synchronization** and select the **Enable NTP Synchronization** checkbox.
3. Click **OK**.

   A confirmation window appears to restart NetScaler Console. Click **Yes** to continue.

Configure system settings

September 27, 2025

Before you start using NetScaler Console to manage and monitor your instances and applications, it is recommended that you configure a few system settings ensure optimal performance of your NetScaler Console server.

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

Configure system alarms

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 a syslog message.

To configure system alarms:

1. Navigate to **Settings > SNMP**, and then click the **Alarms** tab on the upper-right corner.
2. Select the alarm you want to configure, and click **Edit**.
3. On the **Configure Alarm** page, select the alarm severity, and set the Threshold.
4. To view the alarms that have breached the threshold or for which an event has occurred, navigate to **Settings > Auditing** and click **Syslog Messages**.

Configure system notifications

You can send notifications to select groups of users for various system-related functions. You can set up a notification server in NetScaler Console, and you can configure email and Short Message Service (SMS) gateway servers to send email and text notifications to users. Setting notification ensures that you are notified of any system-level activities such as user login or system restart.

To configure system notifications:

1. Navigate to **Settings > Administration**. In the **System Administration** page, under **Event Notifications**, click **Configure Event Notification and Digest > Event Notification**.
2. On the **Configure System Notification Settings** page, select the category or category of events generated by NetScaler Console.
3. Then, configure either the email server or the SMS server to receive notification through email or SMS or both.

Configure system backup settings

NetScaler Console automatically backs up the system every day at 00:30 hours. By default, it saves three backup files. You might want to retain more number of backups of the system. You can also encrypt the backup file. You can also choose to save the backup on an external server.

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

To configure system backup settings:

1. Navigate to **Settings > Administration**.
2. Under **Backup**, click **Configure System and Instance backup**.
3. Click **System** and on the **Configure System Backup Settings** page, specify the required values.

Configure instance backup settings

If you back up the current state of a NetScaler instance, you can use the backup files to restore stability if the instance becomes unstable. Doing so is especially important before performing an upgrade. By default, a backup is taken every 12 hours and three backup files are retained in the system.

To configure instance backup settings:

1. Navigate to **Settings > Administration**.
2. Under **Backup**, click **Configure System and Instance backup**.
3. Click **Instance**, under **Configure Instance Backup Settings**, and specify the required values.

Enable or disable NetScaler Console features

As an administrator, you can enable or disable the following features in the **Settings > Administration > 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 service redistributes the NetScaler instances of the inactive agent with other active agents. For more information, see Configure on-prem 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.
- **Instance configuration audit** - Monitor configuration changes across managed NetScaler instances, troubleshoot configuration errors, and recover unsaved configurations.
- **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.

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

- **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.

To enable a feature, perform the following steps:

1. Select the feature from the list that you want to enable.
2. Click **Enable**.

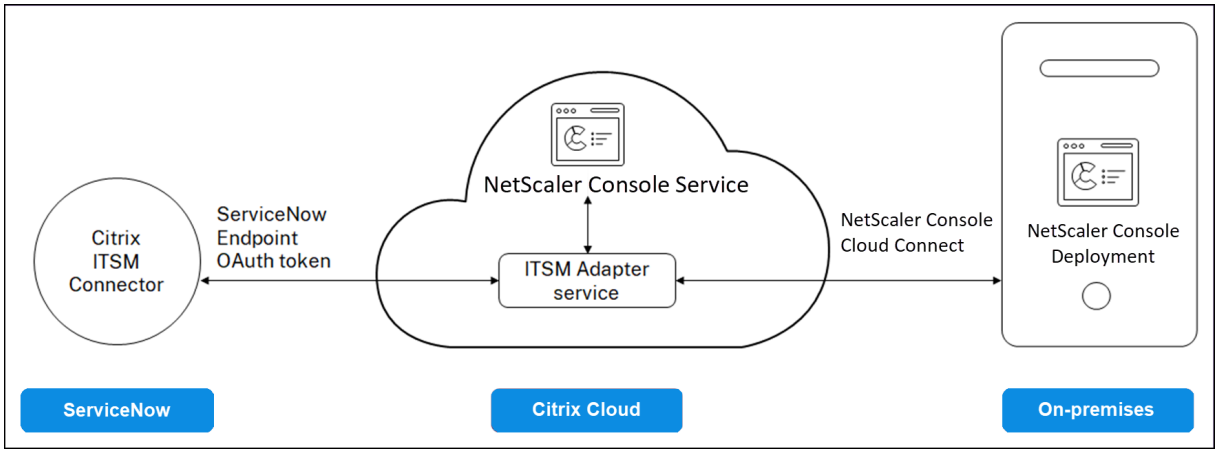
> **Important**
>
> If a feature is disabled, the user cannot perform the operations associated with that feature.

Integrate NetScaler Console with the ServiceNow instance

September 27, 2025

When you want to enable ServiceNow notifications for NetScaler and NetScaler Console events, integrate NetScaler Console with the ServiceNow instance. This integration uses Citrix ITSM connector to communicate between NetScaler Console and the ServiceNow instance.

The ServiceNow integration with NetScaler Console uses the ITSM Adapter service for token based authentication. To do so, it creates an endpoint instance in ServiceNow. For more information, see How ITSM Adapter works.



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

To connect your NetScaler Console on-prem deployment with an ITSM adapter, ensure that you have configured Cloud Connect. For more information, see Cloud Connect.

For ServiceNow integration with NetScaler Console build 14.1 4.x or earlier, ensure to configure customer identity. For more information, see, Configure customer identity.

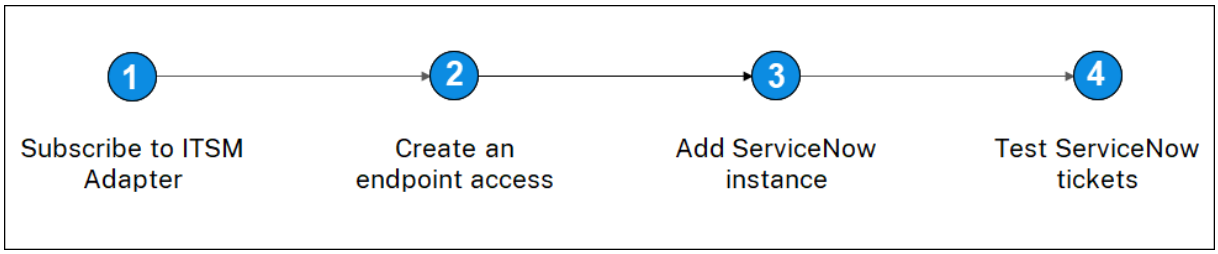
Prerequisites

Before you integrate NetScaler Console with ServiceNow, ensure the following:

1. Sign Up for Citrix Cloud. Make sure you have access to manage Citrix Cloud administrators. For more information, see Manage Citrix Cloud administrators.

How to integrate NetScaler Console with ServiceNow?

Perform the following steps to integrate NetScaler Console with ServiceNow using the ITSM connector:

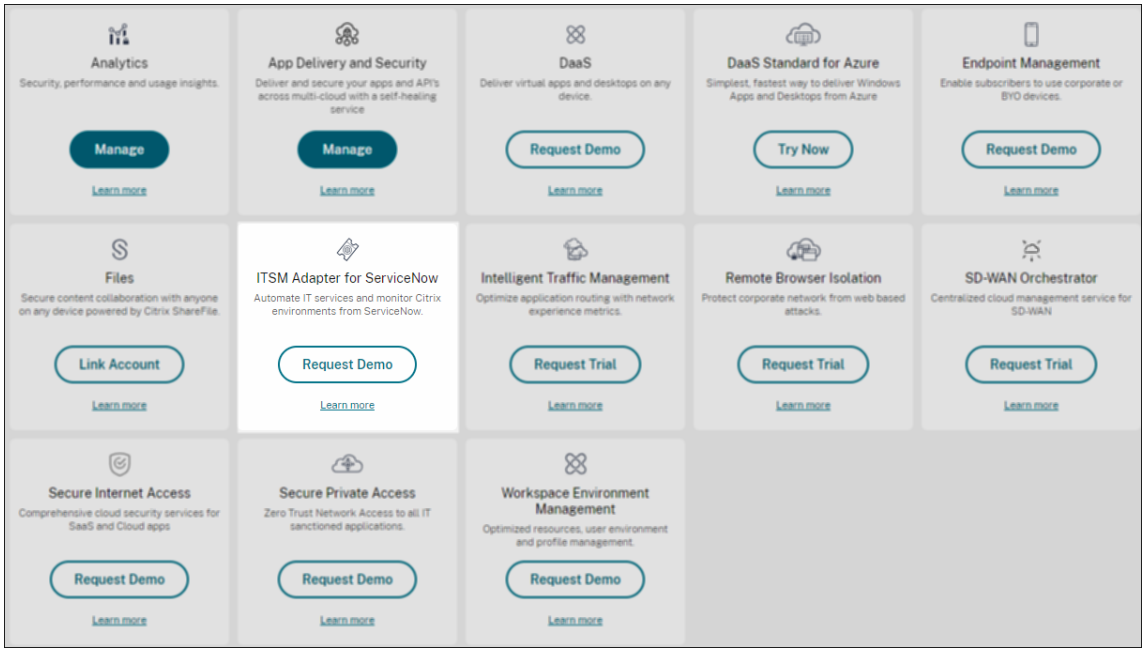


1. Subscribe to ITSM Adapter service in Citrix Cloud™.
2. Create an endpoint access in the ServiceNow instance.
3. Add a ServiceNow instance.
4. Test auto-generation of ServiceNow tickets in NetScaler Console.

Step 1 - Subscribe to ITSM Adapter service in Citrix Cloud

1. On the **ITSM Adapter** tile, click **Request Trial**.

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

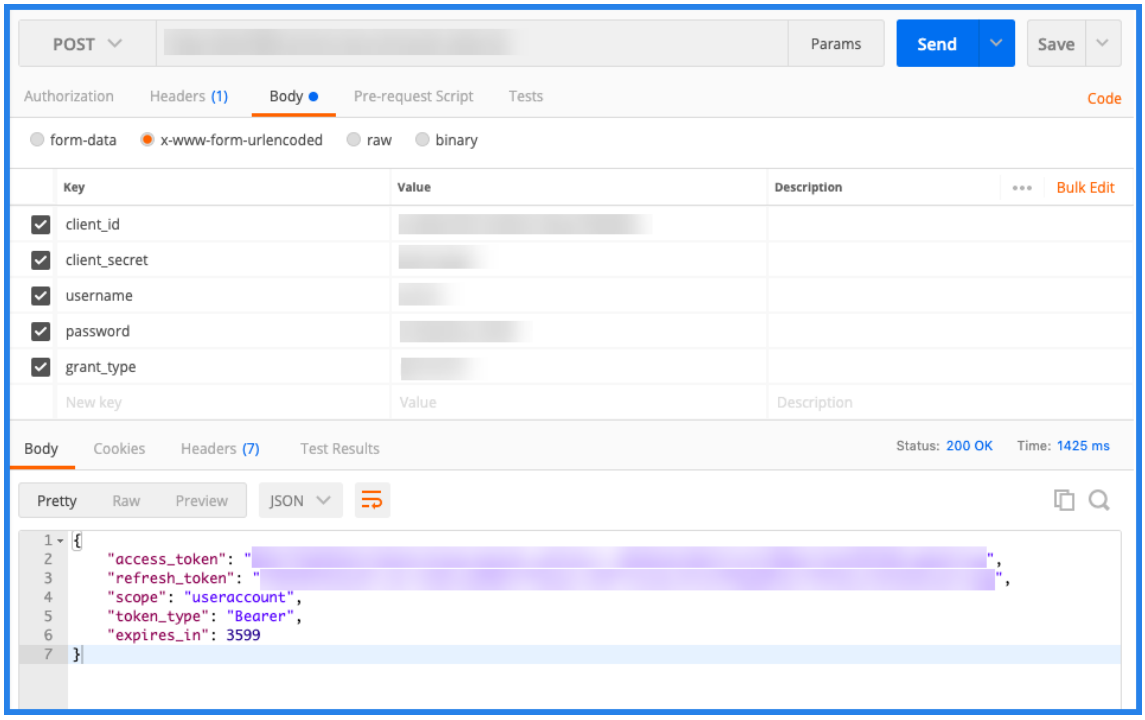


2. Navigate to **Identity Access and Management** > **API Access** and note the **Client ID** and **Client Secret** information.

Step 2 - Create an endpoint access in the ServiceNow instance

1. Log in to your ServiceNow instance with an administrator credentials.
2. Go to ServiceNow store. Download and install the **Citrix ITSM connector**.
3. On the **Citrix ITSM Connector** pane, select **Home** and then click **Authenticate**. Type the Client ID and Secret that you have noted from Citrix Cloud.
4. Test the connection.
5. Save the configuration. An acknowledgment from ServiceNow appears indicating that the connection is active.
6. Create an endpoint to access a ServiceNow instance. See Create an endpoint for clients to access the instance.
7. Obtain the Access and Refresh tokens using the Client ID and Client Secret. See OAuth tokens.

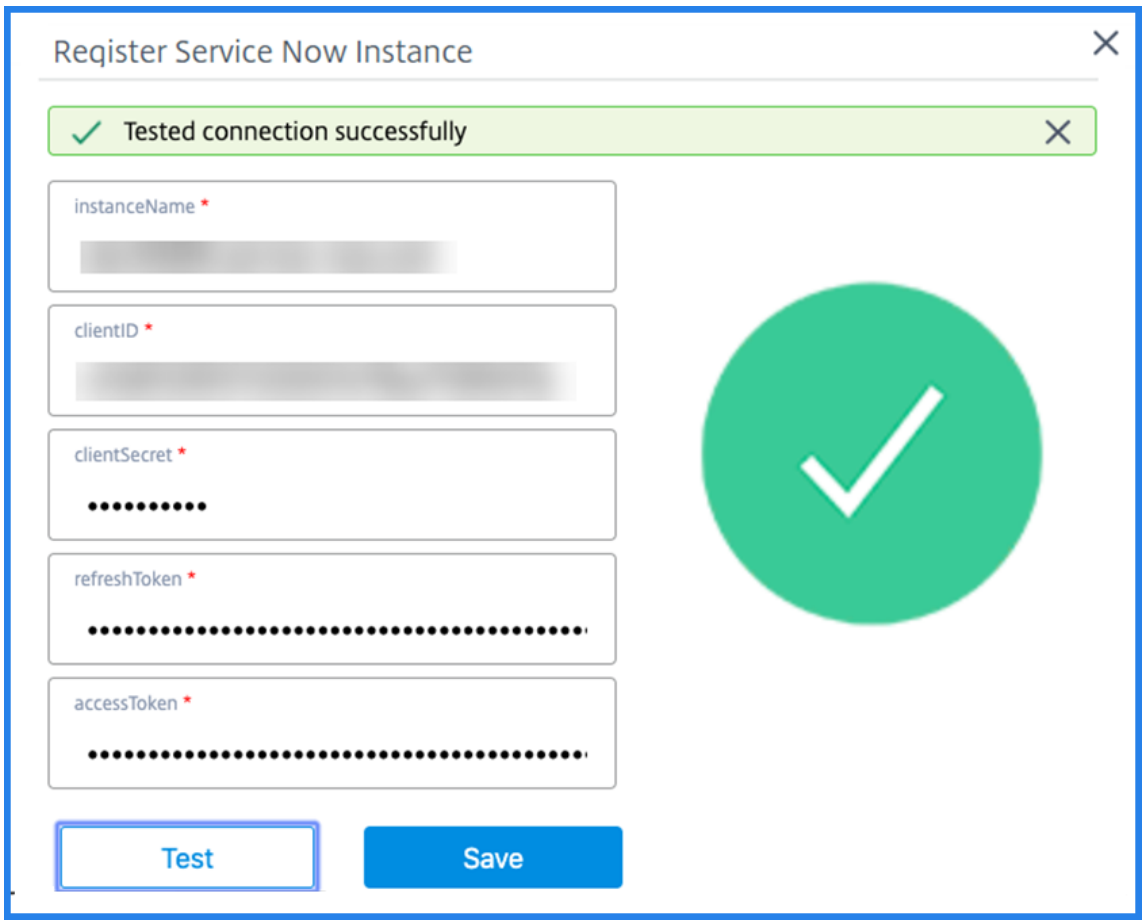
© 1997–2025 Citrix Systems, Inc. All rights reserved.



Step 3 - Add a ServiceNow instance

1. In the **Manage** tab, select Add ServiceNow Instance.
2. Specify the **Instance Name**, **Client ID**, **Client Secret**, **Refresh Token**, and **Access Token**.
3. Click **Test**.

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



The ServiceNow instance is now connected to the ITSM Adapter service.

4. After testing the connection successfully, click **Save** to add a ServiceNow instance.

Step 4 - Test auto-generation of ServiceNow tickets in NetScaler Console

1. Log in to NetScaler Console.
2. Navigate to **Account > 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**.

Set ServiceNow notifications in NetScaler Console

After the ServiceNow instance is registered on the ITSM adapter, you can set up ServiceNow notifications for the following events in the NetScaler Console GUI:

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

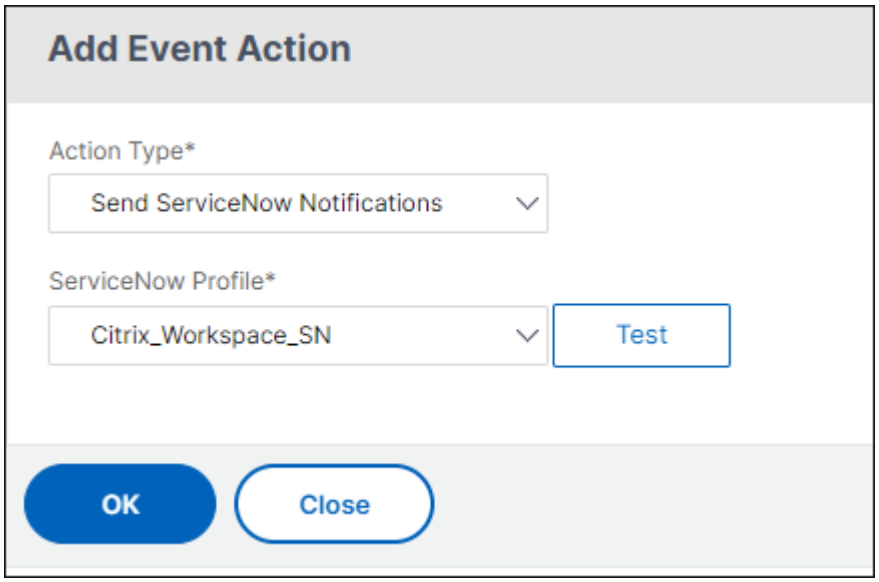
> **Important**
>
> This feature is supported on ServiceNow Cloud.

- **NetScaler events**: NetScaler Console can generate the ServiceNow incidents for the selected set of NetScaler events from selected managed NetScaler instances.

  To send ServiceNow notifications for NetScaler events from the managed instances, you must configure an event rule and assign the rule action as **Send ServiceNow Notifications**.

  Create an event rule on the NetScaler Console by navigating to **Infrastructure > Events > Rules**. For more information, see Send ServiceNow notifications.

- **Application Analytics**: NetScaler Console can generate ServiceNow incidents for the applications that breach the specified threshold.



  In this example, a ServiceNow incident is generated when the App score of applications falls under 90.

- **The SSL certificate and NetScaler Console license events**: NetScaler Console can generate the ServiceNow incidents for the SSL certificate expiry and NetScaler Console license expiry events.

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

  To send ServiceNow notifications for a NetScaler Console license expiry, see The NetScaler Console license expiry.

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

Export or schedule export reports

September 27, 2025

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 **Network > Instances > NetScaler** and click the export icon. You can export these reports in PDF, JPEG, PNG, and CSV file format.

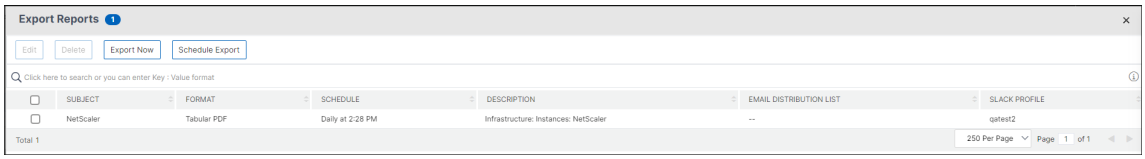
In **Export Reports**, you can perform the following actions:

- 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



4. Select the file format that you want to save the report on your local computer.
5. Click **Export**.

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

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**.
3. Click **Schedule**.



View and edit the scheduled export reports

To view the export reports, perform the following:

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

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**.

Upgrade

November 25, 2025

Each NetScaler Console release offers new and updated features with increased functionality. We recommend you upgrade NetScaler Console to the latest release to avail of the new features and bug fixes. A comprehensive list of enhancements, known issues, and bug fixes is included in the release notes accompanying every release announcement. It is also important to understand the licensing framework and the types of licenses that can be used before you start to upgrade. For NetScaler Console licensing information, see Licensing.

Before you upgrade

Download the upgrade package from the NetScaler Console Downloads page and follow the instructions in this article to upgrade your system to the latest 14.1 build. After the upgrade process begins, NetScaler Console restarts and the existing connections are terminated and reconnected when the upgrade completes. The existing configuration is preserved, but NetScaler Console does not process any data until the upgrade completes.

> **Important**
>
> The NetScaler Console version and build should be **equal to or higher** than your NetScaler version and build. For example, if you have installed NetScaler Console 12.1 Build 50.39, then ensure you have installed NetScaler 12.1 Build 50.28/50.31 or earlier.

Points to note before upgrading to 14.1:

- If you upgrade from version 11.1 or version 12.0 56.x and previous builds, perform the following steps:

  1. Upgrade from the existing version to 12.0 build 57.24.
  2. Upgrade to the latest build of version 12.1.
  3. Upgrade to version 13.1.
  4. Upgrade to version 14.1.

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

- If you upgrade from 12.0 build 57.24 and higher, first upgrade to 12.1, then to 13.1, and then to 14.1.
- If you upgrade from 12.1, you must first upgrade to 13.0 64.xx, and then directly to 14.1
- If you upgrade from versions lower than 13.0 64.xx, for better user experience, first upgrade to 13.0 64.xx and then to 14.1.
- To upgrade from version 13.1 to version 14.1, first upgrade to the latest build of version 13.1 and then upgrade to version 14.1.
- After the successful upgrade to 14.1 and you login to the GUI, it recommends you to change the password if you are using the default password.

Important points to note before upgrading to 14.1 xx.xx and later

When you upgrade the NetScaler Console to version 14.1 xx.xx, your NetScaler Console database is also migrated. This data migration happens because NetScaler Console now uses PostgreSQL version 10.11.

> **Note:**
>
> Downgrading the NetScaler Console is unsupported. Do not attempt to downgrade.

Recommended precautions:

- Take a snapshot of the NetScaler Console server for each upgrade, if you are upgrading to 14.1 xx.xx and later.
- Back up the NetScaler Console server before you upgrade.
- After the upgrade, you might have to reestablish connections between the NetScaler Console server and the managed instances. A confirmation prompt warns you that connections can fail if you proceed.
- For NetScaler Console servers in high availability setup, when upgrading, do not make any configuration changes on either of the nodes.

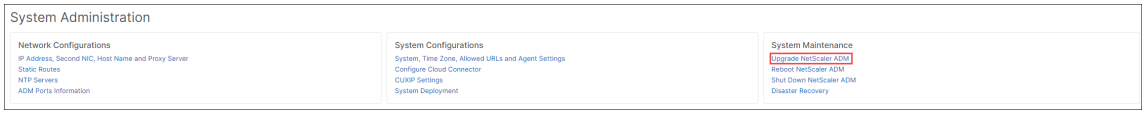
  > **Warning:**
  >
  > Do not refresh the browser until the upgrade process is successfully completed. Check the GUI for the approximate time for the upgrade to complete.

Upgrade a single NetScaler Console server to 14.1 xx.xx

1. Log on to NetScaler Console with administrator credentials.

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

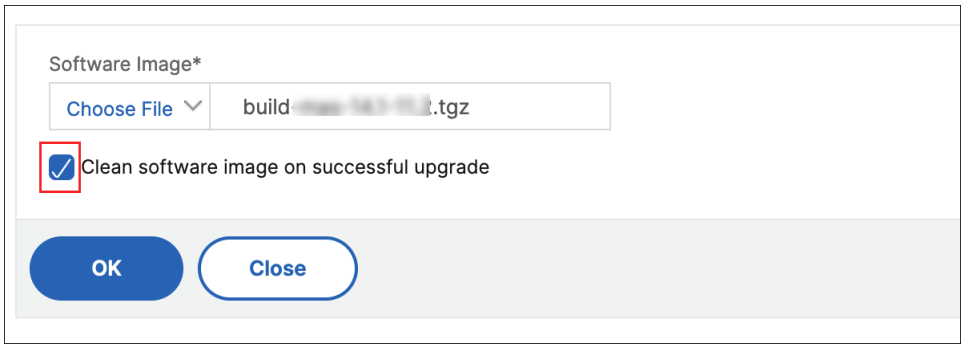
2. Navigate to **Settings** > **Administration**. Under **System Maintenance**, click **Upgrade NetScaler Console**.



3. On the **Upgrade NetScaler Console** page, select the **Clean software image on successful upgrade** checkbox to delete image files after upgrade. Selecting this option removes the NetScaler Console image files automatically upon upgrade.

> **Note:**
>
> This option is selected by default. If you do not select this checkbox before starting the upgrade process, you must manually delete the images.

4. You can then upload a new image file by selecting either **Local** (your local machine) or **Appliance**. The build file must be present on the NetScaler Console virtual appliance.



5. Click **OK**.
   The Confirm dialog box is displayed. Click **Yes**.

   The upgrade process starts.

After your configuration is migrated, you can log on to the NetScaler Console GUI. Upon logon, the historical data starts to migrate at the background while you can continue to work on NetScaler Console.

During historical data migration, some of the old data might not be available. The time taken to migrate your database depends on the size of data and the number of tables.

You can monitor the database migration using the NetScaler Console GUI. Click **View upgrade progress** and the **Database Migration Status** appears.

Upgrade a high availability pair to 14.1 release

For NetScaler Console servers in a high availability mode, you can upgrade by either accessing the active node or the floating IP address. Both the NetScaler Console servers are automatically upgraded

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

to the latest build once you initiate the upgrade process in either of the servers.

Upgrade NetScaler Console disaster recovery deployment

> **Note:**
>
> - Ensure that the password is same for both HA pair and disaster recovery node.
> - Upgrade the Disaster Recovery node only after upgrading the standalone node or HA node. If you upgrade the Disaster Recovery node before upgrading the primary or HA node, you might observe database synchronization issues.

Upgrading NetScaler Console disaster recovery deployment is a two-step process:

- Upgrade the NetScaler Console nodes configured in high availability mode in the primary site. Later you must upgrade the disaster recovery node.
- Ensure that you have upgraded the NetScaler Console servers that are deployed in high availability, before upgrading the disaster recovery node.

Upgrade the NetScaler Console disaster recovery node

1. Download NetScaler Console upgrade image file from NetScaler site.
2. Upload this file to the disaster recovery node using `nsrecover` credentials.
3. Log on to the disaster recovery node using the `nsrecover` credentials.
4. Navigate to the folder where you placed the image file and unzip the file.
5. Run the following script:

   ./installmas

Upgrade on-prem agents for multisite deployment

Upgrading NetScaler agent deployment is a three-step process.
Ensure that you have completed the following tasks before upgrading the on-prem agents:

1. Upgrade the NetScaler Console servers that are deployed in high availability.
2. Upgrade the NetScaler Console disaster recovery node.

   For more information, see Upgrade NetScaler Console disaster recovery deployment.

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

Upgrade the on-prem agent

1. Download NetScaler agent upgrade image file from NetScaler site.
2. Upload this file to the agent node using `nsrecover` credentials.
3. Ensure that you download the correct agent upgrade image.
4. Log on to the on-prem agent using the `nsrecover` credentials.
5. Navigate to the folder where you placed the image file and unzip the file.

```
login as: nsrecover
Using keyboard-interactive authentication.
Password:
Last login: Thu Aug 30 08:50:48 2018 from 10.252.241.37
bash-3.2# cd /var/mps/mps_images/
bash-3.2# tar zxvf build-masagent-12.1-502.109.tgz
```

6. Run the following script:

   `./installmasagent`

```
bash-3.2# ./installmasagent
```

Add an extra disk to the NetScaler Console server

If your NetScaler Console storage requirement exceeds the default disk space (120 GB), you can attach an extra disk. You can attach more disk in both single-server and high availability deployments.

When you upgrade NetScaler Console from release version 12.1–13.10, the partitions that you had created on the additional disk in the earlier version remain the same. The partitions are not removed or resized.

The procedure to attach more disk remains the same in the upgraded build. You can now use the new disk partitioning tool in NetScaler Console to create partitions in the newly added disk. You can also use the tool to resize the partitions in the existing more disk. For more information on how to attach more disks and to use the new disk partitioning tool, see How to attach an extra disk to NetScaler Console.

Authentication

September 27, 2025

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

Users can be authenticated either internally by NetScaler Console, externally by an authenticating server, or both. If local authentication is used, the user must be in the NetScaler Console security database. If the user is authenticated externally, the user "external name"must match the external user identity registered with the authenticating server, depending on the selected authentication protocol.

NetScaler Console supports external authentication by RADIUS, LDAP, and TACACS servers. This unified support provides a common interface to authenticate and authorize all the local and external Authentication, Authorization, and Accounting server users who are accessing the system. NetScaler Console can authenticate users regardless of the actual protocols they use to communicate with the system. When a user attempts to access a NetScaler Console implementation that is configured for external authentication, the requested application server sends the user name and password to the RADIUS, LDAP, or TACACS server for authentication. If the authentication is successful, the user is granted access to NetScaler Console.

External authentication servers

NetScaler Console sends all authentication, authorization, and auditing service requests to the remote RADIUS, LDAP, or TACACS server. The remote authentication, authorization, and auditing server receive the request, validates the request, and sends a response to NetScaler Console. When configured to use a remote RADIUS, TACACS, or LDAP server for authentication, NetScaler Console becomes a RADIUS, TACACS, or LDAP client. In any of these configurations, authentication records are stored in the remote host server database. The account name, assigned permissions, and time-accounting records are also stored on the authentication, authorization, and auditing server for each user.

Also, you can use the internal database of NetScaler Console to authenticate users locally. You create entries in the database for users and their passwords and default roles. You can also select the authentication order for specific types of authentication. The list of servers in a server group is an ordered list. The first server in the list is always used unless it is unavailable, in which case the next server in the list is used. You can configure servers to include the internal database as a fallback authentication backup to the configured list of authentication, authorization, and auditing servers.

You can configure and add the following servers in NetScaler Console:

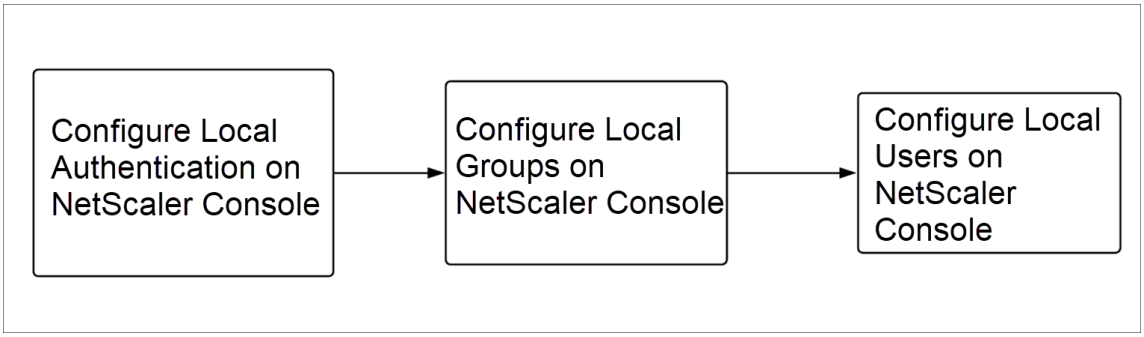
- LDAP authentication server
- RADIUS authentication server
- TACACS authentication server
- Enable external authentication servers and fallback options
- Two factor authentication (2FA) support with LDAP, RADIUS, and TACACS

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

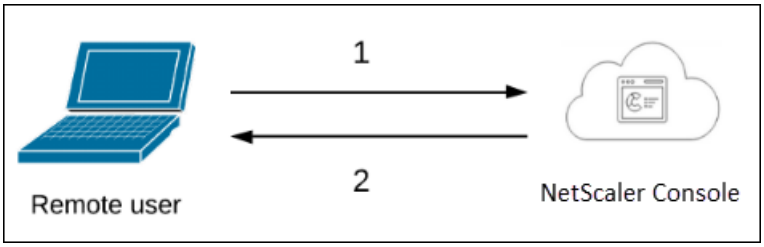
Authenticate users in NetScaler Console

You can authenticate your users in NetScaler Console in two ways:

- Local users configured in NetScaler Console



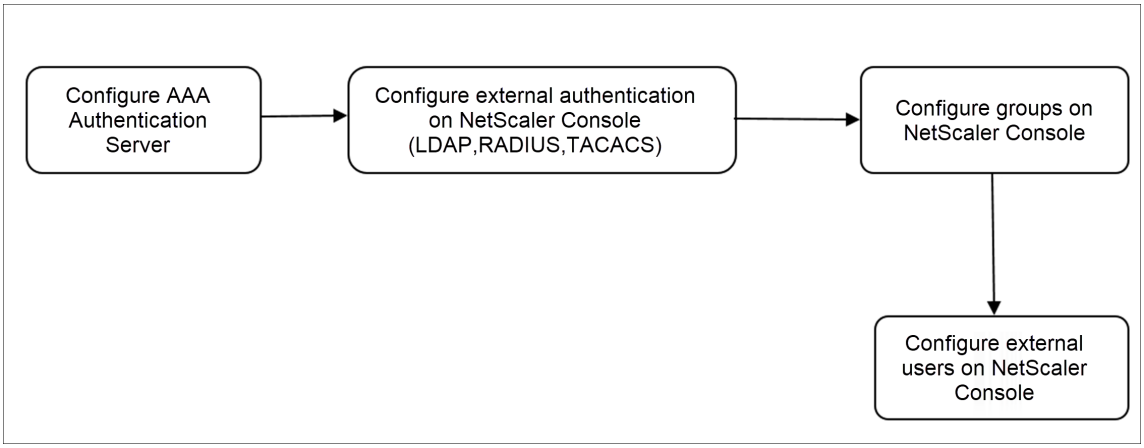
After configuration, the following is the workflow for user authentication in the local server.



1 –The user logs on to NetScaler Console

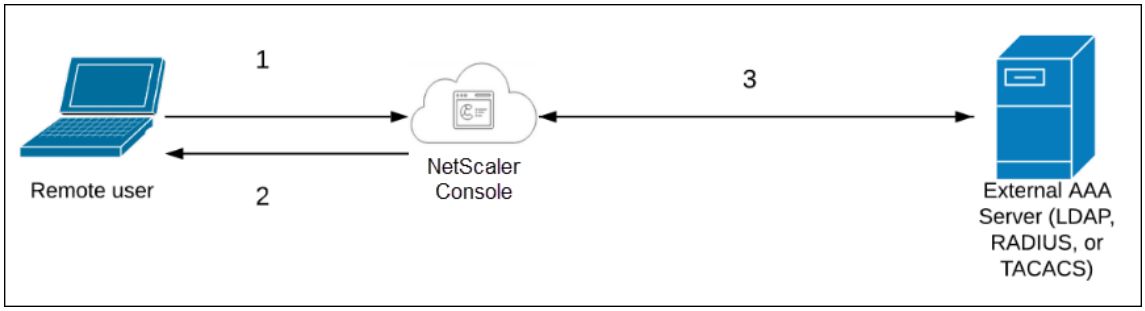
2 –NetScaler Console prompts the users for credentials for authentication and checks if the credentials match in the NetScaler Console database.

- Using external authentication servers



After configuration, the following is the workflow for user authentication in the external authentication, authorization, and auditing server:

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



1 –The user connects with NetScaler Console

2 –NetScaler Console prompts the user for credentials

3 –NetScaler Console validates the user credentials with the external authentication, authorization, and auditing server. If the validation is successful, the user can continue to log on

Add LDAP authentication server

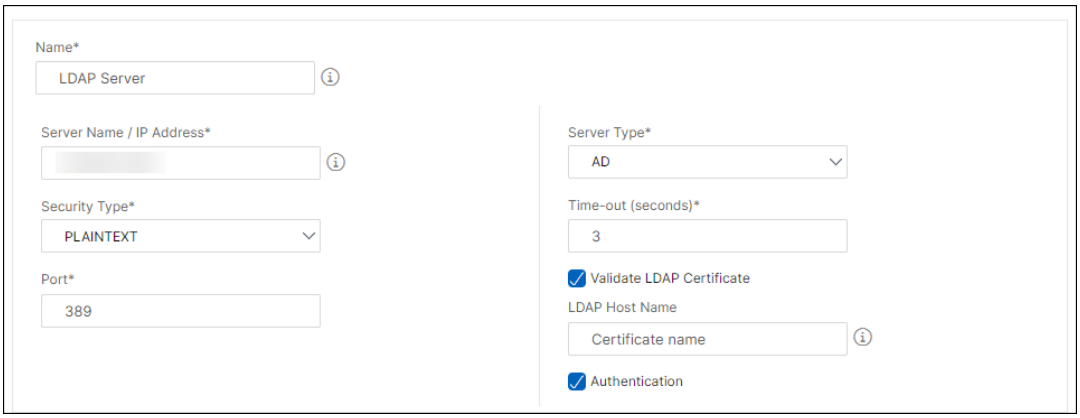
September 27, 2025

When you integrate LDAP protocol with RADIUS and TACAS authentication servers, you can use NetScaler Console to search and authenticate user credentials from distributed directories.

1. Navigate to **Settings > Authentication**.
2. Select the **LDAP** tab and then click **Add**.
3. On the **Create LDAP Server** page, specify the following parameters:
    a) **Name** –Specify the LDAP server name
    b) **Server Name/IP address** –Specify the LDAP IP address or server name
    c) **Security Type** –Type of communication required between the system and the LDAP server. Select from the list. If plain text communication is inadequate, you can choose encrypted communication by selecting either Transport Layer Security (TLS) or SSL
    d) **Port** –By default, port 389 is used for PLAINTEXT. You can also specify port 636 for SSL/TLS
    e) **Server Type** –Select Active Directory (AD) or Novell Directory Service (NDS) as the type of LDAP server
    f) **Time-out (seconds)** –Time in seconds for which the NetScaler Console system waits for a response from the LDAP server
    g) **LDAP Host Name** –Select Validate LDAP Certificate check box and specifying the host name to be entered on the certificate

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

Clear the **Authentication** option and specify the SSH Public Key. With key-based authentication, you can now fetch the list of public keys that are stored on the user object in LDAP server through SSH.



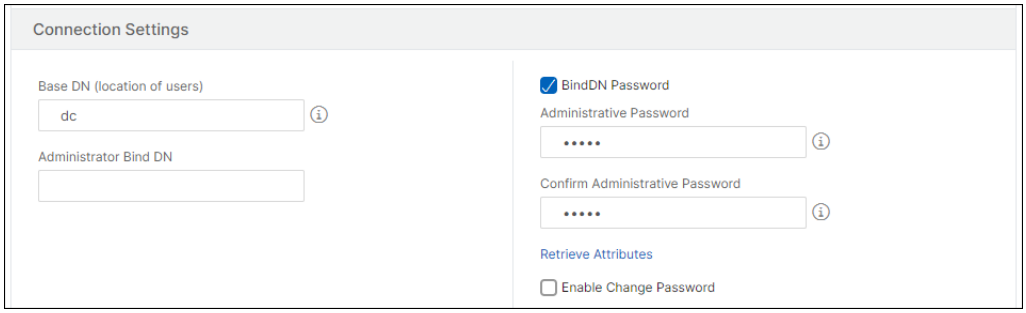
Under Connection Settings, specify the following parameters:

i. **Base DN** –The base node for LDAP server to start the search

ii. **Administrator Bind DN** –User name to it bind to LDAP server. For example, admin@aaa.local.

iii. **Bind DN password** –Select this option to provide a password for authentication

iv. **Enable Change Password** –Select this option to enable password change



Under **Other Settings**, specify the following parameters

i. **Server Log on Name Attribute** –Name attribute used by the system to query the external LDAP server or an Active Directory. Select **samAccountname** from the list.

ii. **Search Filter** –Configure external users for two-factor authentication according to the search filter configured in LDAP server. For example, vpnallowed=true with ldaploginame `samaccount` and the user-supplied user name bob would yield an LDAP search string of: &(`vpnallowed`=**`true`**)(`samaccount`=`bob`).

> Note

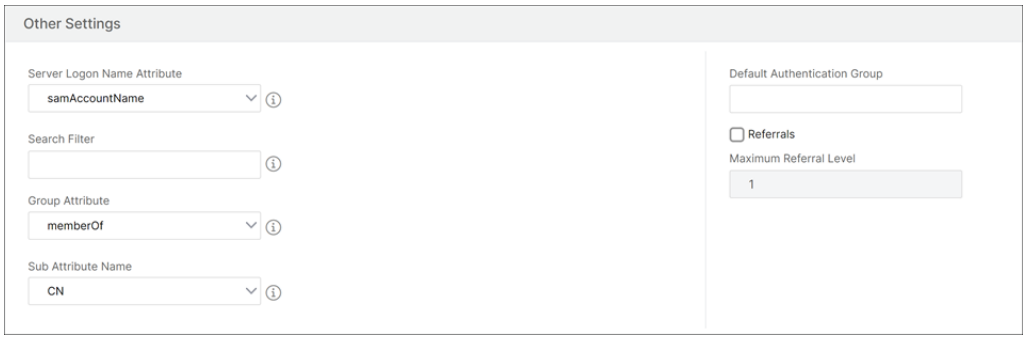
© 1997–2025 Citrix Systems, Inc. All rights reserved.

> By default, the values in the search filter are enclosed in brackets.

iii. **Group Attribute** –Select memberOf from the list.

iv. **Sub Attribute Name** –The Sub attribute name for group extraction from the LDAP server.

v. **Default Authentication Group** –Default group to choose when the authentication succeeds in addition to extracted groups.



4. Click **Create**.

   The LDAP server is now configured.

   > **Note**:
   >
   > If the users are Active Directory group members, the group and the users'names on NetScaler Console must have the same names of Active Directory group members.

5. Enable the external authentication servers.

   For more information about enabling external authentication servers, see Enable external authentication servers and fallback options.

Add RADIUS authentication server

September 27, 2025

1. Navigate to **Settings > Authentication**.
2. Select the **RADIUS** tab and then click **Add**.

   On the **Create RADIUS Server** page, specify the following parameters:

   a) **Name** –Specify a RADIUS server name

   b) **Server Name / IP address** –Specify the RADIUS server IP address

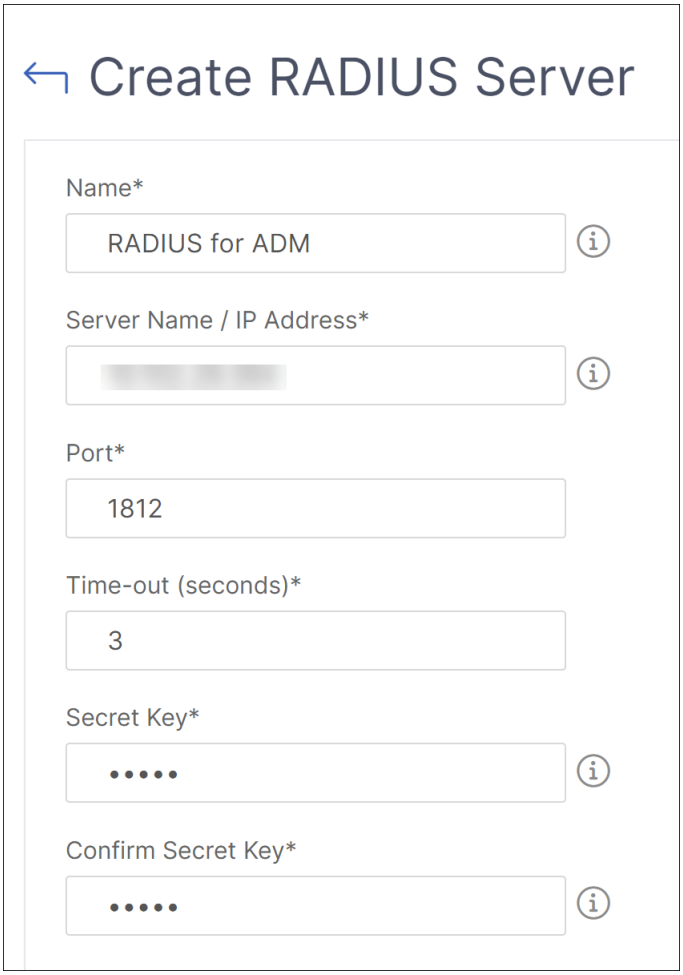
© 1997–2025 Citrix Systems, Inc. All rights reserved.

c) **Port** –Specify the port number on which the RADIUS server is hosted. The default port is 1812

d) **Time-out (seconds)** –Time in seconds for which the NetScaler Console system waits for a response from the RADIUS server

e) **Secret Key** –Specify the RADIUS secret key for authentication

f) **Confirm Secret Key** –Specify the key again for confirmation



Under **Details**, specify the following parameters:

i. **NAS ID** –Specify the ID to send the identifier to RADIUS server

ii. **Group Vendor Identifier** –Specify the vendor ID for using RADIUS group extraction

iii. **Group Prefix** - A string that precedes group names within a RADIUS attribute for RADIUS group extraction

iv. **Group Attribute Type** –Specify the attribute type for RADIUS group extraction

v. **Group Separator** –A string that delimits group names within a RADIUS attribute for RADIUS group extraction

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

vi. **IP Address Vendor Identifier** –Vendor ID in RADIUS denotes the intranet IP. A value of 0 denotes that the attribute is not vendor encoded

vii. **Password Vendor Identifier** –Vendor ID password in RADIUS response to extract the user password

viii. **IP Address Attribute Type** –Remote IP address attribute for the RADIUS to respond

ix. **Password Attribute Type** –The password attribute for the RADIUS to respond

x. **Password encoding** –Select pap, chap, mschapv1, or mschapv2 from the list. This denotes how passwords should be encoded in the RADIUS packets traveling from the system to the RADIUS server.

xi. **Default Authentication Group** –Default group to choose when the authentication succeeds in addition to extracted groups

Select Accounting if you want the appliance to log audit information with RADIUS server.

3. Click **Create**.

   The RADIUS server is now configured.

4. Enable the external authentication servers.

   For more information about enabling external authentication servers, see Enable external authentication servers and fallback options.

Add TACACS authentication server

September 27, 2025

1. Navigate to **Settings > Authentication**.
2. Select the **TACACS** tab and then click **Add**.
3. On the **Create TACACS** page, specify the following parameters:

   a) **Name** –Specify a TACACS server name

   b) **IP address** –Specify the TACACS IP address

   c) **Port** –Specify the port number on which the TACACS server is hosted. The default port is 49

   d) **Time-out (seconds)** –Time in seconds for which the NetScaler Console system waits for a response from the LDAP server

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

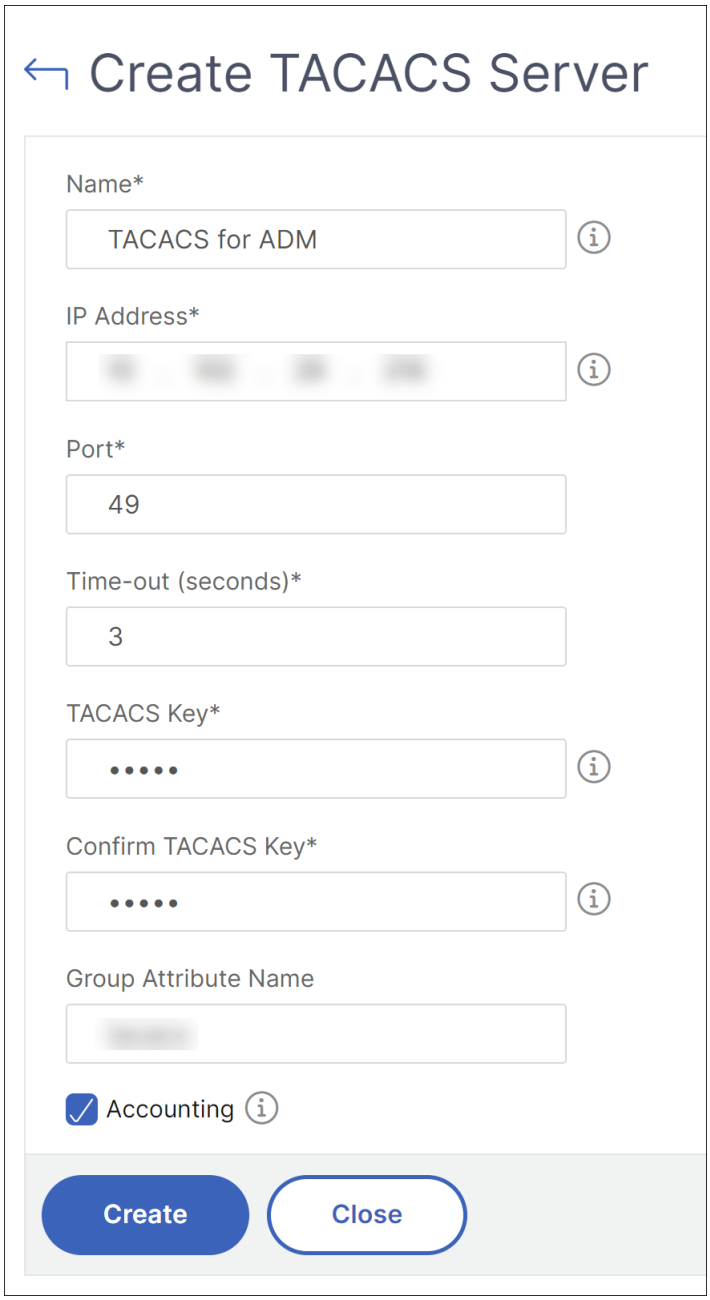
e) **TACACS Key** –Specify the TACACS key for authentication

f) **Confirm TACACS Key** –Specify the TACACS key again for confirmation

g) **Group Attribute Name** –Specify the group name

Select **Accounting** if you want the appliance to log audit information with TACACS server.

4. Click **Create**.



5. Enable the external authentication servers.

For more information about enabling external authentication servers, see Enable external au-

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

thentication servers and fallback options.

Users in NetScaler Console

September 27, 2025

You can create user accounts locally on NetScaler Console to supplement the users on authentication servers. For example, you might want to create local user accounts for temporary users, such as consultants or visitors, without creating an entry for those users on the authentication server.

For more information on configuring users, see Configure Users.

> Note
>
> If the users are on Active Directory, ensure that the group name in NetScaler Console is same as the one for the Active Directory group on the external server.

User Groups in NetScaler Console

NetScaler Console allows you to authenticate and authorize your users by creating groups and adding the users to the groups. A group can have either "admin"or "read-only"permissions and all users in that group will receive equal permissions.

In NetScaler Console:

- A group is defined as a collection of users having similar permissions
- A group can have one or multiple roles
- A user is defined as an entity that can have access based on the permissions assigned
- A user can belong to one or more groups

You can create local groups in NetScaler Console and use local authentication for the users in the groups. If you are using external servers for authentication, configure the groups on NetScaler Console to match the groups configured on authentication servers in the internal network. When a user logs on and is authenticated, if a group name matches a group on an authentication server, the user inherits the settings for the group on NetScaler Console.
If you are using local authentication, create users and add them to groups configured on NetScaler Console. The users then inherit the settings for those groups.

For more information on configuring groups and assigning group permissions, see Configure Groups.

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

Extract an authentication server group

September 27, 2025

> **Note**
>
> TACACS server extraction is supported from **NetScaler Console 13.0**.

NetScaler Console enables you to:

- Extract the list of groups that a user belongs to on the external authentication server.
- Assign them to the group settings that match with the groups configured on the external server.

Advantages:

- You do not have to create users in NetScaler Console, as they are managed on the external server.
- NetScaler Console performs the authorization of users by assigning group permissions to access specific load balancer virtual servers, and for specific applications on the system.

Enable external authentication servers and fallback options

September 27, 2025

Fallback option enables local authentication to take over if the external server authentication fails. A user configured on both NetScaler Console and external authentication server can log on to NetScaler Console, even if the configured external authentication servers are down or not reachable. To ensure fallback authentication work:

- Non-nsroot users must be able to access NetScaler Console if external server is down or not reachable
- You must add at least one external server

NetScaler Console also supports a unified system of authentication, authorization, and accounting (AAA) protocols (LDAP, RADIUS, and TACACS), along with local authentication. This unified support provides a common interface to authenticate and authorize all users and external AAA clients accessing the system.

NetScaler Console can authenticate users regardless of the actual protocols they to communicate with the system.

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

Cascading external authentication servers provides a continuous non-failing process for authenticating and authorizing external users. If authentication fails on the first authentication server, NetScaler Console attempts to authenticate the user by using the second external authentication server, and so on. To enable cascade authentication, you must add the external authentication servers in NetScaler Console. You can add any type of the supported external authentication servers (RADIUS, LDAP, and TACACS).

For example, consider that you want to add four external authentication servers and configured two RADIUS servers, one LDAP server, and one TACACS server. NetScaler Console attempts to authenticate with the external servers, based on the configurations. In this example scenario, NetScaler Console attempts to:

- Connect with the first RADIUS server
- Connect with the second RADIUS server, if the authentication has failed with first RADIUS server
- Connect with the LDAP server, if the authentication has failed with both RADIUS servers
- Connect with the TACACS server, if the authentication has failed with both RADIUS servers and LDAP server.

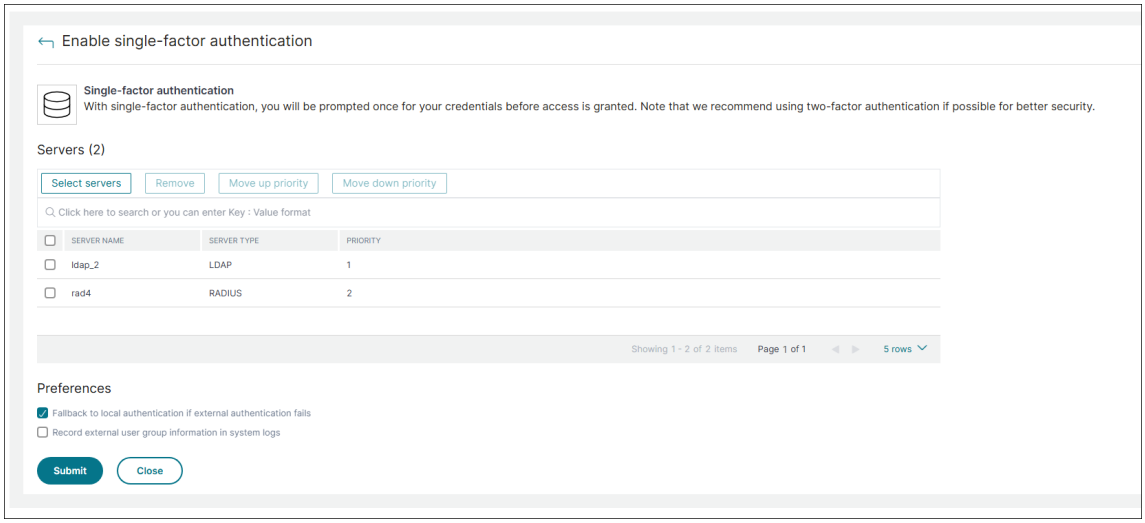
> Note
>
> You can configure up to 32 external authentication servers in NetScaler Console.

Configure fallback and cascade external servers

1. Navigate to **Settings > Authentication > Authentication Settings**.
2. On the **Authentication Settings** page, under **External server authentication**, click **Enable single-factor authentication**.
3. On the **Enable single-factor authentication** page, click **Select servers**. Select one or multiple authentication servers and click **Add**.
4. Select **Fallback to local authentication if external authentication fails** if you want the local authentication to take over when the external authentication fails.
5. Select **Record external user group information in system logs** if you want to capture the external user group information in the system audit log.
6. Click **Submit** to close the page.

   The selected servers are displayed on the **Authentication Settings** page.

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



You can also specify the order of authentication by using the icon next to the server names to move servers up or down the list.

Two factor authentication (2FA) support with LDAP, RADIUS, and TACACS

September 27, 2025

Multifactor authentication is a security best practice today, and most organizations require at least two authentication factors for network appliances to meet compliance standards. Two-factor authentication is a security mechanism by which a product authenticates a user at two levels. Access is granted only after successful validation at both levels.

Starting with NetScaler Console 14.1-43.x and later, two factor authentication (2FA) is supported on NetScaler Console on-premises. You can use LDAP, RADIUS, and TACACS as the authentication factors to NetScaler Console on-premises.

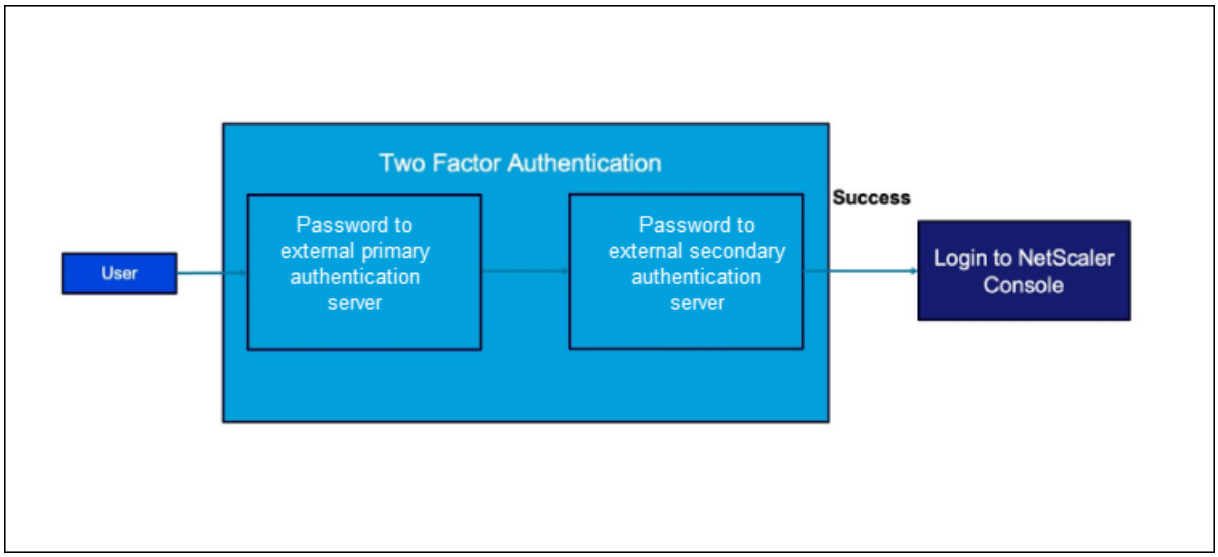
> **Note:**
>
> Two-factor authentication support is available only for external server authentication.

When a user attempts to log in to a NetScaler Console with two-factor authentication enabled, the user is prompted to enter the user name and password for the initial external authentication. Once the initial authentication is successful, the user is prompted for the second level of authentication.

The user is fully authenticated only after both passwords are successfully validated. If the authentication fails, the reason for the failure is displayed to the user.

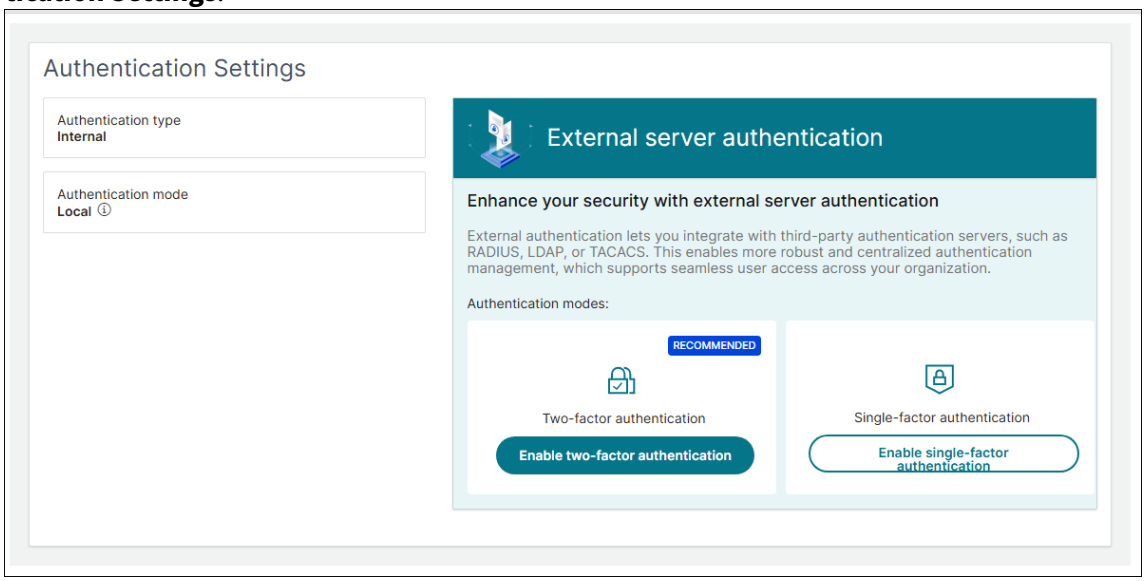
© 1997–2025 Citrix Systems, Inc. All rights reserved.

If a user is authenticated locally, the user profile must be created in the NetScaler Console database. If the user is authenticated externally then, the user name and password must match the user identity registered in the external authentication server.



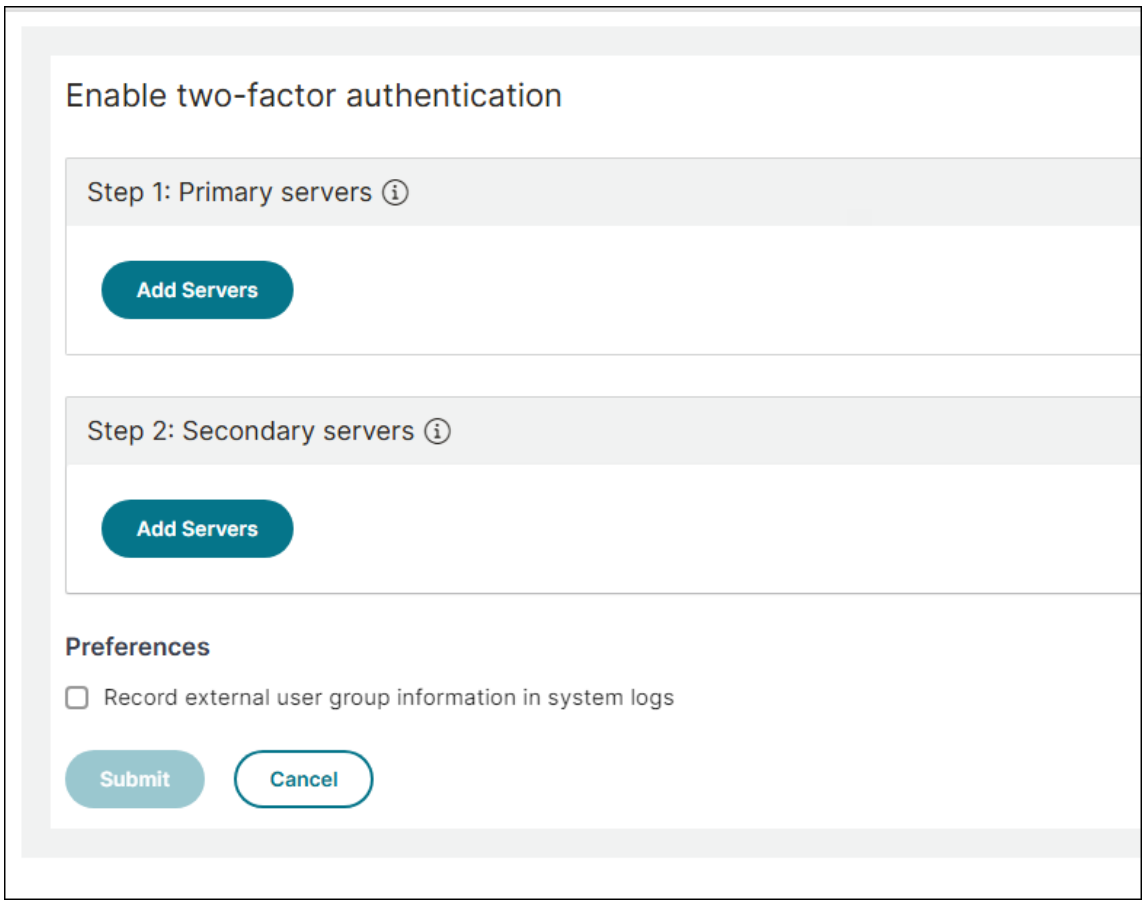
Configure two-factor authentication

1. Log in to NetScaler Console on-premises and navigate to **Settings > Authentication > Authentication Settings**.

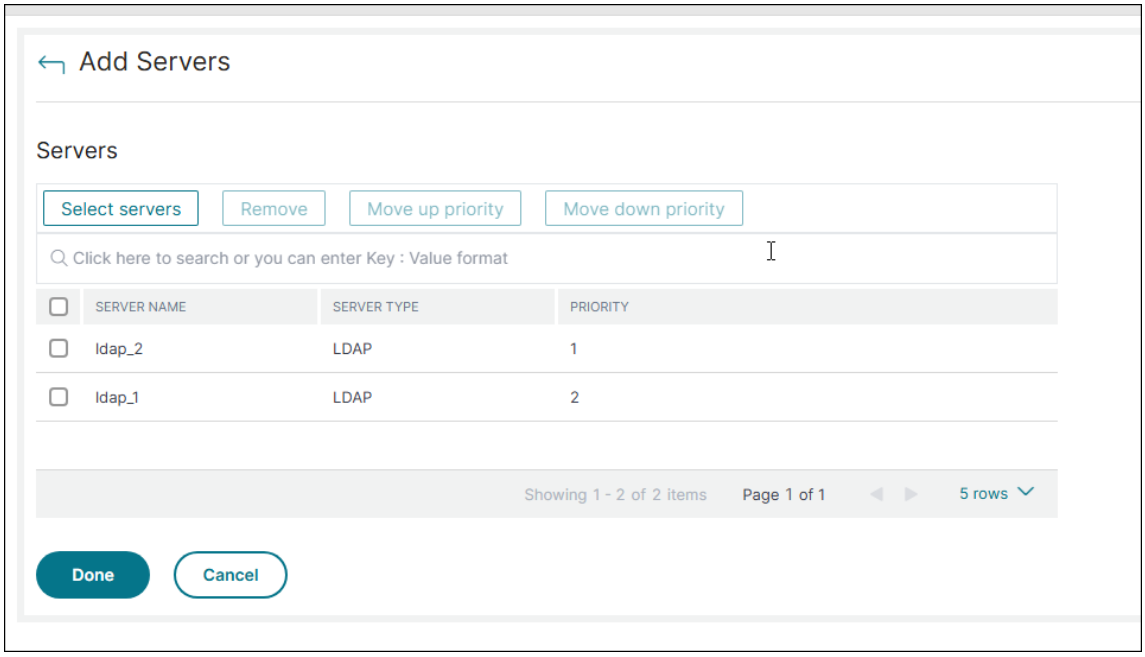


2. In the **External server authentication** section, click **Enable two-factor authentication** under **Authentication modes**.
3. On the **Enable two-factor authentication** page, under **Step 1: Primary servers**, click **Add Servers**.

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



4. Click **Select Servers** and select the required servers. Click **Add** and then click **Done**.

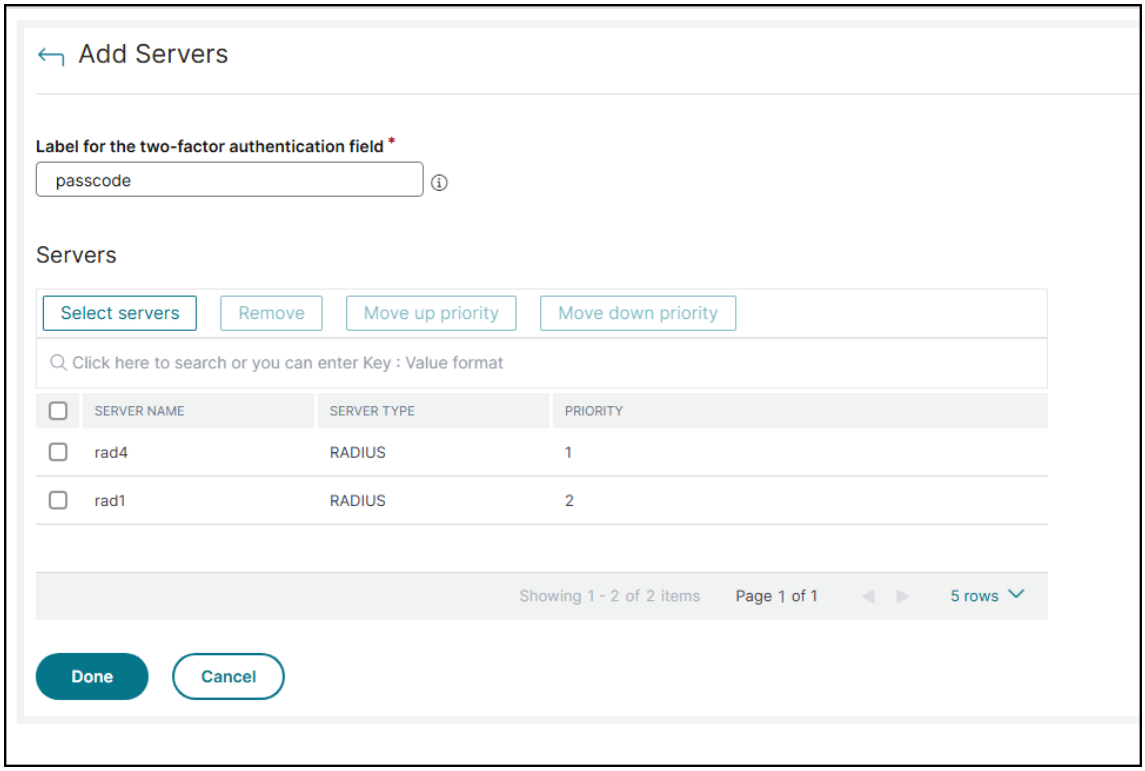


5. On the **Enable two-factor authentication** page, under **Step 2: Secondary servers**, click **Add**

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

Servers.

6. In **Label for the two-factor authentication field**, enter a label that is going to be used for authenticating to the servers configured for second factor authentication.
7. Click **Select Servers** and select the required servers. Click **Add** and then click **Done**.

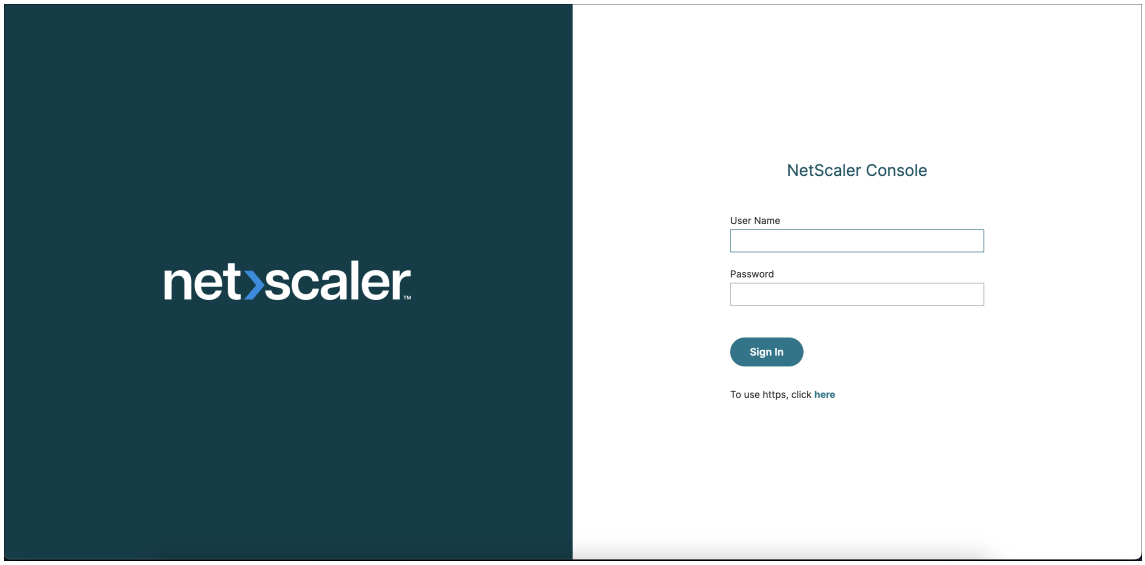


8. Click **Submit**.

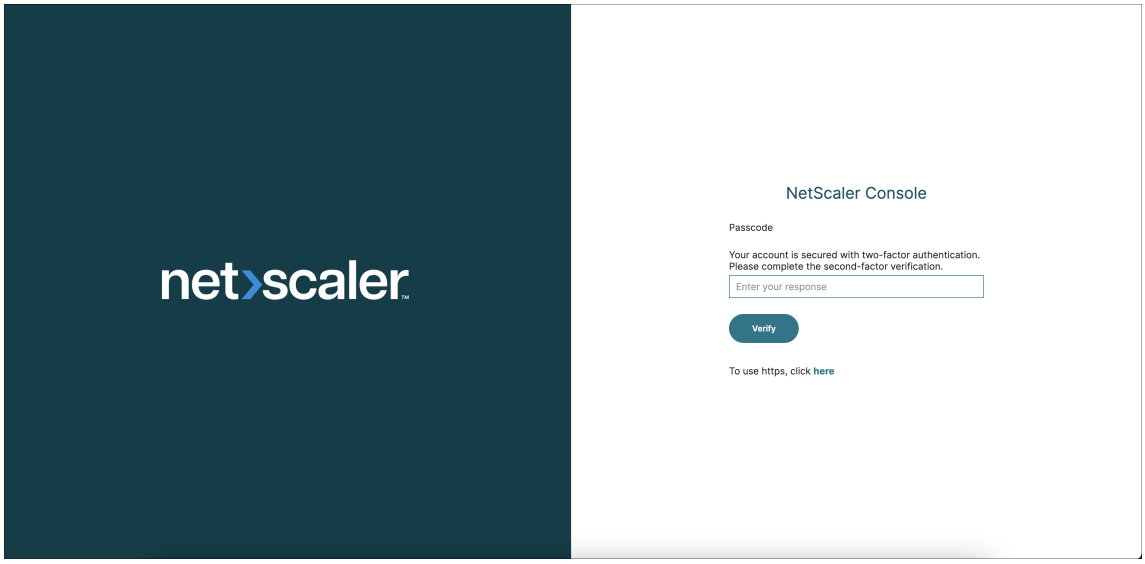
User access to NetScaler® Console with two-factor authentication

1. In a web browser, type the IP address of the NetScaler Console. The login page appears.

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

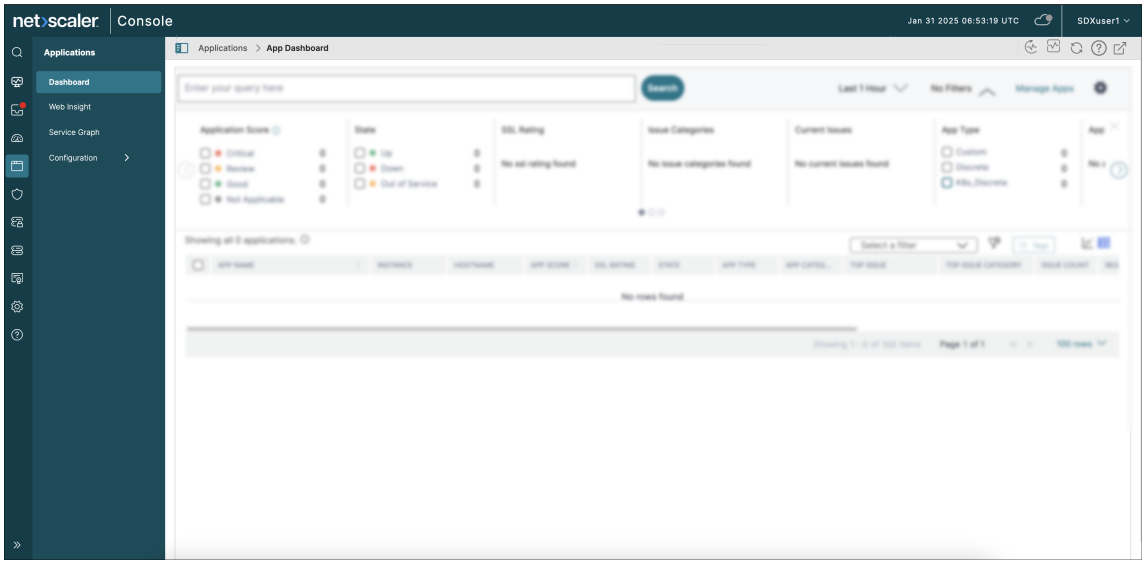


2. Enter the user name and password in the **User Name** and **Password** fields. This step is the first factor authentication.
3. After successful authentication of the first factor, the user is prompted for the second factor authentication. Enter the label that is configured for the second factor authentication.



4. After successful authentication of the second factor, the user is logged into the NetScaler Console GUI.

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



Access Control

September 27, 2025

Authentication is a process by which you verify that someone is who they claim they are. To perform authentication, a user must already have an account created in a system which can be interrogated by the authentication mechanism, or an account must be created as part of the process of the first authentication. NetScaler provides a method for authenticating both local users and external users. While local users are authenticated internally, NetScaler Console supports external authentication with RADIUS, LDAP, and TACACS protocols. When a user attempts to access NetScaler Console that is configured for external authentication, the requested application server sends the user name and password to the RADIUS, LDAP, or TACACS server for authentication. Once authenticated, the required protocol is used to identify the user on NetScaler Console.

Access Control is the process of enforcing the required security for a particular resource. It is a security technique that can be used to regulate who can view or use resources in a computing environment. The purpose of access control is to limit the actions or operations that a legitimate user of a computer system can perform. Access control constrains what a user can do directly, and what programs running on behalf of the users are allowed to do. In this way access control seeks to prevent activity that can lead to a breach of security. Access control assumes that the authentication of the user has been successfully verified prior to enforcement of access control through a reference monitor. NetScaler Console allows fine-grained, role-based access control (RBAC) by which the administrators can provide access permissions to users based on the roles of individual users within an enterprise. RBAC in NetScaler Console is achieved by creating access policies, roles, groups, and users.

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

Role-based access control

September 27, 2025

NetScaler Console provides fine-grained, role based access control (RBAC), with which you can grant access permissions based on the roles of individual users within your enterprise. In this context, 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 creating configuration templates.

Roles are determined by in policies. After creating policies, you 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 or 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 Certificate management and monitoring features, but must have read-only access for system administration operations. An application administrator must be able to access only the resources within the scope.

Example:

Chris, the NetScaler group head, is the super administrator of NetScaler Console in his organization. Chris 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 also have read-only access for system administration operations.

Steve, an application admin, needs access to only specific applications and only specific configuration templates.

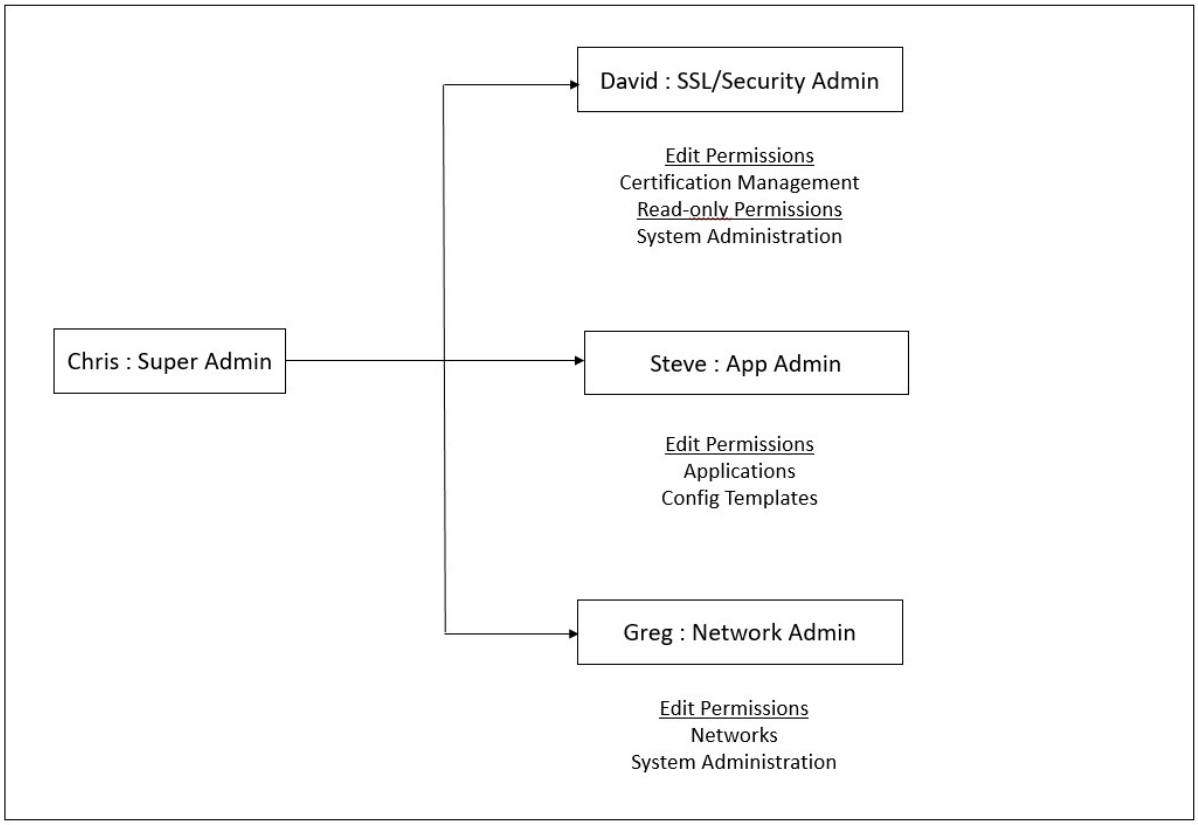
Greg, a network admin, needs access to system and network administration.

Chris also must provide RBAC for all users, irrespective of the fact that they are local or external.

NetScaler Console users can be locally authenticated or can be authenticated through an external server (RADIUS/LDAP/TACACS). RBAC settings must be applicable to all users irrespective of the authentication method adopted.

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

The following image shows the permissions that the administrators and other users have and their roles in the organization.



Limitations

RBAC is not fully supported for the following NetScaler Console features:

- **Analytics** - RBAC is not supported fully in the analytics modules. RBAC support is limited to instance level, and it is not applicable at application level in the Web Insight, SSL Insight, Gateway Insight, HDX™ Insight, and WAF Security Violations analytics modules. For example:

Example 1: Instance based RBAC (Supported)

An administrator who has been assigned a few instances can see only those instances under **Web Insight** > **Instances**, and only the corresponding virtual servers under **Web Insight** > **Applications**, because RBAC is supported at instance level.

Example 2: Application based RBAC (Not Supported)

An administrator who has been assigned a few applications can see all virtual servers under **Web Insight** > **Applications** but cannot access them, because RBAC is not supported at applications level.

- **Orchestration** - RBAC is not supported for Orchestration.

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

Configure access policies

September 27, 2025

Access policies define permissions. A policy can be applied to a single user or group, or to multiple users and multiple groups. NetScaler Console provides four predefined access policies:

1. **adminpolicy**. Grants access all NetScaler Console features. The user has both view and edit permissions, can view all NetScaler Console content, and can perform all edit operations. That is, the user can perform add, modify, and delete operations on the resources.
2. **readonlypolicy**. Grants read-only permissions. The user can view all content on NetScaler Console, but is not authorized to perform any operations.
3. **appAdminPolicy**. Grants administrative permissions for accessing the application features in NetScaler Console. A user bound to this policy can add, modify, and delete custom applications, and can enable or disable the services, service groups, and the various virtual servers, such as content switching, cache redirection, and HAProxy virtual servers.
4. **appReadOnlyPolicy**. 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.

> **Note:**
>
> The predefined policies cannot be edited.

You can also create your own (user-defined) policies.

To create user-define access policies:

1. In NetScaler Console, navigate to **Settings > Users & Roles > Access Policies**.
2. Click **Add**.
3. 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.
4. Click the (+) icon to expand each feature group into multiple features.

   a) Select the permission check box next to the feature name to grant permissions to the users.

   - **View:** This option allows the user to view the feature in NetScaler Console.

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

- **Enable-Disable:** This option is available only for the **Network Functions** features that allow enable or disable action on NetScaler Console. User can enable or disable the feature. And, 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. User can modify the feature and its functions.

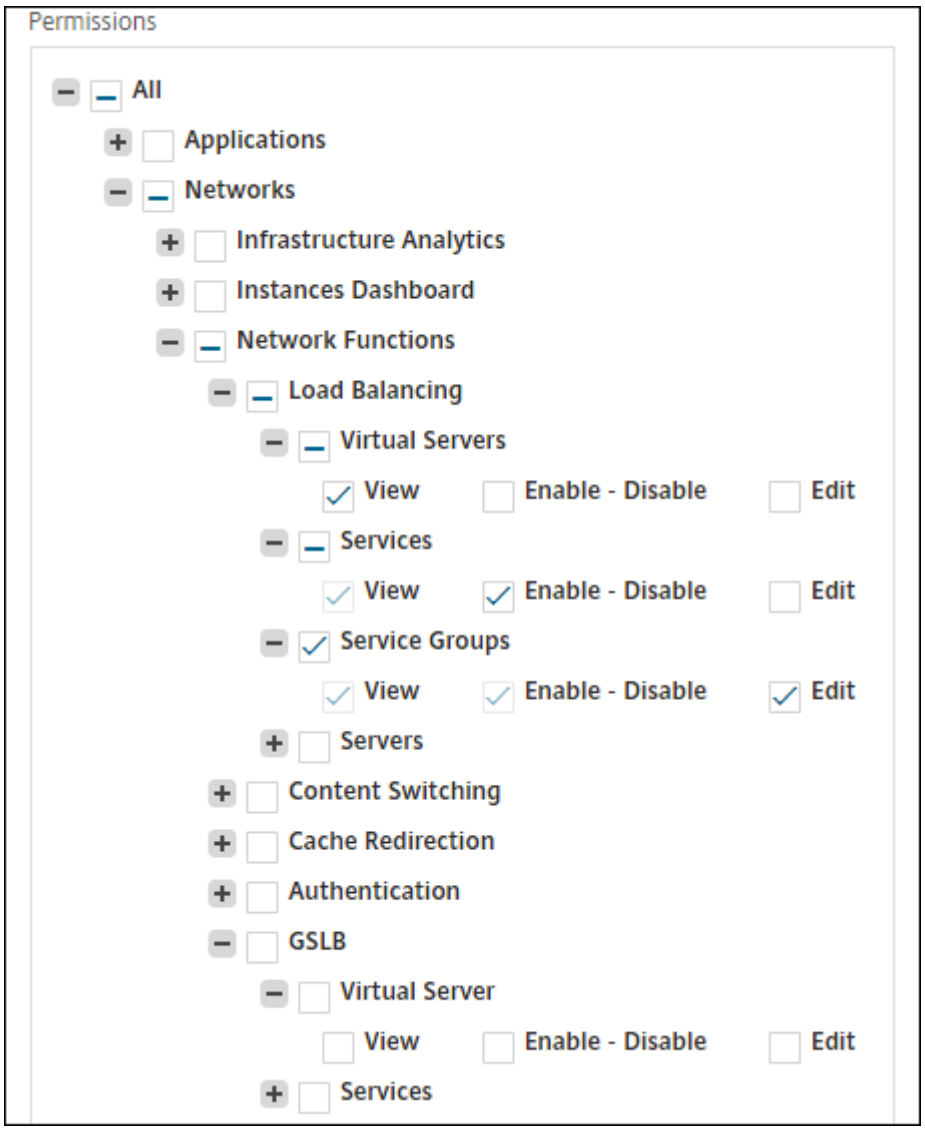
  If you grant the **Edit** permission, both **View** and **Enable-Disable** permissions are granted. You cannot deselect the auto-selected options.

If you select the feature check box, 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. User can enable or disable the services bound to a load balancing virtual server. Also, 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.

> **Note:**
>
> If a user has the **Enable-Disable** permission, the enable or disable action on a service is restricted in the following page:

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

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**.

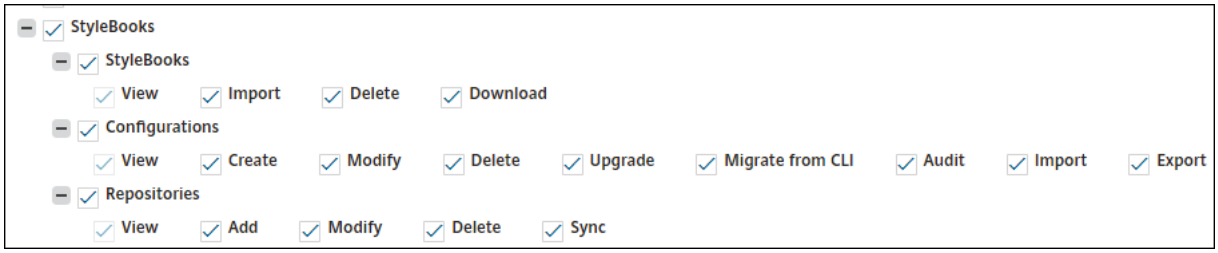
The **Edit** permission is granted to a user for the **Service Groups** feature. This permission grants the full access where **View** and **Enable-Disable** permissions are granted. User can modify the service groups that are bound to a load balancing virtual server. To edit service groups, navigate to **Infrastructure > Network Functions > Load Balancing** and select the **Service Groups** tab.

5. Click **Create**.

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 groups

September 27, 2025

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.

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

You can manage a user access in NetScaler Console at the individual level of network function entities. You can dynamically assign specific permissions to the user or group at the entity level.

NetScaler Console treats virtual server, services, service groups, and servers as network function entities.

- **Virtual server (Applications)** - Load Balancing(lb), GSLB, Context Switching (CS), Cache Redirection (CR), Authentication (`Auth`), and NetScaler Gateway (VPN)
- **Services** - Load balancing and GSLB services
- **Service Group** - Load balancing and GSLB Service groups
- **Servers** - Load balancing Servers

Create a user 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. The maximum allowed length is 64 characters.
4. In the **Group Description** field, type in a description of your group. Providing a good description of the group helps you to understand the role and function of the group in a better way at a later point.
5. In the **Roles** section, add or move one or more roles to the **Configured** list.

   > **Note:**
   >
   > Under 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.

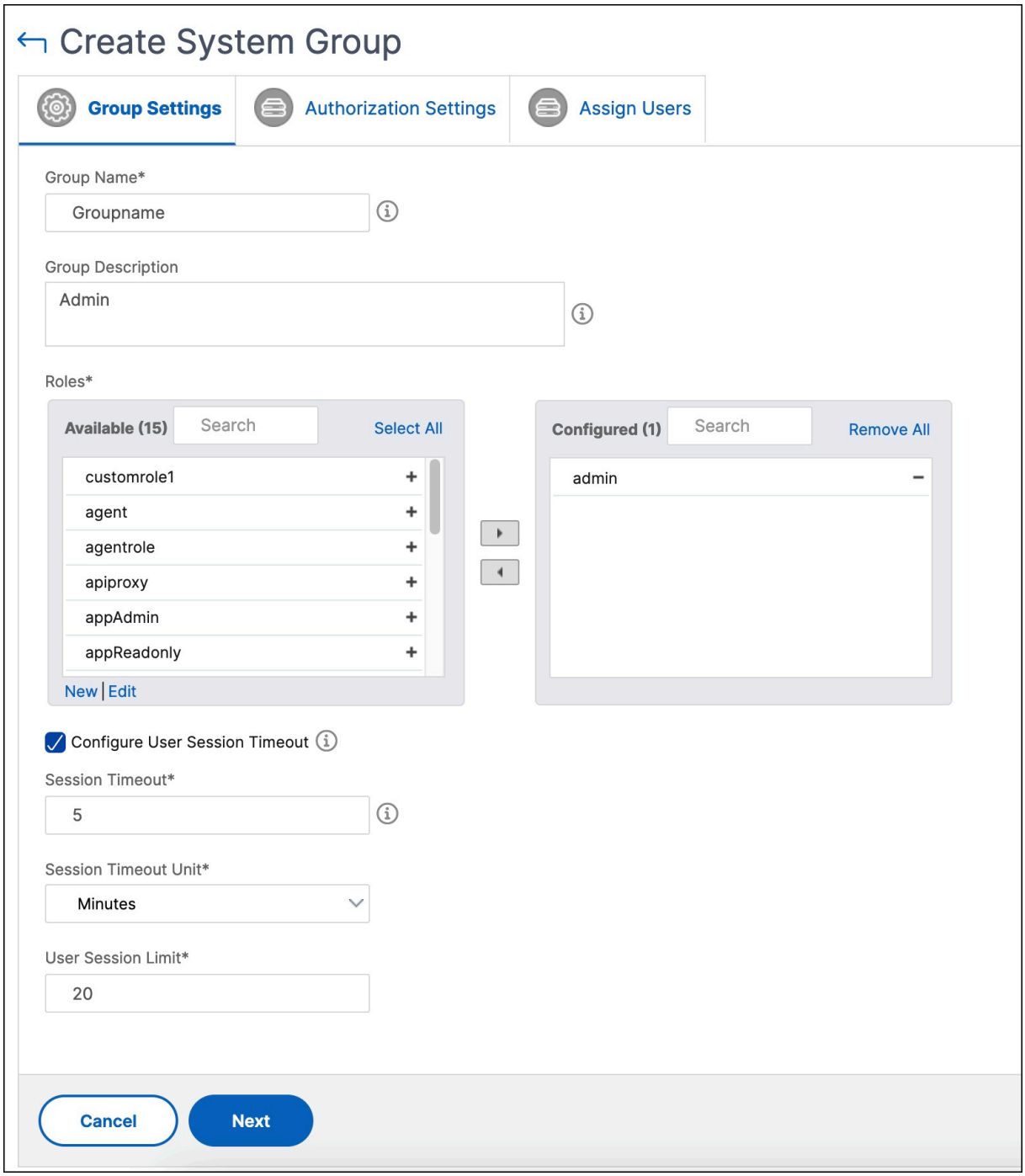
6. Select **Configure User Session Timeout** to configure the time period for a user to remain active.

   When enabled, specify the following parameters:

   - **Session Timeout**: Enter the time period for how long a user session must remain active. The default value is 15.
   - **Session Timeout Unit**: Select the timeout unit from the list, in minutes or hours. The default value is minutes.
7. In the **User Session Limit** field, enter the maximum number of sessions allowed per user.

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

> **Note:**
>
> You can configure up to 40 user sessions. By default, you are assigned 20 user sessions. However, if you belong to the admin and read-only user groups, you are assigned 40 user sessions by default and this value cannot be changed.

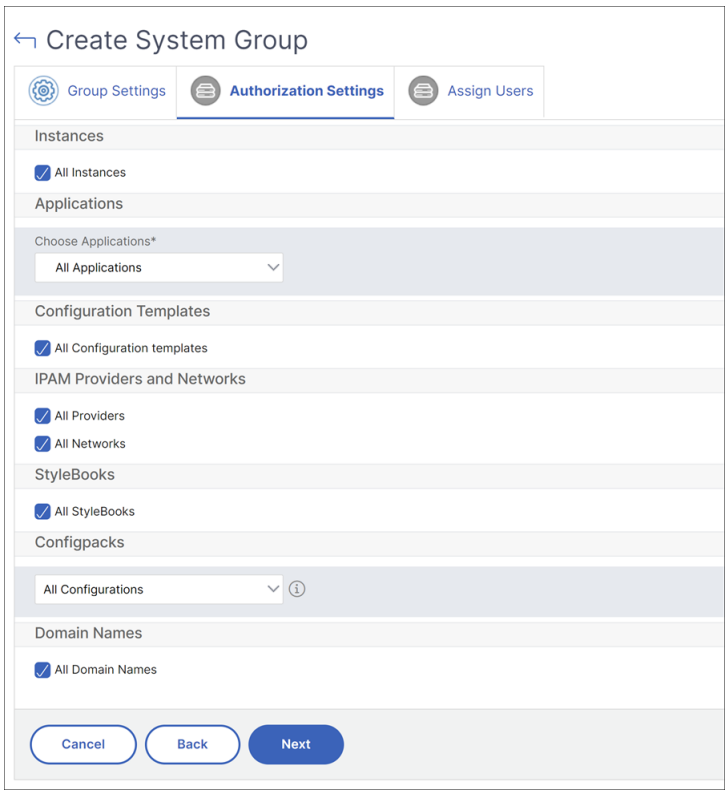


1. Click **Next**. On the **Authorization Settings** tab, you can provide authorization settings for the

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

following resources:

- Autoscale™ Groups
- Instances
- Applications
- Configuration Templates
- StyleBooks
- Config packs
- Domain Names



You might want to select specific resources from the categories to which users can have access.

Autoscale Groups:

If you want to select the specific Autoscale groups that a user can view or manage, do the following steps:

a) Clear the **All AutoScale Groups** checkbox and click **Add AutoScale Groups**.

b) Select the required Autoscale groups from the list and click **OK**.

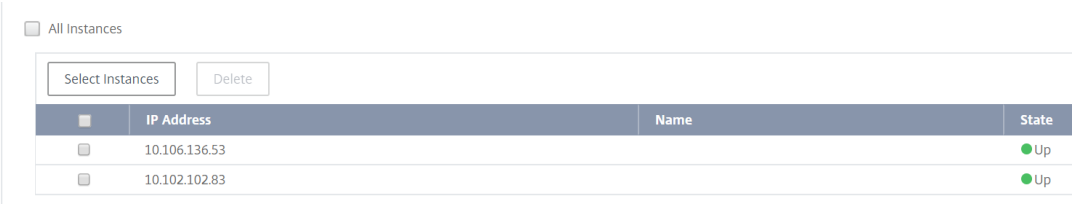
Instances:

If you want to select the specific instances that a user can view or manage, perform the following steps:

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

a) Clear the **All Instances** checkbox and click **Select Instances**.

b) Select the required instances from the list and click **OK**.

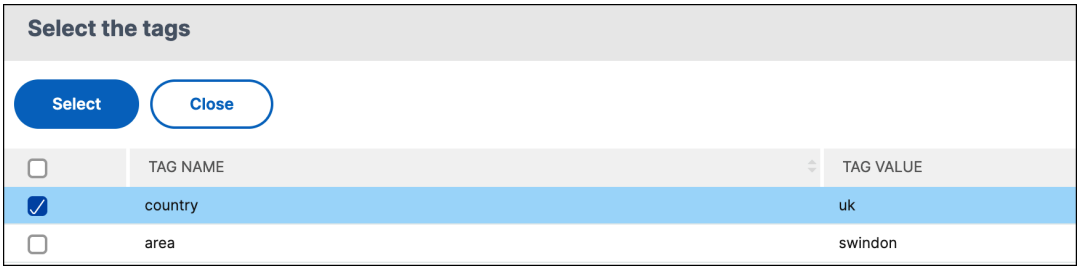


Tags:

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.

You can grant access to applications without selecting their instances. When you grant a user access to an application, the user is authorized to access only that application regardless of instance selection.

The following options are available:

- **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.

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

- **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 a 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.

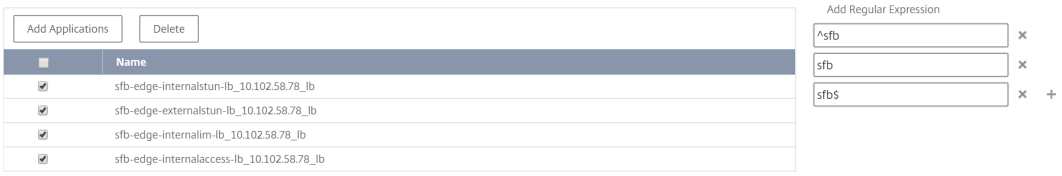
  > **Note:**
  >
  > To authorize bound entities, select only one entity type.

You can use regular expressions to search and add the network function entities that meet the regex criteria for the groups. The specified regex expression is persisted in NetScaler Console. To add a regular expression, perform the following steps:

a) Click **Add Regular Expression**.

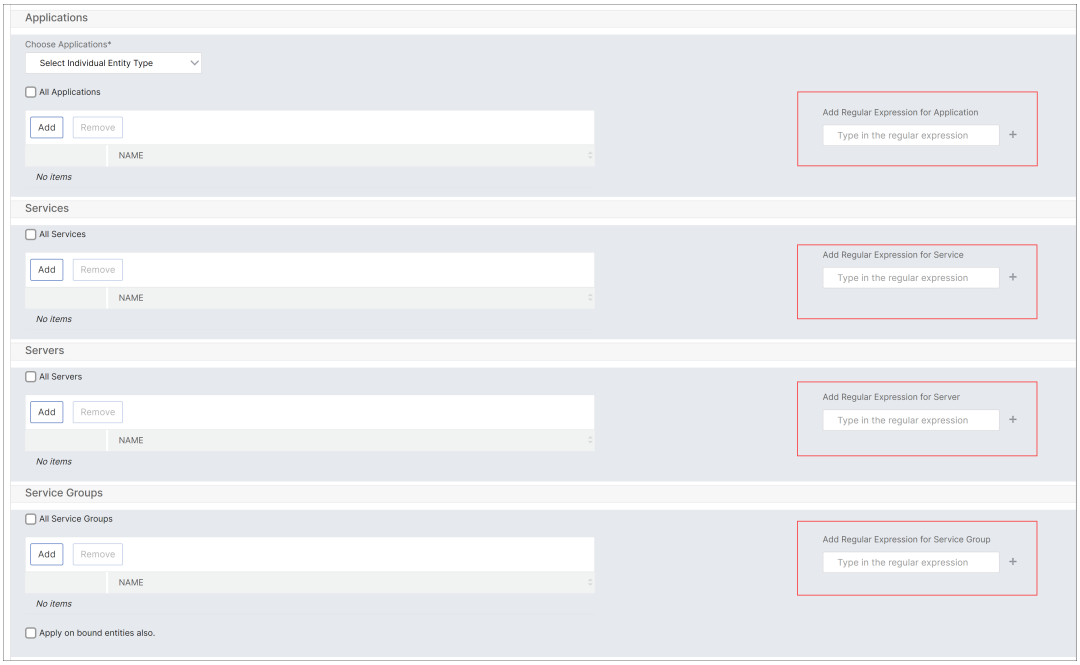
b) Specify the regular expression in the text box.

The following image explains how to use a regular expression to add an application when you select the **Specific Applications** option:



The following image explains how to use regular expression to add network function entities when you choose the **Select the Individual Entity Type** option:

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



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, perform the following steps:

a) Clear the **All Configuration templates** checkbox and click **Add Configuration Template**.

b) Select the required template from the list and click **OK**.

StyleBooks:

If you want to select the specific StyleBook that a user can view or manage, perform 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.

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

If you want to select the individual StyleBooks, select the StyleBooks from the **Individual StyleBooks** pane and click **Save Selection**.

If you want to use a query to search StyleBooks, select the **Custom Filters** pane. A query is a string of key-value pairs where keys are `name`, `namespace`, and `version`.

You can also use regular expressions as values to search and add StyleBooks that meet the regex criteria for the groups. A custom filter query to search StyleBooks supports both `And` and `Or` operation.

Example:

```
name=lb-mon|lb AND namespace=com.citrix.adc.stylebooks AND
   version=1.0
```

This query lists the StyleBooks that meet the following conditions:

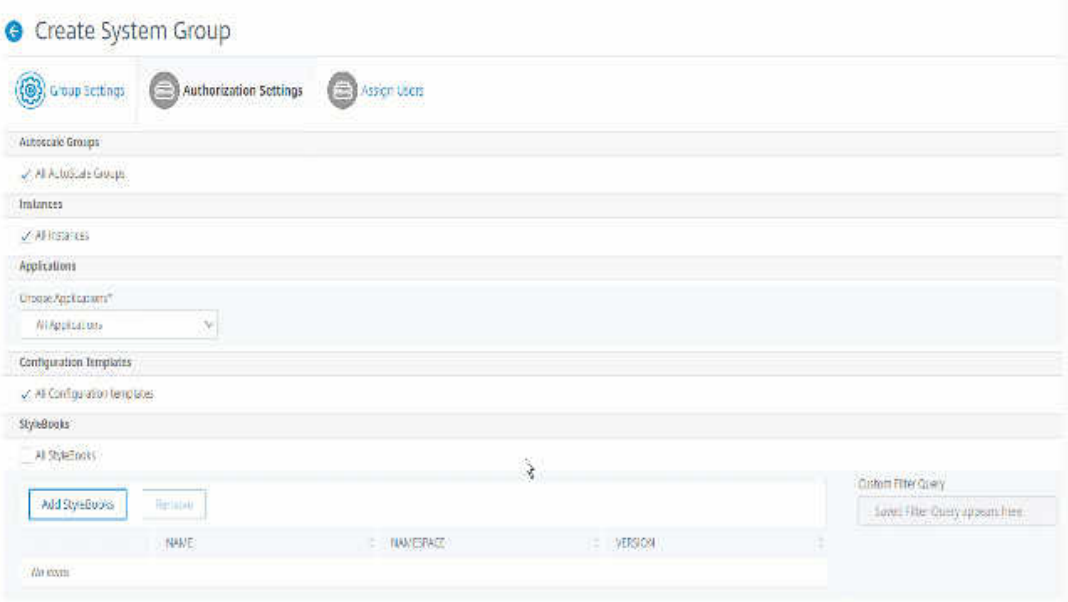
- StyleBook name is either `lb-mon` or `lb`.
- StyleBook namespace is `com.citrix.adc.stylebooks`.
- StyleBook version is `1.0`.

Use an `Or` operation between value expressions that is defined to the key expression.

Example:

- The `name=lb-mon | lb` query is valid. It returns the StyleBooks having a name either `lb-mon` or `lb`.
- The `name=lb-mon | version=1.0` query is invalid.

Press `Enter` to view the search results and click **Save Query**.



The saved query appears in the **Custom Filters Query**. Based on the saved query, the NetScaler Console provides user access to those StyleBooks.

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

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 **Config packs**, select one of the following options:

- **All Configurations**: This option is selected by default. It allows users to manage all the configurations that are in NetScaler Console.
- **All Configurations of the selected StyleBooks**: This option adds all the config packs of the selected StyleBook.
- **Specific Configurations**: This option allows you to add specific configurations of any StyleBook.
- **All Configurations created by the user group**: This option allows users to access only configurations created by users of the same group..

  You can select the applicable config packs when you create groups and assign users to that group.

Domain Names:

If you want to select the specific domain name that a user can view or manage, perform the following steps:

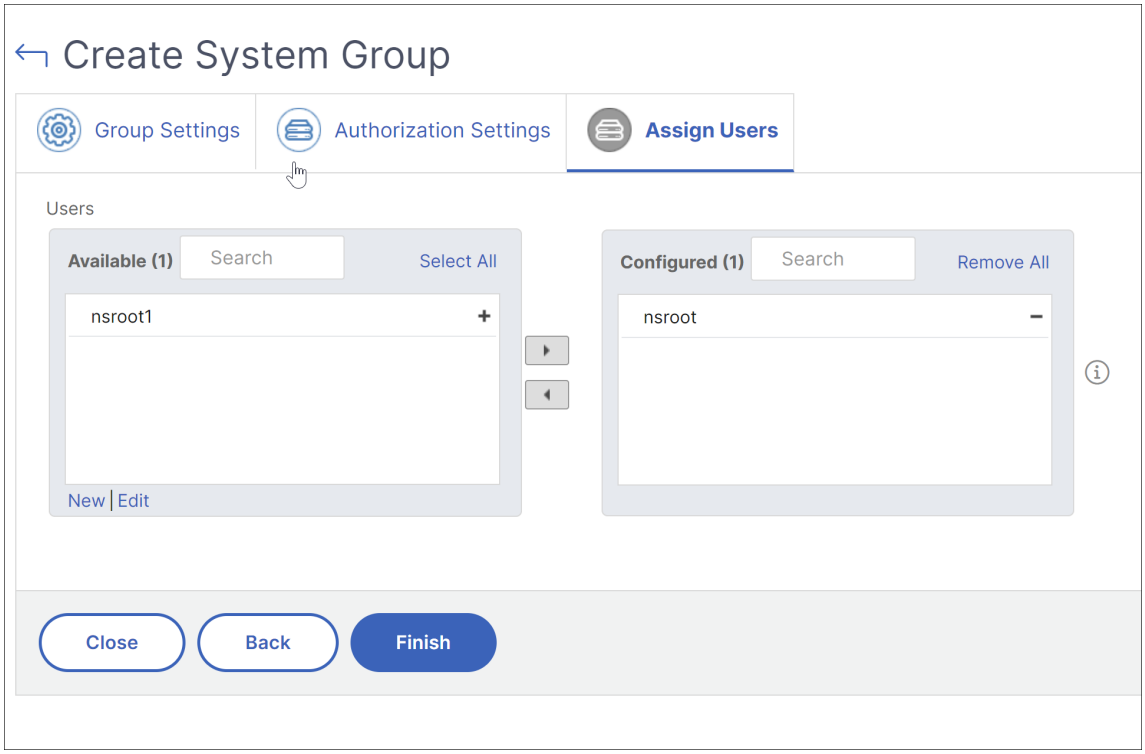
a) Clear the **All Domain Names** checkbox and click **Add Domain Name**.

b) Select the required domain names from the list and click **OK**.

2. Click **Create Group**.
3. 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 users by clicking **New**.

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



4. Click **Finish**.

Manage user access across multiple network function entities

As an administrator, you can manage user access at the individual level of network function entities in NetScaler Console. And, you can dynamically assign specific permissions to the user or a group at the entity level by using the regular expression filter.

This document describes how to define user authorization at the entity level.

Before you begin, create a group. See Configure groups on NetScaler Console for more information.

Usage scenario:

Consider a scenario where one or more applications (virtual servers) are hosted on the same server. A super administrator (George) wants to grant Steve (an application administrator) access only to App1 and not to the hosting server.

The following table illustrates this environment, where Server-A hosts applications App-1 and App-2.

Host Server	Application (virtual server)	Service	Service group
Server A	App1	App-service-1	App-service-group-1

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

Host Server	Application (virtual server)	Service	Service group
Server A	App2	App-service-2	App-service-group-2

> **Note**
>
> NetScaler Console treats virtual server, services, service groups, and servers as network function entities. The entity type virtual server is referred as an application.

To assign user permissions to network function entities, George defines the user authorization as follows:

1. Navigate to **Account > User Administration > Groups** and add a group.
2. In the **Authorization Settings** tab, select Choose Applications.
3. Choose **Select Individual Entity Type**.
4. Select the **All Applications** entity type and add the App-1 entity from the available list.
5. Click **Create Group**.
6. In **Assign users**, select the users who require the permission. For this scenario, George selects Steve's user profile.
7. Click **Finish**.

With this authorization setting, Steve can manage only App-1 and not other network function entities.

> **Note:**
>
> Ensure the **Apply on bound entities also** option is cleared. Otherwise, NetScaler Console grants access to all network function entities that are bound to App-1. As a result, grants access to the hosting server as well.

A super administrator can specify the regular expressions (regex) for each entity type. The regular expression is stored in the system to update the user authorization scope. When new entities match the regular expression of their entity type, NetScaler Console can dynamically grant users access to the specific network function entities.

To grant user permissions dynamically, the super administrator can add regular expressions in the **Authorization Settings** tab.

In this scenario, George adds App* as a regular expression for the Applications entity type and the applications that match the regex criteria appear in the list. With this authorization setting, Steve can access all the applications that match the App* regex. However, his access is limited only to the applications not to the hosted server.

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

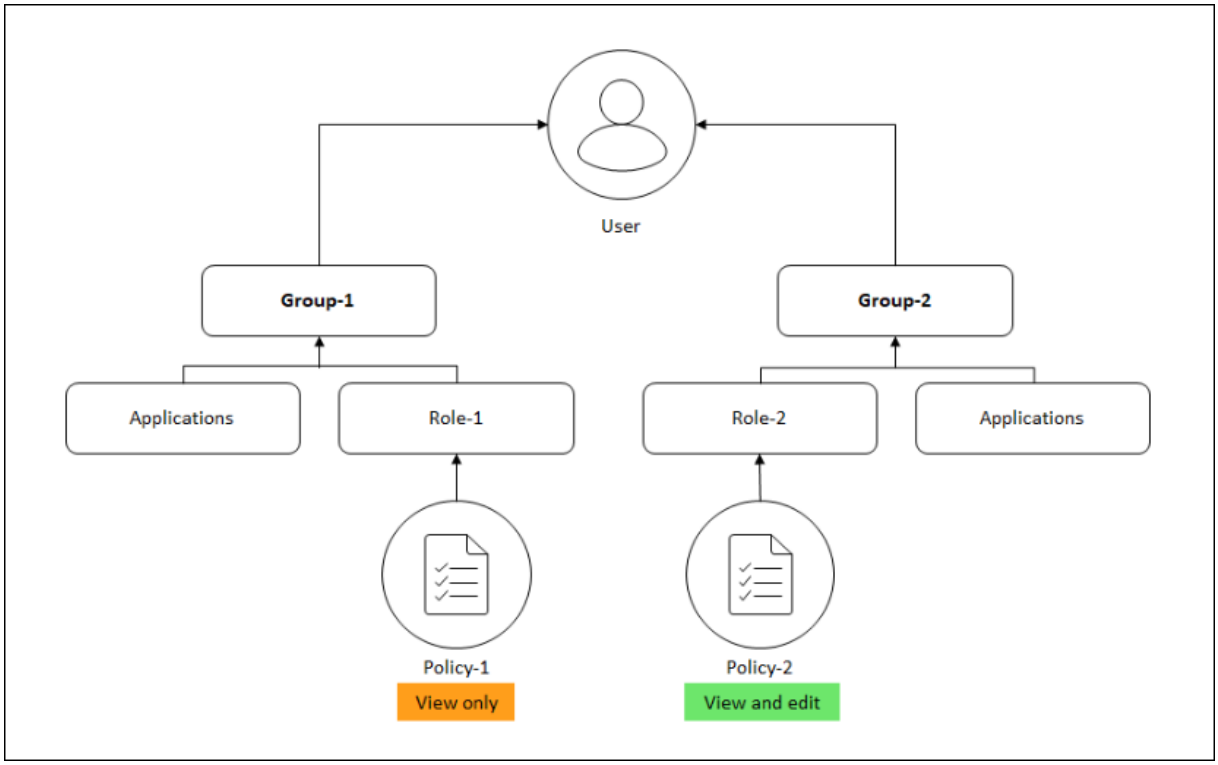
How user access changes based on the authorization scope

When an administrator adds a user to a group that has different access policy settings, the user is mapped to more than one authorization scope 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.

Mapping of RBAC when upgrading NetScaler Console from 12.0 to later releases

When you upgrade NetScaler Console from 12.0 to 13.1, you do not see the options to provide "read-write"or "read"permissions while creating groups. These permissions are replaced with "roles and access policies,"which give you more flexibility to provide role-based permissions to the users. The following table shows how the permissions in release 12.0 are mapped to release 13.1:

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

12.0	Allow Applications Only	13.1
admin read-write	False	`admin`
admin read-write	True	`appAdmin`
admin read-only	False	`readonly`
admin read-only	True	`appReadonly`

Configure roles

September 27, 2025

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 StyleBooks and to configure NetScaler instances.

When multiple policies define edit and read-only permissions for a single feature, the edit permissions have priority.

NetScaler Console provides four predefined roles:

- **admin**. Has access to all NetScaler Console features. (This role is bound to adminpolicy.)
- **readonly**. Has read-only access. (This role is bound to readonlypolicy.)
- **appAdmin**. Has administrative access to only the application features in NetScaler Console. (This role is bound to appAdminPolicy).
- **appReadonly**. Has read-only access to the application features. (This role is bound to appRead-OnlyPolicy.)

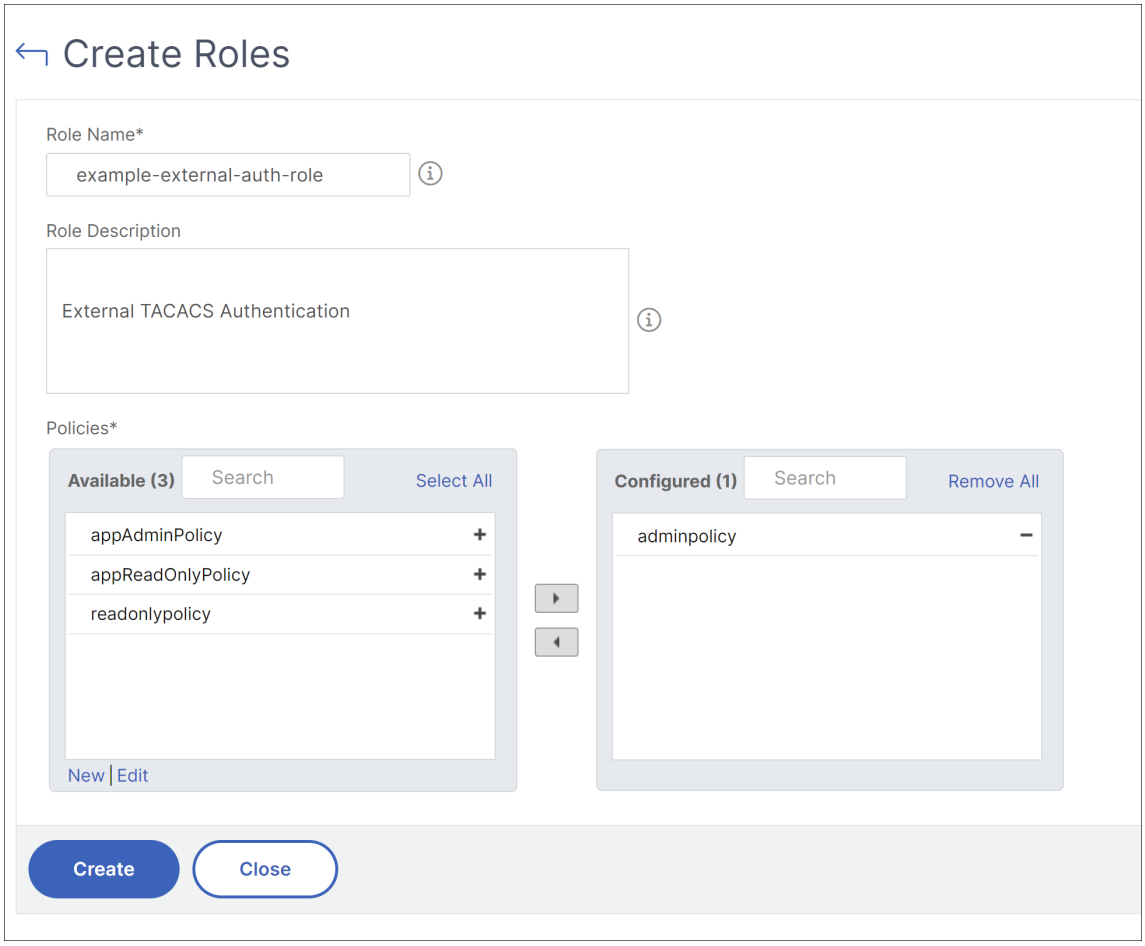
> **Note:**
>
> The predefined roles cannot be edited.

You can also create your own (user-defined) roles.

To create roles and assign policies to them:

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

1. In NetScaler Console, navigate to **Settings > Users & Roles**.
2. Click **Add**.
3. 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 or move one or more policies to the **Configured** list.



5. Click **Create**.

Configure users

September 27, 2025

By default, NetScaler Console has one user:

nsroot - The root user (nsroot) has full administrative privileges on the appliance. The nsroot user is the super admin of NetScaler Console.

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

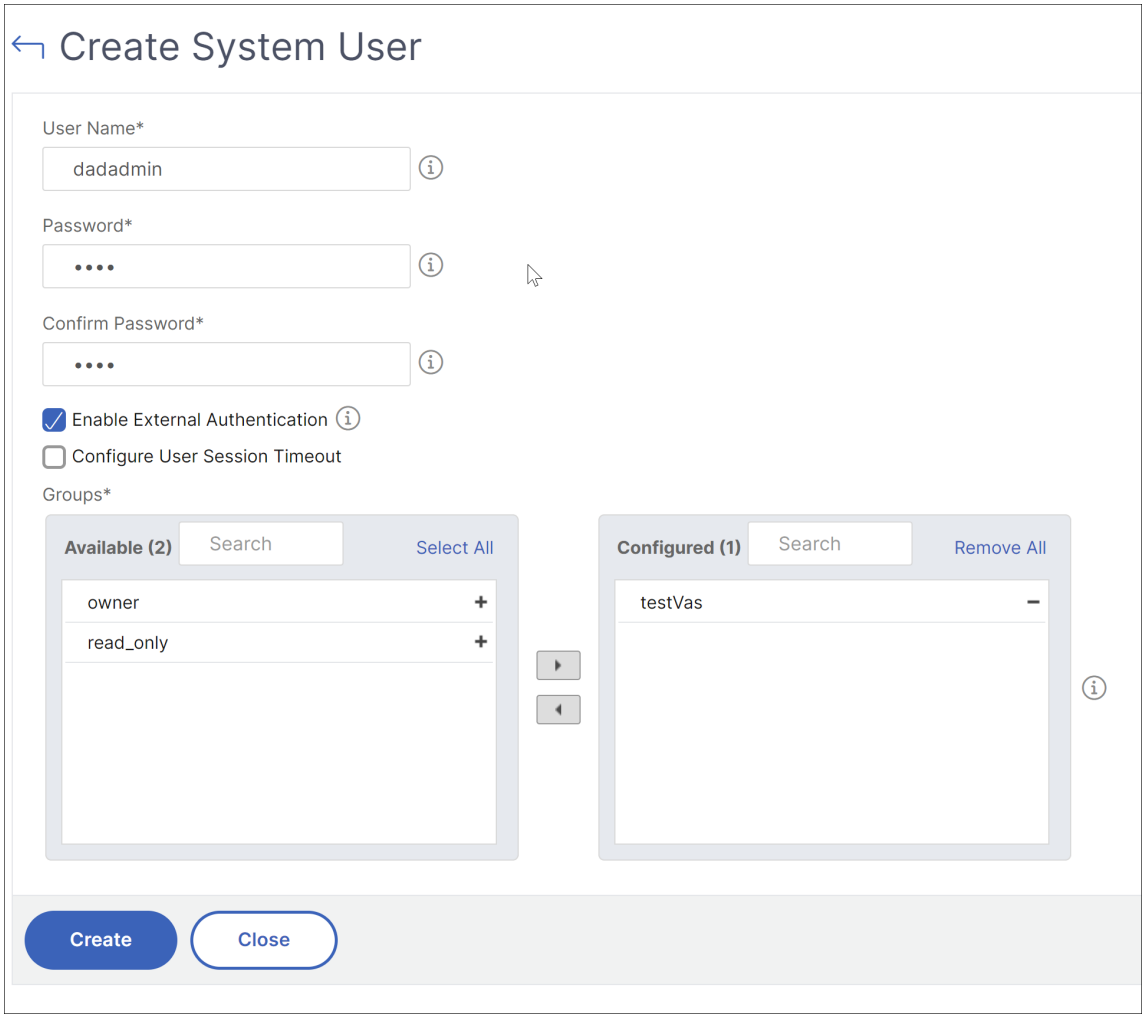
You can create additional users by configuring accounts for them. When you add new users to NetScaler Console, you can define their permissions by assigning the appropriate groups, roles, and policies.

You can assign a user to a group and bind the group to roles. You can define one-to-one, one-to-many, or many-to-many relationship between users, groups, roles, and access policies. A user can be assigned to multiple groups. A group can have multiple roles, and multiple groups can have identical roles.

To configure users in NetScaler Console:

1. In NetScaler Console, navigate to **Settings > Users & Roles**.
2. Click **Add**.
3. Enter the following details:
    a) **User Name**. Name of the user
    b) **Password**. Password with which the user logs on to NetScaler Console
4. Optionally, select **Enable External Authentication**, so that the user can be authenticated through an external authentication server.
5. If you have created groups and want to assign the user to a group, in the **Groups** section, move one or more groups from the **Available** list to the **Configured** list.

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



6. Click **Create**.

Actionable tasks and recommendations

November 28, 2025

> **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 in-

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

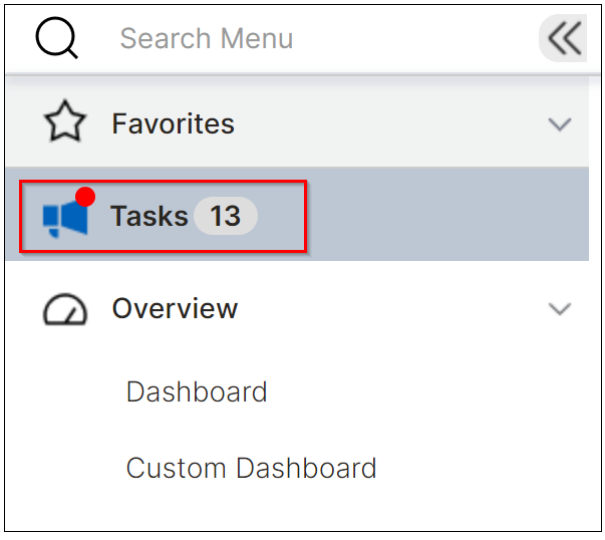
stances and your applications are efficiently managed to get insights for better prioritizing and troubleshooting.

As you scale-up your infrastructure more, you might also need to focus on the critical issues impacting your instances and applications that need your immediate attention. You must also ensure that your NetScaler Console deployment is efficient, secure, and compliant. Based on your current utilization and subscription, the **Tasks** feature in NetScaler Console enables you to view both actionable **Tasks** that you must take immediate action and **Recommendations** to ensure efficient deployment.

As an administrator, by making use of these actionable **Tasks** and **Recommendations**, you can:

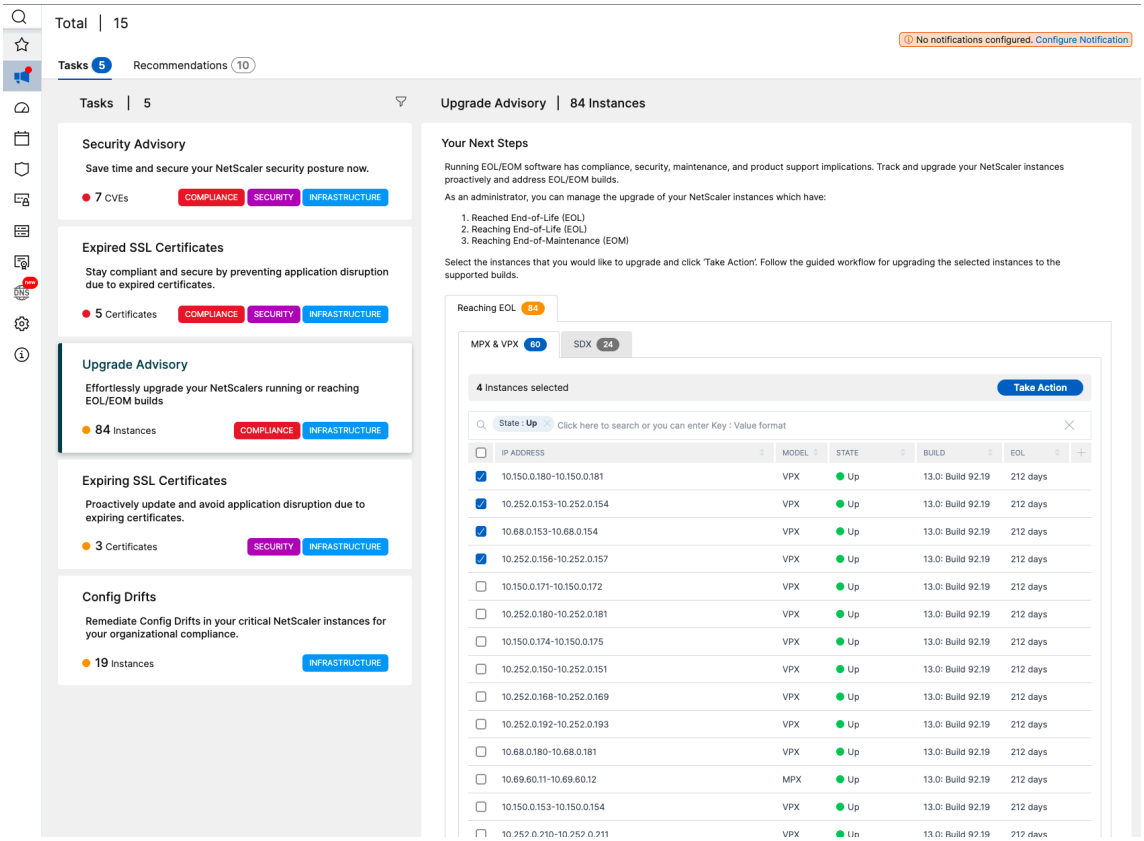
- Get instant visibility on any observations or issues that require your immediate action.
- Configure notifications to receive notification whenever NetScaler Console detects any tasks and proactively take action.
- Achieve an efficient deployment of NetScaler Console and NetScaler instances.
- Reduce the crucial time and effort in identifying the critical issues.
- Ensure that you are making use of 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 4 tasks. The tasks are displayed based on the severity (Critical and Medium).

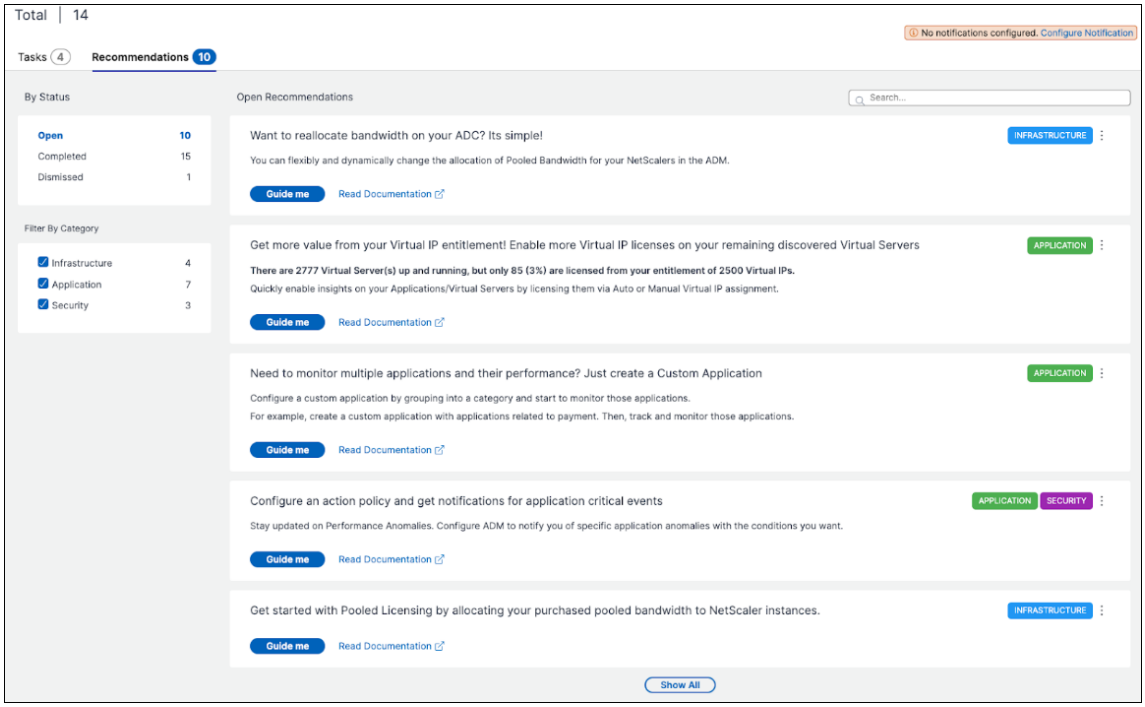
© 1997–2025 Citrix Systems, Inc. All rights reserved.



- **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**.

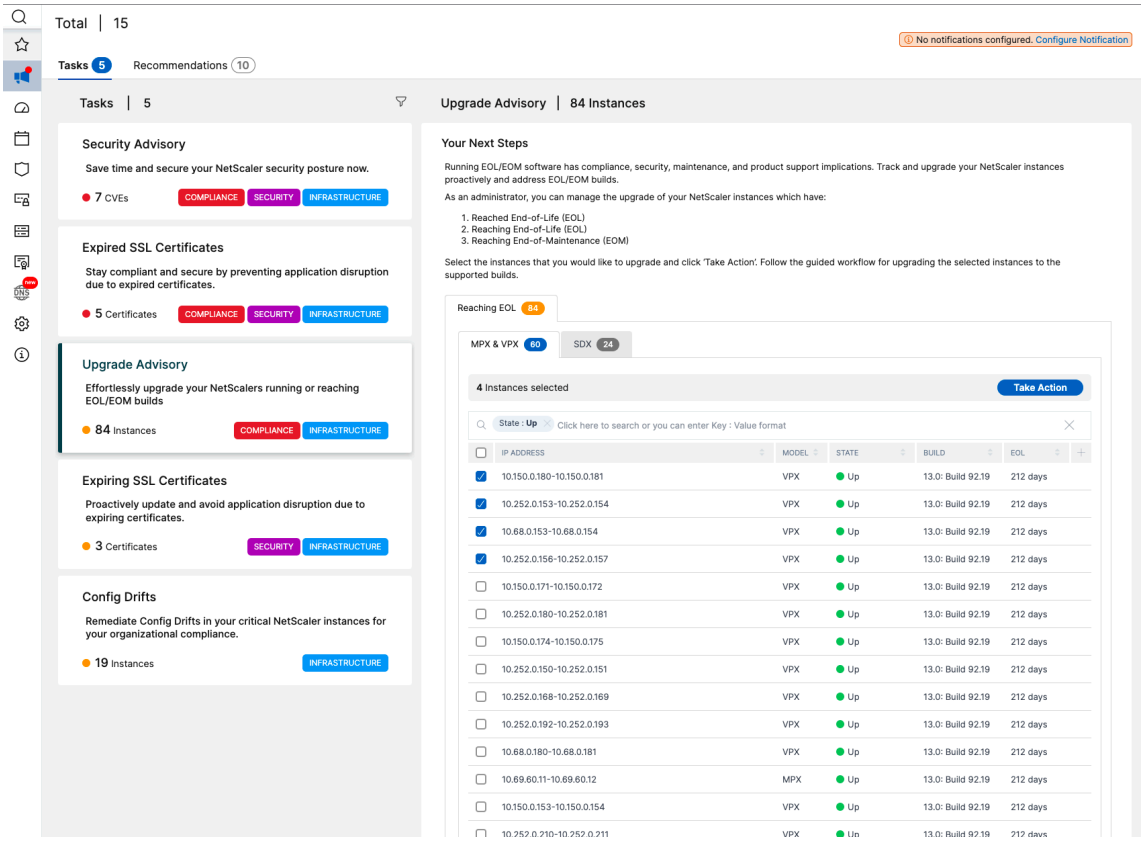
    Recommended Action: You are redirected to the **Security Advisory** page in **Infrastructure > Instance Advisory > Security Advisory**. Follow the documentation to complete the task.

  - **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.

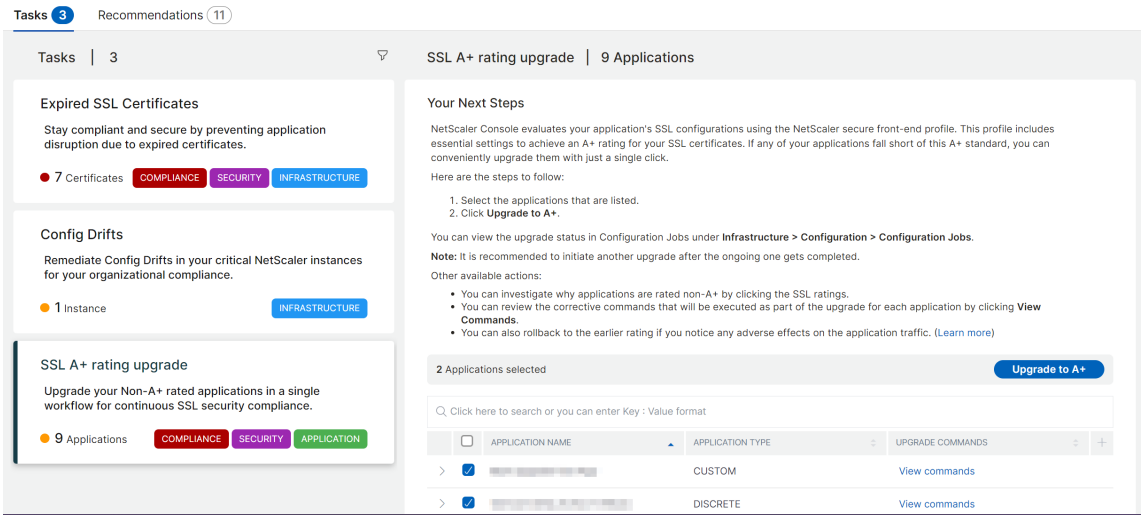
- **Upgrade Advisory**: Provides information about your NetScaler® instances that have already reached or about to reach End of Life (EOL) or End of Maintenance (EOM) within 90 days.

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



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

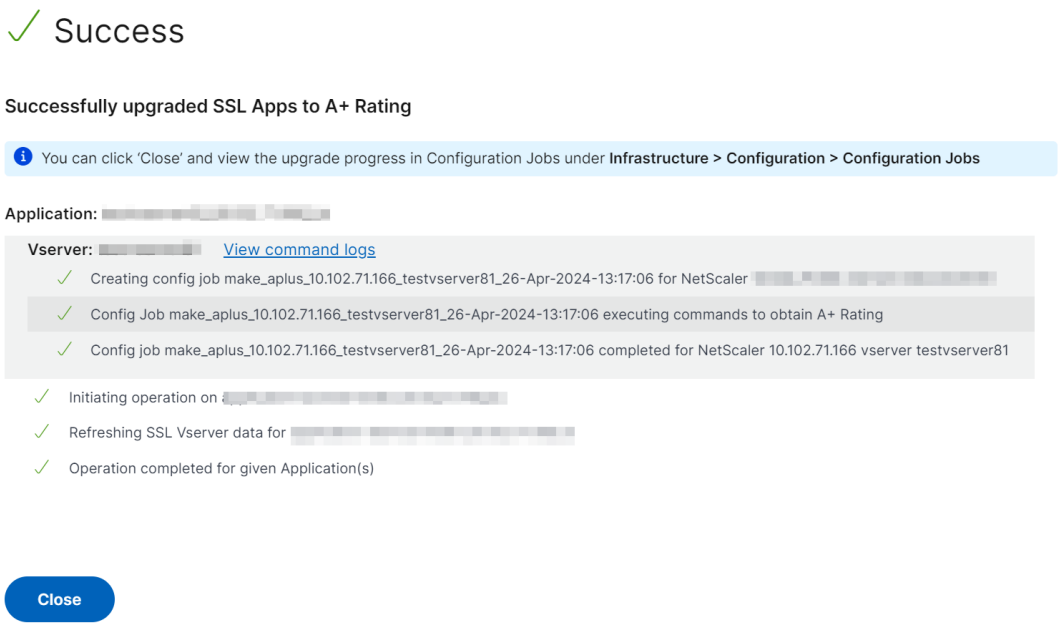
- **SSL A+ rating upgrade**: Provides information about your applications that are not compliant with an A+ rating.



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.



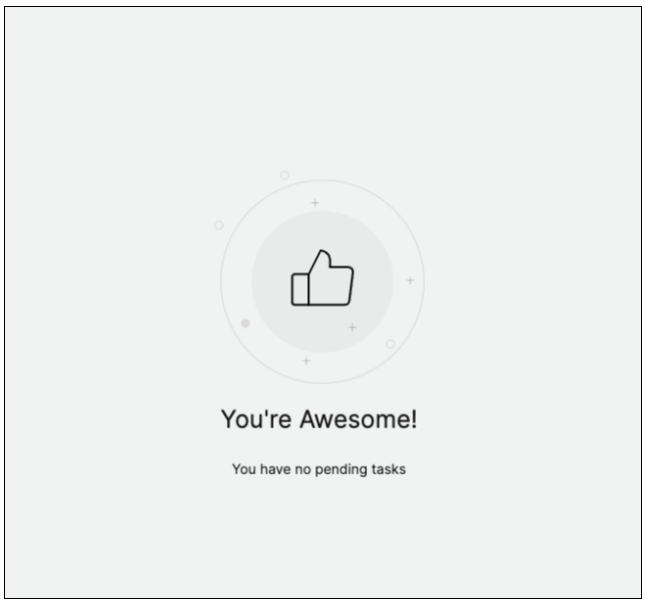
After the upgrade is completed, the application details are removed from the task.

Points to note:

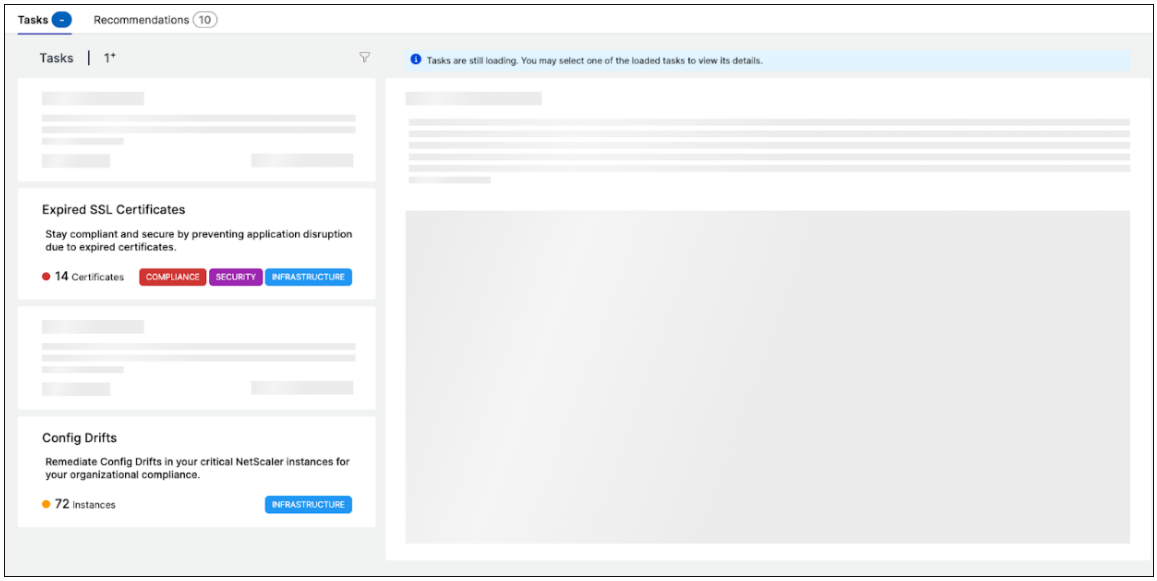
- Depending upon the number of applications selected, the duration for the upgrade completion process might vary.
- After you initiate an upgrade process, it is recommended to initiate another upgrade process after the ongoing one gets completed.
- You can also view the status for the upgrade process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

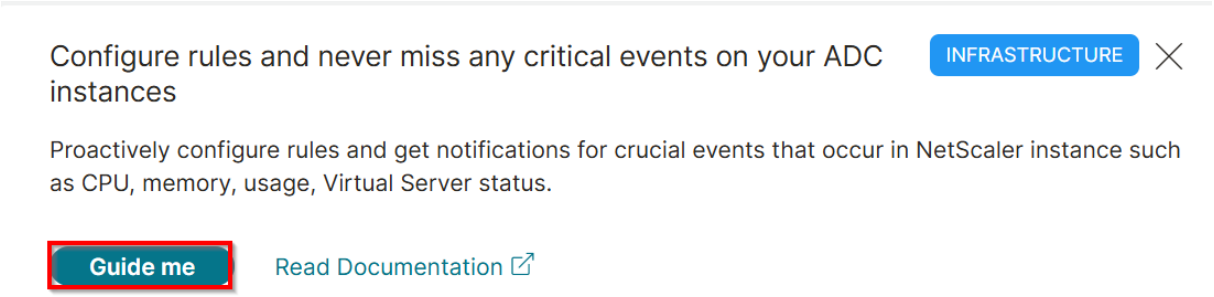
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 NetScaler Console?	If ServiceNow integration in NetScaler Console is not yet configured.
Automate SSL Certificate management using Venafi and NetScaler Console	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:

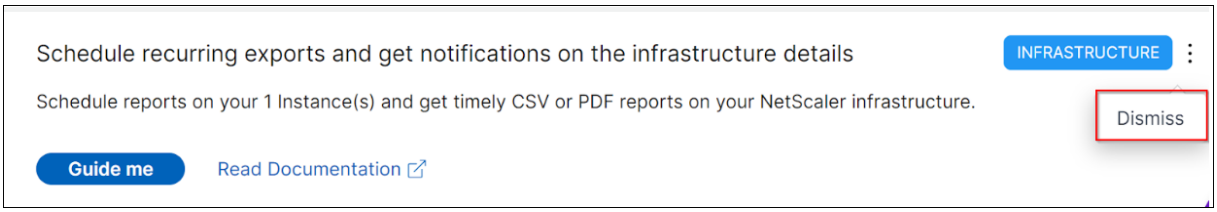
© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.

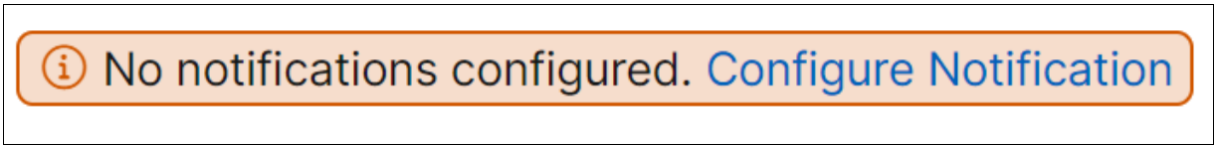
After you complete creating a rule, the recommendation is complete and it is moved to **Completed**.

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. 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

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

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.

2. What happens if I dismiss any recommendation?

   The recommendations that you dismiss are moved to **Dismissed**. You can complete these recommendations later.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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

September 27, 2025

In NetScaler Console, you can view various insights about the usage and performance of applications, NetScaler infrastructure, security (Bot and WAF) violations, and so on. As an administrator, you might have to navigate to various options in the NetScaler Console GUI to view multiple insights. For example, to check the virtual servers (applications) and NetScaler instance insights:

- You must first navigate to **Applications > Dashboard** to view insights for applications.
- Then you must navigate to **Infrastructure > Infrastructure Analytics** to view insights for NetScaler instances.

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

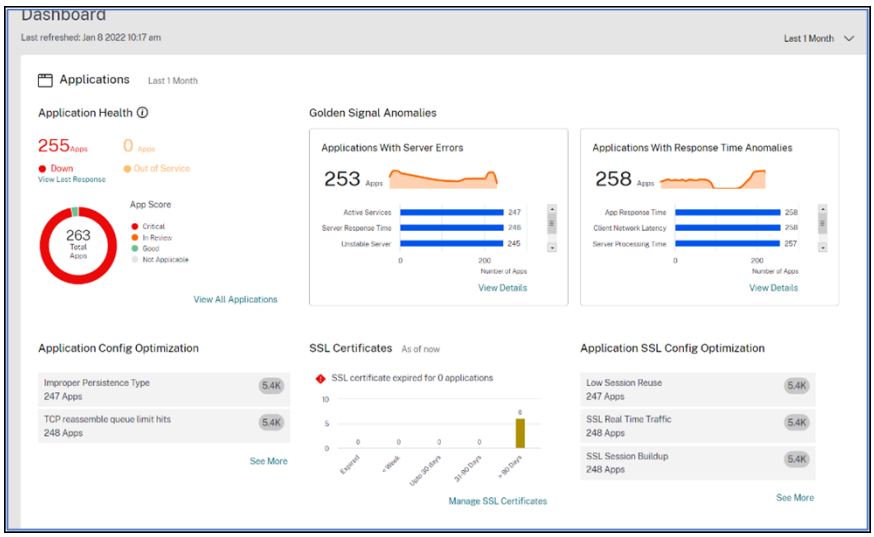
For a better monitoring experience, it is necessary for you to have a privilege that contains an overview of all the required insights. Navigate to **Overview > Dashboard** to visualize a single-pane dashboard with an overview of the key metrics details based on the following categories:

- Applications
- NetScaler Infrastructure
- Application security
- Gateway

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).
- **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.



Application Security

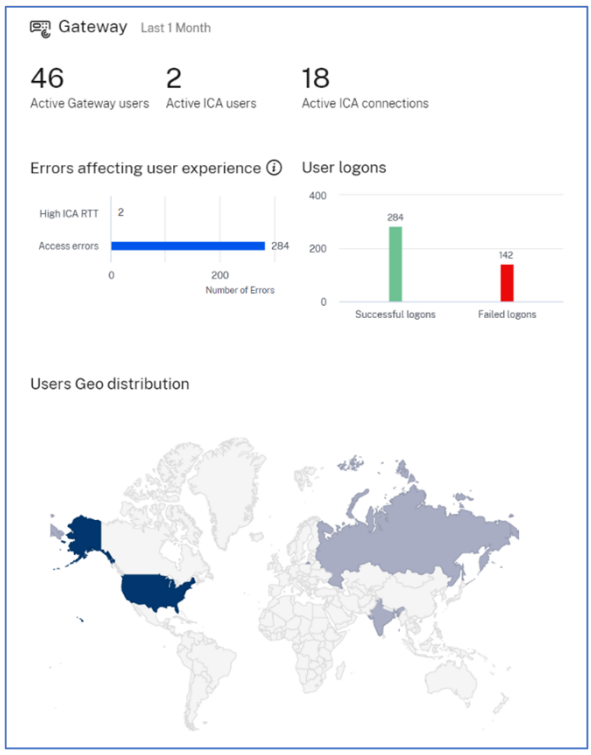
Provides an overview of total affected applications and total violations (Bot and WAF) reported for the selected duration. Click **View Security Dashboard** to view the security and bot violation details.

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



Gateway

Provides an overview of total active gateway users, total active ICA® users, and total active ICA connections. You can also view errors, user logon details, and a geo map that provides details on the user locations.



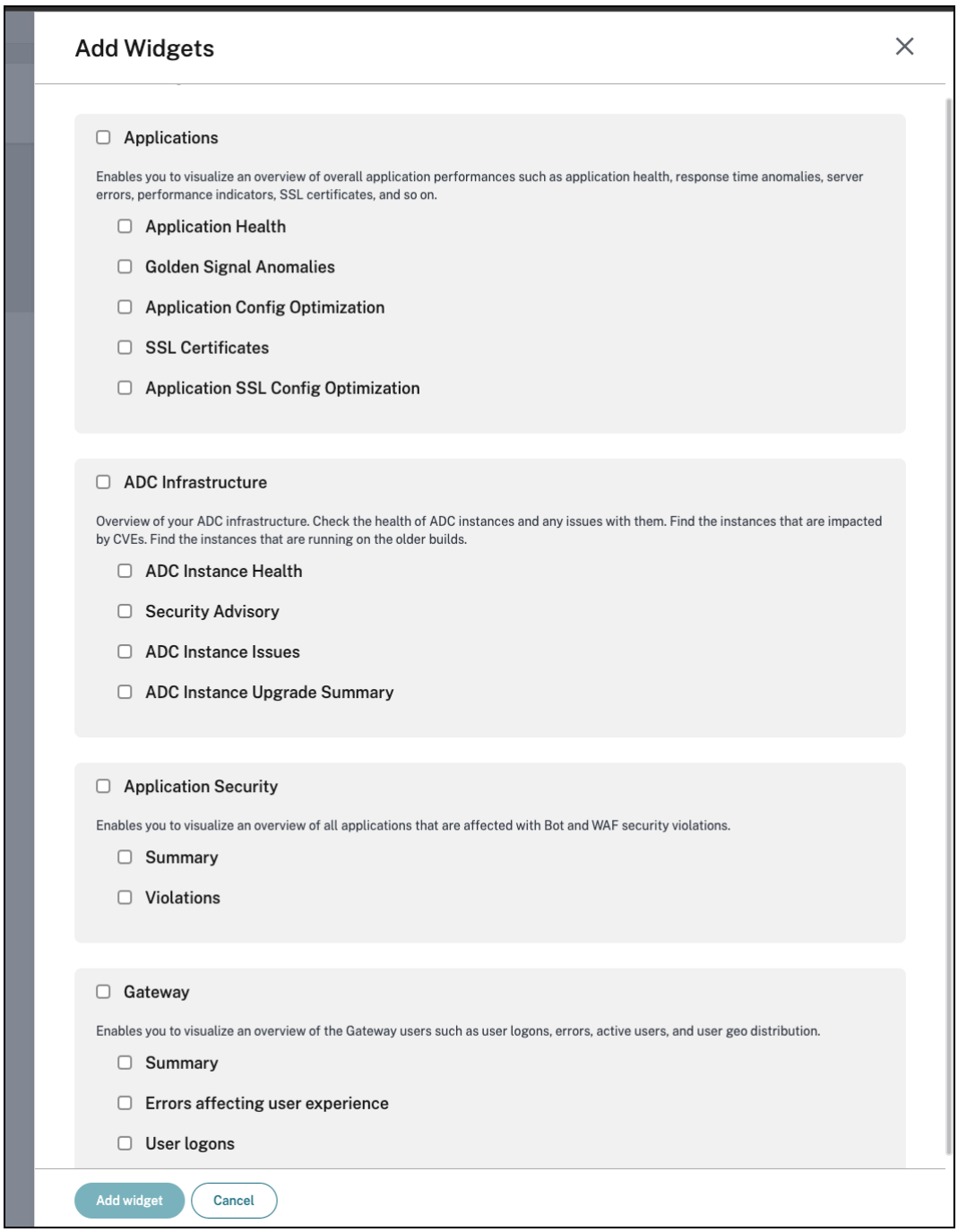
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

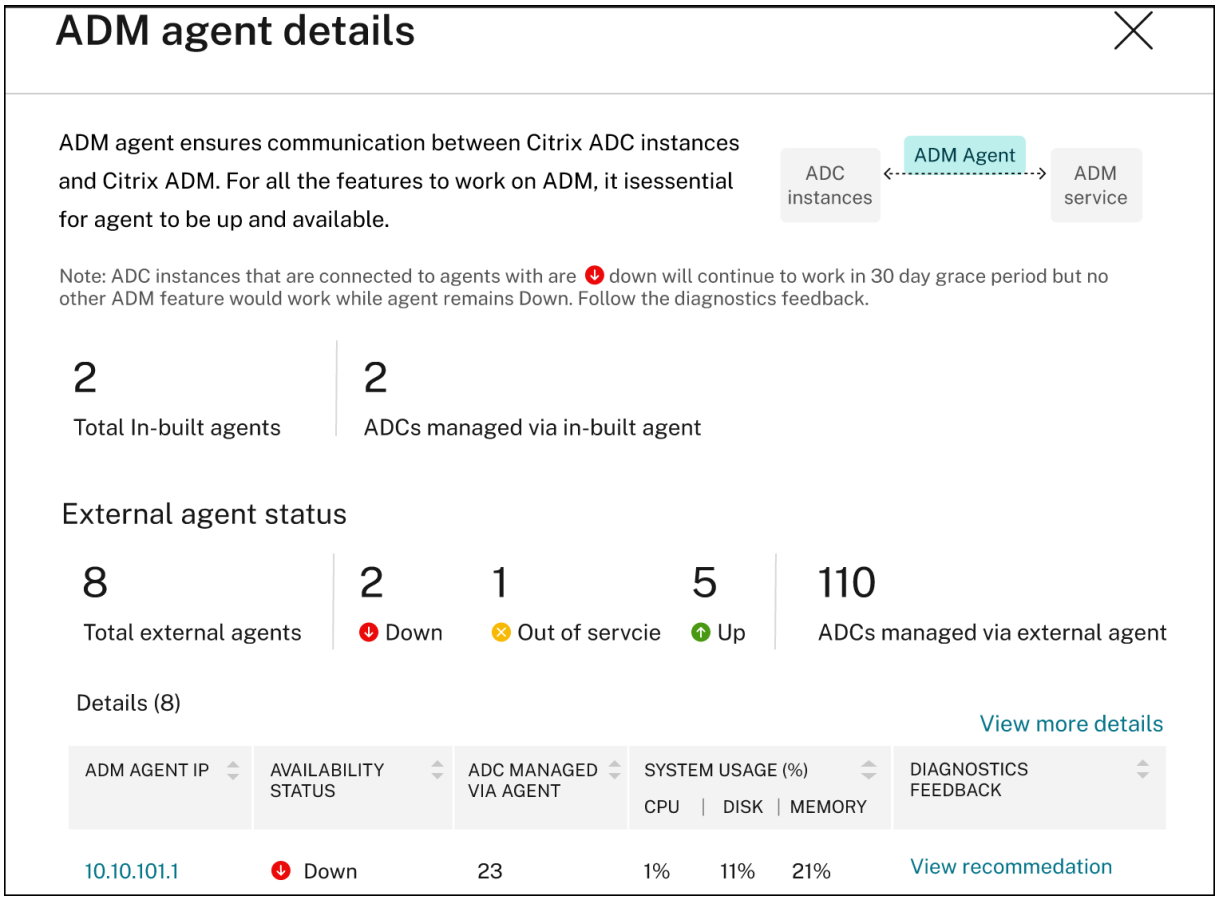
> and again use the **Reset to default** option, all widgets get added to the dashboard.
>
> - The **Reset to last saved** option loads the previously saved configuration.

View agent details

In the unified dashboard, you can visualize an overview of agent details. In **Overview > Dashboard**, next to the **NetScaler® 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

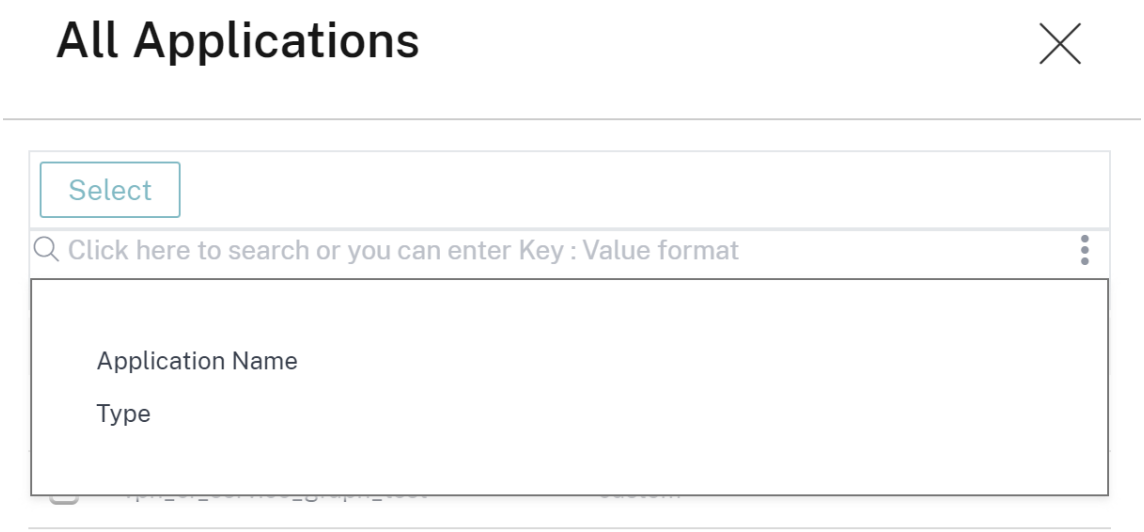
You can apply filters and view insights only for the selected instances or applications in the following:

- 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.

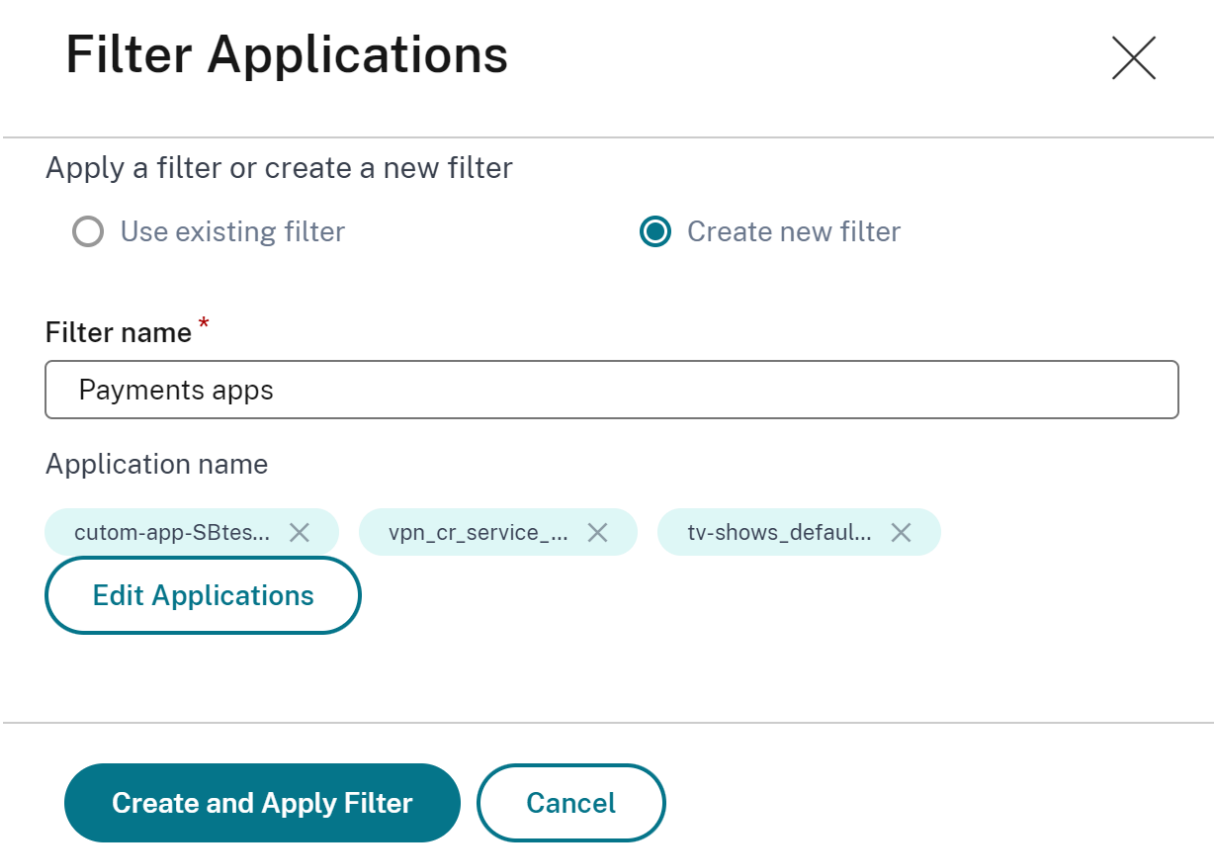
In the **Filter Applications** window:

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.



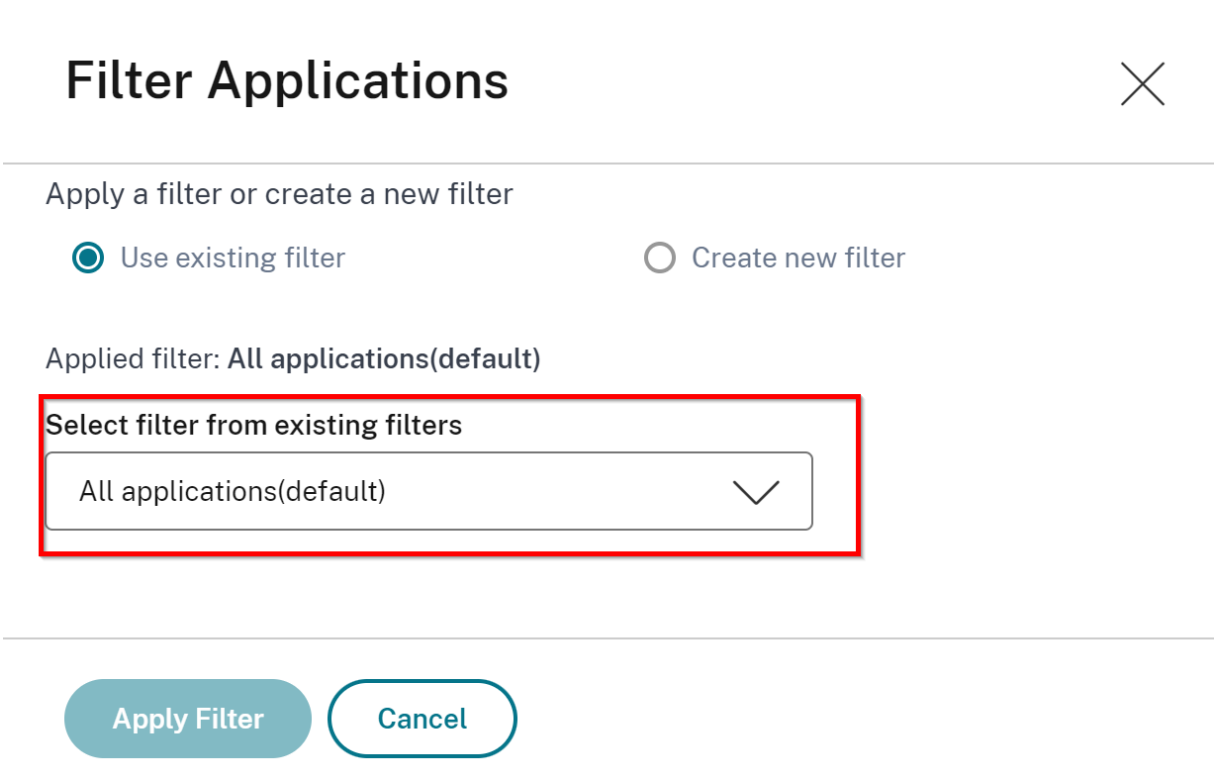
4. Click **Create and Apply filter**.

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



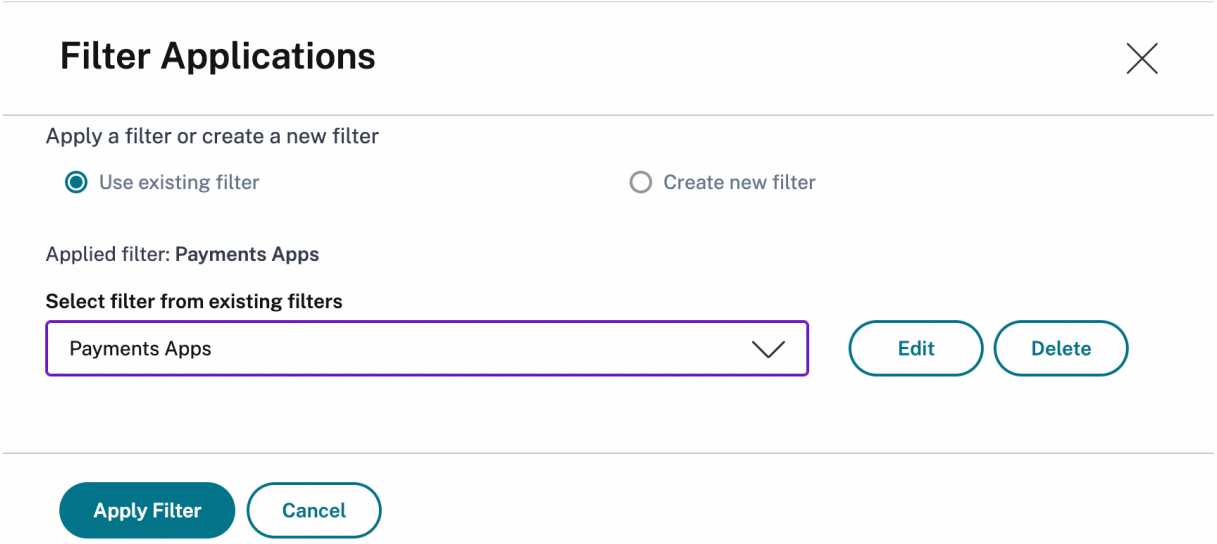
The filter is now created and applied. You can create more filters by following the same procedure. After you create filters, you can select and apply filters through the **Select filter from existing filters** list.

© 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

October 8, 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.

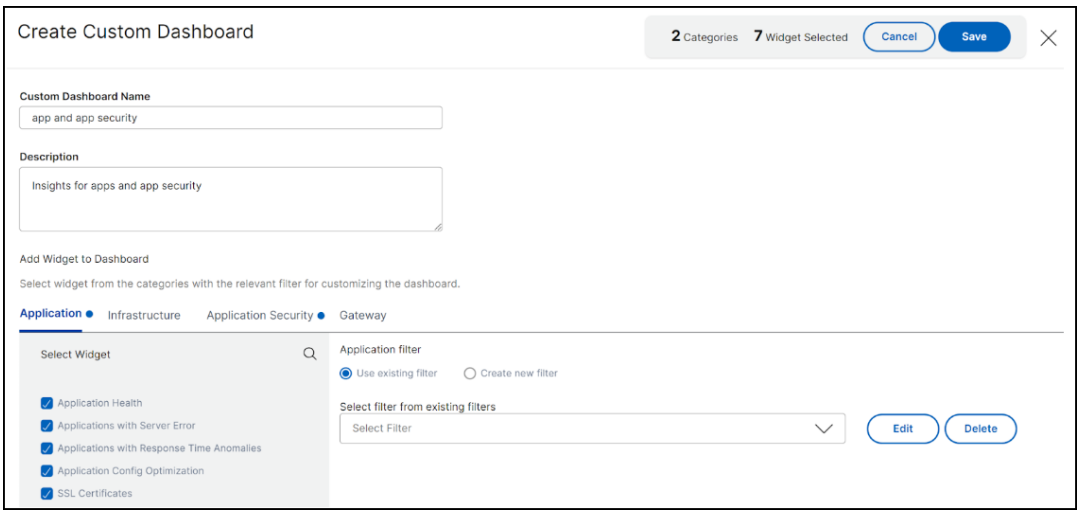
   b) **Description** - Provide a brief description to have additional details.

   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.

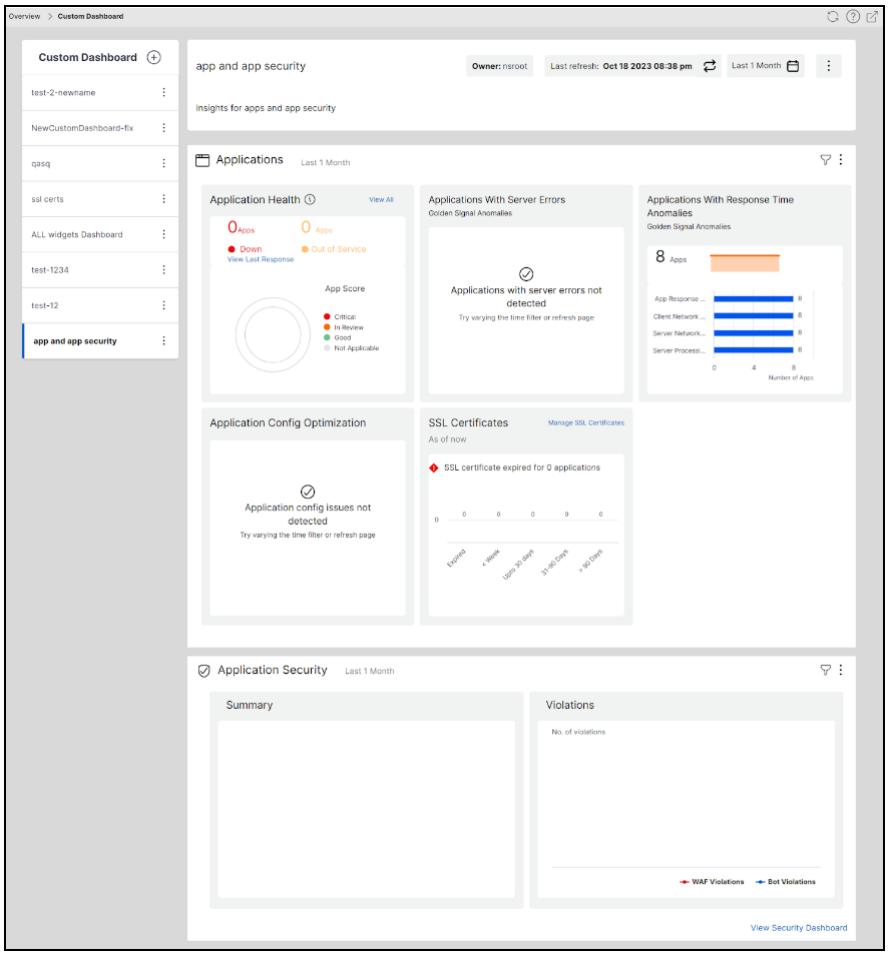
   d) **Application filter** - By default, the filter is applied to all applications. You can also create a filter and select only specific applications. For more information, see Create and apply filters.

   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.



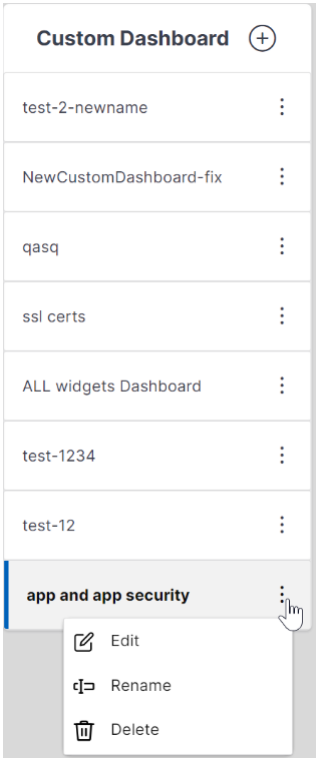
You can use the following options after you create a custom dashboard:

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

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

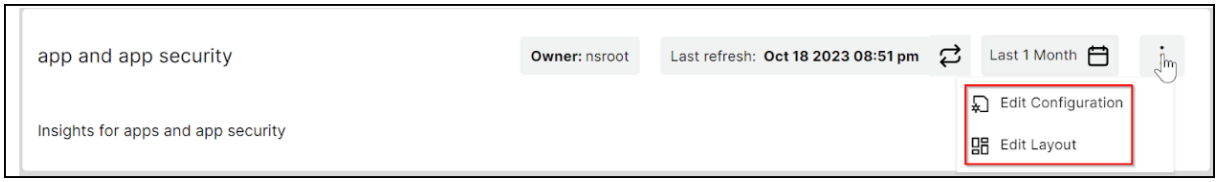
and so on.

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



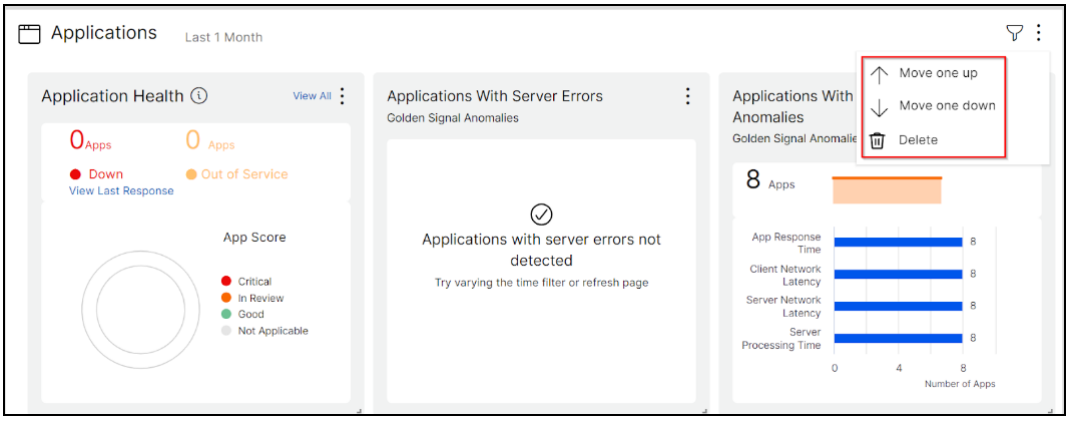
More options in the dashboard

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

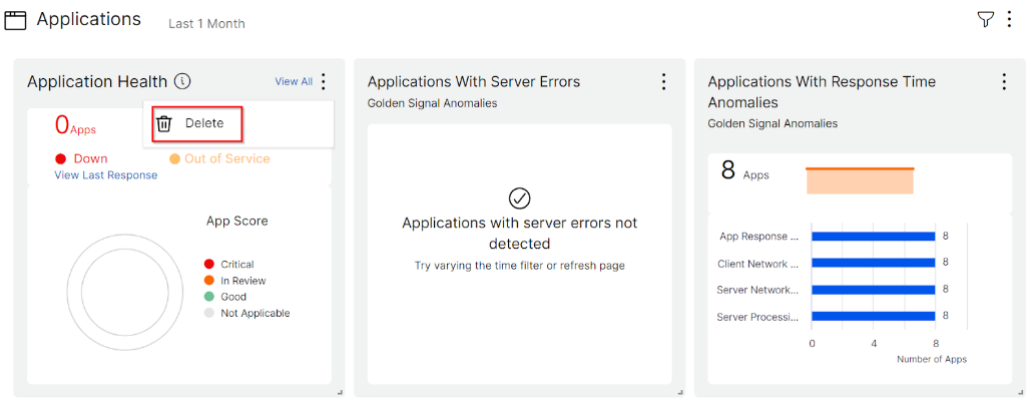


- **Edit Configuration**: You can also use this option to edit the dashboard by adding more widgets or removing widgets, applying filters, and so on.
- **Edit Layout**: You can use this option to have additional customization to the dashboard.
  - You can select to move up, down, or delete.

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

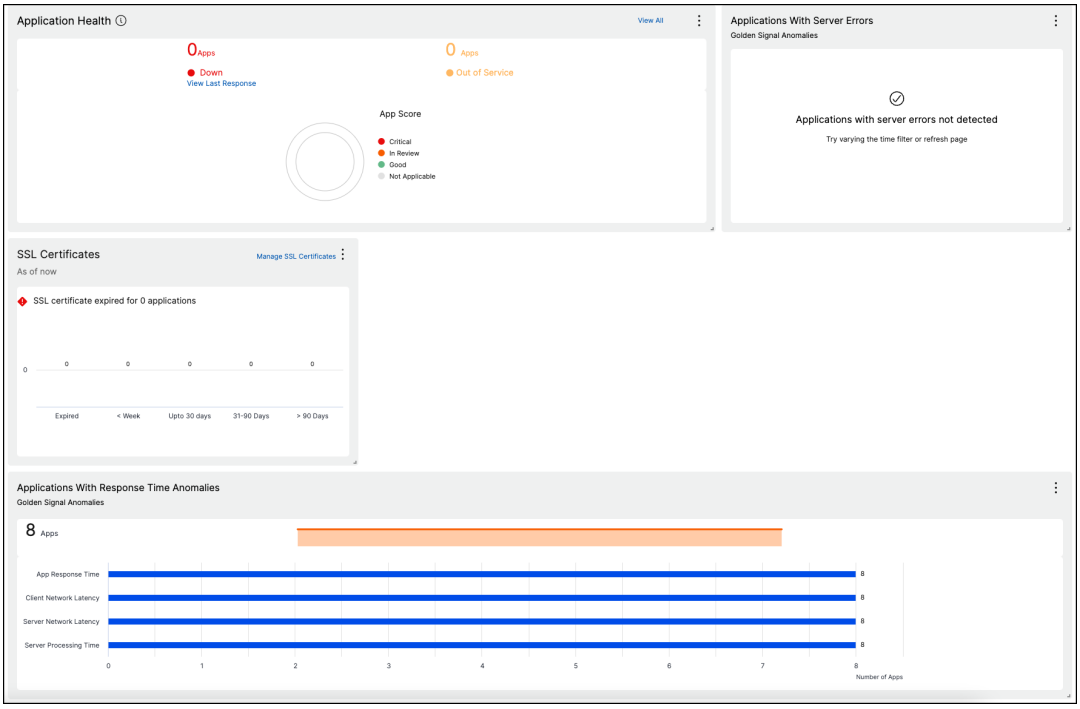


- In the Widgets, you can delete any widget by selecting the Delete option.



- Drag and drop 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.

Applications

September 27, 2025

The application analytics and management feature of NetScaler Console enables you to monitor the applications through 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 server or client
- Detect anomalies in the application traffic flows and take corrective actions

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

> **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 valid license for your NetScaler instances. For more information, see Licensing
- Ensure you have applied license for virtual servers. For more information, see Manage licensing on virtual servers

Application overview

Applications can be:

- Discrete applications
- Custom applications
- Microservices applications (k8s_discrete)

Discrete applications

All virtual servers that are licensed 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.

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.

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

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"**.
- By default, NetScaler Console enables you to add licenses for up to 2 applications. Depending upon your license, you can select and apply licenses for the applications that you want to monitor.

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 27, 2025

> **Note:**
>
> Starting from release 14.1 build 51.x, Web Insight analytics are visible for virtual servers that are configured with an IPv6 address.

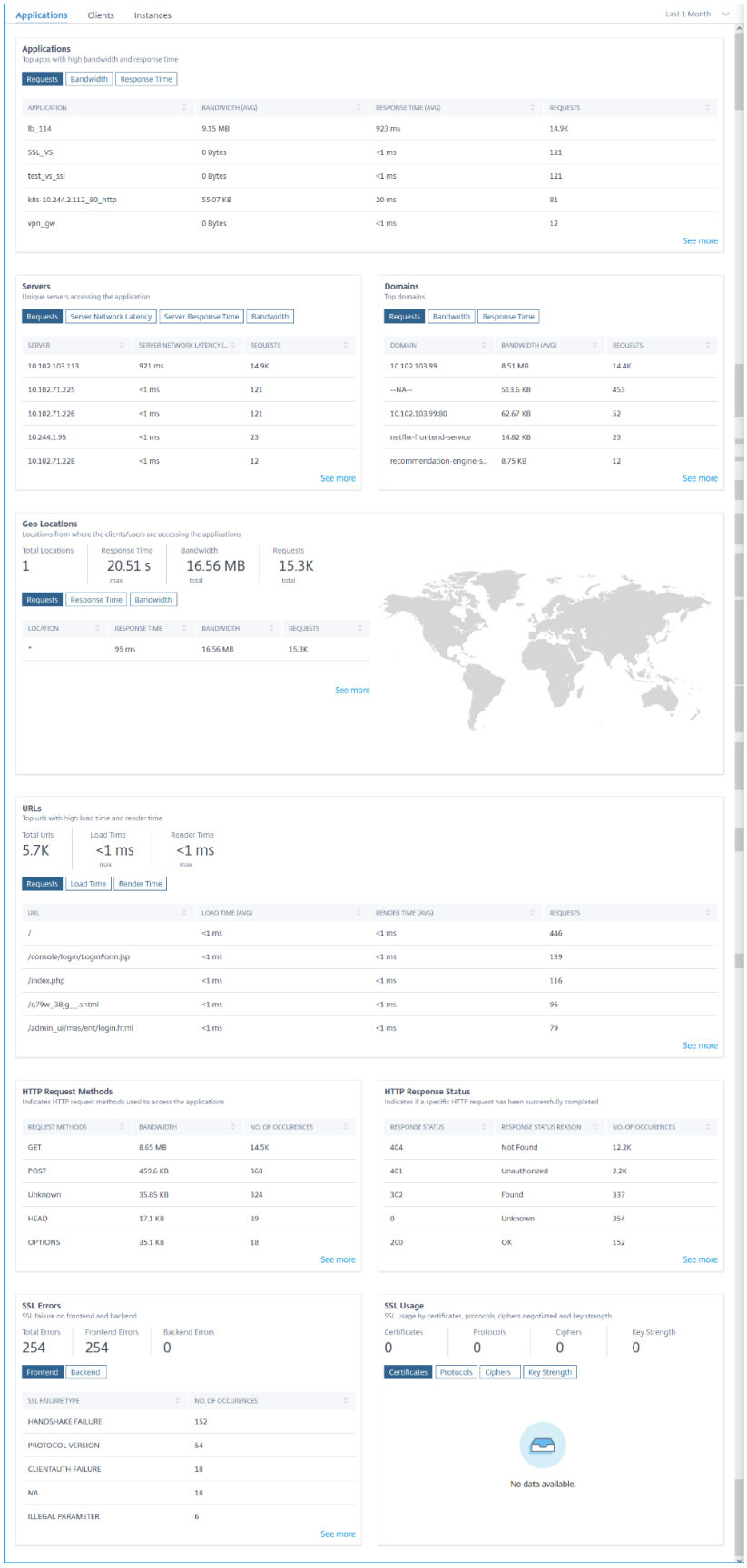
The improved Web Insight feature is augmented and provides visibility into detailed metrics for web applications, clients, and NetScaler instances. This improved Web Insight enables you to evaluate and visualize the complete application from the perspectives of performance and usage together. As an administrator, 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	Instances
Applications	Clients	Instance Metrics
Servers	Geo Locations	Applications
Domains	HTTP Request Methods	Domains
Geo Locations	HTTP Response Status	URLs
URLs	URLs	HTTP Request Methods
HTTP Request Methods	Operating System	HTTP Response Status
HTTP Response Status	Browsers	Clients
SSL Errors	SSL Errors	Servers
SSL Usage	SSL Usage	Operating System
		Browsers

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



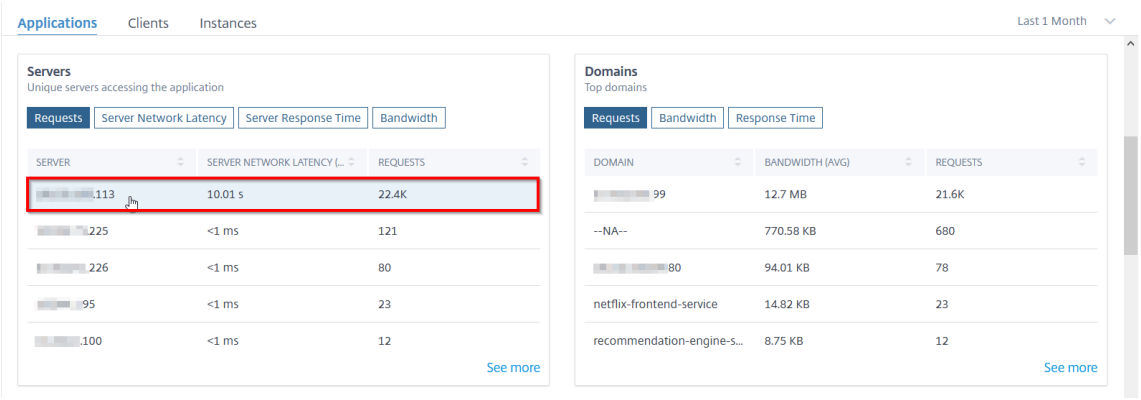
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 **14.1-4.x** 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.

For example, consider that you want to analyze the server network latency for 1-month time duration and take decision whether to scale up or scale down the production environment. To analyze this:

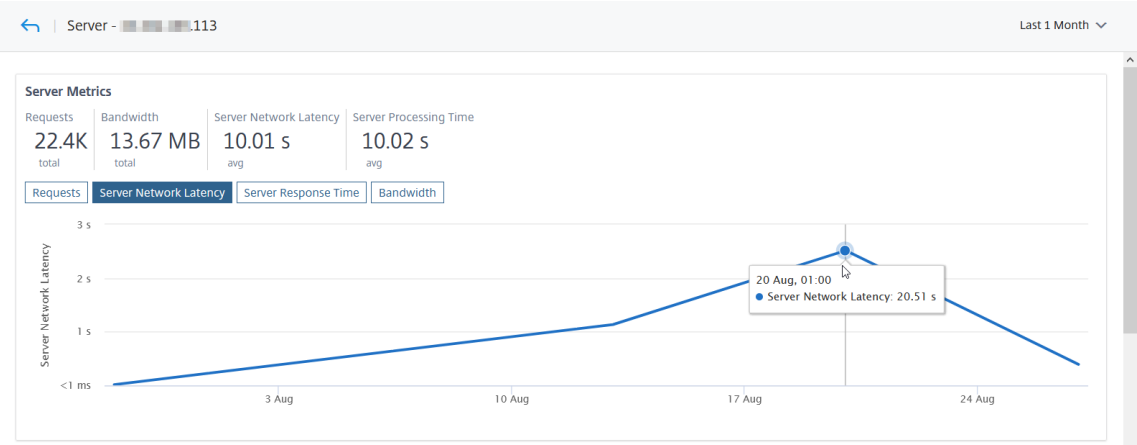
1. Select Last 1 Month from the list and from the **Applications** tab, scroll down to **Servers**, and click a server.



   The metrics details for the selected server are displayed.

2. Select the **Server Network Latency** tab to analyze the latency.

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

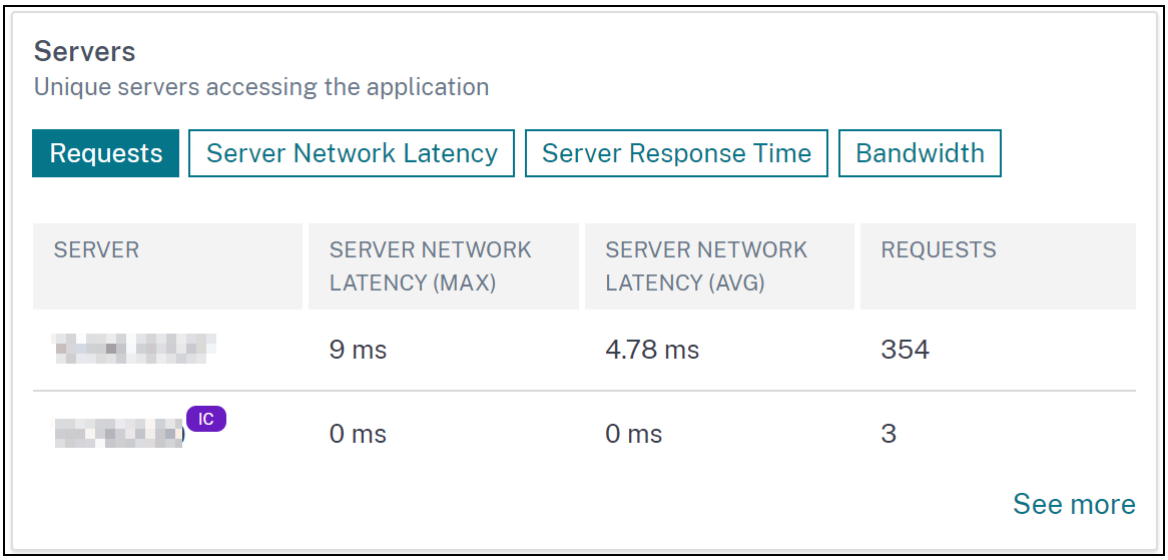


The average latency indicates 10.01 s and from the graph, you can analyze that the server network latency for the last 1 month seems to be high. As an administrator, you can take decision to scale up the production environment.

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.

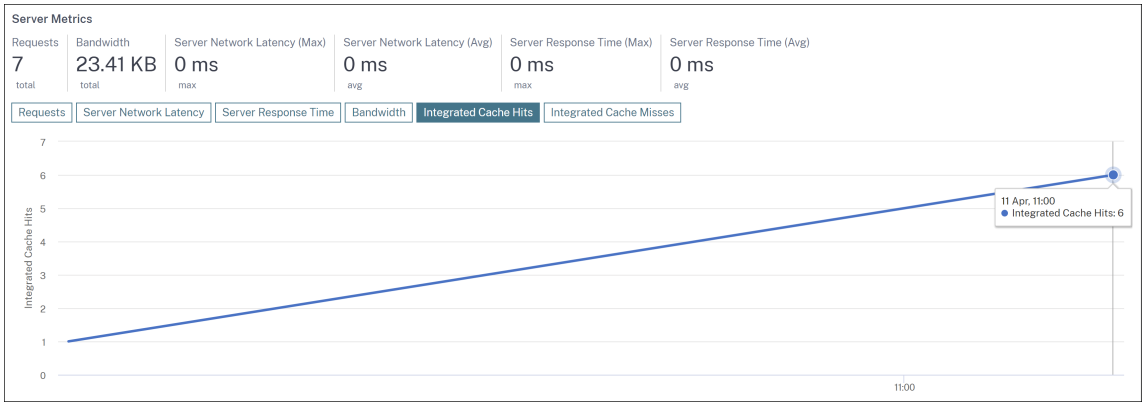


When you drill down a server to view more details, the **Server Metrics** display integrated cache hits and misses tabs.

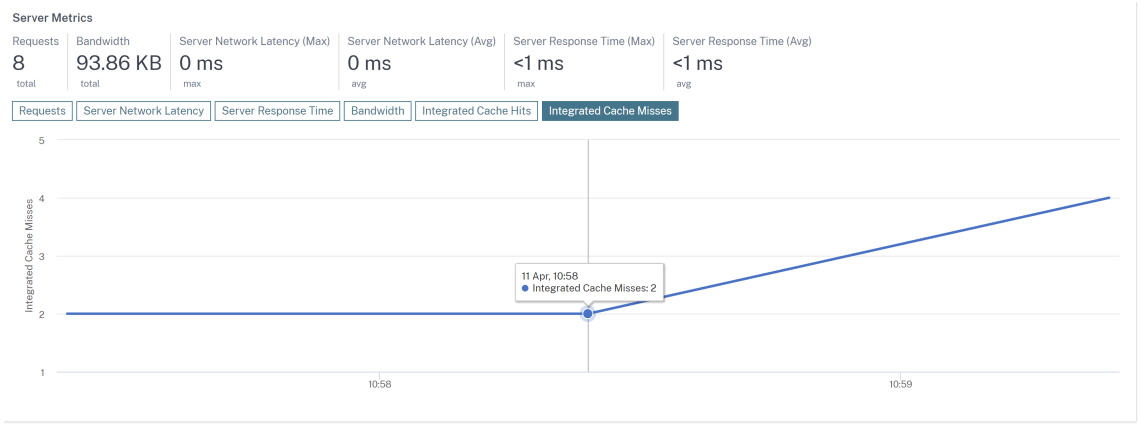
The graph view in:

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

- The **Integrated Cache Hits** tab enables you to view the total responses that the NetScaler appliance serves from the cache.



- The **Integrated Cache Misses** tab enables you to view the total responses that the NetScaler appliance serves from the origin server.



Troubleshoot Web Insight issues

For details, see the troubleshooting document Troubleshoot Web Insight issues.

View the root cause for application latency

September 27, 2025

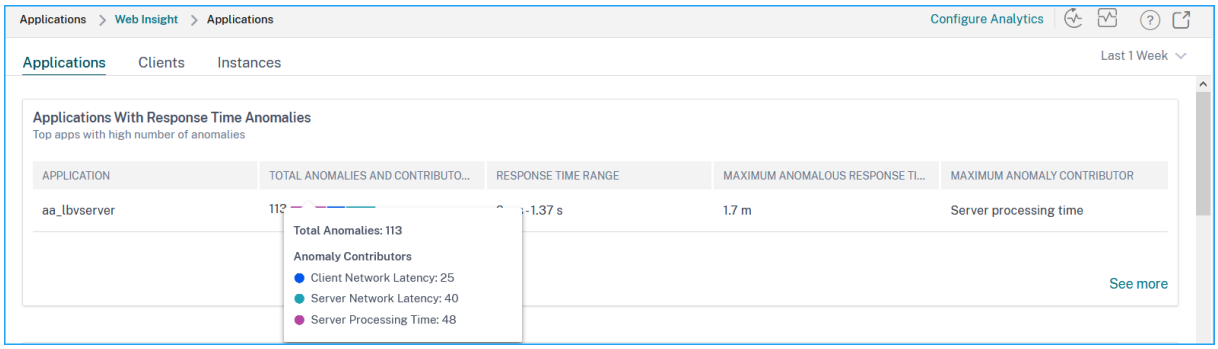
Application slowness is a major concern for any organization because it results in business impact or productivity. In **Applications > Web Insight**, you can now view a new metric called **Applications with Response Time Anomalies**. Using this metric, as an administrator, you can analyze whether the application latency arises from the following causes:

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

- Client network latency
- Server network latency
- Server processing time

NetScaler Console performs anomaly checks every hour and reports anomalies for the 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.

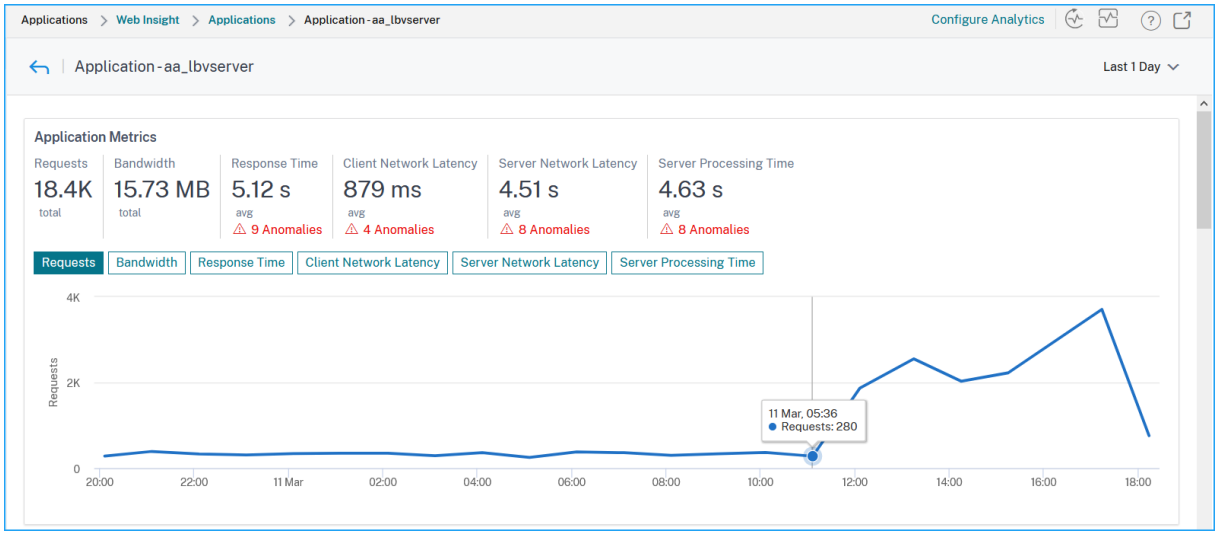


- **Application** –Denotes the application name.
- **Total Anomalies and Contributors** –Denotes the total anomalies from the application. When you hover the mouse pointer, you can view the total anomalies that are from the client network latency, server network latency, and server processing time respectively.
- **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:

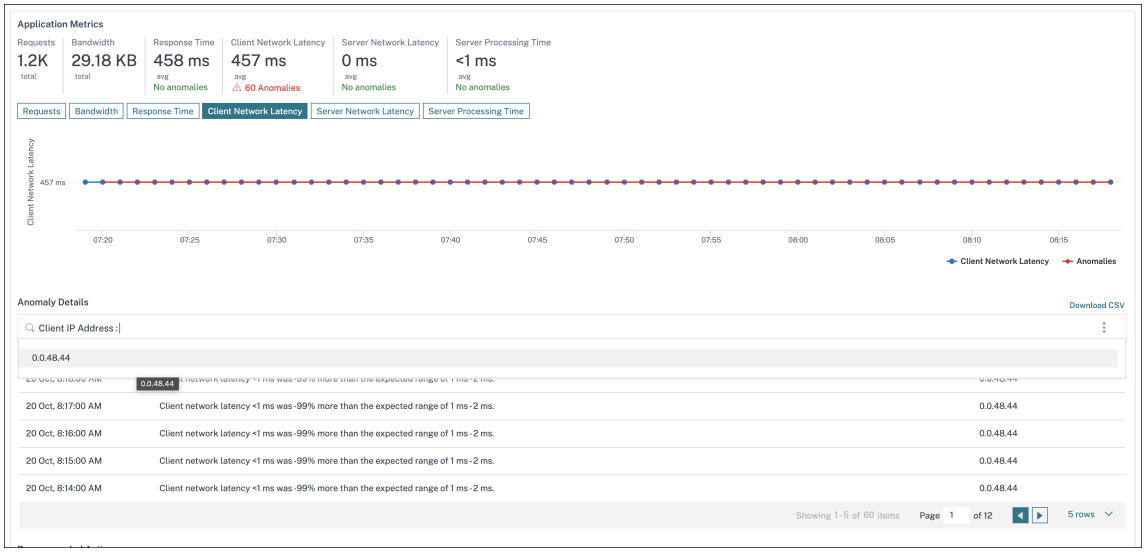
- **Summary** –An overview to visualize the application performance such as Response Time, Requests, and Bandwidth.
- **Requests** –The total requests received by the application. You can also view requests from the top 5 clients based on the total requests.
- **Bandwidth** –The total bandwidth processed 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:

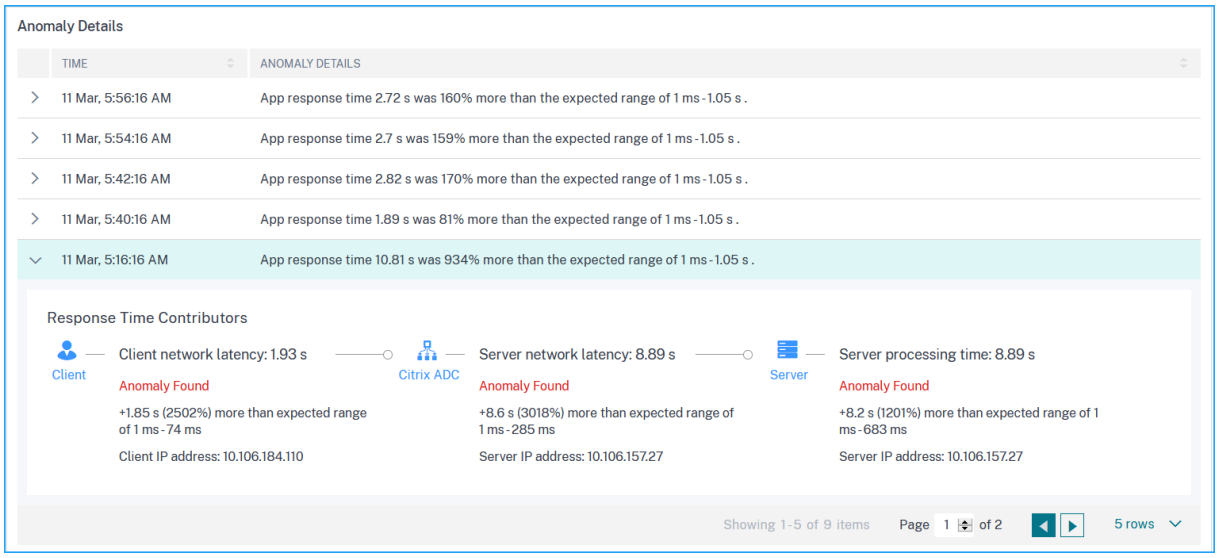
- **A search bar** - Click the search bar to view the IP address of all clients (in Client Network Latency) and servers (in Server Network Latency). You can select the IP address to filter results.
- **An export option** - Click **Download CSV** to export the details in CSV format.

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



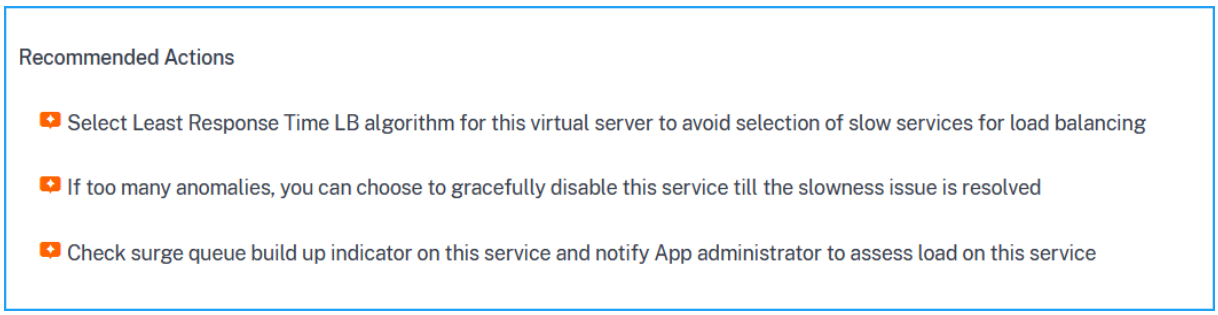
Response Time

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.

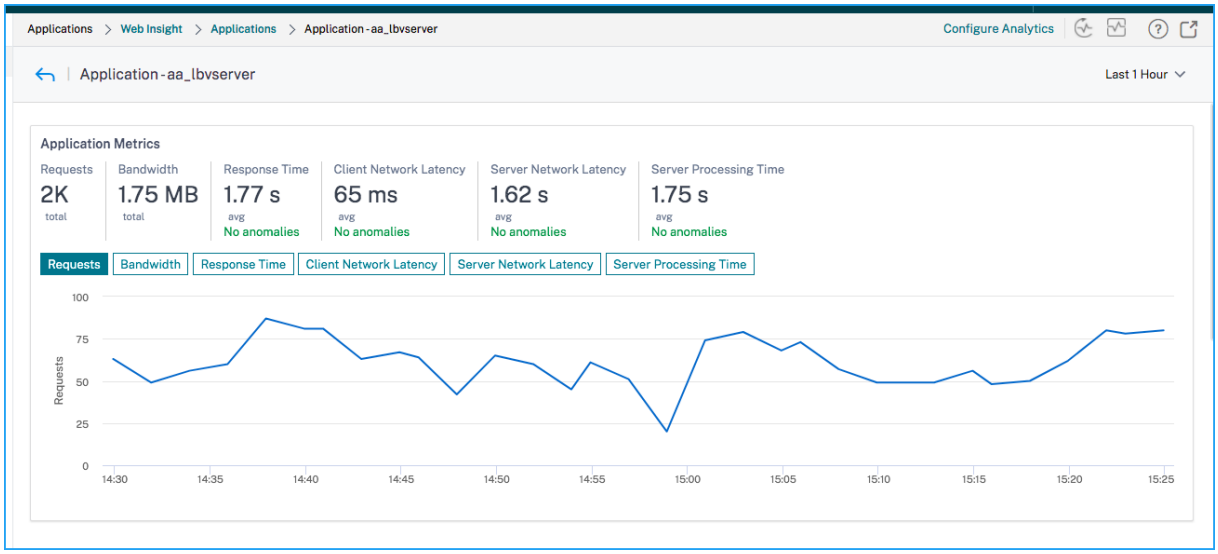
© 1997–2025 Citrix Systems, Inc. All rights reserved.



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 27, 2025

The service graph feature in NetScaler Console enables you to monitor all services in a graphical representation. This feature also enables you to view a detailed analysis and actionable metrics of the services. You can 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 view:

- 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

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

September 27, 2025

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 Lync.

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

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 NetScalers, and can also be moved among instances.
- **Auto-Generated UI**: NetScaler Console auto-generates UI forms used to fill in the parameters of the StyleBook when configuration is done using the NetScaler Console GUI. StyleBook authors do not need to learn a new GUI language or separately create UI pages and forms.
- **API-driven**: All configuration operations are supported by using the NetScaler Console GUI or through REST APIs. The APIs can be used in synchronous or asynchronous mode. In addition to the configuration tasks, the StyleBooks APIs also allow you to discover the schema (parameters description) of any StyleBook at runtime.

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

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 execute 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 execute it on the same or a different NetScaler 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 executed.

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 information:

- How to view StyleBooks
- Default StyleBooks
- Stylebooks developed for business applications
- Custom StyleBooks
- APIs in StyleBooks
- StyleBooks grammar

Application Security Dashboard

December 31, 2023

The **App Security** dashboard provides you the overview of security metrics for the discovered/licensed applications. This dashboard displays the security attack information for the discovered/licensed applications, such as sync attacks, small window attacks, DNS flood attacks, and so on.

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.

     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

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

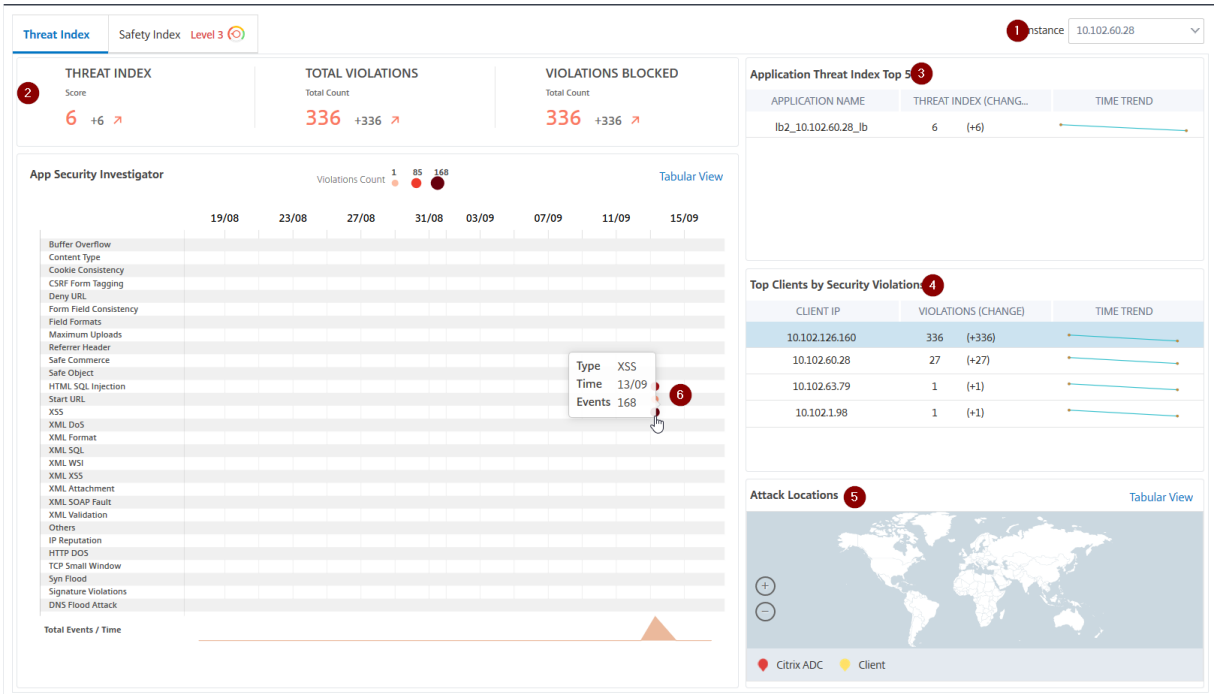
on the application. Violation information is sent to NetScaler Console only when a violation or attack occurs. A large number of breaches and vulnerabilities lead to a high threat index value.

- **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 the 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.

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 the results.

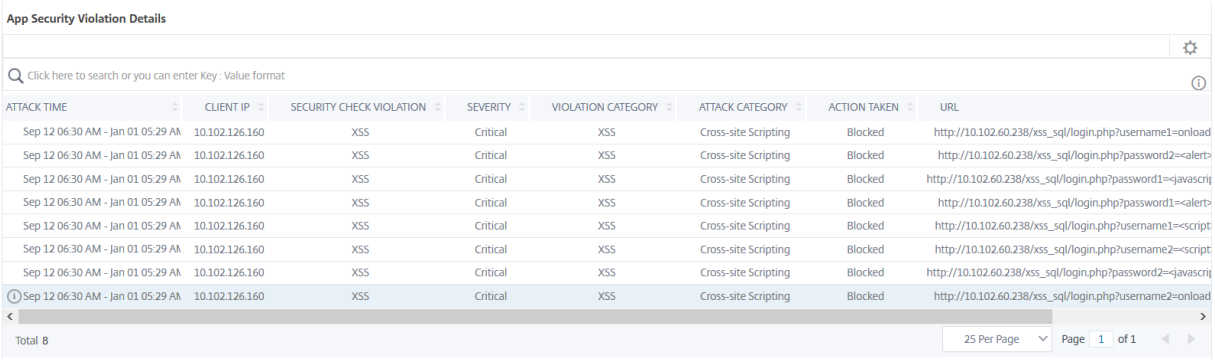
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 scripting (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.

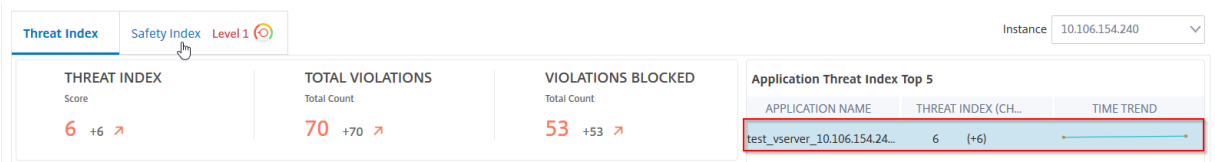
Safety index details

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:

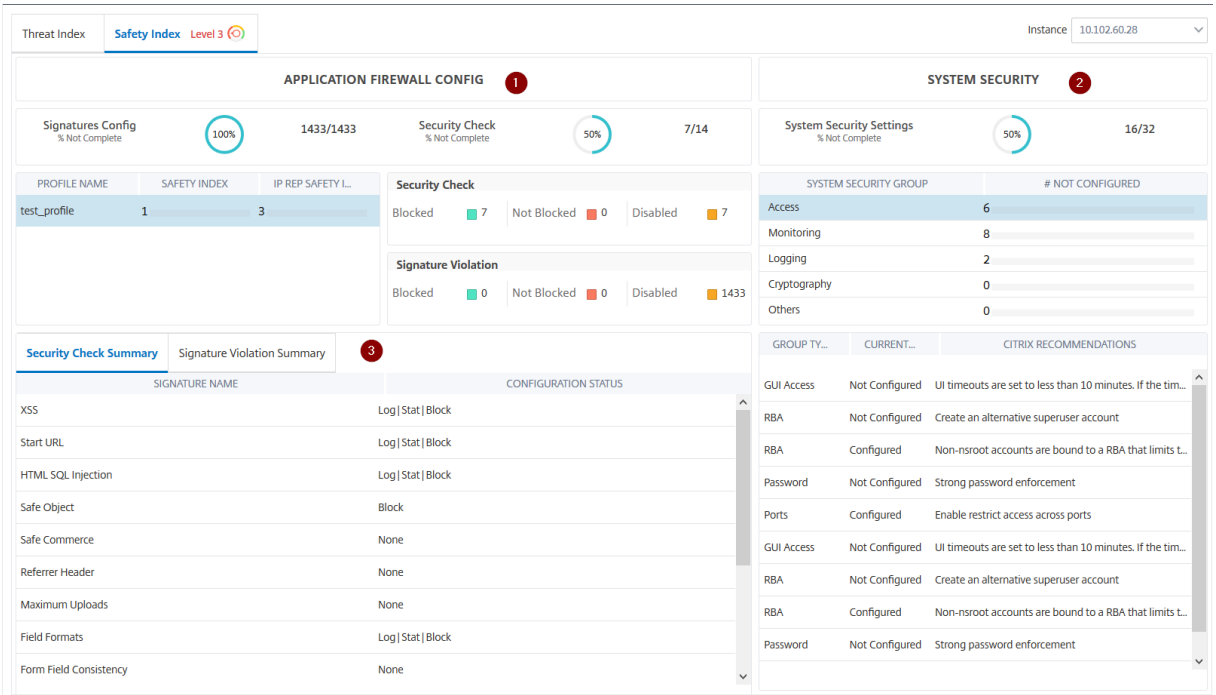
- **Application Firewall Configuration**. Shows how many signature and security entities are not configured.
- **NetScaler Console System Security**. Shows how many system security settings are not configured.

To view the **Safety Index** details, select a virtual server/application and click the **Safety Index** tab.



The details are displayed.

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



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 current status and Citrix recommendations.

3 - Displays the summary for Security Check and Signature Violation.

You can also view summary of the threat environment by enabling the **WAF Security Violations** for virtual servers and then navigating to **Security** > **Security Violations**.

Unified Security dashboard

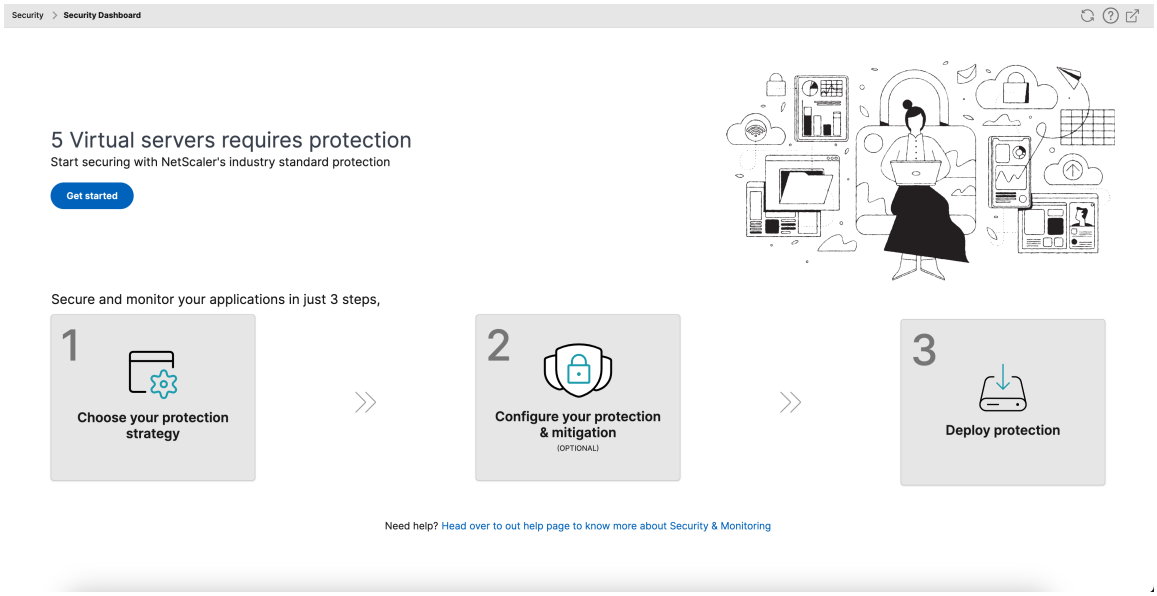
September 27, 2025

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 Style-Books or directly on NetScaler® instances, the following page appears after you click **Secu-**

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

rity > Security Dashboard.

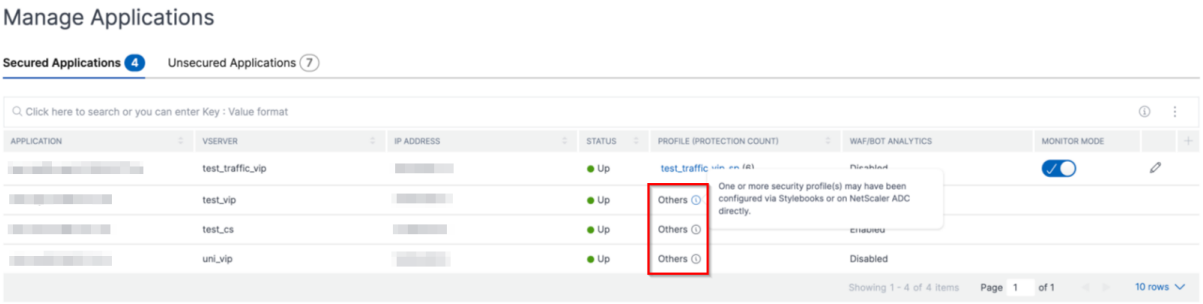


- You can view the total number of virtual servers that require protection. Click **Get Started** to view details in **Unsecured Applications**.
- The eligible virtual server types for configuring protections are load balancing and content switching.

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**.

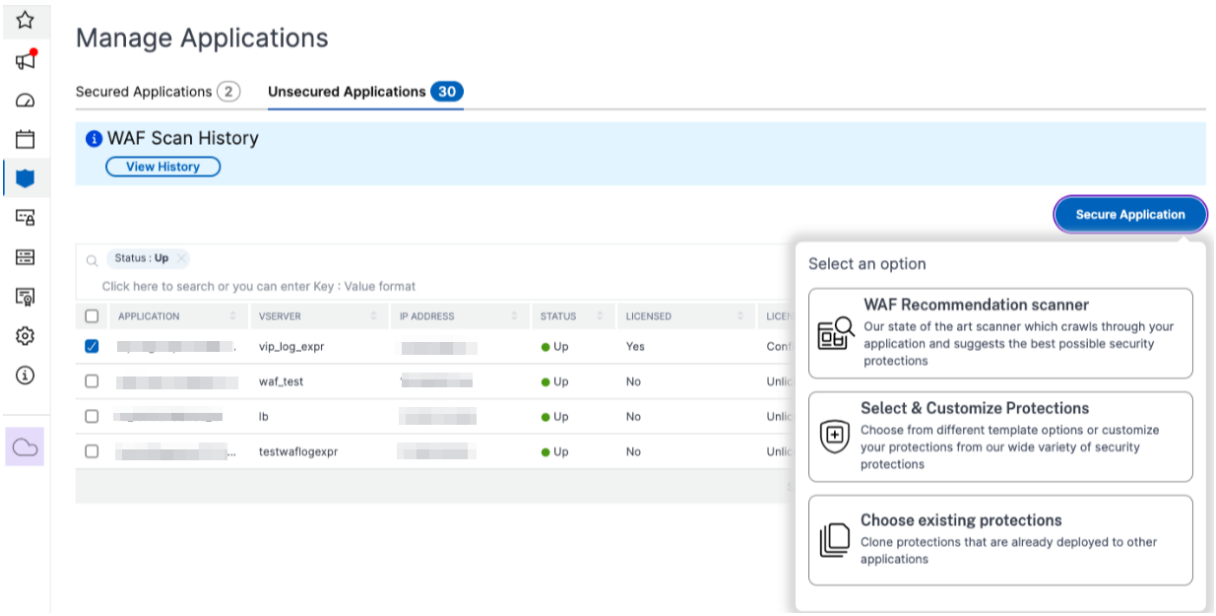


Configure protections for unsecured applications

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

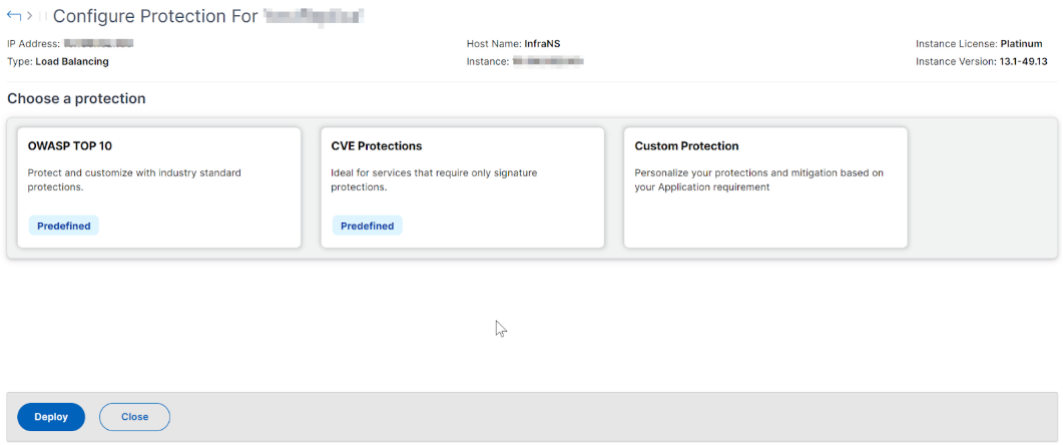
> **Note:**
>
> The maximum supported configuration entities (rules) in Block list is 32.

In the **Unsecured Applications** tab, select an application, and click **Secure Application**.



You can select either of the following options to protect your application:

- **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

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

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 click **View Report** and then apply recommendations later.

Prerequisites:

- The NetScaler instance must be 13.0 41.28 or later (for security checks) and 13.0 or later (for signatures).
- Must have the premium license.
- Must be the load balancing virtual server.

To get started with WAF recommendation scan, you must provide the following information:

1. Under **Scan Parameters**:
   - **Domain Name** –Specify a valid accessible IP address or the publicly reachable domain name that is associated with the application. For example: www.example.com.
   - **HTTP/HTTPS Protocol** –Select the protocol of the application.
   - **Traffic Timeout** –The wait time (in seconds) for a single request during the scan. The value must be greater than 0.

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

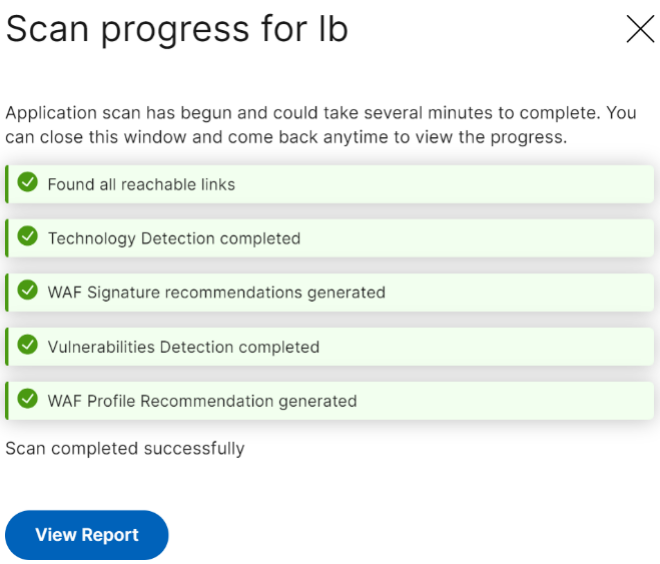
- **URL to start scan from** –The home page of the application to initiate the scan. For example, `https://www.example.com/home`. The URL must be a valid IPv4 address. If the IP addresses are private, then you must ensure that the private IP address is accessible from the NetScaler Console on-prem management IP.
- **Login URL** –The URL to which the login data is sent for authentication. In HTML, this URL is commonly known as the action URL.
- **Authentication Method** –Select the supported authentication method (form based or header based) for your application.
  - Form-based authentication requires submitting a form to the login URL with the login credentials. These credentials must be in the form of form fields and their values. The application then shares the session cookie that is used to maintain sessions during the scan.
  - Header-based authentication requires the Authentication header and its value in the headers section. The Authentication header must have a valid value and is used to maintain sessions during the scan. The form-fields should be left empty for Header-based.
- **Request Method** –Select the HTTP method used when submitting form data to the login URL. The allowed request method is **POST**, **GET**, and **PUT**.
- **Form Fields** –Specify the form data to be submitted to the login URL. Form Fields are required only if you select the form-based authentication. You must specify in the key-value pairs, where **Field Name** is the Key and **Field Value** is the Value. Ensure that all form fields needed for login to work are added correctly, including passwords. The values are encrypted before storing it in the database. You can click **Add** to add multiple form fields. For example, **Field Name** –user name and **Field Value** –admin.
- **Logout URL** –Specify the URL that terminates the session after accessing. For example: `https://www.example.com/customer/logout`.

2. Under **Scan Configurations**:
   - **Vulnerabilities to check** –Select the vulnerabilities for the scanner to detect them. Currently, this is done for SQL Injection and Cross-site scripting violations. By default, all the violations are selected. After selecting the vulnerabilities, it simulates these attacks on the application to report the potential vulnerability. It is recommended to enable this detection that is not in the production environment. All other vulnerabilities are also reported, without simulating these attacks on the application.
   - **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).

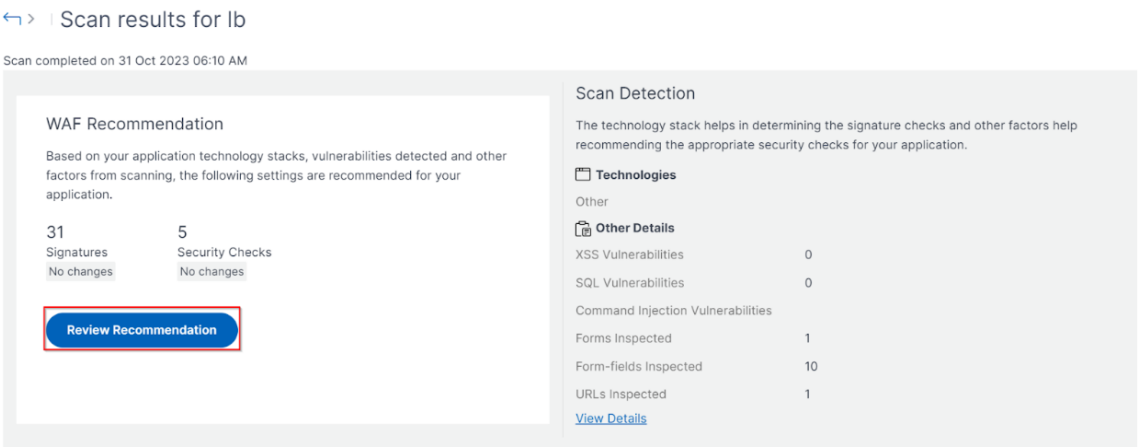
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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**.

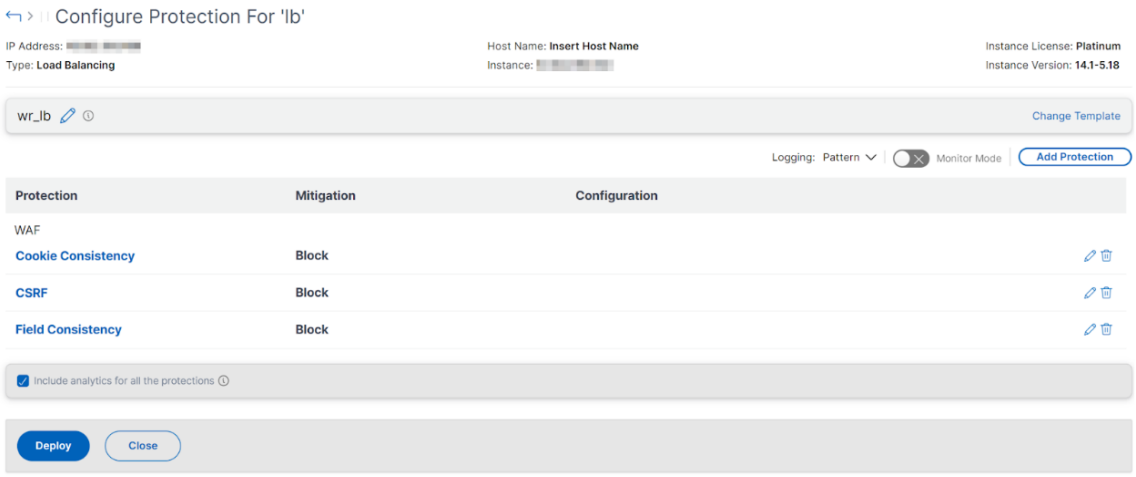


4. In the scan results page, click **Review Recommendation**.



5. Review the protections or edit/add any other protections, and click **Deploy**.

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

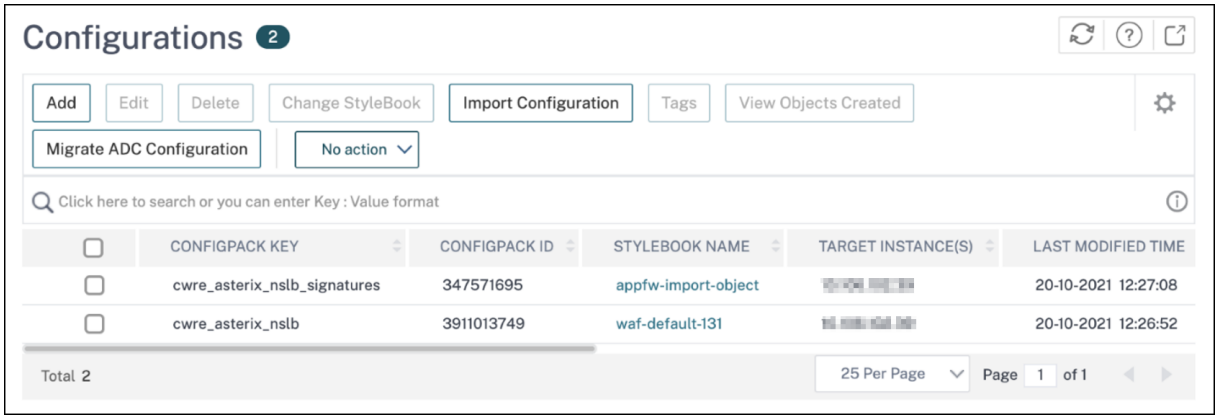


When you apply security checks successfully:

- 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.

> **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**.



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

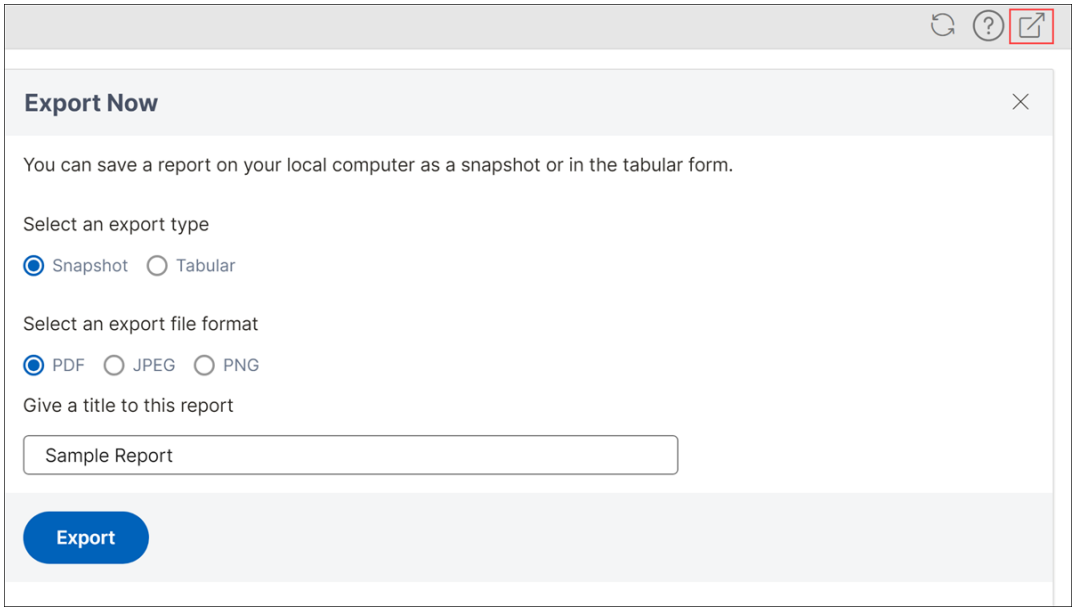
Export the WAF scanner report

To export the WAF scanner report, follow these steps:

1. Navigate to **Security > Dashboard > Manage Applications.**
2. In the **Unsecured Applications** tab, click **View History**.
3. On the **Scan History** page, select the desired scan and click **View Report**.
4. On the **Scan Results** page, click the **Export** icon.
5. On the **Exports Now** page, choose the export type.

For **Snapshot** export type:

1. Select an export file format: PDF, JPG, or PNG
2. Enter a title for the report.
3. Click **Export**.

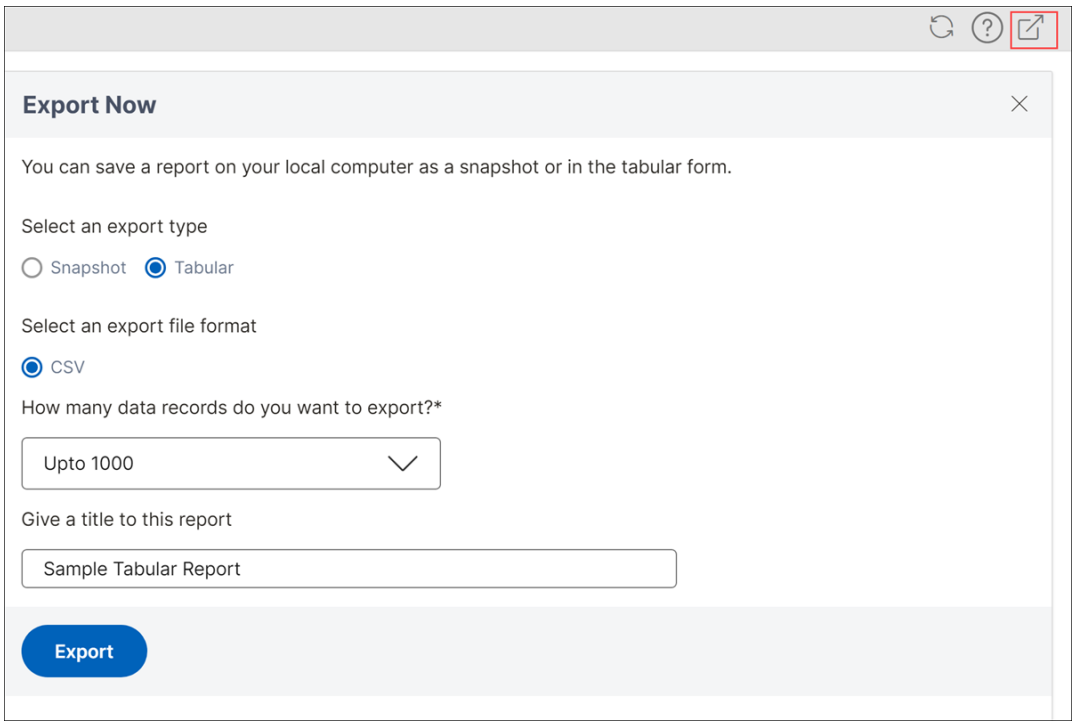


For **Tabular** export type:

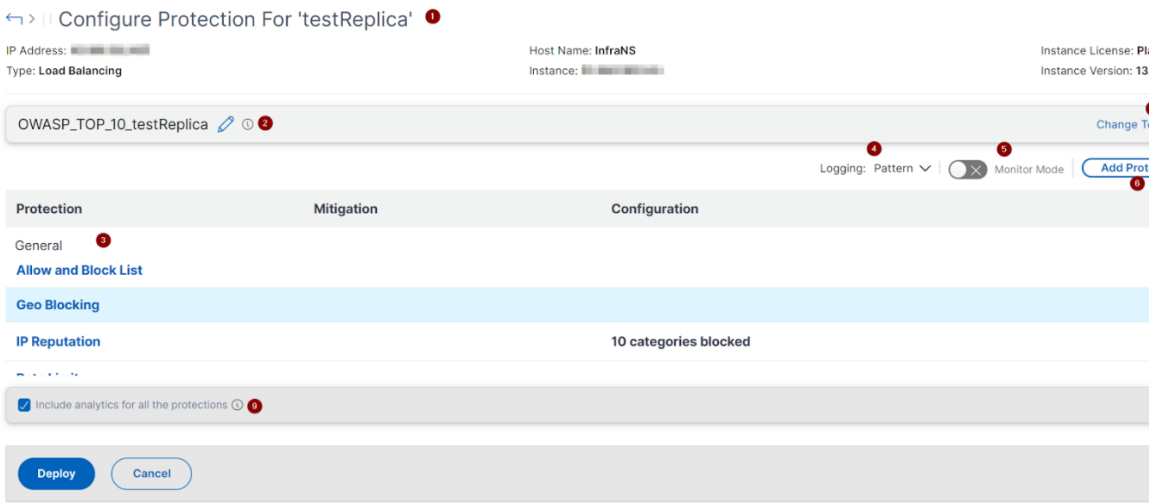
Starting from release 14.1 build 25.x, you can export the WAF scanner report in a tabular format.

1. Select the CSV file format.
2. Select the number of data records to export from the list.
3. Enter a title for the report.
4. Click **Export**.

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



Select and customize protections



OWASP Top 10

1 - Provides information about the application such as IP address, virtual server type, license type, from which instance the application is configured, and so on.

2 - Displays the selected template. You can rename it based on your choice.

3 - Displays the protections. Some protections require additional information.

4 - Displays the verbose log type. You can select the following options:

- **Pattern**. Logs only violation pattern.

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

- **Pattern payload**. Logs violation pattern and 150 bytes of extra JSON payload.
- **Pattern, payload, header**. Logs violation pattern, 150 bytes of extra JSON payload and HTTP header information.

5 - Allows you to enable the Monitor Mode. If you enable Monitor Mode, the traffic is only logged and mitigations are not activated.

6 - Enables you to add more protections. Click **Add Protections** and review them to add.

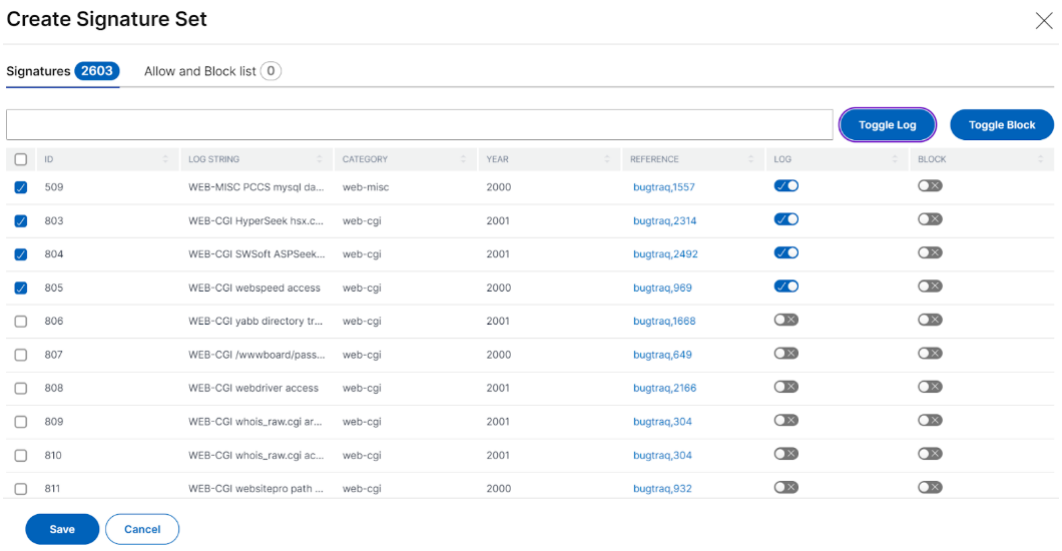
7 - Allows you to choose a new template by using the Change Template option.

8 - Enables you to edit or delete the protection.

9 - Enables analytics for the protections that you select. This option is selected by default. You can view analytics for the configured protections at **Security > Security Violations**.

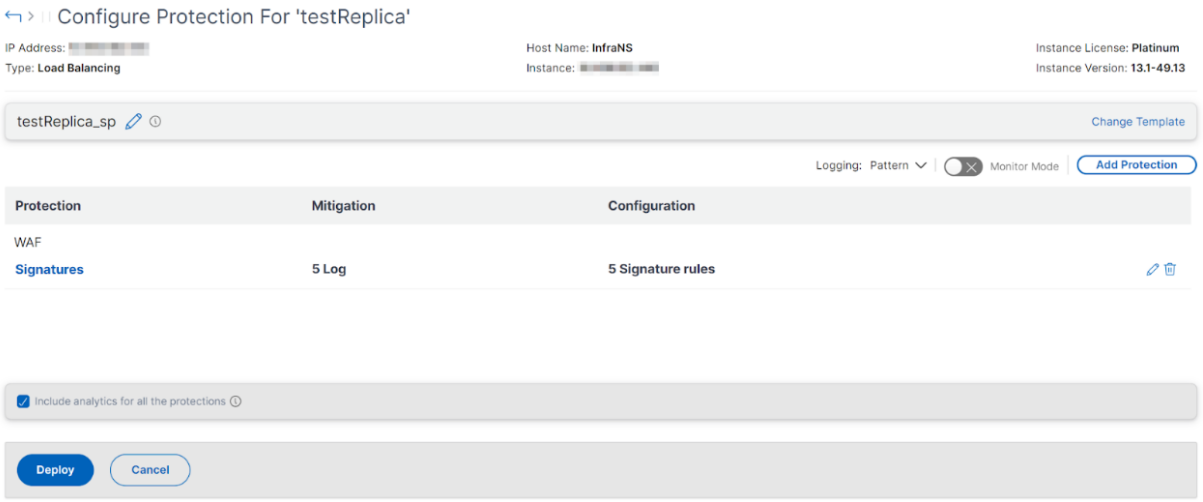
After you configure the protections, click **Deploy**.

CVE protections To deploy the CVE protections, click **Create CVE Protection**. In the **Create Signature Set** page, select the signatures from the list to configure the log or block action, and then click **Save**.



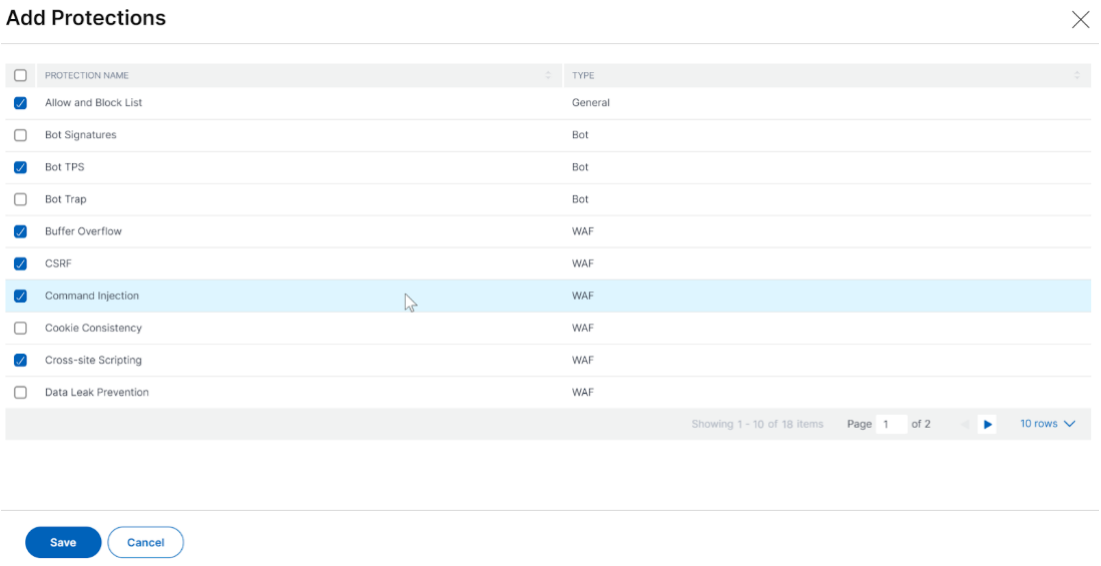
After you click **Save**, you can view the signatures added to the configuration page.

© 1997–2025 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**.

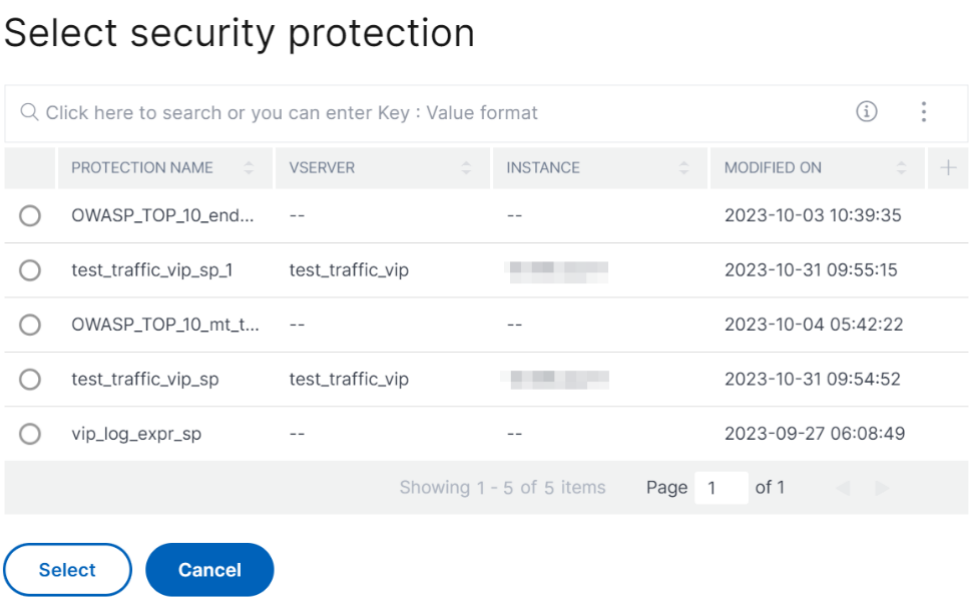


After you click **Save**, review the selected protections in the configuration page, and then click **Deploy**.

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

September 27, 2025

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 Security Violations and Bot Security Violations
- 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.

Prerequisite

Ensure if **Metrics Collector** is enabled. For more information, see Configure Intelligent App Analytics.

View API analytics

September 27, 2025

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 that you enable Web Insight on the API instances. For more information, see Configure analytics on virtual servers.

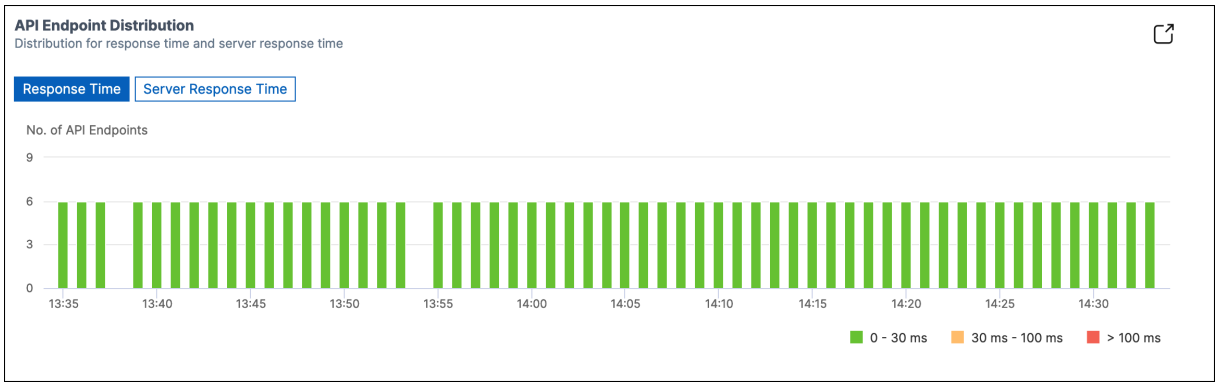
In **API Analytics**, you can monitor the response time of API instances and endpoints that are added as part of API definitions. It also displays the bandwidth consumed by API instances and endpoints.



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.



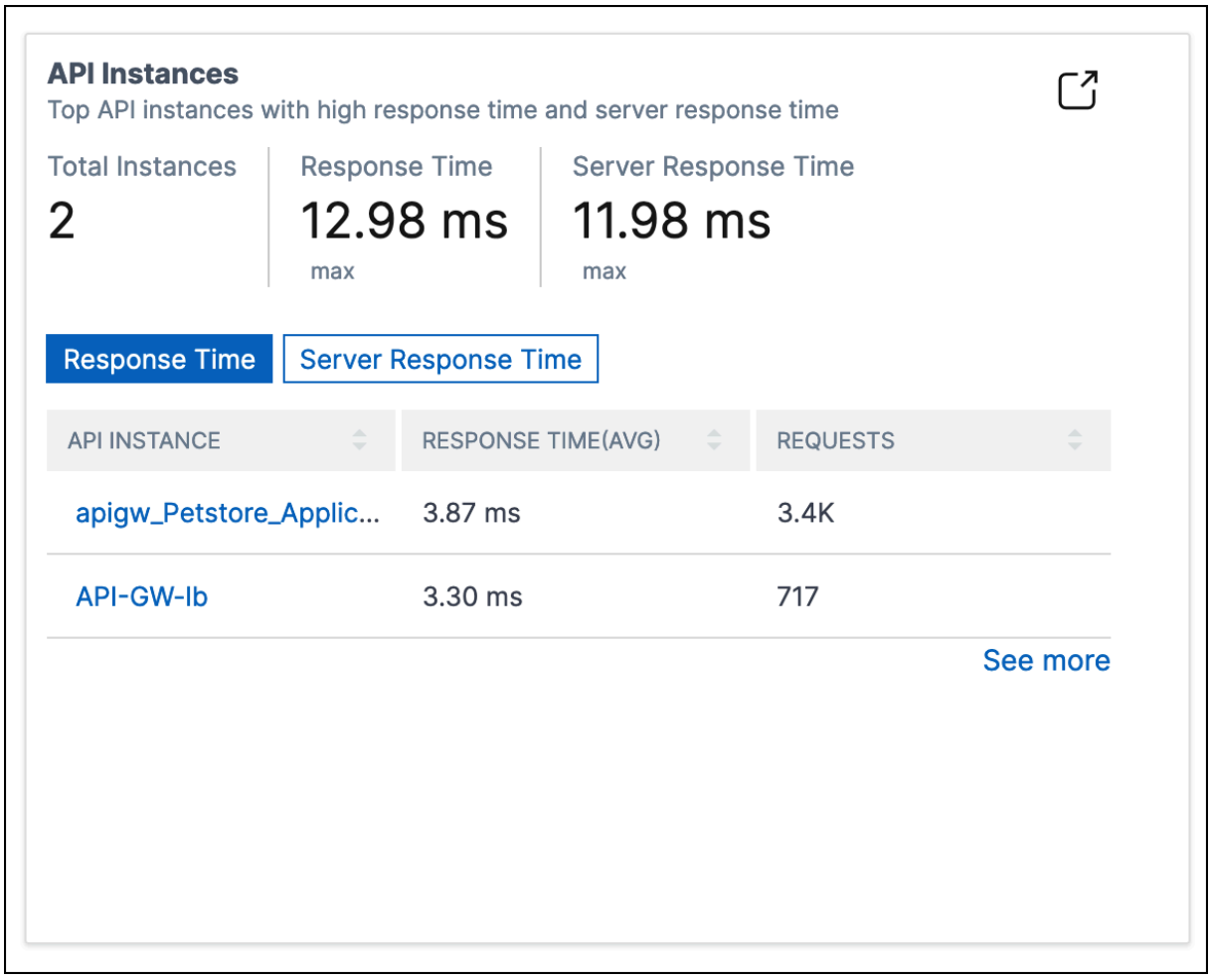
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.



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

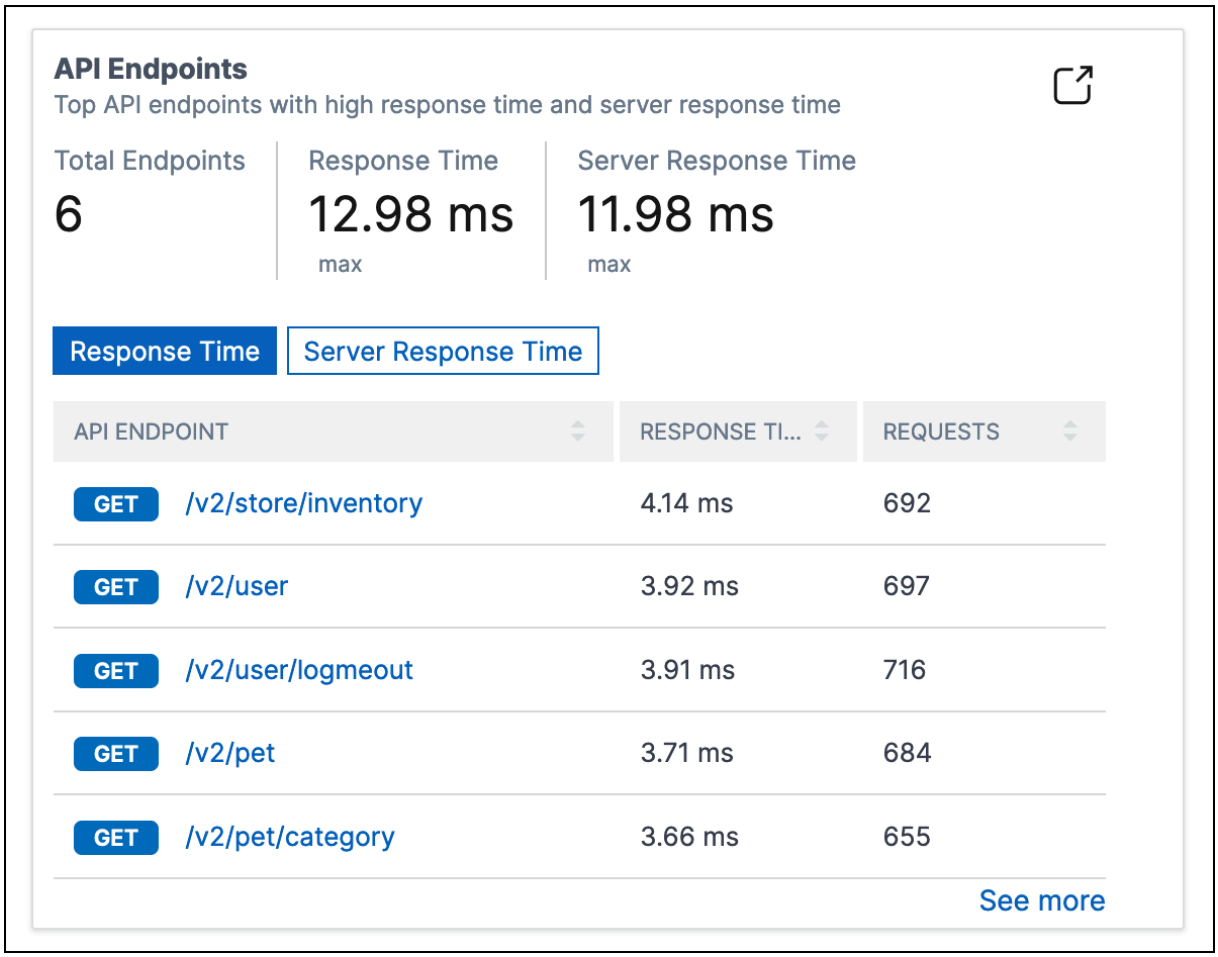
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Authentication failures

API Endpoints	Requests	Response Time	Server Response Time	Bandwidth	Auth Failures
5	3.5K	3.88 ms	1.98 ms	3.04 MB	0

API endpoints

The **API Endpoints** tile displays the top endpoints with high application and server response time.

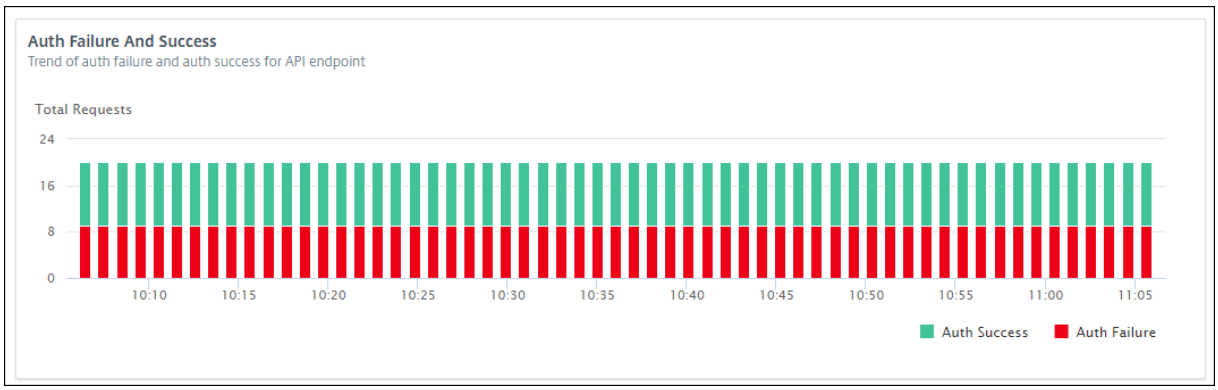


Select an API endpoint to view performance, usage, and security details.

Authentication failures

The **Auth Failures** tile displays top API endpoints that have more authentication failures. The authentication failure or success happens based on the policy added to an API definition.

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



If you want to view authentication failure and success rate in an API endpoint, do the following:

1. Select an endpoint from **API Endpoints**.
2. Select the **Security** tab. This tab displays the authentication failures and successes in the selected endpoint.



If you want to view the authentication failure and success rate in the API endpoints of an instance, do the following:

1. Select an instance from **API Instance**.
2. Select the **Security** tab. This tab displays the authentication failures and successes in the endpoints of the selected instance.

View different API insights

Navigate across API Analytics to view a specific information on the following:

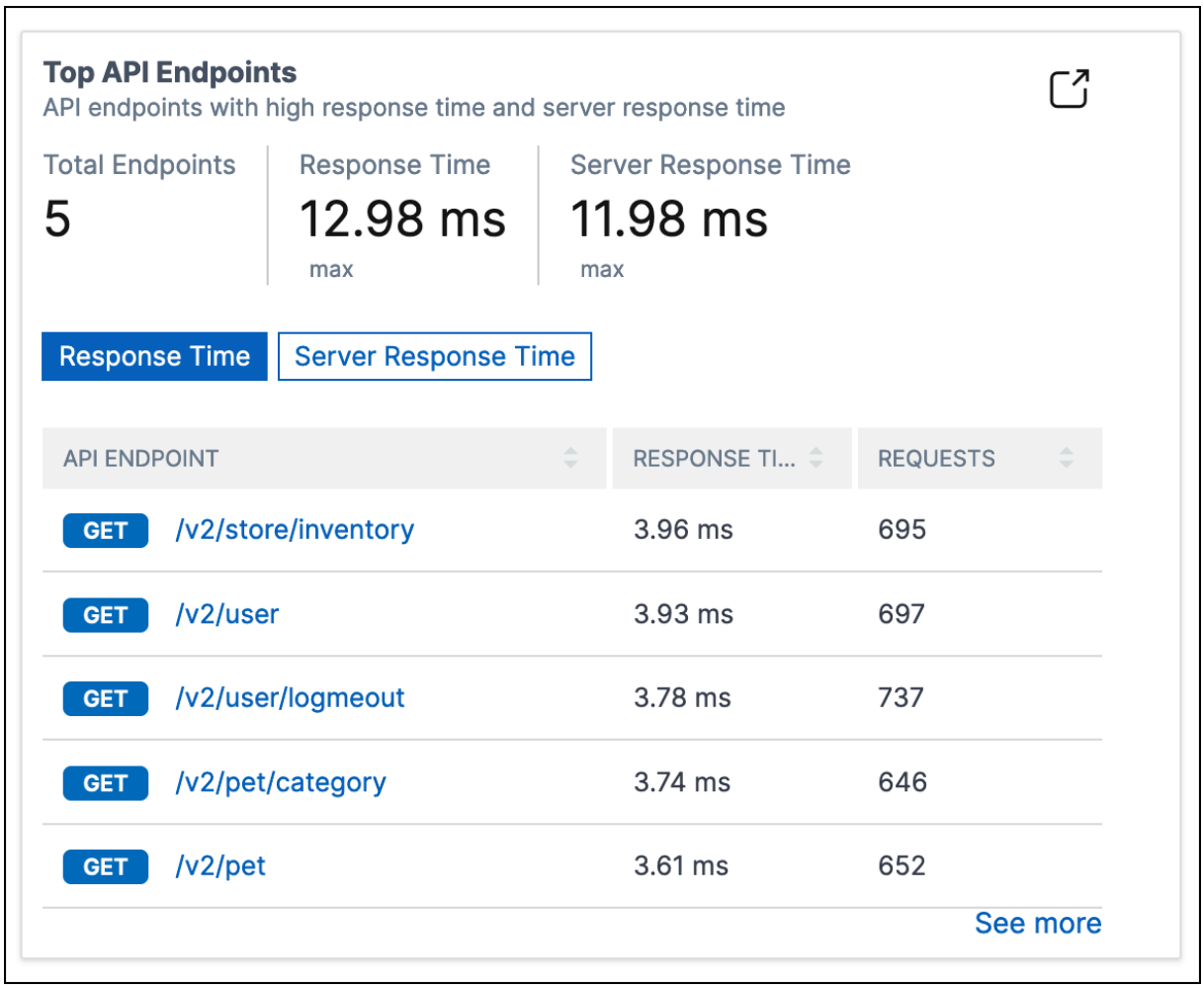
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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

View top API endpoints in an instance

The **API Analytics** page displays the top endpoints that have high response time. If you want to view similar endpoints of an instance, select an instance from **API Instances**.

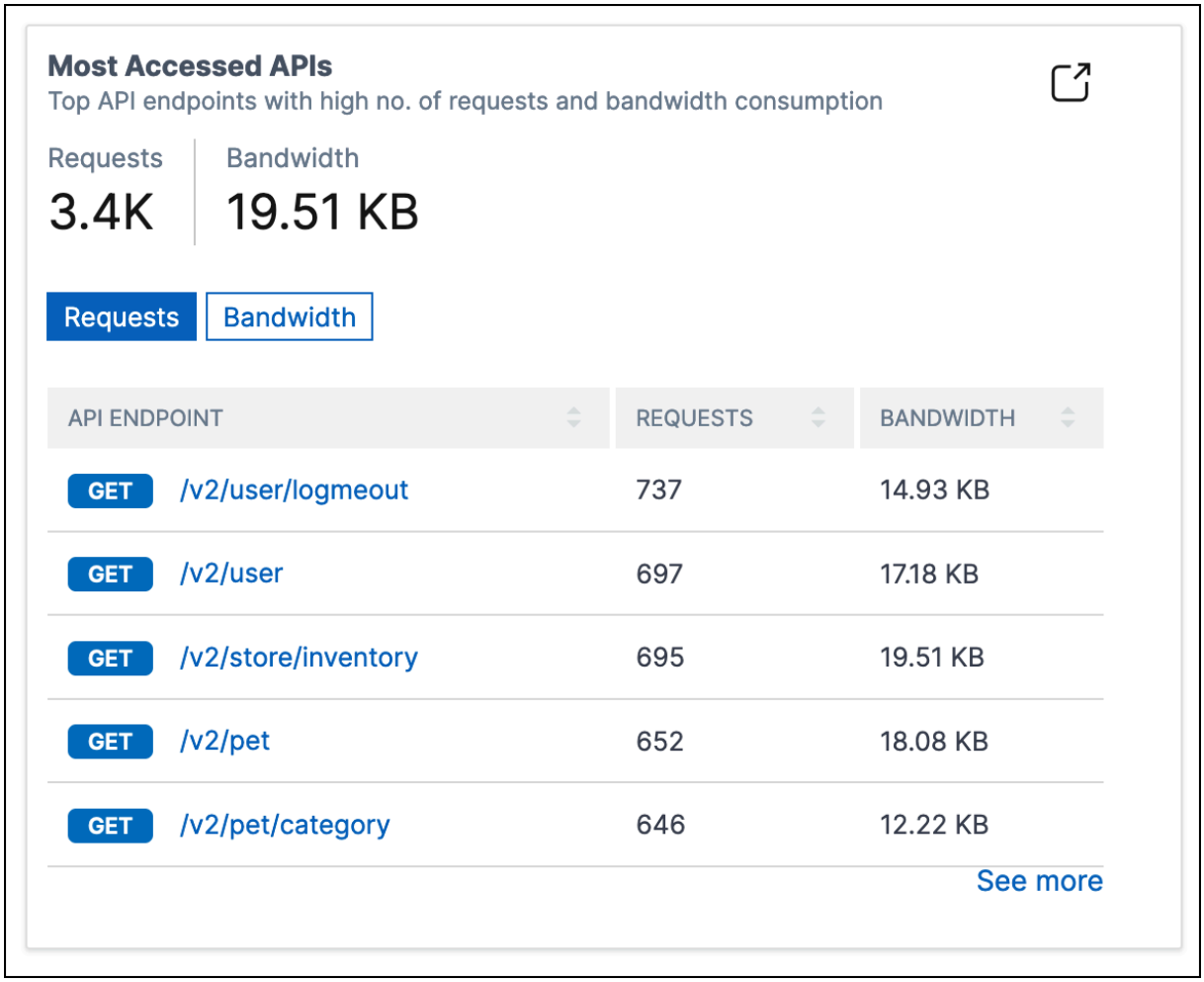
The **Top API Endpoints** tile displays the endpoints that have high application and server response time.



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

View most accessed APIs

In **API Analytics**, select an API instance from API instances. The **Most Accessed APIs** tile displays the top endpoints that have more requests and bandwidth.

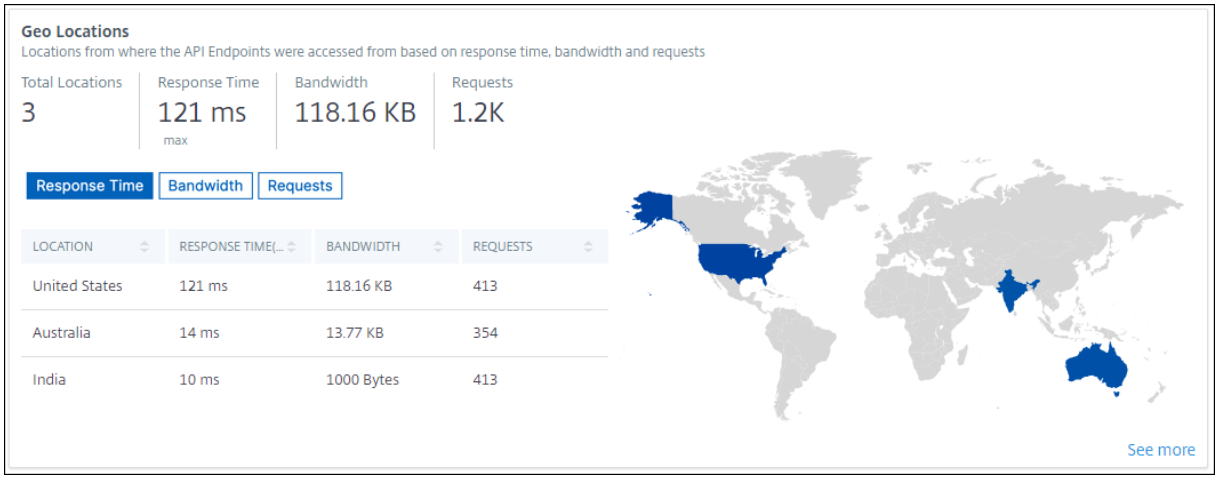


View geo-location of an endpoint

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.

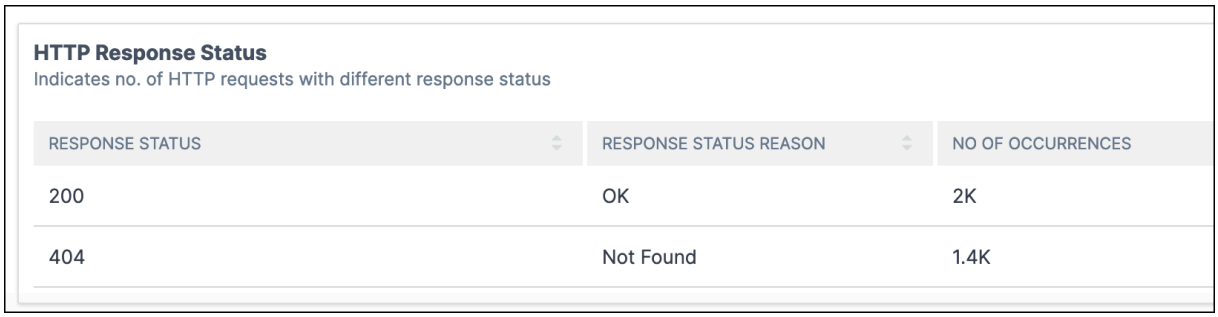


View HTTPS response status

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**.

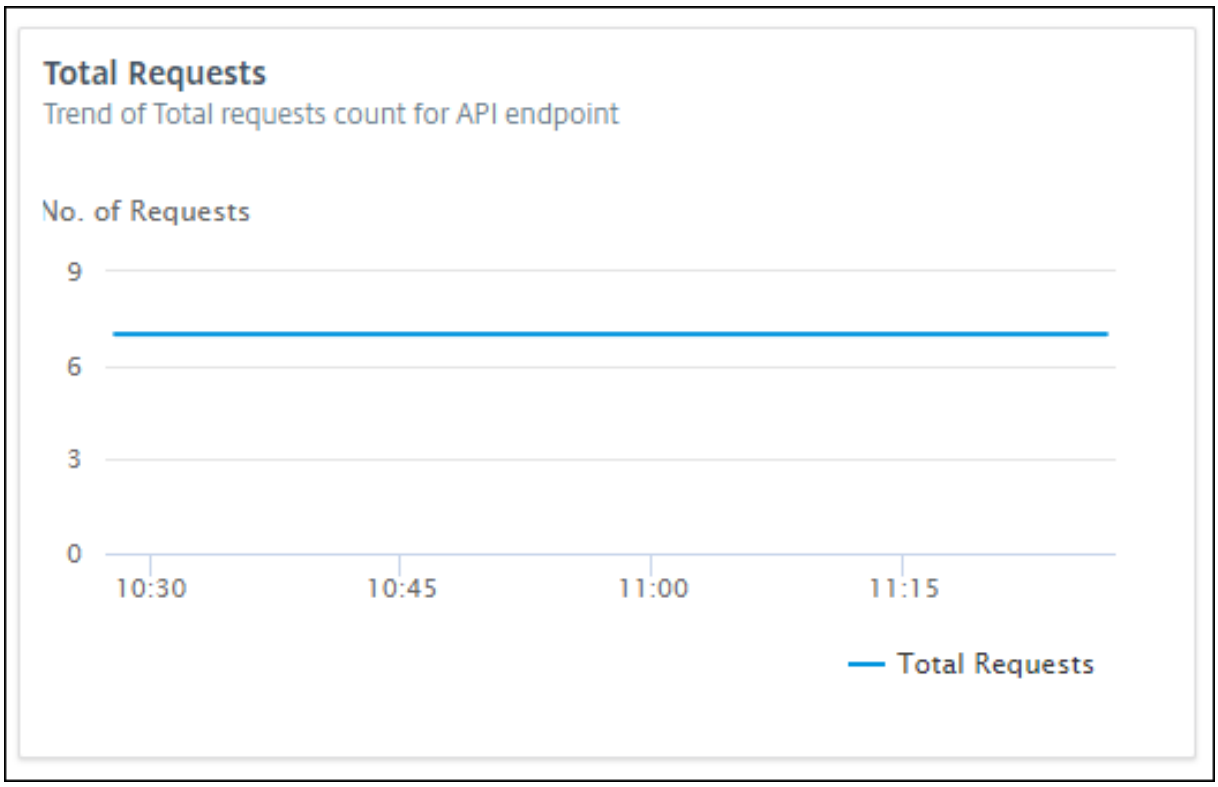
This tile appears in the **Performance and Usage** tab.



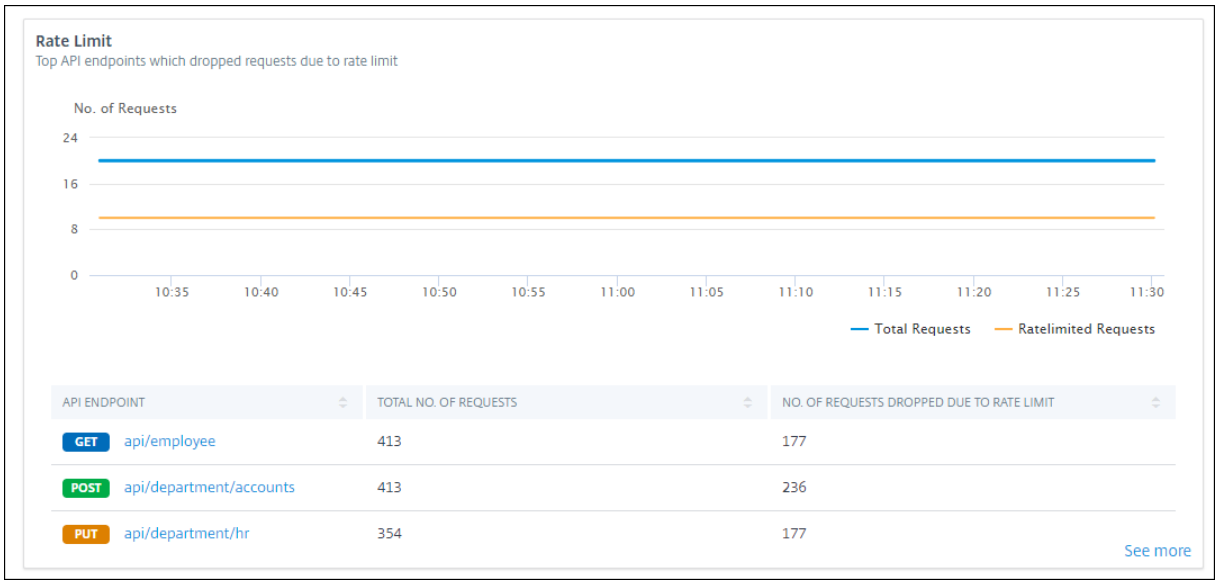
View API requests trend

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.

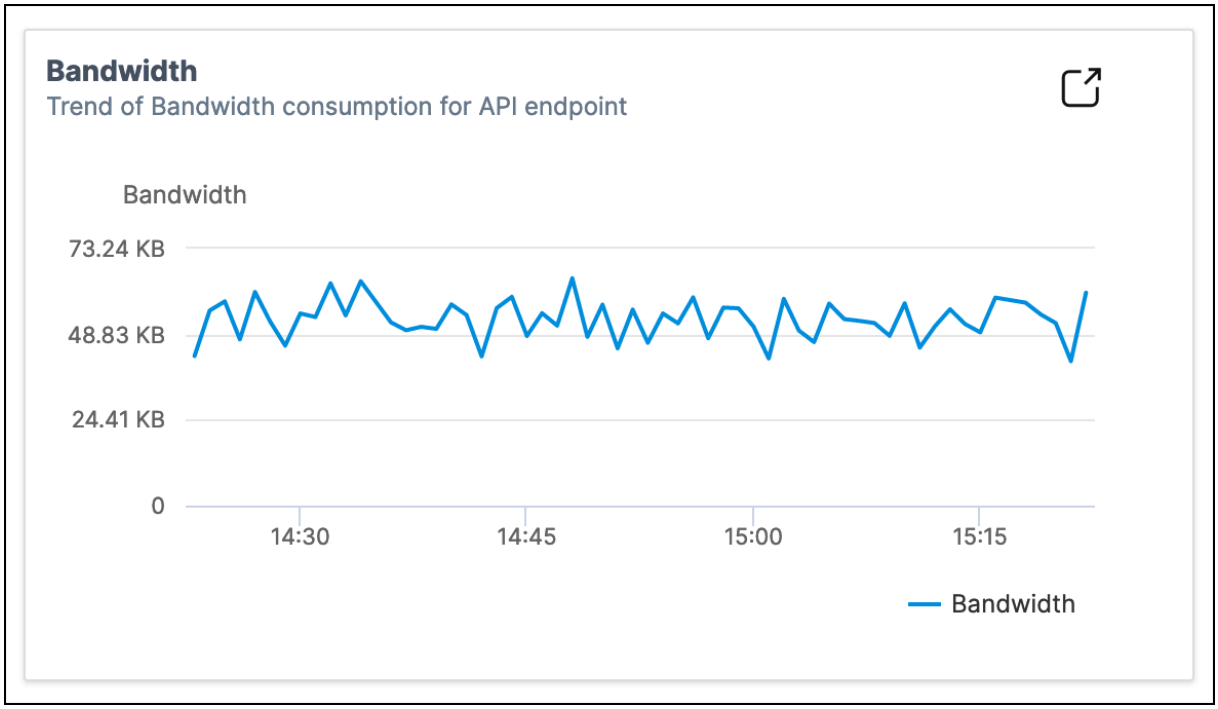


With this comparison, you can determine how many requests are dropped because of a rate limit among total requests.

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

View bandwidth consumption of an endpoint

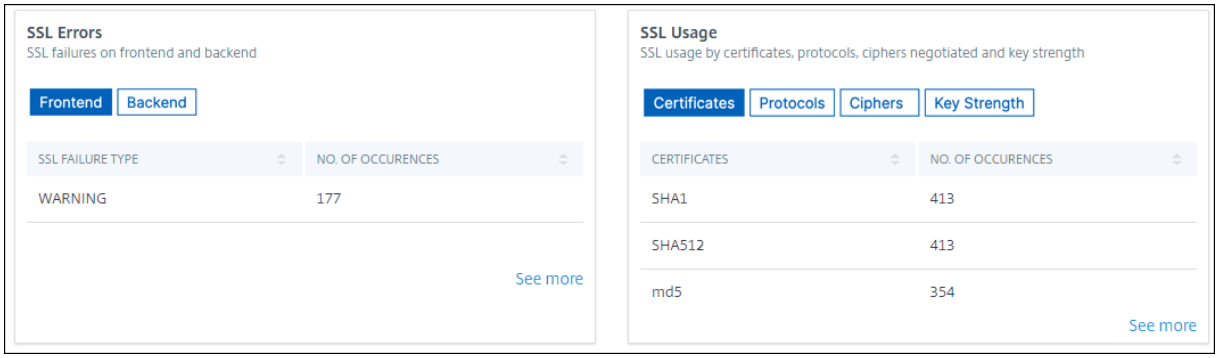
To view the bandwidth consumption trend by an endpoint, select an endpoint from the API endpoints. The **Bandwidth** tile displays a bandwidth consumption graph.



View SSL errors and usage

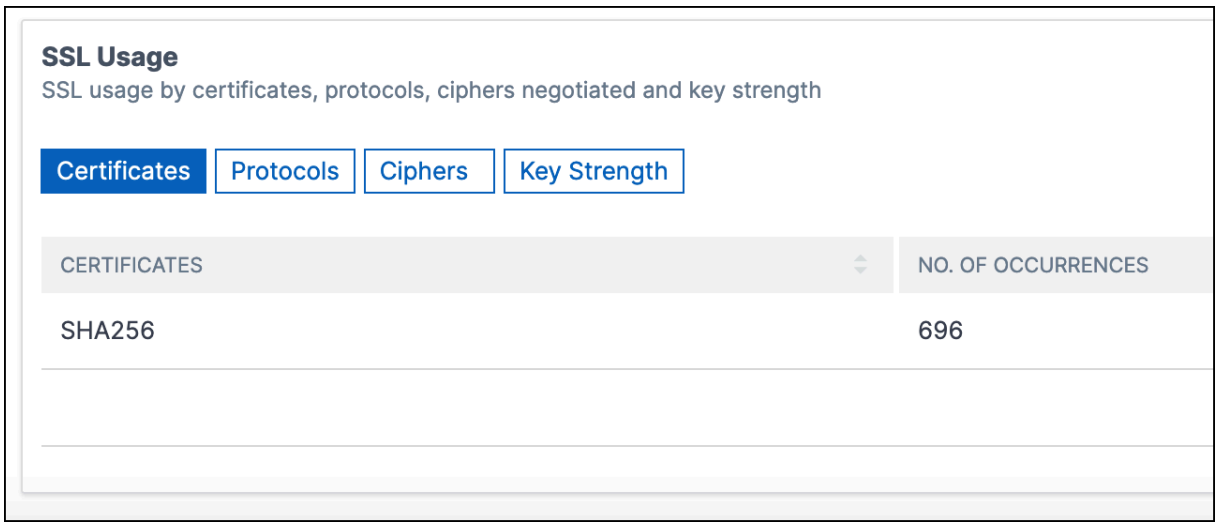
Select an instance from **API Instances**. In **Security**, the following tiles appear:

- **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

September 27, 2025

Use API Security to view the discovered API endpoints in your organization. NetScaler Console discovers the API endpoints based on the API traffic received on NetScaler instances.

In NetScaler Console, the **Security > API Security > API Discovery** page displays the discovered API endpoints.

The **VServers** 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.

> **Note:**
>
> Ensure to configure analytics and enable Web Insights on virtual servers. See, Enable Web Insight on API instances.

View API endpoints

In **API Discovery**, when you select a virtual server, the NetScaler Console GUI displays the API endpoints and their details such as:

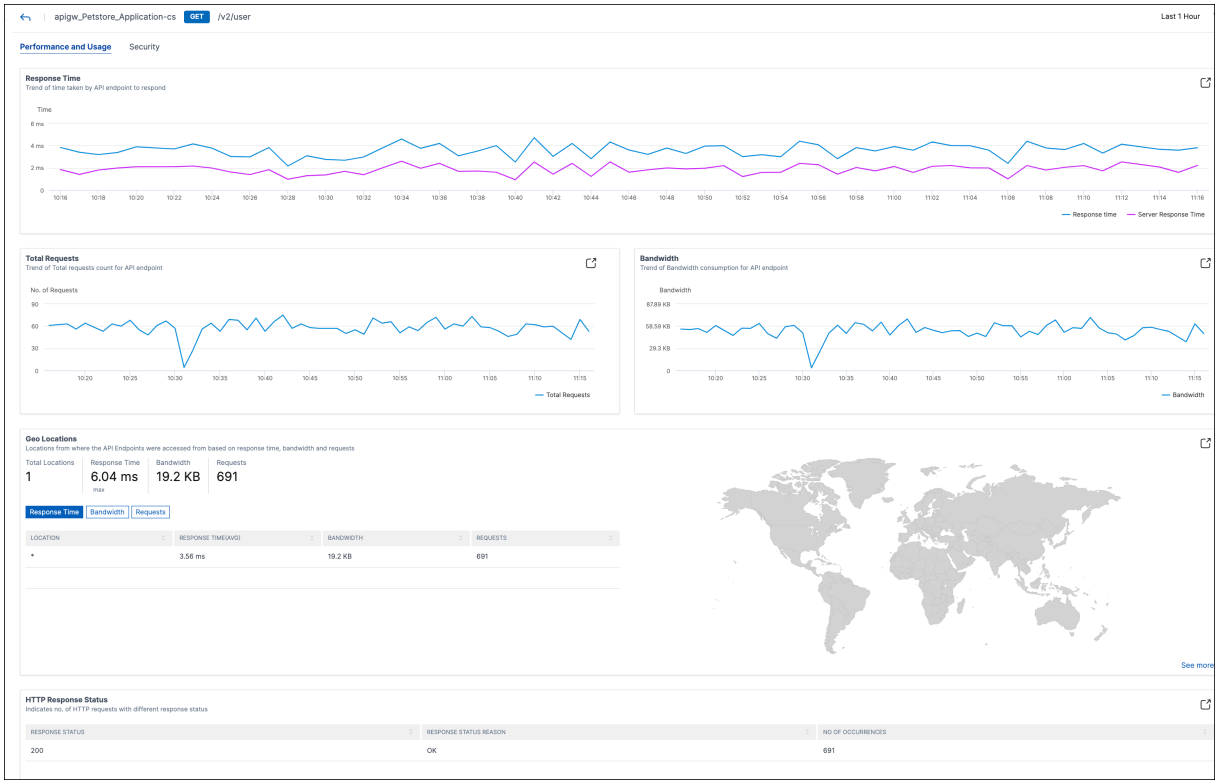
- **Method** - It displays the method used in an API endpoint. For example, GET and POST methods.
- **Total requests** - It displays the count of API requests on the API endpoint.
- **Response statuses** - It displays the count for each response status. For example, 2xx, 3xx, 4xx, and 5xx.

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

The API endpoints in a virtual server are available as follows:



You can also select the required API endpoint to view its detailed analytics report.



For more information about each section, see View API analytics.

Gateway Insight

September 27, 2025

In a NetScaler Gateway deployment, visibility into a user's access details is essential for troubleshooting access failure issues. As a 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. This information is typically not available unless the user sends a request for resolution.

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

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, the number of total and active sessions, the number of total bytes, and the 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 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.

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 the 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 a must 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.
- For Gateway Insight reporting, geo location information is not provided from the NetScaler appliance.
- Successful user logons, latency, and application-level details for virtual ICA applications and desktops are visible only on the HDX™ Insight Users dashboard.

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

- 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.
- 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-OpenID Connect

      For the OAuth-OpenID Connect authentication, NetScaler can act as an OAuth-OpenID connect relying party (RP) or OAuth-OpenID connect identity provider (IdP). When the authentication succeeds, the user name is reported under the Users tab in the Gateway Insight report. However, you cannot identify whether the session was created at IdP or RP.

      Note: OAuth-OpenID Connect authentication is supported from NetScaler Console release 13.1 build 4.xx and later.

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 Devices.

> **Note**
>
> To view end-point analysis (EPA) failures in NetScaler Console, you must enable AppFlow authentication, authorization, and auditing user name logging on the NetScaler Gateway appliance.

The following procedure to enable gateway insight is applicable if your NetScaler Console is **13.0 Build 36.27**:

1. Navigate to **Infrastructure > Instances**, and select the instance for which you want to enable AppFlow.
2. From the **Select Action** list, select **Configure Analytics**.

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

3. In the **Configure Insight** page, under **Configure Analytics**, select **NetScaler Gateway**.
4. Select the virtual server and then click **Enable AppFlow**.
5. On the **Enable AppFlow** screen, in the **Select Expression** list, click true.
6. Next to **Transport Mode**, select the **Logstream** check box.

   > **Note**
   >
   > You can choose either **IPFIX** or **Logstream** as transport mode.
   >
   > For more information about **IPFIX** and **Logstream**, see **Logstream overview**.

7. Click **OK**.

For NetScaler Console version 13.0 Build 41.x or later

1. Navigate to **Infrastructure > Instances**, and select the instance.
2. From the **Select Action** list, select **Configure Analytics**.
3. Select the virtual server and click **Enable Analytics**.
4. Under **Advanced Options**:
   a) Select **Logstream**
   b) Select **NetScaler Gateway**
5. Click **OK**.

Enable AppFlow authentication, authorization, and auditing user name logging on a 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**.

Viewing Gateway Insight reports

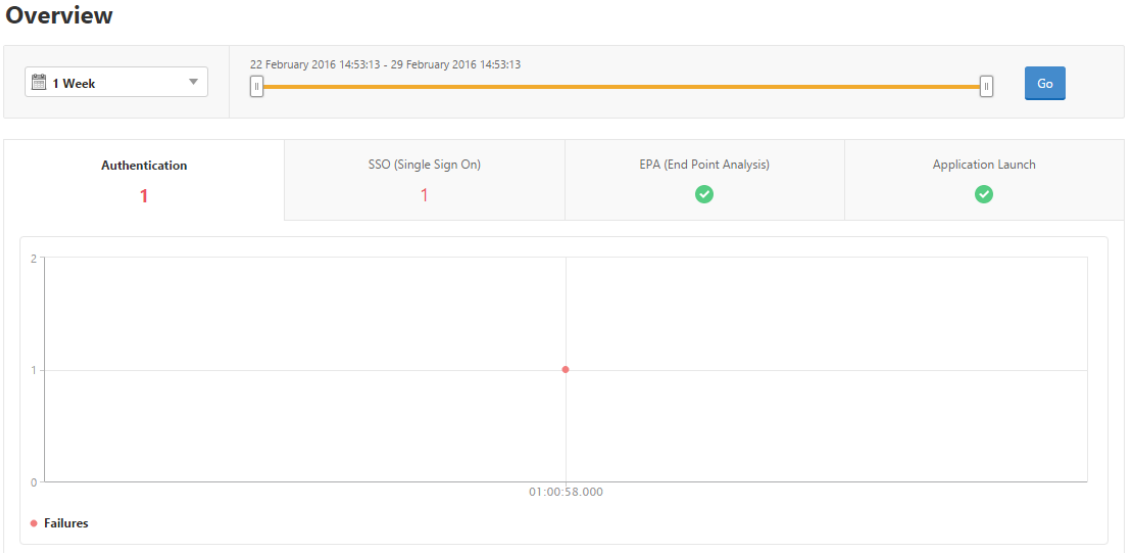
In NetScaler Console, you can view reports for all users, applications, and gateways associated with the NetScaler Gateway appliances, and you can view details for a particular user, application, or gateway. In the **Overview** section, you can view the EPA, SSO, Authentication, and Application Launch 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.

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

> **Note**
>
> When you create a group, you can assign roles to the group, provide application-level access to the group, and assign users to the group. NetScaler Console analytics now supports virtual IP address based authorization. Your users can now see reports for all Insights for only the applications (virtual servers) that they are authorized to. For more information on groups and assigning users to the group, see Configure Groups.

To view EPA, SSO, authentication, authorization, and application launch failures

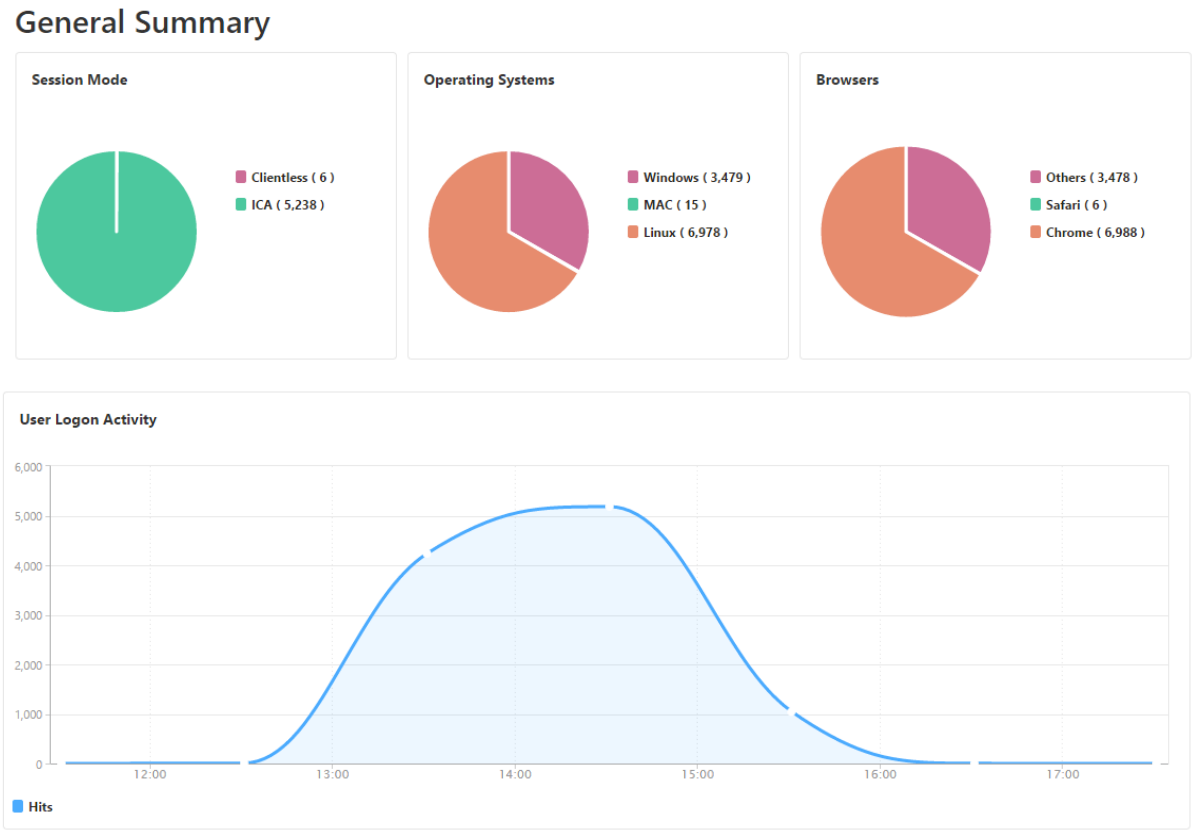
1. In NetScaler Console, navigate to **Gateway > Gateway Insight**.
2. Select the time period for which you want to view the user details. You can use the time slider to further customize the selected period. Click **Go**.
3. Click the EPA (End Point Analysis), Authentication, Authorization, SSO (Single Sign On), or Application Launch tabs to display the failure details.



To view a 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.



Viewing Gateway Insight reports for users

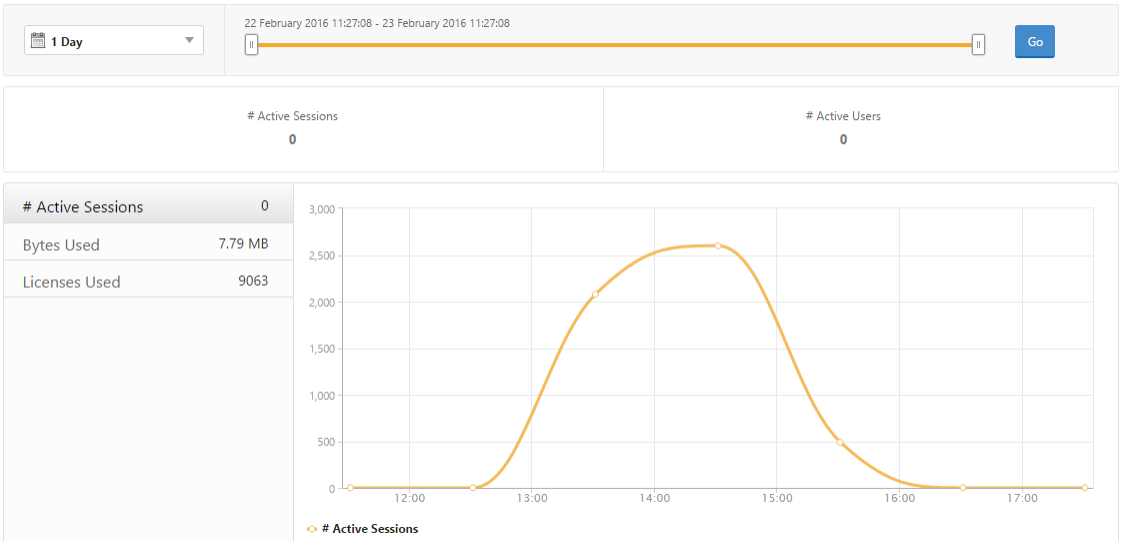
You can view the reports for:

- All users associated with the NetScaler Gateway appliances.
- The EPA, authentication, SSO, and application launch failures for a user.
- The details of active and terminated sessions for a user.
- The types of session modes such as Full Tunnel, clientless VPN, and ICA® Proxy.

To 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, bytes, and licenses used 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.

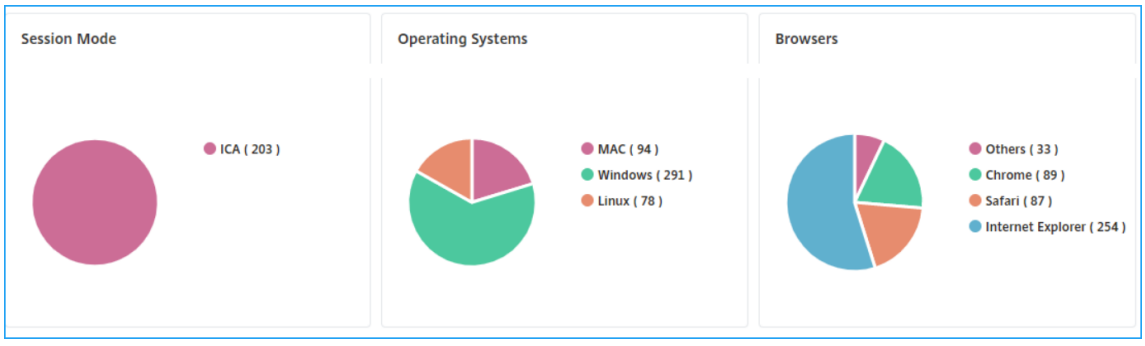


Users | Active Users

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

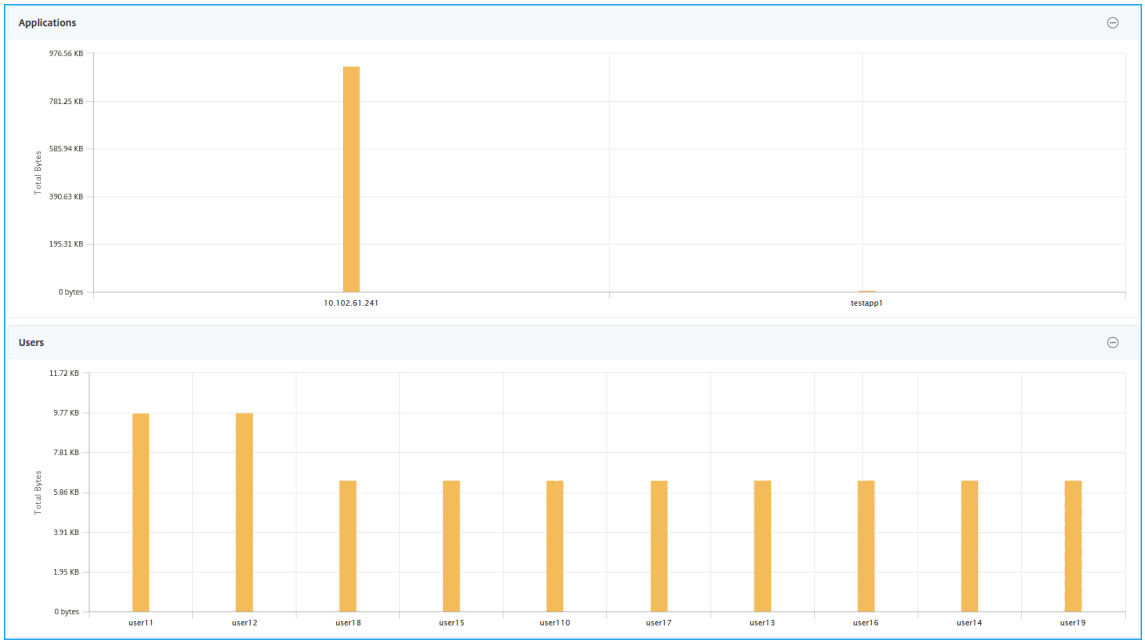
On the **Users** or **Active Users** tab, click a user to view the following user details:

- **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.

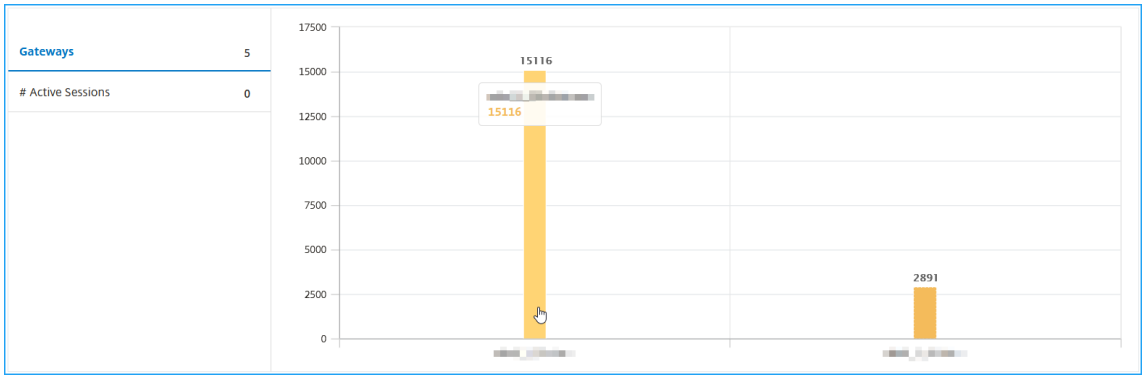


- **Users and applications for the selected gateway** - Navigate to **Gateway** > **Gateway Insight** > **Gateway** and click a gateway domain name to view the top 10 applications and top 10 users that are associated with the selected gateway.

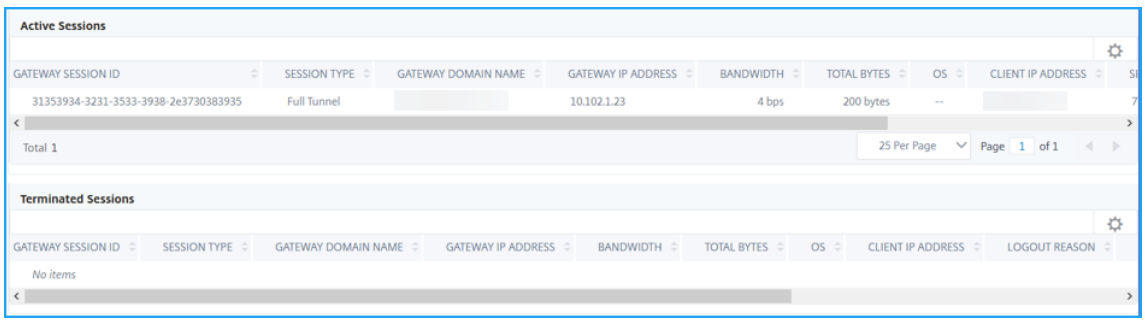
© 1997–2025 Citrix Systems, Inc. All rights reserved.



- **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.

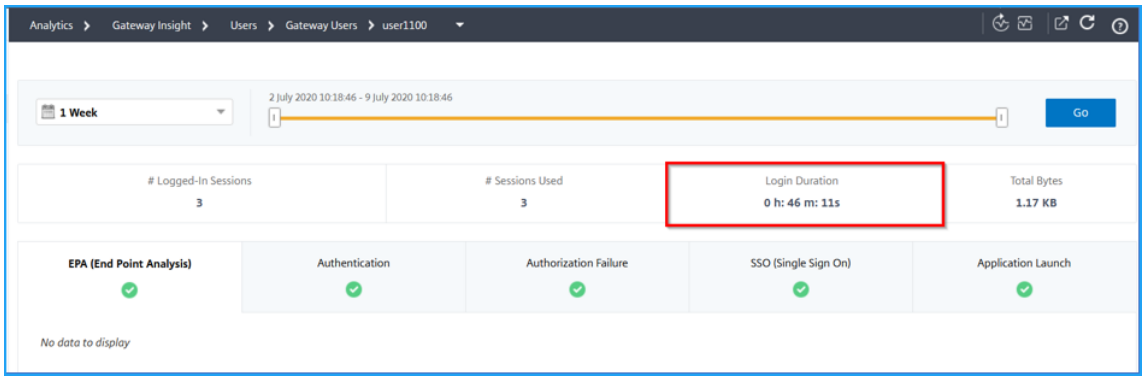


- The user **Active Sessions** and **Terminated Sessions**.



© 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

Viewing Gateway Insight reports for applications

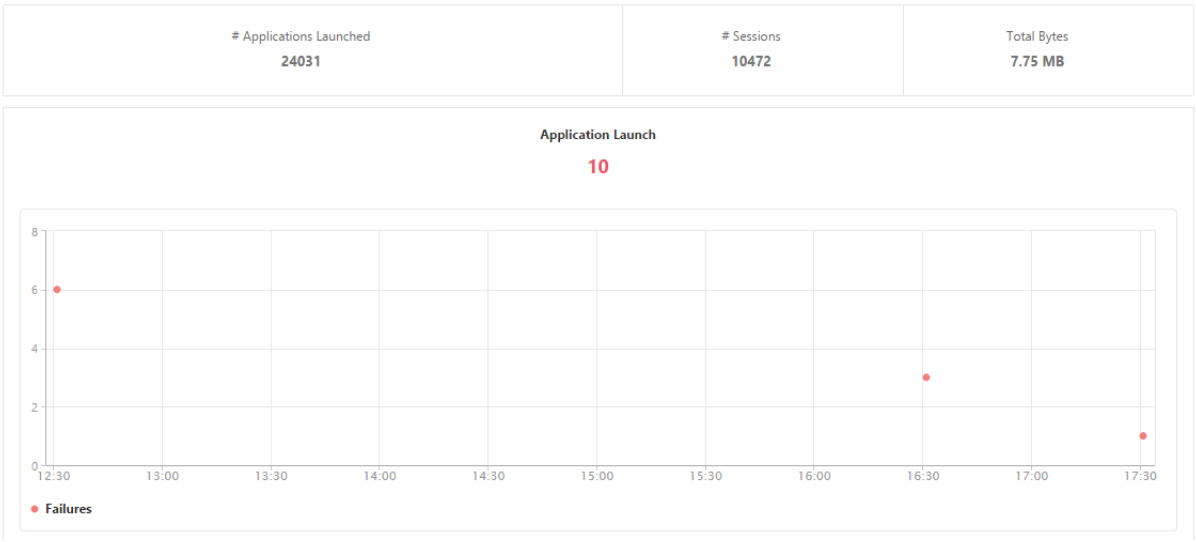
You can view the number of applications launched, the number of total and active sessions, the number of total bytes and bandwidth consumed by the applications. You can view details of the users, sessions, bandwidth, and launch errors for an application.

To 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, the 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.

Viewing Gateway Insight reports for gateways

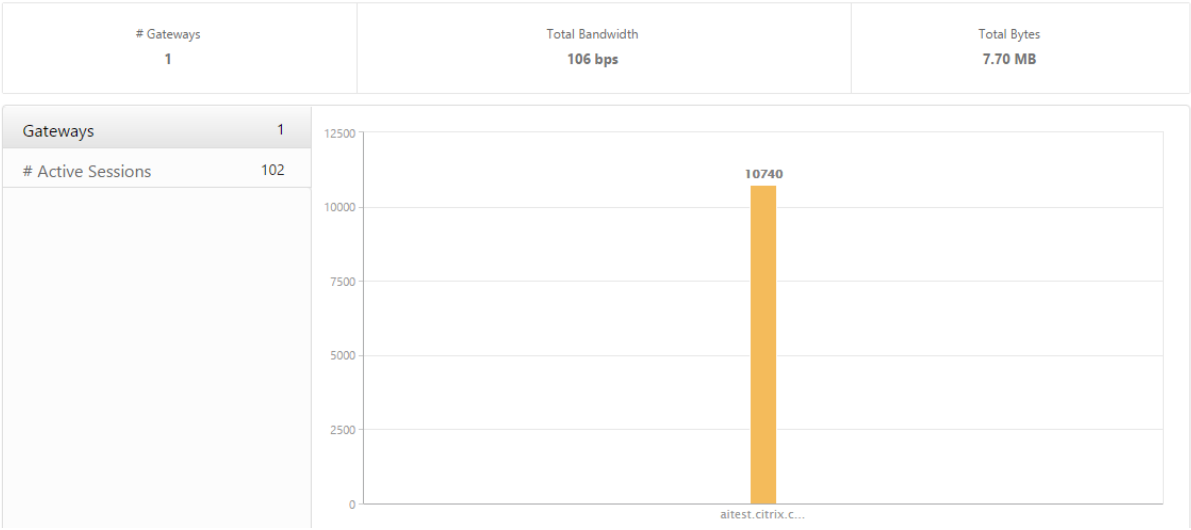
You can view the number of gateways, number of active sessions, total bytes, and bandwidth used by all gateways associated with a NetScaler Gateway appliance at any given time. You can view the EPA, authentication, single sign-on, and application launch failures for a gateway. You can also view the details of all users associated with a gateway and their logon activity.

To view gateway details

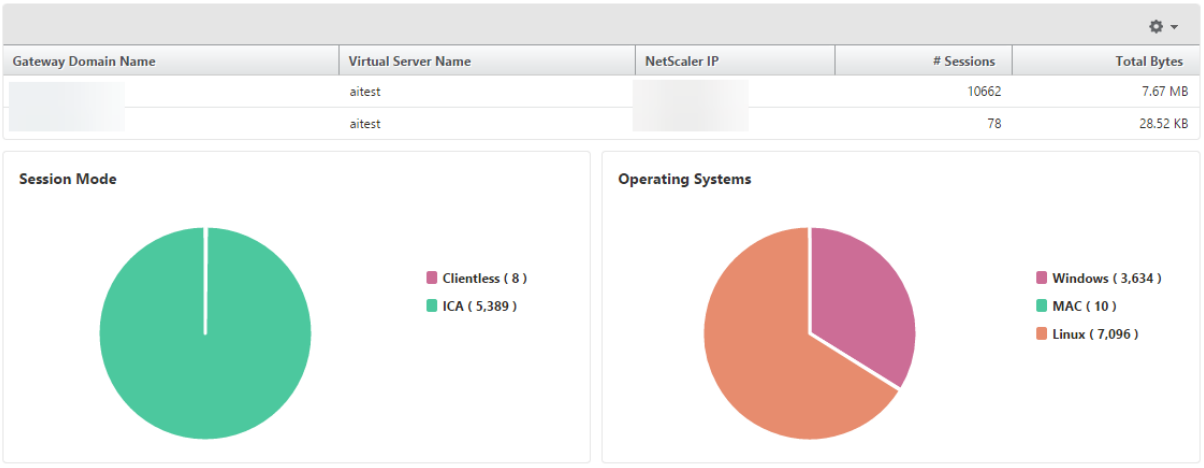
1. In **NetScaler Console**, navigate to **Gateway > Gateway Insight > Gateways**.
2. Select the time period for which you want to view the gateway details. You can use the time slider to further customize the selected time period. Click **Go**.

© 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.

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.

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

> **Note**
>
> - Users with read only access cannot export reports.
> - Geo map reports are exported only if the NetScaler Console has internet connectivity.

To 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**.

To add an email server or an email distribution list:

1. On the **Configuration** tab, navigate to **Settings > 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.

A user is not able to log in 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:

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

- 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:

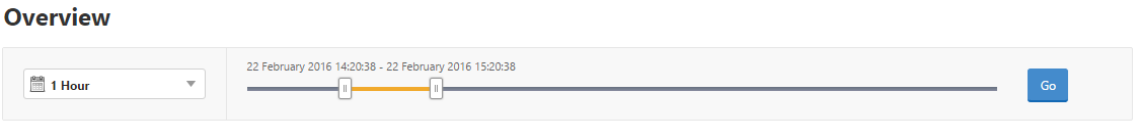
In NetScaler Console, navigate to **Gateway > Gateway Insight** and, in the **Search for Users** text box, specify the user you want to search.

Authentication failures

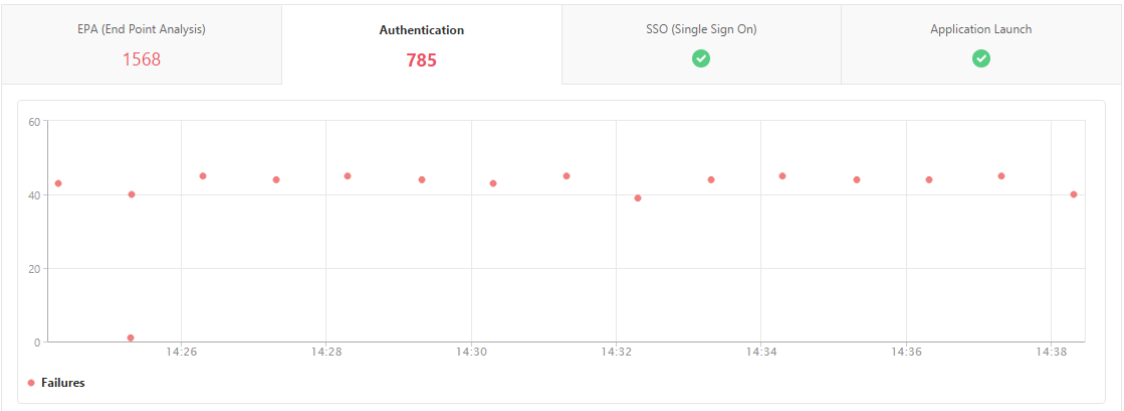
You can view authentication errors such as incorrect credentials or no response from the authentication server. You can also see the factor at which the authentication failed.

To 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**.

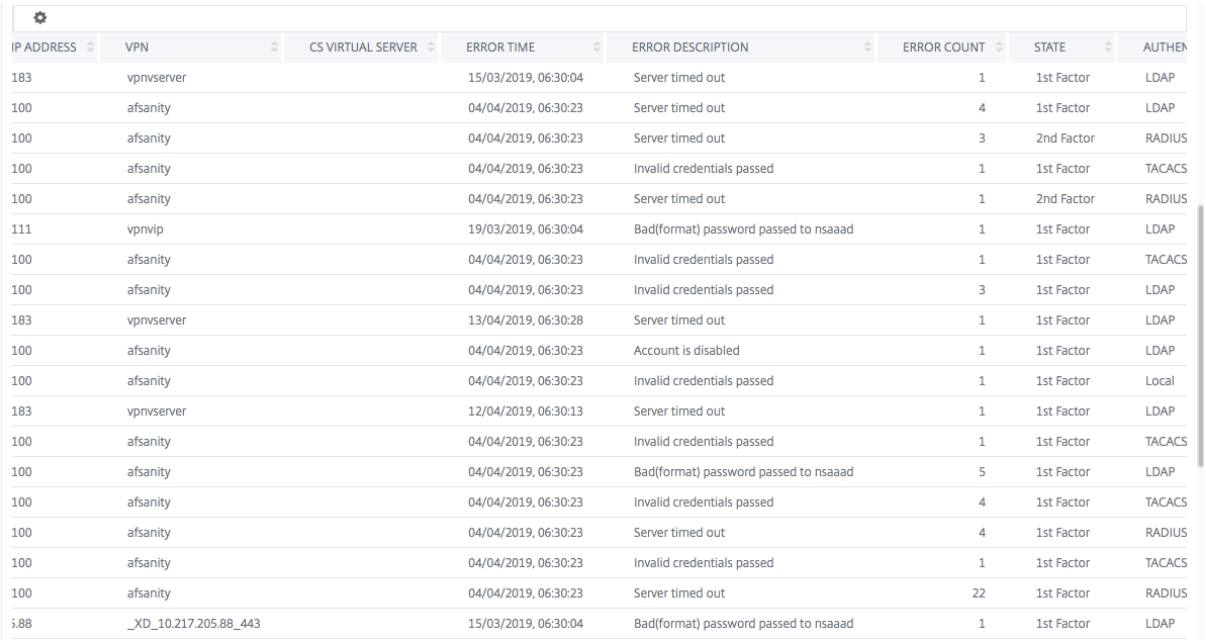


3. Click the **Authentication** tab. You can view the number of authentication errors at any given time in the **Failures** graph.



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 the nth factor at which the failure occurred.

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



IP ADDRESS	VPN	CS VIRTUAL SERVER	ERROR TIME	ERROR DESCRIPTION	ERROR COUNT	STATE	AUTHEN
183	vpnvserver		15/03/2019, 06:30:04	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Server timed out	4	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Server timed out	3	2nd Factor	RADIUS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	1	2nd Factor	RADIUS
111	vpnvip		19/03/2019, 06:30:04	Bad(format) password passed to nsaaad	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	3	1st Factor	LDAP
183	vpnvserver		13/04/2019, 06:30:28	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Account is disabled	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	Local
183	vpnvserver		12/04/2019, 06:30:13	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Bad(format) password passed to nsaaad	5	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	4	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	4	1st Factor	RADIUS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	22	1st Factor	RADIUS
.88	_XD_10.217.205.88_443		15/03/2019, 06:30:04	Bad(format) password passed to nsaaad	1	1st Factor	LDAP

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 icon.

> **Important:**
>
> If OAuth-OpenID Connect authentication fails, the user name is displayed as **NA** in the Gateway Insight report for some of the failures, for example "Token verification failure". In this failure, the user names are not available for authentication failure due to "Token verification failure"at the OAuth-OpenID connect relying party.



USERNAME	CITRIX ADC IP ADDRESS	CLIENT IP ADDRESS	GATEWAY IP ADDRESS	VPN	CS VIRTUAL SERVER	ERROR DESCRIPTION
-NA-				gitest.citrix.com		Relying party: Token verification failed
-NA-				gitest.citrix.com		Relying party: Incoming URL query parameter from user agent is NULL in /nf/auth/doOAuth requ
-NA-				gitest.citrix.com		Relying party: Action query parameter isn't present in the URL from user agent in /nf/auth/doOA
-NA-				gitest.citrix.com		Relying party: Action query parameter isn't present in the URL from user agent in /nf/auth/doOA
-NA-				vpnvserver		Relying party: Token verification failed
-NA-				vpnvserver		Relying party: Token verification failed
-NA-				vpnvserver		Relying party: Token verification failed
-NA-				vpnvserver		Relying party: Token decryption failure

EPA failures

You can view EPA failures at the pre-authentication or post-authentication stage.

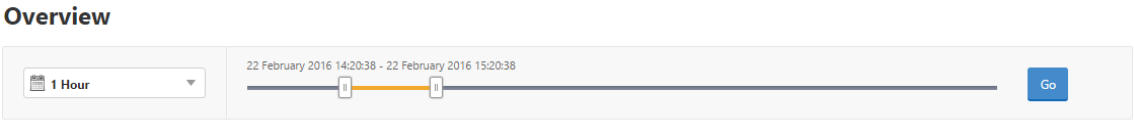
> **Important:**
>
> NetScaler Gateway reports EPA failures to NetScaler Console for both classic and advanced expressions. For the advanced expressions, the policy names are not displayed in the Gateway In-

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

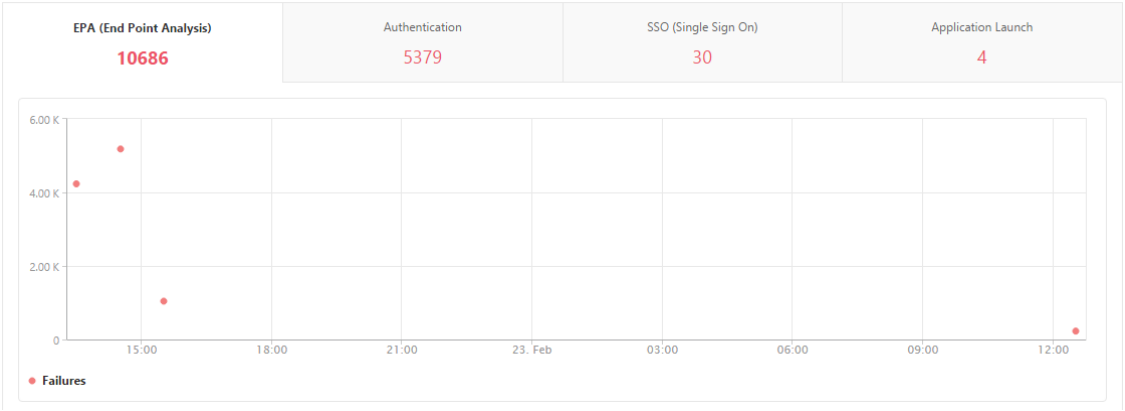
> sight dashboard. The failures are reported if EPA is configured as one of the factors in the nFactor authentication flow.

To view EPA failure details:

1. In NetScaler Console, navigate to **Gateway > Gateway Insight**.
2. In the Overview section, select the time period for which you want to view the EPA errors. You can use the time slider to further customize the selected time period. Click **Go**.



3. Click the **EPA (End Point Analysis)** tab. You can view the number of EPA errors at any given time in the **Failures** graph.



Scroll down to view details of each EPA error such as **Username, NetScaler IP Address, Gateway IP Address, VPN, Error Time, Policy Name, Gateway Domain Name** and more from the table on the same tab.

The **Error Description** column in the table displays the reason for the EPA failure. For example, the error message "EPA pre-auth check failures"appears when an EPA check fails due to nFactor EPA failures.

The **Policy Name** column displays the policy that resulted in the failure.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	Policy Name	EPA Method	Gateway Domain Name
user1097	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1098	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1491	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1633	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 3:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user17	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1774	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user197	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com

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

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 downward arrow. The case ID is displayed on entries that do not have a username assigned if EPA is used as a factor in the nFactor authentication flow.

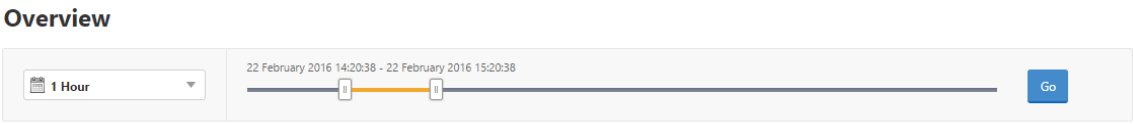
> **Note**
>
> NetScaler Gateway doesn't report the EPA failures when the "clientSecurity"expression is configured as a VPN session policy rule.

SSO failures

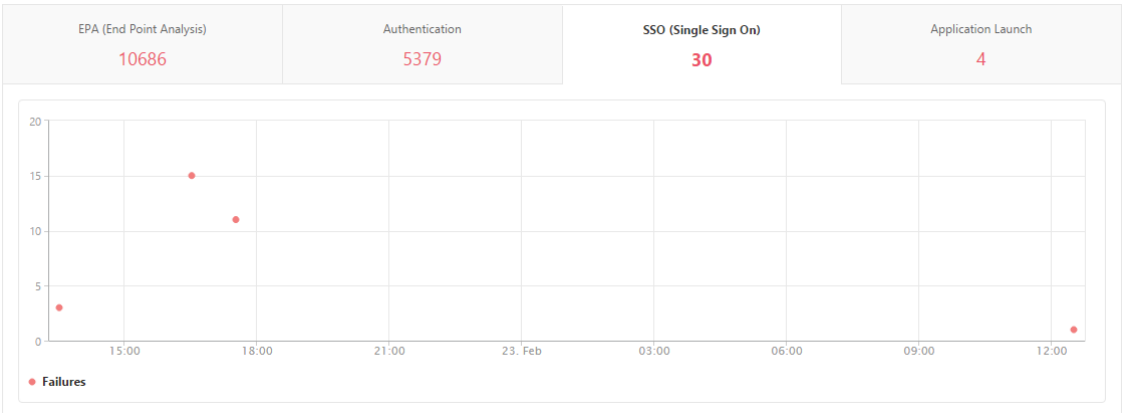
You can view the all the SSO failures at any stage for a user accessing any applications through the NetScaler Gateway appliance.

To view the 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.

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

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	SSO Method	Gateway Domain Name
user11	10.102.61.201	10.102.61.210	10.144.2.35	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 5:30:54 PM	Single Sign ON failed	11	NTLM	aitest.citrix.com
user5	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/23/2016, 12:30:54 PM	Single Sign ON failed	1	Basic	aitest.citrix.com
user31	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user23	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 4:30:54 PM	Single Sign ON failed	15	NTLM	aitest.citrix.com

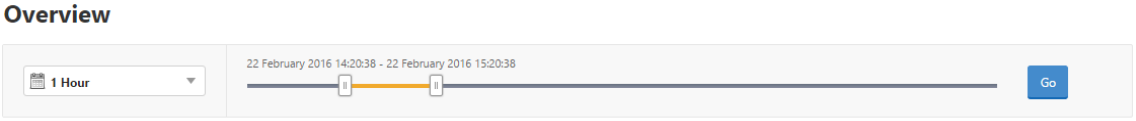
You can click a user in the **Username** column to display the SSO errors and other details for that user. You can customize the table to add or delete columns by using the downward arrow.

After successfully logging on to NetScaler Gateway, a user is not able to launch any virtual application

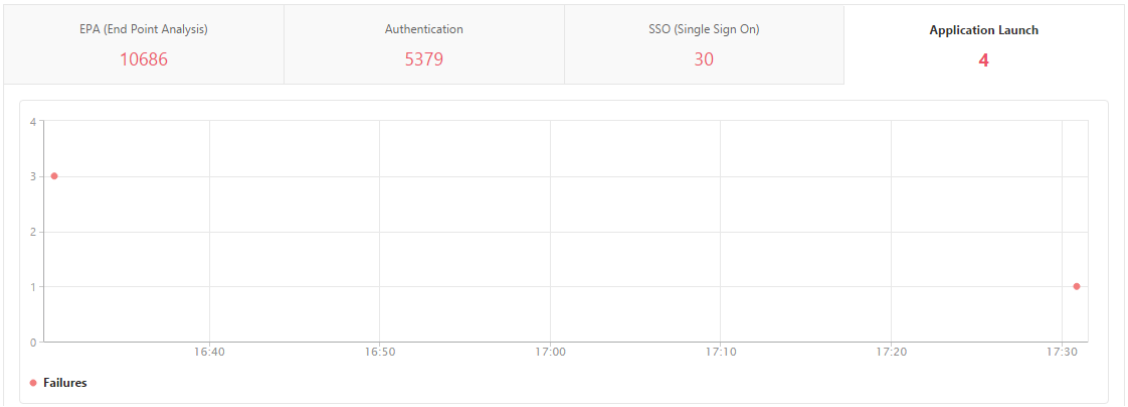
For an application-launch failure, you can gain visibility into the reasons, such as inaccessible Secure Ticket Authority (STA) or Citrix Virtual App server, or invalid STA ticket. You can view the time the error occurred, details of the error, and the resource for which STA validation failed.

To view the 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.



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

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 downward arrow.

After successfully launching a new application, a user wants to view the total bytes and bandwidth consumed by that application

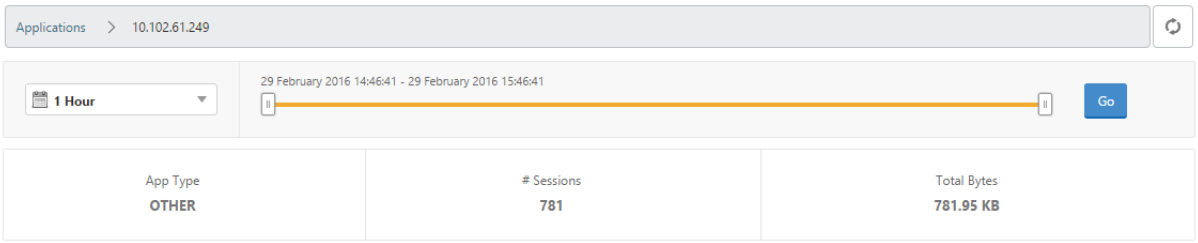
After you have successfully launched a new application, in NetScaler Console, you can view the total bytes and bandwidth consumed by that application.

To 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.

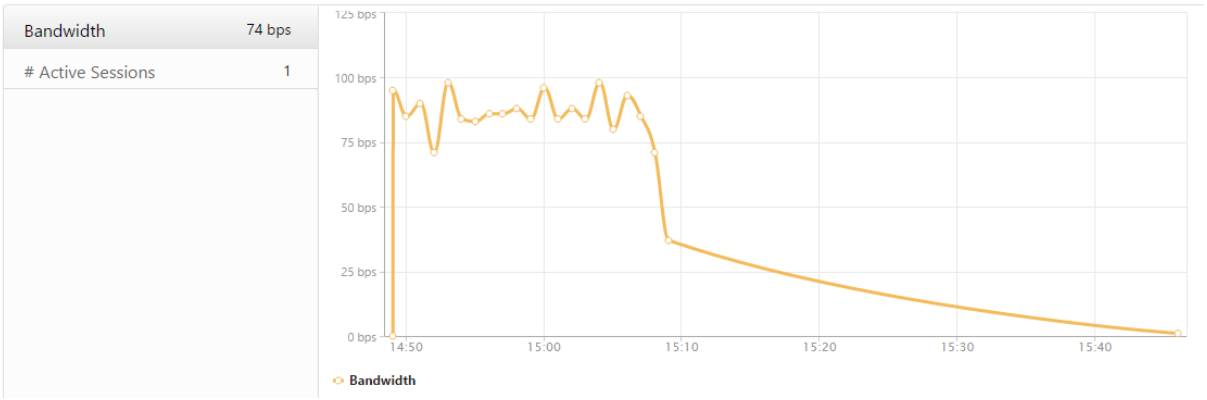


You can view the number of sessions and the total number of bytes consumed by that application.



You can also view the bandwidth consumed by that application.

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

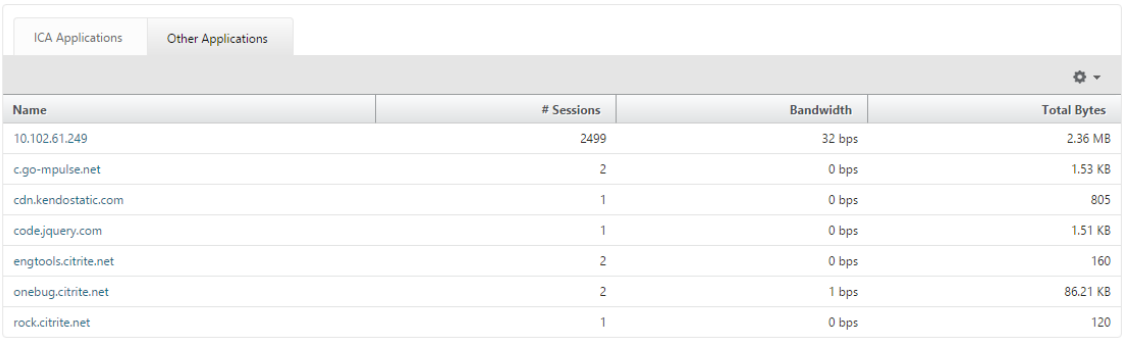


A user has logged on to NetScaler Gateway successfully, but is unable to access certain network resources in the internal network

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.

To view user access for resources:

1. In NetScaler Console, **navigate to Gateway > Gateway Insight > Applications**.
2. On the screen that appears, scroll down, and on the **Other Applications** tab, select the application to which the user was unable to log on.



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

3. Scroll down and in the **Users** table, all the users that have access to that application are displayed.

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

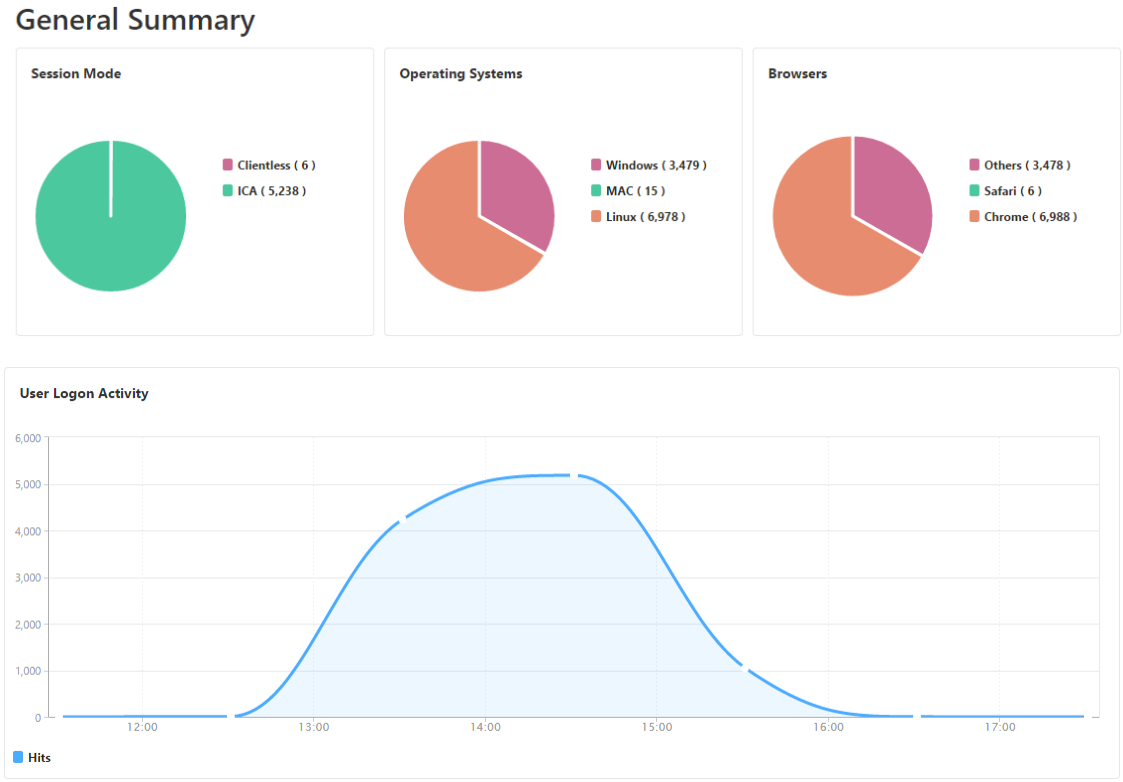
With Gateway Insight, you can view a summary of the different session modes used by users to log on, the types of clients, and the number of users logged on every hour. You can also determine whether a user's deployment is a unified gateway or classic NetScaler Gateway deployment. For unified gateway

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

deployments, you can view the content switching virtual server name and IP address and the VPN virtual server name.

To view the summary of session modes, type of clients, and number of users logged on:

1. In NetScaler Console, navigate to **Gateway > Gateway Insight**.
2. In the **Overview** section, scroll down to view the **Session Mode, Operating Systems, Browsers**, and **User Logon Activity** charts display the different session modes used by users to log on, the types of clients, and the number of users logged on every hour.



Troubleshoot Gateway Insight issues

September 27, 2025

If the Gateway Insight solution is not functioning as expected, the issue might be with one of the following. Refer to the checklists in the respective sections for troubleshooting.

- Gateway Insight configuration.
- Connectivity issue between NetScaler and NetScaler Console.
- Record generation in NetScaler.
- Validations in NetScaler Console.

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

Gateway Insight configuration checklist

- Make sure that the AppFlow feature is enabled in the NetScaler appliance. For details, see Enabling AppFlow.
- Check the Gateway Insight configuration in the NetScaler running configuration.

  Run the `show running | grep -i <appflow_policy>` command to check the Gateway Insight configuration. Make sure that the bind type is REQUEST. For example;

  ```
  1  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

  Bind type OTHERTCP_REQUEST is also required for Gateway Insight.

  ```
  1  bind vpn vserver afsanity -policy afp -priority 100 -type
       OTHERTCP_REQUEST
  ```

- For single-hop, Access Gateway, or Unified Gateway deployment, make sure that Gateway Insight AppFlow policy is bound to the VPN virtual server, where VPN traffic is flowing. For details, see Enabling HDX Insight data collection.
- For double-hop, Gateway Insight must be configured on both the hops.
- Check `appflowlog` parameter in NetScaler Gateway/VPN virtual server. For details, see Enabling AppFlow for Virtual Servers.

Connectivity between NetScaler and NetScaler Console checklist

- Check AppFlow collector status in NetScaler. For details, see How to check the status of connectivity between NetScaler and AppFlow Collector.
- Check Gateway Insight AppFlow® policy hits.

  Run the command `show appflow policy <policy_name>` to check the AppFlow policy hits.

  You can also navigate to **Settings > AppFlow > Policies** in the GUI to check the AppFlow policy hits.
- Validate any firewall blocking AppFlow ports 4739 or 5557.

Record generation in NetScaler checklist

- Run the `nsconmsg -d stats -g ai_tot` command and check for the stats increments in NetScaler.
- Capture `nstrace logs` and check for CFLOW packets to confirm NetScaler exports AppFlow records.

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

> **Note:**
>
> The `nstrace logs` are required only for IPFIX. For Logstream, nstrace logs do not confirm if the NetScaler appliance exported the AppFlow records.

Validation of records in NetScaler Console

- Run the `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: vpn_"` command to check the logs to confirm NetScaler Console is receiving AppFlow records.
- Make sure that the NetScaler instance is added to the NetScaler Console.
- Make sure that the NetScaler Gateway/VPN virtual server is licensed in NetScaler Console.

Validation of Logstream logs in NetScaler Console

Validation of Logstream data received by NetScaler Console can be done using the following methods:

- **Enabling data record logging in NetScaler Console**

  Once enabled, the logs can be seen in the /var/mps/log/mps_afdecoder.log

- **Enabling ULFD library logging**

  Run the command `/mps/decoder_enable_debug`

  The logs are captured in `/var/ulflog/libulfd.log`

  You can disable logging by using the command `/mps/decoder_disable_debug`

Gateway Insight counters

The following Gateway Insight counters are available.

- ai_tot_preauth_epa_export
- ai_tot_auth_export
- ai_tot_auth_session_id_update_export
- ai_tot_postauth_epa_export
- ai_tot_vpn_update_export
- ai_tot_ica_fileinfo_export
- ai_tot_app_launch_failure
- ai_tot_logout_export
- ai_tot_skip_appflow_export

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

- ai_tot_sso_appflow_export
- ai_tot_authz_appflow_export
- ai_tot_appflow_pol_eval_failure
- ai_tot_vpn_export_state_mismatch
- ai_tot_appflow_disabled
- ai_tot_appflow_pol_eval_in_gwinsight
- ai_tot_app_launch_success

AppFlow records in NetScaler log

Starting from release 13.0 build 71.x, you can check the NetScaler logs to confirm if the AppFlow records are exported. The default log level of `syslogparams` captures all the error and information logs. In case you do not find a clue about the errors, enable all log levels including DEBUG in `syslogparams` to capture even the DEBUG logs.

Sample logs

```
<local0.info> ... GMT 0-PPE-0 : default SSLVPN Message 147 0 : "
    GwInsight: Sent auth record Func=ns_sslvpn_export_auth_data Username
    =<name> Clientip=<ip>:<port> Destip=0:80 SessSeq=0 Sessid=<sessid>
    Gwip=<ip>:443 StatusCode=0 CSappid=0 CSAppname=(null) VPNfqdn=<
    vpnfqdn> Authtype=3 EPAid=(null) AuthStage=1 AuthDuration=309
    AuthAgent=<auth_server_ip> Groupname= Policyname=<name>
    CurfactorPolname=<name> NextfactorPolname= CSecExpr= Devicetype
    =16777219 Deviceid=0 email="
<local0.err> ... GMT 0-PPE-0 : default SSLVPN Message 143 0 : "GwInsight
    : Func=ns_aaa_copy_email_id_to_vpn_record input hash_attrs_len is
    zero"
<local0.err> ... GMT 0-PPE-0 : default SSLVPN Message 148 0 : "GwInsight
    : Func=update_session_appflow_collector pcb or session is NULL"
<local0.info> ... GMT 0-PPE-0 : default SSLVPN Message 165 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<> Clientip=<ip>:<port> Destip
    =<ip>:80 SessSeq=1 Sessid=<sessid> Gwip=<ip>:443 StatusCode=0
    CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=0 SessState
    =2 SessMode=2 IIP=0 AppByteCount=0 ReqURL=/Citrix/Store
Web BackendServername= SSOurl= email="
SSO logs:
```

```
<local0.info> ... GMT 0-PPE-0 : default SSLVPN Message 463 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
    Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
    =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=1
    SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
    BackendServername=<> SSOurl= email="
```

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

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 582 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
    Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
    =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=3
    SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
    BackendServername=<> SSOurl= email="
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 513 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
    Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
    =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=2
    SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
    BackendServername=<> SSOurl= email="
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 29796 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
    Destip=<ip>:443 SessSeq=c Sessid=<sessid> Gwip=<ip>:443 StatusCode
    =155 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=6
    SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
    BackendServername=<> SSOurl= email="
```

Contact Citrix technical support

For a speedy resolution, make sure that you have the following information before contacting Citrix technical support:

- Details of the deployment and network topology.
- NetScaler and NetScaler Console versions.
- Tech support bundle for NetScaler and NetScaler Console.
- `nstrace` capture during the issue.

Known Issues

Refer NetScaler release notes for known issues on Gateway Insight.

HDX™ Insight

September 27, 2025

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

HDX Insight provides end-to-end visibility for HDX traffic to Citrix Virtual Apps and Desktop passing through NetScaler. It also enables administrators to view real-time client and network latency metrics, historical reports, End-to-end performance data, and troubleshoot performance issues. Availability of both real-time and historical visibility data enables NetScaler Console to support a wide variety of use cases.

For any data to appear you need to enable AppFlow on your NetScaler Gateway virtual servers. AppFlow can be delivered by the IPFIX protocol or the LogStream method.

> **Note**
>
> To allow ICA® round trip time calculations to be logged, enable the following policy settings:

- ICA Round Trip Calculation
- ICA Round Trip Calculation Interval
- ICA Round Trip Calculation for Idle Connections

If you click an individual user, you can see each HDX session, active or terminated, that the user made within the selected time frame. Other information includes several latency statistics and bandwidth consumed during the session. You can also get bandwidth information from individual virtual channels such as audio, printer mapping, and client drive mapping.

> **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.

You can also navigate to **Gateway > 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 **Gateway > HDX Insight > Users.**

> **Note** HDX insight supports Admin Partitions configured in NetScaler instances running on software version 12.0.

The following Thin Clients support HDX Insight:

- WYSE Windows-based Thin Clients
- WYSE Linux-based Thin Clients
- WYSE ThinOS-based Thin Clients
- 10ZiG Ubuntu-based Thin Clients

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

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.

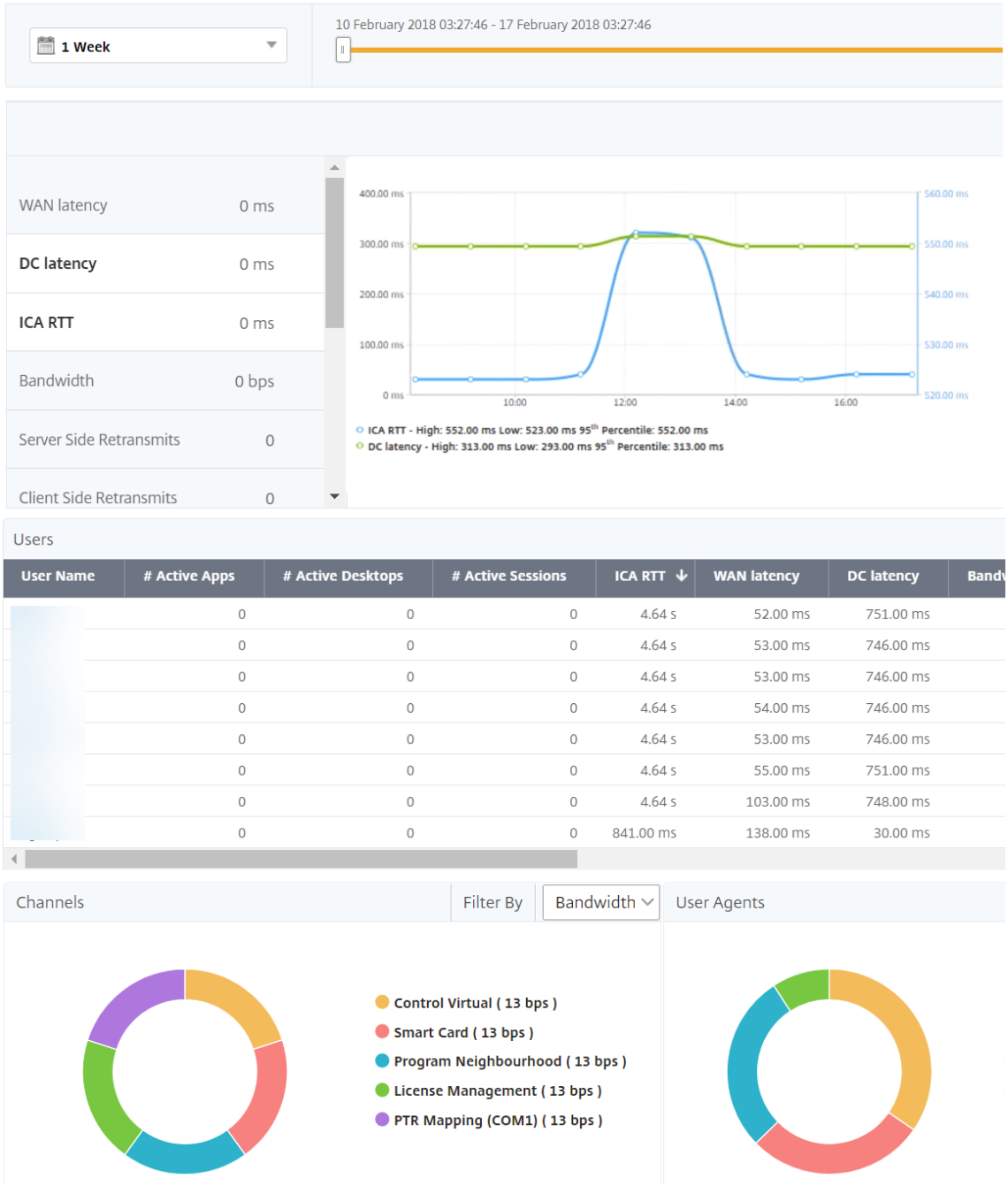
To identify the root cause of the issue, analyze the following metrics:

- WAN Latency
- DC Latency
- Host Delay

To view the client metrics:

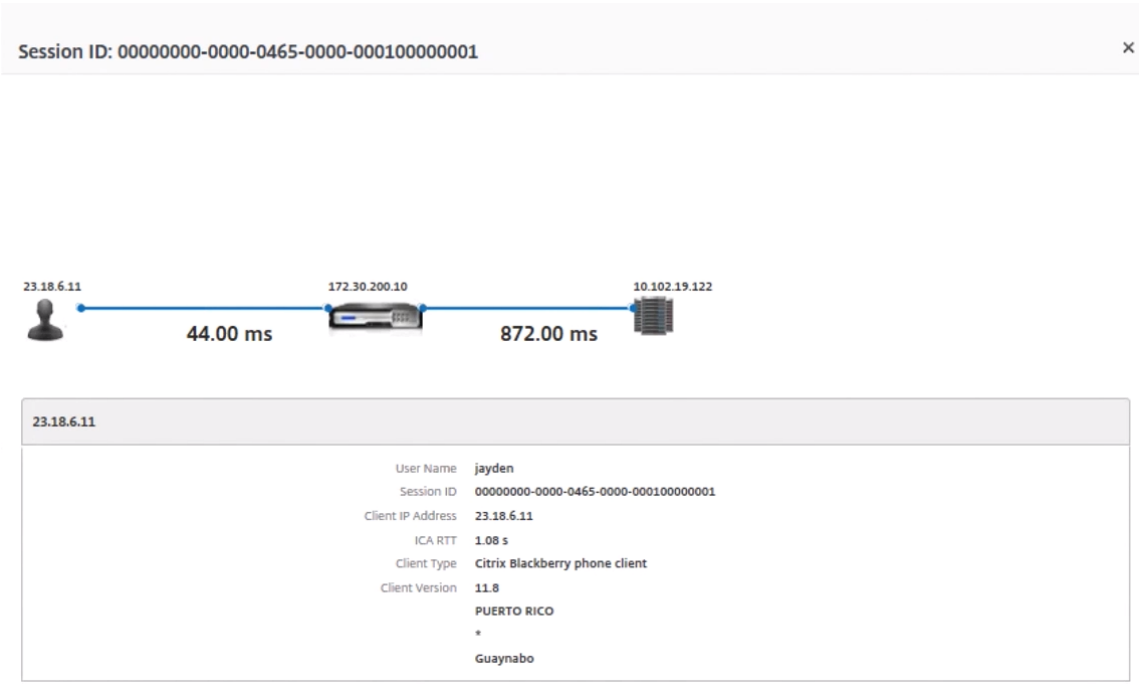
1. Navigate to **Gateway > HDX Insight> Users**.
2. Scroll down and select the user name and select the period from the list. The period can be one day, one week, one month, or you can even customize the period for which you want to see the data.
3. The chart displays the ICA RTT and DC latency values of the user for the specified period as a graph.

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



4. On the **Current Sessions** table, hover the mouse over the **RTT** value and note the host delay, DC latency, and WAN latency values.
5. On the **Current 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 App or Desktop

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:

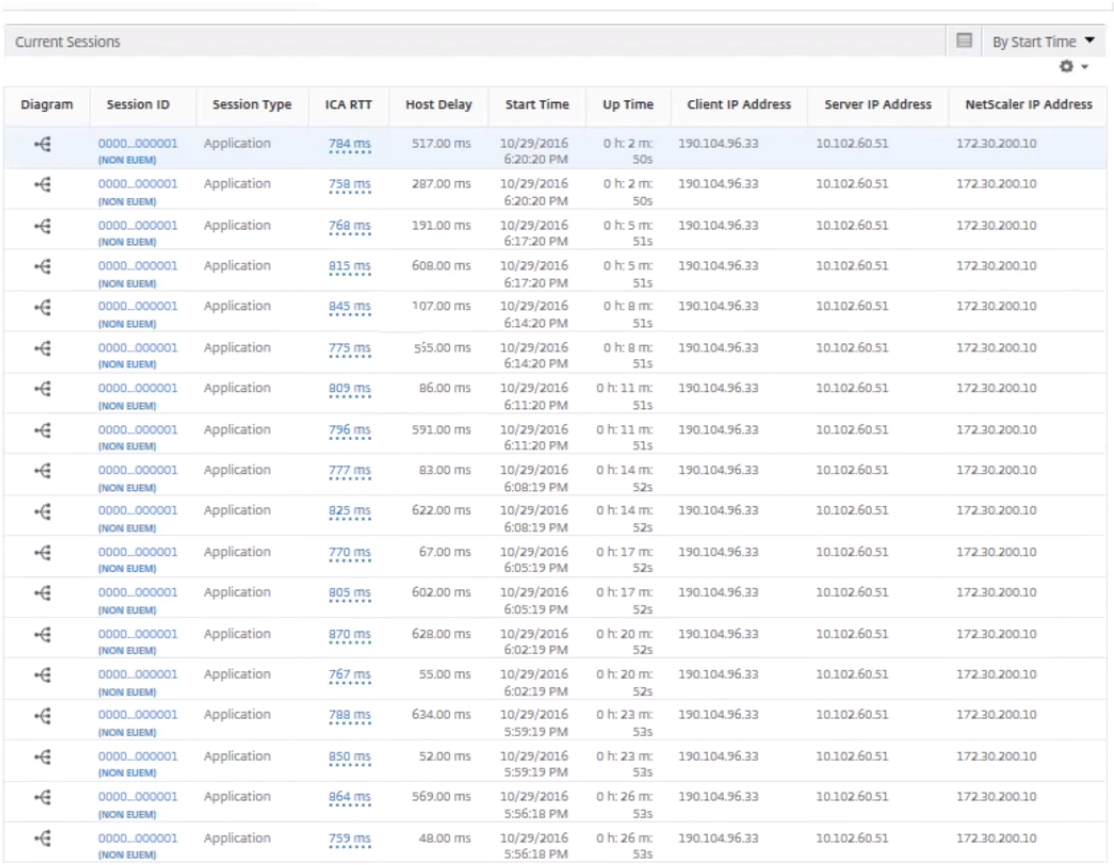
- WAN latency
- DC latency
- Host delay

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 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.



Geomaps for HDX Insight

The NetScaler Console geomaps functionality displays the usage of applications across different geographical locations on a map. Administrators can use this information to understand the trends in application usage across various geographical locations.

You can configure NetScaler Console to display the geomaps for a particular geographical location or LAN by specifying the private IP range (start and end IP address) for the location.

You can also view the historical and active users' details from the geo location maps in HDX Insight. Navigate to **Gateway > HDX Insight**, and in the **World** section of the map, click the country or region for which you want to see the details. You can further drill down to view information by city and state.

To configure a geomap for data centers:

Navigate to **Settings > Analytics Settings > IP Blocks** to configure geomaps for a particular location.

Use case

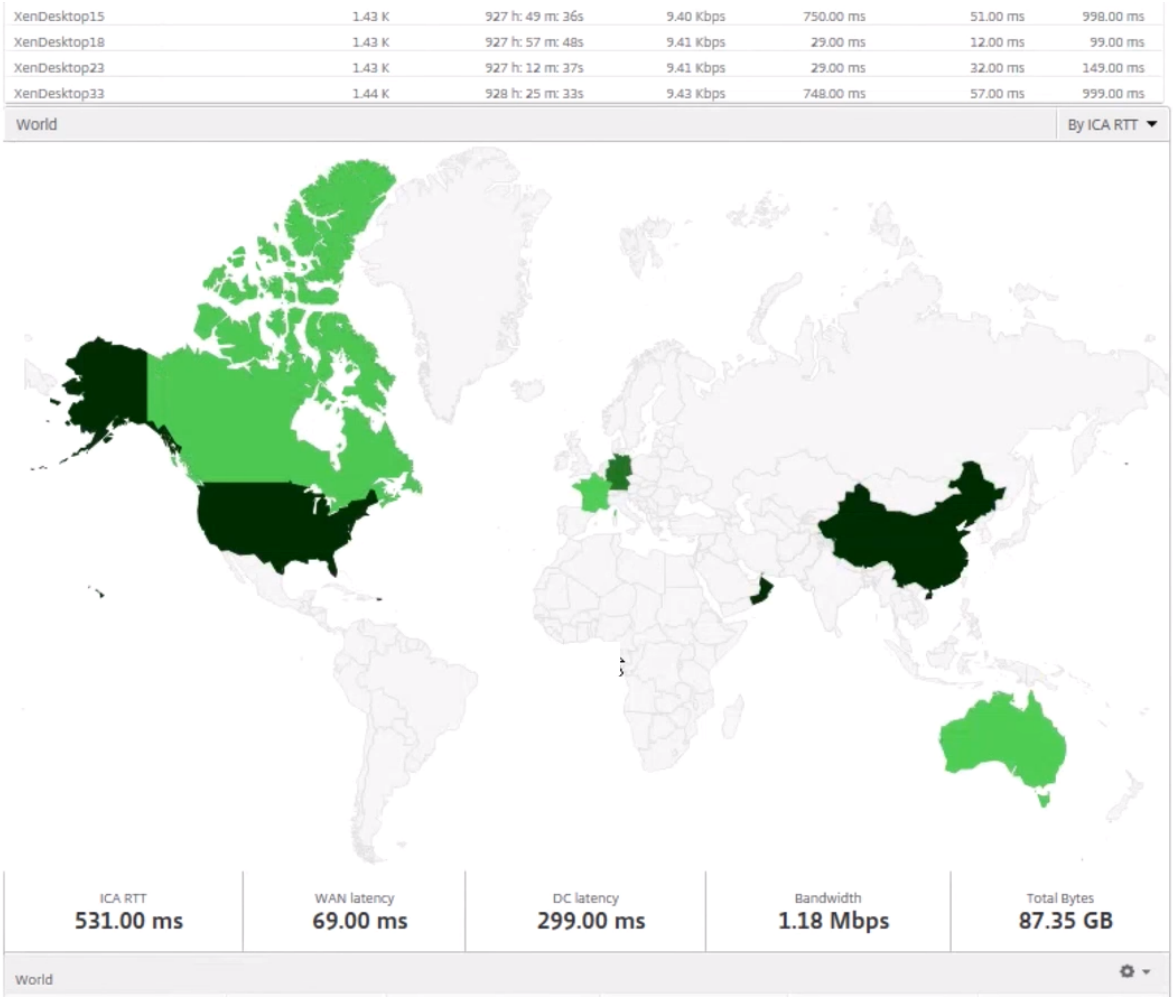
Consider a scenario in which organization ABC has 2 branch offices, one in Santa Clara and the other in India.

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.

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

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.



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.

Enabling HDX™ Insight data collection

September 27, 2025

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

HDX Insight enables IT to deliver an exceptional user experience by providing unprecedented end-to-end visibility into the ICA traffic that passes through the NetScaler instances and is a part of NetScaler Console Analytics. 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.

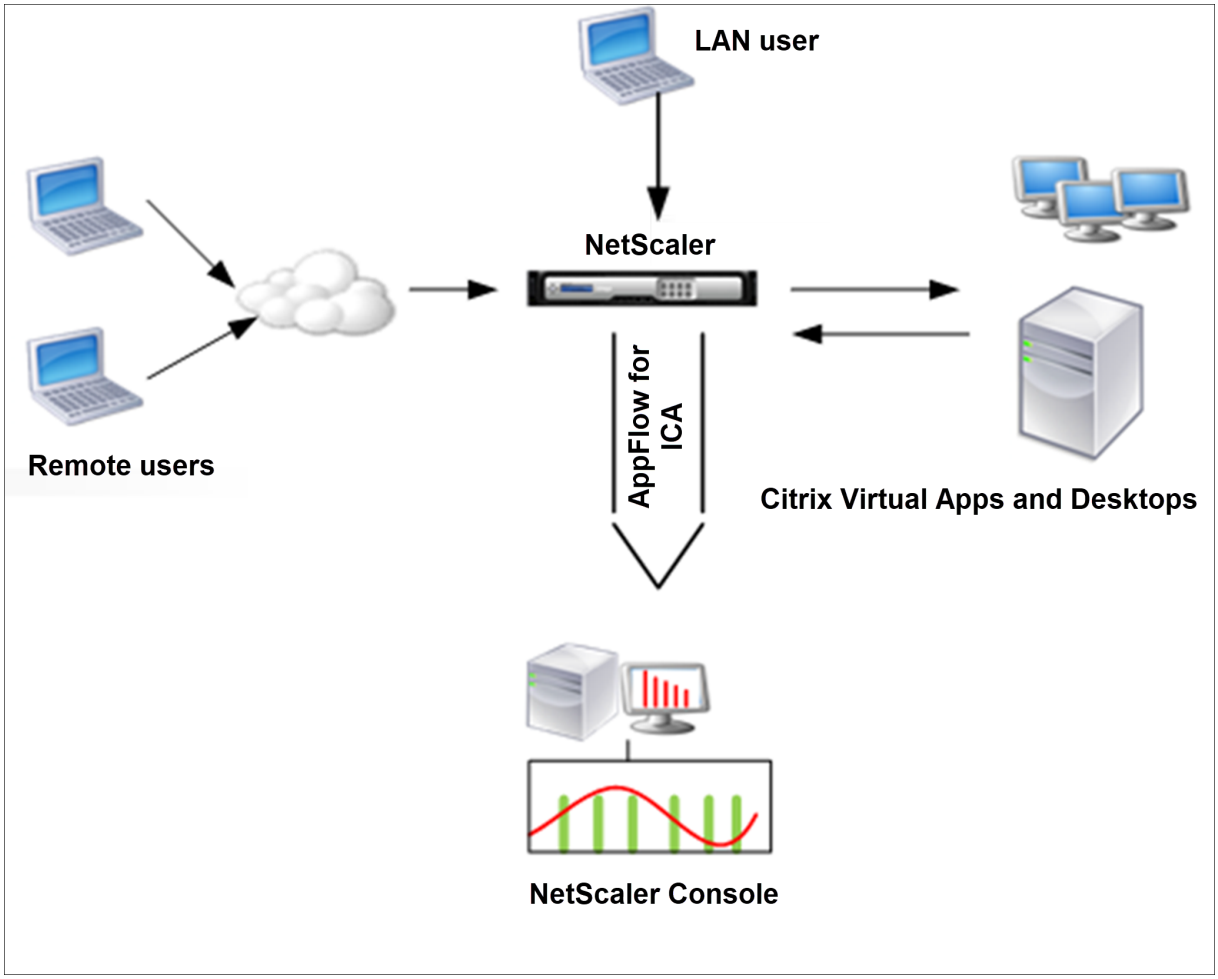
The configuration to enable data collection in the NetScaler differs with the position of the appliance in the deployment topology.

Enabling data collection for monitoring NetScalers deployed in LAN user mode

External users who access Citrix Virtual App and 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 App and Desktop applications, you can deploy the NetScaler appliance in a LAN user mode by configuring a cache redirection virtual server, which acts as a SOCKS proxy on the NetScaler Gateway appliance.

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



> **Note:** NetScaler Console and NetScaler Gateway appliance reside in the same subnet.

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:**
>
> - On a NetScaler instance, you can navigate to **Settings > AppFlow > Collectors**, to check if the collector (that is, NetScaler Console) is up or not. NetScaler instance sends AppFlow records to NetScaler Console using NSIP. But the instance uses its SNIP to verify connectivity with NetScaler Console. So, ensure that the SNIP is configured on the instance.
> - You cannot enable data collection on a NetScaler deployed in LAN User mode by using the NetScaler Console configuration utility.
> - For detailed information about the commands and their usage, see Command Reference.
> - For information on policy expressions, see Policies and Expressions.

© 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. 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 be applied by a policy that matches the VPN traffic.

```
add vpn trafficAction <name> <qual> [-HDX ( ON or 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.

```
add appflow policy <policyname> <rule> <action>
```

Example:

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

```
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. Type: `save ns config`

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

When you deploy NetScaler Gateway in single-hop mode, it is at the edge of the network. The Gateway instance provides proxy ICA connections to the desktop delivery infrastructure. Single-hop is the simplest and most common deployment. Single-hop 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.

To enable the AppFlow feature from NetScaler Console:

1. In a web browser, type the IP address of the NetScaler Console (for example, http://192.168.100.1).
2. In **User Name** and **Password**, enter the administrator credentials.
3. Navigate to **Infrastructure > Instances**, and select the NetScaler instance you want to enable analytics.
4. From the **Select Action** list, select **Configure Analytics**.

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

5. Select the VPN virtual servers, and click **Enable Analytics**.
6. Select **HDX Insight** and then select **ICA**.
7. Click **OK**.

> **Note**
>
> when you enable AppFlow in single-hop mode, the following commands run in the background. These commands are explicitly specified here for troubleshooting purposes.

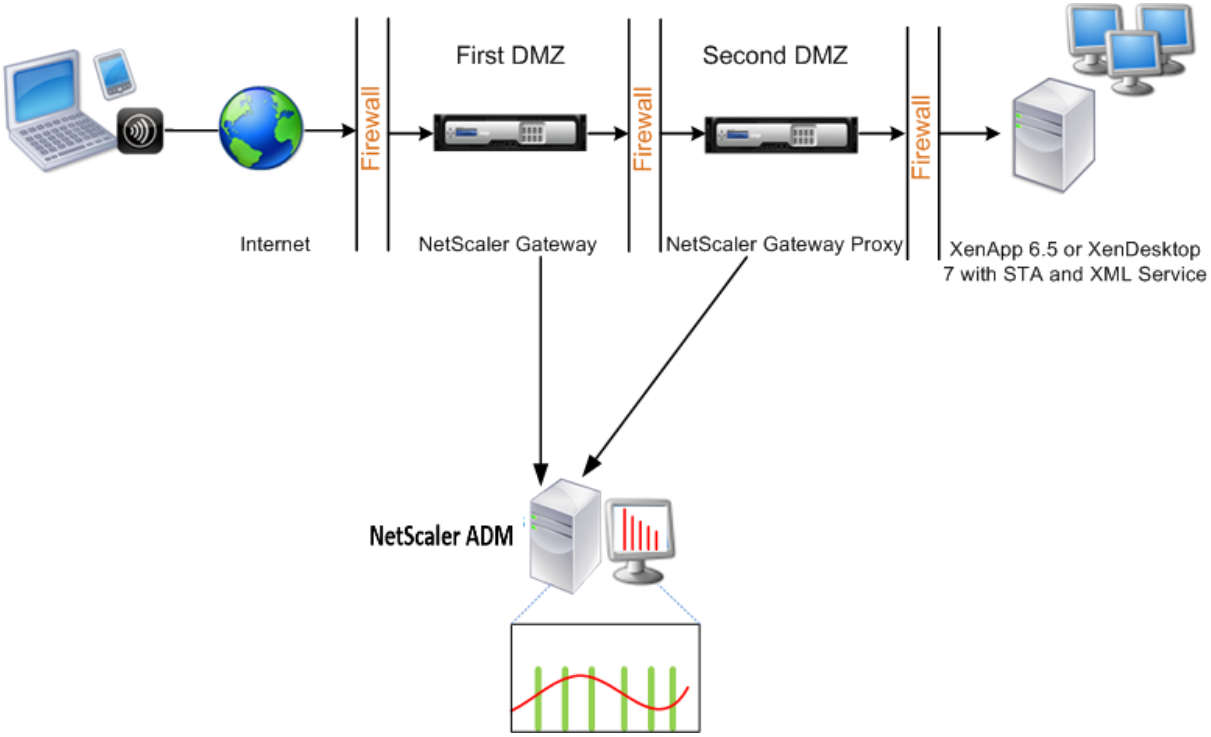
```
1  -  add appflow collector <name> -IPAddress <ip_addr>
2
3  -  add appflow action <name> -collectors <string>
4
5  -  set appflow param -flowRecordInterval <secs>
6
7  -  disable ns feature AppFlow
8
9  -  enable ns feature AppFlow
10
11 -  add appflow policy <name> <rule> <expression>
12
13 -  set appflow policy <name> -rule <expression>
14
15 -  bind vpn vserver <vsname> -policy <string> -type <type> -priority <
      positive_integer>
16
17 -  set vpn vserver <name> -appflowLog ENABLED
18
19 -  save ns config
```

EUEM virtual channel data is part of HDX Insight data that the NetScaler Console receives from Gateway instances. EUEM virtual channel provides the data about ICA RTT. If EUEM virtual channel is not enabled, the remaining HDX Insight data are still displayed on NetScaler Console.

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

The NetScaler Gateway double-hop mode provides additional protection to an organization's internal network because an attacker would need to penetrate multiple security zones or Demilitarized zones (DMZ) to reach the servers in the secure network. If you want to analyze the number of hops (NetScaler Gateway appliances) through which the ICA connections pass, and also the details about the latency on each TCP connection and how it fairs against the total ICA latency perceived by the client, you must install NetScaler Console so that the NetScaler Gateway appliances report these vital statistics.

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



The NetScaler Gateway in the first DMZ handles user connections and performs the security functions of an SSL VPN. This NetScaler Gateway encrypts user connections, determines how the users are authenticated, and controls access to the servers in the internal network.

The NetScaler Gateway in the second DMZ serves as a NetScaler Gateway proxy device. This NetScaler Gateway enables the ICA traffic to traverse the second DMZ to complete user connections to the server farm.

The NetScaler Console can be deployed either in the subnet belonging to the NetScaler Gateway appliance in the first DMZ or the subnet belonging to the NetScaler Gateway appliance second DMZ. In the above image, the NetScaler Console and NetScaler Gateway in the first DMZ are deployed in the same subnet.

In a double-hop mode, NetScaler Console collects TCP records from one appliance and ICA records from the other appliance. After you add the NetScaler Gateway appliances to the NetScaler Console inventory and enable data collection, each of the appliances exports 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

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

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.

Configure HDX Insight on virtual servers used for Optimal Gateway

Steps to configure HDX Insight on virtual servers used for Optimal Gateway:

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 server configured for authentication, and click **Enable Analytics**.
4. Select **HDX Insight** and then select **ICA**.
5. Select other advanced options as required.
6. Click **OK**.
7. Repeat steps 3 through 6 on the other VPN virtual server.

Enable 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. That is both the appliances report the same metrics. To overcome this situation, you must enable AppFlow for ICA on one of the first NetScaler Gateway appliances, and then enable AppFlow for TCP 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. In a web browser, type the IP address of the NetScaler Console (for example, http://192.168.100.1).
2. In **User Name** and **Password**, enter the administrator credentials.
3. Navigate to **Infrastructure > Instances**, and select the NetScaler instance you want to enable analytics.
4. From the **Select Action** list, select **Configure Analytics**.
5. Select the VPN virtual servers, and click **Enable Analytics**.
6. Select **HDX Insight** and then select **ICA** or **TCP** for ICA traffic or TCP traffic respectively.

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

> **Note**
>
> If AppFlow logging is not enabled for the respective services or service groups on the NetScaler appliance, the NetScaler Console dashboard does not display the records, even if the Insight column shows Enabled.

7. Click **OK**.

Configuring NetScaler Gateway appliances to export data

After you install the NetScaler Gateway appliances, you must configure the following settings on the NetScaler Gateway appliances to export the reports to NetScaler Console:

- Configure virtual servers of the NetScaler Gateway appliances in the first and second DMZ to communicate with each other.
- Bind the NetScaler Gateway virtual server in the second DMZ to the NetScaler Gateway virtual server in the first DMZ.
- Enable double hop on the NetScaler Gateway in the second DMZ.
- Disable authentication on the NetScaler Gateway virtual server in the second DMZ.
- Enable one of the NetScaler Gateway appliances to export ICA records
- Enable the other NetScaler Gateway appliance to export TCP records:
- Enable connection chaining on both the NetScaler Gateway appliances.

Configure NetScaler Gateway Using the Command Line Interface:

1. Configure the NetScaler Gateway virtual server in the first DMZ to communicate with the NetScaler Gateway virtual server in the second DMZ.

```
add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [-secure (
    ON or OFF)] [-imgGifToPng]

add vpn nextHopServer nh1 10.102.2.33 8443  – secure ON
```

2. Bind the NetScaler Gateway virtual server in the second DMZ to the NetScaler Gateway virtual server in the first DMZ. Run the following command on the NetScaler Gateway in the first DMZ:

```
bind vpn vserver <name> -nextHopServer <name>

bind vpn vserver vs1 -nextHopServer nh1
```

3. Enable double hop and AppFlow on the NetScaler Gateway in the second DMZ.

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

```
set vpn vserver <name> [- doubleHop ( ENABLED or DISABLED )] [-
    appflowLog ( ENABLED or DISABLED )]

set vpn vserver vpnhop2  – doubleHop ENABLED  – appFlowLog ENABLED
```

4. Disable authentication on the NetScaler Gateway virtual server in the second DMZ.

```
set vpn vserver <name> [-authentication (ON or OFF)]

set vpn vserver vs -authentication OFF
```

5. Enable one of the NetScaler Gateway appliances to export TCP records.

```
bind vpn vserver <name> [-policy <string> -priority <
    positive_integer>] [-type <type>]

bind vpn vserver vpn1 -policy appflowpol1 -priority 101  – type
    OTHERTCP_REQUEST
```

6. Enable the other NetScaler Gateway appliance to export ICA records:

```
bind vpn vserver <name> [-policy <string> -priority <
    positive_integer>] [-type <type>]

bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
    ICA_REQUEST
```

7. Enable connection chaining on both the NetScaler Gateway appliances:

```
set appFlow param [-connectionChaining (ENABLED or DISABLED)]

set appflow param -connectionChaining ENABLED
```

Configure 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**.

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

b) In the right pane, double-click the virtual server, and in the **Basic Settings** group, click the edit icon.

c) Expand more, select **Double Hop** and click **OK**.

3. Disable authentication on the virtual server on the NetScaler Gateway in the second DMZ.

a) On the **Configuration** tab expand **NetScaler Gateway** and click **Virtual Servers**.

b) In the right pane, double-click the virtual server, and in the **Basic Settings** group, click the edit icon.

c) Expand **More**, and clear **Enable Authentication**.

4. Enable one of the NetScaler Gateway appliances to export TCP records.

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 theChoose 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, double-click **Change Appflow Settings**.

c) Select **Connection Chaining** and Click **OK**.

7. 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.

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

a) On the Configuration tab expand **NetScaler Gateway** and click **Virtual Servers**.

b) In the right pane, double-click the virtual server, and in the **Advanced group**, expand **Published Applications**.

c) Click **Next Hop Server** and bind a next hop server to the second NetScaler Gateway appliance.

8. 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**.

9. 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**.

10. 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**.

11. 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**.

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

e) Add a policy binding, and click **Close**.

12. Enable connection chaining on both the NetScaler Gateway appliances.

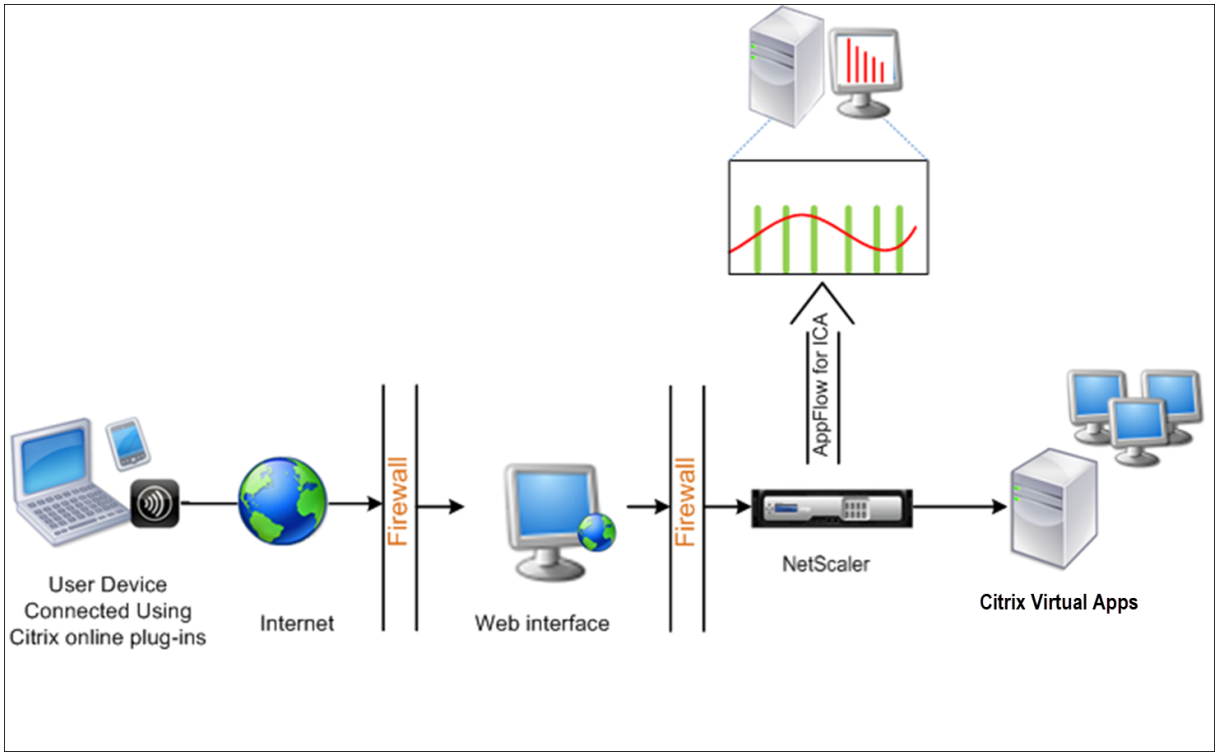
Enable data collection for monitoring NetScalers deployed in transparent mode

When a NetScaler is deployed in transparent mode the clients can access the servers directly, with no intervening virtual server. If a NetScaler appliance is deployed in transparent mode in a Citrix Virtual Apps and Desktop 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 figure 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
```

> **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:

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

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

> **Note**
>
> The value of **type** must be ICA_REQ_OVERRIDE or ICA_REQ_DEFAULT to apply to ICA traffic.

7. Set the value of the flowRecordInterval parameter for AppFlow to 60 seconds.

```
set appflow param -flowRecordInterval 60
```

Example:

```
set appflow param -flowRecordInterval 60
```

8. Save the configuration. Type: `save ns config`

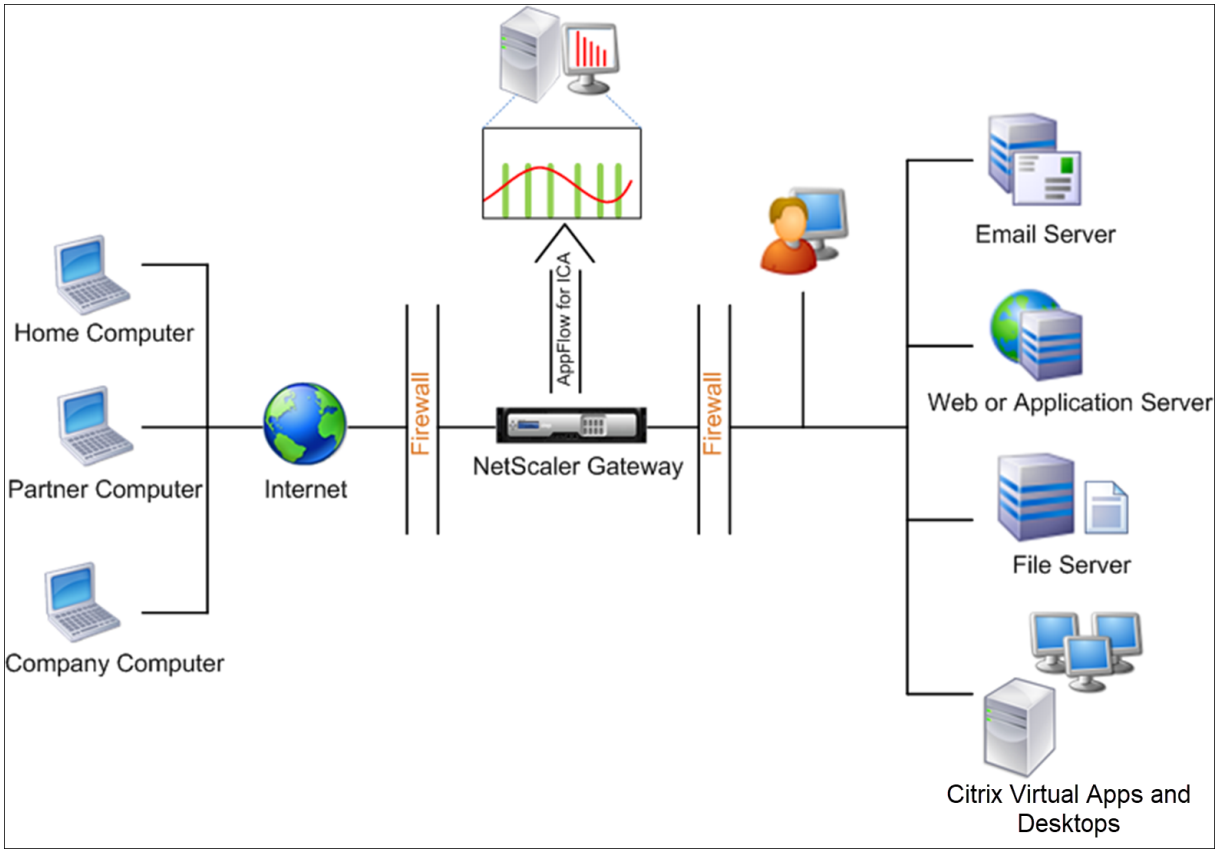
Enable data collection for NetScaler Gateway appliances deployed in single-hop mode

September 27, 2025

When you deploy NetScaler Gateway in single-hop mode, it is at the edge of the network. The Gateway instance provides proxy ICA connections to the desktop delivery infrastructure. Single-hop is the simplest and most common deployment. Single-hop 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.

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



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 **Action** list, select **Enable/Disable Insight**.
3. Select the **VPN virtual servers**, and click **Enable AppFlow®**.
4. In the **Enable AppFlow** field, type **true**, and select **ICA®**.
5. Click **OK**.

> **Note**
>
> When you enable AppFlow in single-hop mode, the following commands run in the background. 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`
> - `enable ns feature AppFlow`
> - `add appflow policy \<name\> \<rule\> \<expression\>`

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

```
• 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
```

EUEM virtual channel data is part of HDX Insight data that the NetScaler Console receives from Gateway instances. EUEM virtual channel provides the data about ICA RTT. If EUEM virtual channel is not enabled, the remaining HDX Insight data are still displayed on NetScaler Console.

Enable data collection to monitor NetScalers deployed in transparent mode

September 27, 2025

When a NetScaler is deployed in transparent mode the clients can access the servers directly, with no intervening virtual server. If a NetScaler is deployed in transparent mode in a Citrix Virtual Apps and Desktops environment, the ICA traffic is not transmitted over a VPN.

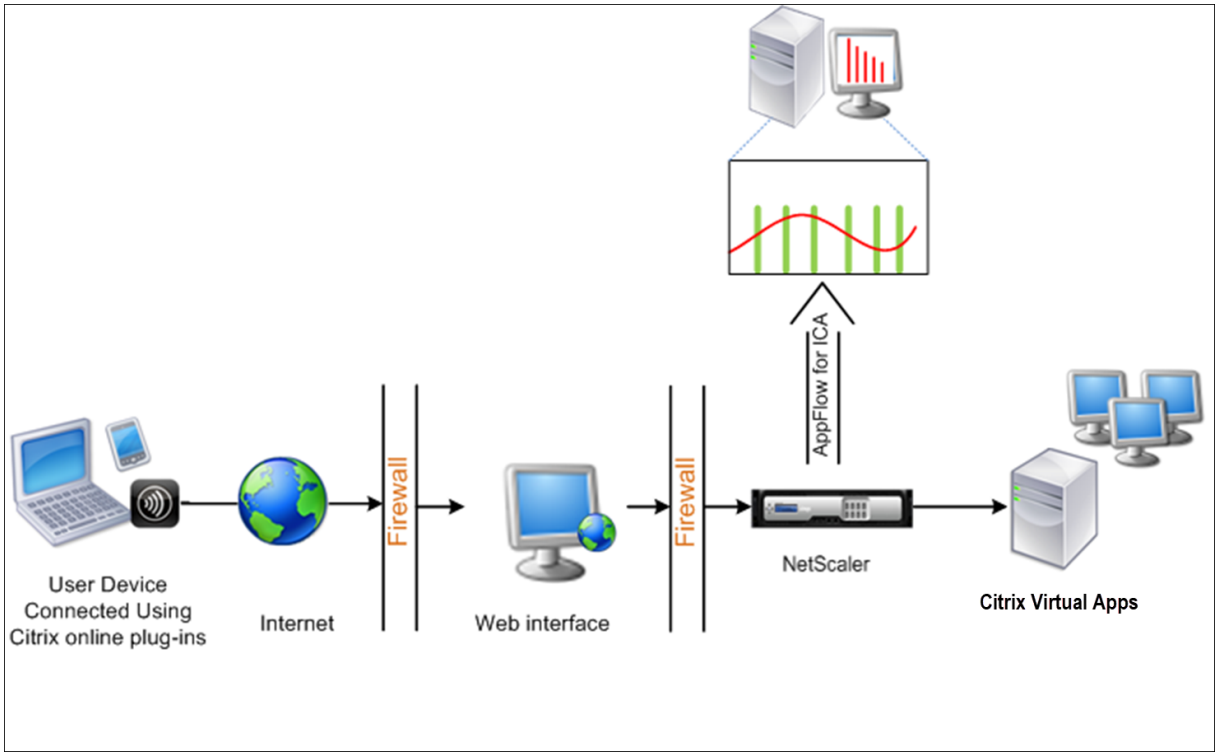
After you add the NetScaler to the NetScaler Console inventory, you must enable AppFlow for data collection. Enabling data collection depends on the device and the mode. In that case, you have to add NetScaler Console as an AppFlow collector on each NetScaler instance, and you must configure an AppFlow 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 figure 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 instance.

```
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 instance, 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
```

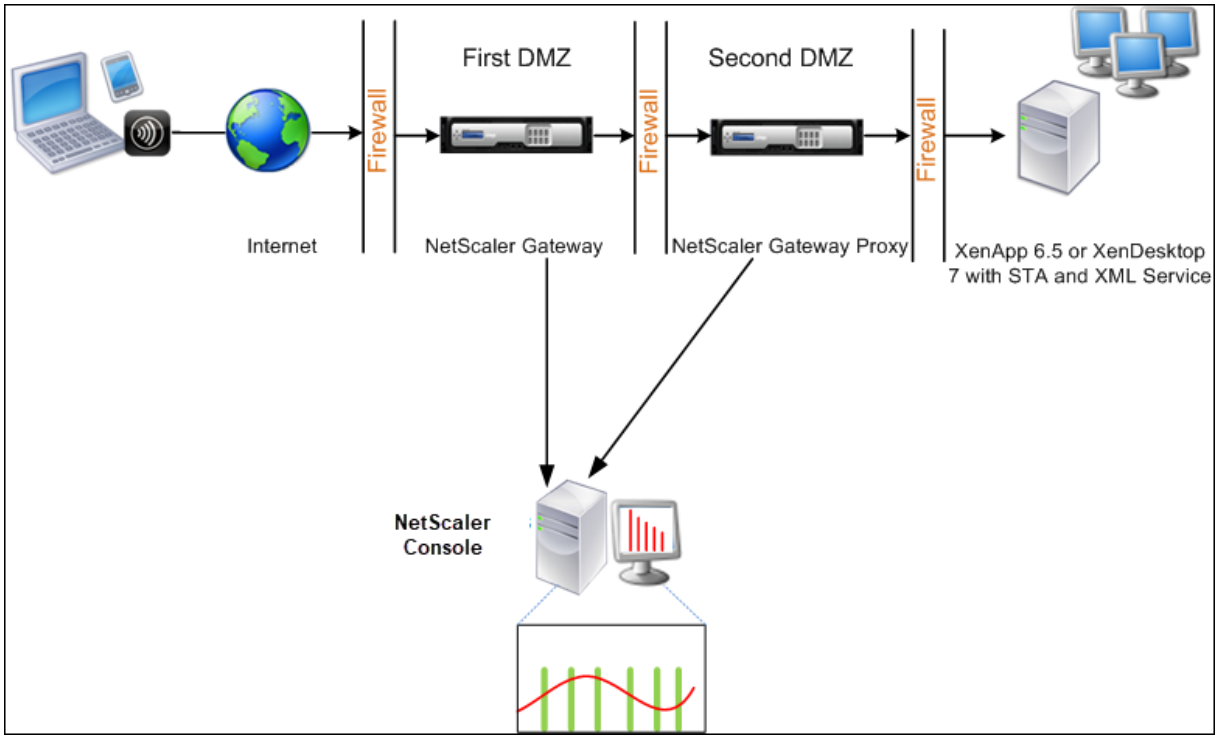
Enable data collection for NetScaler Gateway appliances deployed in double-hop mode

September 27, 2025

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

The NetScaler Gateway double-hop mode provides extra protection to an organization's internal network, because an attacker would need to penetrate multiple security zones or Demilitarized zones (DMZ) to reach the servers in the secure network. If you want to analyze the number of hops (NetScaler Gateway appliances) through which the ICA connections pass, and also the details about the latency on each TCP connection and how it fairs against the total ICA latency perceived by the client, you must install NetScaler Console, so that the NetScaler Gateway appliances report these vital statistics.

Figure 3. NetScaler Console deployed in double-hop mode



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 the above image, the NetScaler Console and NetScaler Gateway in the first DMZ are deployed in the same subnet.

In a double-hop mode, NetScaler Console collects TCP records from one appliance and ICA records from the other appliance. After you add the NetScaler Gateway appliances to the NetScaler Console inventory and enable data collection, each appliance exports the reports by keeping track of the hop count and connection chain ID.

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

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.

Enable 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. That is both the appliances report the same metrics. To overcome this situation, you must enable AppFlow for TCP on one of the first NetScaler Gateway appliances, 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 **Action** list, select **Enable/Disable Insight**.
3. Select the VPN virtual servers, and click **Enable AppFlow®**.
4. In the **Enable AppFlow** field, type **true**, and select **ICA/TCP** for ICA traffic a TCP traffic respectively.

   > **Note**
   >
   > If AppFlow logging is not enabled for the services or service groups on the NetScaler appliance, the NetScaler Console dashboard does not display the records, even if the Insight column shows Enabled.

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:

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

- Configure virtual servers of the NetScaler Gateway appliances in the first and second DMZ to communicate with each other.
- Bind the NetScaler Gateway virtual server in the second DMZ to the NetScaler Gateway virtual server in the first DMZ.
- Enable double hop on the NetScaler Gateway in the second DMZ.
- Disable authentication on the NetScaler Gateway virtual server in the second DMZ.
- Enable one of the NetScaler Gateway appliances to export ICA records
- Enable the other NetScaler Gateway appliance to export TCP records:
- Enable connection chaining on both the NetScaler Gateway appliances.

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**] ...

```
add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON
```

2. Bind the NetScaler Gateway virtual server in the second DMZ to the NetScaler Gateway virtual server in the first DMZ. Run the following command on the NetScaler Gateway in the first DMZ:

   bind vpn vserver <name> **-nextHopServer** <name>

```
bind vpn vserver vs1 -nextHopServer nh1
```

3. Enable double hop and AppFlow on the NetScaler Gateway in the second DMZ.

set vpn vserver [**- doubleHop** (ENABLED DISABLED)] [**- appflowLog** (ENABLED DISABLED)]

```
set vpn vserver vpnhop2 –doubleHop ENABLED –appFlowLog ENABLED
```

4. Disable authentication on the NetScaler Gateway virtual server in the second DMZ.

set vpn vserver [**-authentication** (ON OFF)]

```
set vpn vserver vs -authentication OFF
```

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

5. Enable one of the NetScaler Gateway appliances to export TCP records.

   bind vpn vserver<name> [**-policy**<string> **-priority**<positive_integer>] [**-type**<type>]

   ```
   1 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>]

   ```
   1 bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type ICA\
       _REQUEST
   ```

7. Enable connection chaining on both the NetScaler Gateway appliances:

---

set appFlow DISABLED)]
param [**-connectionChaining** (ENABLED

```
1 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**.

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

b) In the right pane, double-click the virtual server, and in the **Basic Settings** group, click the edit icon.

c) Expand **More**, and clear **Enable Authentication**.

4. Enable one of the NetScaler Gateway appliances to export TCP records.

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** drop-down 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** drop-down list, select **AppFlow**, and from theChoose Type drop-down 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 **Settings > 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

September 27, 2025

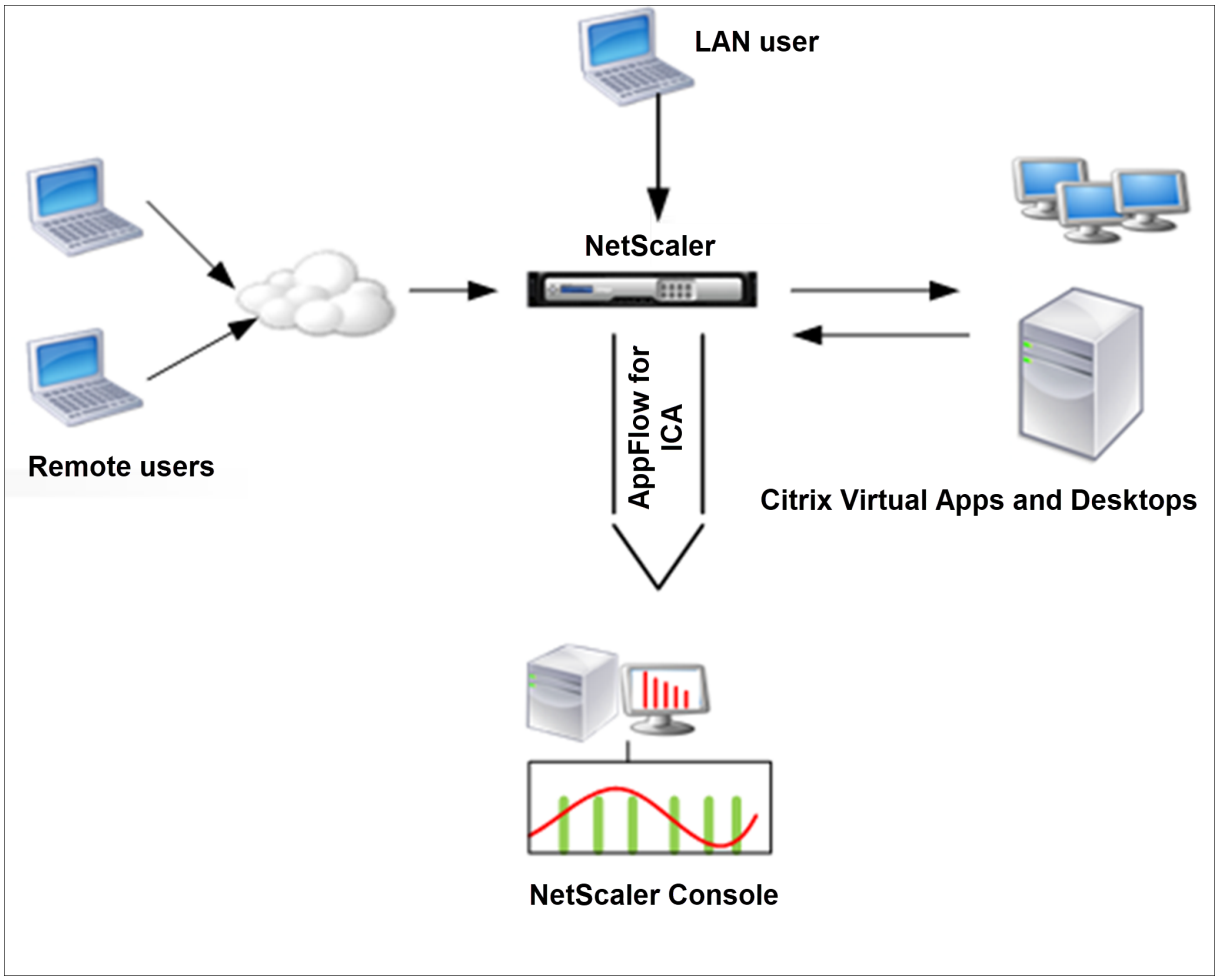
External users who access Citrix Virtual App or Desktop applications must authenticate themselves on the NetScaler Gateway. Internal users, however, might not require to be redirected to the NetScaler

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

Gateway. Also, in a transparent mode deployment, the administrator must manually apply the routing policies, so that the requests are redirected to the NetScaler appliance.

To overcome these challenges, and for LAN users to directly connect to Citrix Virtual Apps and Desktops applications, you can deploy the NetScaler appliance in a LAN user mode by configuring a cache redirection virtual server, which acts as a SOCKS proxy on the NetScaler Gateway appliance.

Figure 4. NetScaler Console deployed in LAN User Mode



Note NetScaler Console and NetScaler Gateway appliance reside in the same subnet.

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

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

> NetScaler Console configuration utility.
> - For detailed information about the commands and their usage, see Command Reference.
> - For information on policy expressions, see Policies and Expressions.

To configure data collection on a NetScaler appliance by using the command line interface:

At the command prompt, do the following:

1. Log on to an 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 be applied by 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
```

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

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
```

Example:

```
set appflow param -flowRecordInterval 60
```

8. Save the configuration.

```
save ns config
```

Create thresholds and configure alerts for HDX™ Insight

September 27, 2025

HDX Insight on NetScaler Console allows you to monitor the HDX traffic passing through 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 various 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 case of 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 and/or receive the alert as an email 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 NetScaler Gateway and

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

Citrix GSLB based redirection. Eric, the Citrix Virtual Apps and Desktops admin for ABC Inc. wants to track the user experience for all their offices to optimize the apps and desktop delivery for anywhere, anytime access. Eric also wants to check the user-experience-metrics like ICA RTTs, latencies, and raise any deviations proactively.

The users of ABC Inc. have a distributed presence. Some users are located close to the data center, while a few are located at further away from the data center. As the user base is distributed widely, the metrics and the corresponding thresholds also vary among these locations. For example, the ICA RTT for a location near to the data center can be 5–10 ms whereas the same for a remote location can be around 100 ms.

With threshold rule group management for HDX Insight, Eric can set geo-specific threshold rule groups for each location and be alerted through email or SMS for breaches per area. Eric is also able to combine tracking of more than one metric within a threshold rule group and narrow down the root cause to capacity issues if any. Eric is now able to proactively track any deviation without having to worry about the complexity of manually looking through all Citrix Virtual Apps and Desktops portfolio metrics.

To 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.

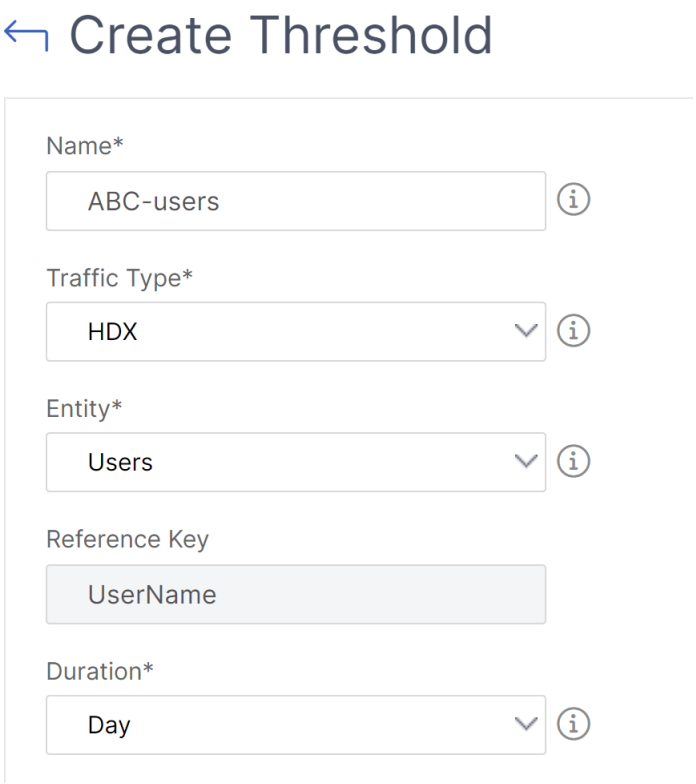
    b) **Traffic Type**. From the list box, select HDX.

    c) **Entity**. From the list box, 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.

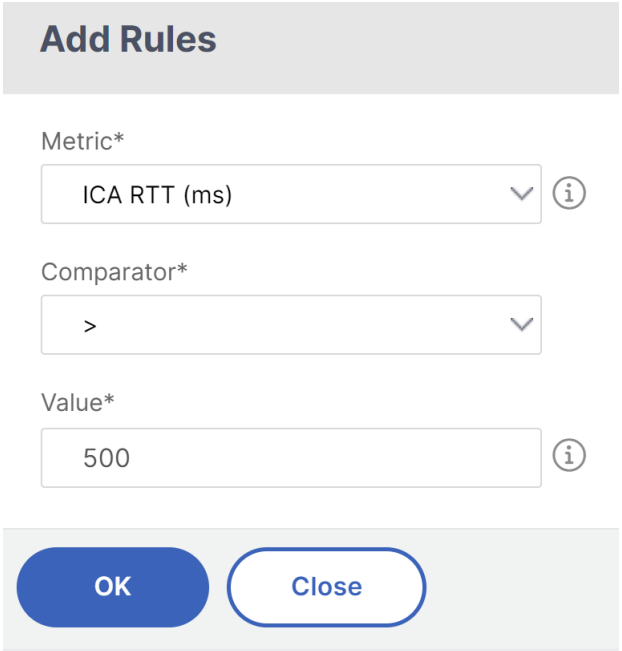
    e) **Duration**. From the list box, select the time interval for which you want to monitor the entity. You can monitor the entities for an hour, or for a day, or for a week's duration.

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



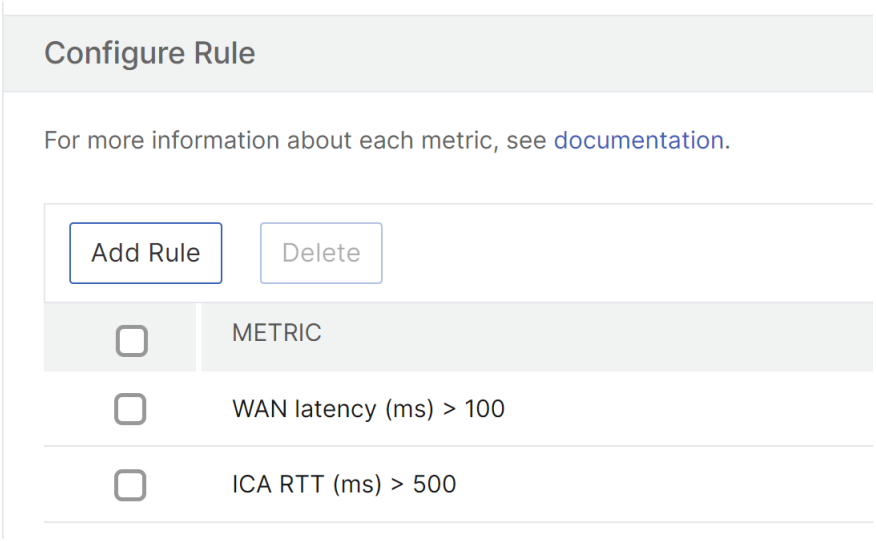
3. Creating threshold rules group for all entities:

   For HDX traffic, you must create a rule by clicking **Add Rule.** **E**nter the values in the **Add Rules** pop-up window that opens.



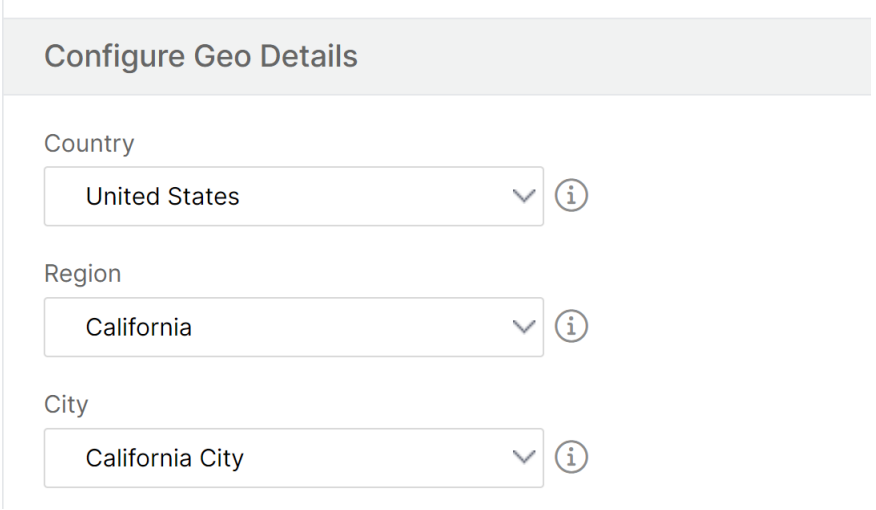
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 notifications and SMS notifications.
7. Click **Create** to create a threshold rule group.

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

Viewing HDX™ Insight reports and metrics

September 27, 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 App or Desktop 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 release 14.1 build 51.x, 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**.

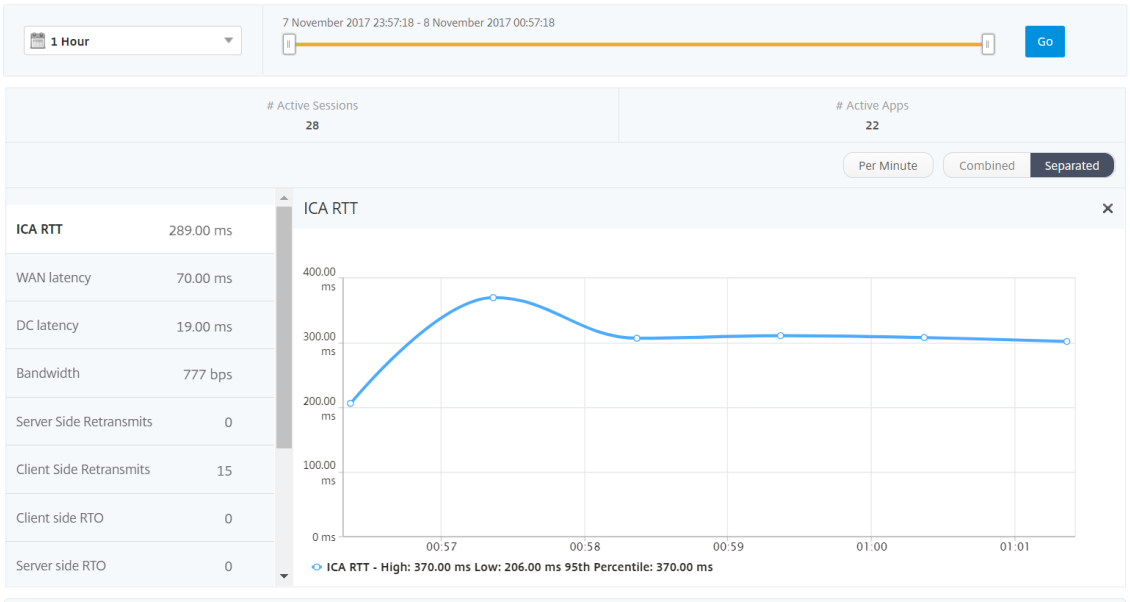
User view reports and metrics

The reports and metrics in this view are displayed per Citrix Virtual Apps and Desktops user.

To navigate to the users view:

1. Navigate to **Gateway > HDX Insight > Users**

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



User view reports and metrics consist of the following sections:

- Summary View
- Per User View
- Per User Session View

Summary view

The summary view displays the reports for all the users that have logged in during the selected time-line. All the metrics/reports in this view display the values corresponding to them for the selected time period unless specified otherwise.

To change the selected time period:

1. Use the time period list or the time slider to set the desired time interval.
2. Click **Go**.

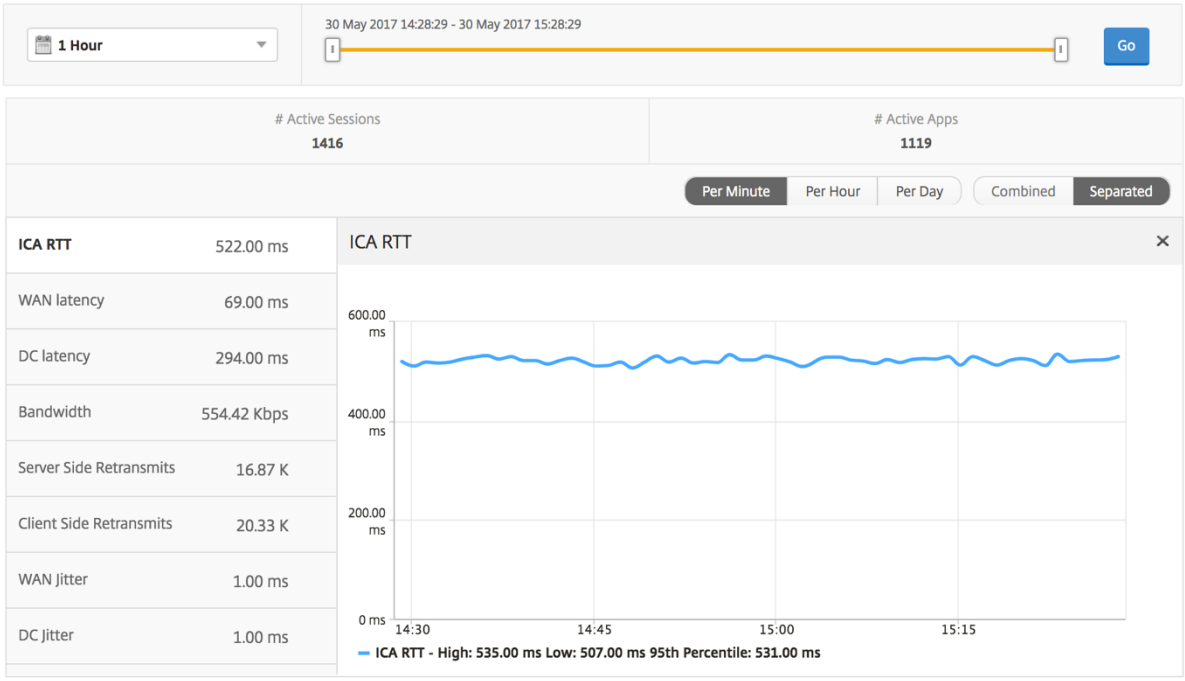
Line chart

Metrics	Description
Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
Active Apps	This number indicates the count of active Citrix Virtual App sessions.

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

Metrics	Description
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI OR CVAD or StoreFront servers.
Bandwidth	Total bytes per second taken for end-to-end communication during the selected time interval.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.

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



User summary report Following are the metrics that are specific to this report.

Metrics	Description
Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Bandwidth	Total bytes per second taken for end-to-end communication during the selected time interval.

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

Metrics	Description
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Total App Launch Count	Total Apps launched by the user during the selected time period.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Active Desktops	Total number of active Citrix Virtual Desktops during a given time interval.

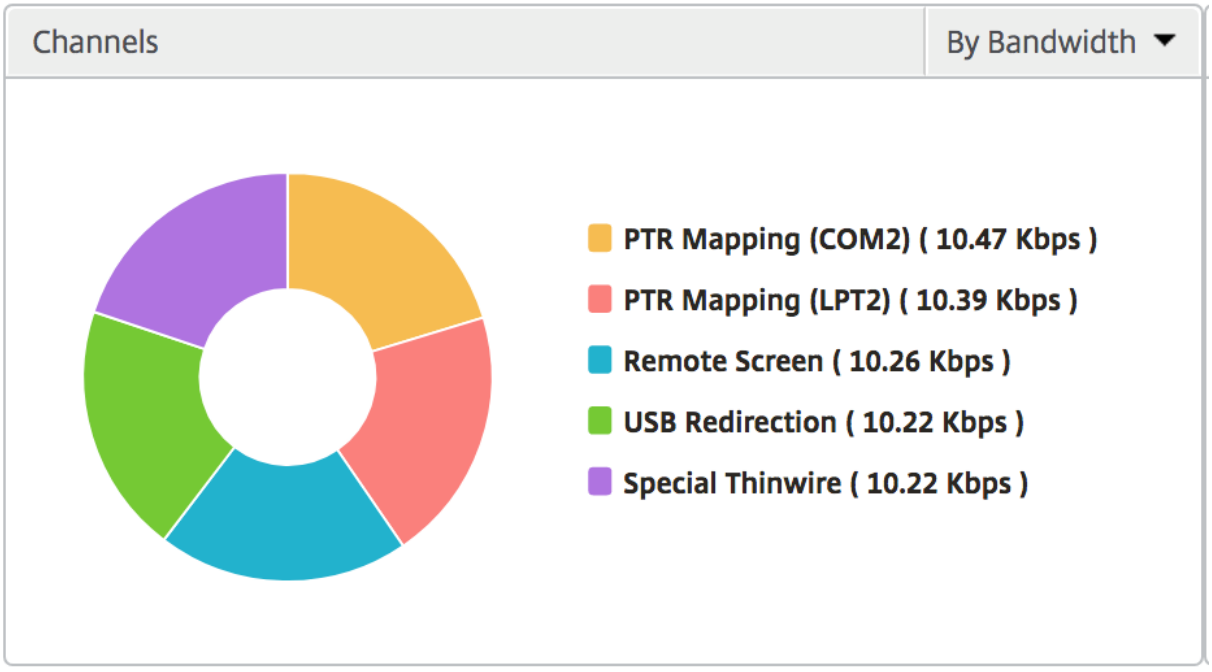
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Users

Search

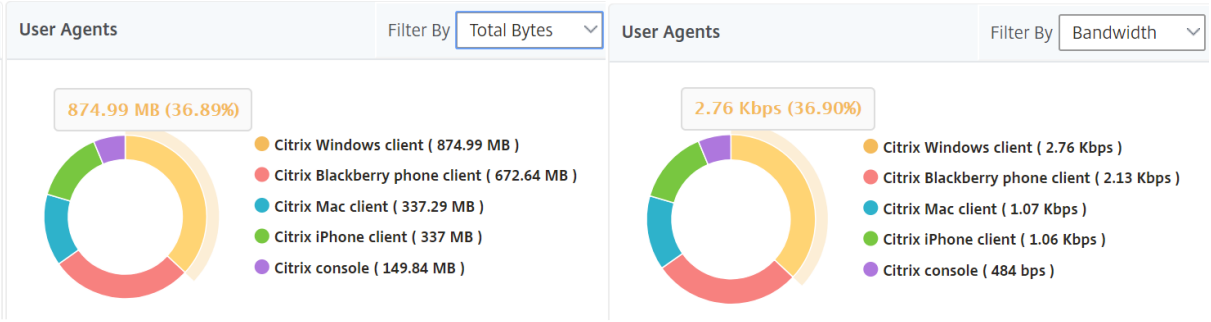
User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Cl
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	23.66 Kbps	1.88 K	
ramas	59	0	59	997.00 ms	778.00 ms	1.00 ms	7.03 Kbps	0	
omerp	59	0	59	997.00 ms	57.00 ms	754.00 ms	23.80 Kbps	1.89 K	
grahmm	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.80 Kbps	1.89 K	
ryan	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.69 Kbps	1.88 K	
rajivs	59	0	59	801.00 ms	11.00 ms	1.00 ms	23.97 Kbps	0	
alexisc	117	0	118	622.00 ms	56.00 ms	392.00 ms	47.67 Kbps	1.88 K	
juan	59	59	118	169.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
lennoxl	59	0	59	169.00 ms	31.00 ms	30.00 ms	23.86 Kbps	0	
daniel	59	59	118	149.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
woojunek	58	0	59	149.00 ms	31.00 ms	30.00 ms	23.85 Kbps	0	
parkerf	59	0	59	149.00 ms	31.00 ms	30.00 ms	23.88 Kbps	0	
randyb	59	59	118	99.00 ms	11.00 ms	29.00 ms	47.71 Kbps	0	
bradp	177	0	177	74.00 ms	27.00 ms	1.00 ms	71.75 Kbps	0	

Channels Channels represent the overall bandwidth or the total bytes consumed by each ICA® virtual channel in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.

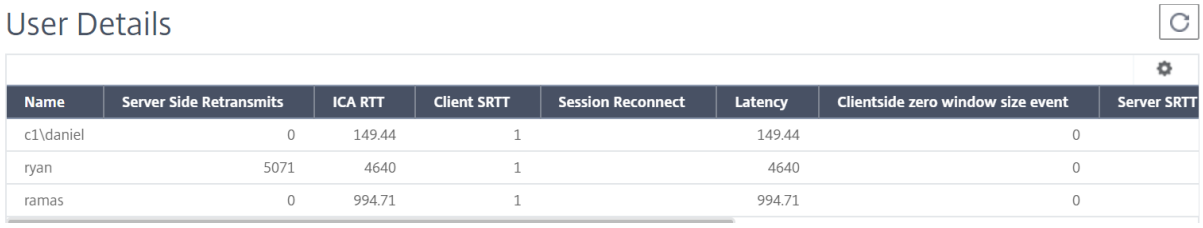


© 1997–2025 Citrix Systems, Inc. All rights reserved.

User agents User agents represent the overall bandwidth/total bytes consumed by each workspace client in the form of a doughnut chart. Each colored segment in the chart represents one workspace client. The length of the segment depends on the number of users launching their applications on that workspace client. You can also sort the metrics by bandwidth, or total bytes.



Click each segment to view the details of the users using that workspace client.



Name	Server Side Retransmits	ICA RTT	Client SRTT	Session Reconnect	Latency	Clientside zero window size event	Server SRTT
c1\daniel	0	149.44	1		149.44	0	
ryan	5071	4640	1		4640	0	
ramas	0	994.71	1		994.71	0	

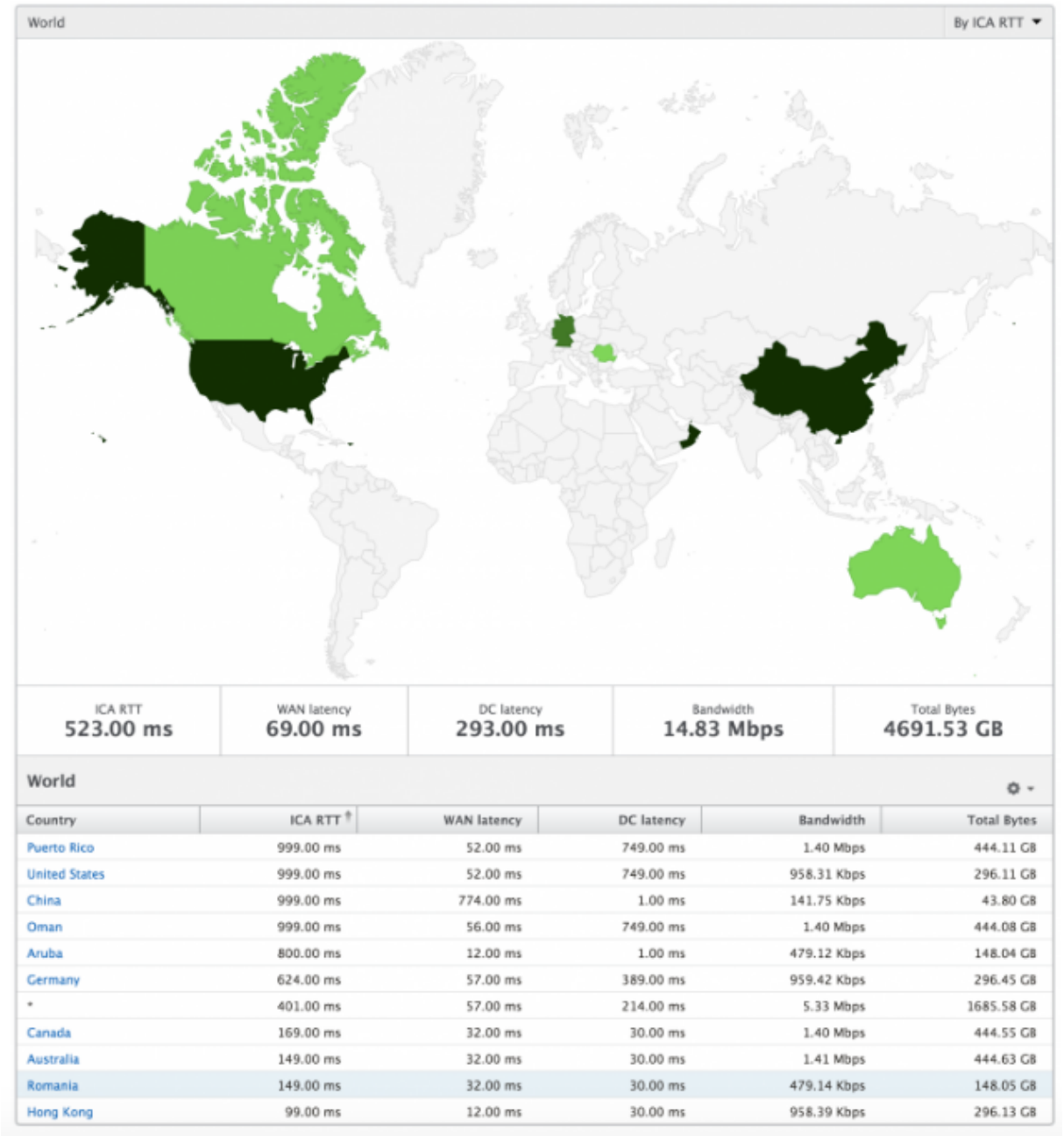
Thresholds breach count The Thresholds breach count metrics represent the count of thresholds breached in the selected time period.

World map The World map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill down to a particular country and further into cities as well by simply clicking the region. The administrators can further drill down to view information by city and state. From NetScaler Console version 12.0 and later, you can drill down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metric is displayed in the form of a heat map:

- ICA RTT
- WAN Latency
- DC Latency
- Bandwidth
- Total Bytes

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



Per User view

The per user view provides detailed end user experience reporting for any particular selected user.

To navigate to specific user's metrics:

1. Log on to your NetScaler Console using a supported web browser.
2. Navigate to **Gateway > HDX Insight > Users**.
3. Select a particular user from the Users summary report.

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

Line chart Line chart displays the summary of all the metrics for the particular selected user during the selected time period.

Current/Terminated sessions report This report is pertinent to all current/terminated user sessions for the selected user. These metrics can be sorted by start time, session reconnects and ACR count.

Metrics	Description
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScalers caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.
Server IP Address	Backend/ Citrix Virtual App server IP.
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Workspace type- Citrix Windows Client and so on
Client Version	Workspace version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.
Country	Country from which the session was established.

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

Metrics	Description
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.

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

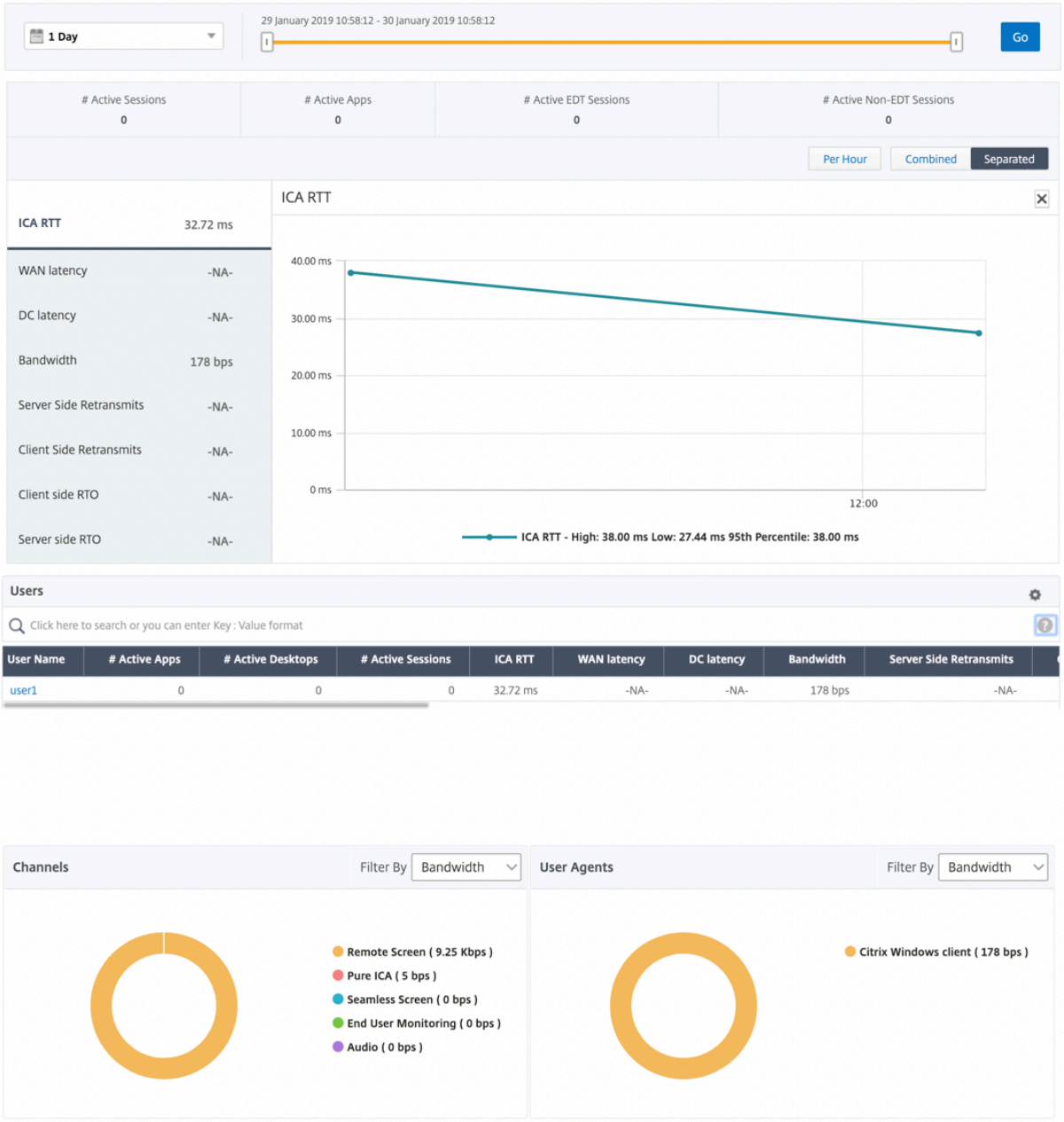
Metrics	Description
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.

Support for EDT in HDX insight

NetScaler Console now supports enlightened data transport (EDT) for displaying analytics for HDX Insight. That is, NetScaler Console now supports both UDP and TCP protocol. EDT support for NetScaler Gateway ensures a high definition in-session user experience of virtual desktops for users running Citrix Workspace.

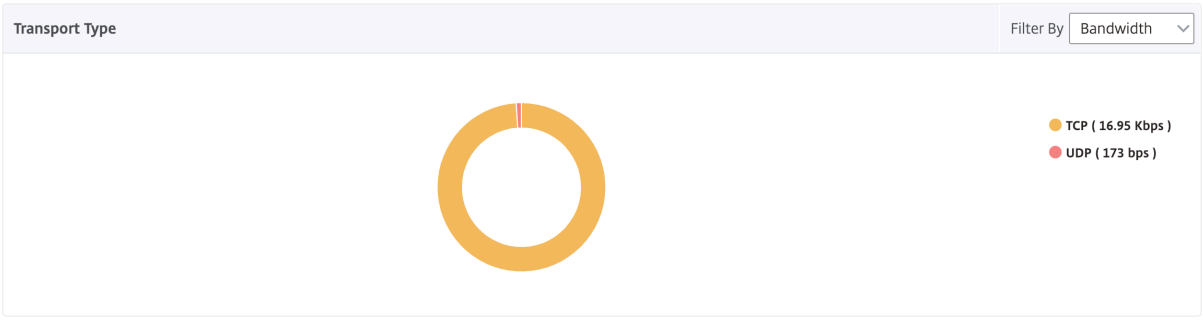
HDX Insight now displays the number of EDT sessions and non-EDT sessions as part of the active sessions report. The Users table displays a detailed report of all the users in the system. The table shows metrics such as WAN latency, DC latency, retransmits, RTOs and some of these metrics are not available for users who do have EDT sessions as they are calculated from the TCP stack currently. Therefore, they appear as "NA".

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



A new donut chart has been introduced to allow you to see bandwidth consumed by the user and also the total number of bytes based on the type of protocol used by the users.

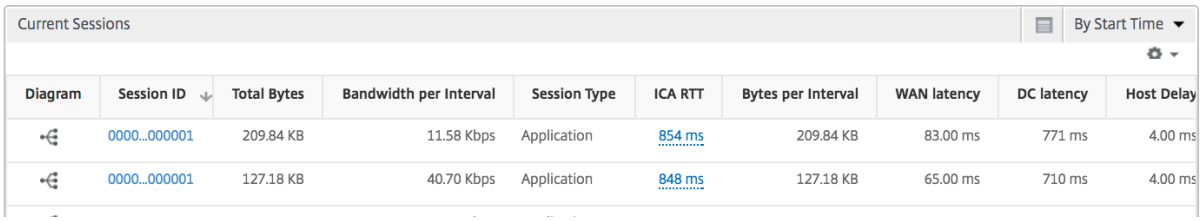
© 1997–2025 Citrix Systems, Inc. All rights reserved.



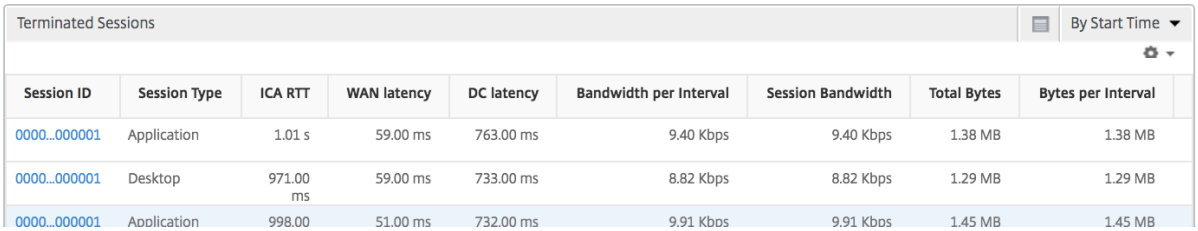
> **Note**
>
> EDT in HDX Insight is supported on NetScaler Console from release 12.1 build 50.28 and is available on ADC instances from release 12.1 build 49.23.

HDX Insight metrics available from NetScaler Console 12.0 and later:

L7 Client-side Latency	The average L7 latency observed between the ICA client and the NetScaler instance. This metric is useful in case of non-Citrix devices being present in the delivery path.
L7 Server-side Latency	The average L7 latency observed between the NetScaler device and the Citrix Virtual App. This metric is useful in case of non-Citrix devices being present in the delivery path.
Maximum Breach Latency	The highest value of the L7 latency when a breach of a defined threshold for a set time interval occurs.
Average Breach Latency	The average value of L7 latency when the system is in a “L7 latency breached”state.
L7 Threshold Breach Count	The number of times a L7 threshold breach has occurred.

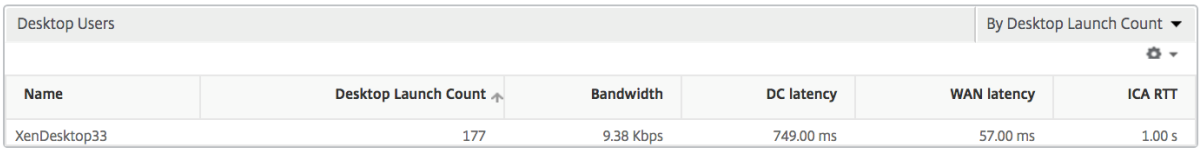


© 1997–2025 Citrix Systems, Inc. All rights reserved.



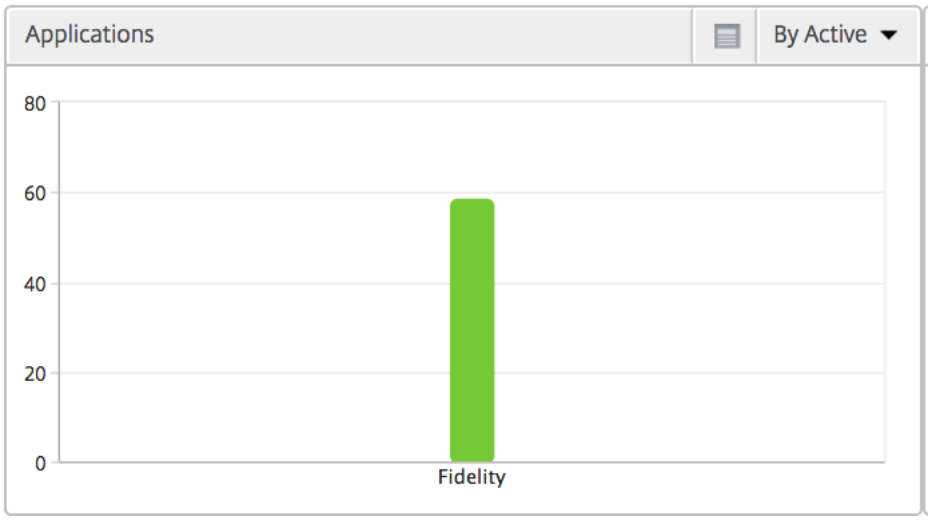
Desktop users This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

Metrics	Description
Name	Name of the Citrix Virtual Desktop.
Desktop Launch Count	Number of times the desktop has launched.
Bandwidth	Total bytes per second taken for end-to-end communication during the selected time interval.
DC latency	Latency caused by the server side of the network. between NetScaler Gateway and VDI or CVAD or StoreFront servers.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.

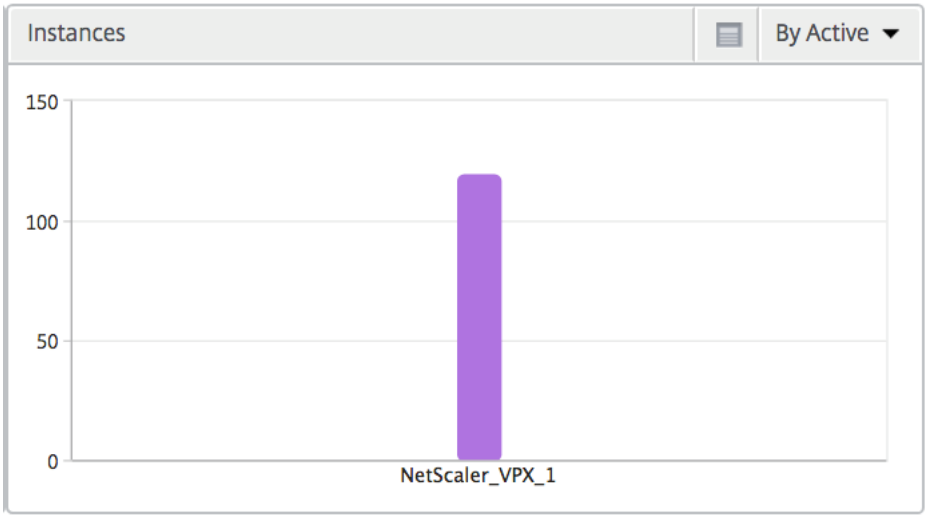


Applications A bar graph representing apps sorted by Active, total session launch count, total app launch count, and launch duration.

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

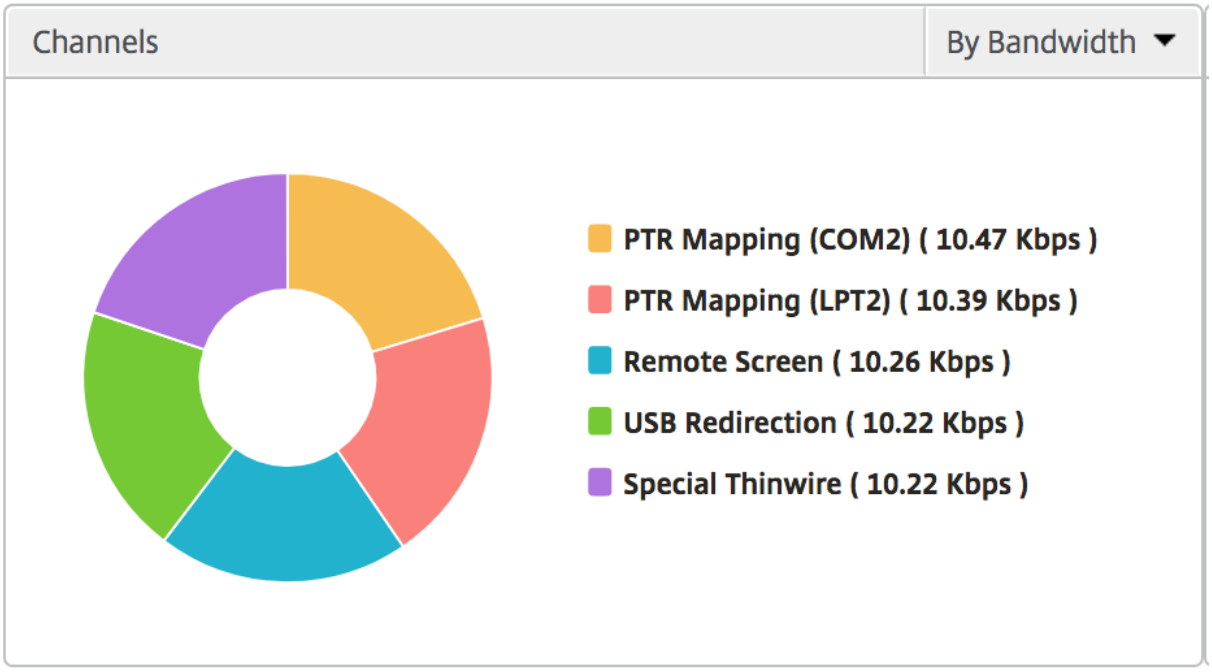


Instances A bar graph representing NetScaler instances sorted by Active and total apps

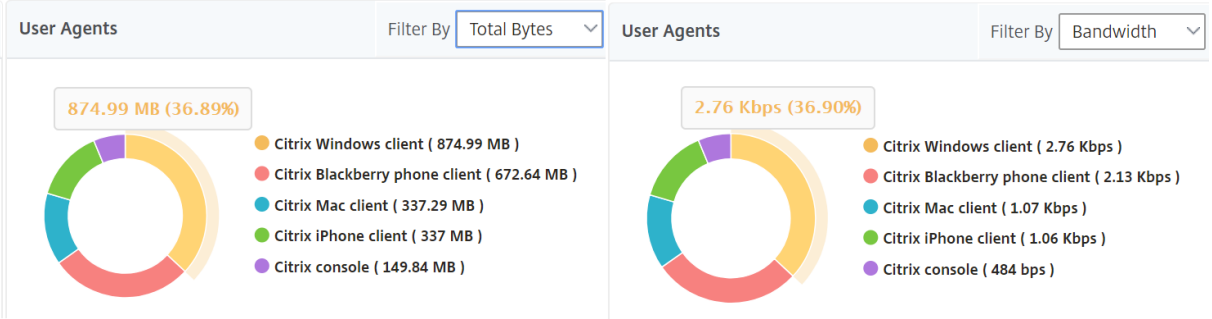


Channels Channels represent the overall bandwidth or the total bytes consumed by each ICA virtual channel in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.

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



User agents User Agents represent the overall bandwidth/total bytes consumed by each end point in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.



Per User session view The per user session view provides reporting for a particular selected user's session.

To view the metrics for a selected user's session:

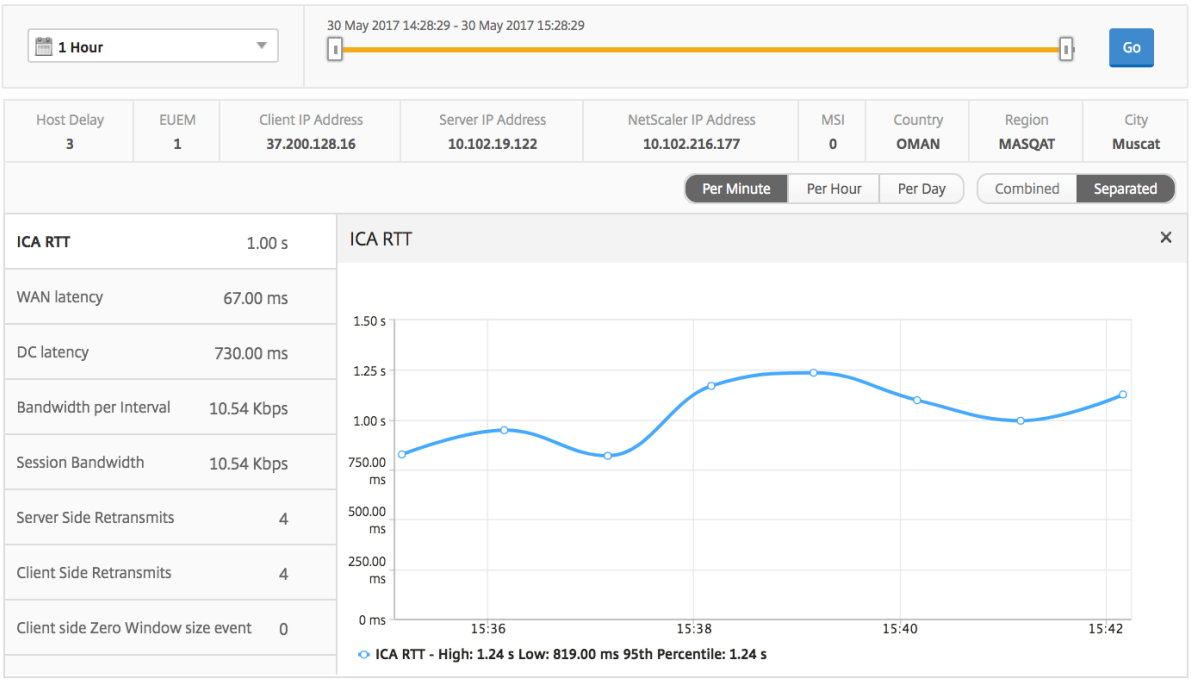
1. Navigate to **Gateway > HDX Insight > Users**.
2. Select a particular user from the **User Summary Report** section.
3. Select a session from **Current Sessions** or **Terminated Sessions** column.

Timeline chart

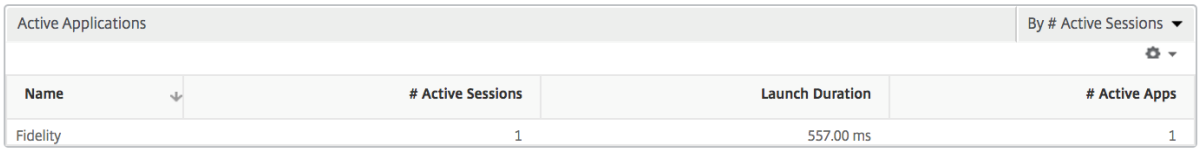
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Metrics	Description
Session Reconnects	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
ACR Counts	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps or Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.

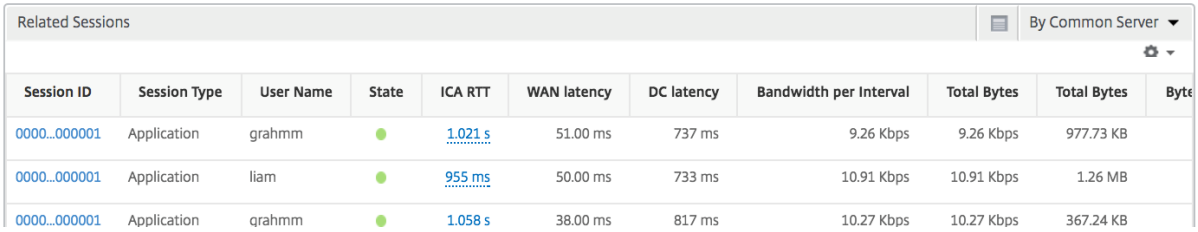
© 1997–2025 Citrix Systems, Inc. All rights reserved.



Active application The **Active Applications** section displays the active applications of the selected user. These applications can also be sorted by number of active sessions and launch durations.



Related sessions The related Sessions section displays the related sessions of the selected user's sessions. The relationship can be selected as common servers or common NetScaler.



Application view reports and metrics

The reports and metrics in this view are focused on the Citrix Virtual Apps.

To navigate to the Application view:

1. Navigate to **Gateway > HDX Insight > Applications**.

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

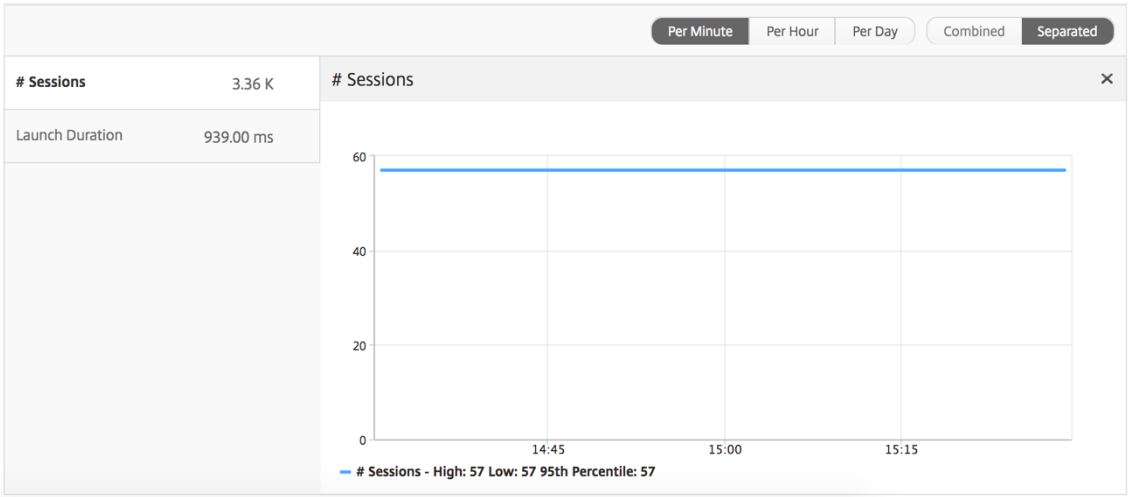
Summary view

The summary view displays the reports for all the applications that are logged in during the selected timeline.

All the metrics/reports, unless explicitly mentioned will have the values corresponding to them for the select time period.

Line chart

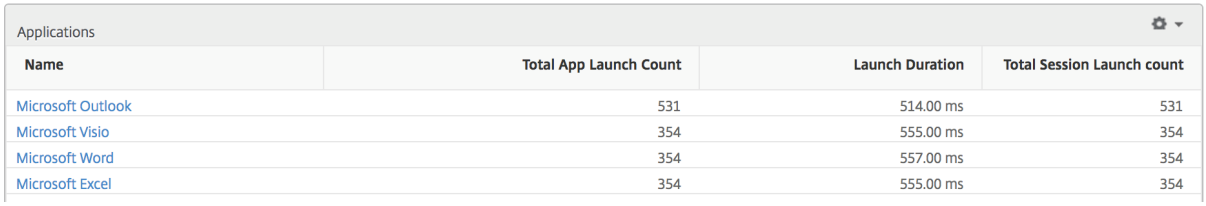
Metrics	Description
Sessions	Total number of sessions during a given time interval.
Launch duration	Average time taken to launch an application.



Applications summary report

Metrics	Description
Name	Name of the Citrix Virtual App.
Total Session Launch count	Total number of active Citrix Virtual App sessions during the given time interval.
Total App Launch Count	Total number of Citrix Virtual App applications launched during the given time interval.
Launch Duration	Average time taken to launch the Citrix Virtual App.

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

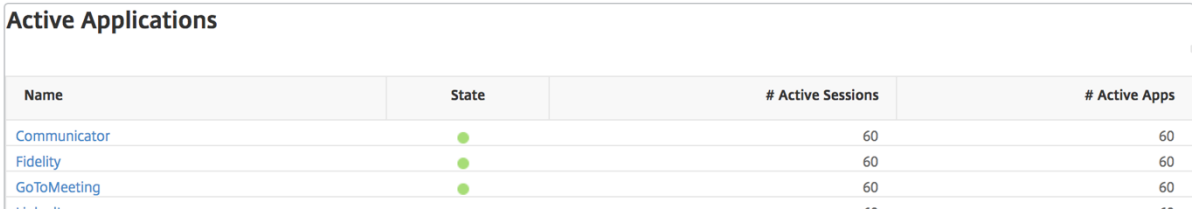


Applications

Name	Total App Launch Count	Launch Duration	Total Session Launch count
Microsoft Outlook	531	514.00 ms	531
Microsoft Visio	354	555.00 ms	354
Microsoft Word	354	557.00 ms	354
Microsoft Excel	354	555.00 ms	354

Active application report

Metrics	Description
Name	Name of the Citrix Virtual App.
State	Displays the state of the application: Green-Active, Red-Inactive
#Active Sessions	Number of active user sessions using this app during a given time interval.
#Active Apps	Number of active sessions for this application.



Active Applications

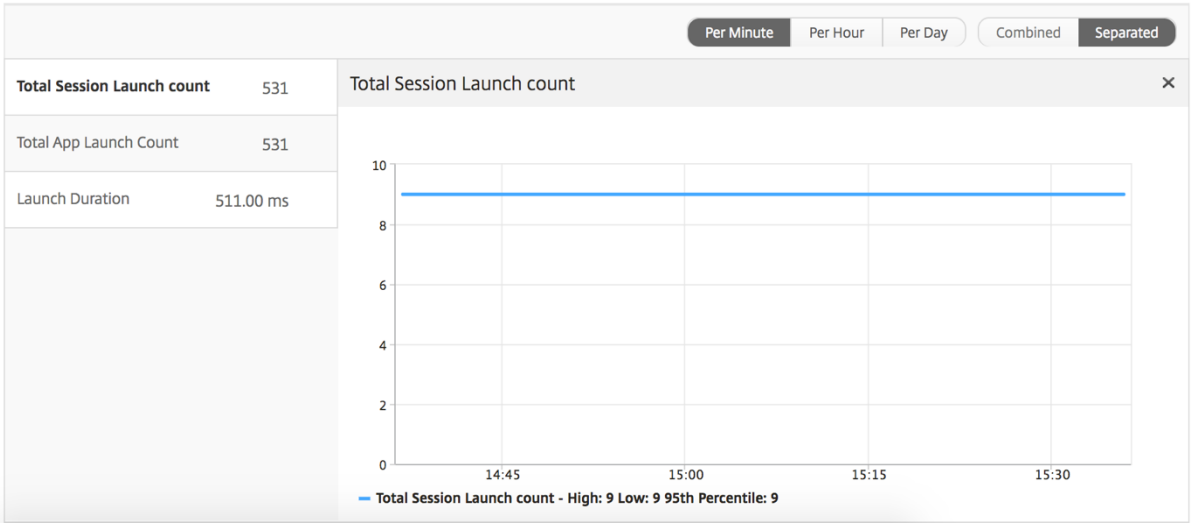
Name	State	# Active Sessions	# Active Apps
Communicator		60	60
Fidelity		60	60
GoToMeeting		60	60

Threshold report The Threshold Report represents the count of thresholds breached where the *entity* is selected as Application in the selected period. For more information, see how to create thresholds.

Line chart

Metrics	Description
Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
Launch duration	Average time taken to launch an application.

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



Current sessions report

Metrics	Description
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScalers caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.
Server IP Address	Backend/ Citrix Virtual App server IP.
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Workspace type- Citrix Windows Client and so on
Client Version	Workspace version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.

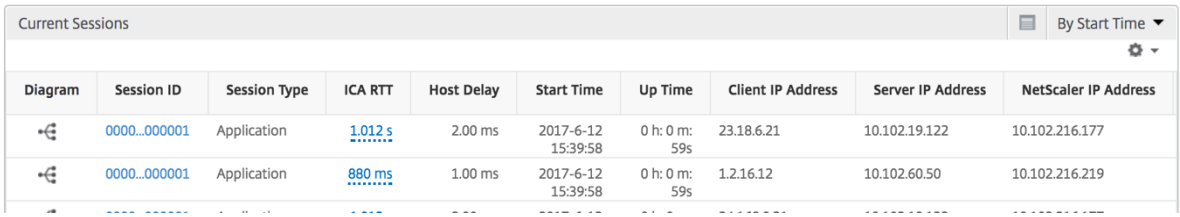
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Metrics	Description
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.
Country	Country from which the session was established.
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps or Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.

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

Metrics	Description
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
User Name	The user name of the user accessing this particular Citrix Virtual App.
Session ID	Unique identifier for the Citrix Virtual App session.
Session Type	Will be “Application”.
State	Session state: Green for active, Red for in-active.
Maximum Breach Latency	The highest value of the L7 latency when a breach of a defined threshold for a set time interval occurs.
Average Breach Latency	The average value of L7 latency when the system is in a “L7 latency breached”state.
L7 Threshold Breach Count	The number of times a L7 threshold breach has occurred.
L7 Client-side Latency	The average L7 latency observed between the ICA client and the NetScaler instance. This metric is useful in case of non-Citrix devices being present in the delivery path.
L7 Server-side Latency	The average L7 latency observed between the NetScaler device and the Citrix Virtual App. This metric is useful in case of non-Citrix devices being present in the delivery path.

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



Per application session view

The per application session view displays reports for a particular selected application session.

To view the Session reports:

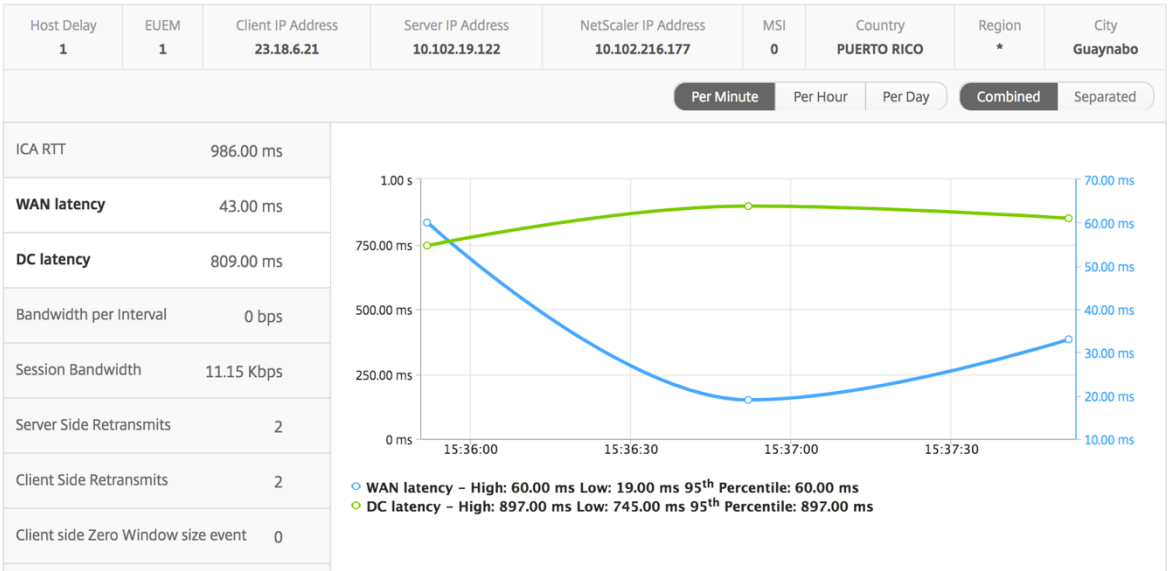
1. Log on to your NetScaler Console using a supported web browser.
2. Navigate to **Gateway > HDX Insight > Applications**.
3. Select a particular user from the Application Summary Report.
4. Selected a session from current sessions report.

Line chart

Metrics	Description
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
Server side Zero Window size event	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.

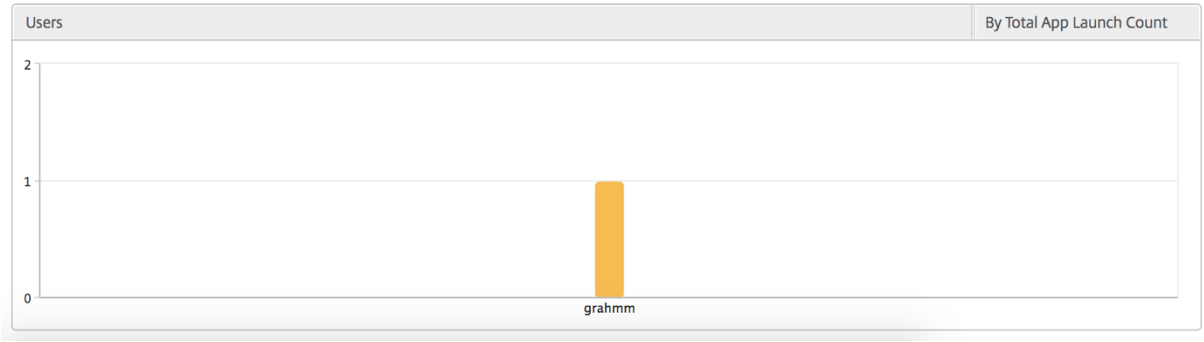
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Metrics	Description
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.



User bar graph The User's bar graph represents the users logged into this particular app.

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



Desktop view reports and metrics

The reports and metrics in this view are focused on the Citrix Virtual Desktops.

To navigate to the Desktop view:

1. Log on to your NetScaler Console using a supported web browser.
2. Navigate to **Gateway > HDX Insight > Desktop**.

Summary view

The summary view displays the reports for all the Citrix Virtual Desktops that are logged in during the selected timeline.

All the metrics/reports, unless explicitly mentioned will have the values corresponding to them for the select time period.

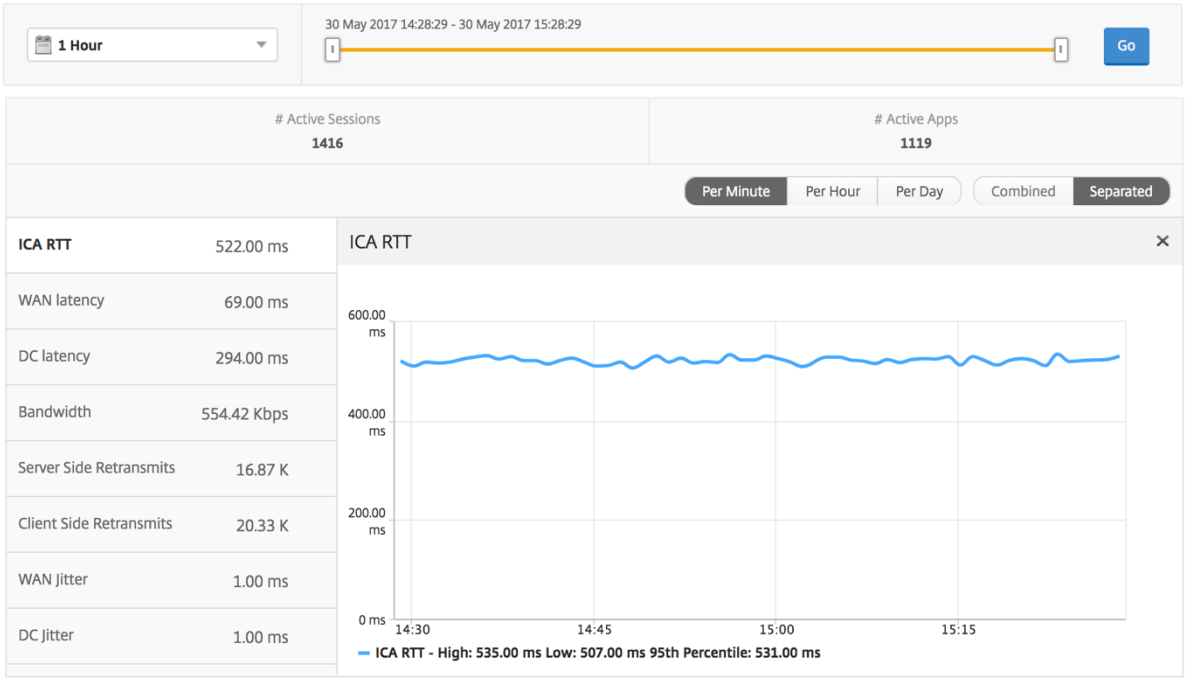
Line chart

Metrics	Description
Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.

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

Metrics	Description
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Bandwidth	Total bytes per second taken for end-to-end communication during the selected time interval.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.

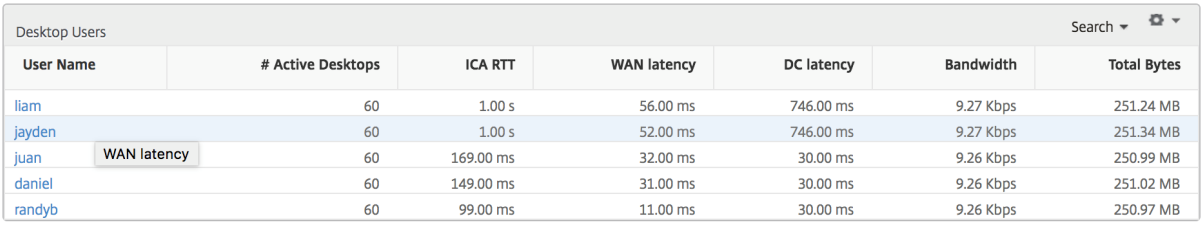
© 1997–2025 Citrix Systems, Inc. All rights reserved.



Desktop summary report

Metrics	Description
Active Sessions	Total number of active Citrix Virtual Desktop sessions during a given time interval.
Active Desktops	Total number of active Citrix Virtual Desktops during a given time interval.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Bandwidth	Total bytes per second taken for end-to-end communication during the selected time interval.
Total Bytes	Total Bytes consumed by the user during the selected time period.

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



Threshold report The threshold report represents the count of thresholds breached where the *entity* is selected as Desktop in the selected period. For more information, see how to create thresholds.

Per Desktop view

Per desktop view provides detailed end user experience reporting for a selected Citrix Virtual Desktop.

To navigate to the particular Desktop view:

1. Log on to your NetScaler Console using a supported web browser.
2. Navigate to **Analytics > HDX Insight > Desktop**.
3. Select a particular **Desktop** from the **Desktop Summary Report**.

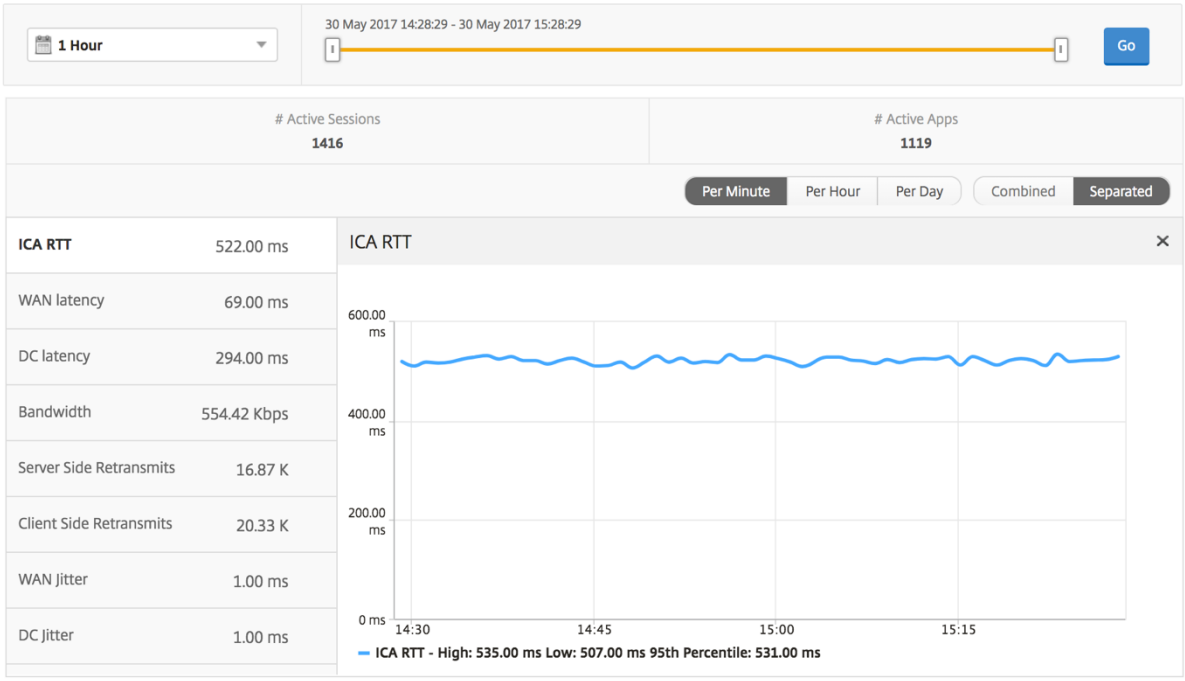
Line chart

Metrics	Description
Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.

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

Metrics	Description
Bandwidth	Total bytes per second taken for end-to-end communication during the selected time interval.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.

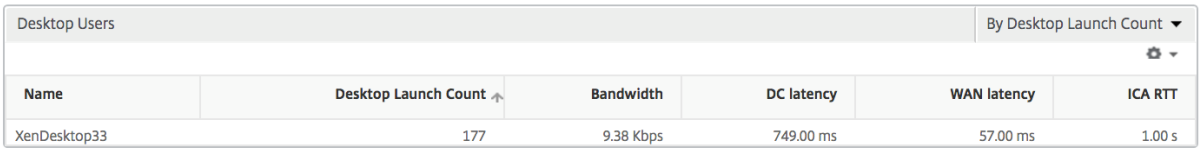
© 1997–2025 Citrix Systems, Inc. All rights reserved.



Desktop Users report This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

Metrics	Description
Name	Name of the Citrix Virtual Desktop.
Desktop Launch Count	Number of times the desktop has launched.
Bandwidth	Total bytes per second taken for end-to-end communication during the selected time interval.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.

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



User Desktops Active/Inactive report These following metrics can be sorted by Bandwidth per interval, session reconnects, and ACR counts.

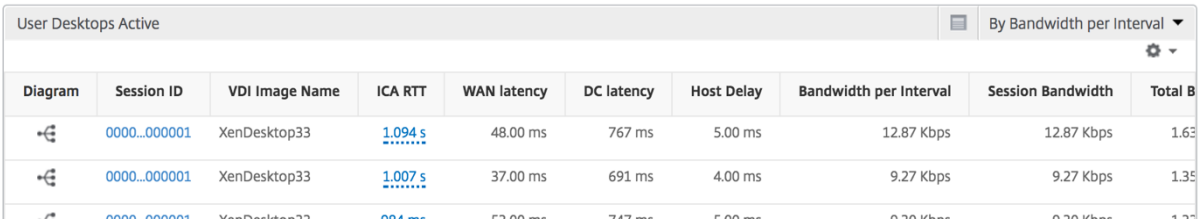
Metrics	Description
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScalers caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.
Server IP Address	Backend/ Citrix Virtual App server IP.
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Workspace type- Citrix Windows Client and so on
Client Version	Workspace version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.

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

Metrics	Description
Country	Country from which the session was established.
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.

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

Metrics	Description
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
VDI Image Name	Name of the Citrix Virtual Desktop to which the user is connected
Diagram	



Per Desktop session view

Per desktop session view provides reporting for a particular selected Citrix Virtual Desktop session.

To navigate to the Desktop session view:

1. Log on to your NetScaler Console using a supported web browser.
2. Navigate to **Analytics > HDX Insight > Desktop**.
3. Select a particular desktop from the **Desktop Summary Report**.
4. Select a session from current sessions report.

Timeline chart The per user session view provides reporting for a particular selected user's session.

To view the metrics for a selected user's session:

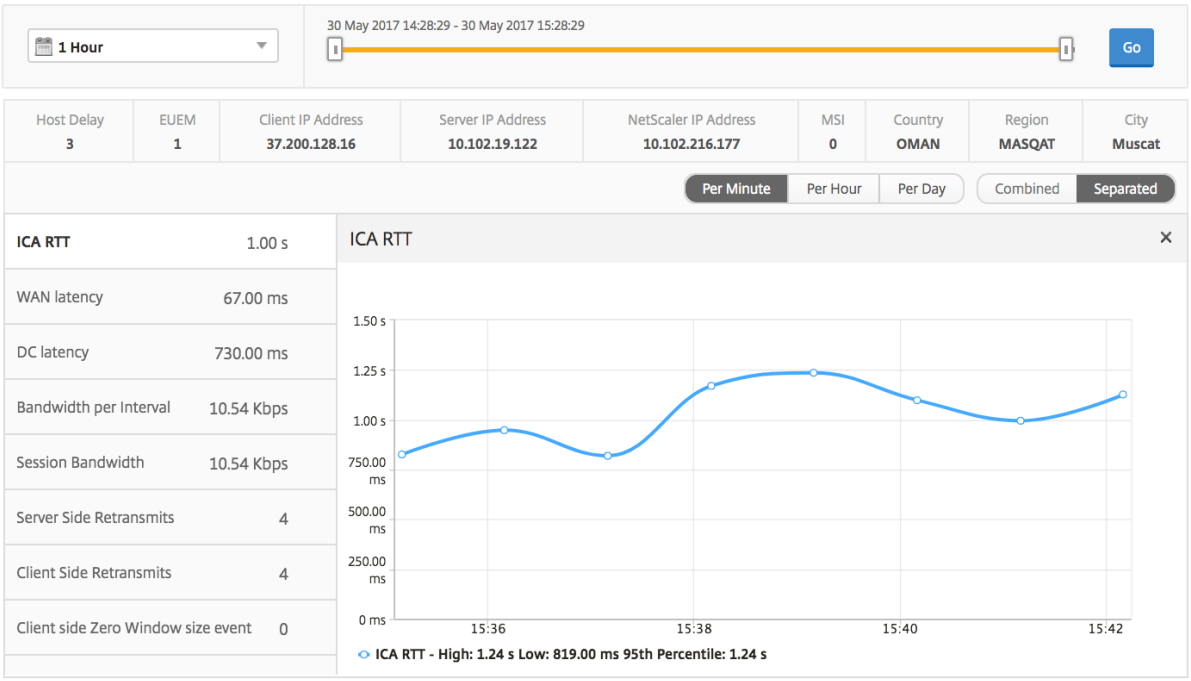
1. Log on to your NetScaler Console using a supported web browser.
2. Navigate to **Gateway > HDX Insight > Users**.
3. Select a particular user from the **User Summary Report** section.

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

4. Select a session from **Current Sessions** or **Terminated Sessions** column.

Metrics	Description
Session Reconnects	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
ACR Counts	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.

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



Related Desktop sessions report These following metrics can be sorted by Bandwidth per interval, session reconnects, and ACR counts.

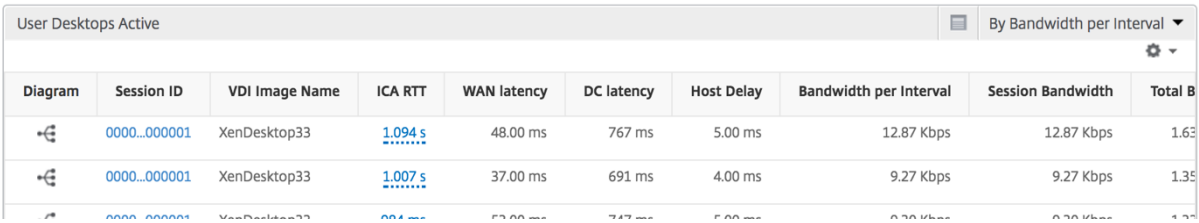
Metrics	Description
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScalers caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.
Server IP Address	Backend/ Citrix Virtual App server IP.

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

Metrics	Description
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Workspace type- Citrix Windows Client and so on
Client Version	Workspace version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.
Country	Country from which the session was established.
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
Total Bytes	Total Bytes consumed by the user during the selected time period.

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

Metrics	Description
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.



Instance view reports and metrics

The reports and metrics in the instance view are focused on the NetScaler instances.

To navigate to the Instance view:

1. Log on to your NetScaler Console using a supported web browser.
2. Navigate to **Analytics > HDX Insight > Instances**.

Instance view reports and metrics consist of the following sections:

- Instance Summary View
- Per Instance View

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

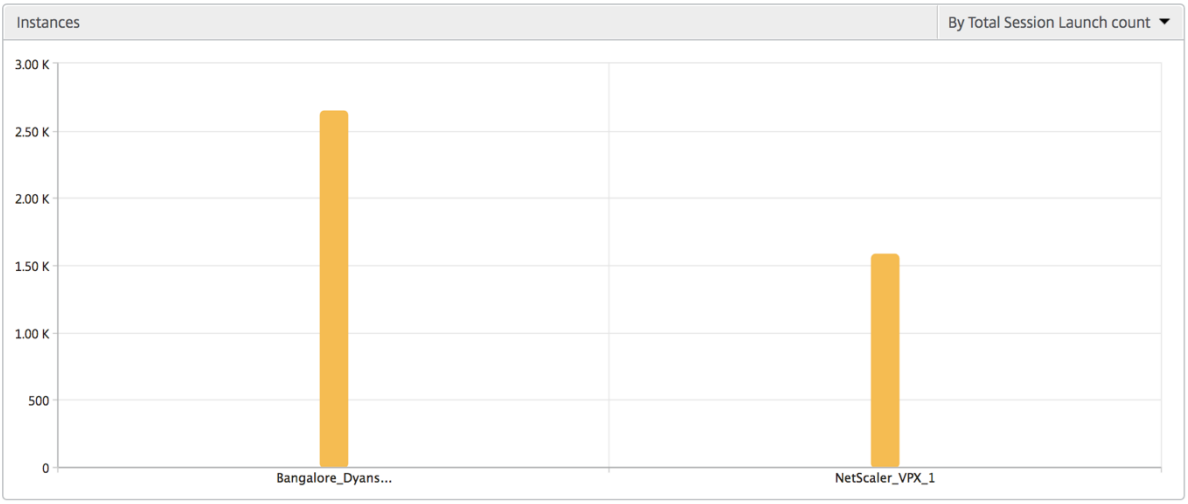
Instance summary view

This view is called the summary view as it shows the reports for all the NetScaler instances that are added to NetScaler Console.

All the below metrics/reports, unless explicitly mentioned will have the values corresponding to them for the selected time period.

Instance bar graph

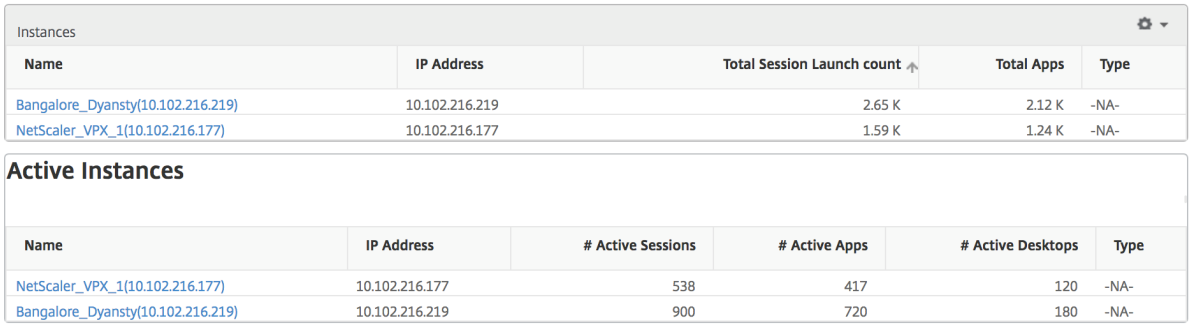
This graph displays the instance vs the Total Session Launch count	Total Apps which can be selected from the list on the top right on the graph canvas.



Instance/Active instances summary report

Metrics	Description
Name	Host name of the NetScaler instance.
IP Address	NetScaler IP address.
Total Session Launch count	Total number of unique user sessions created during a given time interval.
Total Apps	Total number of unique applications launched during a given time interval.
Type	N/A

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



Instances

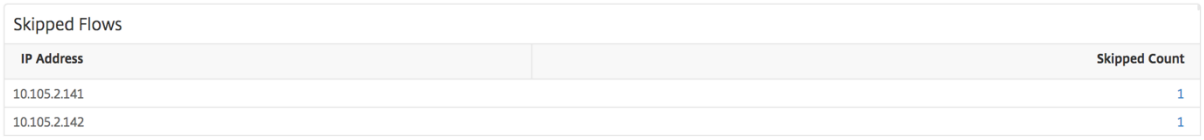
Name	IP Address	Total Session Launch count	Total Apps	Type
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	2.65 K	2.12 K	-NA-
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	1.59 K	1.24 K	-NA-

Active Instances

Name	IP Address	# Active Sessions	# Active Apps	# Active Desktops	Type
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	538	417	120	-NA-
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	900	720	180	-NA-

Threshold report Threshold report represents the count of thresholds breached where the *entity* is selected as Instance in the selected period. For more information, see how to create thresholds.

Skipped flows A skipped flow is a record which skipped parsing ICA connection. This can occur due to multiple reasons like using unsupported Citrix Virtual Apps and Desktops versions, unsupported version of workspace or workspace type and so on This table shows the IP address and the skipped flow count. These workspaces may not be part of whitelisted workspaces. Hence these sessions are skipped from monitoring.



Skipped Flows

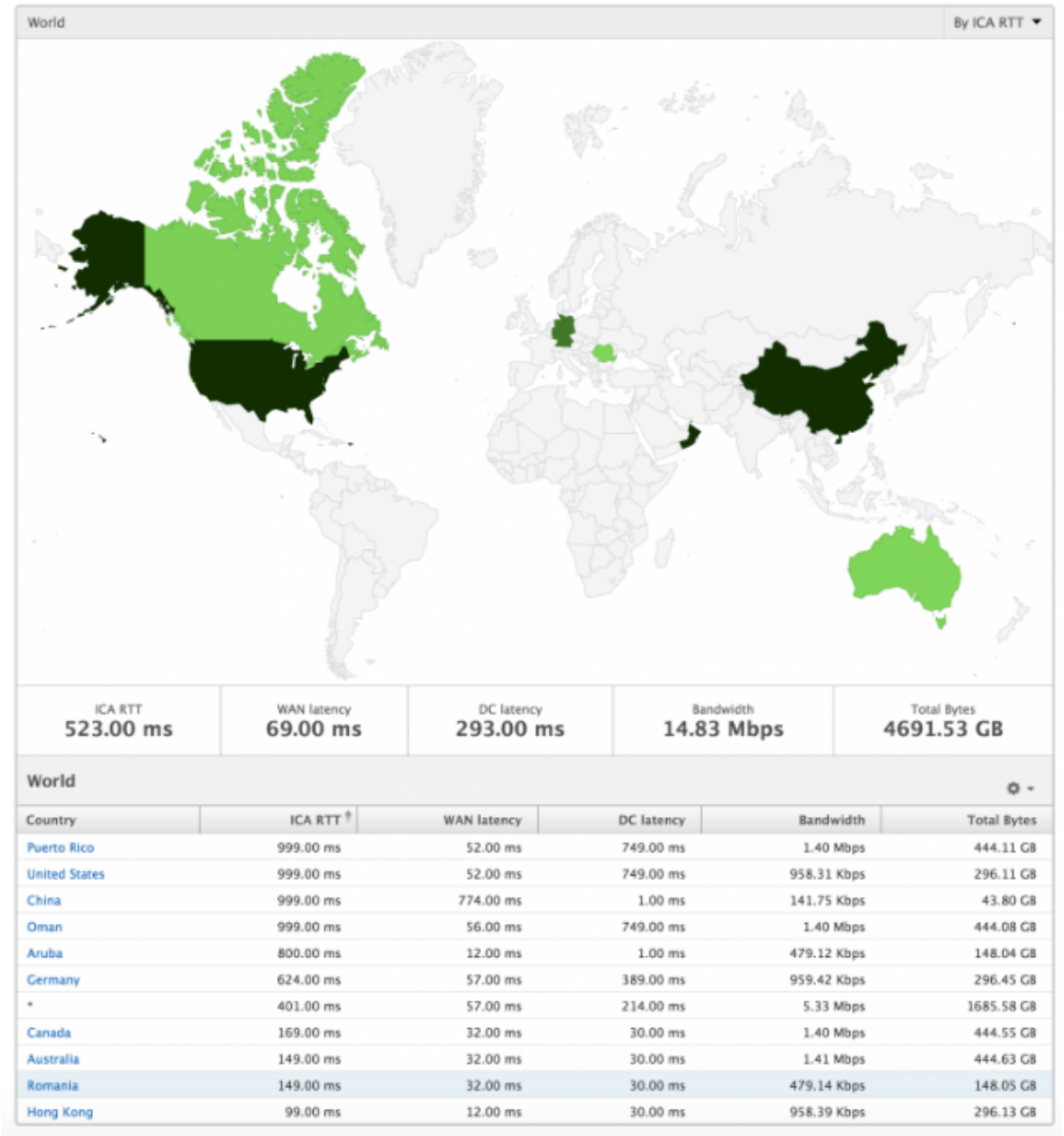
IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

World view The World Map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill-down to a particular country and further into cities as well by simply clicking the region. The administrators can further drill down to view information by city and state. From NetScaler Console version 12.0 and later, you can drill down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metric is displayed in the form of a heat map:

- ICA RTT
- WAN Latency
- DC Latency
- Bandwidth
- Total Bytes

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



Per instance view

Per instance view provides detailed end user experience reporting for a particular selected NetScaler instance.

To navigate to the instance view:

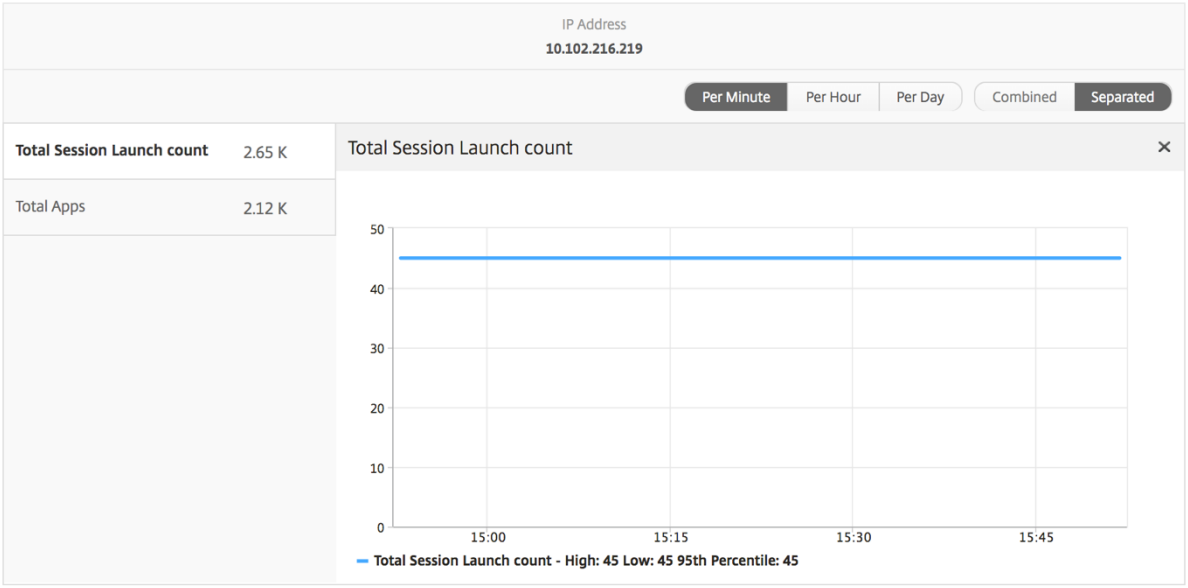
1. Log on to your NetScaler Console using a supported web browser.
2. Navigate to **Analytics > HDX Insight > Instances**.

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

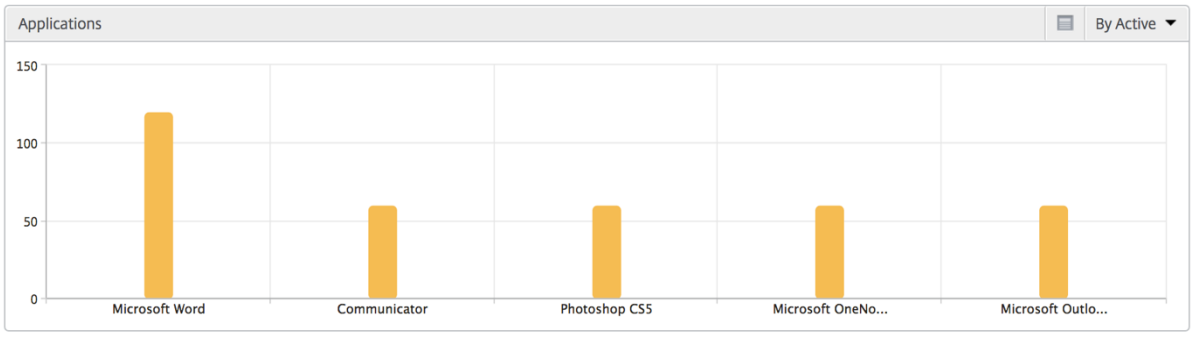
3. Select a particular instance from the **Instance Summary Report**.

Line chart

Metrics	Description
IP Address	This represents the NetScaler IP address of the selected instance.
Total session launch count	Total number of active Citrix Virtual App sessions during the given time interval.
Total Apps	Total number of unique applications launched during a given time interval.



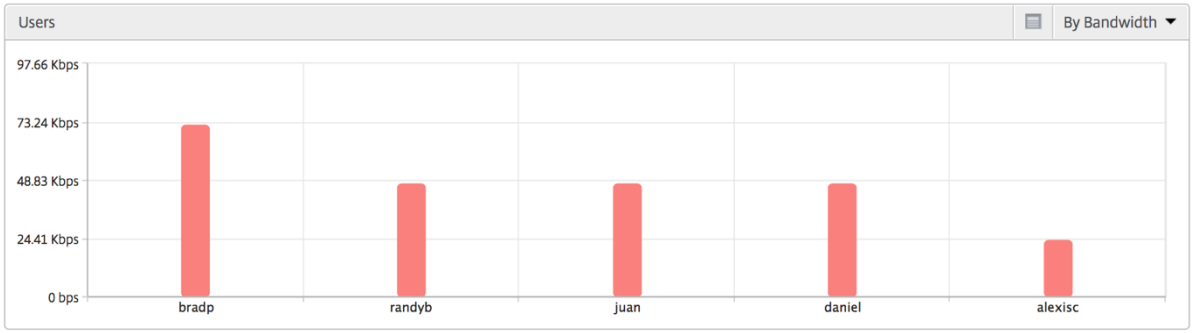
Applications bar graph Displays top 5 applications based on the following criteria- by Active apps, total session launch count, total app launch count, or launch duration.



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

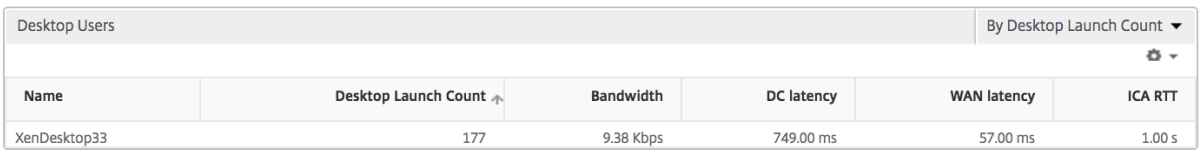
Users bar graph The Users bar graph displays top 5 users based on the following criteria

- Bandwidth
- WAN Latency
- DC Latency
- ICA RTT



Desktop Users report This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

Metrics	Description
Name	Name of the Citrix Virtual Desktop.
Desktop Launch Count	Number of times the desktop has launched.
Bandwidth	Total bytes per second taken for end-to-end communication during the selected time interval.
DC latency	Latency caused by the server side of the network. That is, between NetScaler Gateway and VDI or CVAD or StoreFront servers.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.



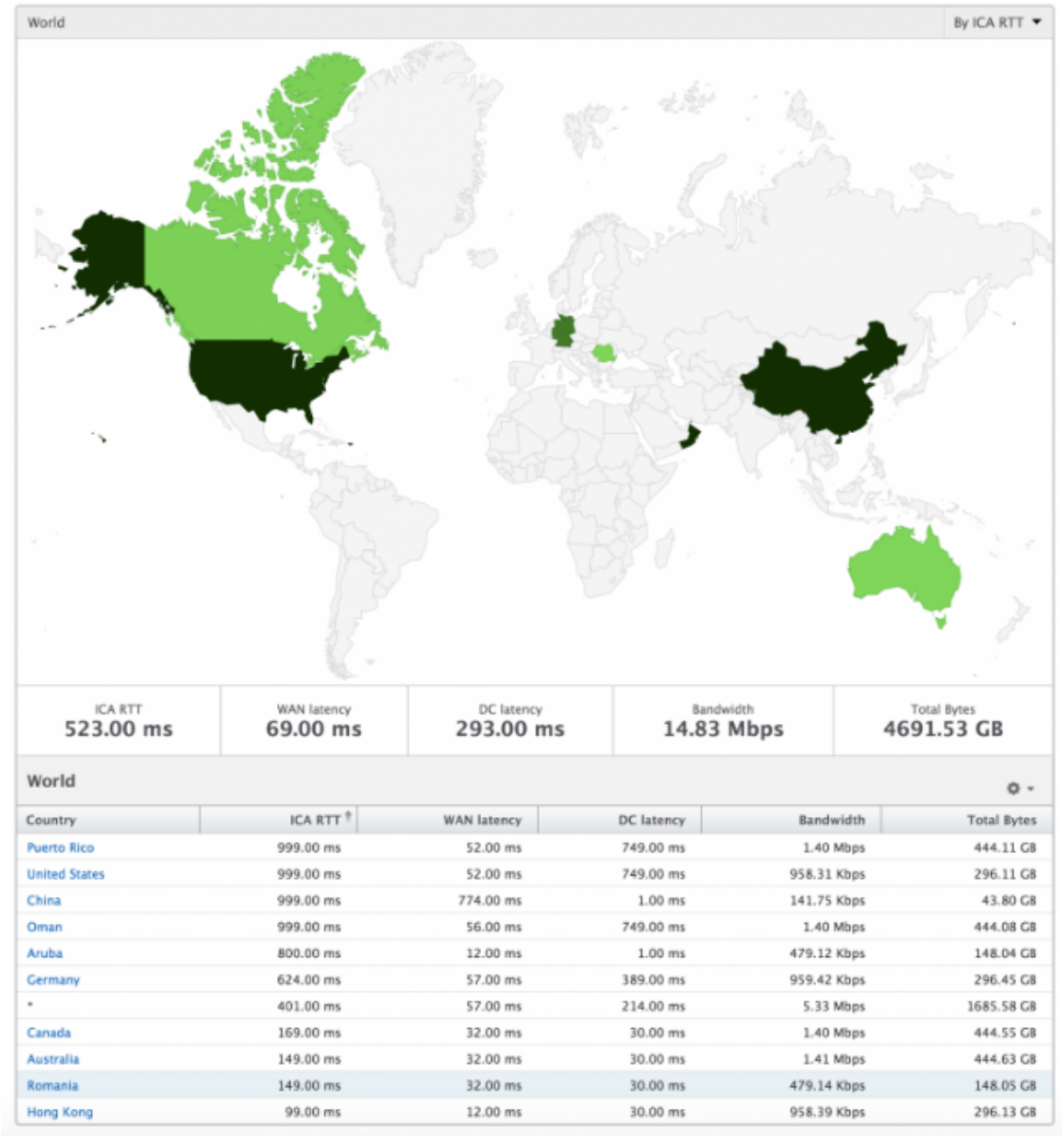
© 1997–2025 Citrix Systems, Inc. All rights reserved.

World view The World Map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill-down to a particular country and further into cities as well by clicking the region. The administrators can further drill-down to view information by city and state. From NetScaler Console version 12.0 and later, you can drill-down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metric is displayed in the form of a heat map:

- ICA RTT
- WAN Latency
- DC Latency
- Bandwidth
- Total Bytes

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



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

License view reports and metrics

The license view gives details on the NetScaler Gateway license information.

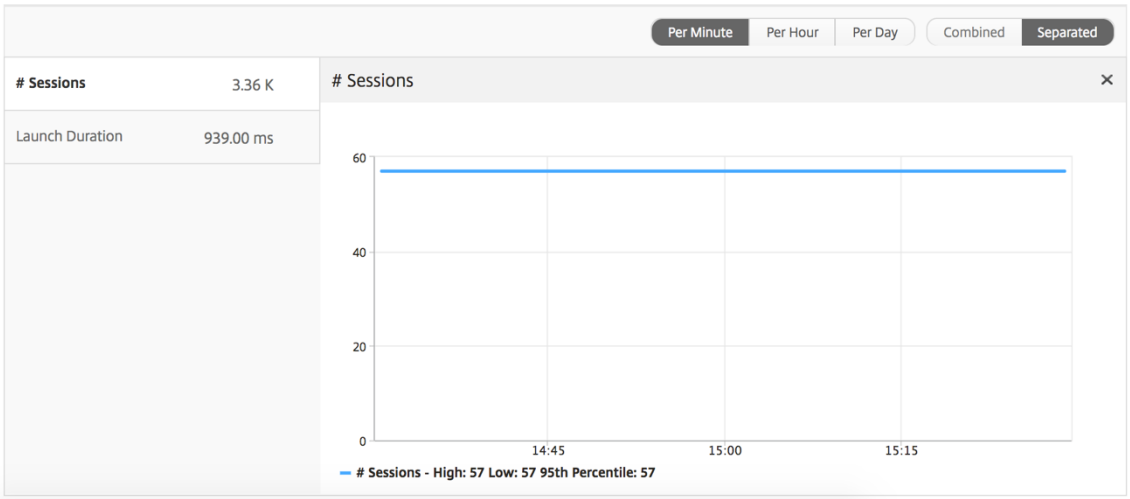
To navigate to the License view:

1. Log on to your NetScaler Console using a supported web browser.
2. Navigate to **Analytics > HDX Insight > Licenses**.

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

Line chart

Metrics	Description
Licenses in use	The NetScaler Gateway CCU licenses being used during the selected timeline. Each count represents the number of user sessions. This is independent of the application and desktop sessions launched by that user.
Total licenses	Total number of NetScaler Gateway CCU licenses available for the customer to utilize.



Threshold report The threshold report represents the count of thresholds breached where the *entity* is selected as License in the selected period. For more information, see how to create thresholds.

Application View Reports and Metrics

September 27, 2025

The reports and metrics in this view are focused on the Citrix Virtual Apps.

To navigate to the Application view:

1. Navigate to **Gateway > HDX™ Insight > Applications**.

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

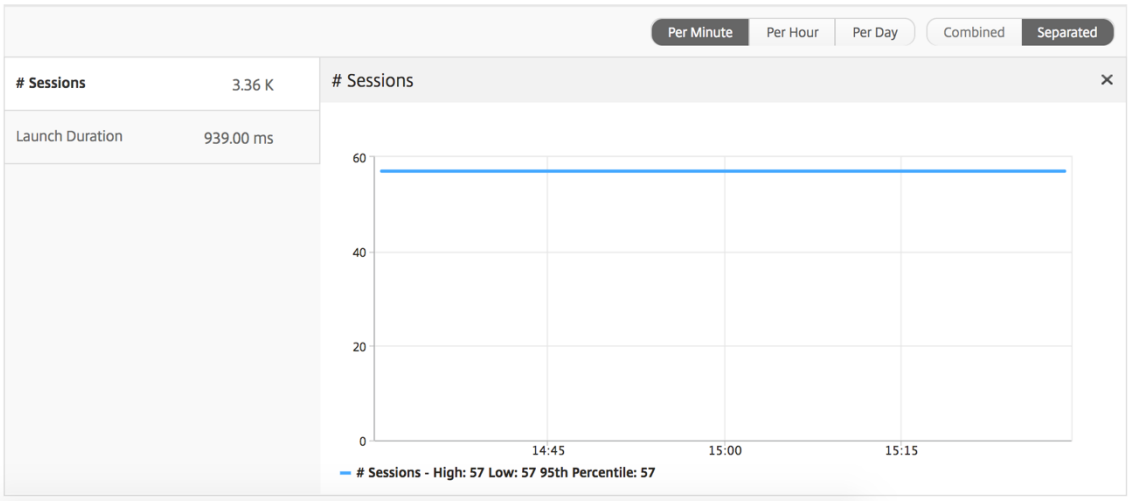
Summary view

The summary view displays the reports for all the applications that are logged in during the selected timeline.

All the below metrics/reports, unless explicitly mentioned will have the values corresponding to them for the select time period.

Line chart

Metrics	Description
Sessions	Total number of sessions during a given time interval.
Launch duration	Average time taken to launch an application.

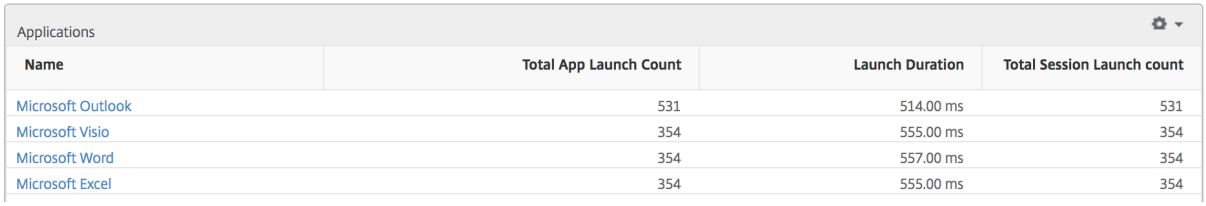


Applications summary report

Metrics	Description
Name	Name of the Citrix Virtual App.
Total Session Launch count	Total number of active Citrix Virtual App sessions during the given time interval.
Total App Launch Count	Total number of Citrix Virtual App applications launched during the given time interval.

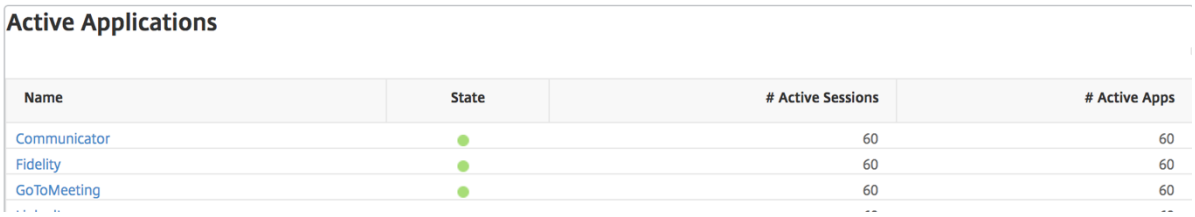
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Metrics	Description
Launch Duration	Average time taken to launch the Citrix Virtual App.



Active application report

Metrics	Description
Name	Name of the Citrix Virtual App.
State	Displays the state of the application: Green-Active, Red-Inactive
#Active Sessions	Number of active user sessions using this app during a given time interval.
#Active Apps	Number of active sessions for this application.



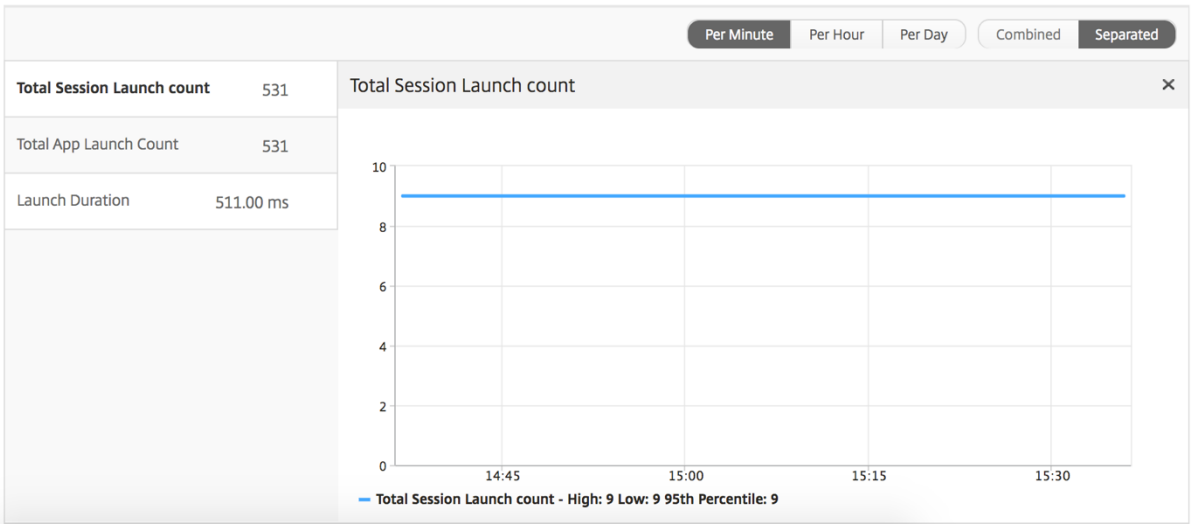
Threshold report

The Threshold Report represents the count of thresholds breached where the *entity* is selected as Application in the selected period. For more information, see how to create thresholds and alerts.

Line chart

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

Metrics	Description
Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
Launch duration	Average time taken to launch an application.



Current sessions report

Metrics	Description
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScalers caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.

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

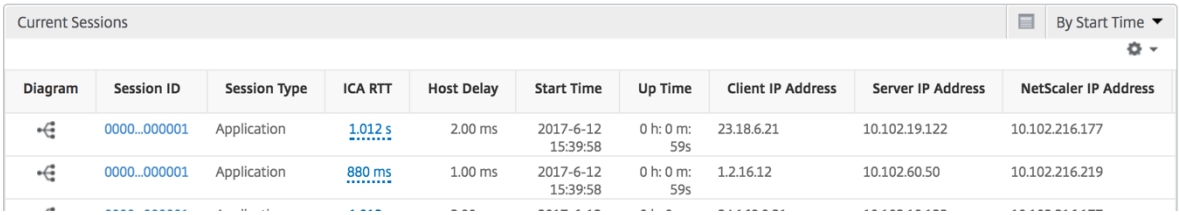
Metrics	Description
Client IP Address	End user IP.
Server IP Address	Backend/ Citrix Virtual App server IP.
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Workspace type- Citrix Windows Client and so on
Client Version	Workspace version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.
Country	Country from which the session was established.
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.

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

Metrics	Description
Total Bytes	Total Bytes consumed by the user during the selected time period.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
User Name	The user name of the user accessing this particular Citrix Virtual App.
Session ID	Unique identifier for the Citrix Virtual App session.
Session Type	Will be “Application”.
State	Session state: Green for active, Red for in-active.
Maximum Breach Latency	The highest value of the L7 latency when a breach of a defined threshold for a set time interval occurs.
Average Breach Latency	The average value of L7 latency when the system is in a “L7 latency breached”state.
L7 Threshold Breach Count	The number of times a L7 threshold breach has occurred.

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

Metrics	Description
L7 Client-side Latency	The average L7 latency observed between the ICA client and the NetScaler instance. This metric is useful in non-Citrix devices being present in the delivery path.
L7 Server-side Latency	The average L7 latency observed between the NetScaler device and the Citrix Virtual App. This metric is useful in non-Citrix devices being present in the delivery path.



Per Application session view

The per application session view displays reports for a particular selected application session.

To view the Session reports:

1. Navigate to **Gateway > HDX Insight > Applications**.
2. Select a particular user from the Application Summary Report.
3. Selected a session from current sessions report.

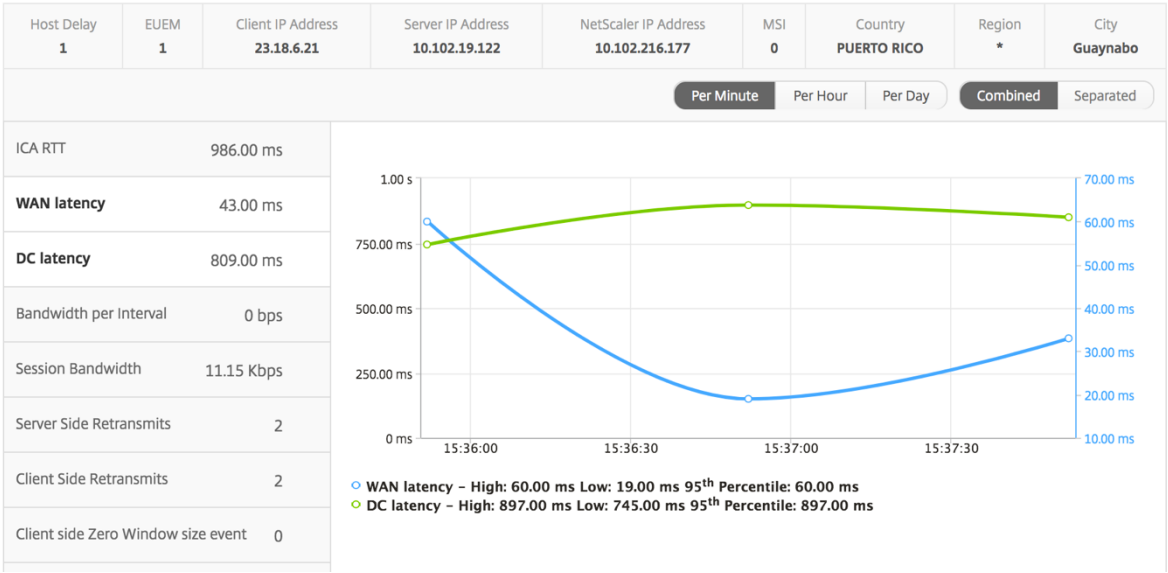
Line chart

Metrics	Description
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.

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

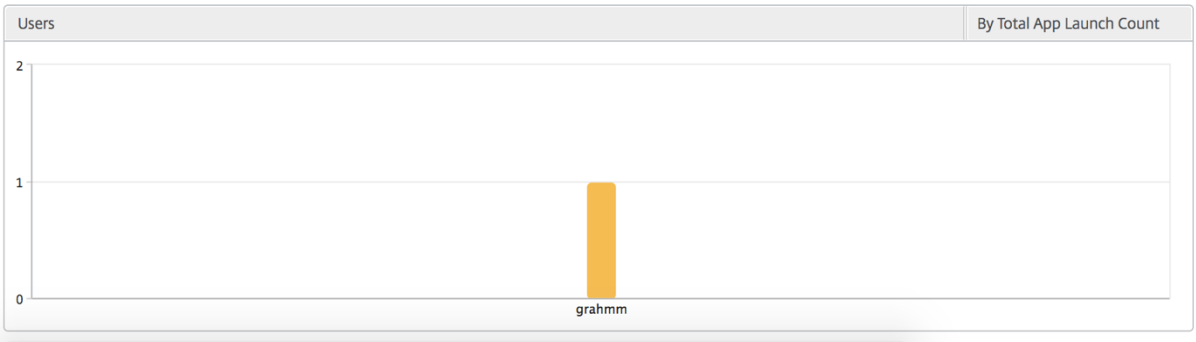
Metrics	Description
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
Server side Zero Window size event	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.

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



User bar graph

The User's bar graph represents the users logged into this particular app.



Desktop View Reports and Metrics

September 27, 2025

The reports and metrics in this view are focused on the Citrix Virtual Desktops.

To navigate to the Desktop view:

1. Navigate to **Gateway > HDX™ Insight > Desktop**.

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

Summary view

The summary view displays the reports for all the Citrix Virtual Desktops that are logged in during the selected timeline.

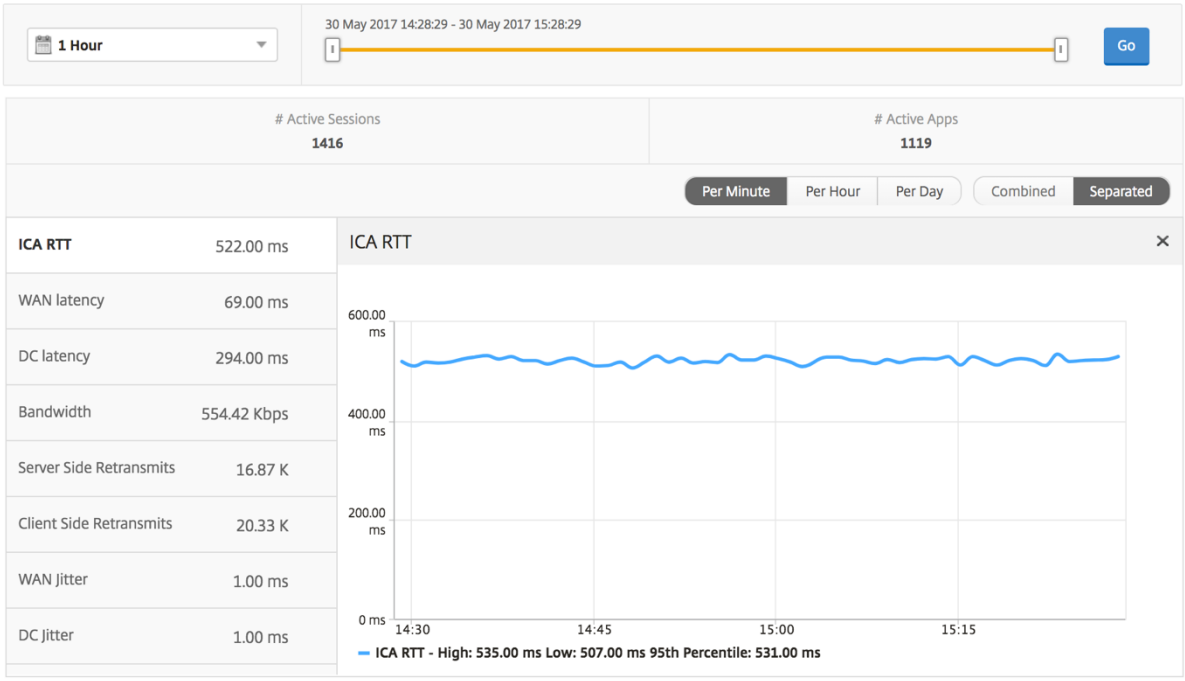
All the metrics/reports, unless explicitly mentioned will have the values corresponding to them for the select time period.

Line chart

Metrics	Description
Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.

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

Metrics	Description
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.

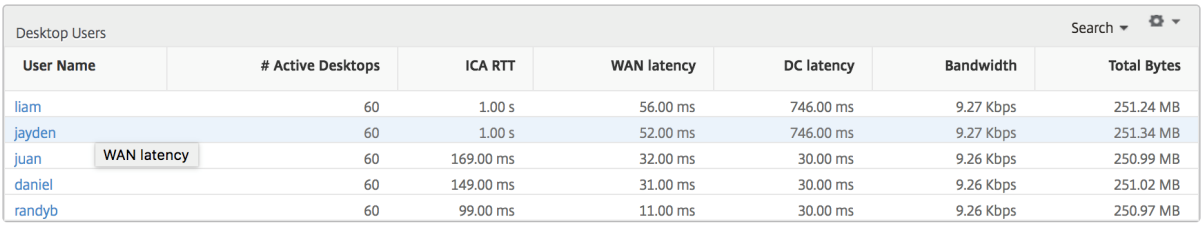


Desktop summary report

Metrics	Description
Active Sessions	Total number of active Citrix Virtual Desktop sessions during a given time interval.
Active Desktops	Total number of active Citrix Virtual Desktops during a given time interval.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.

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

Metrics	Description
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
Total Bytes	Total Bytes consumed by the user during the selected time period.



Threshold report

The threshold report represents the count of thresholds breached where the *entity* is selected as Desktop in the selected period. For more information, see how to create thresholds and alerts.

Per desktop view

Per desktop view provides detailed end user experience reporting for a selected Citrix Virtual Desktop.

To navigate to the particular Desktop view:

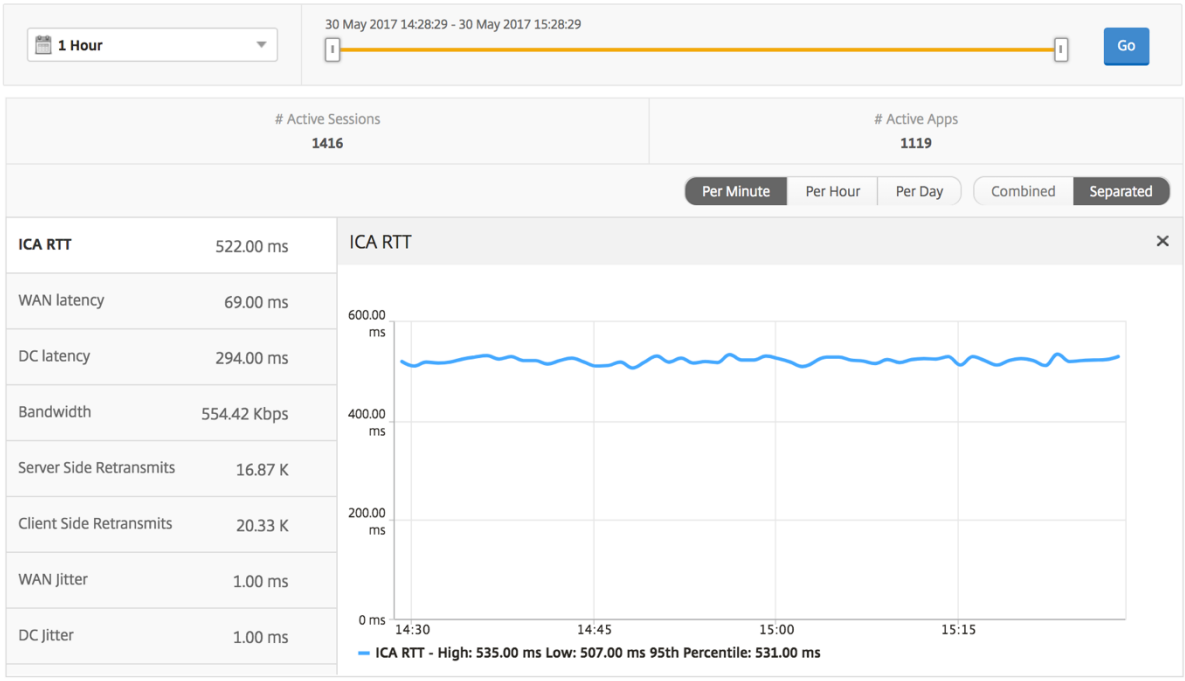
1. Navigate to **Analytics > HDX Insight > Desktop**.
2. Select a particular **Desktop** from the **Desktop Summary Report**.

Line chart

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

Metrics	Description
Active Sessions	This number indicates the count of active Citrix Virtual Apps and Desktops sessions.
Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.

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

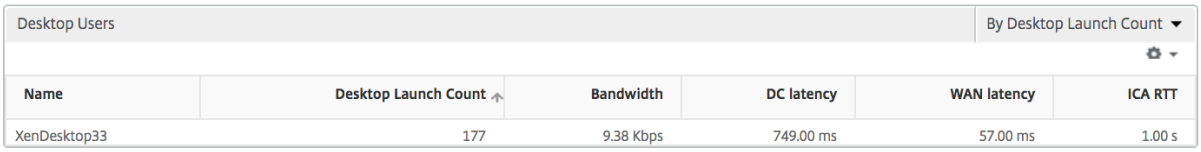


Desktop users report

This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

Metrics	Description
Name	Name of the Citrix Virtual Desktop.
Desktop Launch Count	Number of times the desktop has launched.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps and Desktops respectively.

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



User desktops active/inactive report

These following metrics can be sorted by Bandwidth per interval, session reconnects, and ACR counts.

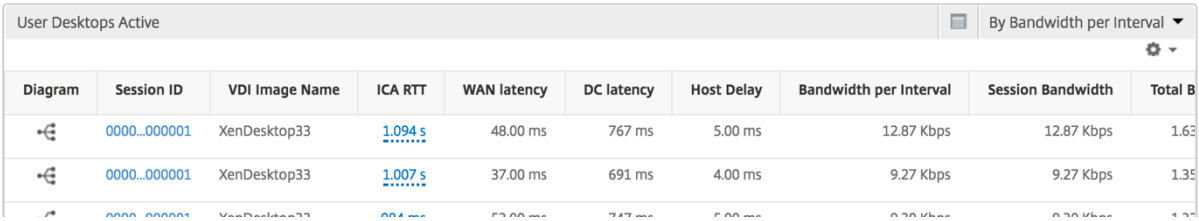
Metrics	Description
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScaler instances caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.
Server IP Address	Backend/ Citrix Virtual App server IP.
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Workspace type- Citrix Windows Client and so on
Client Version	Workspace version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.

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

Metrics	Description
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.
Country	Country from which the session was established.
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual Apps or Desktops respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.

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

Metrics	Description
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
VDI Image Name	Name of the Citrix Virtual Desktop to which the user is connected
Diagram	



Per desktop session view

Per desktop session view provides reporting for a particular selected Citrix Virtual Desktop session.

To navigate to the Desktop session view:

1. Navigate to **Gateway > HDX Insight > Desktop**.
2. Select a particular desktop from the **Desktop Summary Report**.
3. Select a session from current sessions report.

Timeline chart

The per user session view provides reporting for a particular selected user's session.

To view the metrics for a selected user's session:

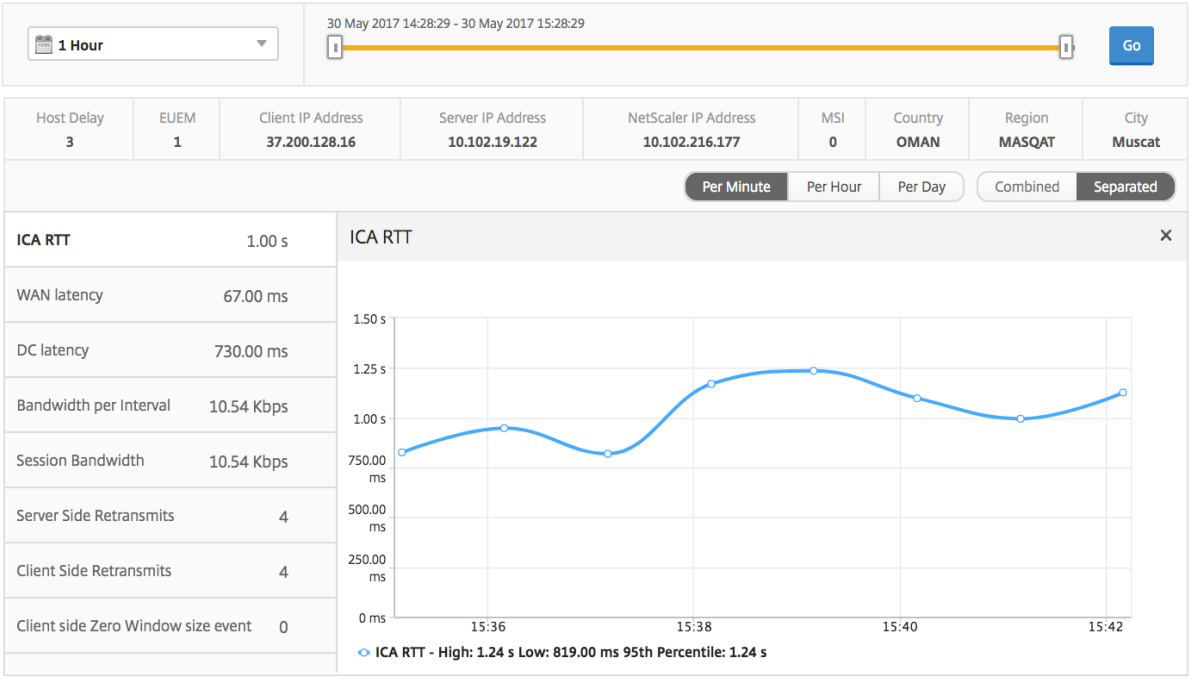
1. Navigate to **Gateway > HDX Insight > Users**.
2. Select a particular user from the **User Summary Report** section.

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

3. Select a session from **Current Sessions** or **Terminated Sessions** column.

Metrics	Description
Session Reconnects	This number indicates the count of active Citrix Virtual App and Desktop sessions.
ACR Counts	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App and Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.

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



Related desktop sessions report

These following metrics can be sorted by Bandwidth per interval, session reconnects, and ACR counts.

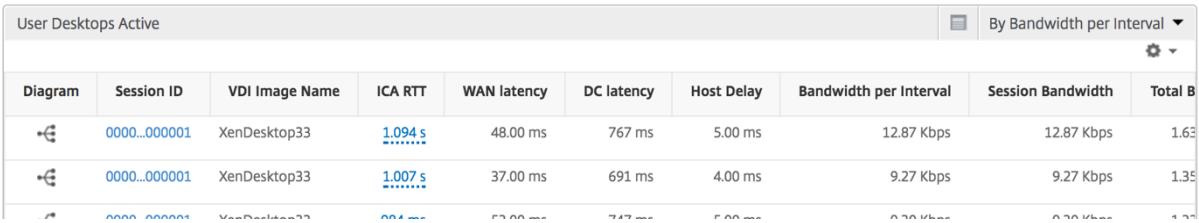
Metrics	Description
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScalers caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.

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

Metrics	Description
Server IP Address	Backend/ Citrix Virtual App server IP.
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Receiver type- Citrix Windows Client and so on
Client Version	Receiver version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.
Country	Country from which the session was established.
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.

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

Metrics	Description
Total Bytes	Total Bytes consumed by the user during the selected time period.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and back end server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and back end server.
VDI Image Name	Name of the Citrix Virtual Desktop to which the user is connected



User View Reports and Metrics

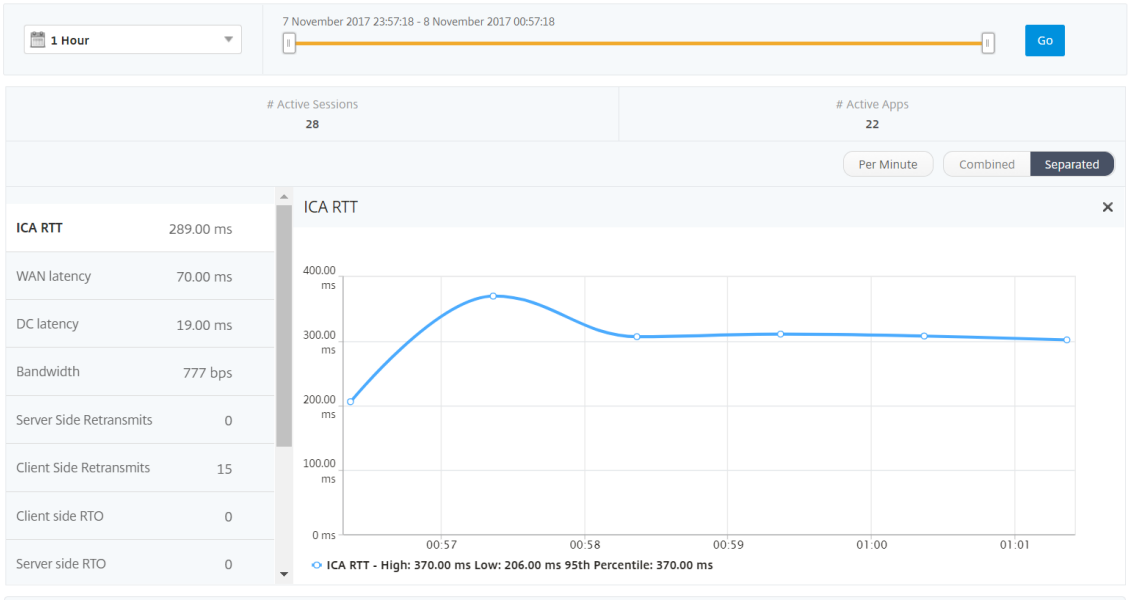
September 27, 2025

The reports and metrics in this view are displayed per Citrix Virtual Apps™ and Desktop users.

To navigate to the Users view:

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

1. Navigate to **Gateway > HDX™ Insight > Users**



Summary view

The summary view displays the reports for all the users that have logged in during the selected time-line. All the metrics/reports in this view display the values corresponding to them for the selected time period unless specified otherwise.

To change the selected time period:

1. Use the time period list or the time slider to set the desired time interval.
2. Click **Go**.

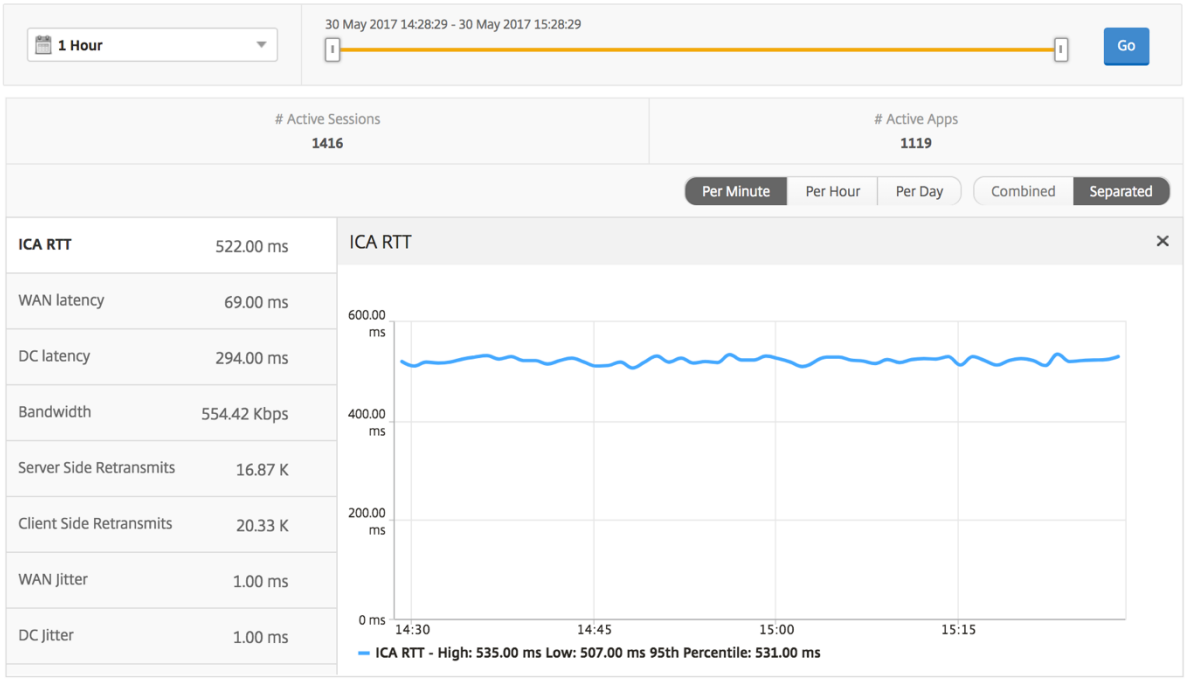
Line chart

Metrics	Description
Active Sessions	This number indicates the count of active Citrix Virtual App and Desktop sessions.
Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.

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

Metrics	Description
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to backend servers.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and backend server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and backend server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.

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



User summary report

Following are the metrics that are specific to this report.

Metrics	Description
Active Sessions	This number indicates the count of active Citrix Virtual App and Desktop sessions.
Active Apps	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to backend servers.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.

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

Metrics	Description
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and backend server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and backend server.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Total App Launch Count	Total Apps launched by the user during the selected time period.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Active Desktops	Total number of active Citrix Virtual Desktops during a given time interval.

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

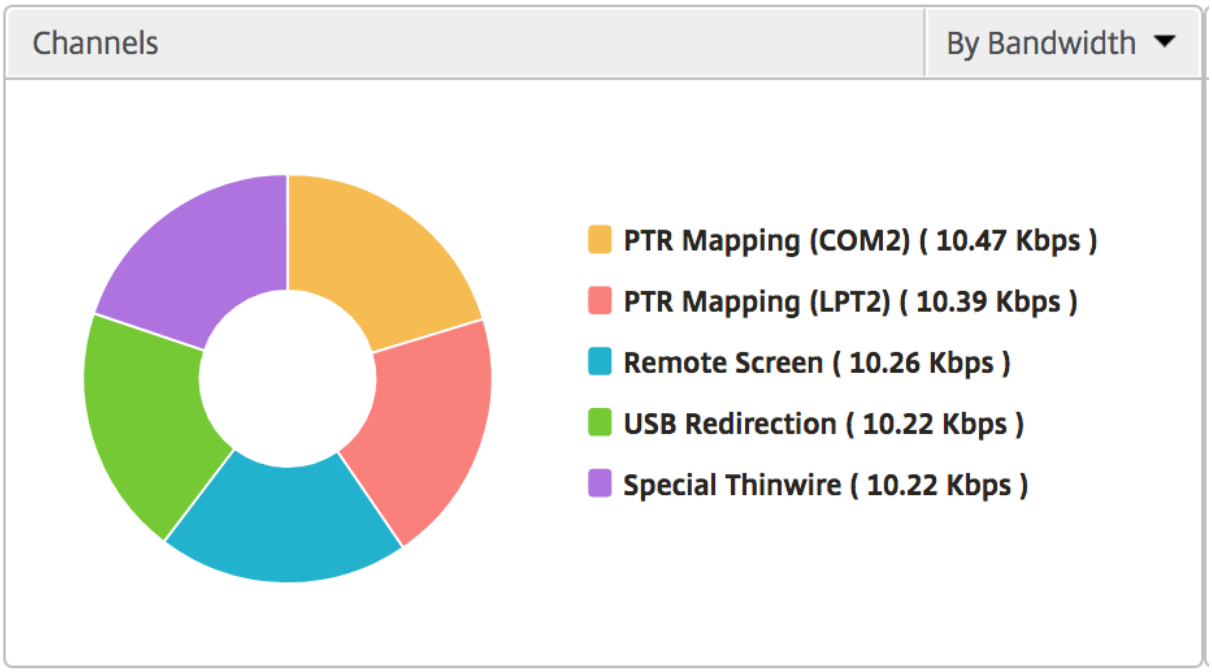
Users

Search

User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Cl
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	23.66 Kbps	1.88 K	
ramas	59	0	59	997.00 ms	778.00 ms	1.00 ms	7.03 Kbps	0	
omerp	59	0	59	997.00 ms	57.00 ms	754.00 ms	23.80 Kbps	1.89 K	
grahmm	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.80 Kbps	1.89 K	
ryan	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.69 Kbps	1.88 K	
rajivs	59	0	59	801.00 ms	11.00 ms	1.00 ms	23.97 Kbps	0	
alexisc	117	0	118	622.00 ms	56.00 ms	392.00 ms	47.67 Kbps	1.88 K	
juan	59	59	118	169.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
lennoxl	59	0	59	169.00 ms	31.00 ms	30.00 ms	23.86 Kbps	0	
daniel	59	59	118	149.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
woojunek	58	0	59	149.00 ms	31.00 ms	30.00 ms	23.85 Kbps	0	
parkerf	59	0	59	149.00 ms	31.00 ms	30.00 ms	23.88 Kbps	0	
randyb	59	59	118	99.00 ms	11.00 ms	29.00 ms	47.71 Kbps	0	
bradp	177	0	177	74.00 ms	27.00 ms	1.00 ms	71.75 Kbps	0	

Channels

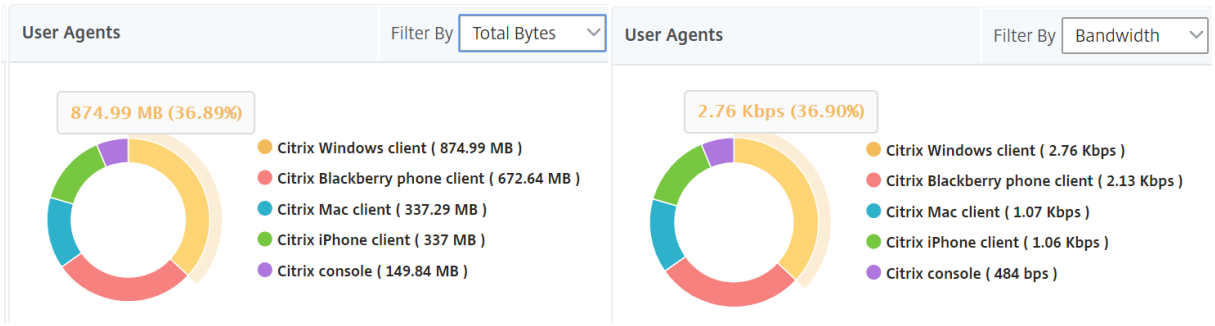
Channels represent the overall bandwidth or the total bytes consumed by each ICA® virtual channel in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.



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

User agents

User Agents represent the overall bandwidth/total bytes consumed by each end point in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.



Thresholds breach count

The Thresholds breach count metrics represent the count of thresholds breached in the selected time period. For more information, see how to create thresholds and alerts.

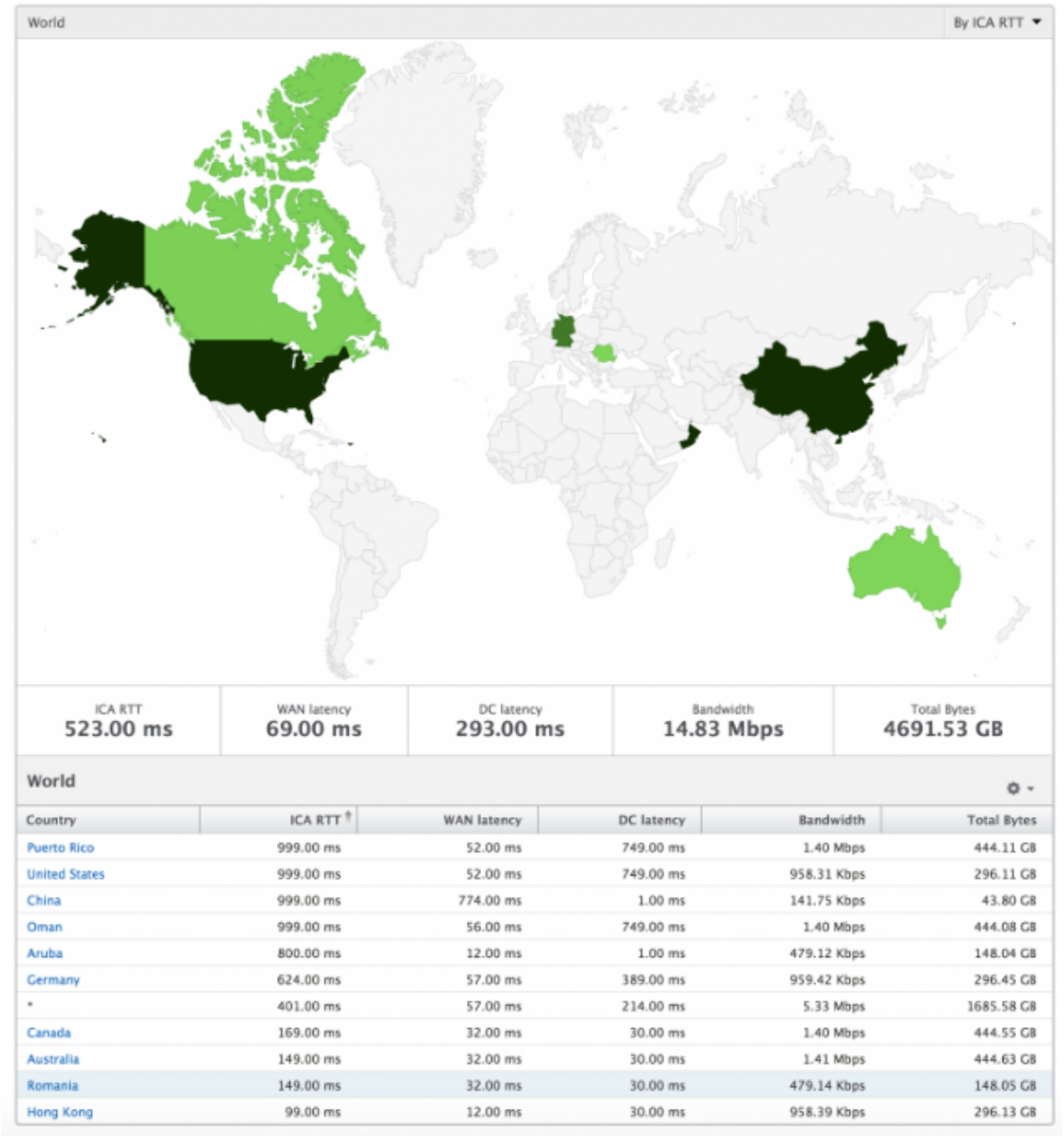
World map

The World map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill-down to a particular country and further into cities as well by clicking the region. The administrators can further drill-down to view information by city and state. From NetScaler Console version 12.0 and later, you can drill-down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metric is displayed in the form of a heat map:

- ICA RTT
- WAN Latency
- DC Latency
- Bandwidth
- Total Bytes

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



Per user view

The per user view provides detailed end user experience reporting for any particular selected user.

To navigate to specific user's metrics:

1. Navigate to **Gateway > HDX Insight > Users**.
2. Select a particular user from the Users summary report.

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

Line chart

Line chart displays the summary of all the metrics for the particular selected user during the selected time period.

Current/Terminated sessions report

This report is pertinent to all current/terminated user sessions for the selected user. These metrics can be sorted by start time, session reconnects and ACR count.

Metrics	Description
Session ID	A unique identity for an ICA session.
Session Type	Application/Desktop.
State	Green/Red for active/Inactive sessions.
Host Delay	Average delay in ICA traffic that passes through the NetScaler instances caused by server network.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Bytes per Interval	Number of bytes consumed by the session during that particular interval of time.
Start Time	Session start time.
Up Time	Session duration.
Client IP Address	End user IP.
Server IP Address	Backend/ Citrix Virtual App server IP.
NetScaler IP Address	NetScaler Management IP (NSIP).
Client Type	Workspace type- Citrix Windows Client and so on
Client Version	Workspace version.
MSI	Boolean (Yes/No). Indicates if the session is multi-stream ICA.
Session Reconnects	Number of times the session reconnected.
ACR Counts	Total number of times a client automatically reconnects users to disconnected sessions.

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

Metrics	Description
User Access Type	Displays the mode of access of the ICA session. For example, NetScaler Gateway user/transparent mode.
Country	Country from which the session was established.
Region	Region from which the session was established.
City	City from which the session was established.
USB Status	Active/Inactive -Green/Red.
Number of USB Instances Accepted	The count of USB instances accepted.
Number of USB Instances Rejected	The count of USB instances rejected.
Number of USB Instances Stopped	The count of USB instances stopped.
Client Host Name	The host name of the client.
HA Failover Count	Number of times HA failover occurred.
Reason for termination	Displays the reason for a session termination. For example, ICA Session Timeout, Session terminated by the user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to backend servers.
Total Bytes	Total Bytes consumed by the user during the selected time period.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and backend server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.

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

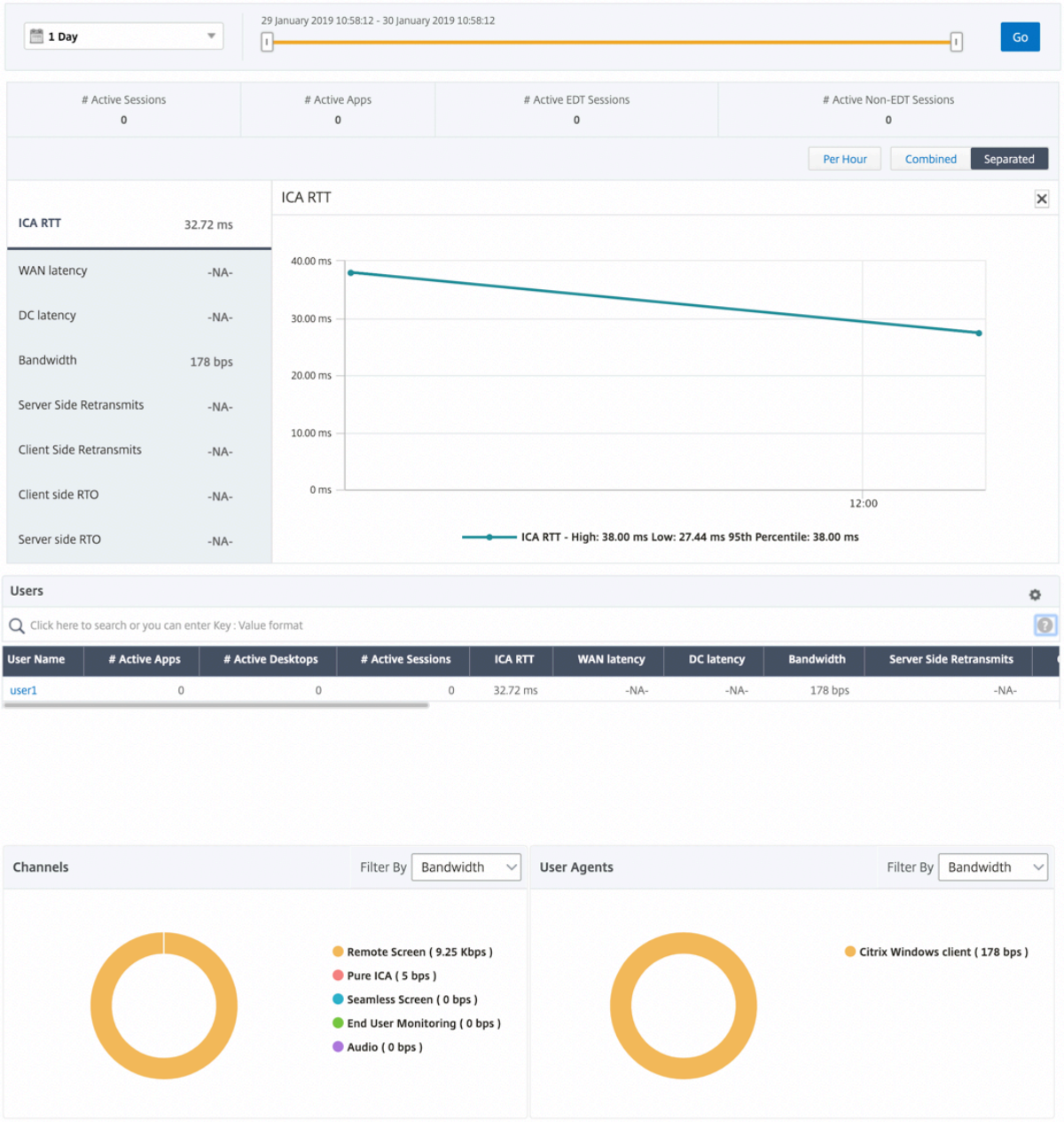
Metrics	Description
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and backend server.

Support for EDT in HDX insight

NetScaler Console now supports enlightened data transport (EDT) for displaying analytics for HDX Insight. That is, NetScaler Console now supports both UDP and TCP protocol. EDT support for NetScaler Gateway ensures a high definition in-session user experience of virtual desktops for users running Citrix Workspace.

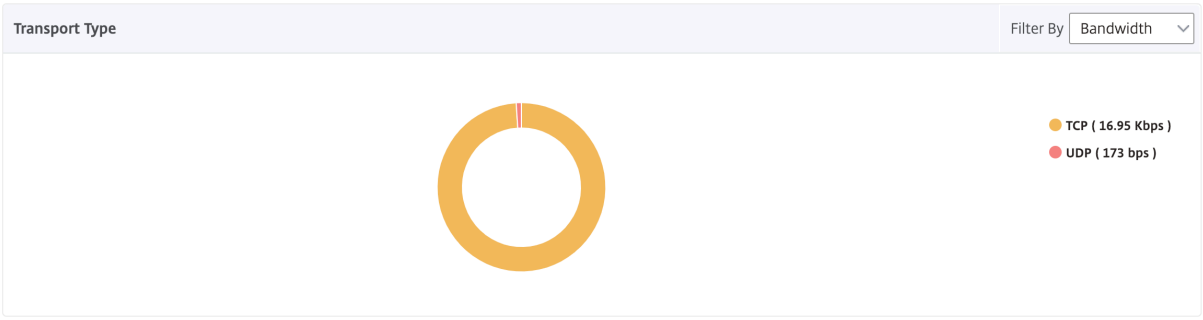
HDX Insight now displays the number of EDT sessions and non-EDT sessions as part of the active sessions report. The Users table displays a detailed report of all the users in the system. The table shows metrics such as WAN latency, DC latency, retransmits, and RTOs. Some of these metrics are not available for users who do have EDT sessions as they are calculated from the TCP stack currently. Therefore, they appear as "NA".

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



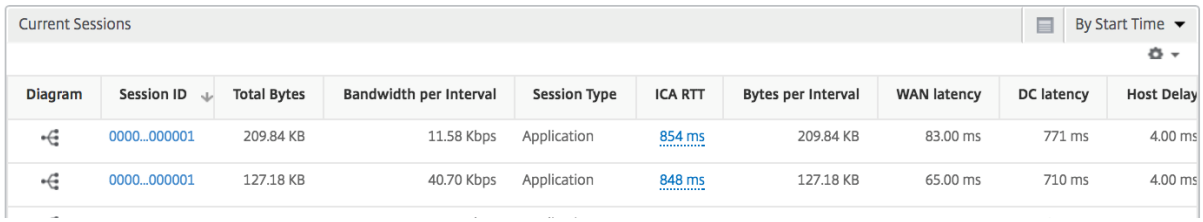
A new donut chart has been introduced to allow you to see bandwidth consumed by the user and also the total number of bytes based on the type of protocol used by the users.

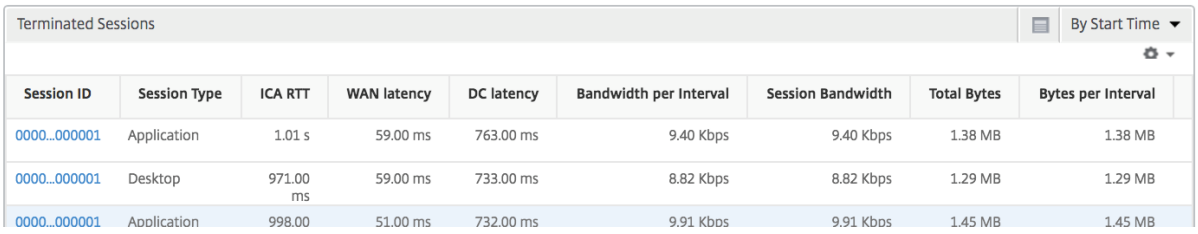
© 1997–2025 Citrix Systems, Inc. All rights reserved.



HDX Insight metrics available from NetScaler Console 12.0 and later:

L7 Client-side Latency	The average L7 latency observed between the ICA client and the NetScaler instance. This metric is useful in case of non-Citrix devices being present in the delivery path.
L7 Server-side Latency	The average L7 latency observed between the NetScaler device and the Citrix Virtual App. This metric is useful in case of non-Citrix devices being present in the delivery path.
Maximum Breach Latency	The highest value of the L7 latency when a breach of a defined threshold for a set time interval occurs.
Average Breach Latency	The average value of L7 latency when the system is in a “L7 latency breached”state.
L7 Threshold Breach Count	The number of times a L7 threshold breach has occurred.



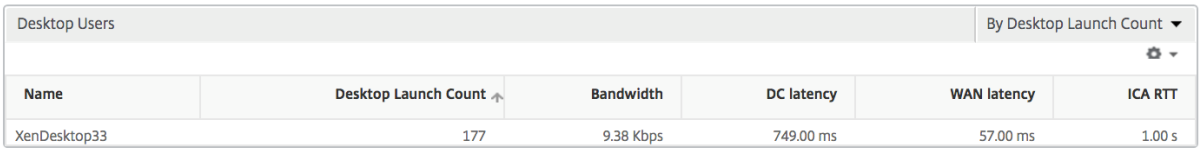


© 1997–2025 Citrix Systems, Inc. All rights reserved.

Desktop Users

This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

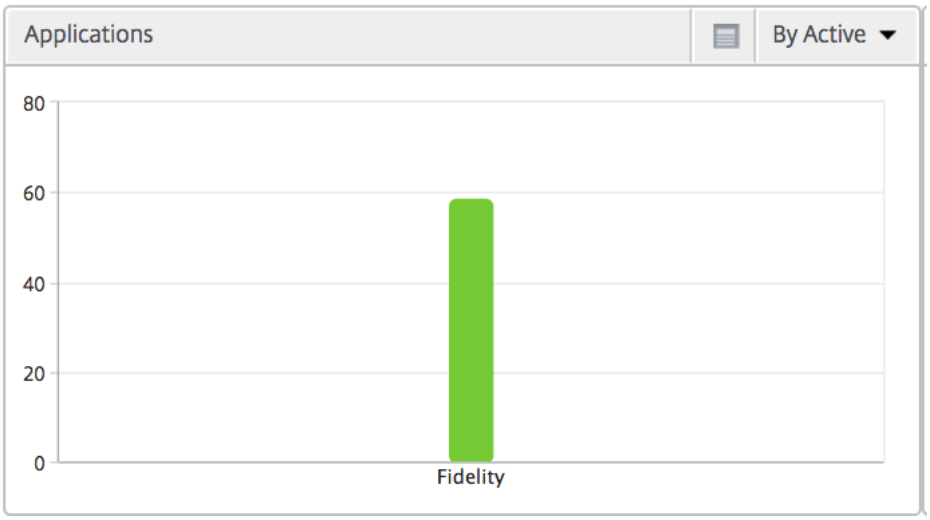
Metrics	Description
Name	Name of the Citrix Virtual Desktop.
Desktop Launch Count	Number of times the desktop has launched.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to backend servers.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.



Applications

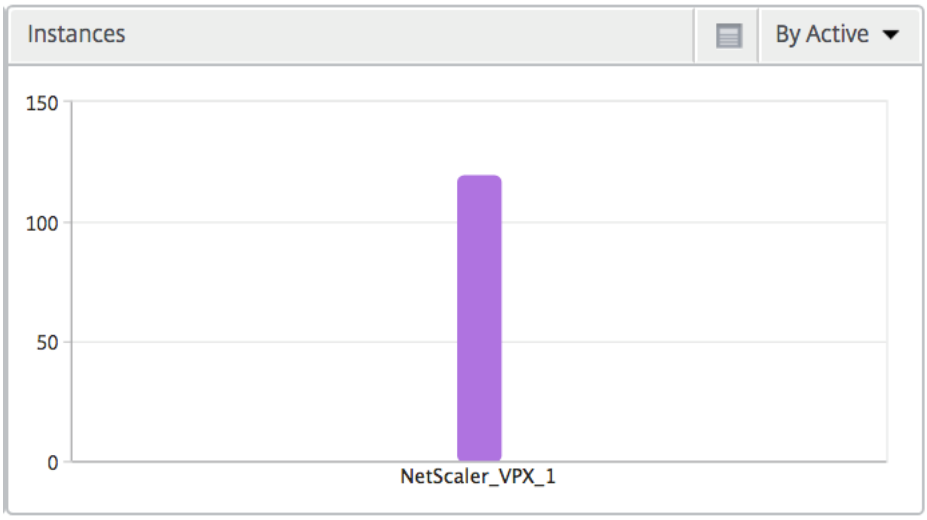
A bar graph representing apps sorted by Active, total session launch count, total app launch count, and launch duration.

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



Instances

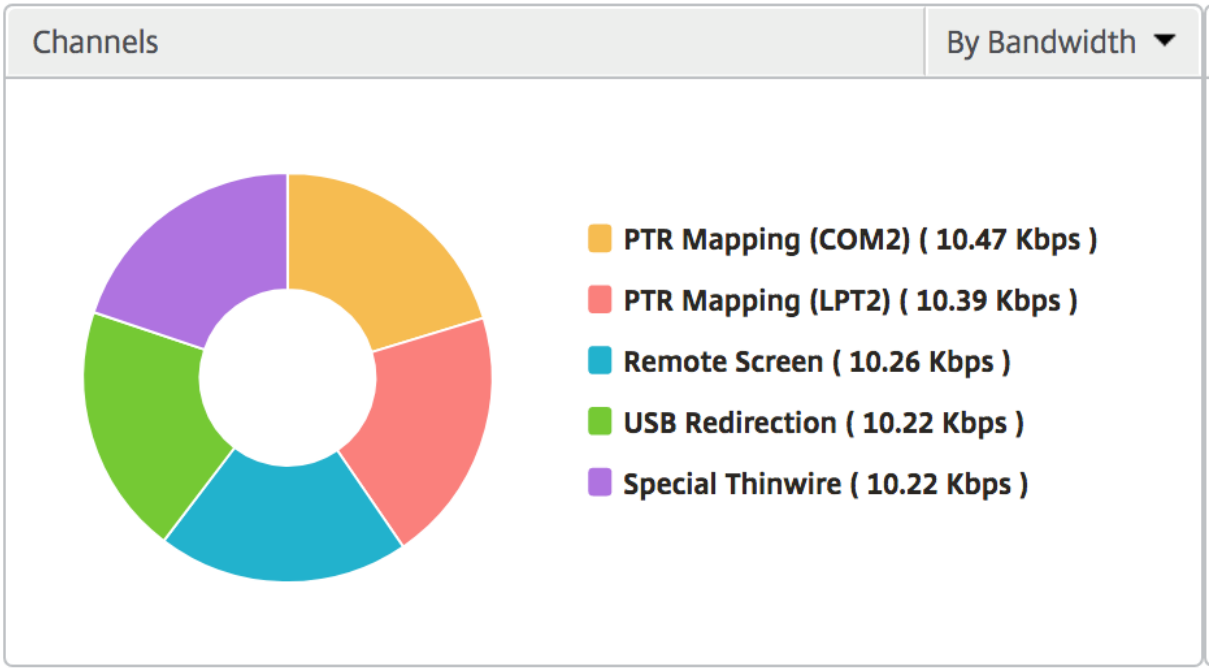
A bar graph representing NetScaler Instances sorted by Active and total apps



Channels

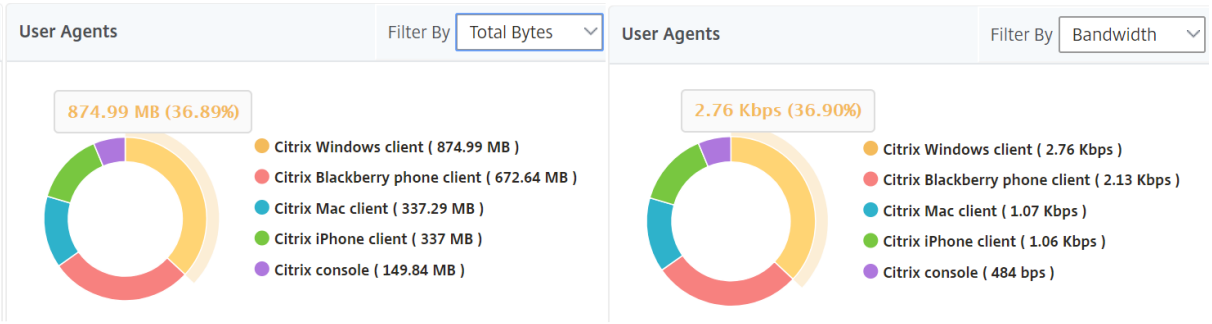
Channels represent the overall bandwidth or the total bytes consumed by each ICA virtual channel in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.

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



User agents

User Agents represent the overall bandwidth/total bytes consumed by each end point in the form of a doughnut chart. You can also sort the metrics by bandwidth, or Total bytes.



Per User session view

The per user session view provides reporting for a particular selected user's session.

To view the metrics for a selected user's session:

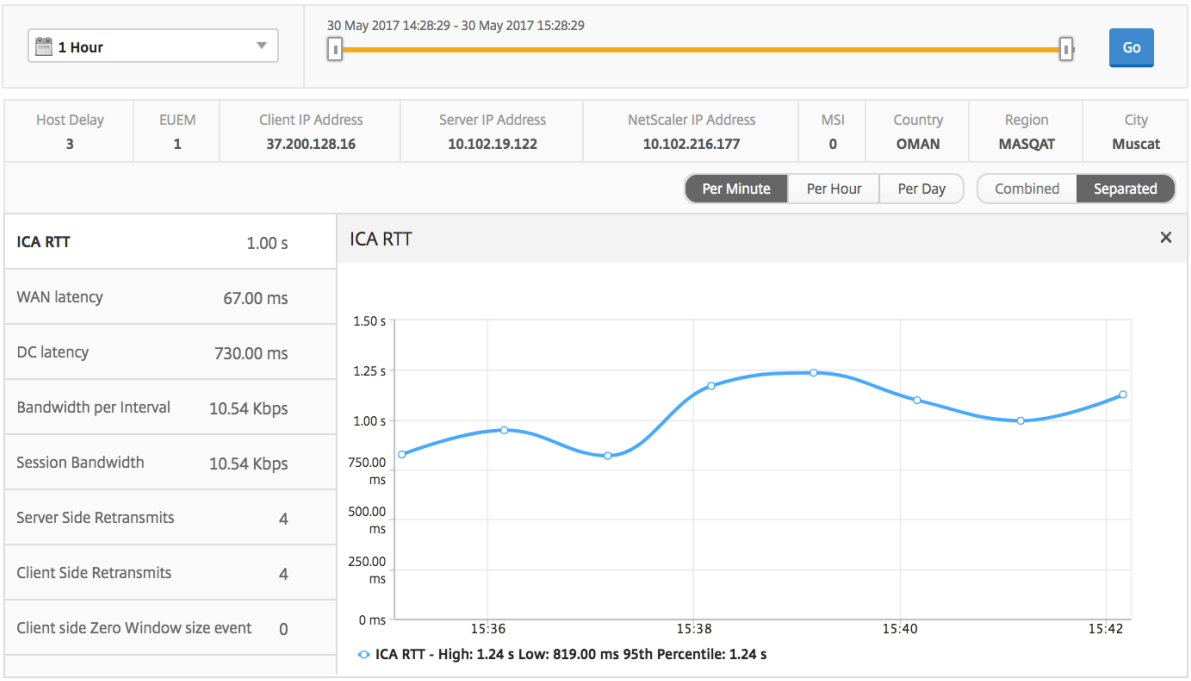
1. Navigate to **Gateway > HDX Insight > Users**.
2. Select a particular user from the **User Summary Report** section.
3. Select a session from **Current Sessions** or **Terminated Sessions** column.

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

Timeline chart

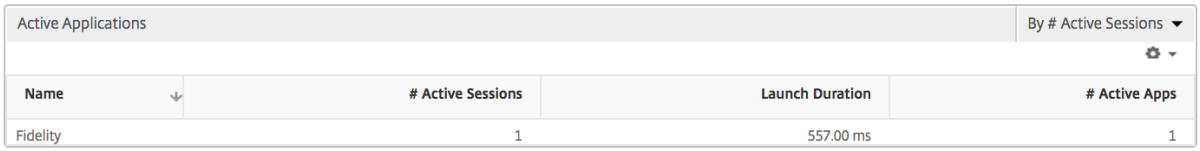
Metrics	Description
Session Reconnects	This number indicates the count of active Citrix Virtual App and Desktop sessions.
ACR Counts	This number indicates the count of active Citrix Virtual App sessions.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to backend servers.
Session Bandwidth	The bandwidth consumed by the session irrespective of the interval of time.
Server Side Retransmits	The number of packets retransmitted on the connection between NetScaler and backend server.
Client Side Retransmits	The number of packets retransmitted on the connection between NetScaler and the end user. A high value of this metric does not mean that the user experience will not be seamless but indicates high bandwidth utilization due to retransmits.
Client side fast RTO	Number of times the retransmission timeout occurred the connection between NetScaler and the end user.
Server side fast RTO	Number of times the retransmission timeout occurred on the connection between NetScaler and backend server.
Bandwidth per Interval	The bandwidth consumed by the session during that particular interval of time.
Server side Zero Window size event	This counter indicates the number of times the server advertised a zero TCP window.
Client side Zero Window size event	This counter indicates the number of times the client advertised a zero TCP window.

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



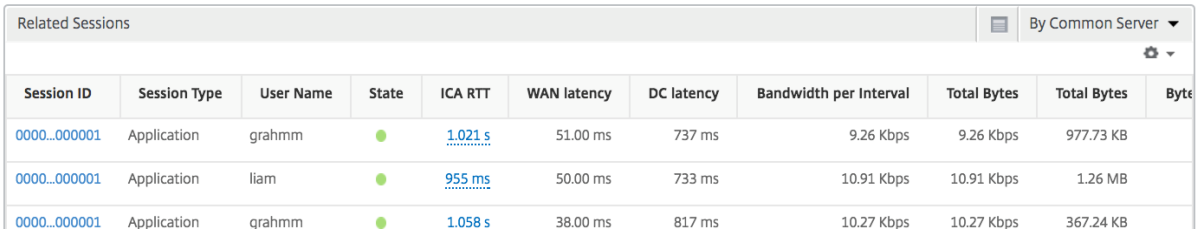
Active application

The **Active Applications** section displays the active applications of the selected user. These applications can also be sorted by number of active sessions and launch durations.



Related sessions

The related Sessions section displays the related sessions of the selected user's sessions. The relationship can be selected as common servers or common NetScaler.



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

Instance View Reports and Metrics

September 27, 2025

The reports and metrics in the instance view are focused on the NetScaler instances.

To navigate to the instance view:

1. Navigate to **Gateway > HDX™ Insight > Instances**.

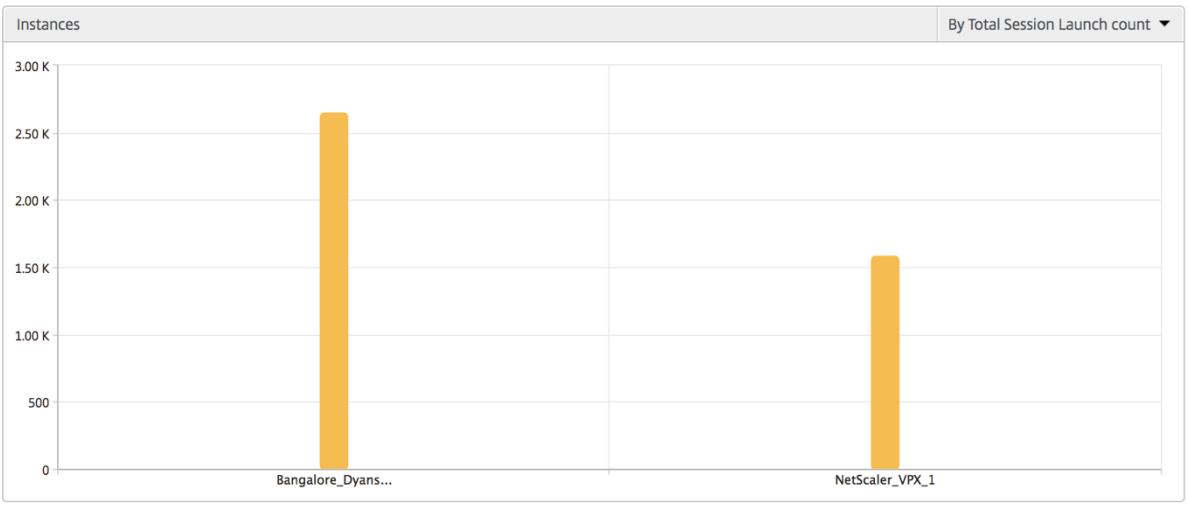
Instance summary view

This view is called the summary view as it shows the reports for all the NetScaler instances that are added to NetScaler Console.

All the metrics/reports, unless explicitly mentioned will have the values corresponding to them for the selected time period.

Instance bar graph

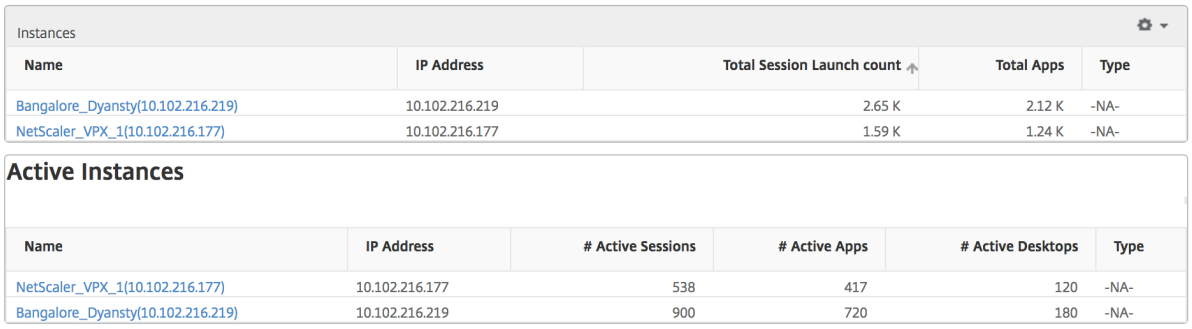
This graph displays the instance vs the Total Session Launch count and Total Apps which can be selected from the list on the top right on the graph canvas.



Instance/Active instances summary report

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

Metrics	Description
Name	Host name of the NetScaler instance.
IP Address	NetScaler IP address.
Total Session Launch count	Total number of unique user sessions created during a given time interval.
Total Apps	Total number of unique applications launched during a given time interval.
Type	N/A



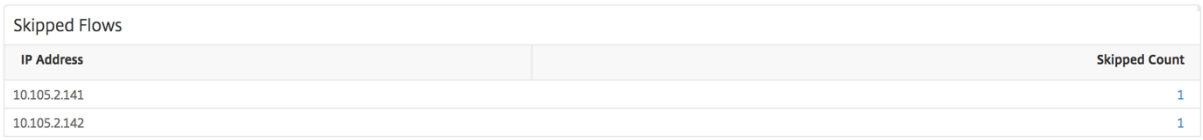
Threshold report

Threshold report represents the count of thresholds breached where the *entity* is selected as Instance in the selected period. For more information, see how to create thresholds and alerts.

Skipped flows

A skipped flow is a record which skipped parsing ICA connection. This can occur due to multiple reasons like using unsupported Citrix Virtual Apps and Desktops versions, unsupported version of workspace or workspace type, and so on. This table shows the IP address and the skipped flow count. These workspaces may not be part of whitelisted workspaces. Hence these sessions are skipped from monitoring.

See **Error! Hyperlink reference not valid** for more details on issues related to ICA parsing.



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

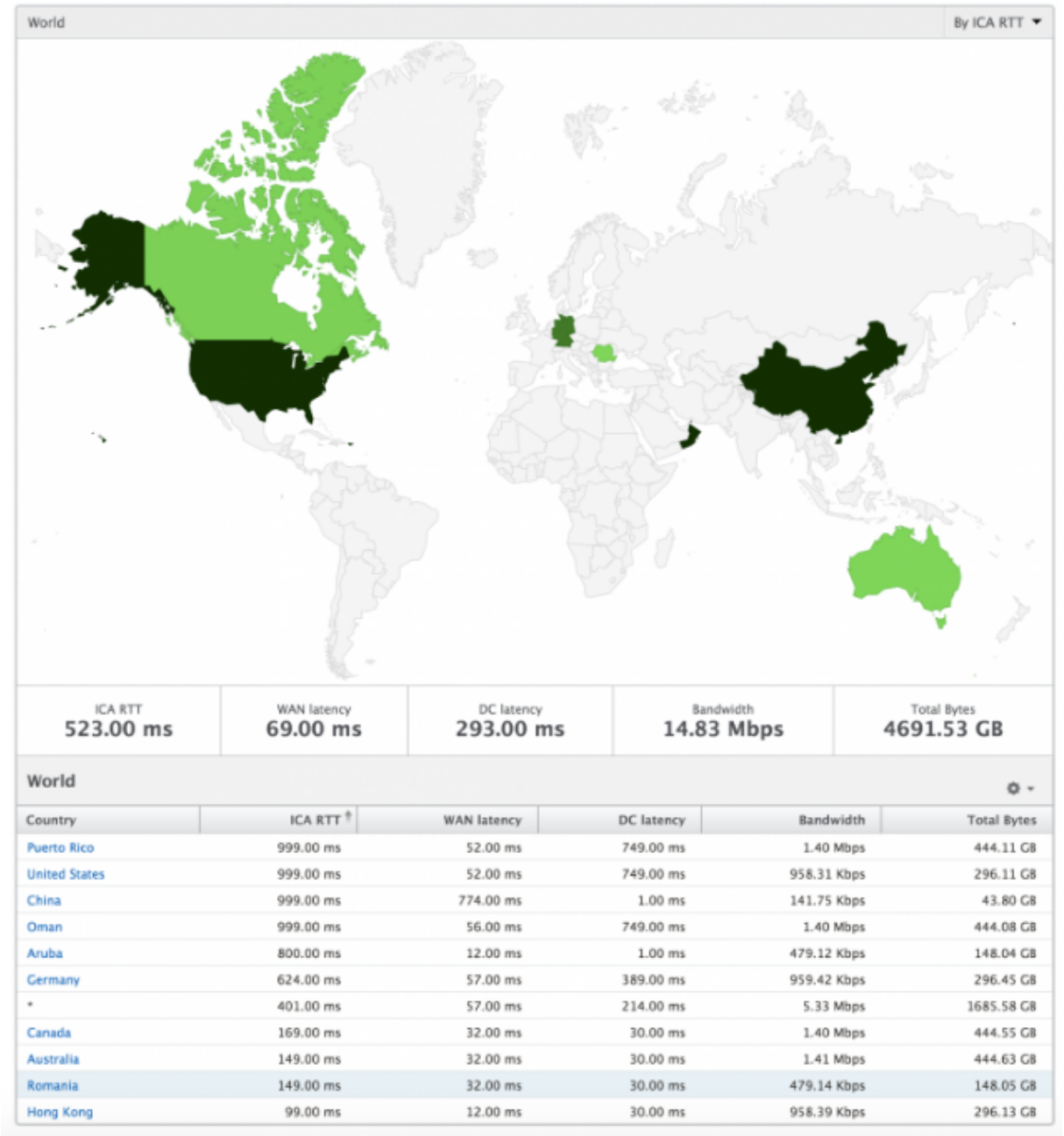
World view

The World Map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill-down to a particular country and further into cities as well by clicking the region. The administrators can further drill down to view information by city and state. From NetScaler version 12.0 and later, you can drill down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metric is displayed in the form of a heat map:

- ICA® RTT
- WAN Latency
- DC Latency
- Bandwidth
- Total Bytes

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



Per instance view

Per instance view provides detailed end user experience reporting for a particular selected NetScaler instance.

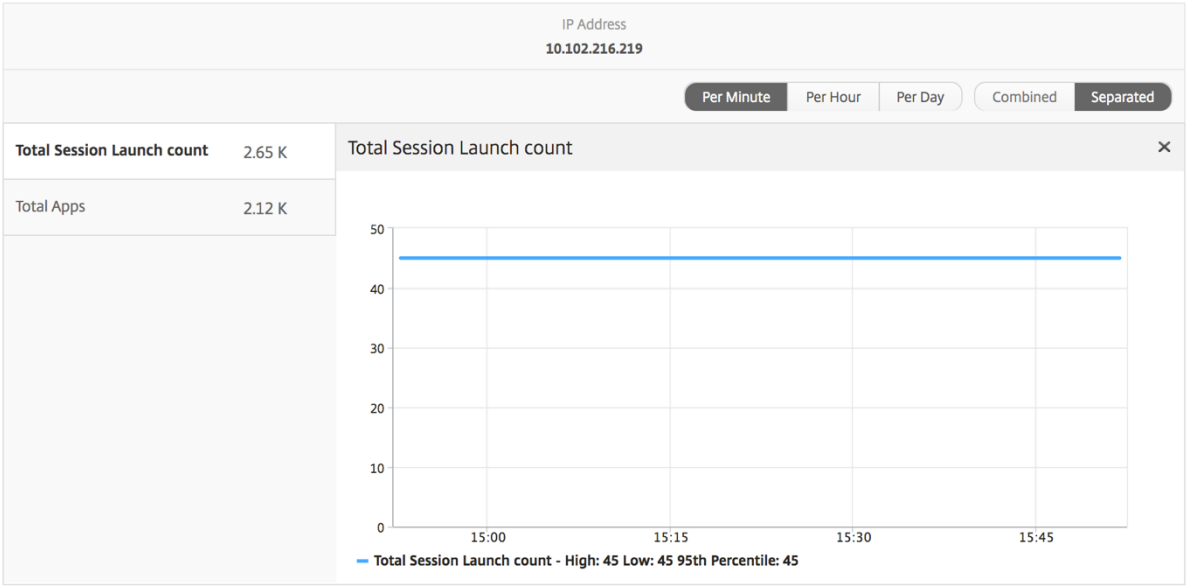
To navigate to the instance view:

1. Navigate to **Gateway > HDX Insight > Instances**.
2. Select a particular instance from the **Instance Summary Report**.

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

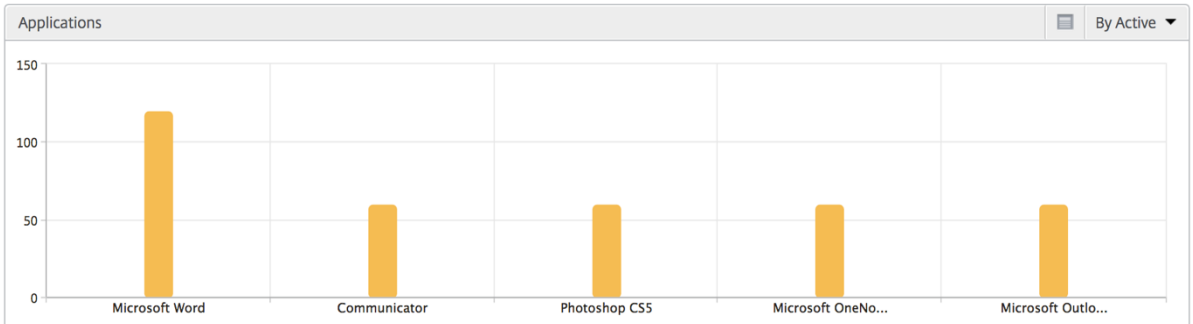
Line chart

Metrics	Description
IP Address	This represents the NetScaler IP address of the selected instance.
Total session launch count	Total number of active Citrix Virtual App sessions during the given time interval.
Total Apps	Total number of unique applications launched during a given time interval.



Applications bar graph

Displays top 5 applications based on the following criteria- by Active apps, total session launch count, total app launch count, or launch duration.

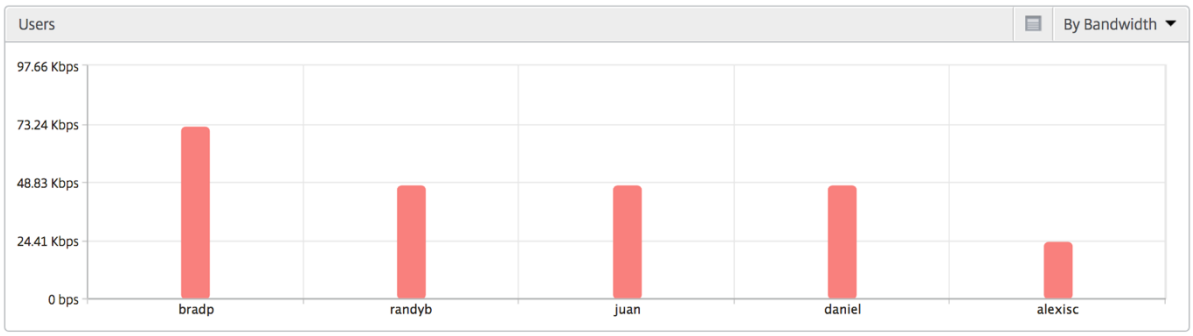


© 1997–2025 Citrix Systems, Inc. All rights reserved.

Users bar graph

The Users bar graph displays top 5 users based on the following criteria

- Bandwidth
- WAN Latency
- DC Latency
- ICA RTT

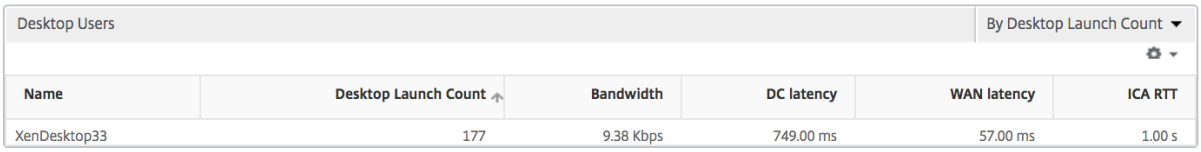


Desktop users report

This table gives the insight into the Citrix Virtual Desktop sessions for a particular user. These metrics can be sorted by Desktop Launch Count and Bandwidth.

Metrics	Description
Name	Name of the Citrix Virtual Desktop.
Desktop Launch Count	Number of times the desktop has launched.
Bandwidth	Total bytes per second taken for end to end communication during the selected time interval.
DC latency	Latency caused by the server side of the network. That is, from NetScaler to back end servers.
WAN latency	Latency caused by the client side of the network. That is, from NetScaler to end user.
ICA RTT	ICA RTT is the screen lag that the user experiences while interacting with an application or desktop hosted on Citrix Virtual App or Desktop respectively.

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



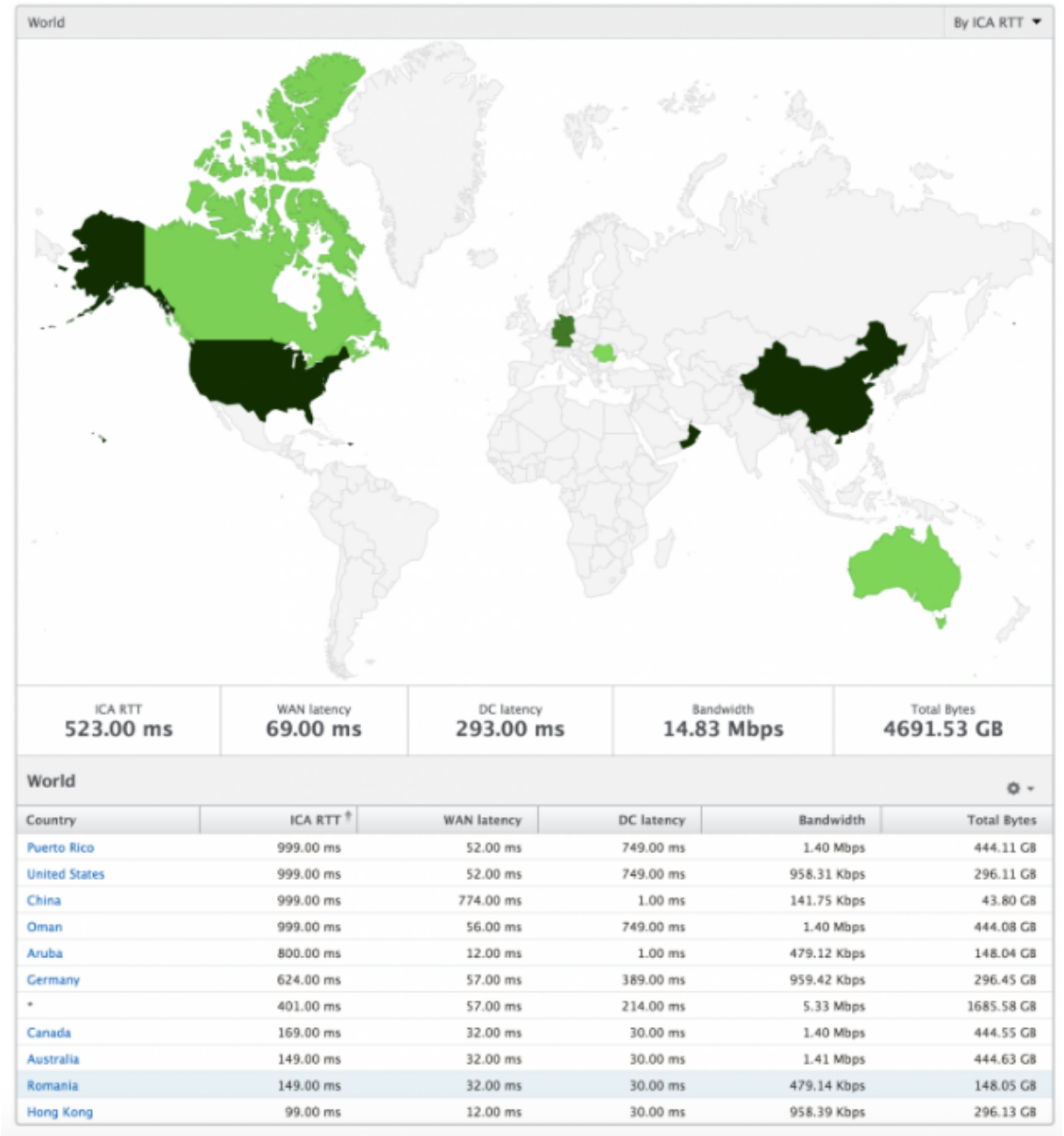
World view

The World Map view in HDX insight allows the administrators to view the historical and active users details from a geographical point of view. The administrators can have a World view of the system, drill down to a particular country and further into cities as well by clicking the region. The administrators can further drill down to view information by city and state. From NetScaler Console version 12.0 and later, you can drill down to users connected from a Geo location.

The following details can be viewed on the World Map in HDX insight, and the density of each metric is displayed in the form of a heat map:

- ICA RTT
- WAN Latency
- DC Latency
- Bandwidth
- Total Bytes

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



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

License View Reports and Metrics

September 27, 2025

The license view gives details on the NetScaler Gateway license information.

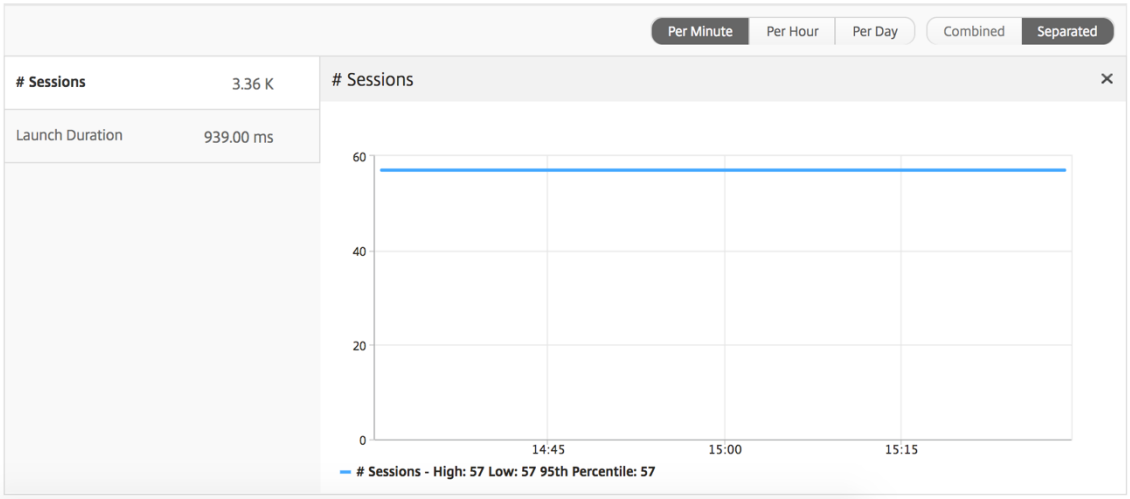
To navigate to the license view:

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

1. Navigate to **Gateway > HDX™ Insight > Licenses**.

Line chart

Metrics	Description
Licenses in use	The NetScaler Gateway CCU licenses being used during the selected timeline. Each count represents the number of user sessions. This is independent of the application and desktop sessions launched by that user.
Total licenses	Total number of NetScaler Gateway CCU licenses available for the customer to utilize.



Threshold report

The threshold report represents the count of thresholds breached where the *entity* is selected as License in the selected period. For more information, see how to create thresholds and alerts.

Troubleshoot HDX™ Insight issues

September 27, 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

- Make sure 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 ICA_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 "enableSRon-HAFailover"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.

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

You can also navigate to **Settings > AppFlow > Policies** in the GUI to check the AppFlow policy hits.

- Validate any firewall blocking AppFlow ports 4739 or 5557.

Record generation for HDX/ICA traffic in NetScaler checklist

Run the command `tail -f /var/log/ns.log | grep -i "default ICA Message"` for log validation. Based on the logs that are generated, you can use this information for troubleshooting.

- Log: **Skipped parsing ICA connection - HDX Insight not supported for this host**

  Cause: Unsupported Citrix Virtual Apps and Desktops versions

  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

  Solution: Upgrade Citrix Workspace to a supported version. For details, see Citrix Workspace app.

- 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.

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

- Log: **Skip code**

  If you see any of the following values for skip code, then the Insight details are skip parsed.

  > Skip code 0 indicates that the record is successfully exported from NetScaler.

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_FA	Failed to expand channel data
111	NS_ICA_ERR_REDUC_BYTES_V3_OOB	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

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

Skip Code	Error message	Cause of error
116	NS_ICA_ERR_MEM_REDUC_CTX_ALLOC	Memory allocation error for expander context
117	NS_ICA_ERR_ICA_OLD_SERVER	Old server, capability blocks not supported
118	NS_ICA_ERR_PIR_MANY_FRAG	Packet Init request is fragmented, unable to process
119	NS_ICA_ERR_INIT_ICA_CAPS	ICA capability initialization error
120	NS_ICA_ERR_NO_MSI_SUPPORT	Host does not support MSI feature. Indicates for XenApp version lower than 6.5 or XenDesktop versions lower than 5.0
121	NS_ICA_ERR_CGP_INVALID_CMD	Invalid CGP command encountered
122	NS_ICA_ERR_INSUFFICENT_CHANNEL_BYTES	Insufficient bytes over channel
123	NS_ICA_ERR_CHANNEL_DATA	Incorrect data on EUEM, CONTROL, or SEAMLESS channel
124	NS_ICA_ERR_INVALID_PURE_CMD	Invalid command received while processing pure ICA channel data
125	NS_ICA_ERR_INVALID_PURE_LEN0	Invalid length encountered while processing pure ICA channel data
126	NS_ICA_ERR_INVALID_PURE_LEN	Invalid length encountered while processing PURE ICA channel data
127	NS_ICA_ERR_INVALID_CLNT_DATA	Invalid data length received from client
128	NS_ICA_ERR_MSI_GUID_SZ	Error in MSI GUID size
129	NS_ICA_ERR_INVALID_CHANNEL_HEADER	Detected invalid channel header
130	NS_ICA_ERR_CGP_PARSE_RECONNECT_VC	Retrieval of reconnected session failed
131	NS_ICA_ERR_DISABLE_SR_NON_NS_RECONNECT	Error in disabling SR

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

Skip Code	Error message	Cause of error
132	NS_ICA_ERR_REDUC_NOT_V3	Unsupported ICA Reducer version
133	NS_ICA_ERR_HS_COMPRESSION_DISABLED	Compression disabled, not honored by host
134	NS_ICA_ERR_IDENT_PROTO	Unable to identify ICA or CGP protocol, seen with incorrect workspaces
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 1460 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

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

Skip Code	Error message	Cause of error
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
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

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

Skip Code	Error message	Cause of error
168	NS_ICA_ERR_ICAP_INSUFFBYTE	Unexpected number of bytes in ICA handshake
169	NS_ICA_ERR_HIGHER_RECONSEQ	Higher CGP resumption sequence number from peer post reconnects
170	NS_ICA_ERR_DESCSRINFO_ABSENT	Unable to restore ICA parsing state post reconnect
171	NS_ICA_ERR_NSAP_PARSING	Error while parsing Insight channel data
172	NS_ICA_ERR_NSAP_APP	Error while parsing app details from Insight channel data
173	NS_ICA_ERR_NSAP_ACR	Error while parsing ACR details from Insight channel data
174	NS_ICA_ERR_NSAP_SESSION_END	Error while parsing session end details from Insight channel data
175	NS_ICA_ERR_NON_NSAP_SN	Skipped ICA parsing on service node due to the absence of Insight channel support
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
```

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

```
 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
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

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

HDX counter name	Purpose	Category(Stats/Error/Diagnostics)
hdx_dbg_tot_nsap_conn	Indicates total number of NSAP supported connections detected by NS	Stats
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

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

HDX counter name	Purpose	Category(Stats/Error/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
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 and HDX Insight skips this connection.	Error
hdx_err_skip_old_server	Old unsupported server version	Error
hdx_err_clnt_not_whitelist	Client workspace 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

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

HDX counter name	Purpose	Category(Stats/Error/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
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

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

HDX counter name	Purpose	Category(Stats/Error/Diagnostics)
hdx_dbg_usb_reset_device	Total number of USB devices reset	Diagnostics
hdx_dbg_usb_stop_device	Total number of USB devices stopped	Diagnostics
hdx_dbg_usb_stop_device_response	Total number of responses from stopped USB devices	Diagnostics
hdx_dbg_usb_device_gone	Total number of USB devices gone	Diagnostics
hdx_dbg_usb_device_stopped	Total number of USB devices stopped	Diagnostics

nstrace validation

Check for CFLOW protocol to see all AppFlow records going out of NetScaler.

Population of records in NetScaler Console checklist

- Run the command `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"`and check logs to confirm NetScaler Console is receiving AppFlow records.
- Confirm NetScaler instance is added to NetScaler Console.
- Validate NetScaler Gateway/VPN virtual server is licensed in NetScaler Console.
- Make sure multi-hop parameter setting is enabled for double-hop.
- Make sure NetScaler Gateway is cleared for second-hop in double-hop deployment.

Before contacting Citrix technical support

For a speedy resolution, make sure that you have the following information before contacting Citrix technical support:

- Details of the deployment and network topology.
- NetScaler and NetScaler Console versions.
- Citrix Virtual Apps and Desktops server versions.
- Client Workspace versions.

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

- 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.

Infrastructure Analytics

September 27, 2025

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. They can be able to remediate any probable issues in configuration, setup, connectivity, certificates, and others which might impact application usage or performance. For example, a sudden change in the 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 it to a measurable score that defines the health of an instance. With this feature, the administrators get a single touch point to understand if there is a problem, the origin of the problem, and probable remediations that they can perform.

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

Infrastructure analytics

The NetScaler Console 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 a 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 a 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

- 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 The 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 form 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 may occur while processing the client traffic. This issue causes low performance in a NetScaler instance. By understanding such NetScaler capacity issues, you can allocate additional licenses proactively to steady the NetScaler performance.

To view NetScaler capacity issues,

1. Navigate to **Infrastructure > Infrastructure Analytics**.
2. Expand the instance for which you want to view 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** –The number of packets dropped in the instance after the throughput limit is reached.

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

- **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.

The NetScaler Console calculates the instance score on the defined capacity threshold.

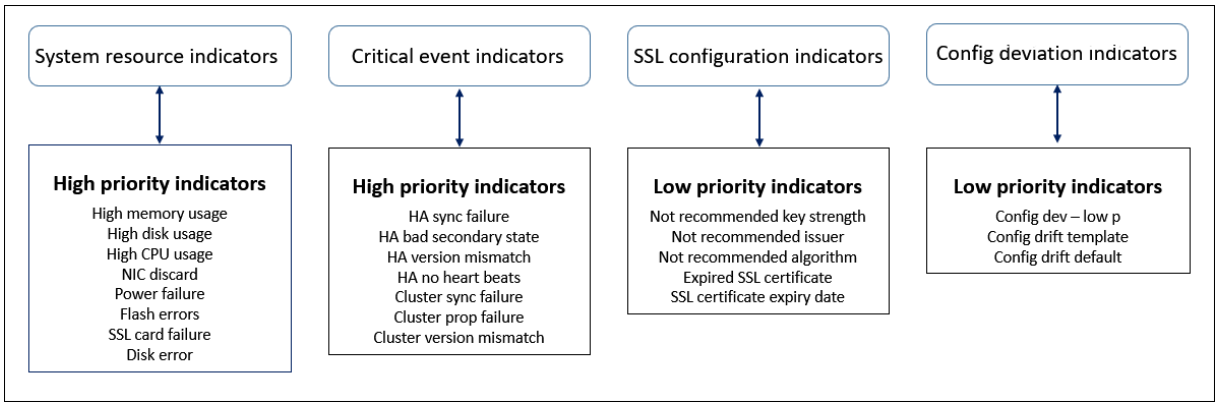
- Low threshold –1 packet drop or rate-limit counter increment
- High threshold –10000 packets drop or rate-limit counter increment

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 `NetScalerCapacityBrea` category. To view these events, navigate to **Accounts > System Events**.

Value of health indicators

The indicators are classified into high priority indicators and low-priority indicators based on their values as follows:



The health indicators within the same group of indicators have different weights assigned to them. One indicator might contribute more to lowered instance score than another indicator. For example, high memory usage brings down the instance score more than high disk usage, high CPU usage, and NIC discard. If an instance has a greater number of indicators detected on it, the lesser is the instance score.

The value of an indicator is calculated based on the following rules. The indicator is said to be detected in one of the following three ways:

1. **Based on an activity**. For example, a System resource indicator is triggered whenever there is a power failure on the instance, and this indicator reduces the value of the instance score. When the indicator is cleared the penalty is cleared, and the instance score increases.

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

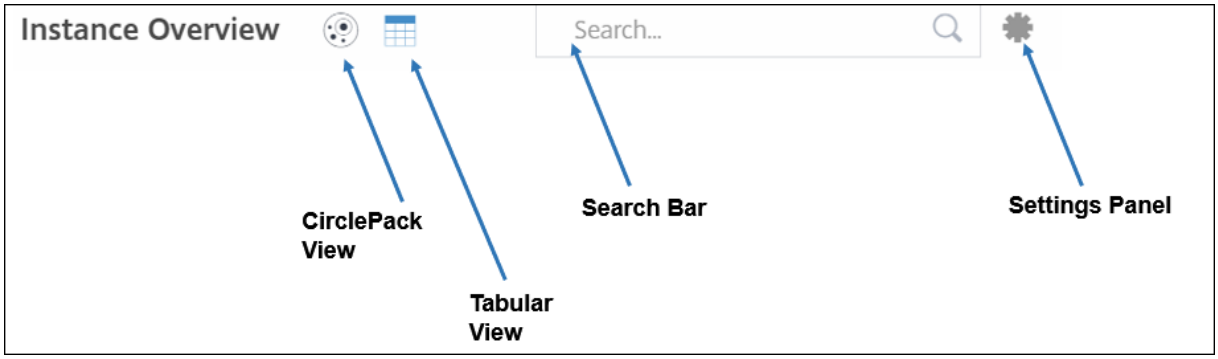
2. **Based on the threshold value breach**. For example, a System resource indicator is triggered when the NIC card discards packets and the threshold level is breached.
3. **Based on the low and high threshold value breach**. Here, an indicator can be triggered in two ways:
    - When the value of the 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**.

The Infrastructure Analytics can be viewed in a **Circle Pack** format or a **Tabular** format. You can toggle between the two formats.

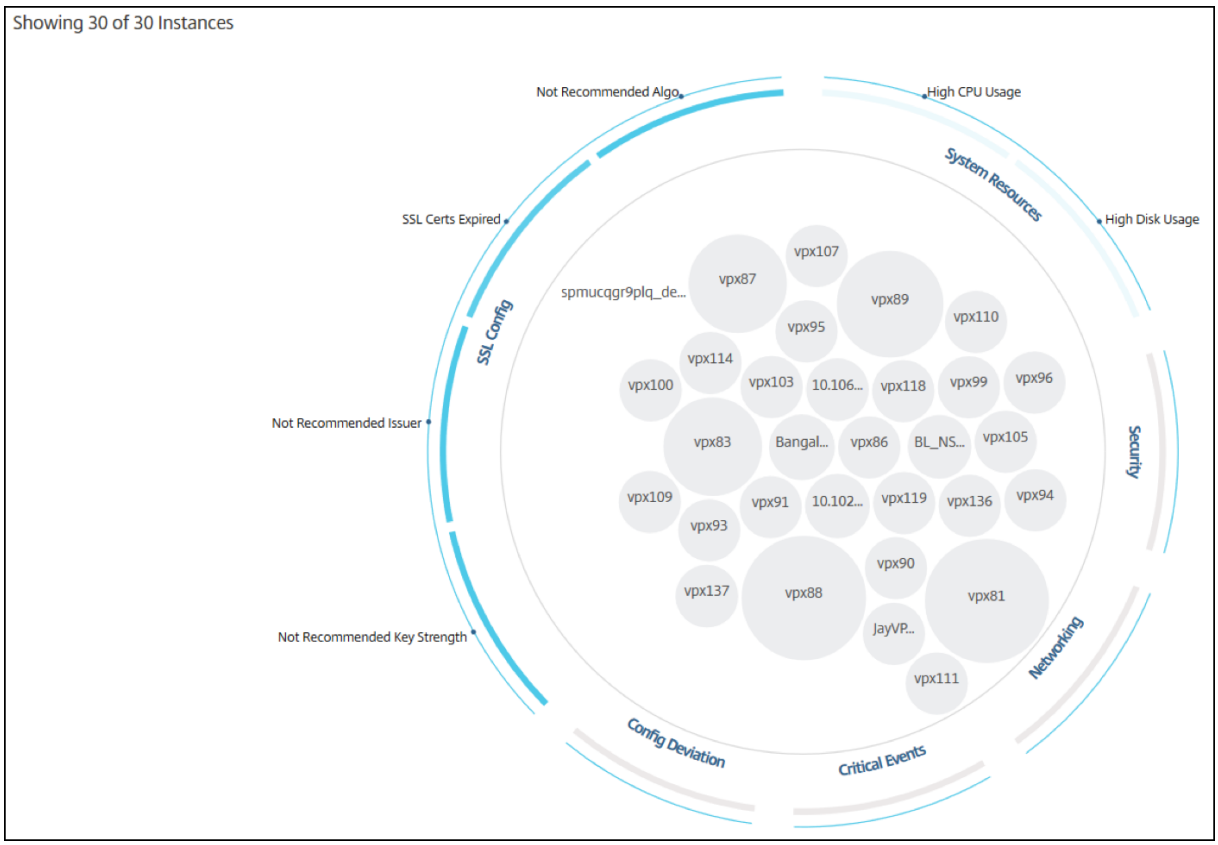


- In the Tabular view, you can search for an instance by typing the host name or the IP address in the Search bar.
- By default, Infrastructure Analytics page displays the Summary Panel on the right side of the page.
- Click the **Settings** icon to display the **Settings** Panel.
- In both the view formats, the Summary Panel displays details of all the instances in your network.

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

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.



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.

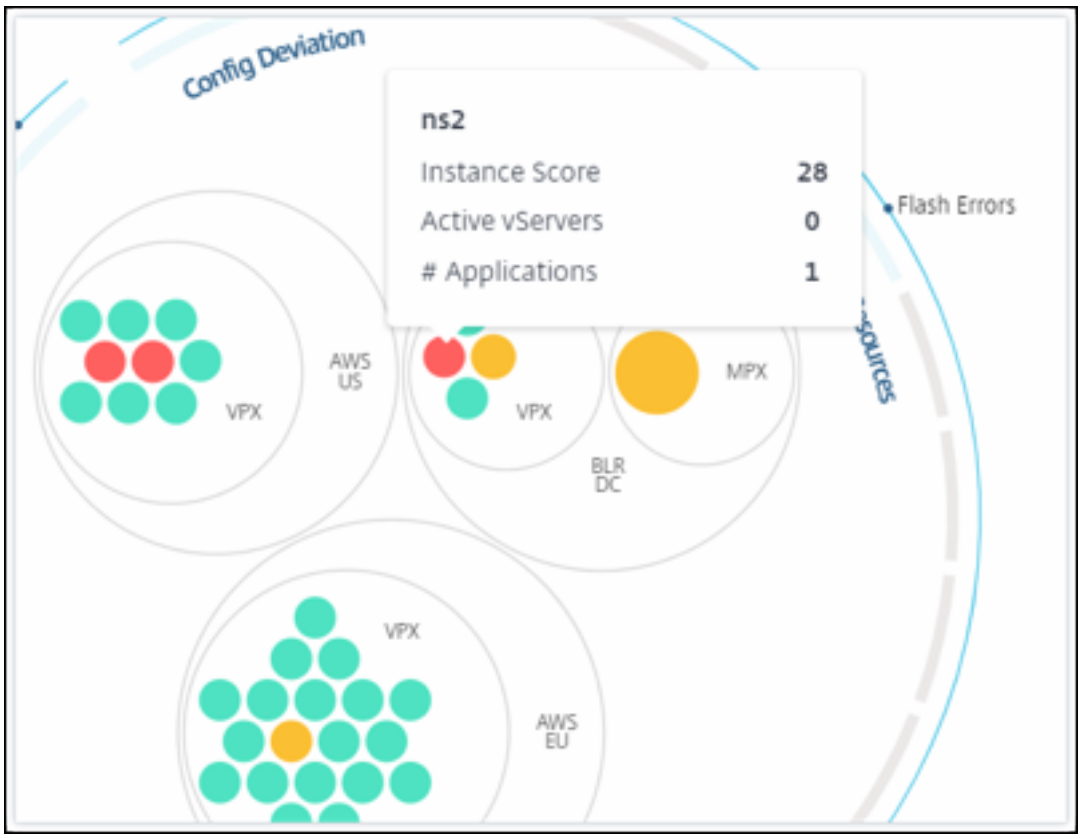
© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.



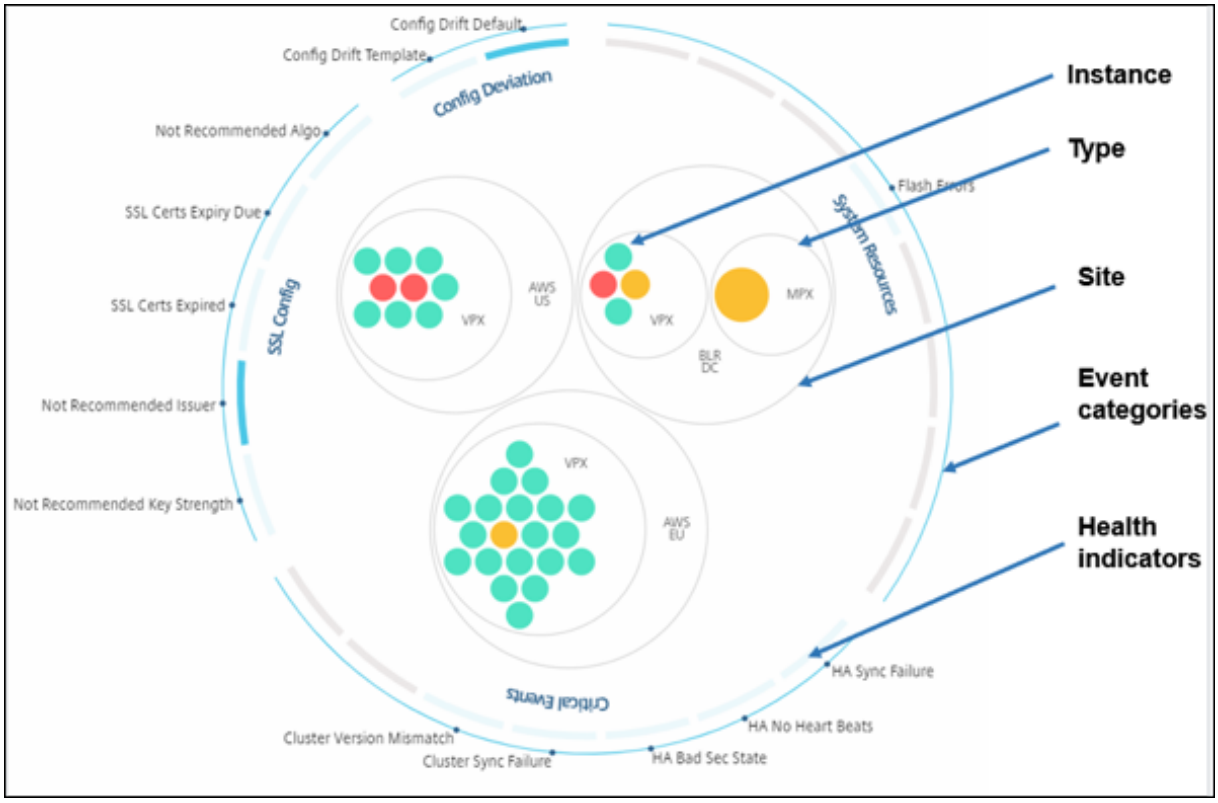
Grouped instance circles

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.



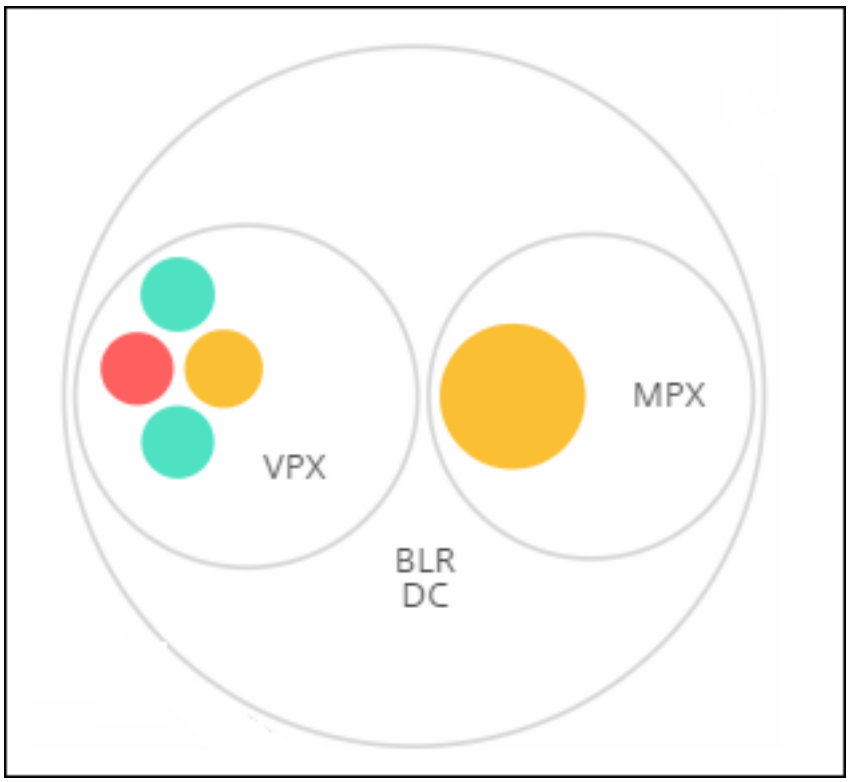
All these nested circles are bounded by two outermost circles. The outer two circles represent the four categories of events monitored by the NetScaler Console (system resources, critical events, SSL configuration, and configuration deviation) and the contributing health indicators.

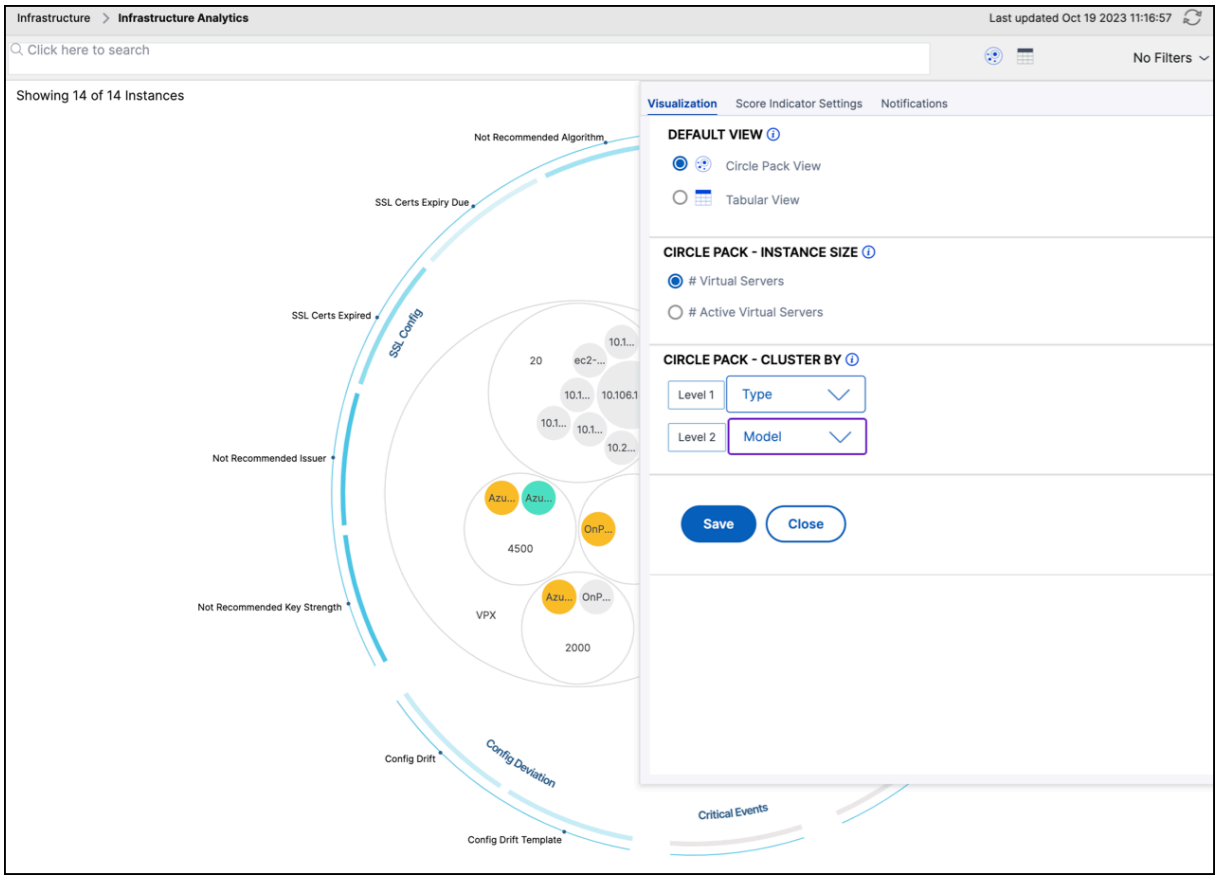
Clustered instance circles

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:

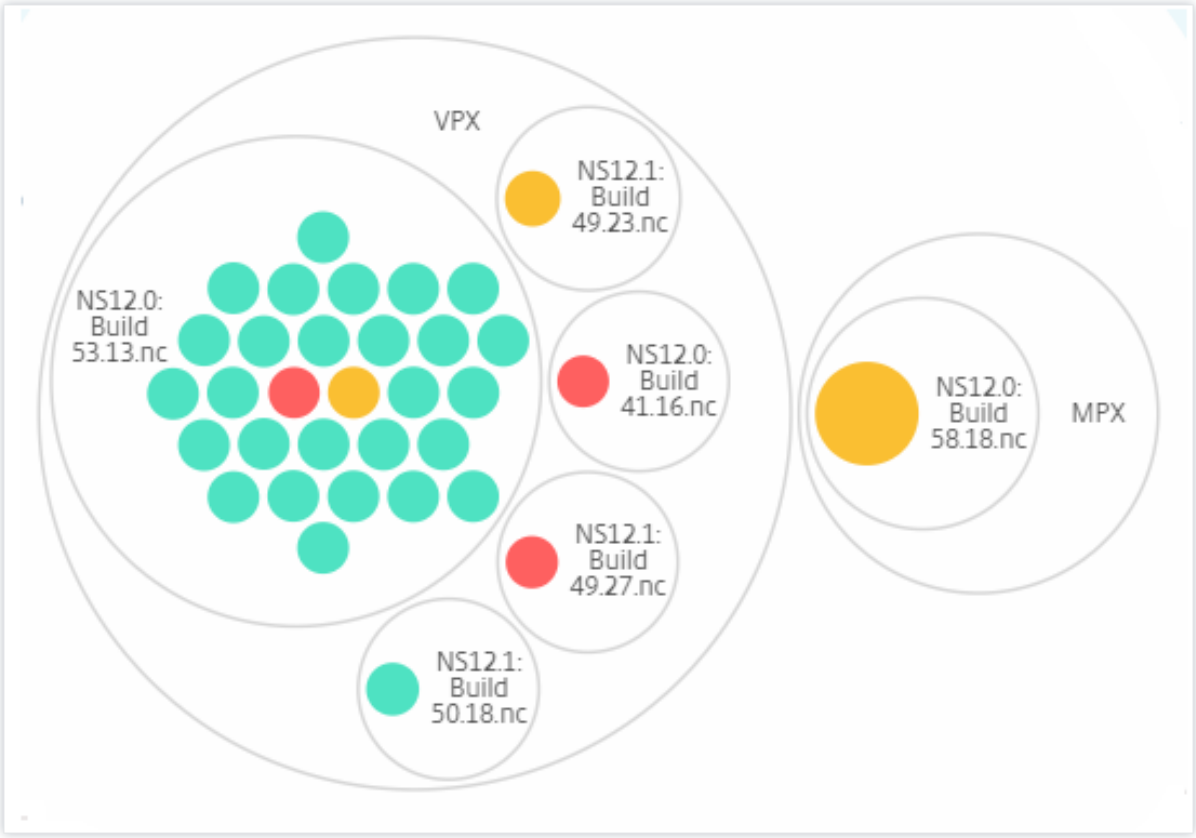
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Site and model:



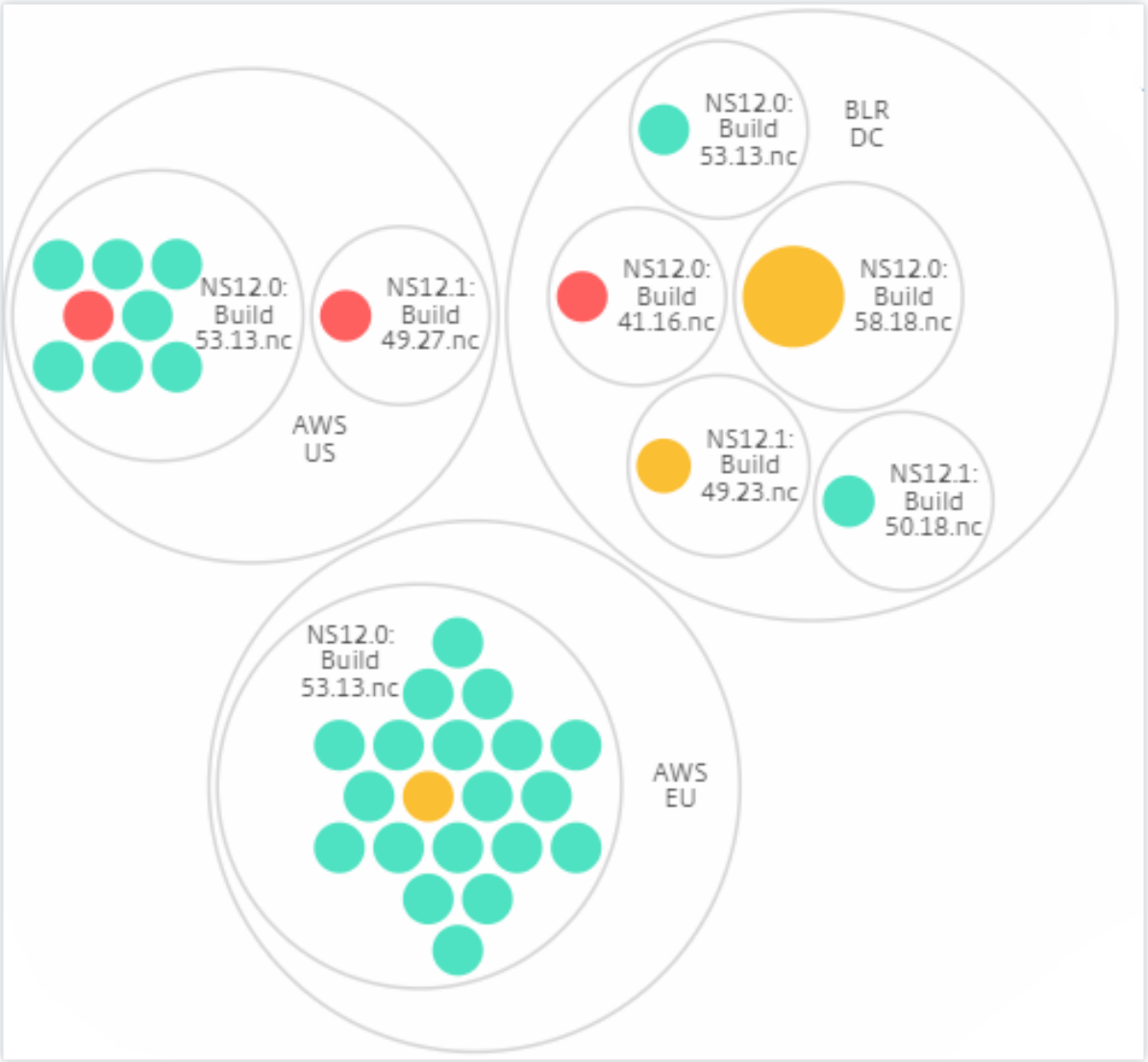
Type and version:

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



Site and version:

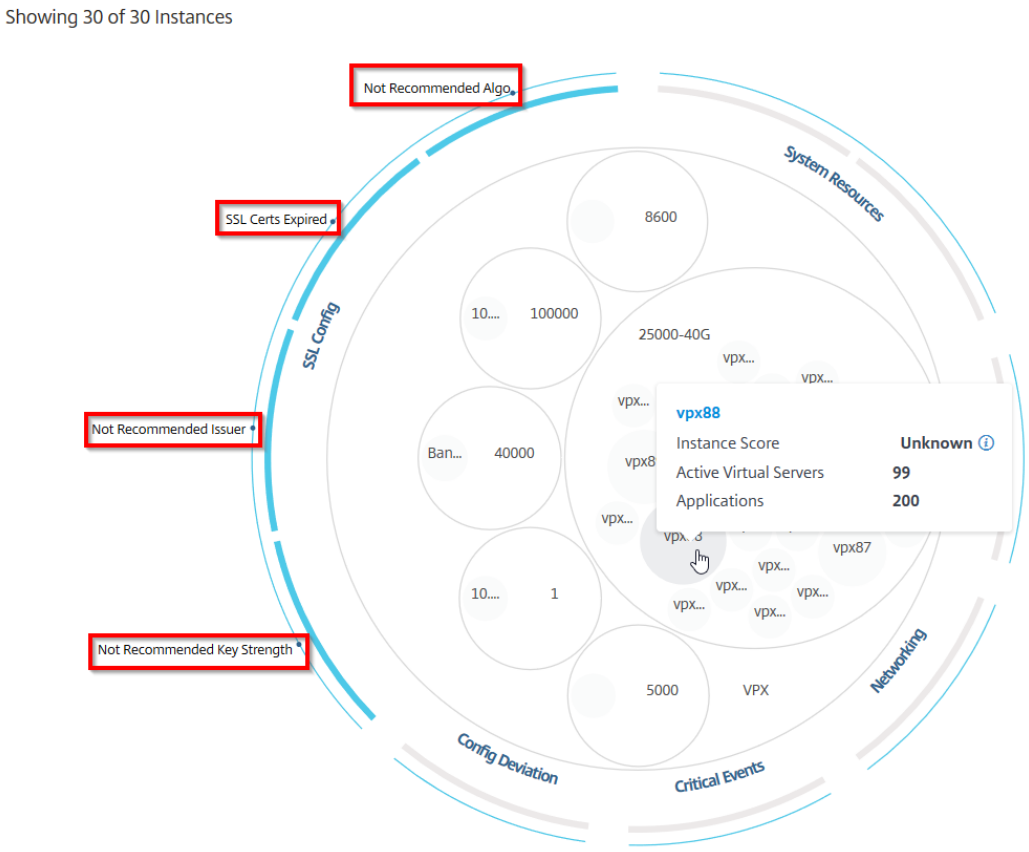
© 1997–2025 Citrix Systems, Inc. All rights reserved.



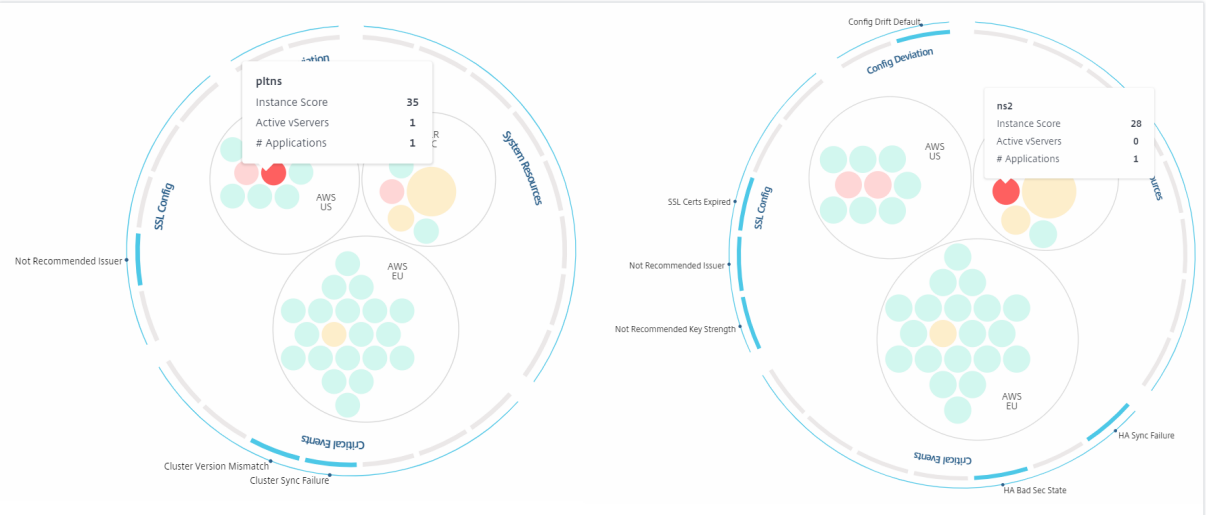
How to use Circle Pack

Click each of the colored circle to highlight that instance.

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

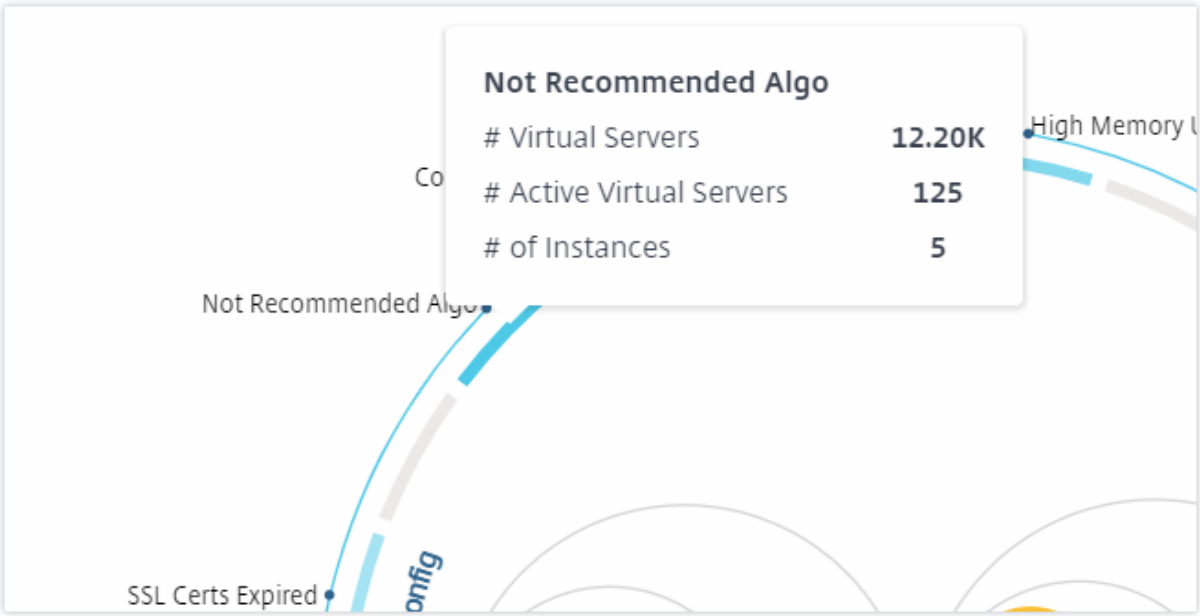


Depending on the events that have occurred in that instance, only those health indicators are highlighted on the outer circles. For example, the following two images of the Circle Pack display different sets of risk indicators, though both instances are in a critical state.



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.



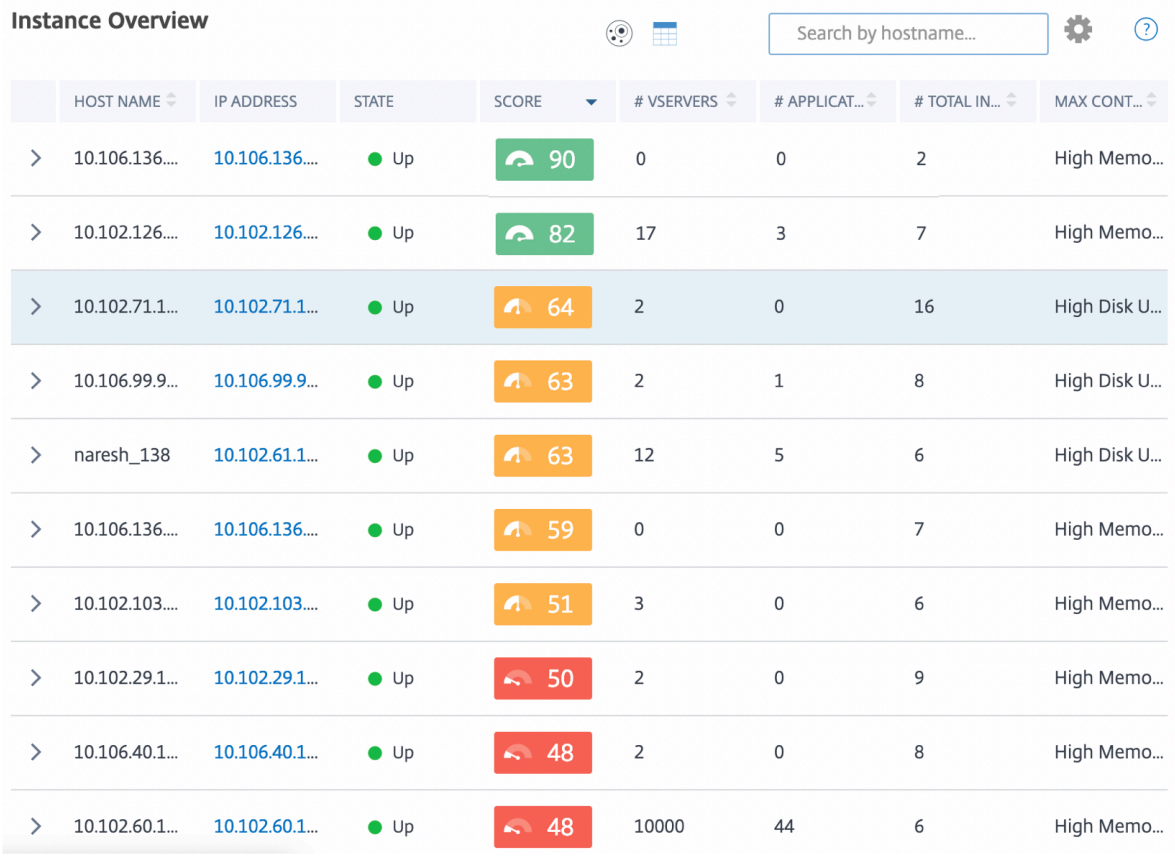
Tabular view

The tabular view displays the instances and the details of those instances in a tabular format. The details that are displayed are as follows:

- Host name of the instance
- The IP address of the instance
- State of the instance
- Instance score
- Number of virtual servers configured on that instance
- Number of applications configured on that instance
- Total number of risk indicators
- The event that is contributing more to a lowered instance score

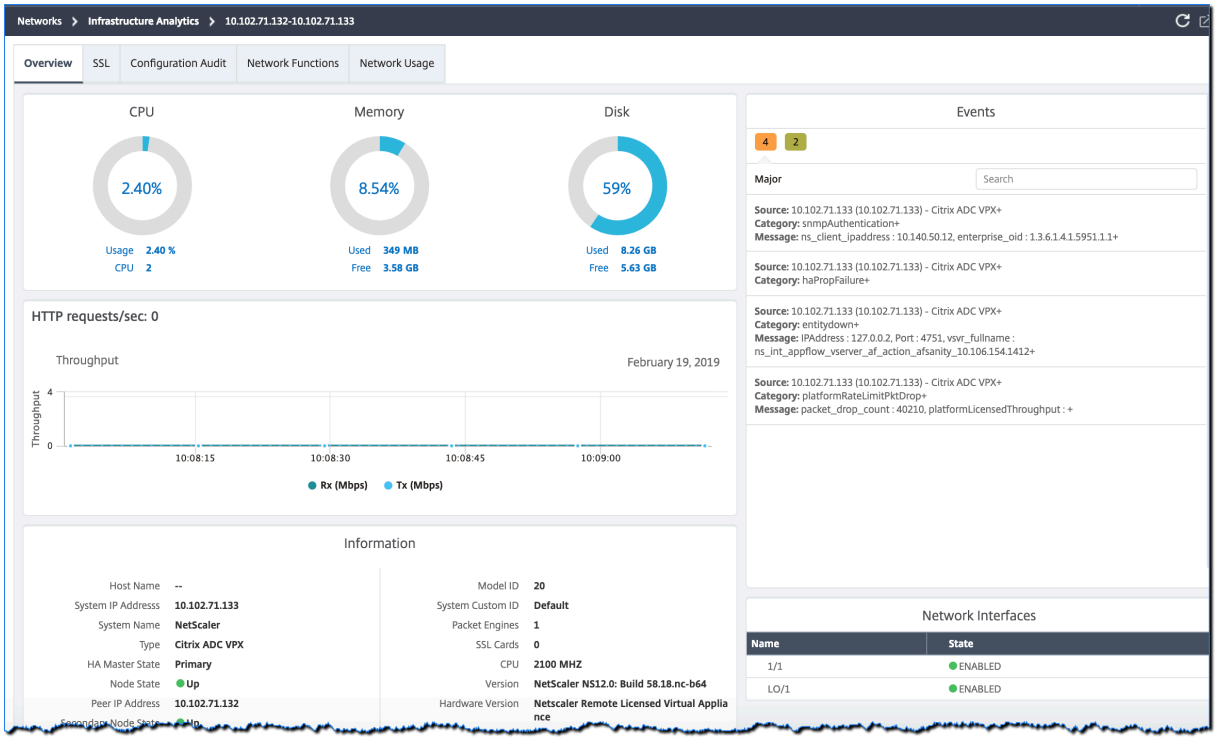
The instances that are in the critical state are at the top of the table, followed by the instances that need to be reviewed and then the healthier instances.

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

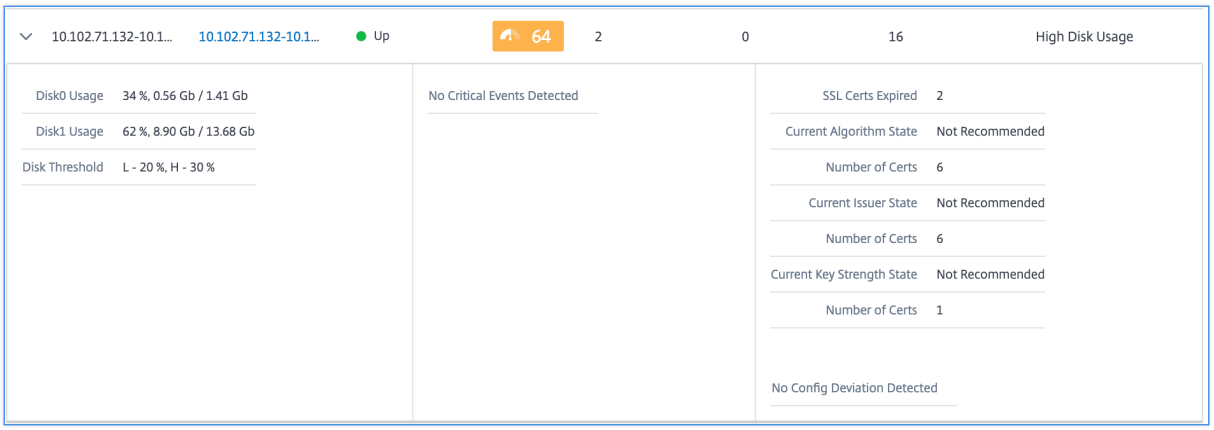


Click the instance IP address in the tabular view to see more details of that instance as a dashboard display. The instance dashboard presents an overview of the instance where you can see the CPU, memory, and the disk usage of the instance. You can also see details related to SSL certificate management, config audit, network functions, and a network report that shows detailed network usage of the instance. Scroll down further to see the list of the features and the modes enabled on this instance.

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



You can also click the arrow at the beginning of each row to expand the row for more details.



The expanded table row displays the errors that have occurred on the instance for all the categories. In the example above, you can view that there have been errors in system resources, SSL configuration, and deviations in configuration files. But there are no critical events reported from the instance.

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

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

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

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:

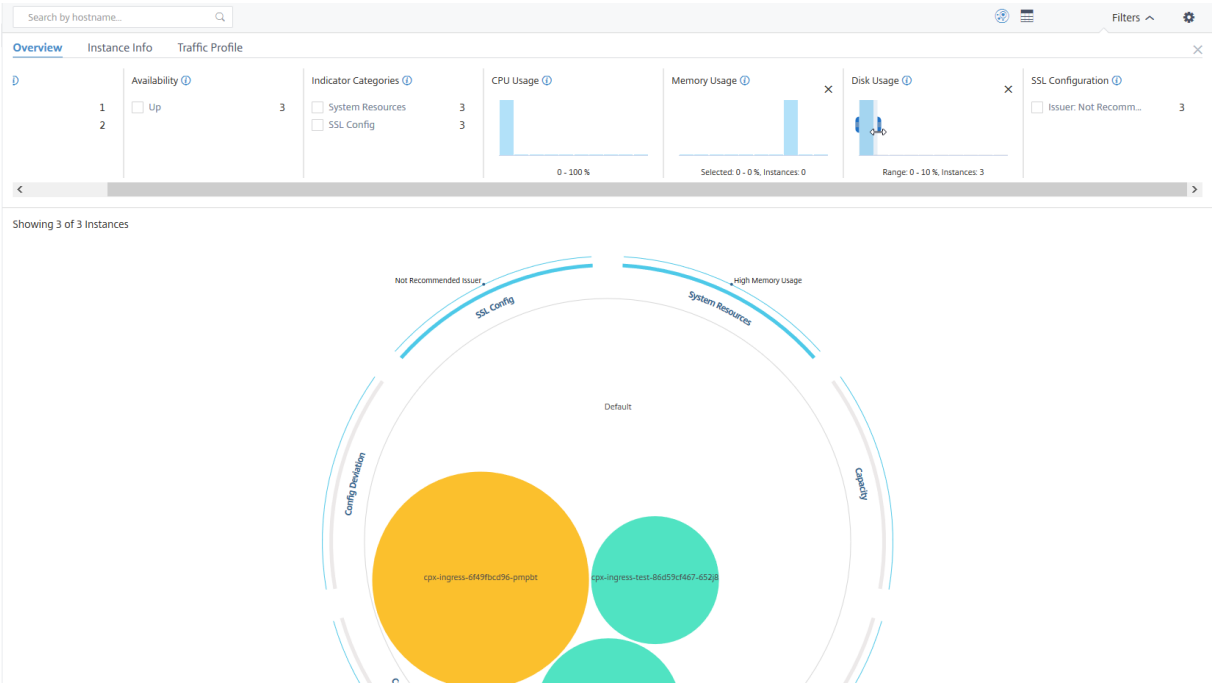
In the memory usage section, click the bar chart. The legend shows that the selected range is 10–20% and there are 29 instances operating in that range.

You can also select multiple ranges in these histograms.

Example 3: View instances that are consuming high disk space in multiple ranges:

To view instances that have consumed disk space between 0 and 10%, drag the mouse pointer over the two ranges.

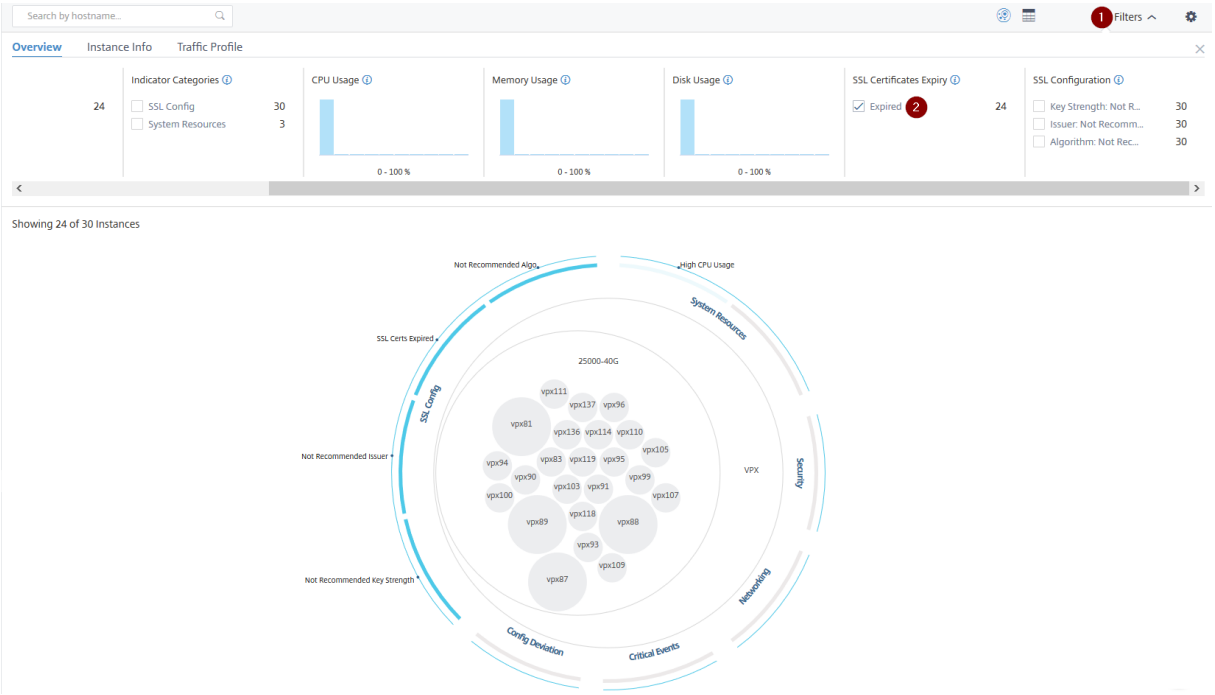
© 1997–2025 Citrix Systems, Inc. All rights reserved.



> **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:



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

1 - Click the **Filter** list.

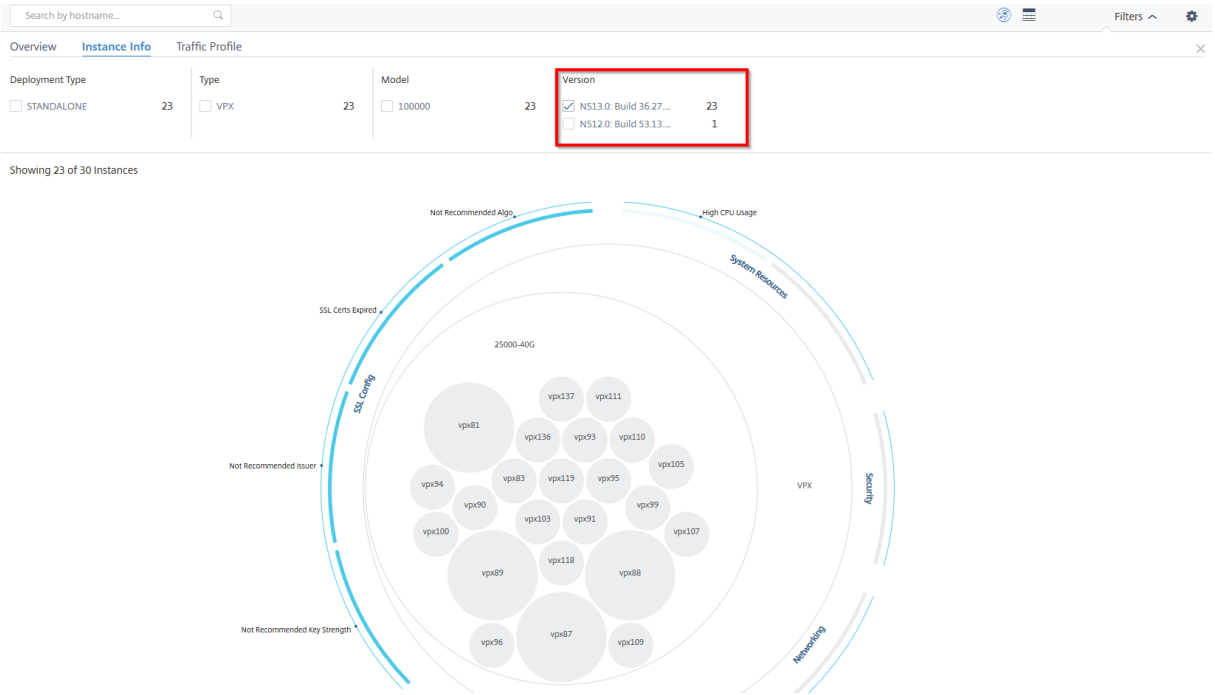
2 - In the **SSL certificates expiry** section, select **Expired** check box to view the instances.

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.



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.

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



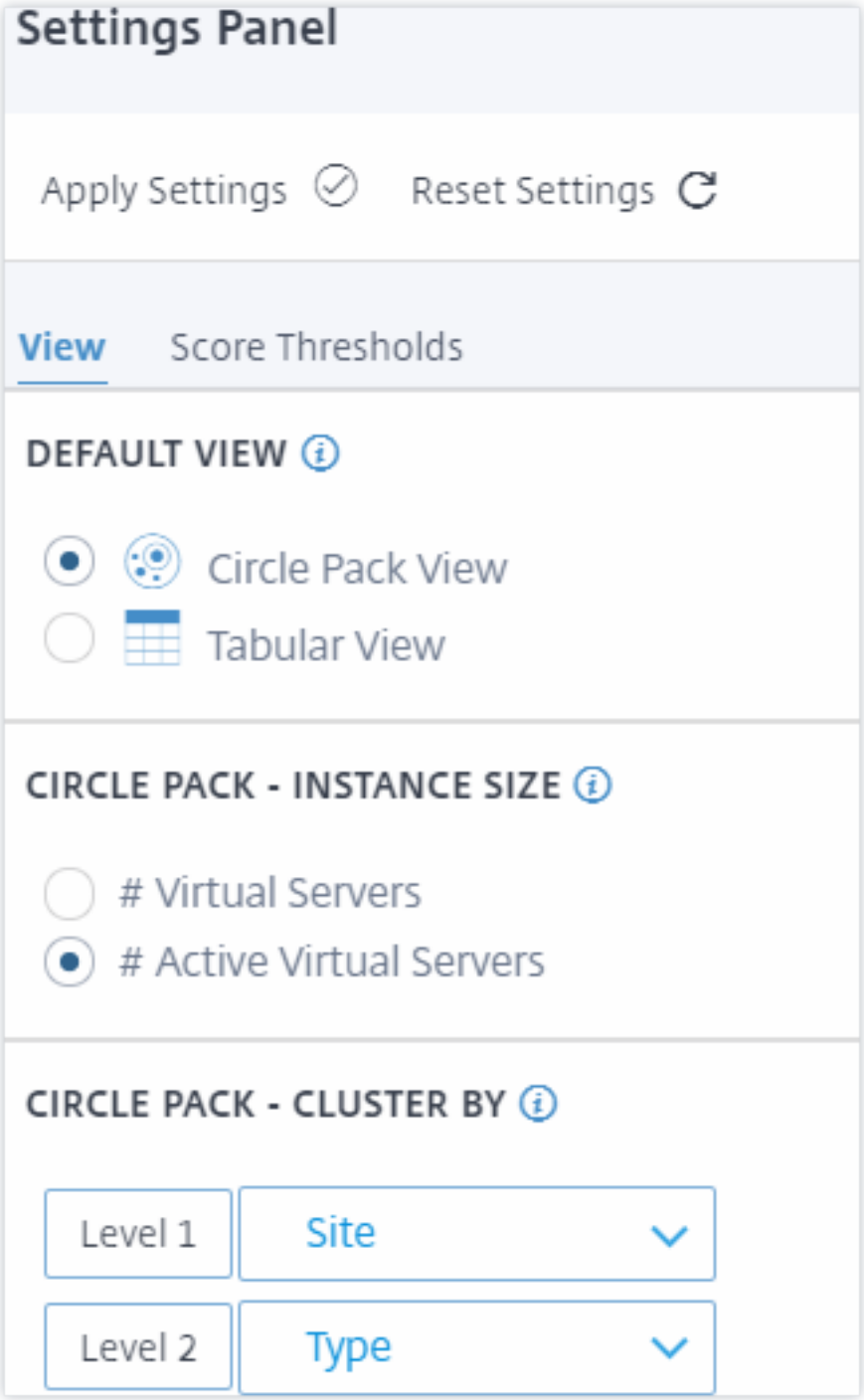
How to use the settings panel

The **Settings** panel allows you to set the default view of the Infrastructure Analytics. It also allows you to set the low and high threshold values for high CPU usage, high disk usage, and high memory usage. The settings panel is divided into two tabs - View and Score Thresholds.

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.

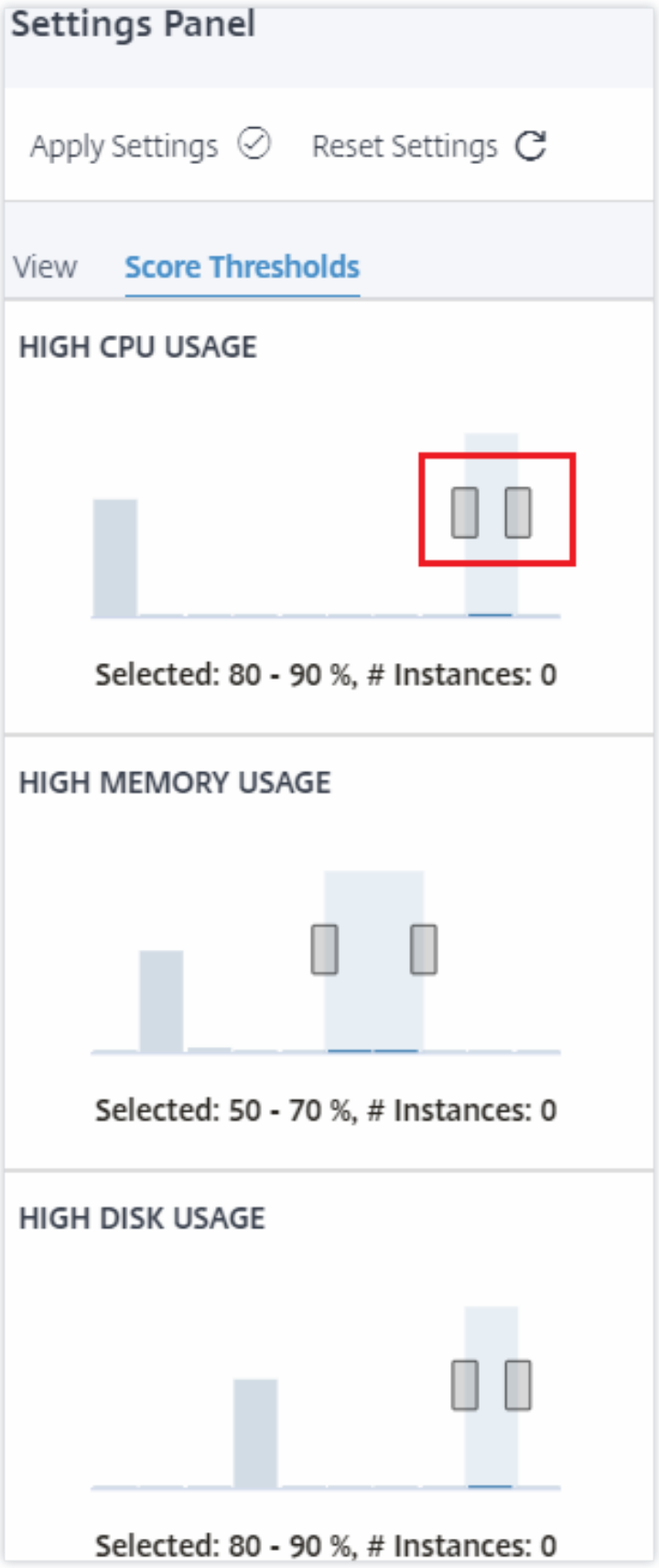
© 1997–2025 Citrix Systems, Inc. All rights reserved.



Score thresholds

You can modify the low and high threshold values for high CPU, memory, and disk usage depending on the traffic requirements in your organization. Drag the handles in each of the selection Histogram to set the values.

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



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

> **Note**
>
> Click **Apply Settings** to apply these changes, or click **Reset** to remove all changes.

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 data visualization in more detail, let us consider the case of Chris, a network admin of ExampleCompany.

Chris maintains many NetScaler instances in the organization. A few of the instances process high traffic, and Chris needs to monitor them closely. Chris notices that a few high-traffic instances are no longer processing the full traffic passing through them. To analyze this reduction, earlier, Chris had to read multiple data reports coming in from various sources. Chris had to spend more time trying to correlate the data manually and ascertain which instances are not in optimal state and need attention.

Chris 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. Chris clicks that instance to see what the issue is. The instance summary displays that there is an SSL card failure on that instance and the 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 Chris clicks the config deviation risk indicator, Chris 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. Chris also notices that the SSL transaction traffic profile for this instance has gone down. Chris exports this report and sends it to the admin to inquire further.

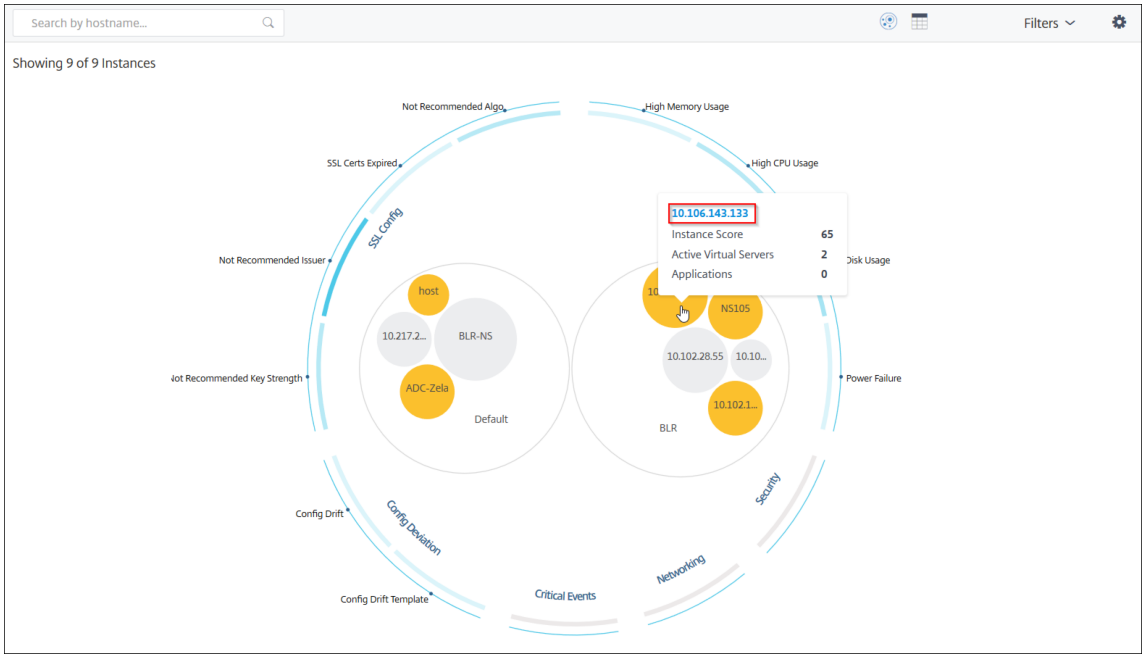
View instance details in Infrastructure Analytics

September 27, 2025

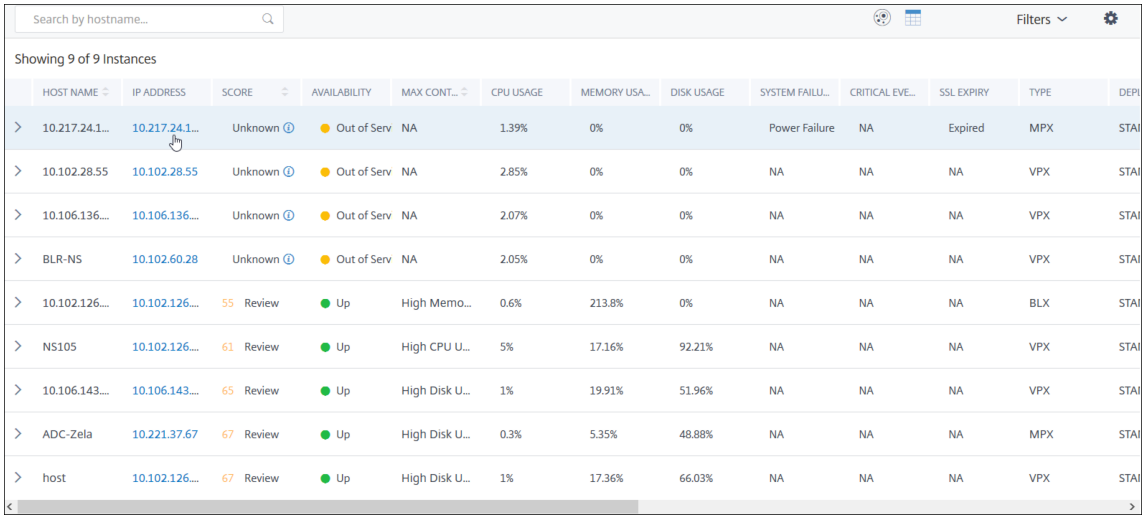
1. Navigate to **Infrastructure > Infrastructure Analytics**

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

2. Click the circle pack view and select the IP address.



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 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 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.

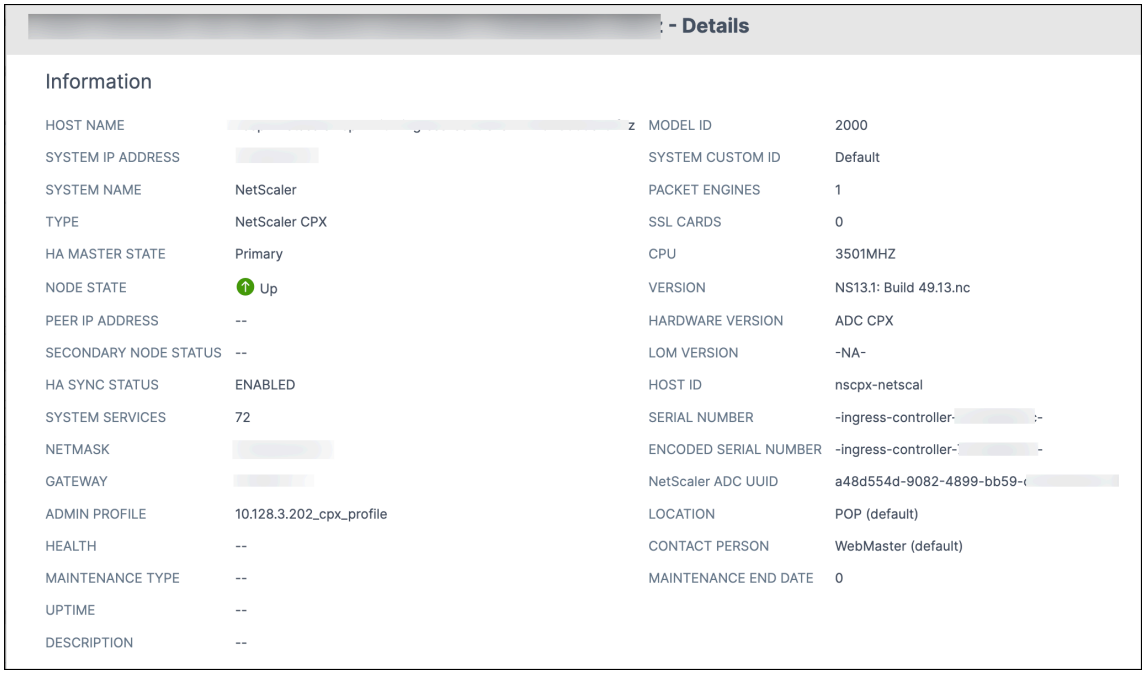
Click **Instance Details** to view the details.



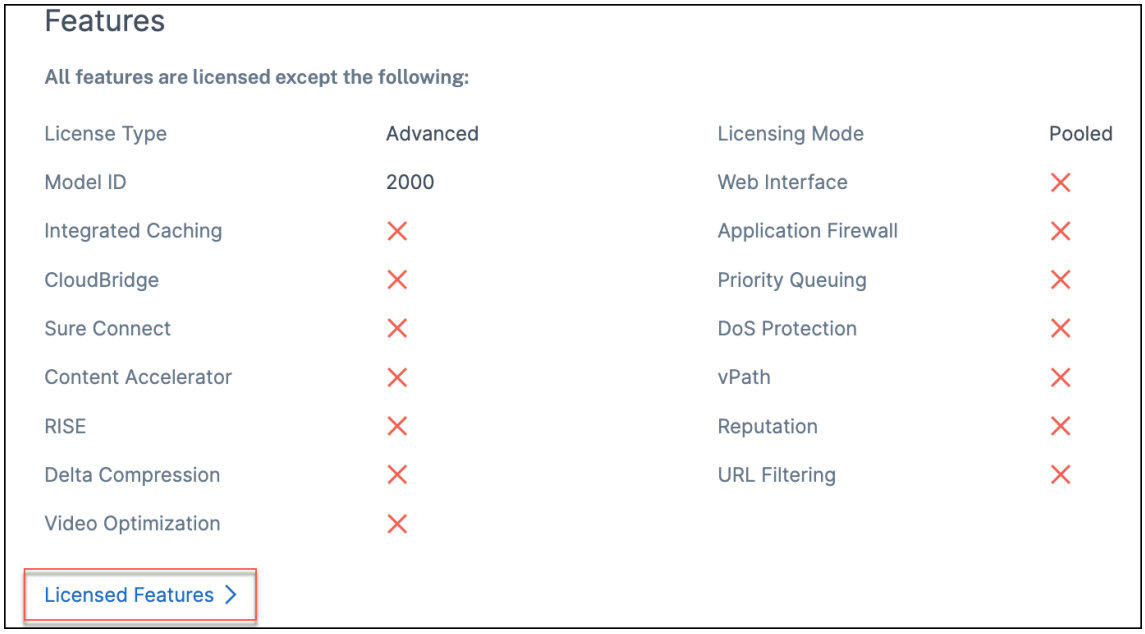
The following details are displayed:

- **Information** - Instance details such as instance type, deployment type, version, model.

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

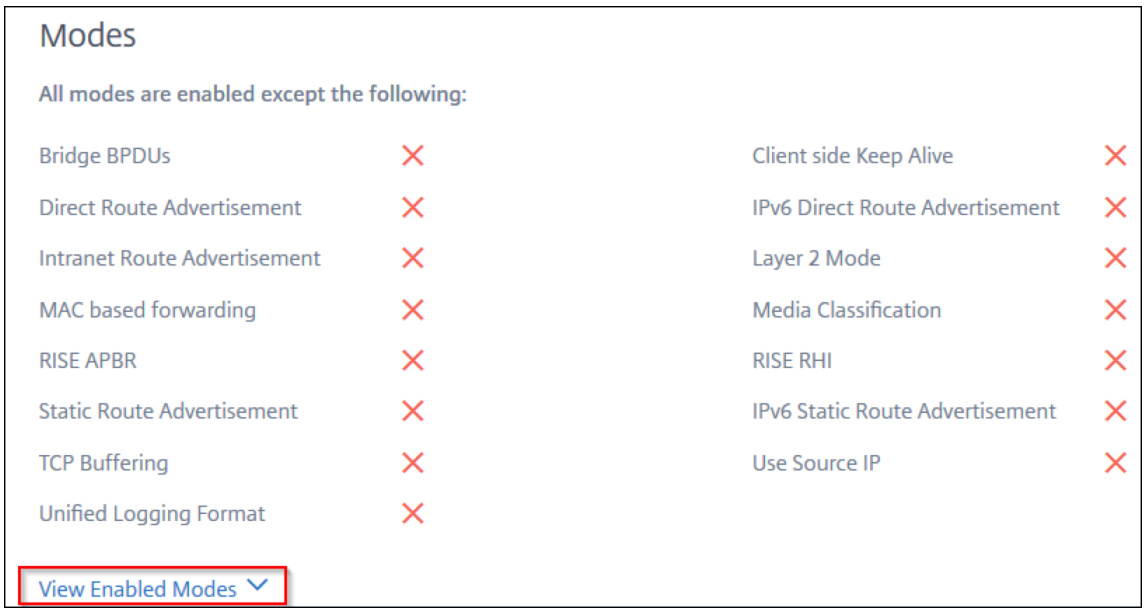


- **Features** –By default, the features that are not licensed are displayed. Click **Licensed Features** to view the features that are licensed.



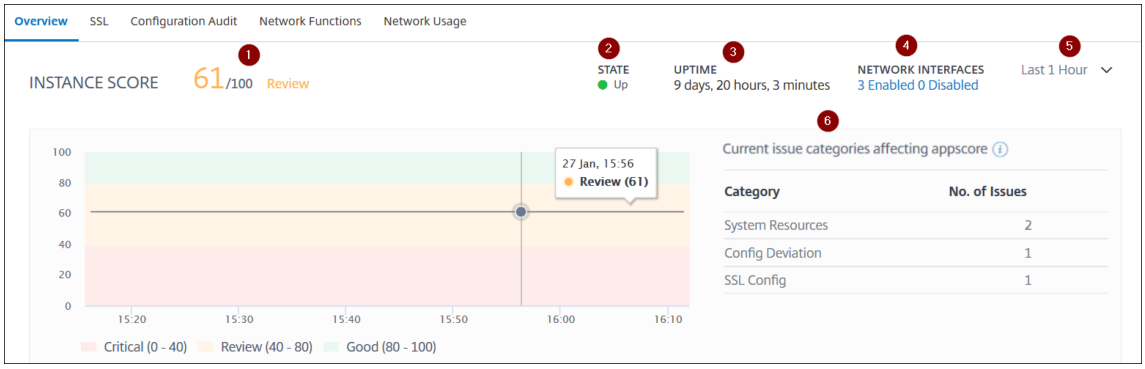
- **Modes** –By default, all modes that are disabled on the instance are displayed. Click **View Enabled Modes** to view the enabled modes on the instance.

© 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 status of the NetScaler instance, such as **Up**, **Down**, and **Out of Service**.

3 –Indicates the duration that the NetScaler instance is up and running.

4 –Indicates the total network interfaces enabled and disabled for the instance. Click to view the details such as network interface name and the status (enabled or disabled).

5 –Select the time duration from the list to view the instance details.

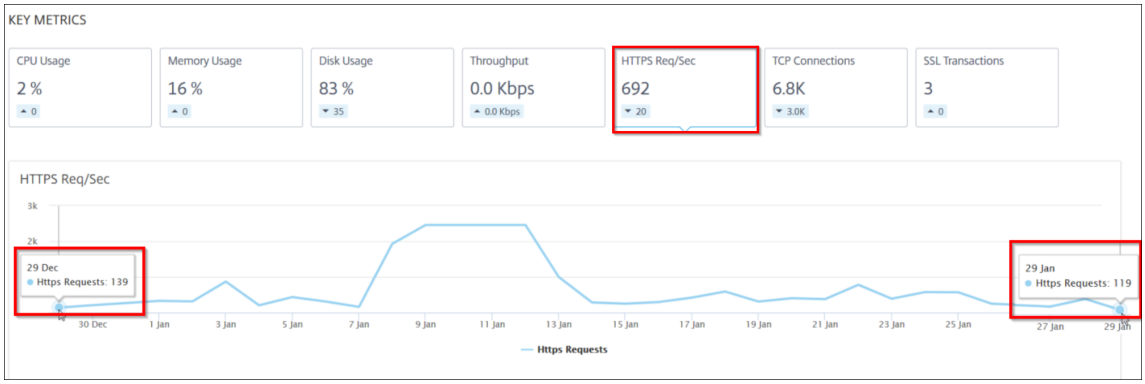
6 –Displays the total issues and issue category of the NetScaler instance.

- **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:

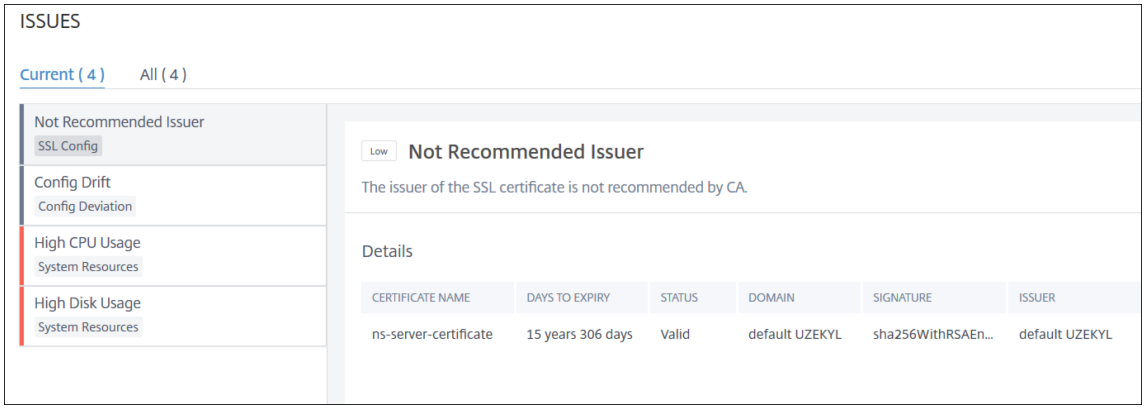
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Issue Category	Description	Issues
System Resources	Displays all issues related to the NetScaler system resource such as CPU, Memory, disk usage.	• 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 Algorithm • 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 Secondary State • HA No Heat Beats • HA Sync Failure

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

Issue Category	Description	Issues
Networking	Displays the operational issues that occur in the instances.	• HA Version Mismatch 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.

View the capacity issues in a NetScaler instance

September 27, 2025

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.

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

> **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:

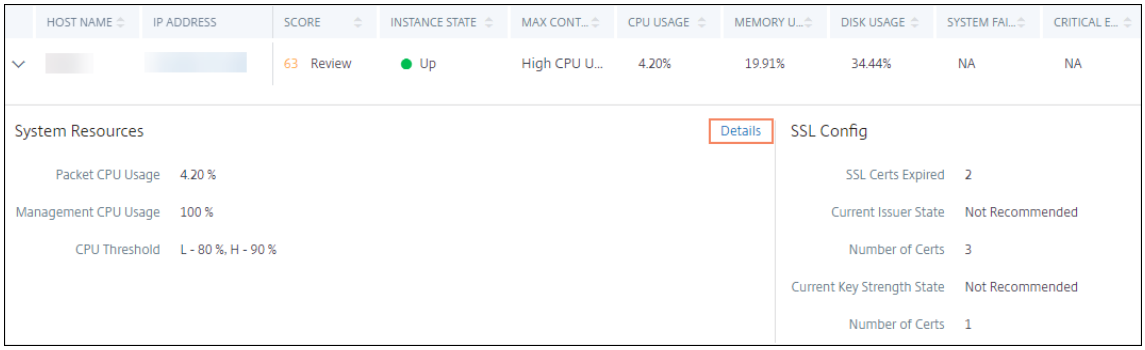
- **Throughput Limit Reached** –The number of packets dropped in the instance after the throughput limit is reached.
- **PE CPU Limit Reached** - The number of packets dropped on all NICs after the PE CPU limit is reached.
- **PPS Limit Reached** –The number of packets dropped in the instance after the 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

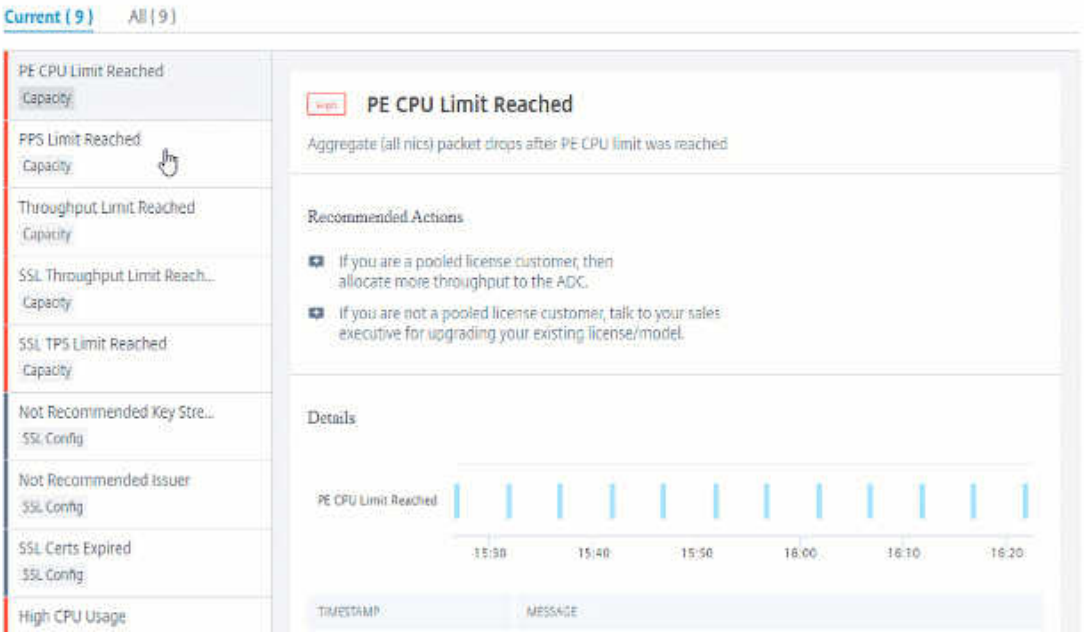
NetScaler Console recommends actions that can solve capacity issues. To view the recommended actions, perform the following steps:

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

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.



NetScaler Console polls these events every five minutes from the NetScaler instance and displays the packet drops or rate-limit counter increments if exists.

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 **Accounts > System Events**.

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

Enhanced Infrastructure Analytics with new indicators

September 27, 2025

Using the NetScaler Console Infrastructure Analytics, you can:

- View a new set of operational issues that occur in NetScaler instances.
- View error messages and check recommendations to troubleshoot the issues.

As an administrator, you can quickly identify the root cause analysis of issues.

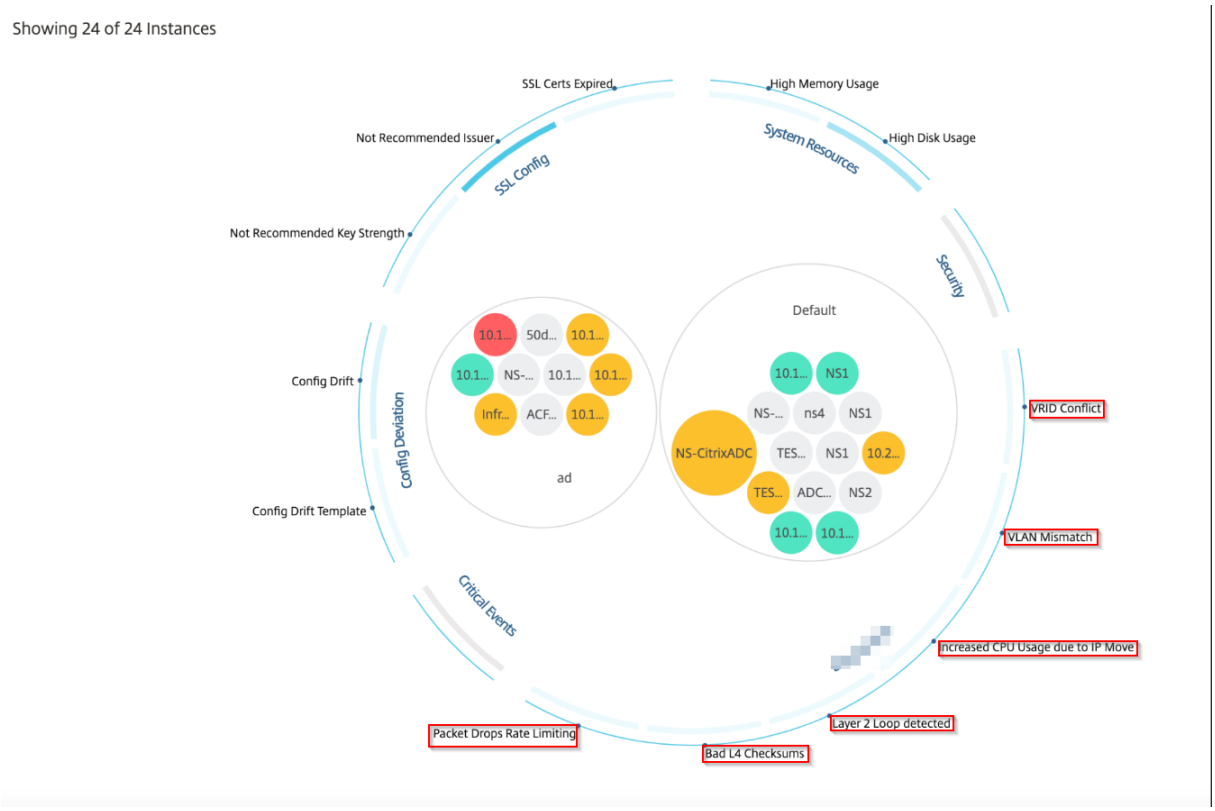
> **Note**
>
> Rule indicators are not supported for:
>
> - NetScaler instances configured in a cluster mode.
> - NetScaler instances configured with admin partitions.

In NetScaler Console, navigate to **Infrastructure > Infrastructure Analytics** to view indicators for:

Indicator name in Infrastructure Analytics	Description
Port allocation failure	Detects when NetScaler uses SNIP to communicate with a new server connection and total ports available on that SNIP are exhausted. The recommended action is to add another SNIP in the same subnet.
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.

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

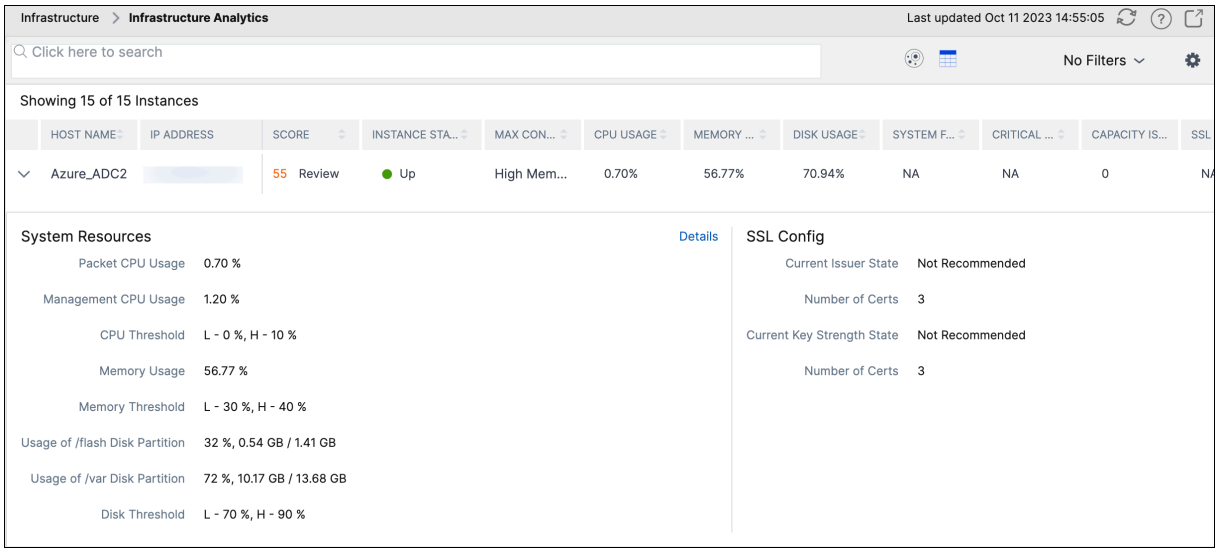
Indicator name in Infrastructure Analytics	Description
Persistence Limit	Detects when maximum hits are imposed on the NetScaler memory.
GSLB site name mismatch	Detects when GSLB configuration synchronization failures occur because of site name mismatch.
Malformed IP header	Detects when sanity checks on IPv4 packets are failed.
Bad L4 checksums	Detects when checksum validation for TCP packets is failed.
Increased CPU usage due to IP move	Detects if a large number of macs need to be updated.
Excessive packet steering	Detects high levels of software packet steering due to the usage of asymmetric rss key type.
Layer 2 loop	Detects the presence of layer 2 loops in the network.
Tagged VLAN mismatch	Detects when tagged VLAN packets are received on an untagged interface.



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

Tabular view

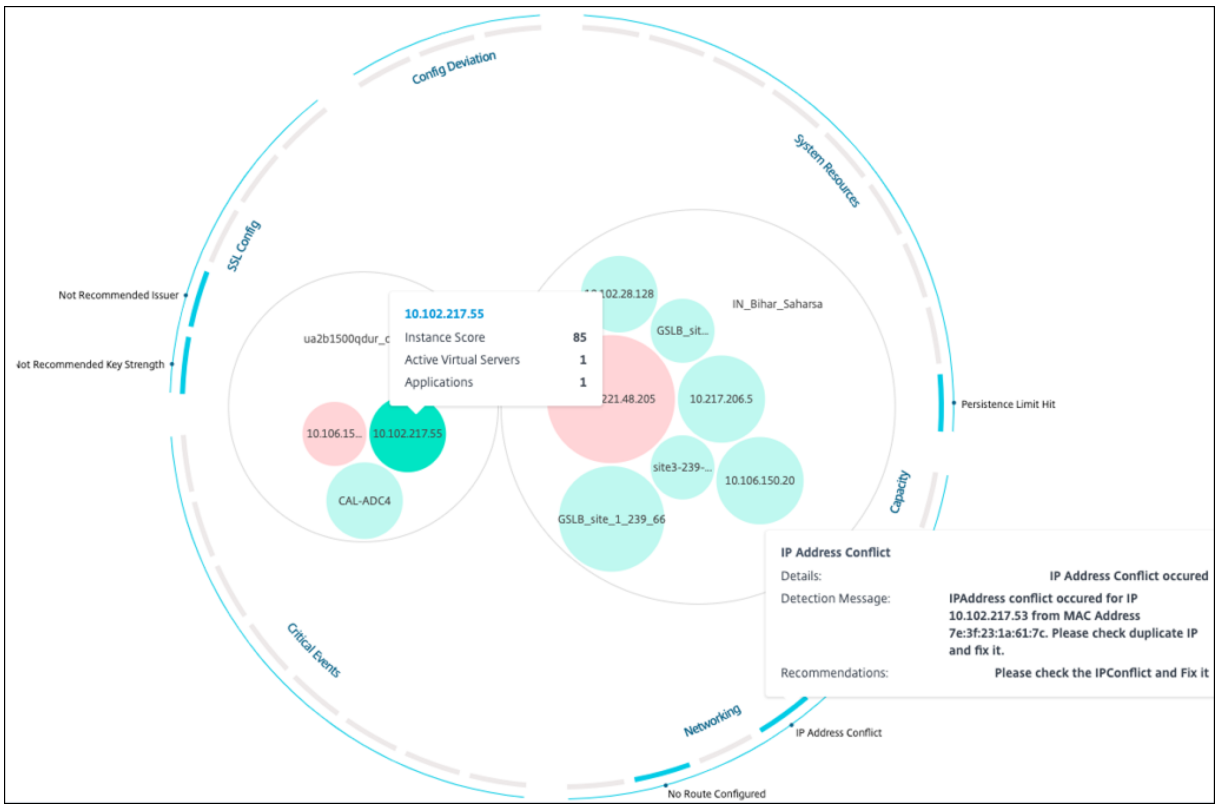
You can also view anomalies using the tabular view option in **Infrastructure Analytics**. Navigate to **Infrastructure > Infrastructure Analytics** and then click  to display all managed instances. Click to expand for details.



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 to view the details.

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



- **Details** - Indicates what anomaly is detected
- **Detection Message** - Indicates the MAC address for which the IP address has the conflict
- **Recommendations** - Indicates the action item to resolve this IP address conflict

Instance management

September 27, 2025

Instances are Citrix NetScaler appliances that you can manage, monitor, and troubleshoot using NetScaler Console. You must add instances to NetScaler Console to monitor them. Instances can be added when you set up NetScaler Console or later. 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 so on. A private IP-block groups your instances based on their geographical locations.

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

Add an instance

You can add instances either while setting up the NetScaler Console server for the first time or later. To add instances, you must specify either the host name or IP address of each NetScaler instance, or a range of IP addresses.

To learn how to add an instance to NetScaler Console, see Add Instances to NetScaler Console.

When you add an instance to the NetScaler Console server, the server implicitly adds itself as a trap destination for the instance and collects 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 click **All Instances**. On the Instances page, select the instance you want to delete and click **Remove**.

How to use the instance dashboard

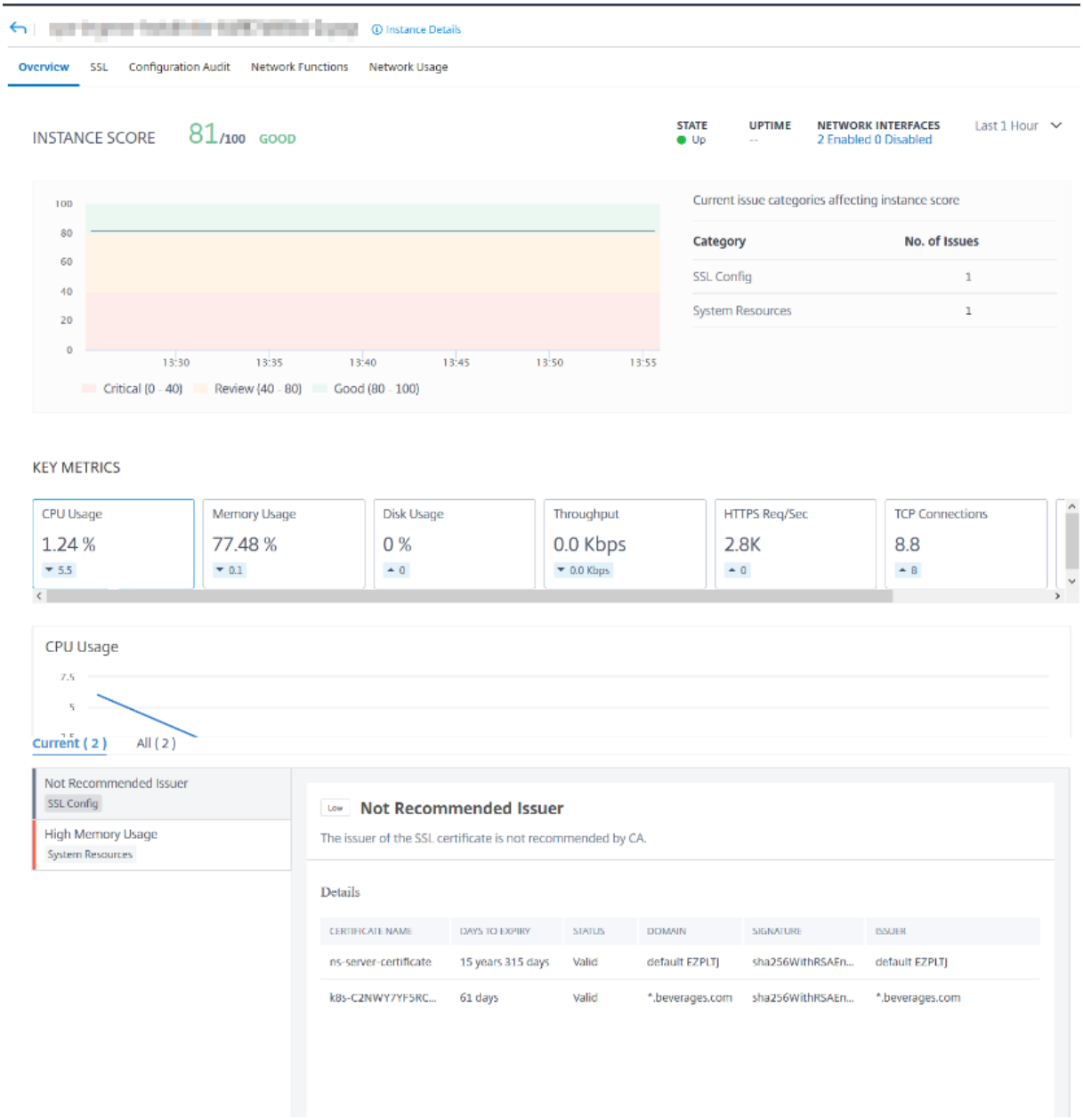
The per-instance dashboard in NetScaler Console displays data in a tabular and graphical format for the selected instance. Data collected from your instance during the polling process is displayed on the dashboard.

By default, every minute, managed instances are polled for data collection. Statistical information such as state, the HTTP requests per second, CPU usage, memory usage, and throughput are continuously collected using NITRO calls. As an administrator, you can view all this collected data on a single page, identify issues in the instance, and take immediate action to rectify them.

To view a specific instance's dashboard, navigate to **Infrastructure > Instances**. From the summary, choose the instance type and then, select the instance you want to view and click **Dashboard**.

The following illustration provides an overview of the various data that is displayed on the per-instance dashboard:

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



- **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 so on is 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.

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

- **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 additional performance report.

Monitor globally distributed sites

September 27, 2025

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 section explains how you can monitor data centers in NetScaler Console.

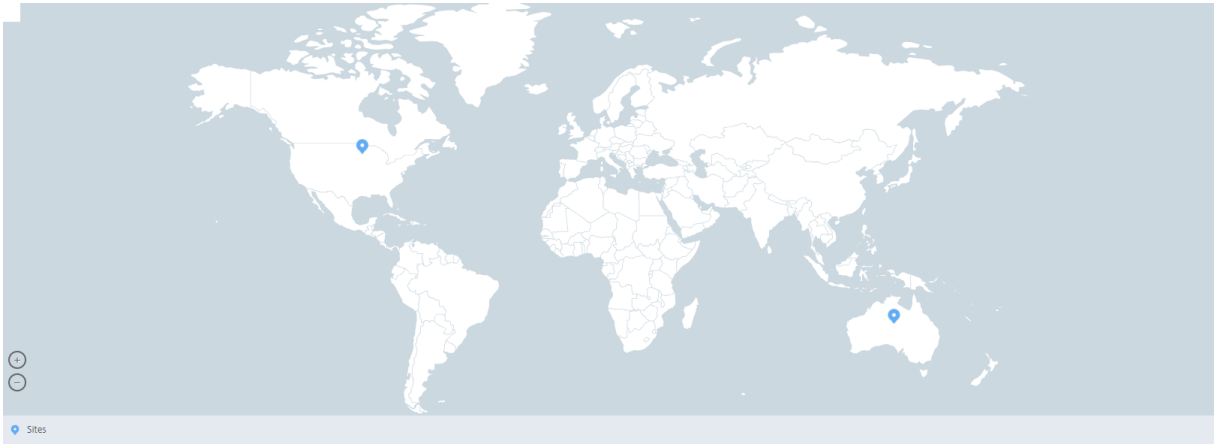
NetScaler Console site is a logical grouping of Citrix NetScaler instances in a specific geographical location. For example, while one site is assigned to Amazon Web Services (AWS) and another site might be assigned to Azure. Still another site is hosted on the premises of the tenant. NetScaler Console 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 navigate to **Infrastructure > Instances** page for a visual representation of the sites created on the world map.

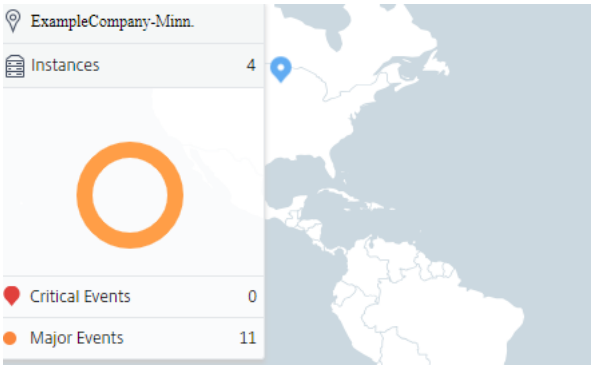
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Use case

A leading mobile carrier company, ExampleCompany, was relying on private service providers for hosting their resources and applications. The company already had two sites - one at Minneapolis in the United States and another in Alice Springs in Australia. In this image, you can see that two markers represent the two existing sites.



The markers also display a number, which shows the number of applications in each site. You can click these markers for more information about each site.



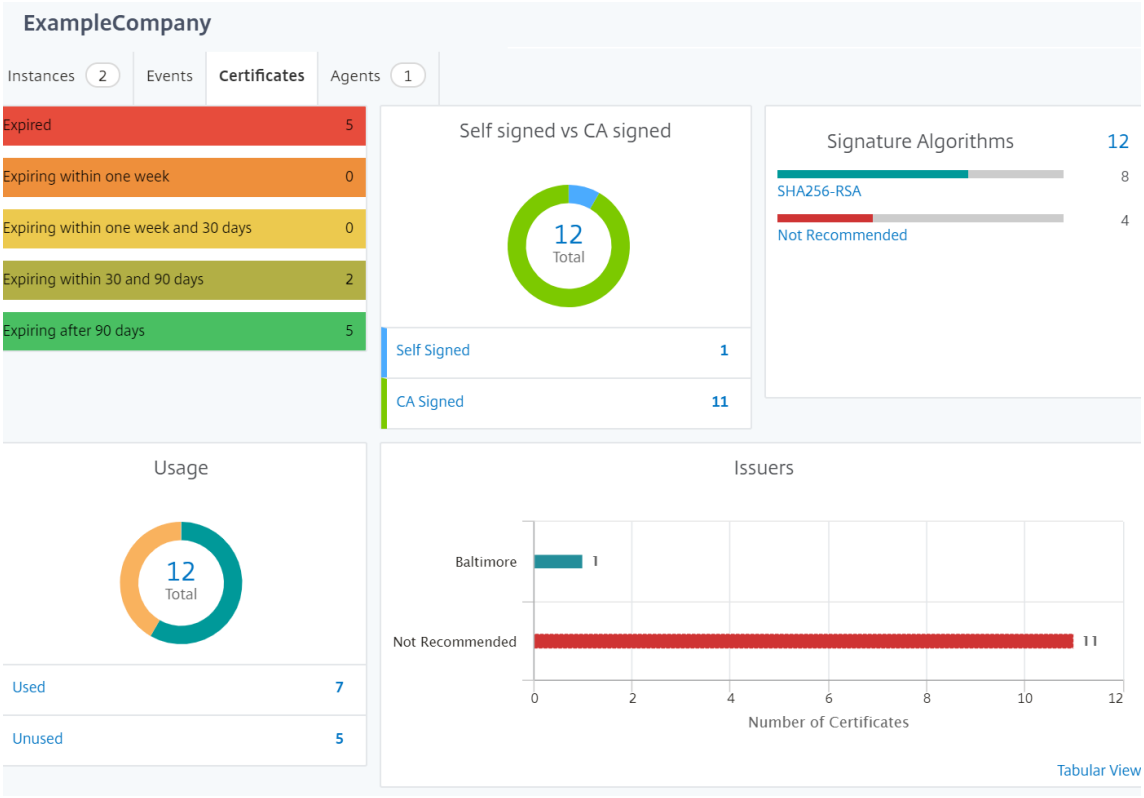
Click the tabs to view more information:

- **Instances** tab: View the following in this tab:
  - IP address of each network instance
  - Type of the instance
  - Number of critical events on them
  - 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:

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

- 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.



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.

To create sites:

Create sites before you add instances in NetScaler Console. Providing location information allows you to locate the site precisely.

Navigate to **Infrastucture > Instances > Sites**, and then click **Add**.

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

1. In the **Create Site** page, specify the following information:

   a) **Site Type**: Select **Data Center**.

   > **Note**
   >
   > The site can function as the primary data center or as a branch. Choose accordingly.

   b) **Type**: Select AWS as the cloud provider from the list.

   > **Note**
   >
   > Check the **Use existing VPC as a site** box accordingly.

   c) **Site Name**: Type the name of the site.

   d) **City**: Type the city.

   e) **Zip Code**: Type the Zip Code.

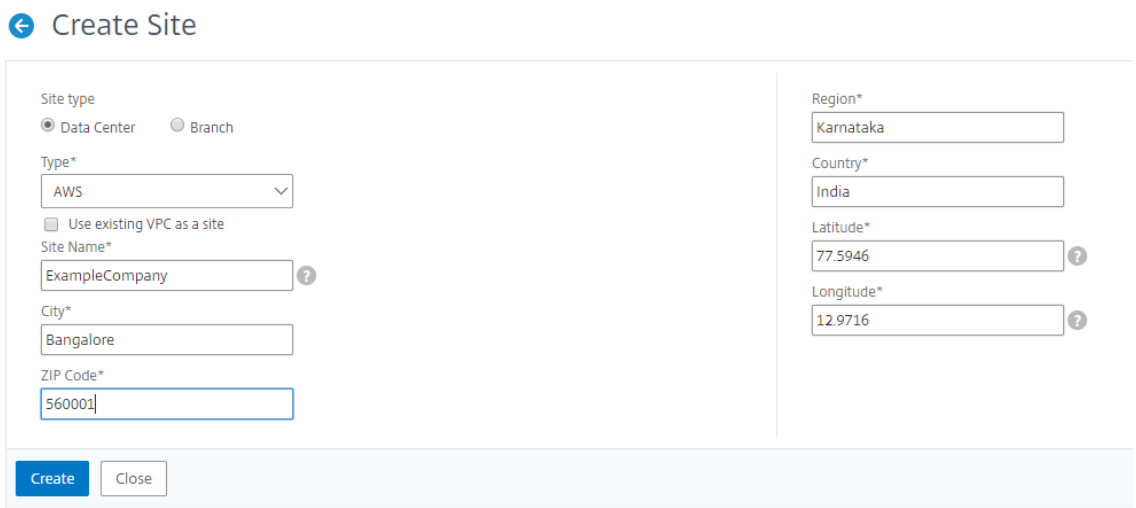
   f) **Region**: Type the Region.

   g) **Country**: Type the Country

   h) **Latitude**: Type the latitude of the location.

   i) **Longitude**: Type the longitude of the location.

2. Click **Create**.



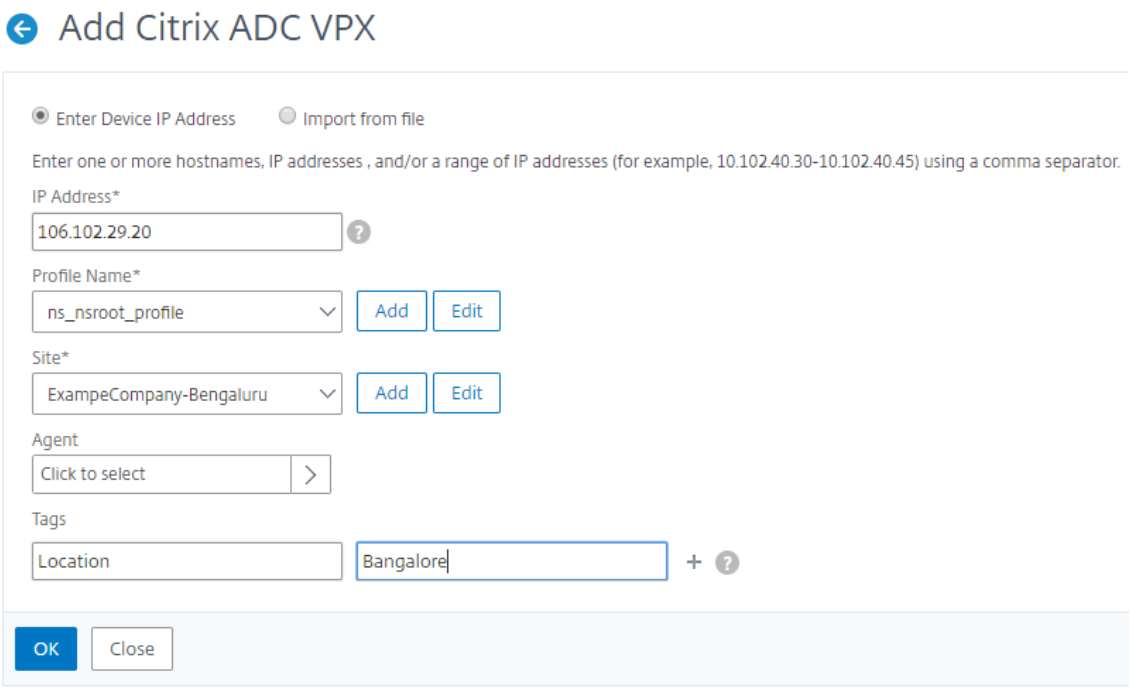
To add instances and select sites:

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.

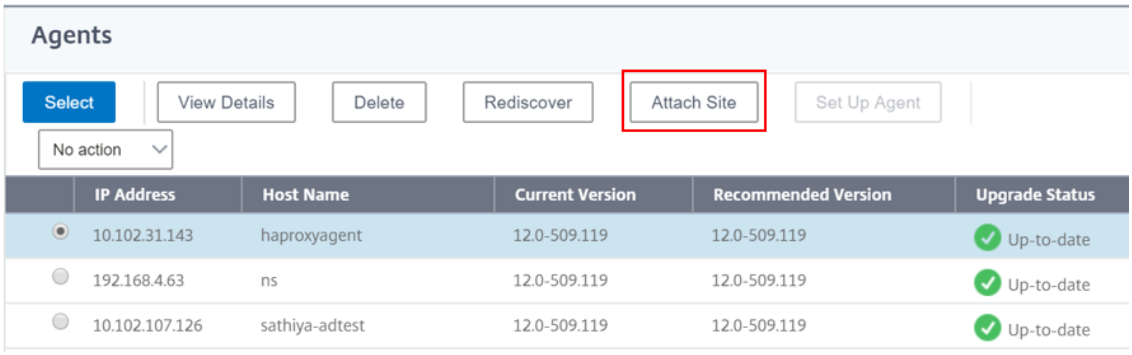
After creating sites, you must add instances in NetScaler Console. You can select the previously created site, or you can also create a site and associate the instance.

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

1. In NetScaler Console, navigate to **Infrastructure > Instances**.
2. Select the type of instance you want to create, 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 + sign next to **Site** field to create a site or click the edit icon to change the details of the default site.
5. Click the right arrow and select the agent from the list that displays.



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**.



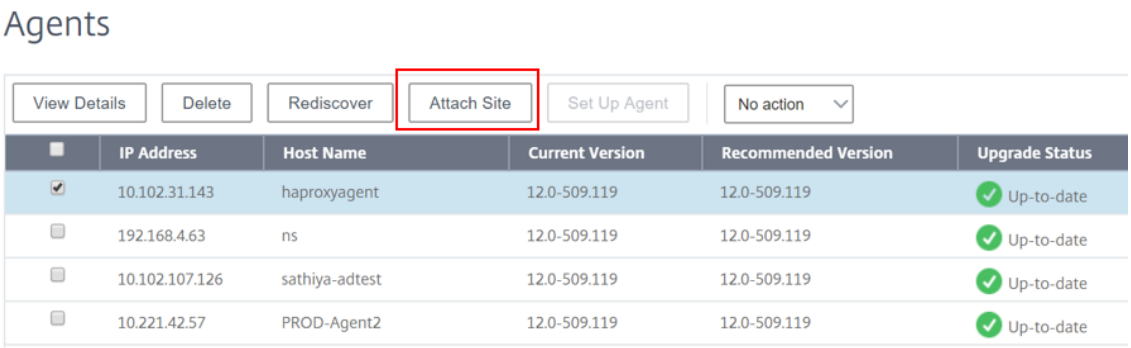
1. Select the site from the list and click **Save**.
1. Click **OK**.

You can also attach an agent to a site by navigating to **Infrastructure > Instances > Agents**.

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

To associate a NetScaler agent with the site:

1. In NetScaler Console, navigate to **Infrastructure > Instances > Agents**.
2. Select the agent, and click **Attach Site**.



1. You can associate the site and click **Save**.

NetScaler Console starts monitoring the NetScaler instances added in Bangalore site along with the instances at the other two sites as well.

How to create tags and assign to instances

September 27, 2025

NetScaler Console now allows you to associate your Citrix 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 helps you to better monitor them.

- **Use case 1**: You can create a tag to identify all instances 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 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 the value as "Staging_NS."This tag helps you to segregate all instances that are being used in the staging environment from the instances that have client requests running through them.

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

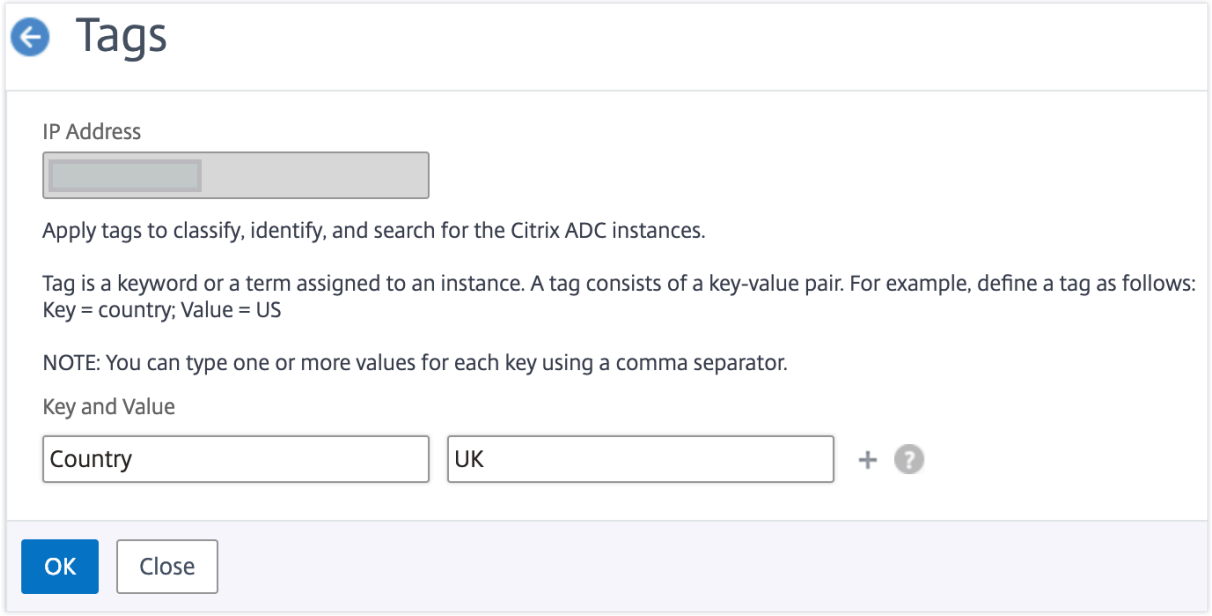
- **Use case 3**: Consider a situation where you want to find out the list of NetScaler instances that are in "Swindon"area in the UK and owned by you, David T. You can create tags for all these requirements and assign that to all the instances that satisfy these conditions.

To assign tags to NetScaler VPX instance:

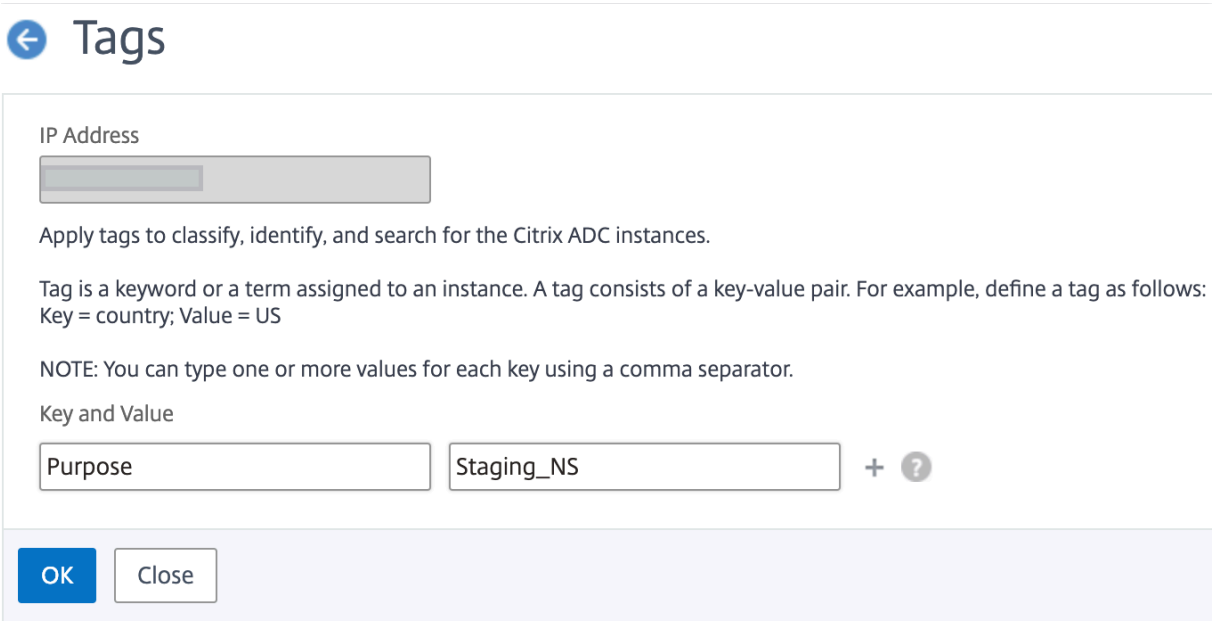
1. In NetScaler Console, navigate to **Infrastructure > Instances > NetScaler**.
2. Select the **NetScaler VPX** tab.
3. Select the required NetScaler VPX.
4. Click **Tags**.
5. Create tags and click **OK**.

The **Tags** window that appears allows you to create your own "key-value"pairs by assigning values to every keyword that you create.

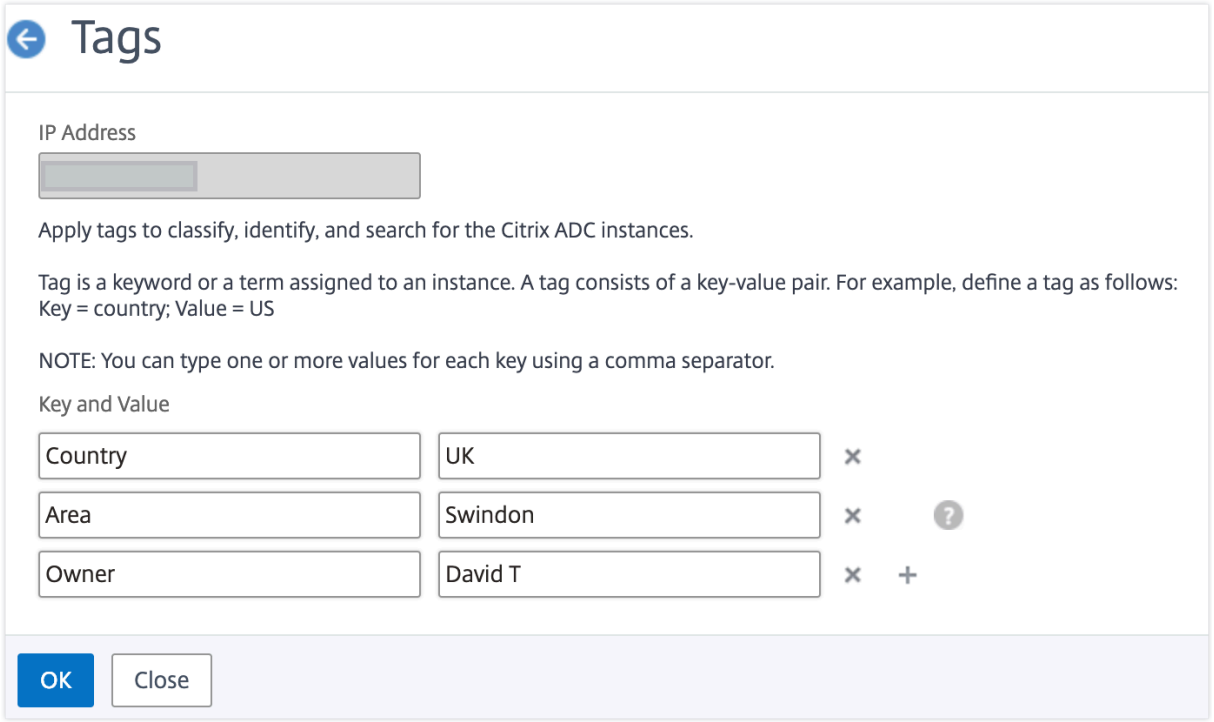
For example, the following images show a few keywords created and their values. You can add your own keywords and type a value for each keyword.



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



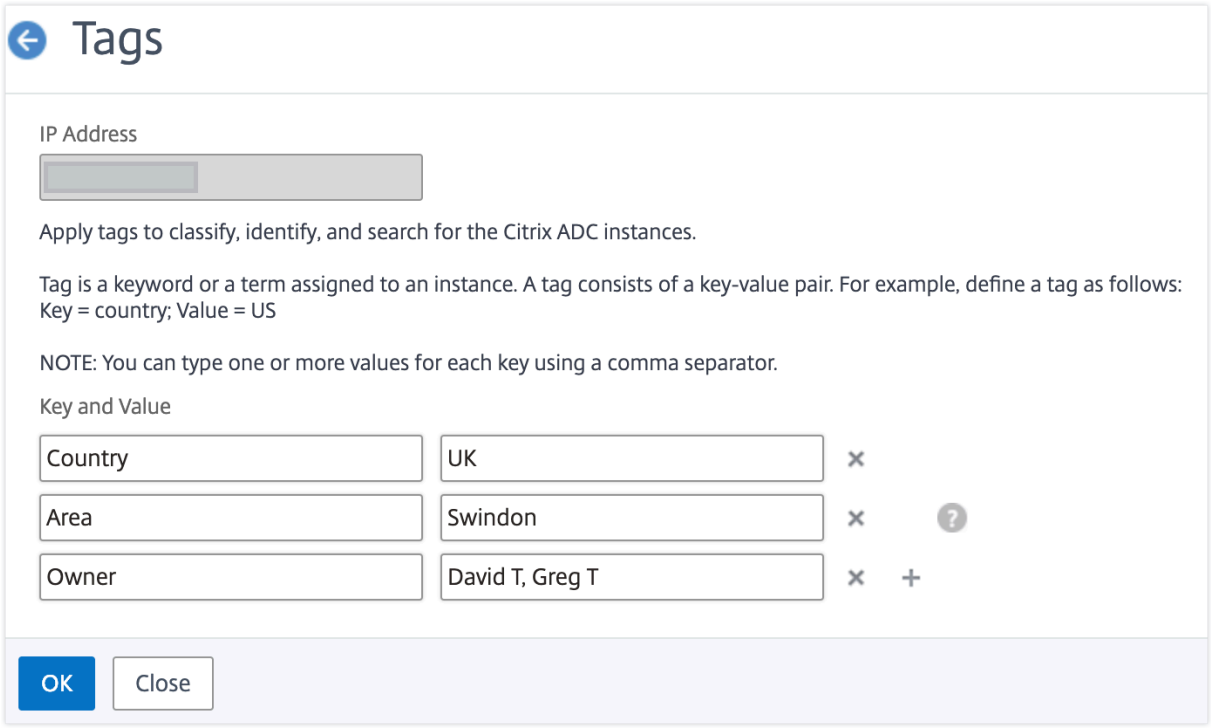
You can also add multiple tags by clicking "+."Adding multiple and meaningful tags allows you to efficiently search for the instances.



You can add multiple values to a keyword by separating them with commas.

For example, you are assigning 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.

> **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

September 27, 2025

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 you can assign 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.

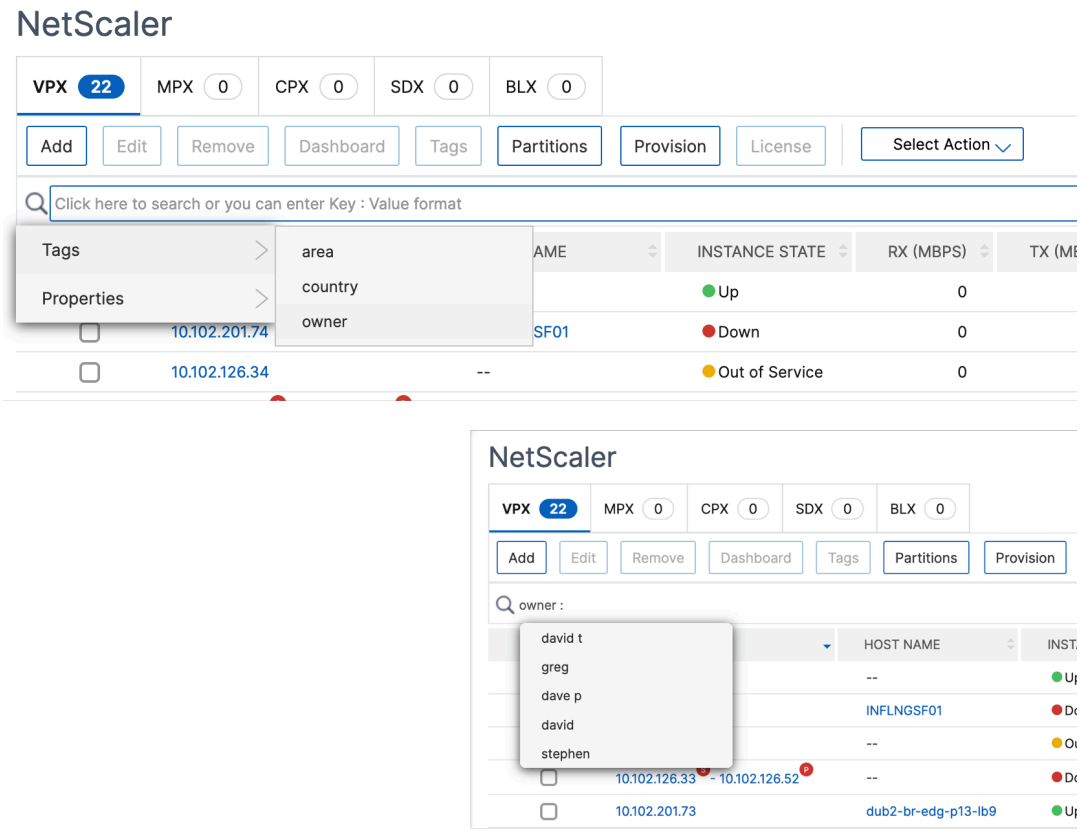
To search for NetScaler VPX instances

1. In NetScaler Console, navigate to **Infrastructure > Instances > NetScaler** > **VPX** tab.
2. 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.

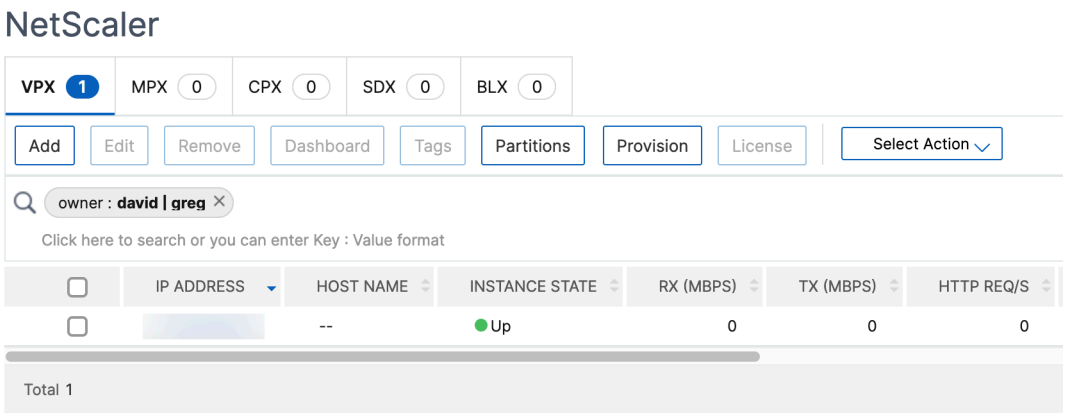
   a) Select **Tags** option and select **Owner**. Select "David T."

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



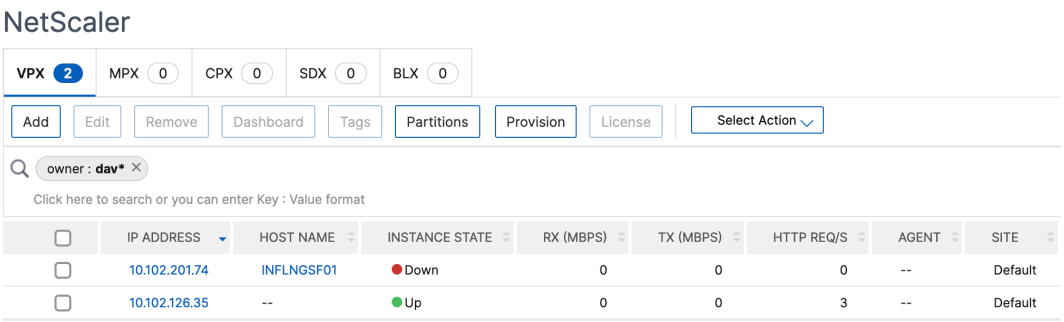
NetScaler Console supports regular expressions and wildcard characters in the search expressions.

b) 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.



c) 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 T 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

September 27, 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.

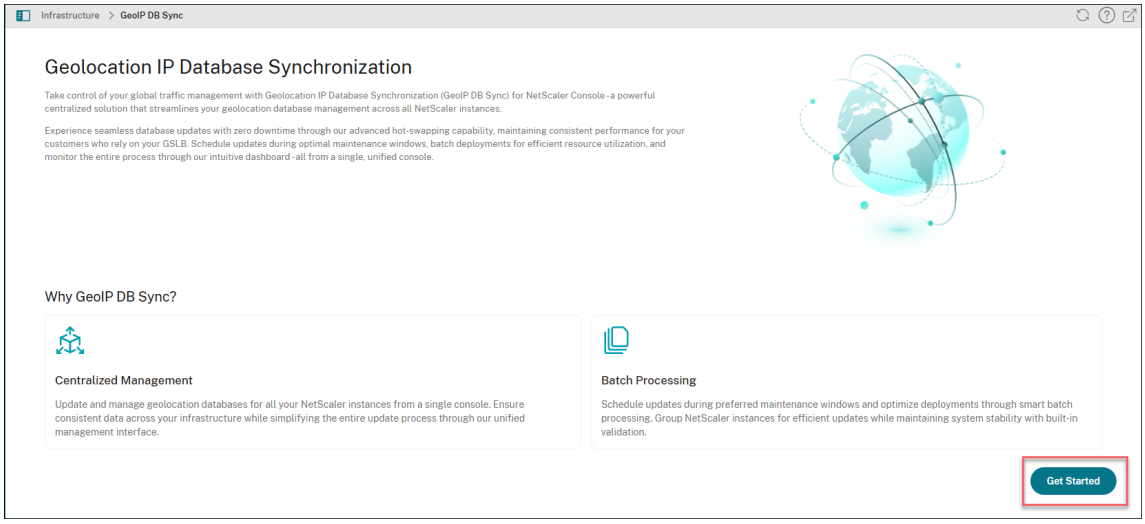
Configuring centralized GeoIP DB Updates through NetScaler Console

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:
   - **Upload a new file**: You can upload a file from your local system.
   - **Use an existing file**: You can choose a file that is already present on a NetScaler Console.

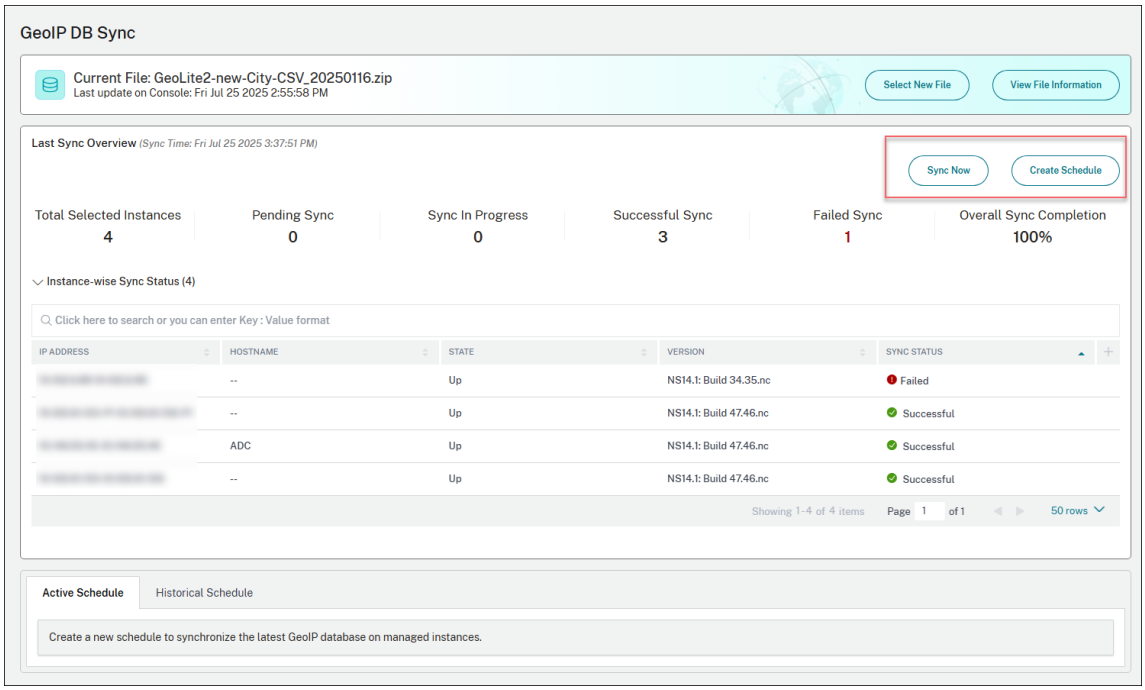
> **Notes:**
>
> - If you are uploading the GeoIP DB file for the first time, you do not see the **Use an existing file** option. Only if the file is already uploaded, then the **Use an existing file** option appears during subsequent uploads.
> - If you upload a MaxMind file, the NetScaler Console service 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.

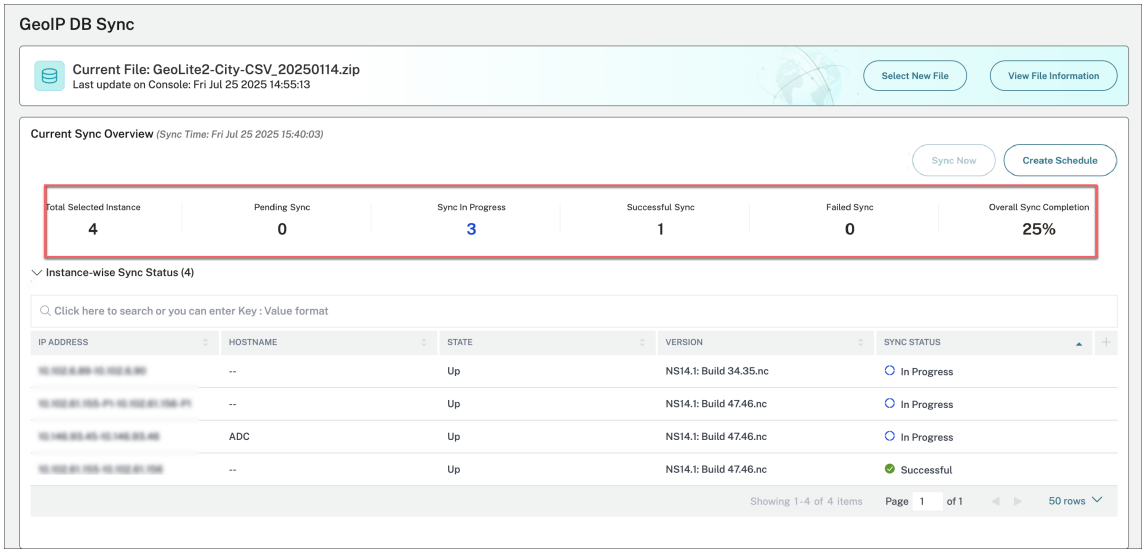
> file from other providers, then it must in CSV format and adhere to the following field order recommended by NetScaler: IP range, country code, region, city.

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.



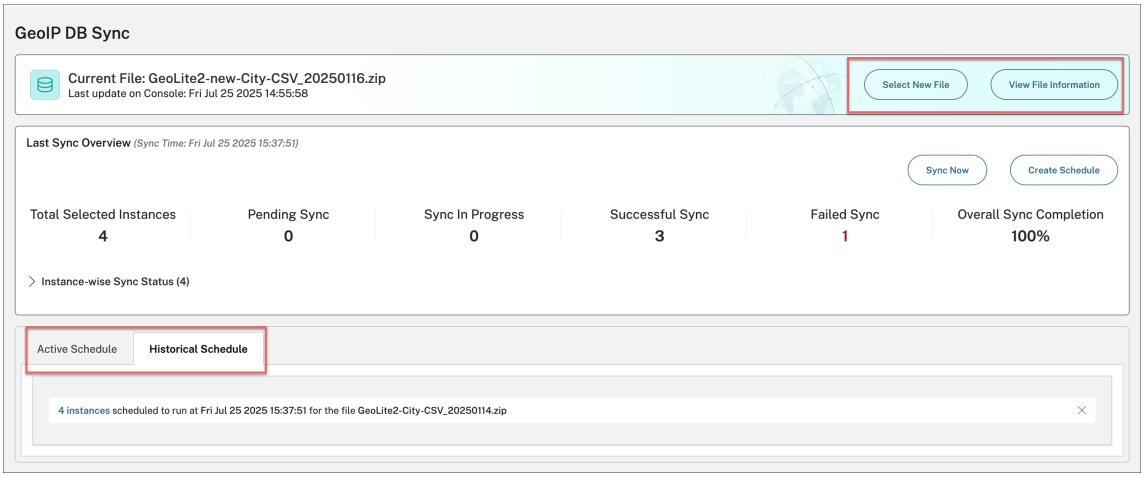
4. View the progress of sync and instance-wise sync status on the **GeoIP DB Sync** page.



5. Based on your requirement, you can perform the following actions:

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

- **Select New File**: Click **Select 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.



Manage admin partitions of NetScaler instances

September 27, 2025

You can configure admin partitions on your Citrix NetScaler instances so that different groups in your organization are assigned different partitions on the same NetScaler instance. A network administrator can be assigned 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. Each user can view and manage only the partitions in the group to which the user belongs. Each admin partition is considered as an instance in NetScaler Console. When you discover a NetScaler instance, the admin partitions configured on that NetScaler instance get added to the system automatically.

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

Consider that you have two NetScaler VPX instances with two partitions configured on each instance. For example, NetScaler instance 10.102.216.49 has Partition_1, Partition_2, and Partition_3, and NetScaler instance 10.102.29.120 has p1 and p2 as shown in the following image.

To view the partitions, navigate to **Infrastructure > Instances > NetScaler > VPX**, and then click **Partitions**.

You can assign user-p1 the following partitions: 10.102.29.120-p1 and 10.102.216.49-Partition_1. And, you can assign user-p2 to manage partitions 10.102.29.80-p2, 10.102.216.49-Partition_2, and 10.102.216.49-Partition_3.

Then , you have to create the two users, user-p1 and user-p2, and you have to assign the users to the groups that you created for them.

First, you have to create two groups with appropriate permissions (example: admin permissions) and include the required admin partition instances in each group. For example, create system group partition1-admin and add NetScaler admin partitions 10.102.29.120-p1 and 10.102.216.49-Partition_1 to this group. Also create system group partition2-admin and add NetScaler admin partitions 10.102.29.120-p2, 10.102.216.49-Partition_2, and 10.102.216.49-Partition_3 and to this group.

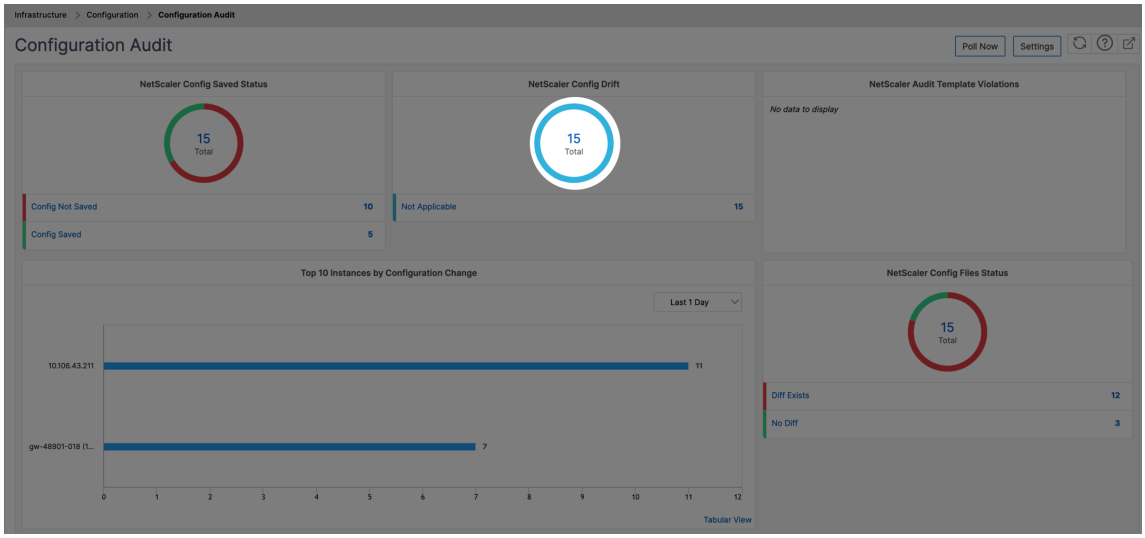
After you have created the admin partition, you can also use the revision history difference feature and the audit template for admin partition feature for auditing purposes

Revision history difference for admin partition allows you to view the difference between the five latest configuration files for a partitioned NetScaler instance. You can compare the configurations files against each other (example Configuration Revision - 1 with Configuration Revision -2) or against the current running/saved configuration with Configuration Revision. Along with the differences in configuration, the correction configurations are also shown. You can export all the corrective commands to your local folder and correct the configurations.

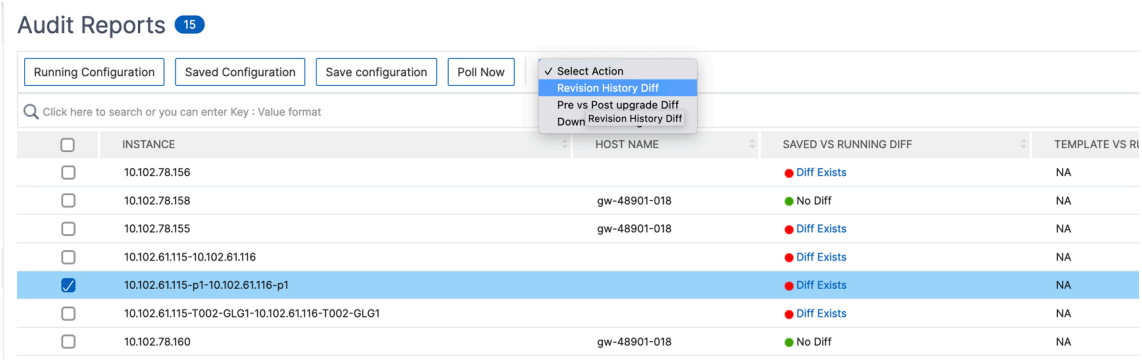
To view the revision history difference:

1. Navigate to **Infrastructure > Configuration Audit.** Click inside the donut chart that represents the instance config status. In the **Audit Reports** page that opens, click the partitioned NetScaler instance.

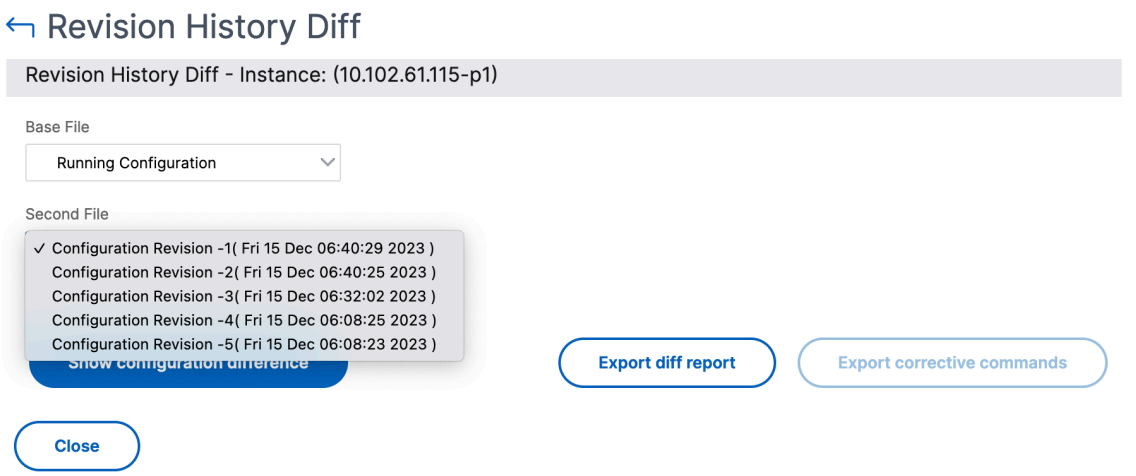
© 1997–2025 Citrix Systems, Inc. All rights reserved.



2. From the **Action** menu, click **Revision History Diff.**

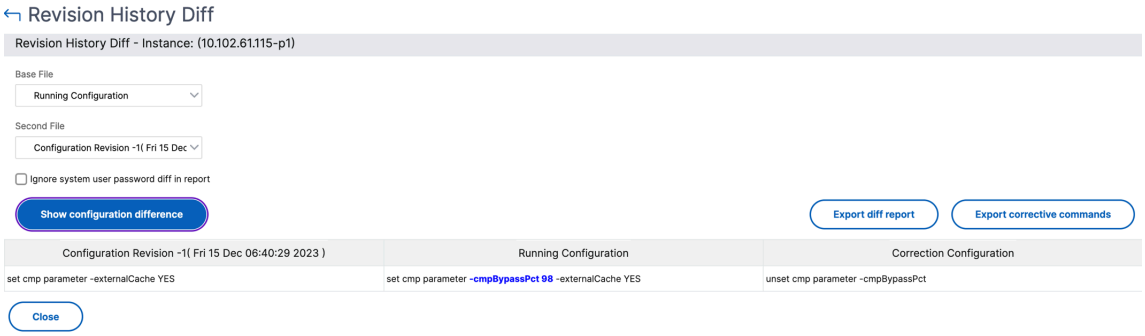


3. On the **Revision History Diff** page, select the files that you want to compare. For example, compare the Saved Configuration with Configuration Revision -1 and then, click **Show configuration difference**.



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

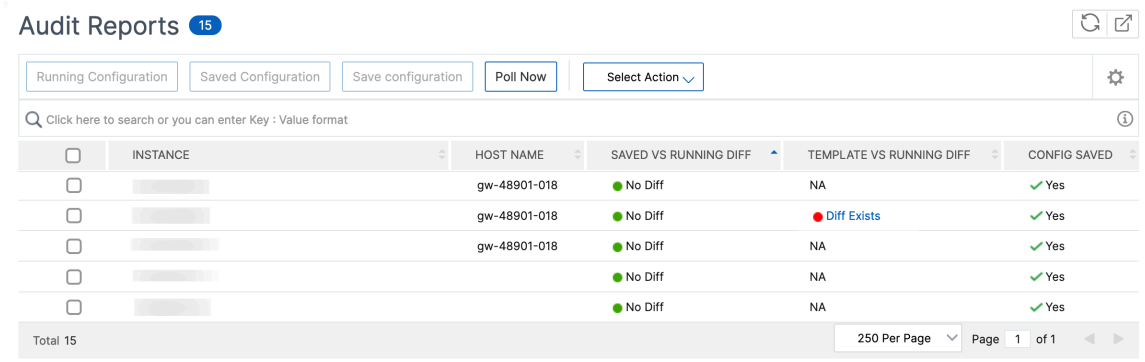
4. You can then view the difference between the five latest configuration files for the selected partitioned NetScaler instance as shown below. You can also view the corrective configuration commands and export these corrective commands to your local folder. These corrective commands are the commands that need to be run on the base file in order to get the configuration to the desired state (configuration file that is being used for comparison).



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.

To view the template vs running difference:

1. From the **Audit Reports** page, click the partitioned NetScaler instance.



2. If there is any difference between the audit template and the running difference, the difference is shown as a hyperlink. Click the hyperlink to view the differences if there is any. Along with the differences in configuration, the correction configurations are also shown. You can also export all the corrective commands to your local folder and correct the configurations.

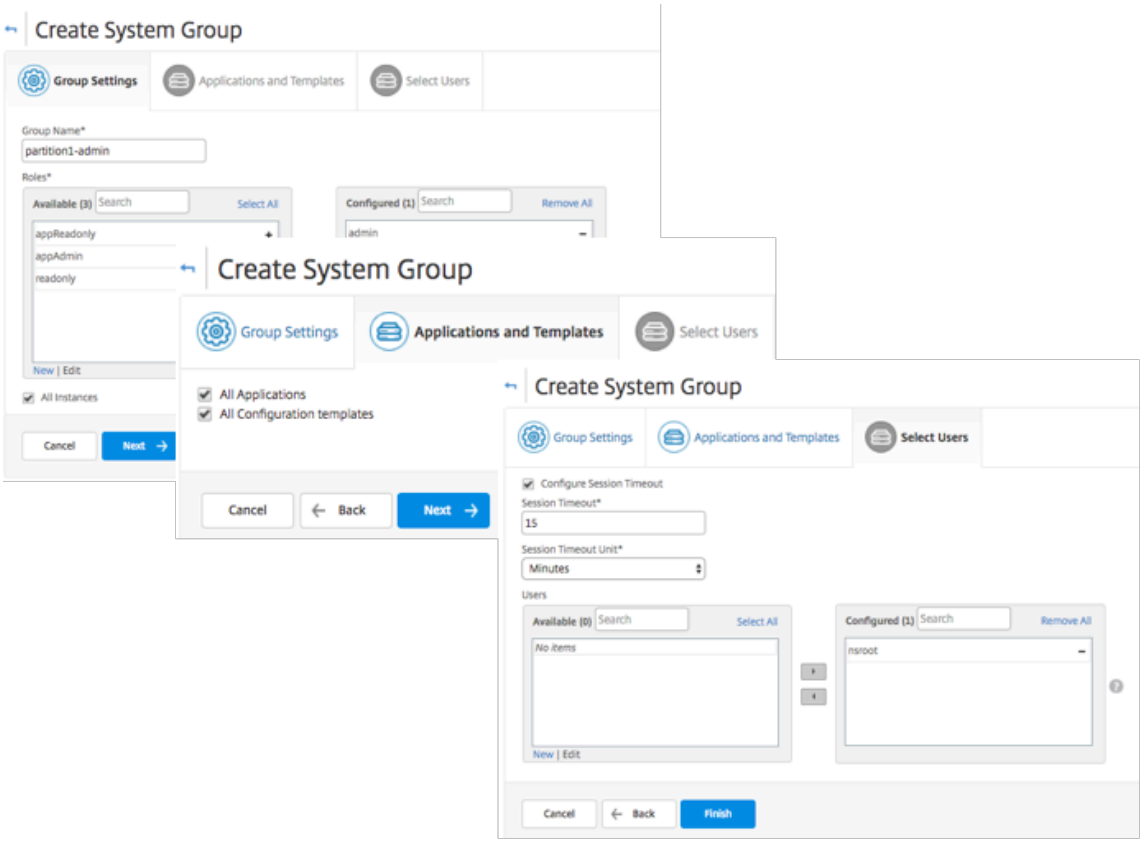
To create groups:

1. Navigate to **Settings > User Administration > Groups**, and then click **Add**.
2. In the **Create System User** page, specify the following:

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

- **Group Settings** tab: Enter the group name and role permissions. To allow access to specific instances, clear the **All Instances** check box, and then choose your instances on the **Select Instances** page.
- **Applications and Templates** tab: You can choose to use this group across all applications and configuration templates.
- **Select Users** tab: Select users that you'd like to add to this group. You can click the **New** link in the **Available** table to create new users. Optionally, configure the session timeout, where you can configure the time period for how long a user can remain active.

3. Click **Finish**.



To create users:

1. Navigate to **Settings > User Administration > Users**, and then click **Add**.
2. On the **Create System User** page, specify the user name and password. Optionally, you can enable external authentication and configure the session timeout.
3. Assign the user to a group by adding the group name from the **Available** list to the **Configured** list.
4. Click **Create**.

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

Now log out and log on with user-p1 credentials. You can view and manage only the admin partitions assigned to you to manage and monitor.

Create a NetScaler high-availability pair

September 27, 2025

A NetScaler high-availability (HA) pair can provide an uninterrupted operation during downtime or network failures. You can create a HA pair of NetScaler instances using NetScaler Console. For more information, see NetScaler high-availability.

Perform the following steps to create a HA pair of NetScaler instances in NetScaler Console:

1. Navigate to **Infrastructure > Instances > NetScaler**.
2. Select a NetScaler instance from the list with which you want to create a HA pair.

   The selected instance becomes a primary instance in the HA pair.
3. Click Select **Action > Create HA Pair**.
4. In **Instance Selection**, perform the following steps:

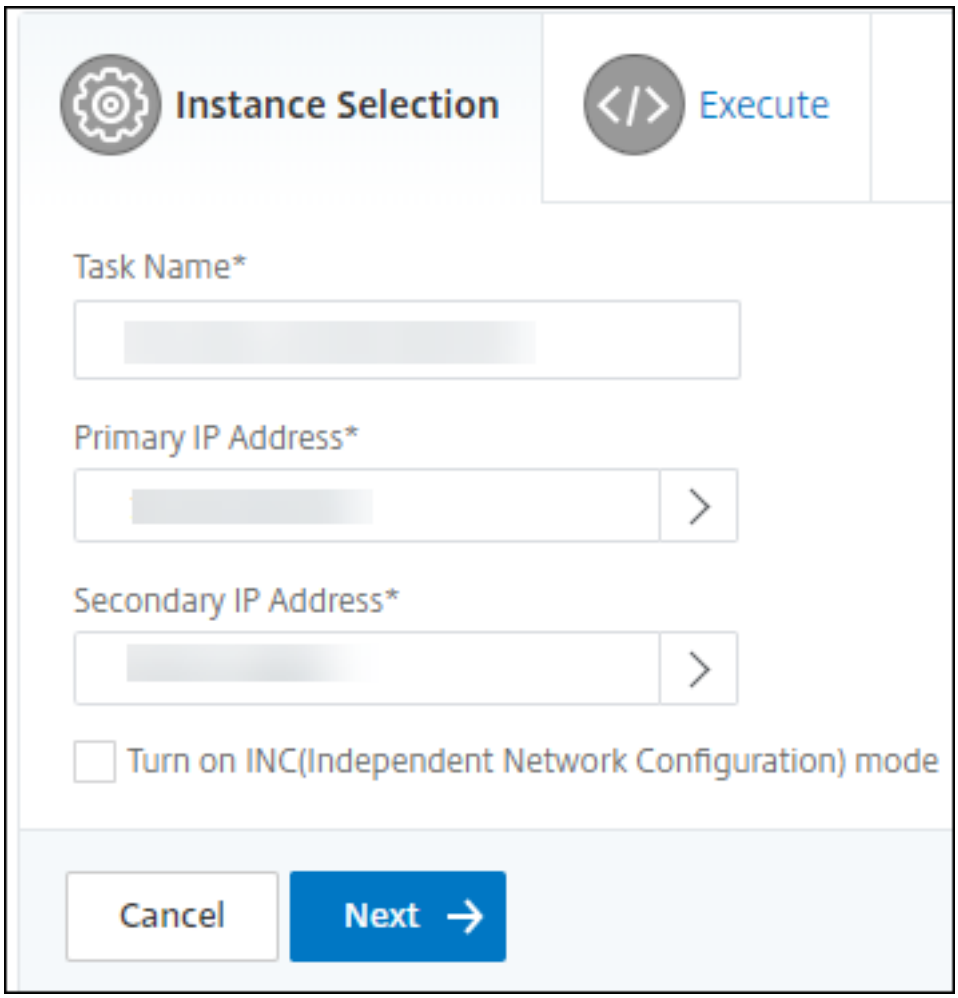
   a) In **Secondary IP Address**, click to select a secondary instance.

   b) Select a NetScaler instance that you want to configure as secondary in the HA pair.

   c) Optional, select **Turn on INC(Independent Network Configuration) mode** if you have the HA pair instances in two subnets.

   d) Click **Next**.

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



5. In **Execute**, you can decide to create a HA pair now or later.

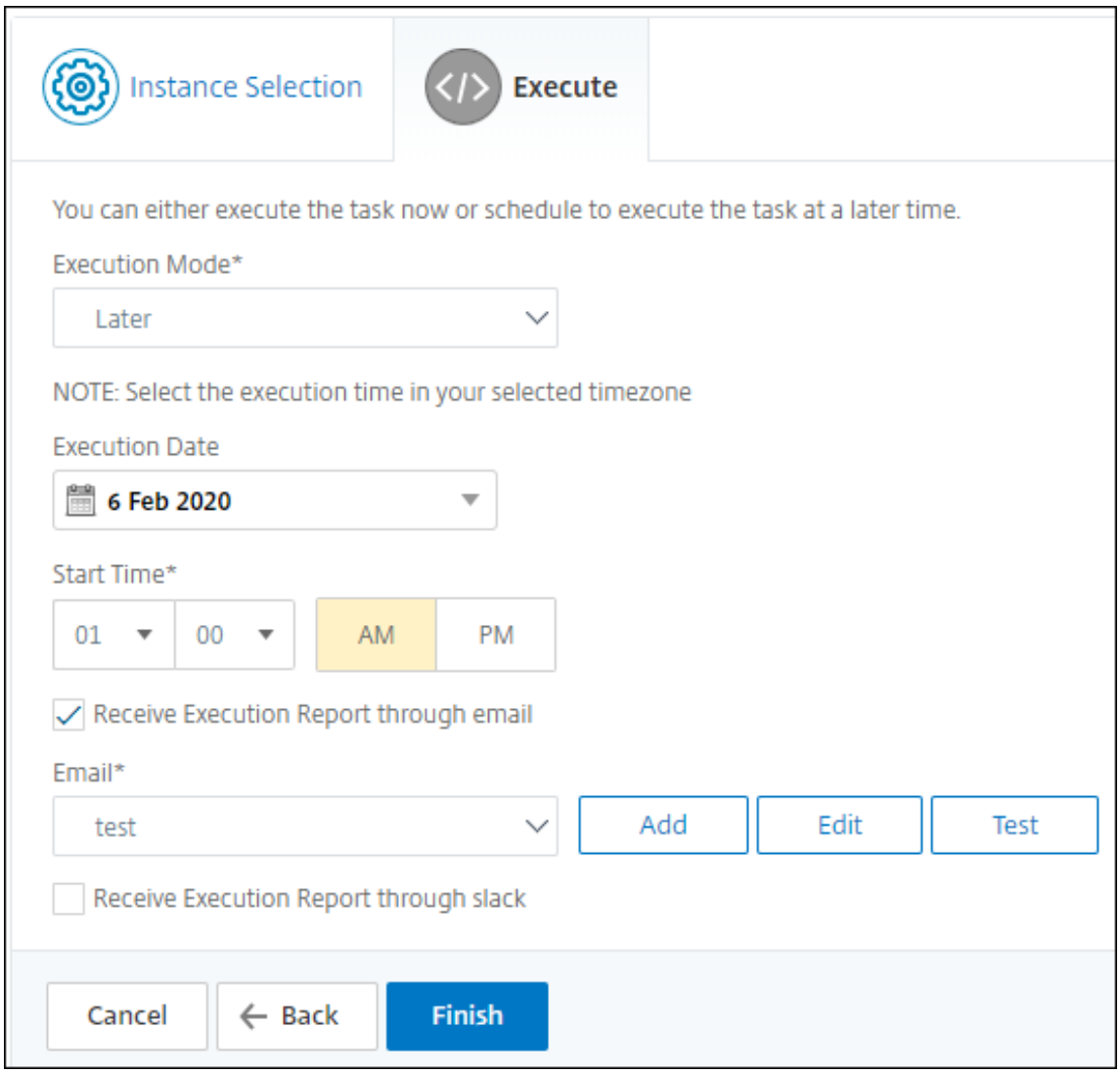
   a) In **Execution Mode**, select one of the following execution modes:

      - **Now** - Select this option to create a HA pair now.
      - **Later** - Select this option to create a HA pair on specific date and time.

   b) If you have selected **Later** in the **Execution Mode** list, select **Execution Date** and **Start Time** when you want to run this task.

      > **Note**
      >
      > The execution time is displayed in the timezone set in NetScaler Console.

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

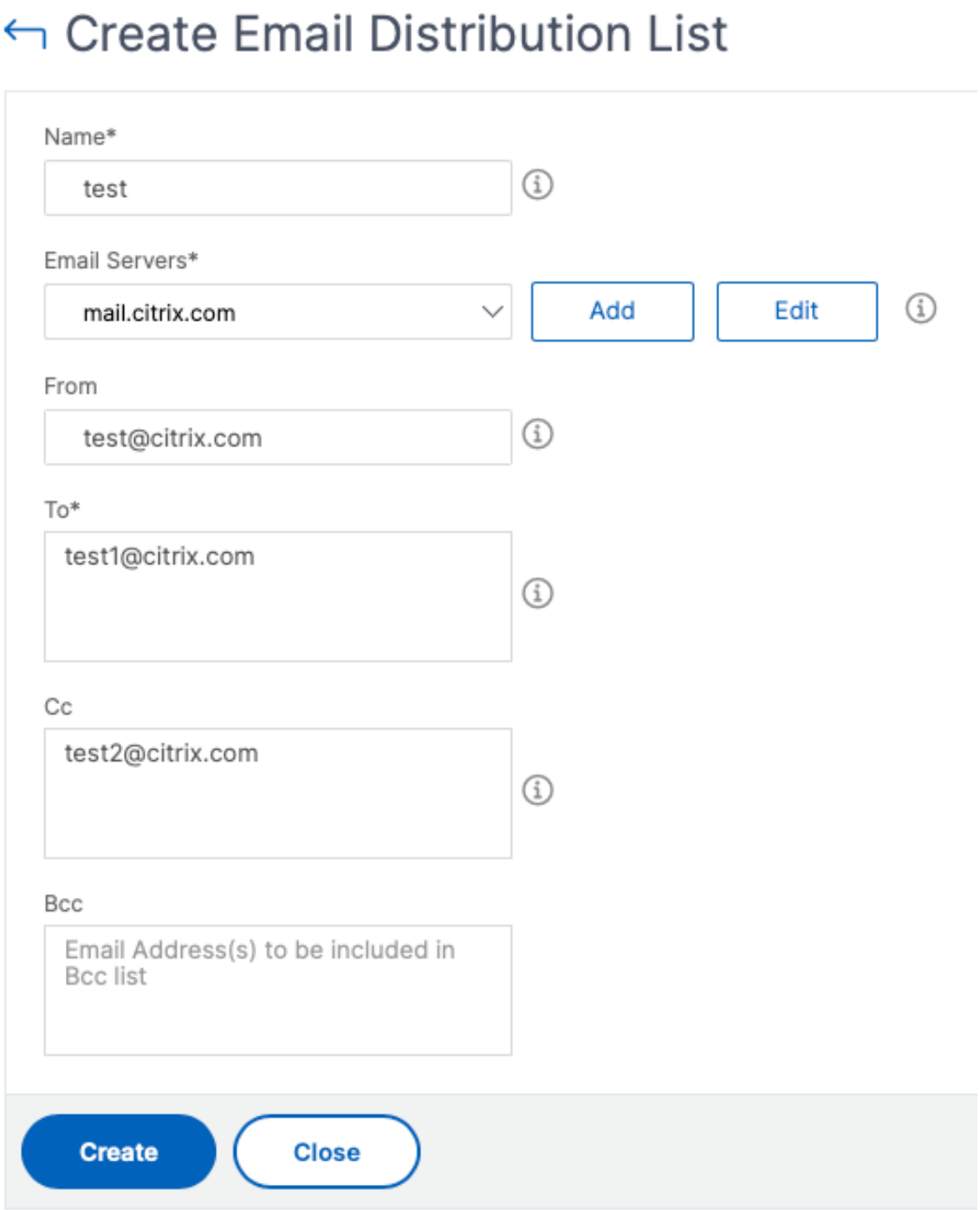


You can receive an execution report of this task through the following:

- **Email** - Select the email distribution from the list.

  To add a distribution list, click **Add**. Specify the required parameters to add the distribution list and click **Create**.

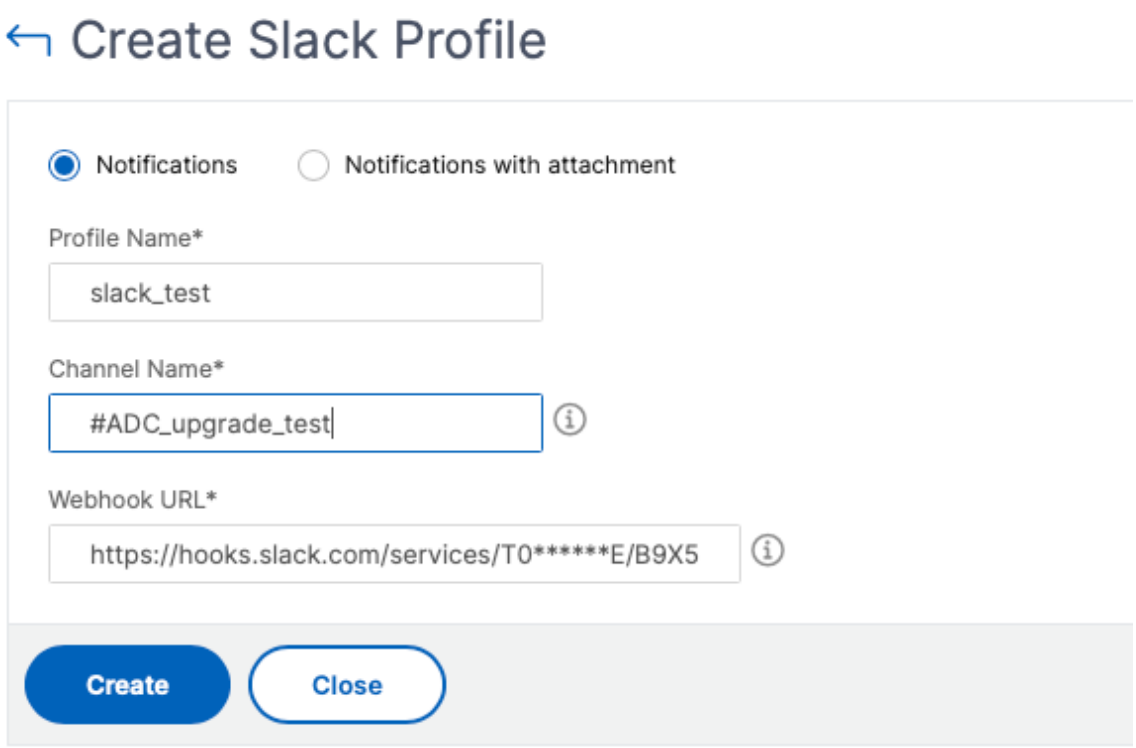
© 1997–2025 Citrix Systems, Inc. All rights reserved.



- **Slack** - Select the Slack profile from the list.

  To add a Slack profile, click **Add**. Specify **Profile Name**, **Channel Name**, and **Token** and click **Create**.

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



Back up and restore NetScaler instances

September 27, 2025

You can back up the current state of a NetScaler instance and later use the backed-up files to restore it to the same state. 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 and CLI. You can also 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.

NetScaler Console creates a complete backup and restores the following NetScaler instance types:

- NetScaler SDX
- NetScaler VPX
- NetScaler MPX
- NetScaler BLX

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

> **Note:**
>
> - Ensure that the NetScaler Console profile has the admin access to backup and restore NetScaler instances.
> - 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/device_backup/
```

To avoid issues due to non-availability of disk space, you can save a maximum of 50 backup files per NetScaler instance 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.

Configure instance backup settings

The **Instance Backup Settings** page allows you to configure settings on NetScaler Console to back up a selected NetScaler instance or multiple instances:

1. In NetScaler Console, navigate to **Settings** > **Administration**.
2. In **Backup**, select **Configure System and Instance backup**.
3. Select **Instance** and specify the following:
    - **Enable Instance Backups**: By default, NetScaler Console is enabled for taking backups of NetScaler instances. Clear this option if you do not want to create backup files for the instances.
    - **Password Protect File**: (optional) Select the password protect option to encrypt the backup file. Encrypting the backup file ensures that all the sensitive information inside the backup file is secure.

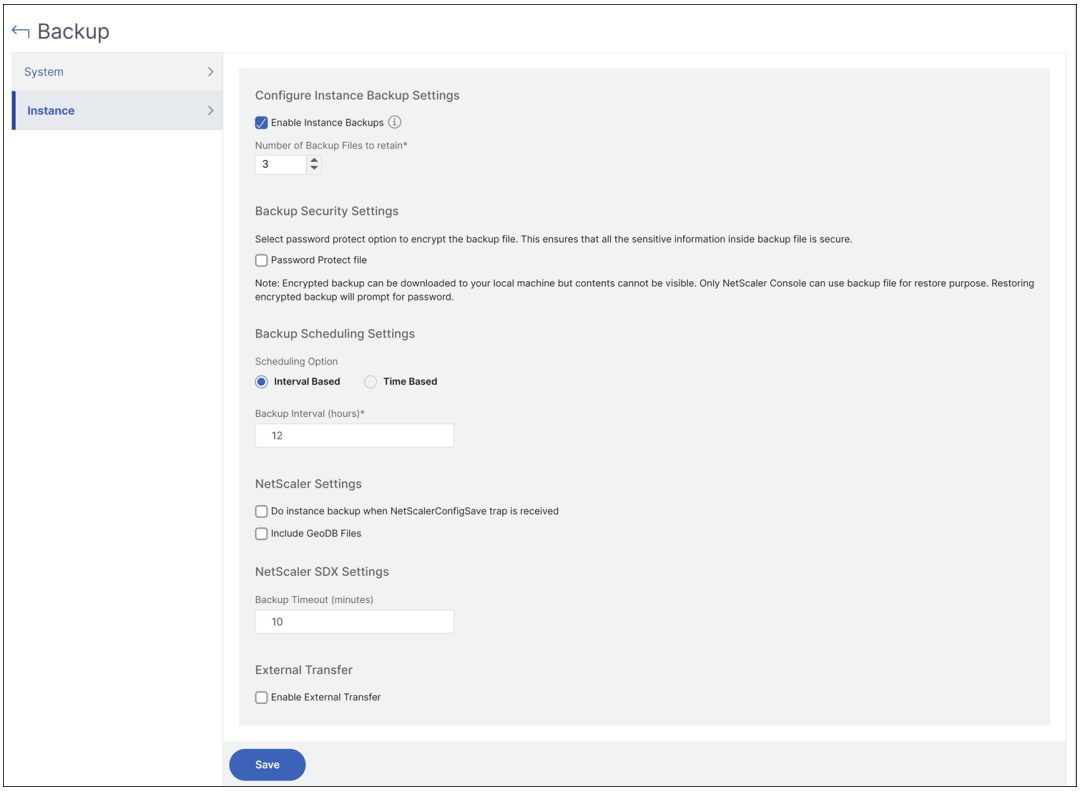
      > **Note:**
      >
      > You can download the encrypted backup file to your local machine, but you cannot open the file either with the NetScaler Console GUI or with any text editor. You are prompted to provide the password when restoring the encrypted backup file. You

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

> can, however, open an unencrypted backup file on your system.

- **Number of Backup Files to retain**: Specify the number of backup files to retain in NetScaler Console. You can retain up to 50 backup files per NetScaler instance. The default is three backup files.

> **Note:**
>
> Each backup file accounts for some storage requirement. We recommend that you store an optimal number of NetScaler backup files on NetScaler Console as per your requirement.

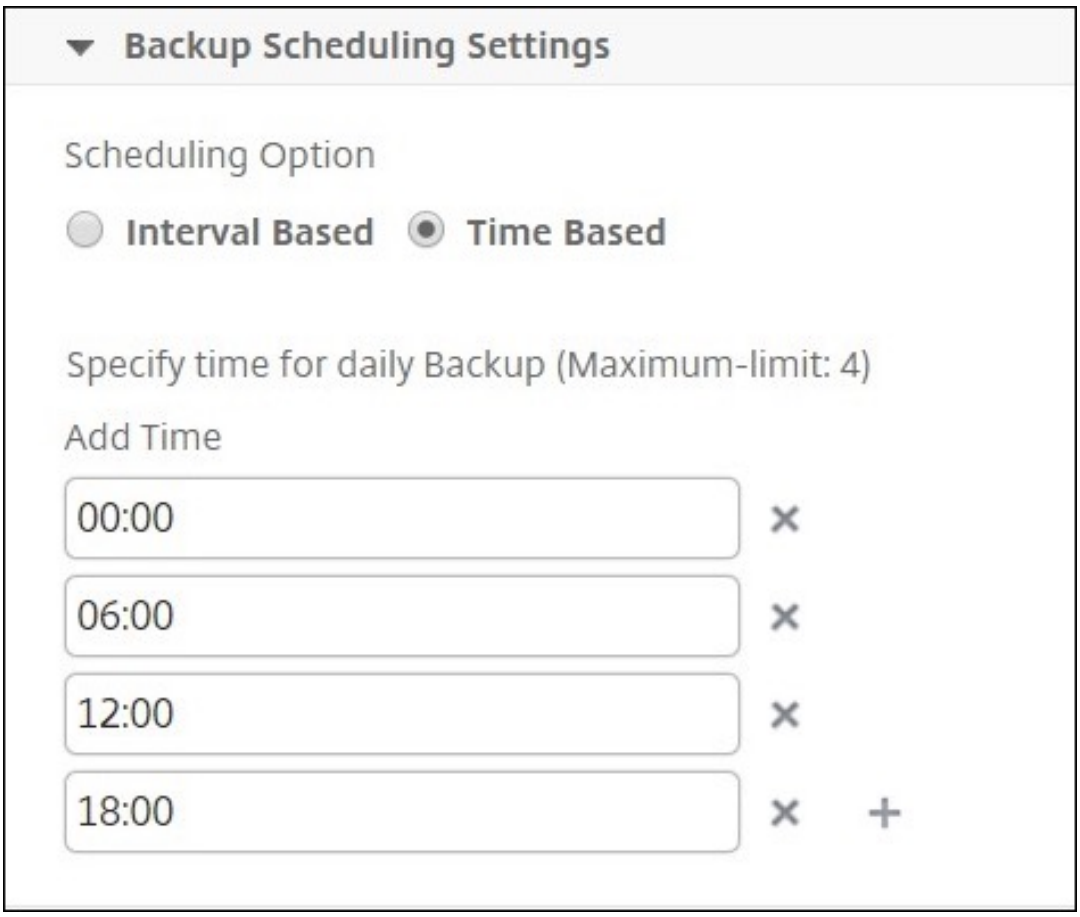


- **Backup scheduling settings**: (optional) There are two options available for creating backup files, though you can use only one option at a time:

  a) The default backup scheduling option is “interval-based.”A backup file is created in NetScaler Console after the specified interval elapses. The default backup interval is 12 hours.

  b) You can also change the type of scheduled backups to “time-based.”In this option, specify the time in `hours:minutes` format to back up instances at the specified time. NetScaler Console allows a maximum of four daily backups to happen on the instances.

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



- **NetScaler settings**: (optional) 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.
- **Geodatabase files**: (optional) By default, NetScaler Console does not back up the Geo-Database files. You can enable the option to create a backup of these files also.



- **External Transfer:**(optional) NetScaler Console allows you to transfer the NetScaler instance backup files to an external location:

  a) Specify the IP address of the location.

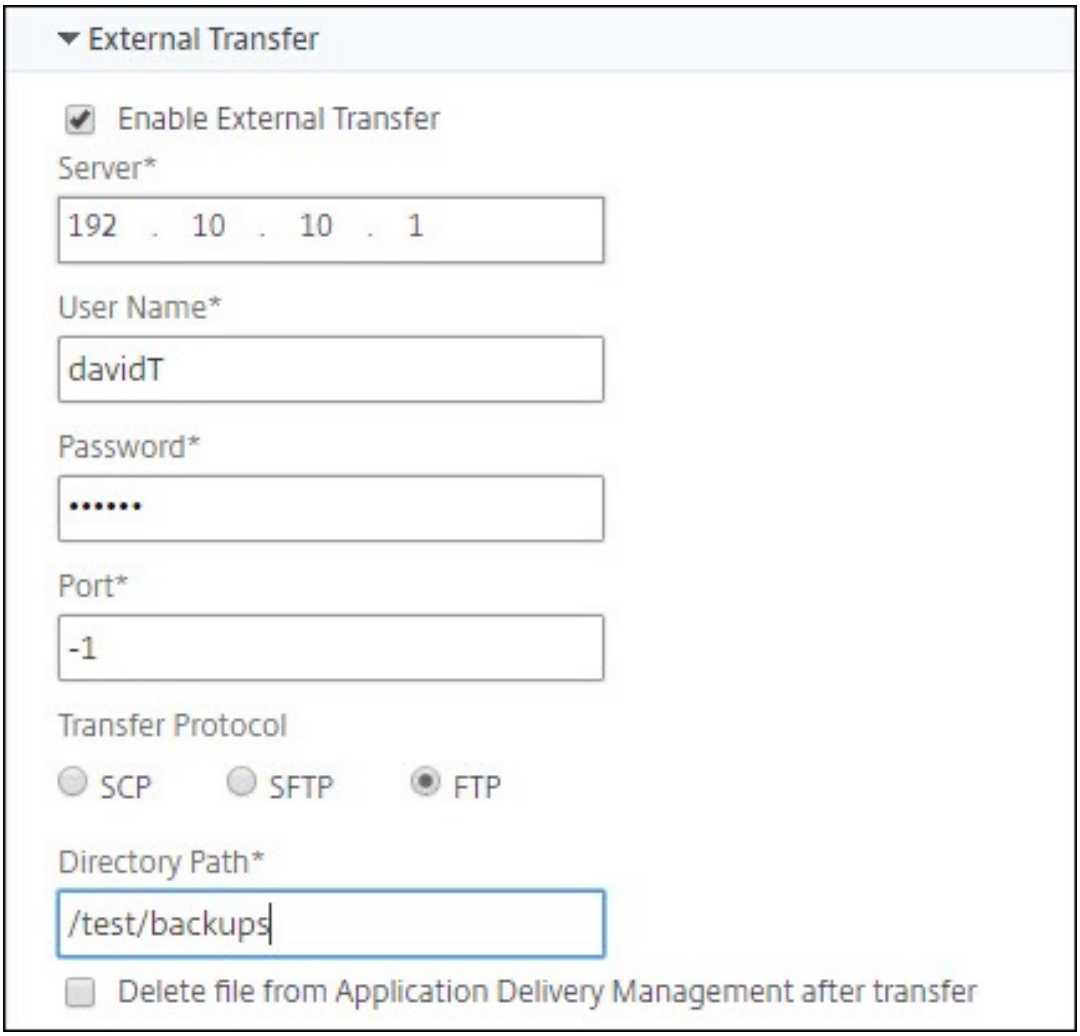
© 1997–2025 Citrix Systems, Inc. All rights reserved.

b) Specify the user name and the password of the external server to which you want to transfer the backup files.

c) Specify the transfer protocol and the port number.

d) You can specify the directory path where the file must be stored.

e) Optional, you can also delete the backup file from NetScaler Console after transferring it to the external server.



> **Note:**
>
> NetScaler Console sends an SNMP trap or a Syslog notification to itself when there is a backup failure for any of the selected NetScaler instances.

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:

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

1. In NetScaler Console, navigate to **Infrastructure > Instances**. Under **Instances**, select the type of instances (for example, NetScaler 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. You can 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**.

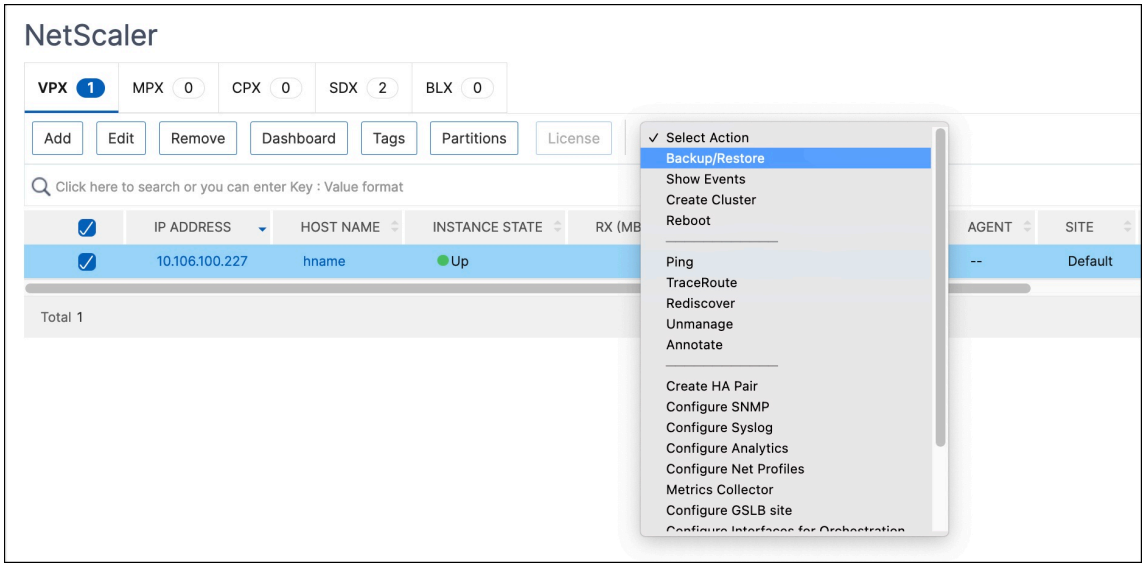
Restore a NetScaler instance by using NetScaler Console

> **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.

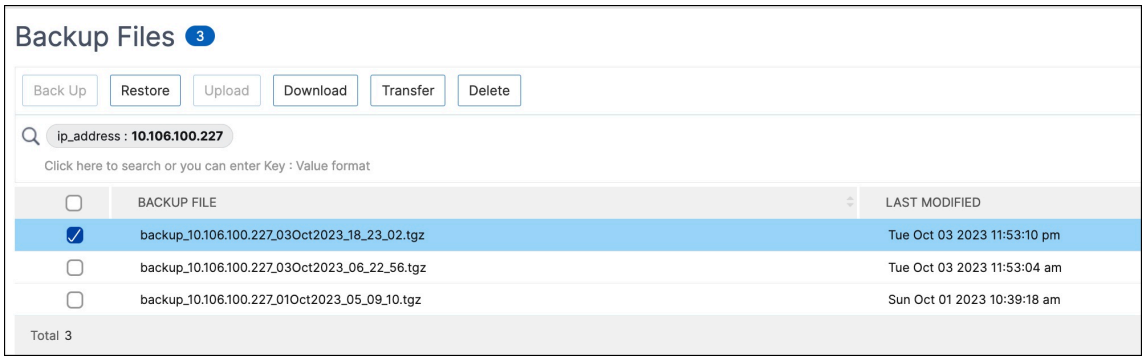
Perform this task to restore a NetScaler instance by using the backup file that you created earlier:

1. Navigate to **Infrastructure > Instances**, select the instance that you want to restore, and then click **Select Action > Backup/Restore**.

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



2. On the **Backup Files** page, select the backup file containing the settings that you want to restore, and then click **Restore**.



Restore a NetScaler SDX appliance using NetScaler Console

In NetScaler Console, the backup of the 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
- 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)

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

- Third Party instance images (if provisioned)

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, ensure that you add the licenses and configure the new appliance's Management Service network settings to match the settings in the backup file before you start the restore process. That is, the new appliance must be licensed and meet the minimum license requirements of the backup file. For example, if the backup had five VPX instances with a total of 5 GB, then the new appliance must also be able to support these requirements. Or if the backup appliance had a platinum license, the new appliance must have the same or higher license. Network settings, such as IP address, netmask, gateway, XenServer IP address, and DNS server must be properly configured on the new appliance.

Before you restore the SDX appliance, ensure that the backed-up SDX appliance platform variant is the same as the appliance. You cannot restore from a different platform variant.

> **Note:**
>
> Before you restore an 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 > SDX**. Select an instance.
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**.

Force a failover to the secondary NetScaler instance

September 27, 2025

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

You might want to force a failover if, for example, you need to replace or upgrade the primary Citrix 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:

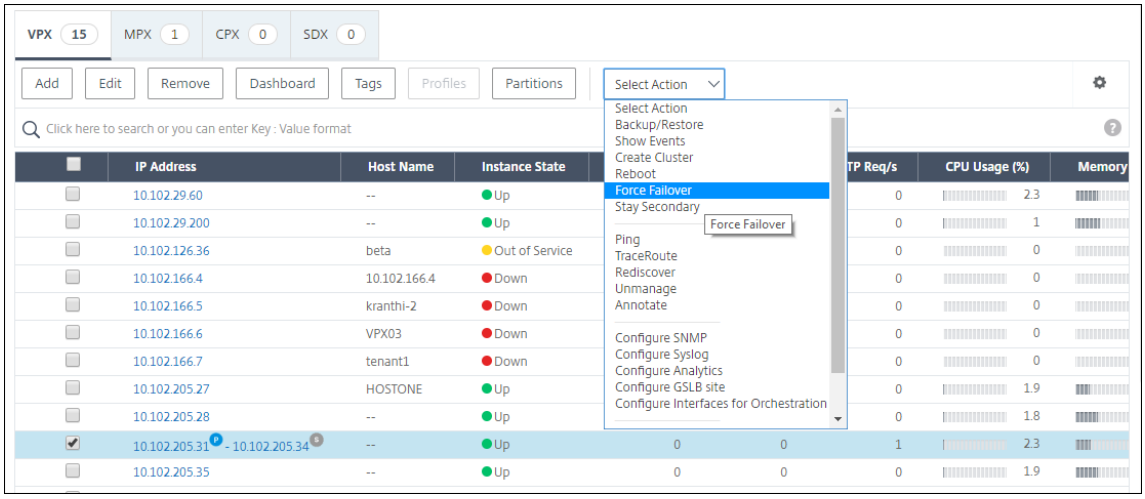
- You force failover on a standalone system.
- The secondary instance is disabled or inactive. If the secondary instance is in an inactive state, you must wait for its state to be UP to force a failover.
- The secondary instance is configured to remain secondary.

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 > NetScaler > VPX** tab, and then select an instance .
2. Select instances in an HA setup from the instances listed under the selected instance type.
3. From the **Action** menu, select **Force Failover.**
4. Click **Yes** to confirm the force failover action.



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

Force a secondary NetScaler instance to stay secondary

September 27, 2025

In an HA setup, the secondary node can be forced to stay secondary regardless of the state of the primary node.

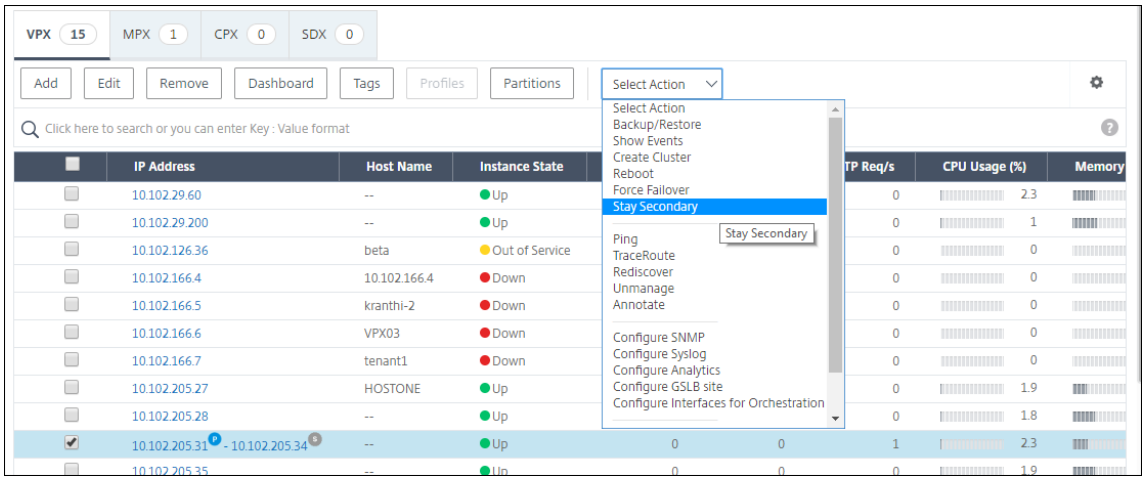
For example, suppose that the primary node needs to be upgraded and the process takes a few seconds. During the upgrade, the primary node might go down for a few seconds, but you do not want the secondary node to take over. You want it to remain the secondary node even if it detects a failure in the 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** > **NetScaler** > **VPX** tab, and then select an instance.
2. Select instances in an HA setup from the instances listed under the selected instance type.
3. From the **Action** menu, select **Stay Secondary**.
4. Click **Yes** to confirm the execution of the "Stay Secondary"action.



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

Create instance groups

September 27, 2025

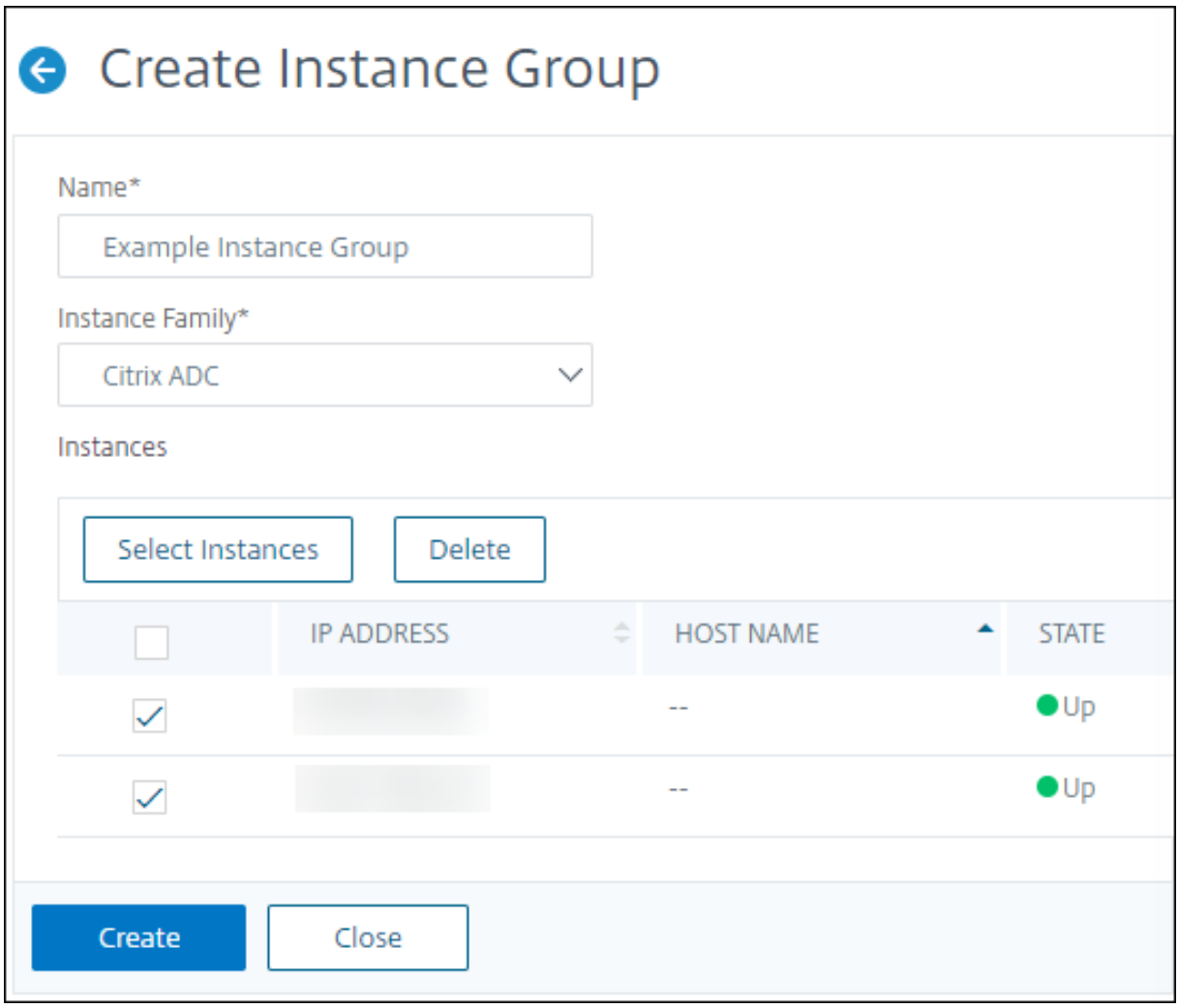
To create an instance group, you must first add all your NetScaler instances to NetScaler Console. After you have added the instances successfully, create instance groups based on their instance family. Creating a group of instances helps you to upgrade, backup, or restore on the grouped instances at one time.

To create an instance group using NetScaler Console

1. In NetScaler Console, navigate to **Infrastructure > Instance Groups**, and then click **Add**.
2. Specify a name to your instance group and select **NetScaler** from the **Instance Family** list.
3. 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**.
4. Click **Create**.

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



Provision NetScaler VPX instances on SDX using NetScaler Console

September 27, 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 restricts you from provisioning 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**.

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

2. In the **SDX** tab, select an SDX instance where you want to provision a VPX instance.
3. In **Select Action**, select **Provision VPX**.

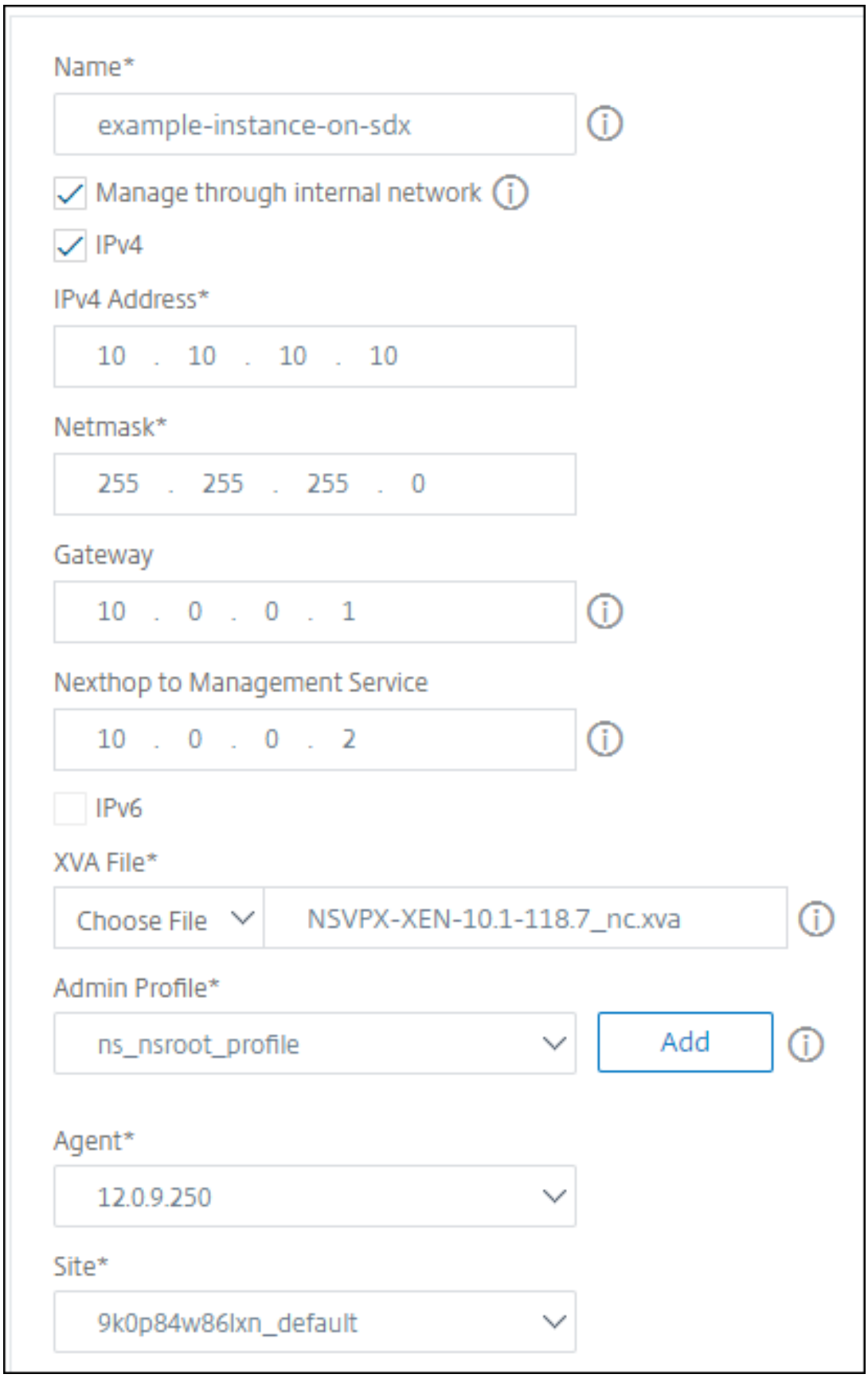
Step 1 - Add a VPX instance

The NetScaler Console uses the following information to configure VPX instances in an SDX appliance:

- **Name** - Specify a name to a NetScaler instance.
- Establish a communication network between SDX and VPX. To do so, select the required options from the list:
    - **Manage through internal network** - This option establishes an internal network for a communication between the NetScaler Console and a VPX instance.
    - **IP address** - You can select an **IPv4** or **IPv6** address or both to manage the NetScaler VPX instance. A VPX instance can have only one management IP (also called NetScaler IP). You cannot remove the NetScaler IP address.

      For the selected option, assign a netmask, default gateway, and next hop to the NetScaler Console server 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 the 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

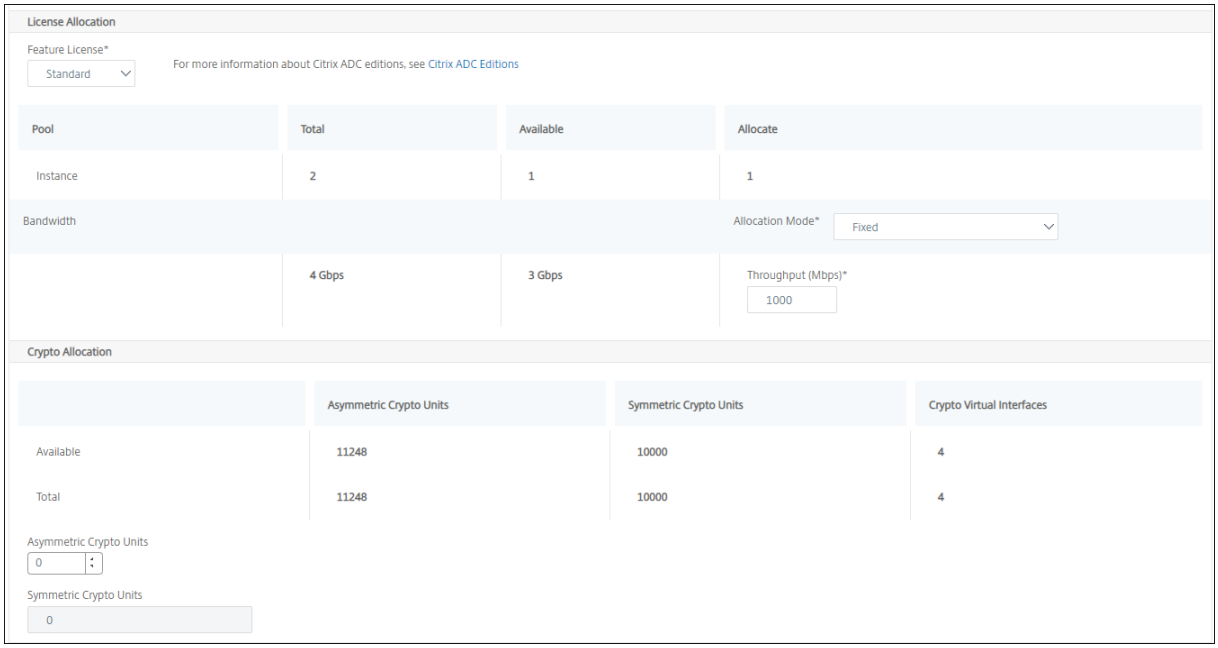
In the **License Allocation** section, specify the VPX license. You can use Standard, Advanced, and Premium licenses.

- **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.

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.

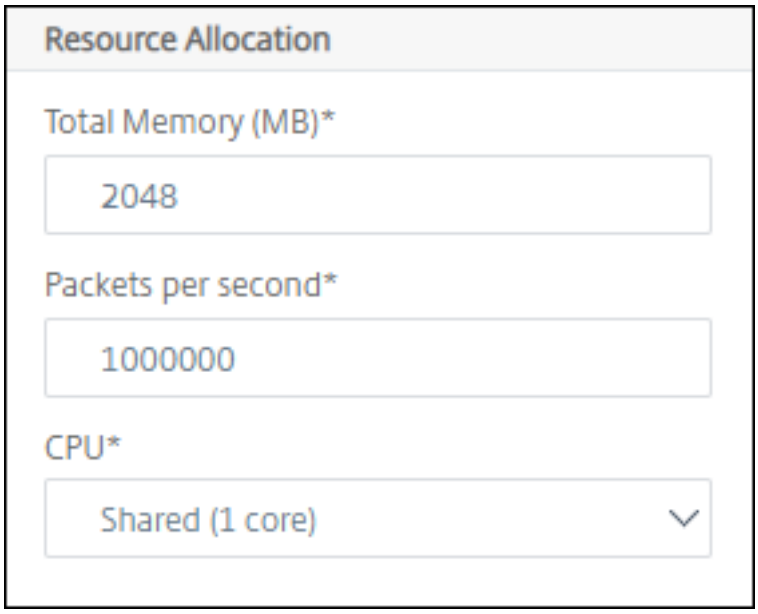
- **CPU** - Specify number of CPU cores to an instance. You can use shared or dedicated CPU cores.

  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.



The following table lists the supported VPX, Single bungle image version, and the number of cores you can assign to an instance:

Platform Name	Total Cores	Total Cores Available for VPX Provisioning	Maximum Cores That Can Be Assigned to a Single Instance
SDX 8015, SDX 8400, and SDX 8600	4	3	3
SDX 8900	8	7	7
SDX 11500, SDX 13500, SDX 14500, SDX 16500, SDX 18500, and SDX 20500	12	10	5

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

Platform Name	Total Cores	Total Cores Available for VPX Provisioning	Maximum Cores That Can Be Assigned to a Single Instance
SDX 11515, SDX 11520, SDX 11530, SDX 11540, and SDX 11542	12	10	5
SDX 17500, SDX 19500, and SDX 21500	12	10	5
SDX 17550, SDX 19550, SDX 20550, and SDX 21550	12	10	5
SDX 14020, SDX 14030, SDX 14040, SDX 14060, SDX 14080 and SDX 14100	12	10	5
SDX 22040, SDX 22060, SDX 22080, SDX 22100, and SDX 22120	16	14	7
SDX 24100 and SDX 24150	16	14	7
SDX 14020 40G, SDX 14030 40G, SDX 14040 40G, SDX 14060 40G, SDX 14080 40G and SDX 14100 40G	12	10	10
SDX 14020 FIPS, SDX 14030 FIPS, SDX 14040 FIPS, SDX 14060 FIPS, SDX 14080 FIPS and SDX 14100. FIPS	12	10	5
SDX 14040 40S, SDX 14060 40S, SDX 14080 40S, and SDX 14100 40S	12	10	5
SDX 25100A, 25160A, 25200A	20	18	9

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

Platform Name	Total Cores	Total Cores Available for VPX Provisioning	Maximum Cores That Can Be Assigned to a Single Instance
SDX 25100-40G, 25160-40G, 25200-40G	20	18	16 (if version is 11.1-51.x or higher); 9 (if version is 11.1-50.x or lower; all versions of 11.0 and 10.5)
SDX 26100, 26160, 26200, 26250	28	26	13
15000-50G	16	14	7
SDX 16000	32	30	16
SDX 9100	10	9	9

> **Note**
>
> On the SDX 26xxx platform, a maximum of 26 CPU cores can be assigned to a VPX instance. If crypto units are assigned to the instance, the maximum number of cores depends on the number of crypto units and data interfaces.
>
> For example, if you assign 24000 crypto units to an instance, you can assign 24 CPU cores and maximum two data interfaces to the instance. The SDX appliance considers data interfaces and crypto units as PCI devices. For 26000 crypto units, VPX instance provisioning fails because of no space to add data interfaces.

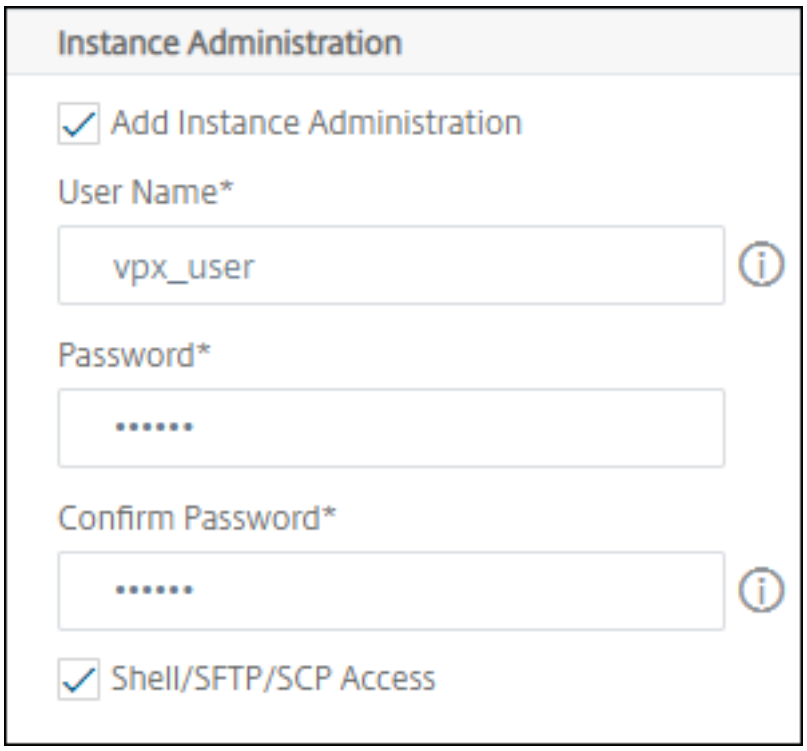
Step 4 - Add instance administration

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:

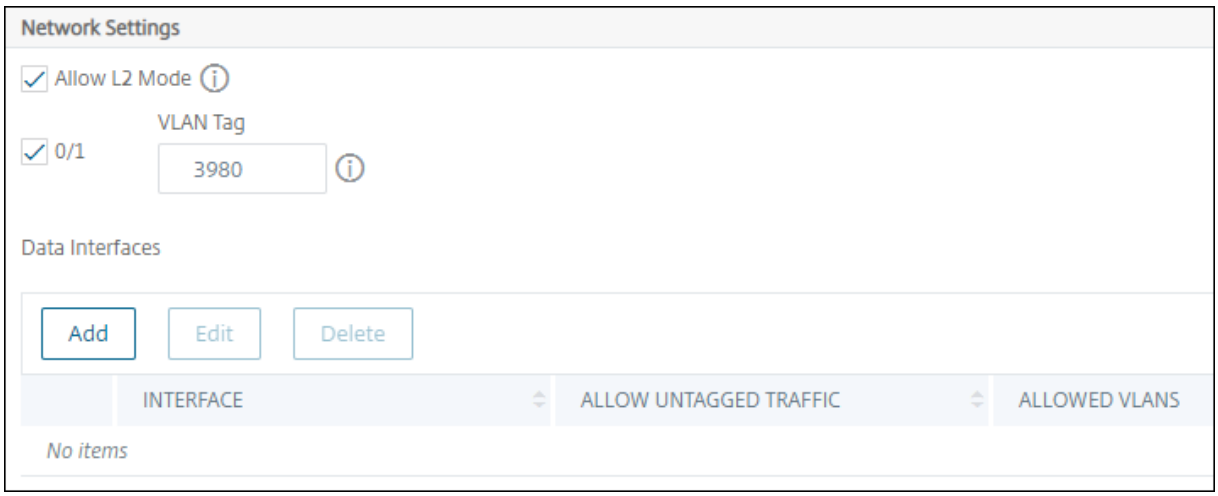
- **Allow L2 Mode under network settings** - You can allow L2 mode on the NetScaler instance. Select Allow L2 Mode under Networking Settings. Before you log on to the instance and enable L2 mode.

  > **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.



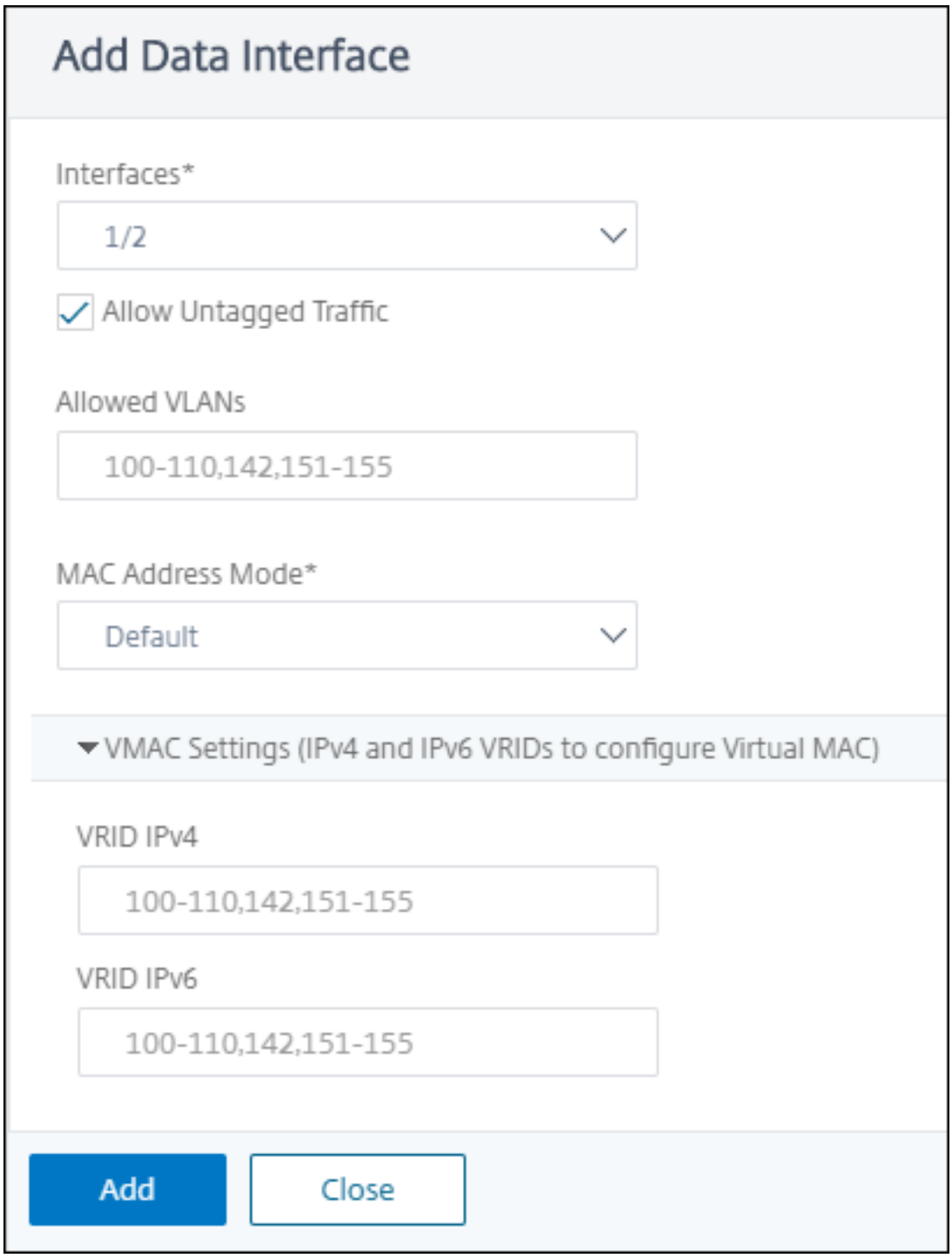
In **Data Interfaces**, click **Add** to add data interfaces and specify the following:

- **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.
- **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.

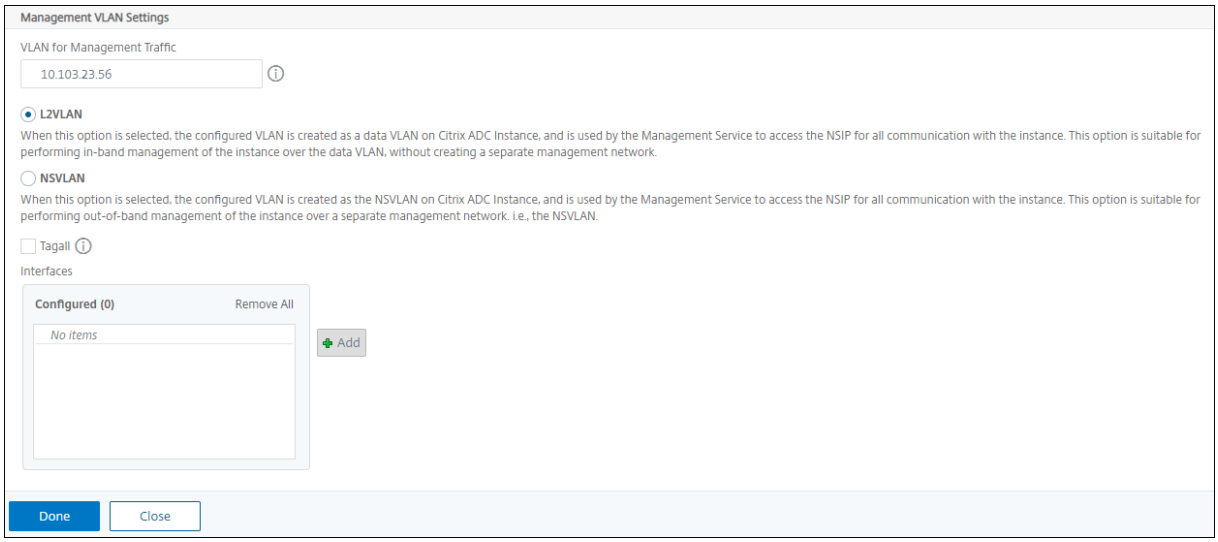
© 1997–2025 Citrix Systems, Inc. All rights reserved.

If the Management Service and the instance are in different subnetworks, specify a VLAN ID while you provision a VPX instance. Therefore, the instance is reachable over the network when it active.

If your deployment requires the NSIP is accessible only through the selected interface while provisioning the VPX instance, select **NSVLAN**. And, the NSIP becomes inaccessible through other interfaces.

- HA heartbeats are sent only on the interfaces that are part of the NSVLAN.
- You can configure an NSVLAN only from the VPX XVA build `9.3-53.4` and later.

> **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.



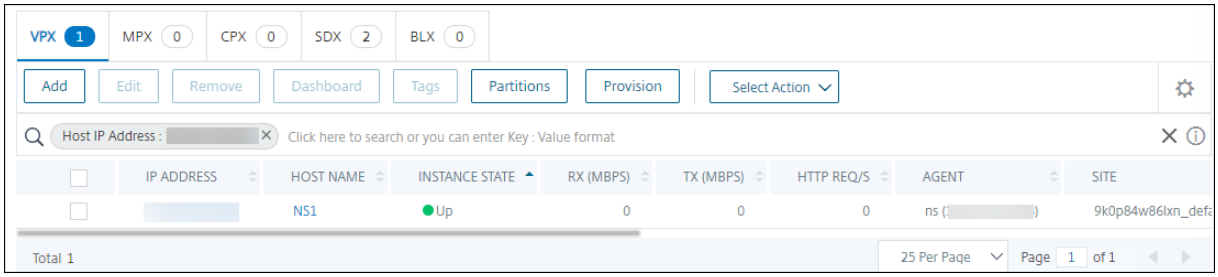
Click **Done** to provision a VPX instance.

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.



Provision NetScaler VPX instances on VMware ESX

September 27, 2025

You can use NetScaler Console to automate a NetScaler VPX instance deployment and management in VMware ESX. When you use NetScaler Console to provision a NetScaler VPX instance on VMware ESX, the instance is readily available to manage in the NetScaler Console GUI.

NetScaler Console uses NetScaler templates of the already deployed instances to provision a new instance in VMware ESX. It stores the datacenter of the VMware vCenter where the required VMware ESX server details are present in a site. Also, it uses cloud access profile to access the VMware vCenter and deploy the VPX on the VMware ESX.

Prerequisites

Before you provision a NetScaler VPX instance in VMware ESX, ensure to complete the following:

1. Install a supported VMware ESXi version (6.0, 6.5, and 6.7).
2. Install VMware Client on a management workstation that meets the minimum system requirements.
3. Downloading the NetScaler VPX setup files.
4. Convert NetScaler VPX files into templates in ESX.
5. Create permissions for NetScaler Console to access VMware vCenter.
6. Create a site in NetScaler Console.

Convert NetScaler VPX files into templates

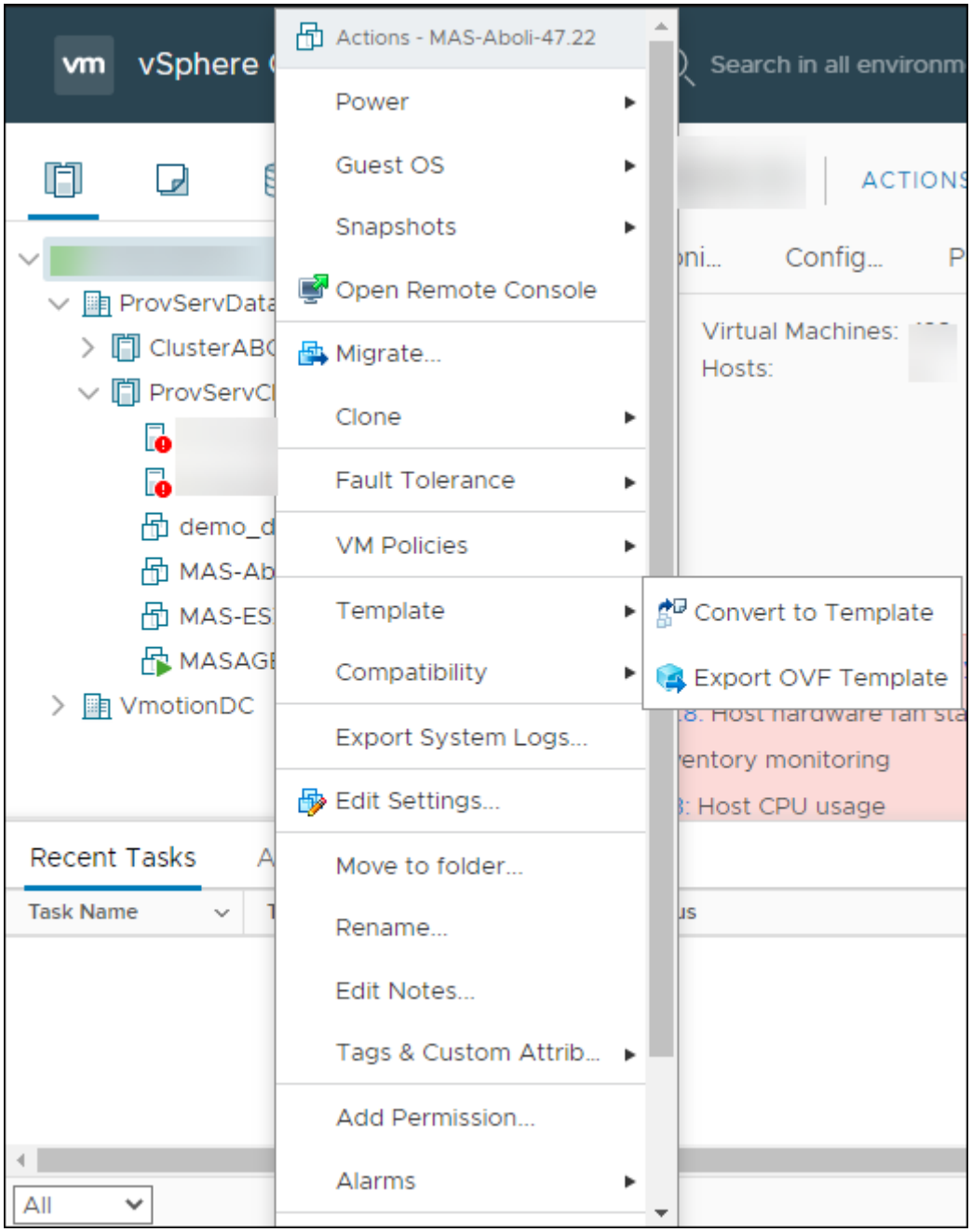
The NetScaler Console uses the NetScaler template in ESX converted by aNetScaler VPX file. Perform the following steps to convert VPX files into templates.

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

1. Deploy a NetScaler VPX instance on VMware using the NetScaler setup files.

   For the first time, use NetScaler setup files to deploy the VPX instance. For more information, see Install NetScaler VPX instance on VMware.

2. Right-click the deployed VM and select **Template**.
3. Click **Convert to Template**.



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

Create permissions for NetScaler Console to access VMware vCenter

To enable NetScaler Console for provisioning and management in VMware vCenter, follow these steps:

1. Create a custom role with privileges
    a) Login to VMware vCenter and navigate to the **Roles** section.
    b) Create a custom role tailored for NetScaler Console.
    c) Assign the following privileges:

```
Datastore.AllocateSpace
Resource.AssignVMToPool
VirtualMachine.Config.AdvancedConfig
VirtualMachine.Inventory.CreateFromExisting
VirtualMachine.Inventory.Delete
VirtualMachine.Interact.PowerOff
VirtualMachine.Interact.PowerOn
VirtualMachine.Provisioning.DeployTemplate
```

2. Create a user
    a) Once the role is defined, navigate to the **Users and Groups** section.
    b) Create a user for NetScaler Console to access the VMware vCenter.
    c) Provide a password for the newly created user.
3. Associate the role with the user
    a) Navigate to the **Global Permissions** section and associate the custom role with the user.
    b) This association provides privileges for NetScaler Console to perform necessary actions on VMware vCenter.

> **Note:**
>
> The listed privileges are the minimum requirements for NetScaler Console to access the VMware vCenter. Creating a user with limited privileges is optional. If any user has privileges that include a superset of the specified privileges, the user can provide those credentials instead.

For more information about configuring user roles with privileges in VMware vCenter, see Configure User access.

Create a site in NetScaler Console

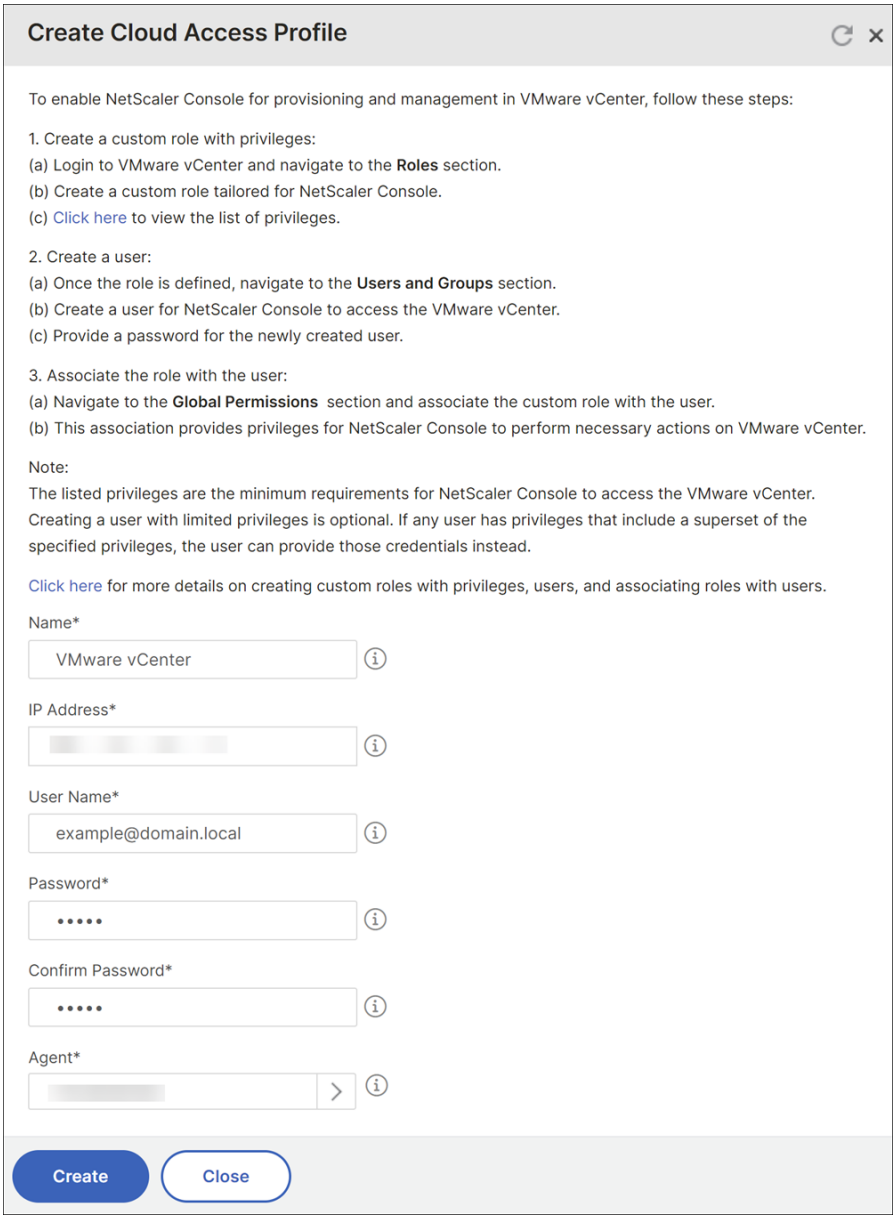
Create a site in NetScaler Console and add the VMware ESX details.

1. In NetScaler Console, navigate to **Infrastructure > Instances > Sites**.

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

2. Click **Add**.
3. In the **Select Cloud** pane,
    a) Select **Data Center** as a **Site** type.
    b) Choose **VMware vCenter** from the **Type** list.
    c) Click **Next**.
4. In the **Choose Region** pane,
    a) In the **Cloud Access Profile** pane, select the profile created for your VMware ESX. If there are no profiles, create a profile.
    b) To create a cloud access profile, click **Add** and specify the following:
        - **Name** –Specify a name to identify your cloud access profile in NetScaler Console.
        - **IP address** –Specify the IP address of the VMware vCenter server where you want to provision VPX instances.
        - **Username** –Specify the user name to access the VMware vCenter server.
        - **Password** –Specify the password to access the VMware vCenter server and confirm the password.

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



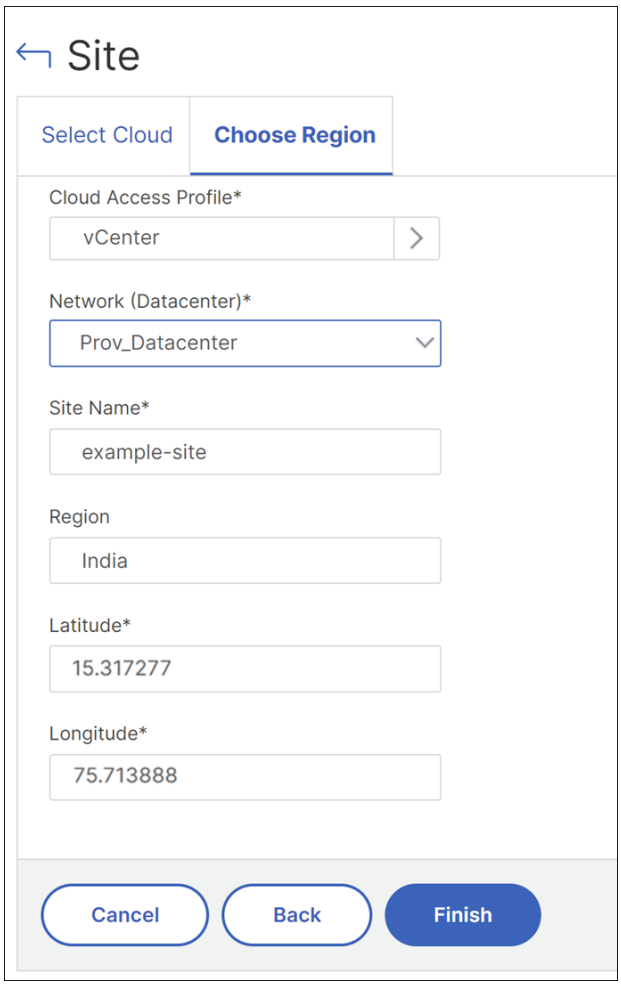
c) In **Network (Datacenter)**, select the data center where you have the NetScaler templates.

d) Specify the **Site Name**.

e) Specify the **Region**, **Latitude**, and **Longitude** to identify the geo-location of your data center.

f) Click **Finish**.

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



Provision an instance on VMware ESX

Use the site that you have associated with your VMware ESX to provision the NetScaler VPX instances.

> **Note:**
>
> Currently, the NetScaler Console supports only to provision standalone NetScaler instances.

1. In NetScaler Console, navigate to **Infrastructure > Instances > NetScaler**.
2. In the **VPX** tab, click **Provision**.

   This option displays the **Provision NetScaler VPX on Cloud** page.
3. Select **VMware vCenter** and click **Next**.

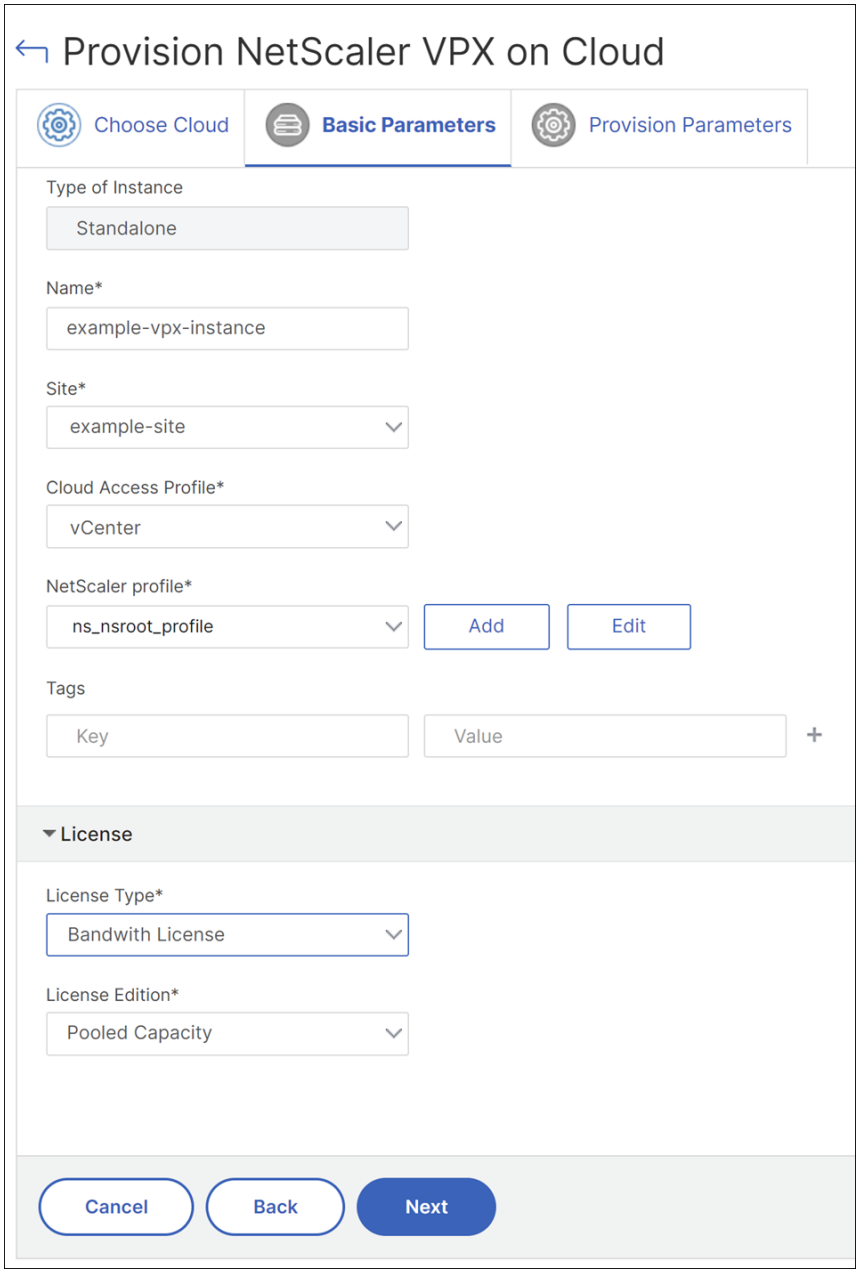
© 1997–2025 Citrix Systems, Inc. All rights reserved.



4. In **Basic Parameters**, specify the following:

    - **Name** –Specify the name of an instance.
    - **Site** –Select the site that you have created earlier.
    - **Cloud Access Profile** –Select the cloud access profile created during site creation.
    - **NetScaler profile** –Select the NetScaler profile to provide authentication.
    - **License** –Use pooled capacity licensing to apply licenses to an instance.

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

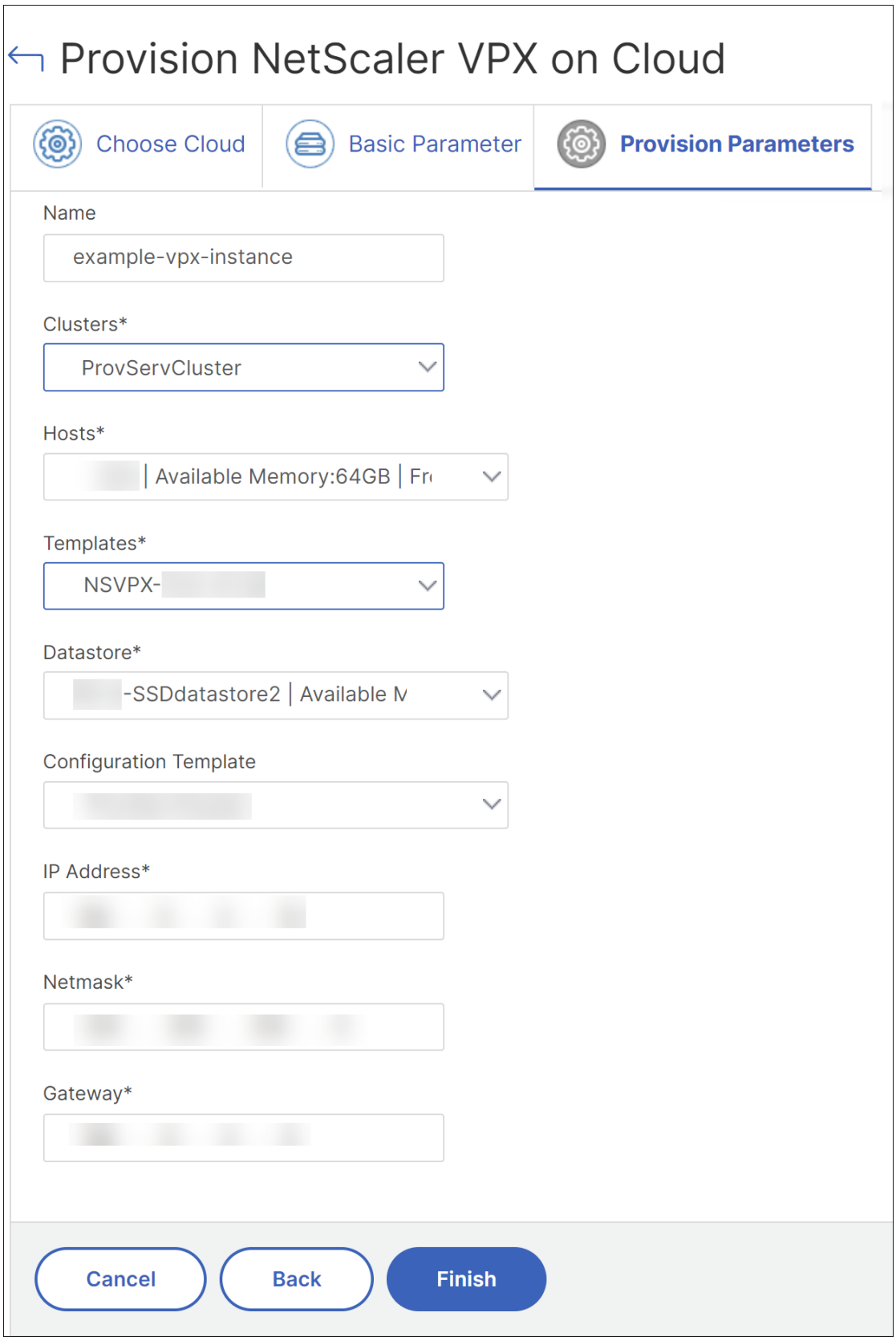


5. Click **Next**.
6. In **Provision Parameters**, specify the following details:
   - **Clusters** –Select the cluster where you want to provision an instance.
   - **Hosts** –Select the required host from the list.
   - **Templates** –Select the template from the list that you want to apply to an instance.
   - **Datastore** –Select the datastore from the list.
   - **IP address** –Specify an IP address to an instance.

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

- **Net mask** –Specify a net mask to an instance.
- **Gateway** –Specify a gateway to an instance.

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



7. Click **Finish** to provision a VPX instance.

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

Rediscover multiple NetScaler VPX instances

September 27, 2025

You can rediscover multiple NetScaler VPX instances in your NetScaler Console setup. Also, you can rediscover multiple NetScaler VPX instances when you want to view the latest states and configurations of those instances. The NetScaler Console server rediscovers all the NetScaler VPX instances and checks whether the Citrix NetScaler instances are reachable.

To rediscover multiple NetScaler VPX instances:

1. In a web browser, type the IP address of the NetScaler Console server (for example, http://192.168.100.1).
2. In the **User Name** and **Password** fields, enter the administrator credentials. The default administrator credentials are `nsroot` and `nsroot`.
3. Navigate to **Infrastructure > Instances > NetScaler** > **VPX** tab and select the instances you want to rediscover.
4. In the **Select Action** menu, click **Rediscover**.
5. When the confirmation message for running the Rediscover utility appears, Click **Yes**.

   The screen reports the progress of rediscovery of each of the NetScaler VPX instances.

Unmanage an instance

September 27, 2025

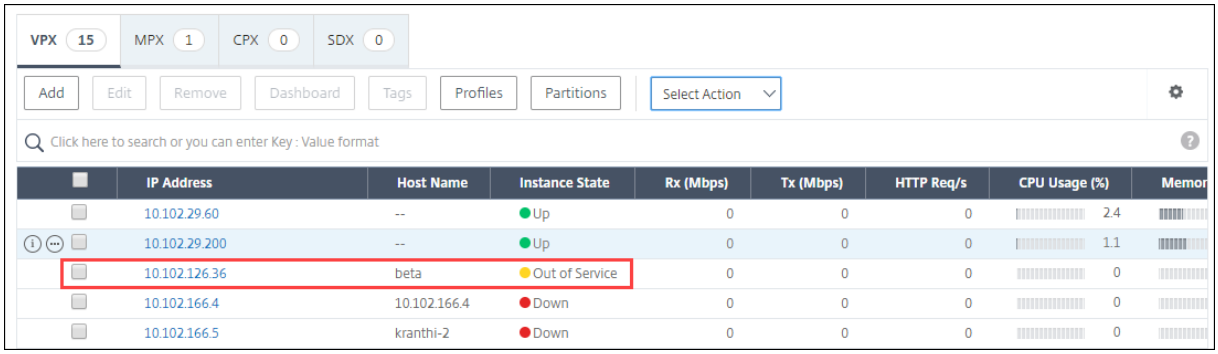
If you want to stop the exchange of information between NetScaler Console and the instances in your network, you can unmanage the instances.

To unmanage an instance:

Navigate to **Infrastructure > Instances > NetScaler** > **VPX** tab. In the list of instances, either right-click an instance and then select **Unmanage**, or select the instance and from the **Select Action** list, select **Unmanage**.

The status of the selected instance changes to **Out of Service** as shown in the following figure.

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



The instance is no longer managed by NetScaler Console, and it no longer exchanges data with NetScaler Console.

Trace the route to an instance

September 27, 2025

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. 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.

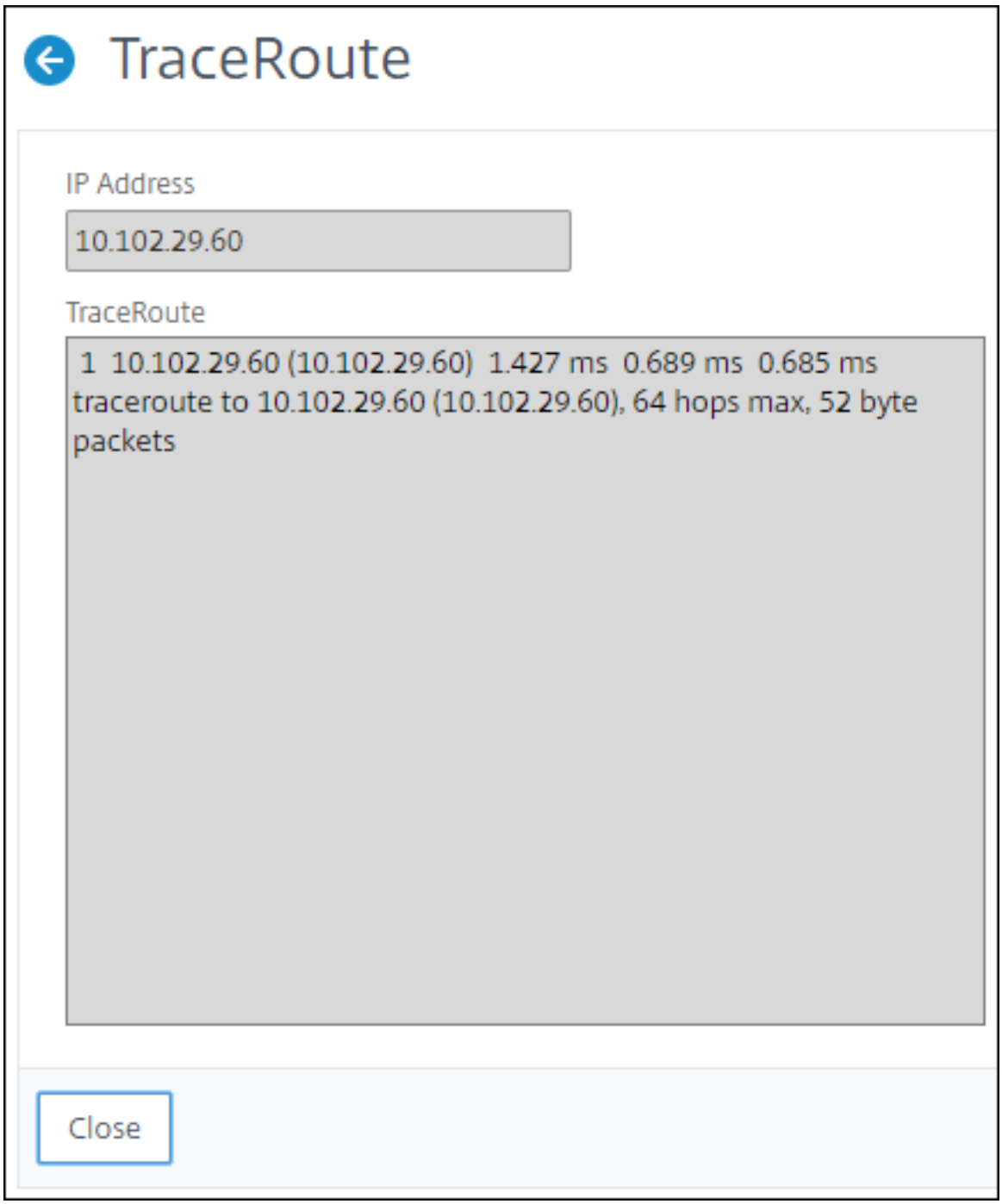
Traceroute also records the time taken by a packet to travel from one hop to another. If there is any interruption in the transfer of packets, traceroute shows where the problem exists.

To trace the route of an instance:

1. In NetScaler Console, navigate to **Infrastructure > Instances > NetScaler** > **VPX** tab.
2. In the list of instances, either right-click an instance and then select **TraceRoute** or select the instance and from the **Select Action** menu, click **TraceRoute**.

The **TraceRoute** message box shows the route to the instance and the amount of time, in milliseconds, consumed by each hop.

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



View NetScaler-owned IP addresses

September 27, 2025

You can view the IP addresses configured on NetScaler instances directly from NetScaler Console GUI.

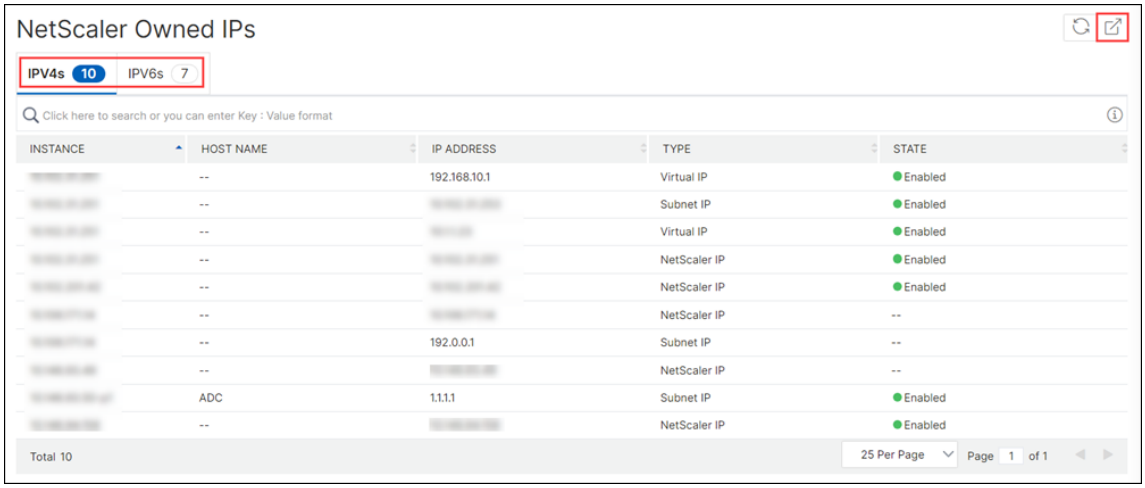
© 1997–2025 Citrix Systems, Inc. All rights reserved.

You can perform the configuration changes and other operations only on NetScaler instances.

To view the NetScaler-owned IP addresses, navigate to **Infrastructure > Instances > NetScaler Owned IPs**.

This feature displays both IPv4 and IPv6 addresses configured on NetScaler instances. The types of IP addresses include:

- NetScaler IP address
- Subnet IP address
- Virtual IP address
- ADNS service IP address
- GSLB IP address
- Cluster IP address
- Mapped IP address



Export NetScaler-owned IP addresses

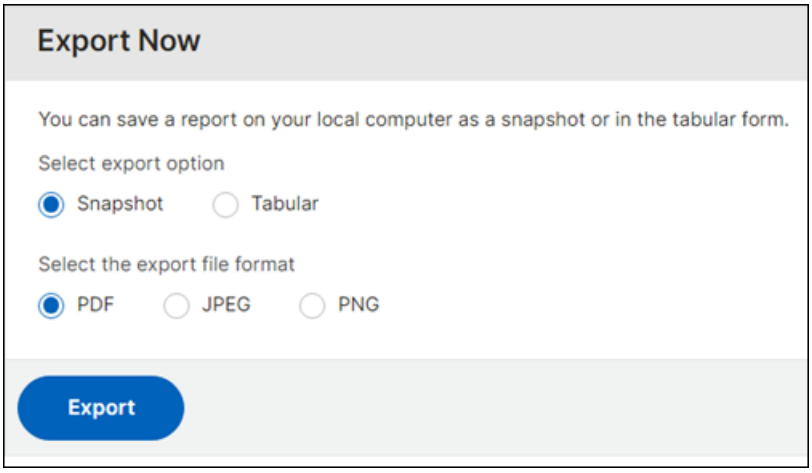
To export NetScaler-owned IP addresses:

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:

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

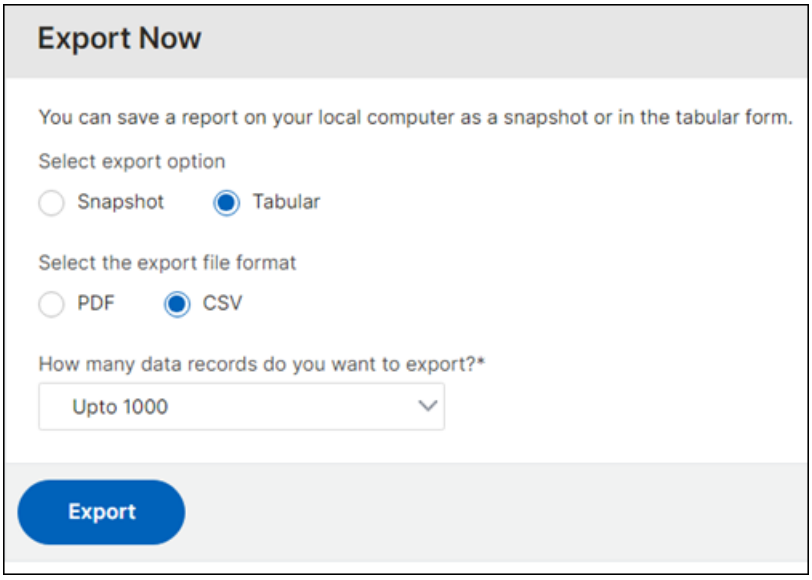
a) Select the export file format: PDF, JPG, or PNG.



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:

1. Navigate to **Infrastructure > Instances > NetScaler Owned IPs**.
2. On the **NetScaler Owned IPs** page, click the export icon at the top-right corner.

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

3. On the **Export Reports** page, click **Schedule Export**.
4. On the **Schedule Export** page, enter the following details:
    a) Enter the subject and description.
    b) Select the export type.

        For **Snapshot** export type:

        - Select the export file format: PDF, JPG, or PNG.

        For **Tabular** export type:

        - Select the export file format: PDF or CSV.
        - Select the number of data records to export from the list.

    c) Select the recurrence: Daily, Weekly or Monthly.
    d) Select the export time.
    e) Select how to send the exported IP addresses: Email, Slack or both.

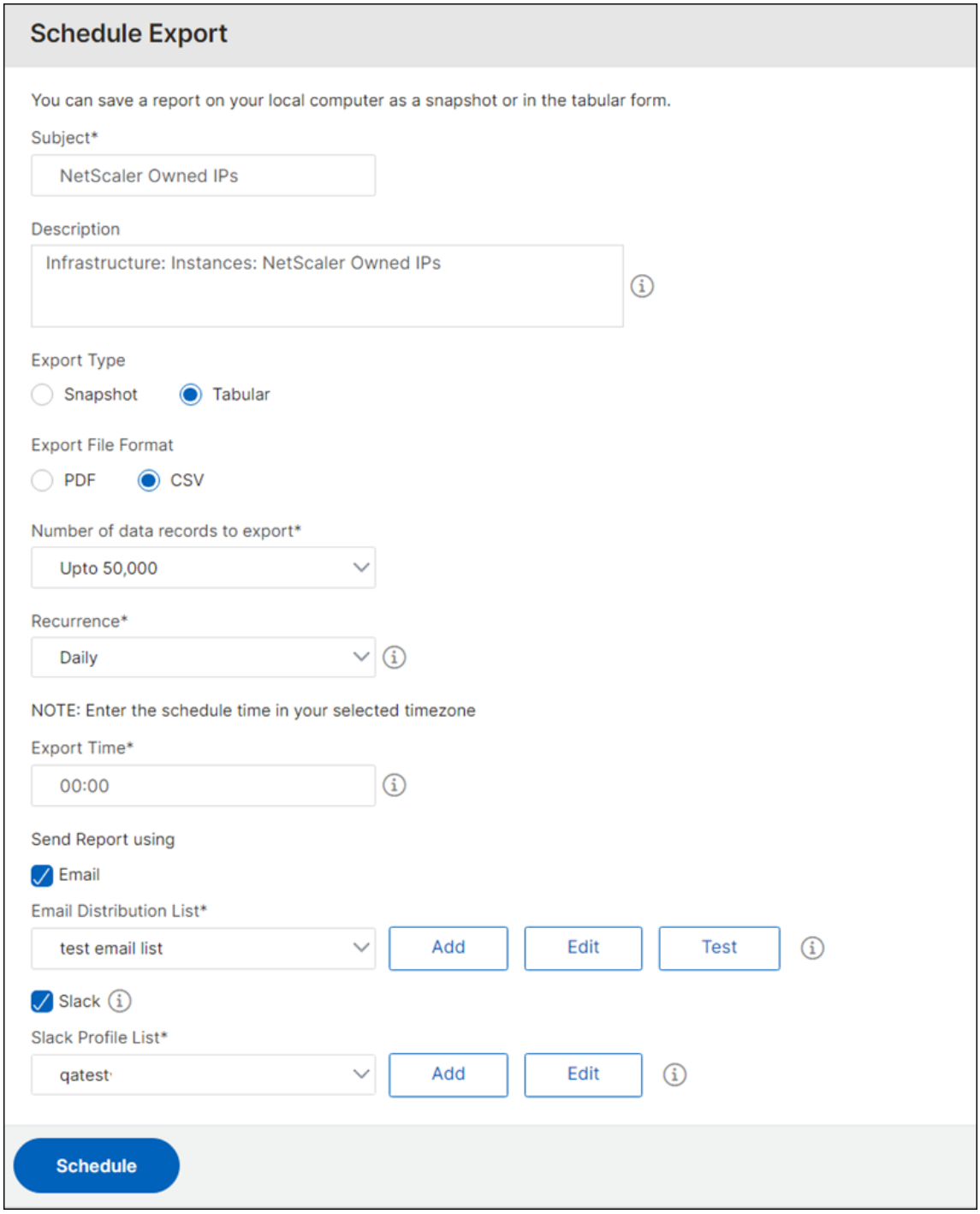
        For Email:

        - Select **Email** and choose the email distribution list to send the list of NetScaler-owned IP addresses.
            - To add an email distribution list, click **Add** and specify the email server details.
            - To edit an email distribution list, click **Edit**.
            - To verify that the email distribution list is working, click **Test**. This will send a test email to the selected email distribution list.

        For Slack:

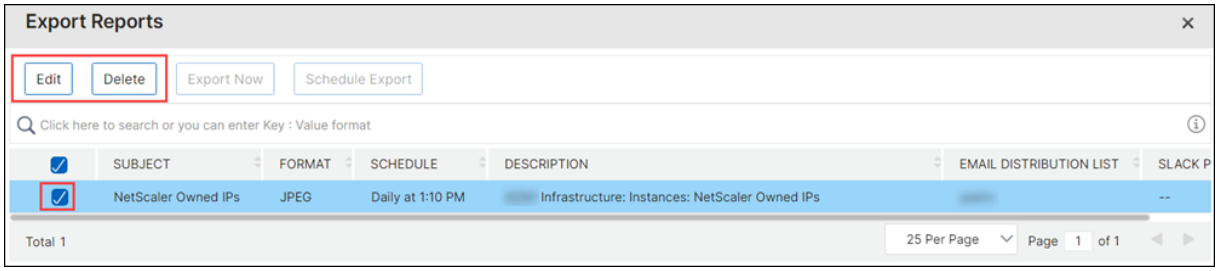
        - Select **Slack** and choose the Slack profile list to send the list of NetScaler-owned IP addresses.
            - To add a Slack profile, click **Add** and specify the **Profile Name**, **Channel Name**, and **Token** of the Slack channel.
            - To edit an existing Slack channel, click **Edit**.
5. Click **Schedule** to schedule the export.

© 1997–2025 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. After editing the selected schedule, click **Save** to save the edited changes. **Delete** deletes the schedule.

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



Replicate configurations from one NetScaler instance to another

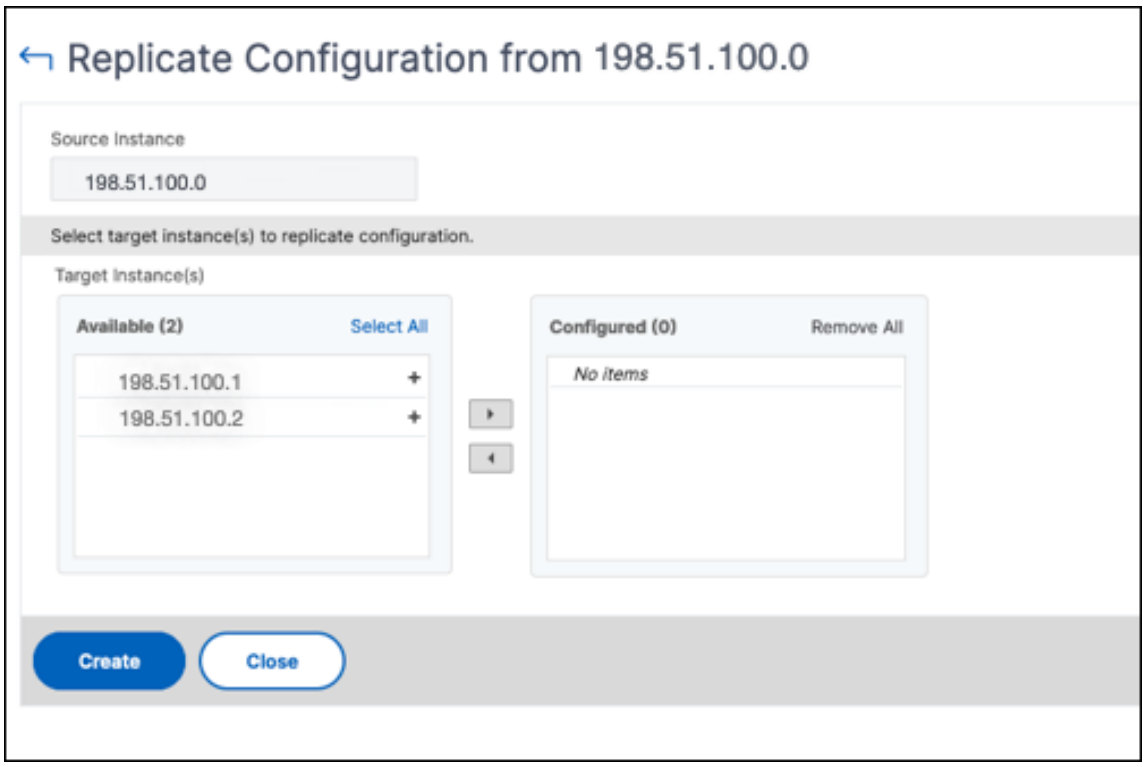
September 27, 2025

You can use the Replicate Configuration feature of NetScaler Console to copy configurations from a NetScaler instance and replicate it on a single instance or many instances.

To replicate configurations from one instance to other NetScaler instances

1. Navigate to **Infrastructure > Instances > NetScaler**. Select the source instance whose configurations you want to replicate on other instances and from the **Select Action** list, click **Replicate Configuration**.
2. In **Replicate Configuration**, select the target instance on which you want to apply the configurations from the source instance. You can replicate the configurations from a single source instance to a single instance or many target instances.

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



3. Click **Create**.

The replicated configurations are added to the list of NetScaler® instances. To view the status of the replicated instances, click the refresh icon.

> **Note:**
>
> During replication, all the network IPs from the source instance are replicated to the target instance. If the target instance is in a different network from the source instance, the IPs in the target instance might not be reachable. When IPs are not reachable, the status of the entities in the target instance is shown as Down.
>
> To view the status of the entities configured on your managed NetScaler instance, navigate to **Infrastructure > Network Functions**.

SSL certificate management

September 27, 2025

Any organization or individual website that requires handling confidential or sensitive information must have an SSL certificate. SSL certificate on a web server helps guarantee the authenticity of the web server to the connecting client. It not only authenticates a website's identity but also helps in generating the session key, which is used later for encryption of the entire session.

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

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 Citrix NetScaler appliance, is used to complete asymmetric key (or public key) encryption and decryption.

NetScaler Console provides you a unified console to automate the installation, updating, deletion, linking, and download of SSL certificates. It helps in retaining the reputation of the website and customer trust. NetScaler Console now streamlines every aspect of certificate management for you. Through a unified console, you can configure automated policies to ensure the recommended issuer, key strength, protocol, and algorithms as per organization IT policies. By doing so, you can keep close watch on certificates that are unused or about to expire.

You can obtain an SSL certificate and key in either of the following ways:

- From an authorized certificate authority (CA), such as Verisign
- By generating a new SSL certificate and key on the NetScaler appliance

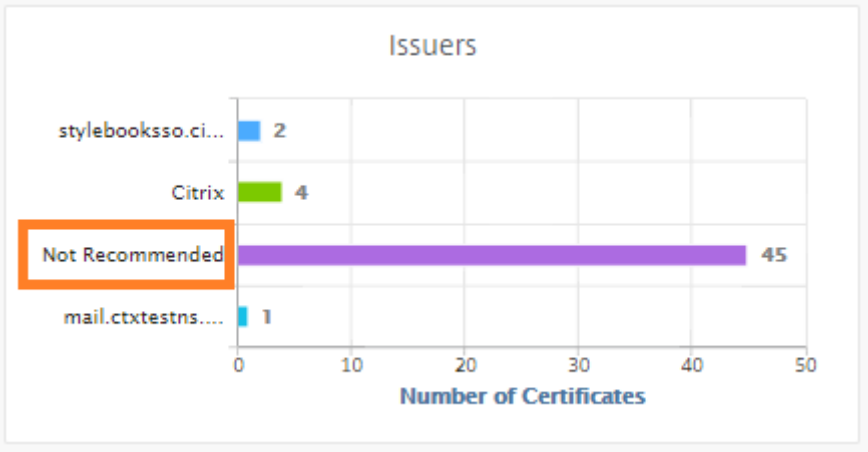
Enterprise SSL policy settings

Every enterprise has its own SSL policy and defines the requirements that all SSL Certificates must adhere to. Security has always been among the top priorities across all enterprise users and hence SSL settings play an important role.

For example, an ABC Company mandates that all certificates must have minimum key strengths of 2,048 bits and above. The certificates must be authorized by trusted CA or issuers. Administrators must check all such SSL parameters to ensure that the certificates abide by the company policy. It is a tedious job to verify each certificate manually. To overcome this scenario, the NetScaler Console helps you to configure enterprise SSL policy settings, and shows any non-compliance certificate with the “Not Recommended”tag.

You can view the summary of the non-compliance (Not Recommended) certificates on the SSL Dashboard.

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



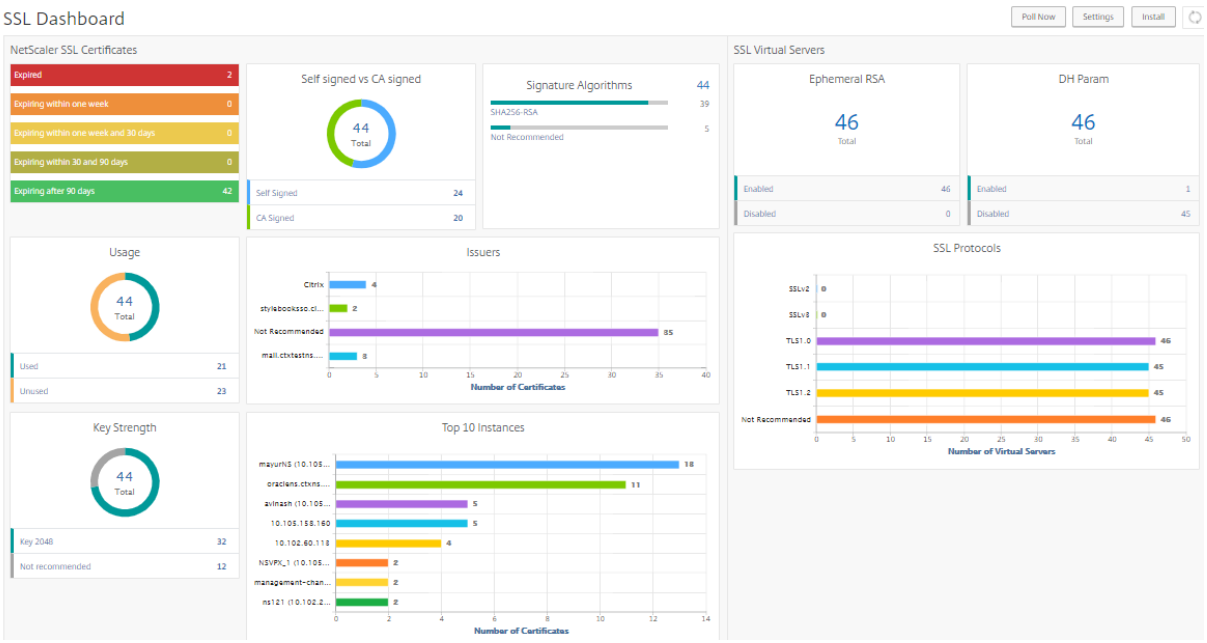
> **Note**
>
> The "Not Recommended"certificates are categorized based on different parameters, and you can view them in relevant components.

How the NetScaler Console certificate works

SSL Dashboard provides you a visual presentation of all the SSL certificates that are installed on different NetScaler instances. SSL dashboard includes the following information for each certificate installed on NetScaler instances. It is categorized based on the following:

- **Self-signed vs CA signed.** The self-signed vs CA signed section helps you to segregate the certificates into Self-signed certificates and, CA signed certificates.
- **Signature Algorithms.** This section segregates the SSL certificates based on signature algorithms being used for encryption.
- **Usage.** This section segregates your SSL certificates based on used and unused certificates. Unused certificates demand special attention as they might have been missed to be bound to the virtual servers.
- **Issuers.** This section segregates the SSL certificates based on the issuer of the certificates.
- **Key Strength.** This section segregates the SSL certificates based on the key strength of a private key.
- **Top 10 Instances.** This section provides the details of the top 10 NetScaler instances based on the number of SSL certificates installed.

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



SSL certificate management use cases

The following use cases describe how you can use the SSL certificate to manage and monitor the certificates across multiple NetScaler instances.

Install SSL certificates

Imagine, you have a fleet of NetScaler instances across, on which you have to deploy the required SSL certificates. NetScaler Console provides you a unified console to deploy the SSL certificates across multiple NetScaler instances in one attempt.

For example, you might want to install some SSL certificates on one or more NetScaler instances. With this approach, you can minimize the manual intervention of installing the SSL certificate on each NetScaler instance. You can do a bulk installation of SSL certificates across one or more NetScaler instances.

To obtain a summary of the SSL certificates, log on to **NetScaler Console**, and then navigate to **Infrastructure > SSL Dashboard**.

Notification settings for certificate expiry

In this use case, you might have many certificates across multiple NetScaler instances, and it becomes an overhead to track the expiry of each certificate. It is a tedious job for you to track each certificate

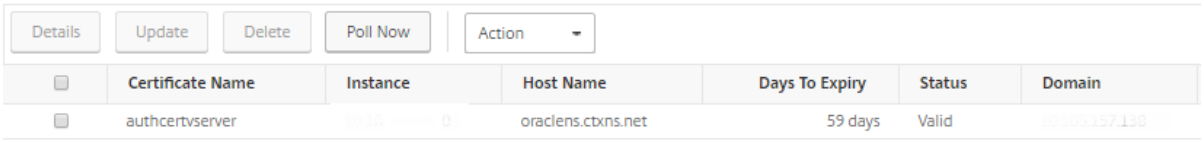
© 1997–2025 Citrix Systems, Inc. All rights reserved.

manually and update it before it expires. To avoid such scenarios, you can configure NetScaler Console to send the notifications or alerts to the configured email, pager, Slack, or ServiceNow profiles. This way you can stay abreast of the certificates expiry dates and renew the certificates well before the expiry dates.

For example, you might forget to track the certificate that is nearing expiry. And the certificate expires causing service outage, which might affect numerous applications to the users. With NetScaler Console certificate expiry notification settings, you can avoid such unforeseen scenarios.

You can view the summary and track the certificates that are nearing expiry on the **SSL Dashboard**.

To view the report of certificates expiring in any duration, you can click the tile to get the details of all such certificates expiring in that window.



Renewal of certificates

You can now renew the certificates from NetScaler Console. You can either renew the existing certificates or create the certificates based on the following:

Update the existing certificate In this use case, you have to update an existing certificate once you receive a renewed certificate from the certificate authority (CA). You can now update the existing certificates from NetScaler Console without logging into NetScaler instances.

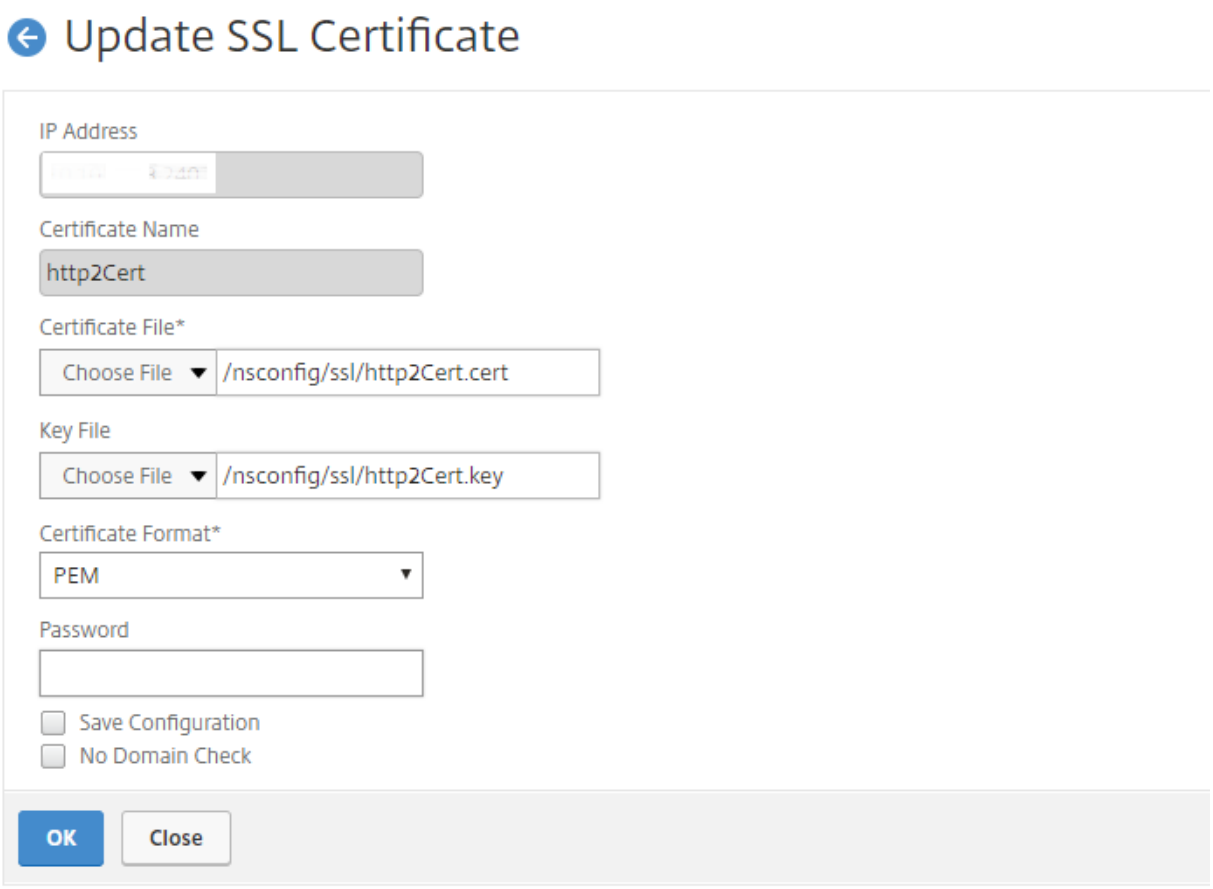
For example, there might be some changes or modifications to the existing certificates. The CA issues renewed certificates. Instead of going to the NetScaler appliance, you can now update the SSL certificate from NetScaler Console.

To update any certificate, log on to NetScaler Console, then navigate to **Infrastructure > SSL Dashboard**.

Select the certificate you want to update, and click **Update**.

You have an option to update the relevant fields of the selected certificate from NetScaler Console.

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

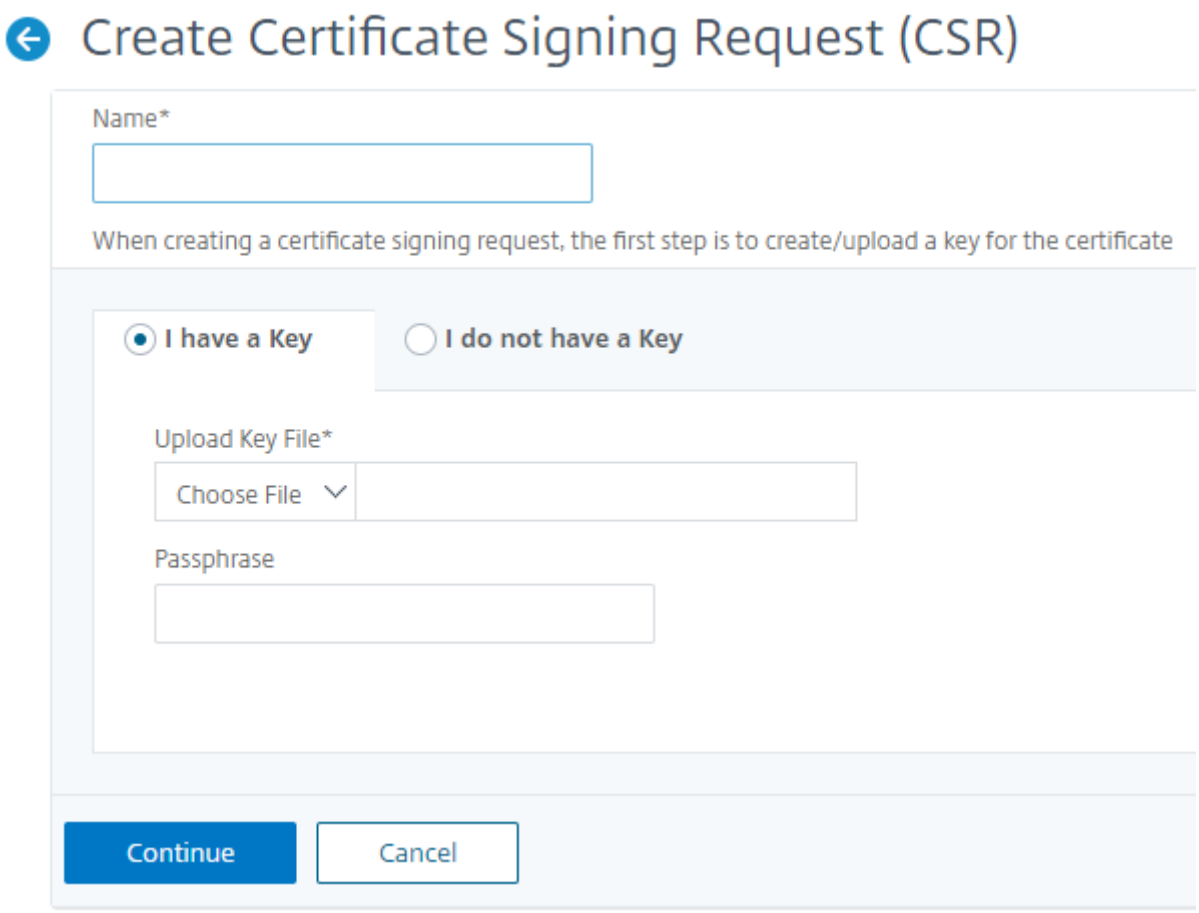


Create certificate signing request Imagine a use case where one of the SSL certificates does not comply with the organization policies. You want to get a new certificate from the certification authority. You can now generate a certificate signing request (CSR) from NetScaler Console. A CSR and a public key can be sent to a CA to obtain the SSL certificate.

To determine and create CSR, select the desired certificate and click **Create CSR**.

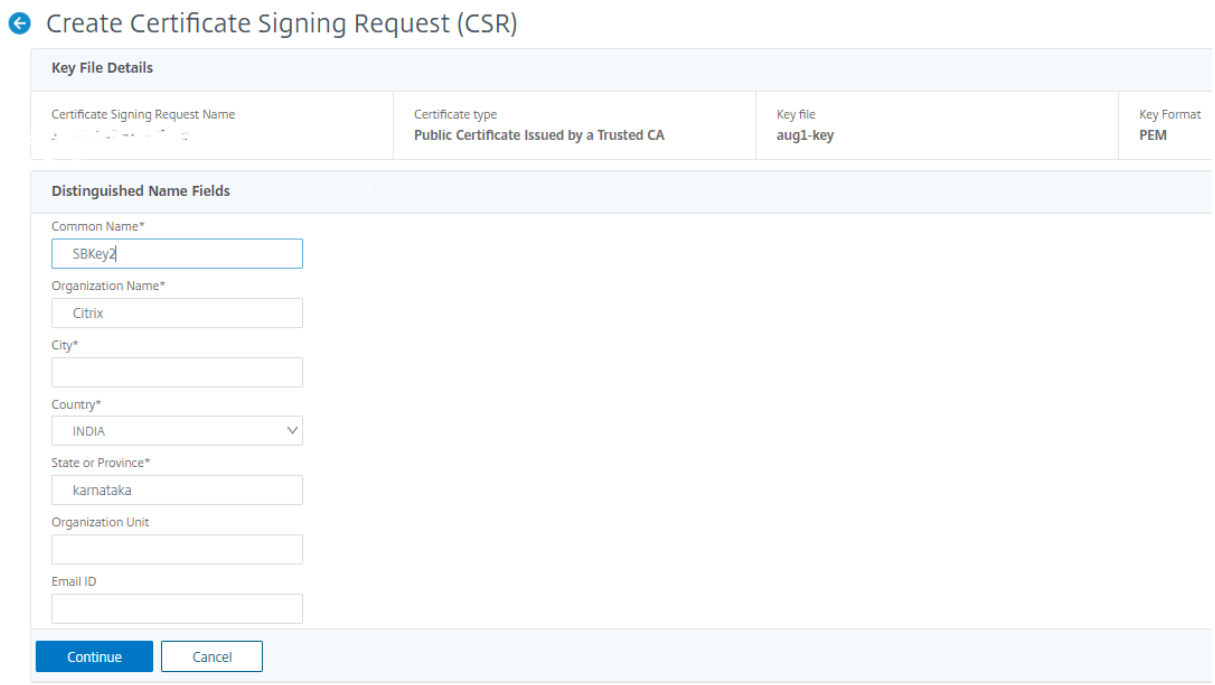
You need to have a public or private key value pair. To upload a key, click **Choose File** and select from the list. To create a key, select **I do not have a Key option** and specify the relevant parameters.

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



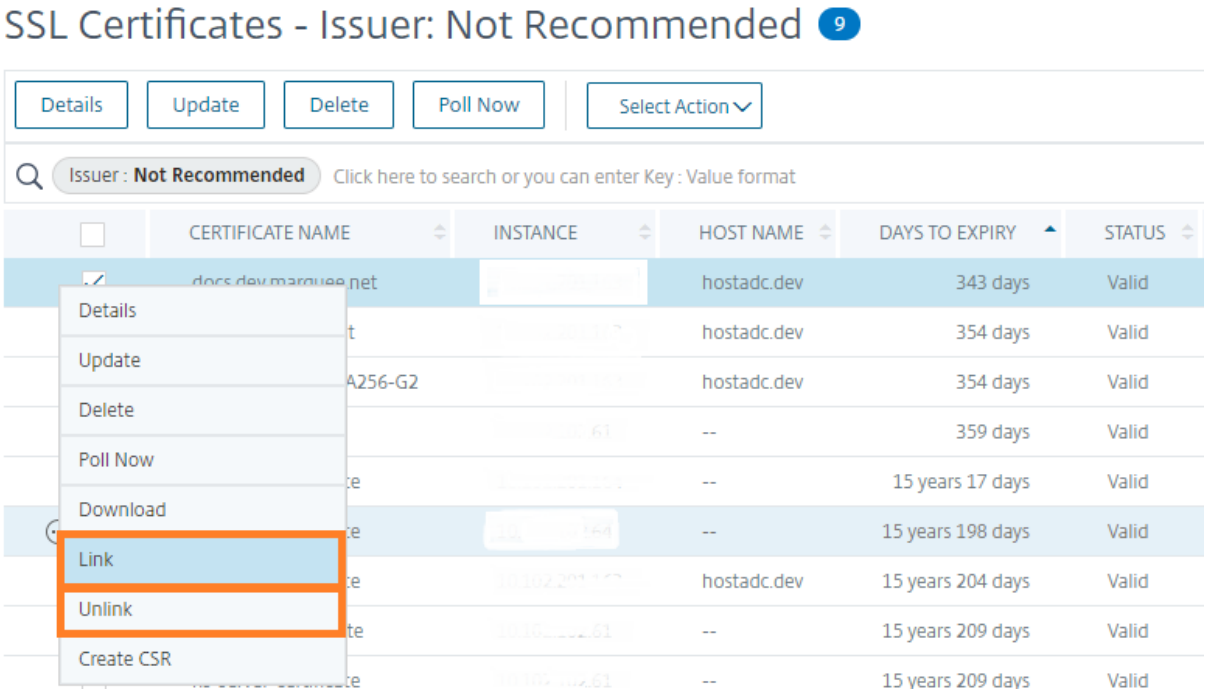
To give more details of the selected key like Common Name, Org Name, City, Country, State, Org Unit, and Email ID to create the CSR.

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



Link and unlink SSL certificates

You can bind multiple SSL certificates to each other to create a certificate bundle. To link a certificate to another certificate, the issuer of the first certificate must match the domain of the second certificate.



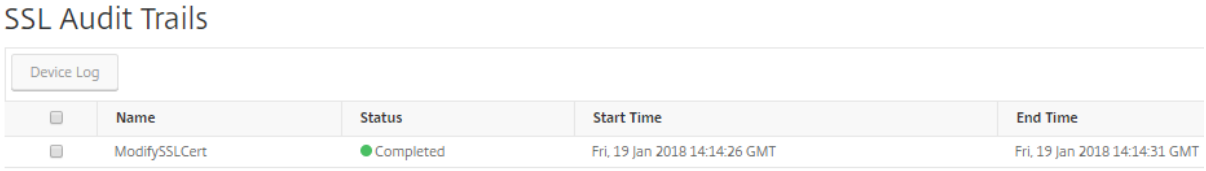
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Audit logs

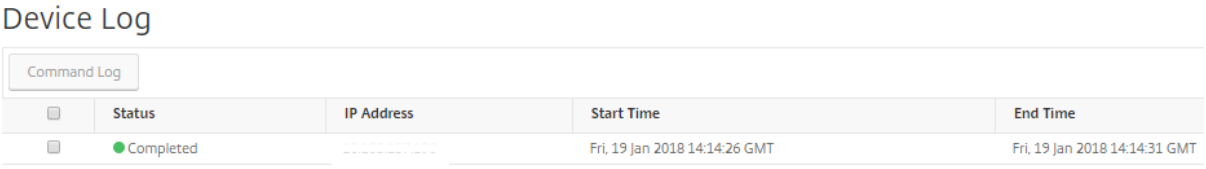
Audit Logs is a collection of text log files generated by the NetScaler Console. It shows a history of SSL certificates that are added, modified, and changed by using NetScaler Console to the specific NetScaler appliance. The Audit Logs also shows the IP Address of the NetScaler appliance, Status, Start Time, and End Time of the particular operation.

In this example, you might want to verify the change that has taken place over a period to the particular certificate. And you have an option to view the history of changes to the certificate over the Device Log and Command Log.

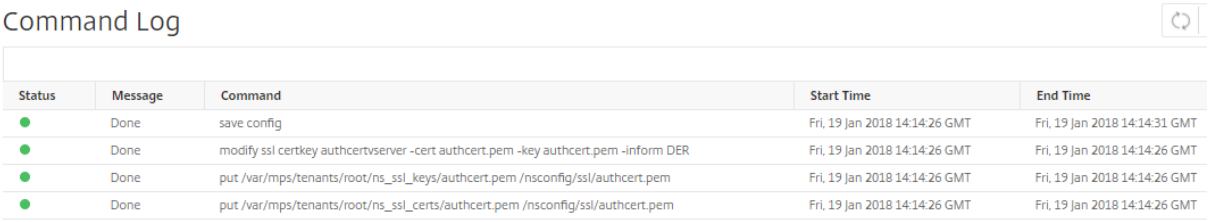
To determine the information of SSL certificates, on the **SSL Dashboard**, click **Audit Log**. The application summary includes the SSL certificates status with Start Time and End Time.



To determine the information of the NetScaler appliance of a particular SSL certificate, choose the relevant certificate check box of your choice. Click **Device Log**.



To view the information of command type, and message, click **Command Log**.



Automated certificate renewal by using the ACME protocol

November 25, 2025

NetScaler Console supports the Automated Certificate Management Environment (ACME), an open protocol designed to automate the renewal of SSL/TLS certificates.

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

Previously, the network administrators had to undergo the labor-intensive, multi-stage manual process of renewing the certificates. ACME support mitigates these challenges by providing a robust framework for automated certificate renewal to perform the following actions:

- Request new certificates from trusted Certificate Authorities (CAs).
- Validate domain ownership using automated methods (For example, DNS-01 challenge).
- Renew certificates automatically before expiry.

ACME support in NetScaler® Console

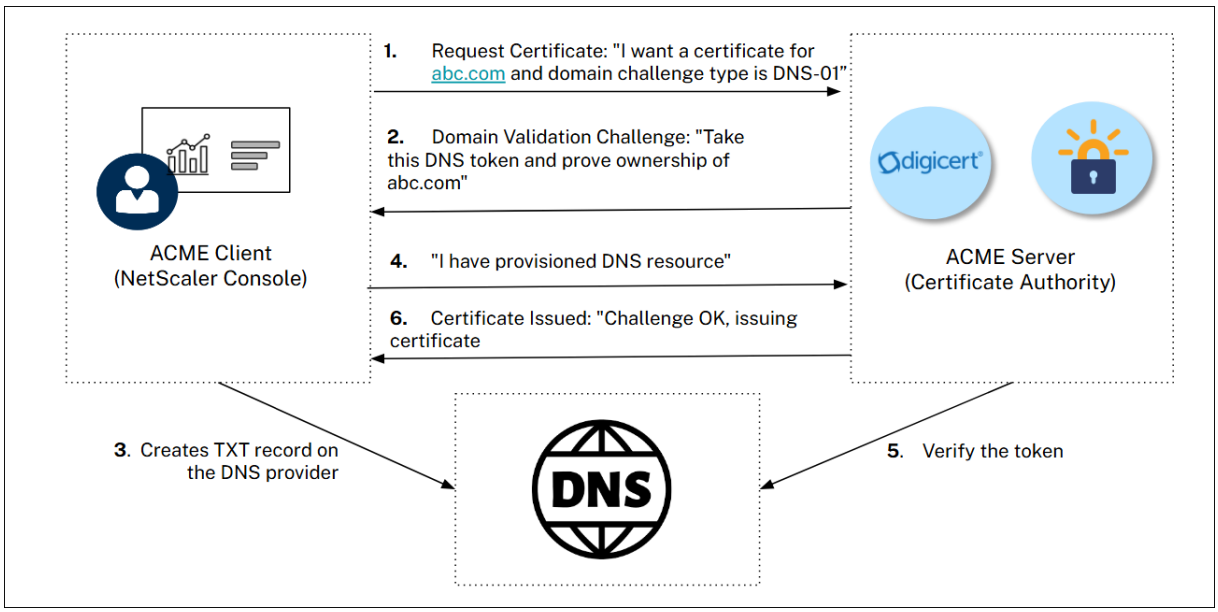
NetScaler Console uses the `acme.sh` client and supports the following Certificate Authorities:

- Let's Encrypt
- DigiCert

The following steps explain how automated certificate renewal happens in NetScaler Console:

1. When NetScaler Console initiates a certificate request for a domain using the `acme.sh` client, the client connects to the chosen Certificate Authority (for example, Let's Encrypt or DigiCert).
2. The CA issues a challenge to prove domain ownership, which in this case is a DNS-01 challenge.
3. NetScaler Console using pre-configured credentials, automatically updates the DNS TXT record for the domain with the value provided by the CA.
4. The CA validates the TXT record, confirming domain ownership.
5. Upon successful validation, the CA issues the SSL/TLS certificate to NetScaler Console.
6. NetScaler Console stores the certificate in the respective store (Certificate store/Zero-touch store).
7. Based on the renewal window provided by you, NetScaler Console automatically repeats this process for renewal before the certificate's expiration date.

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



With ACME support in NetScaler Console, you can perform the following actions:

- Automatically renew certificates before they expire
- Switch from one CA to another during renewal
- Generate or upload CSR and request for new certificate

The following are the key benefits:

- Fully Automated Lifecycle with no manual intervention for certificate issuance or renewal.
- Customizable Renewal Schedule that suits organizational needs (for example, set to renew 7 days before expiry).
- Eliminates downtime due to expired certificates.
- Reduced operational overhead by automating expiry tracking and renewals.
- Improved security posture with always-valid, CA best-practice aligned certificates.

Configuration steps for ACME integration

Integrating ACME is a one-time process and includes the following steps:

- Step 1: Configure Certificate Authority (CA).
- Step 2: Select certificates for renewal.
- Step 3: Add a DNS provider and map the respective domains.

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

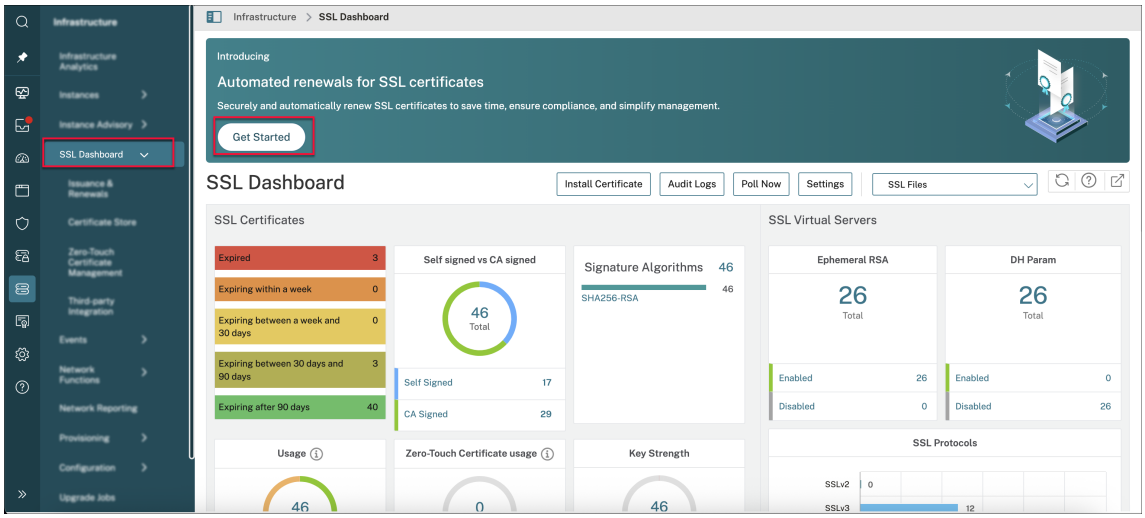
Prerequisites

- Ensure that you must have a valid account for your Certificate Authority (CA) and license for the same.
- Ensure that you have DNS provider access credentials.

Step 1: Configure Certificate Authority (CA)

Perform the following steps to register the Certificate Authority (CA) that is used for renewals:

1. Navigate to **Infrastructure > SSL Dashboard**. If you are configuring ACME for the first time, then you see a banner with "Automated renewals for SSL certificates". Click **Get Started**.

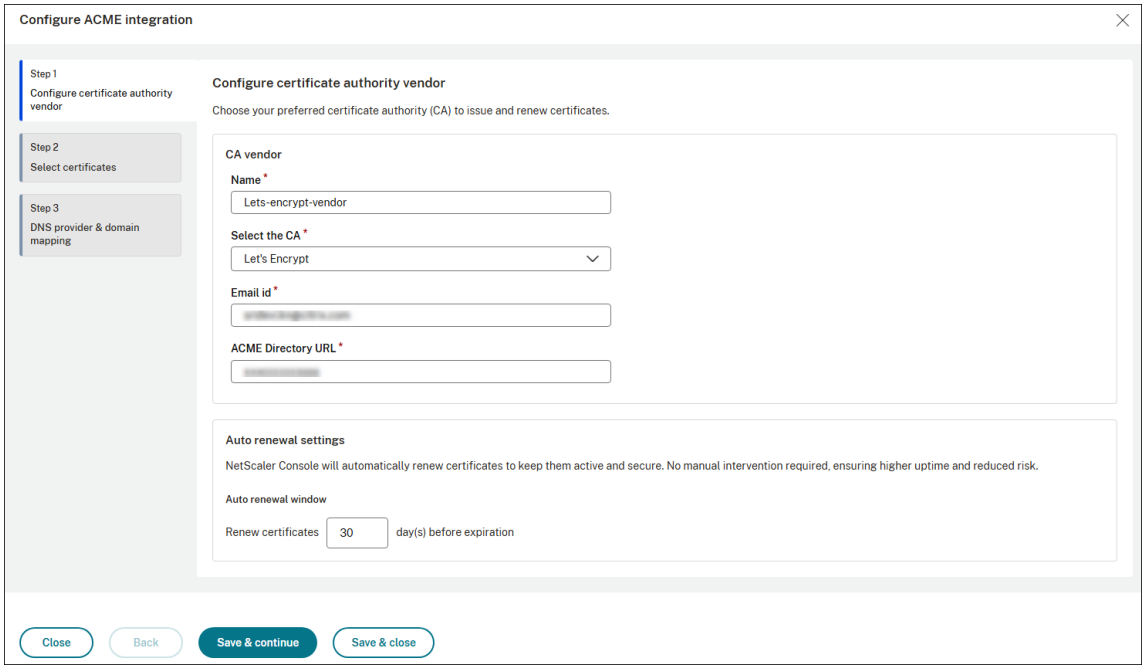


   or

   Navigate to **Infrastructure > SSL Dashboard > Third-party Integration > CA Vendors** and click **Add**.

2. Enter a name and select the CA vendor. Currently, only **Let's Encrypt** and **DigiCert Inc** are supported.
3. Provide the other details such as email address, ACME Directory URL.
4. Enter the number of days before which the NetScaler Console must automatically renew the certificates.
5. Click **Save and continue**. NetScaler Console attempts to connect to the CA. If connectivity fails, review the details provided, correct the configuration details, and then retry.

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

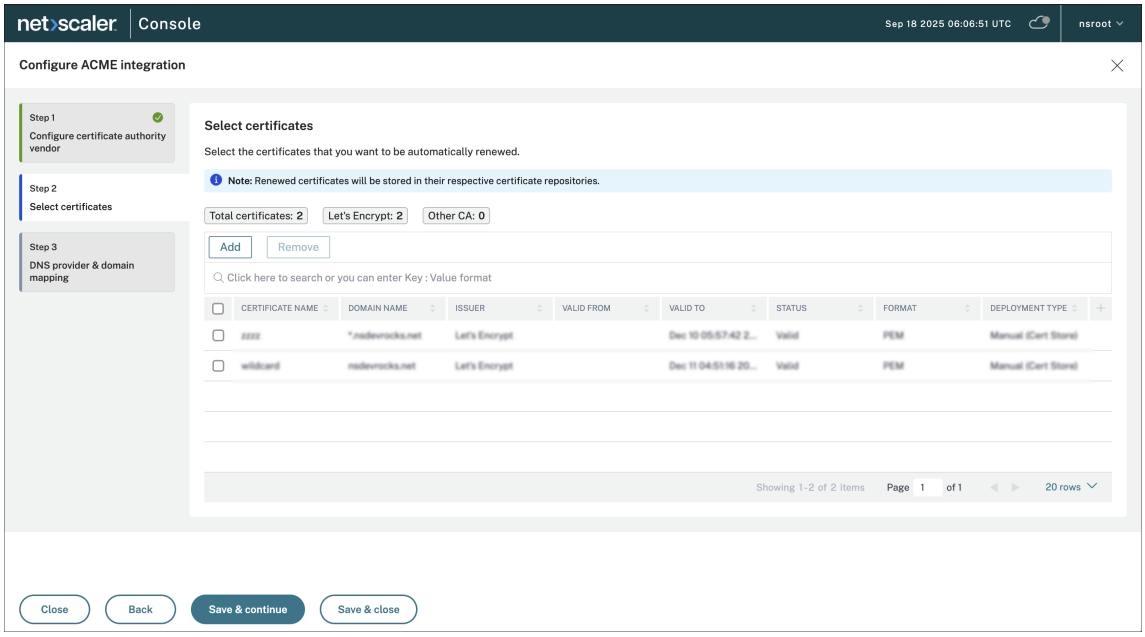


Step 2: Select certificates for renewal

After CA details are added, NetScaler Console automatically scans all certificates (from both the certificate store and the Zero-touch store) and lists the certificates issued by the configured CA separately. Review the certificates listed.

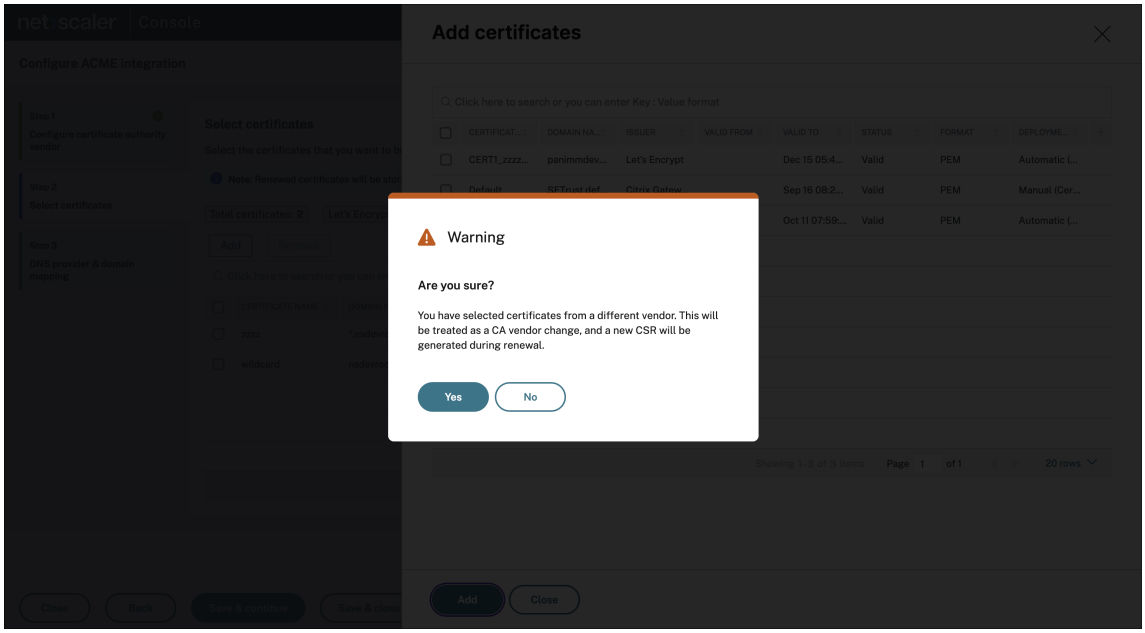
1. Select the certificates that you want to automatically renew. For example, If you configure Let's Encrypt as the CA and have 2 certificates from Let's Encrypt and 2 from another vendor, the dashboard displays: `Let's Encrypt: 2 and Other CA: 2`.

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



2. You can click **Add** to also add certificates issued by a different CA or **Remove** to remove certificates that you do not want to renew automatically. If you select certificates from a different vendor, you get a prompt to confirm the vendor change. Once you confirm, these certificates get renewed through the newly configured CA when their renewal window is reached.

> **Note:**
>
> Ensure that you do not have duplicate certificates in the Certificate store and Zero-touch certificate store. If there are duplicate certificates, then the renewal process happens twice for each store.



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

3. Click **Save and continue**.

> **Note:**
>
> Certificates remain in their respective stores after renewal. For example, if a certificate is stored in the certificate store, its renewed version is also placed in the certificate store. If the certificate is stored in the Zero-touch store, its renewed version is also placed in the Zero-touch store.
>
> Certificate deployment behavior depends on the store type.
>
> - If the certificates are stored in the certificate store, they must be manually deployed to NetScaler.
> - If the certificates are stored in the Zero-touch store, the certificates are automatically deployed to NetScaler without admin intervention.
>
> We recommend you to use Zero-touch Certificate Management for seamless, fully automated deployment of renewed certificates. For more information, see Zero-touch certificate management.

Step 3: Add a DNS provider and map the domains

1. Click **Add** on the **DNS provider & domain mapping** page.
2. Select the DNS providers from the **Select DNS provider** drop-down list. The DNS providers supported by the `acme.sh` are listed in the drop-down list. If you do not see your DNS provider in the list that means it is not supported.
3. Enter provider details such as Access key ID, Secret Access Key and click **Save** to save the configuration.
4. Click **Add Domain** under **Domain Mapping**.
5. Select the domains served by the configured DNS provider.

> **Important:**
>
> Ensure that each domain is linked to the correct DNS provider. NetScaler Console uses these mappings to perform the DNS-01 challenge automatically. During issuance or renewal, NetScaler Console creates the required TXT records in the mapped DNS provider. Once validation succeeds, the CA issues or renews the certificate. Certificates are renewed only when all associated domains are mapped correctly to their DNS providers.
>
> For example, if your organization uses Amazon Route53 as the DNS provider. First, add the Amazon Route53 credentials (Access Key ID and Secret Key) under DNS Provider Details. Then, map the domains managed by Amazon Route53 (for example: example.com,

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

> app.example.com). When a certificate for these domains is issued or renewed, NetScaler Console automatically creates the required TXT records in Amazon Route53. Once validation is successful, the CA issues or renews the certificates.

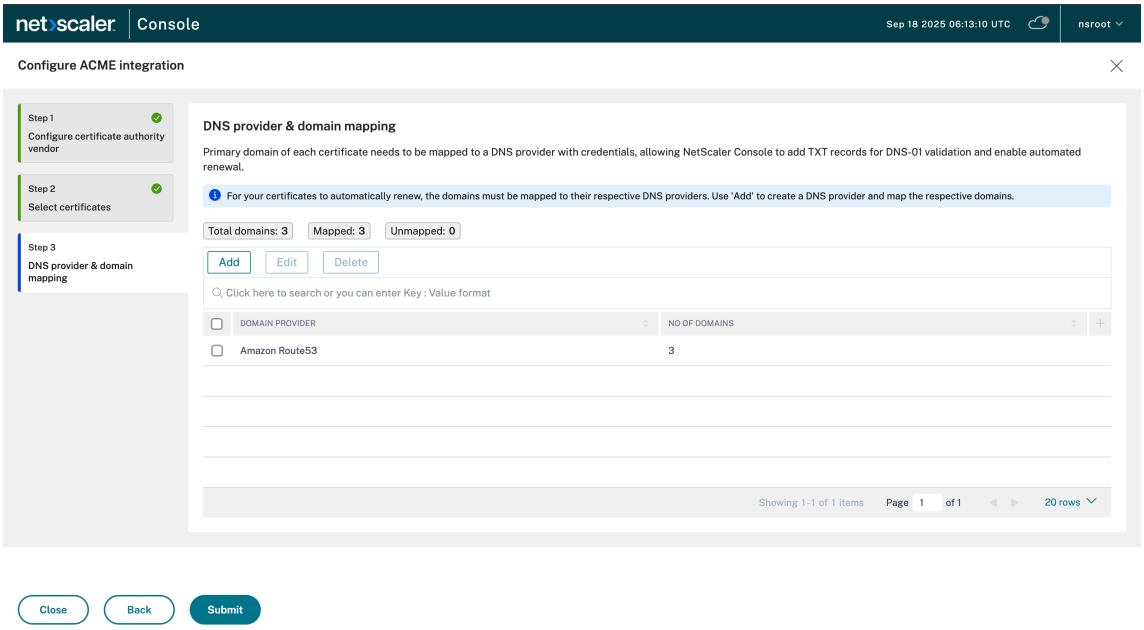
The following public DNS providers are supported:

- ACME DNS
- Active24
- Aliyun
- Alwaysdata
- Amazon Route53
- Azure DNS
- ClouDNS.net
- CloudFlare
- ConoHa
- Core-Networks
- DDNSS.de
- DNSMadeEasy
- DNSPod.cn
- DNSPod.com
- DNSimple
- DigitalOcean
- DirectAdmin
- DreamHost
- DuckDNS.org
- Exoscale
- FreeDNS
- Gandi LiveDNS
- GoDaddy.com
- Google Cloud DNS
- Hurricane Electric
- INWX
- ISPConfig 3.1
- Infoblox
- Knot DNS
- Leaseweb.com
- Linode
- Loopia
- LuaDNS
- MailinaBox
- MaraDNS

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

- Misaka.io
- MyDNS.JP
- NLnetLabs NSD
- NS1.com
- Name.com
- Namecheap
- Namesilo
- Neodigit.net
- Netcup
- Nexcess
- OPNsense
- Online.net
- OpenProvider
- Plesk XML
- PointHQ
- PowerDNS
- RcodeZero
- Schlundtech
- Selectel
- UltraDNS
- VSCALE
- Vultr
- Zilore
- Zonomi
- autoDNS-InternetX
- cyon.ch
- deSEC.io
- durabledns.com
- easyDNS.net
- hosting.de
- jdcloud.com
- nic.ru
- nsupdate
- one.com
- reg.ru

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



Once all three steps are completed, NetScaler Console configures the ACME CA server. The selected certificates are renewed for the mapped domains.
NetScaler Console periodically checks certificate validity and renews them before they expire (based on configured window). With no manual intervention required, certificates always stay valid and up to date.

Issuance and renewals

Navigate to **Infrastructure > SSL Dashboard > Issuance & Renewals** to check all the renewal activities and the new requests raised from the certificate issuance.

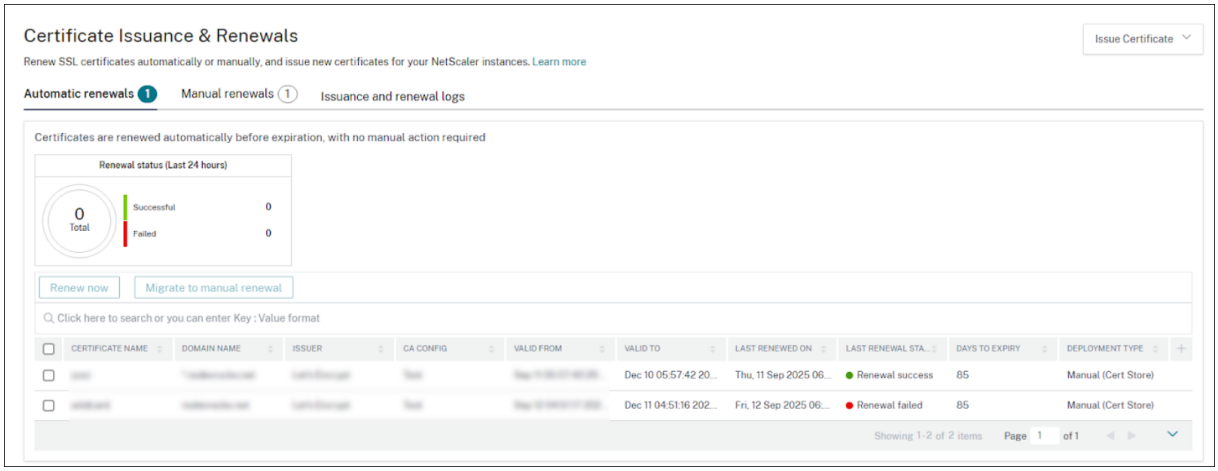
Automatic renewals

The **Automatic renewals** tab lists the certificates that are enrolled for automatic renewal. When the configured renewal window is reached, NetScaler Console renews them automatically.

You can also trigger an on-demand renewal before the scheduled renewal window. For on-demand renewal, select the required certificate, and click **Renew now**.

If you do not want some certificates to be automatically renewed, you can move to manual renewals. To transfer the certificates from automatic renewal to manual renewal, select the required certificates and click **Migrate to manual renewal**.

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



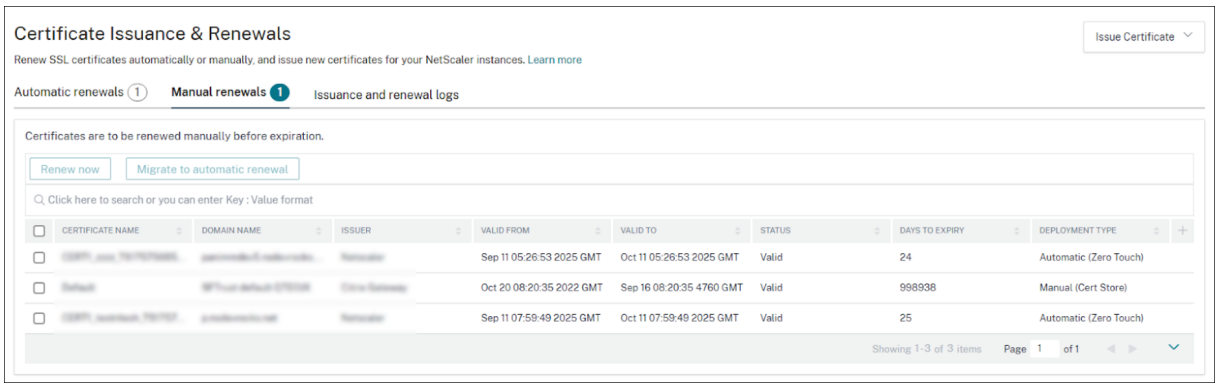
Manual renewals

The **Manual renewals** tab lists all the certificates that must be manually renewed. These certificates must be updated manually, either by renewing the certificate offline and uploading the new certificate to the appropriate store, or by using the **Renew now** option.

To renew a certificate, select a certificate and click **Renew now**. If the certificate is issued by a registered CA and its domain's DNS provider is configured, you can renew it on demand by using ACME without moving it to automated renewals.

You can also move a certificate to automatic renewal. To transfer the certificates from manual renewal to automatic renewal, select the required certificates and click **Migrate to automatic renewal**.

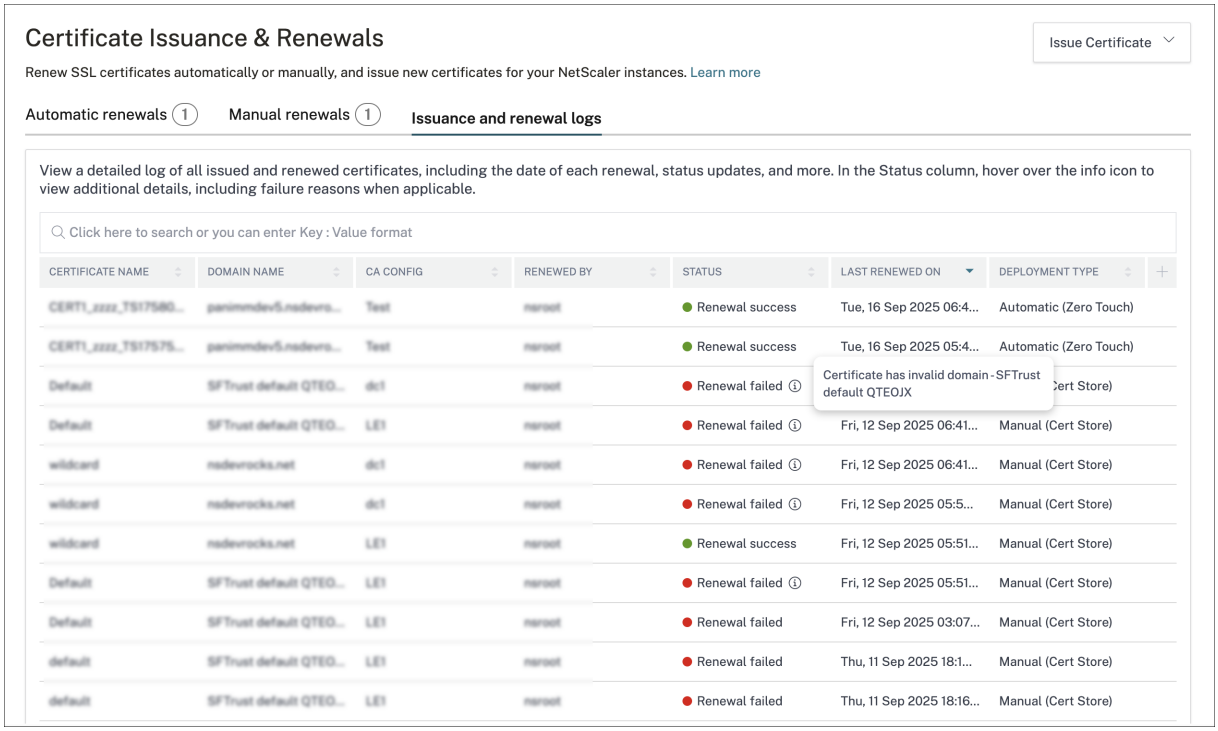
> **Note:**
>
> You can renew or migrate only one certificate at a time.



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

Issuance and renewal logs

The **Issuance and renewal logs** tab provides the list of certificate requests using ACME, including issuances and renewals. For a failed event, you can click the info icon to view detailed error information.



Issue a certificate

ACME integration in NetScaler Console supports requesting new certificates directly by using the ACME protocol. You can either create a CSR within NetScaler Console or upload an existing CSR to request new certificates.

Navigate to **Infrastructure > SSL dashboard > Issuances & Renewal** and click **Issue Certificate** and select one of the following based on your scenario:

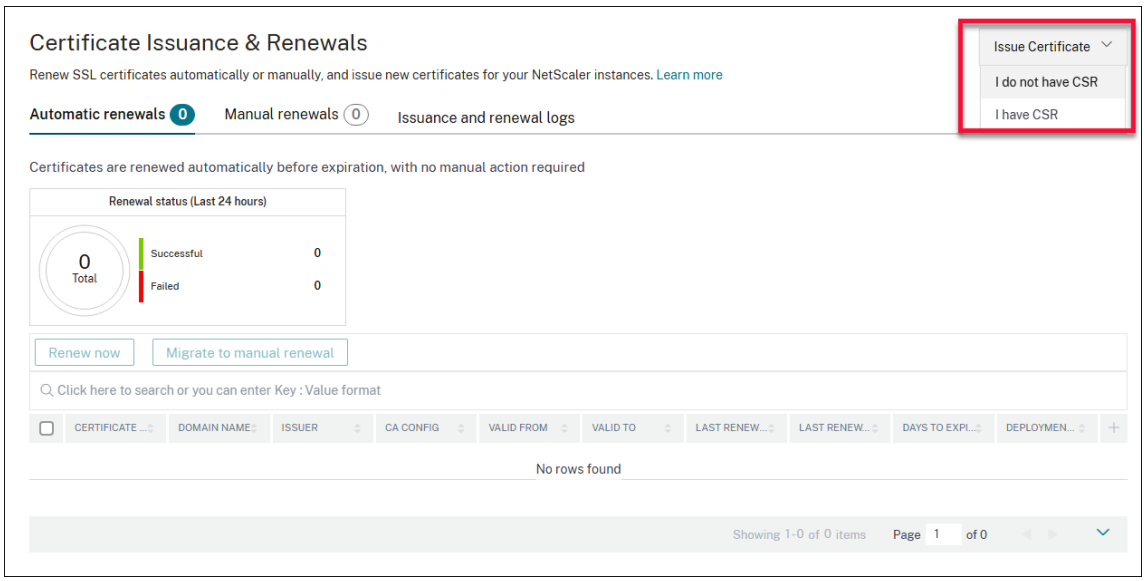
- **I do not have CSR**: If you don't already have a CSR, NetScaler Console allows you to generate one and issue a new certificate.
- **I have CSR**: If you already have a CSR generated offline, you can upload it to issue a certificate.

Issue a certificate without CSR

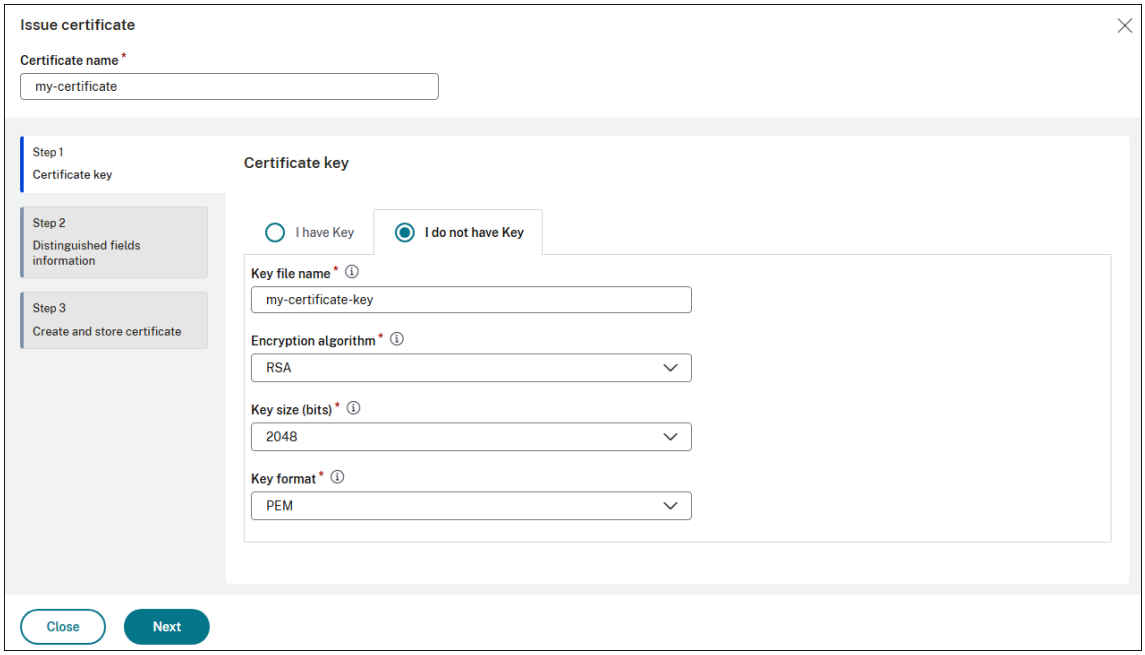
Perform the following steps to generate a CSR and issue a new certificate:

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

1. Navigate to **Infrastructure > SSL dashboard > Issuances & Renewal** and click **Issue Certificate** and select **I do not have CSR**.

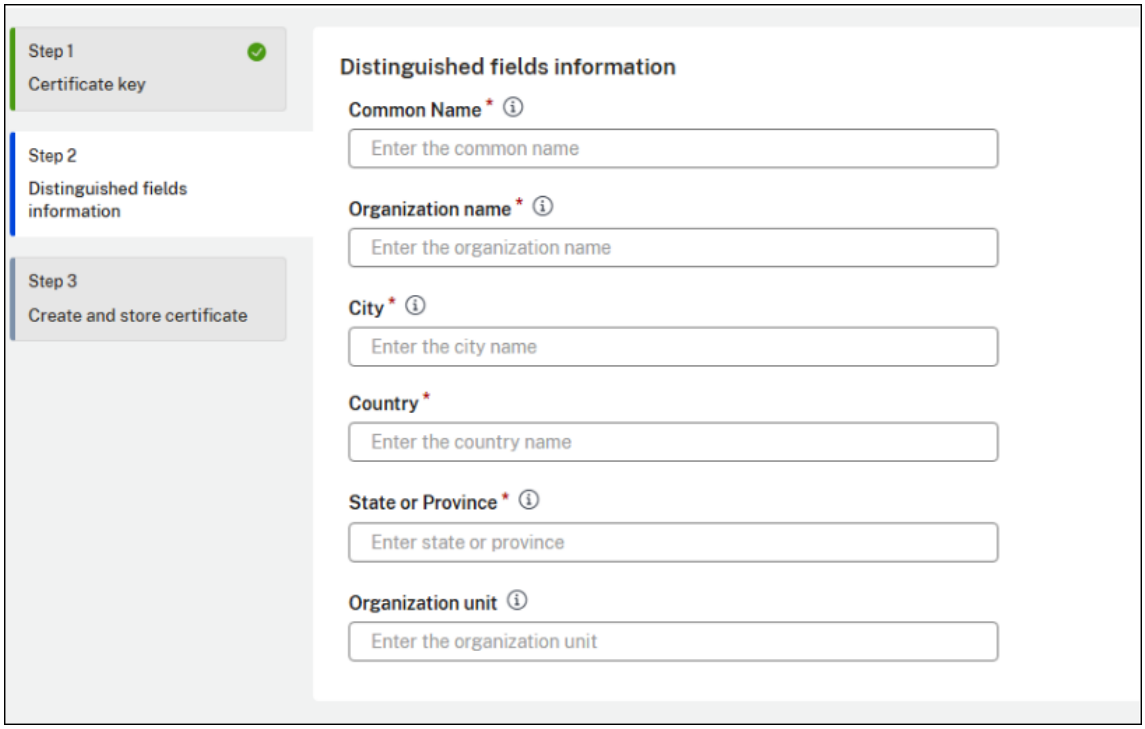


2. On the **Certificate key** page, either upload an existing key by selecting **I have a key** or generate a new one by selecting **I do not have a key**.

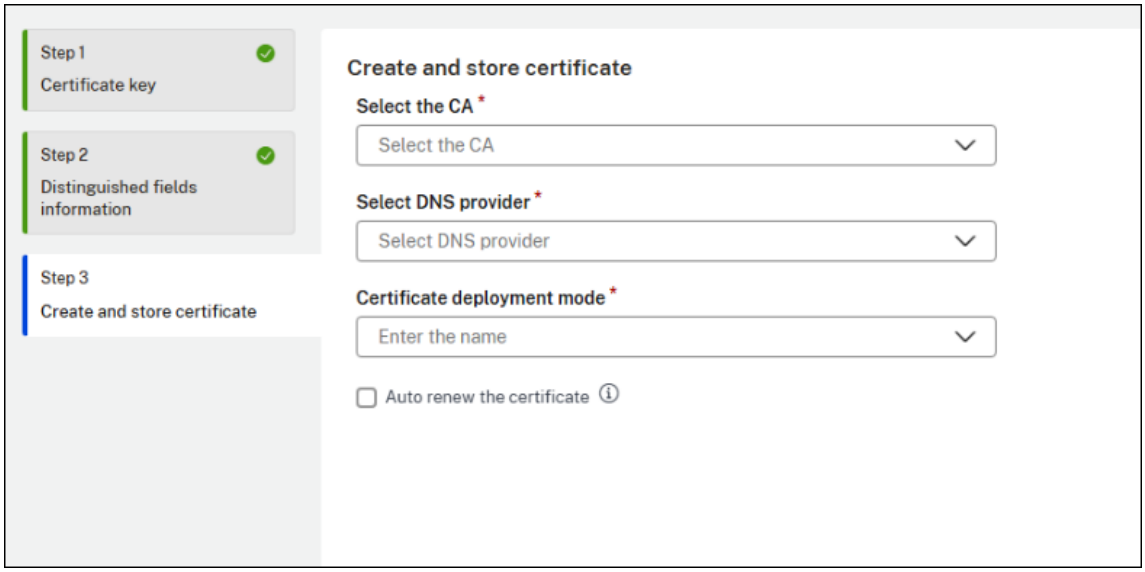


3. Enter the required CSR information.

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



4. Select the CA, DNS provider, and certificate deployment mode for the ACME request. Choose **Cert Store** for manual deployment, or **Zero Touch Store** for automatic deployment on NetScaler.
5. Select **Auto renew the certificate** if you want the certificate to be automatically renewed in future.



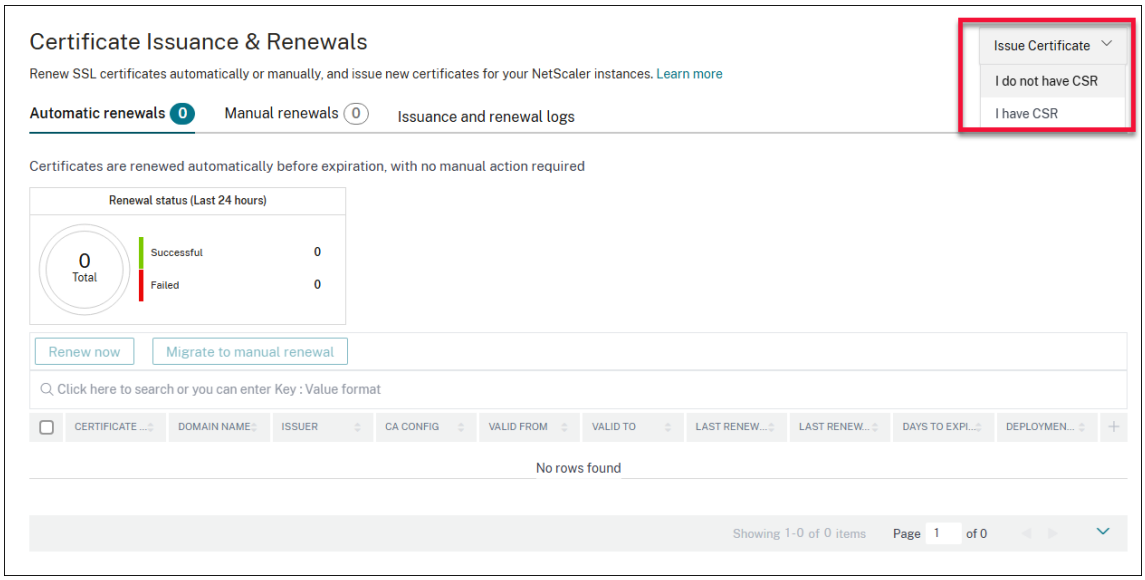
6. Click **Save**.

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

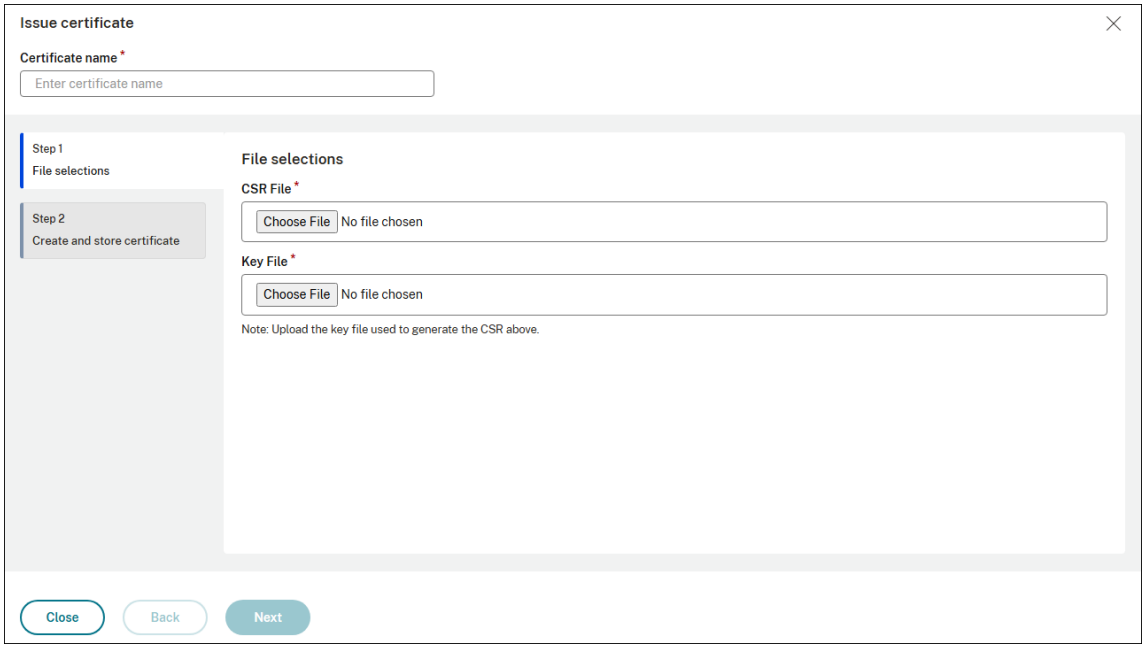
Issue a certificate with CSR

Perform the following steps if you already have a CSR generated offline and you want to upload it to issue a certificate:

1. Navigate to **Infrastructure > SSL dashboard > Issuances & Renewal** and click **Issue Certificate** and select **I have CSR**.



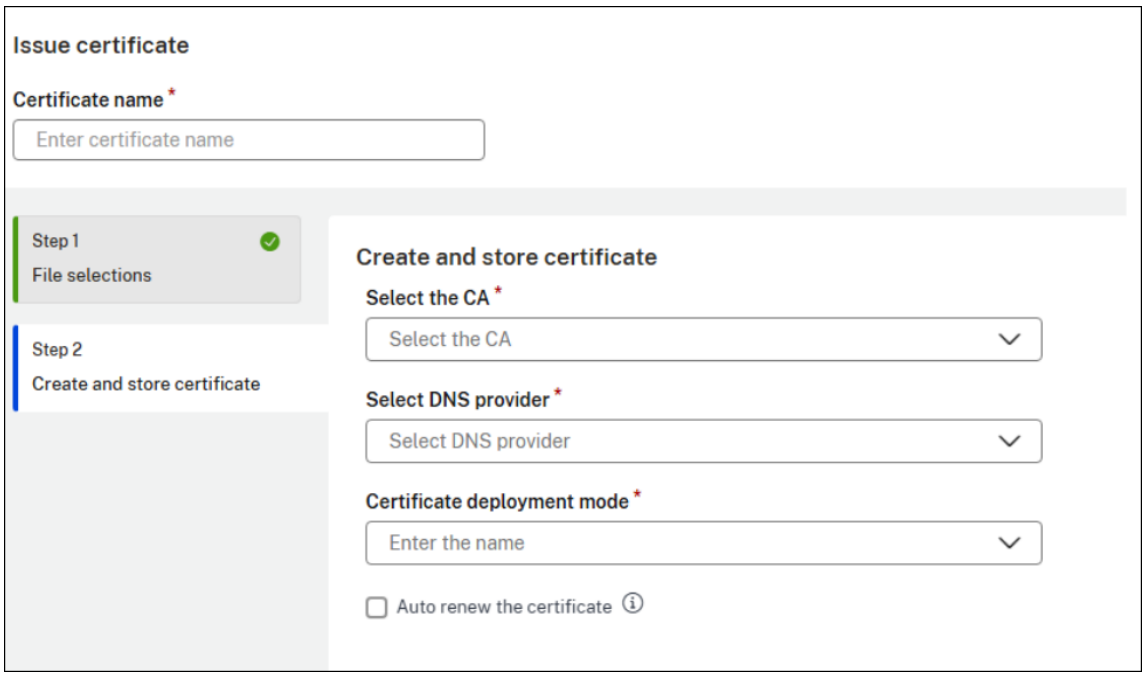
2. Choose the CSR file and associated key file from your local system.



3. Select the CA, DNS provider, and certificate deployment mode for the ACME request. Choose **Cert Store** for manual deployment, or **Zero Touch Store** for automatic deployment on NetScaler.

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

4. Select **Auto renew the certificate** if you want the certificate to be automatically renewed in future.



5. Click **Save**.

Third-party Integration

You can add and manage more than one CA vendor and DNS provider.

You can perform following actions from the **Third Party Integration** page:

- Add or edit a CA vendor
- Change the auto renewal settings
- Add or edit the certificate from an existing configured CA
- Add or edit a DNS provider
- Change domain mappings

Add or edit a CA vendor

You can register more than one CA vendor to manage certificates issued by different vendors. You can also edit the existing CA vendor details.

1. Navigate to **SSL dashboard > Third party integration > ACME > CA Vendors**. Click **Add**.
2. To add a CA vendor, provide a name for the CA vendor and select the CA.
3. To edit an existing CA vendor details, select the CA vendor and click **Edit**.

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

4. Add or update the required details.
5. Click **Save**.

Change the auto renewal settings

To change the auto renewal settings, perform the following steps:

1. Navigate to **SSL dashboard > Third party integration > ACME > CA Vendors**.
2. Select a CA vendor, and click **Edit**
3. In the **Configure certificate Authority vendor**, change the number of days as per your requirement the **Auto renew settings** section.
4. Click **Save and continue**.
5. Complete the workflow.

Add or edit the certificate from an existing configured CA

To add or edit the certificate from an existing configured CA, perform the following steps

1. Navigate to **SSL dashboard > Third party integration > ACME > CA Vendors**.
2. Select a CA vendor, and click **Edit**.
3. Navigate to **Step 2 Select certificates**, and add or remove the required certificates.
4. Click **Save and continue**.
5. Complete the workflow.

> **Note:**
>
> If the certificate has not been unmapped from the original CA, it does not appear in the selection list for the new CA.

Add or edit a DNS provider

To add a new DNS provider or edit existing domain mappings of existing DNS providers, perform the following steps:

1. Navigate to **SSL dashboard > Third party integration > ACME > DNS Providers**.
2. To add a DNS provider, click **Add**. Select the DNS provider, and click **Save**.
3. To edit an existing DNS provider, select a DNS provider and click **Edit**.
4. Add or update the required details.
5. Click **Save**.

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

Change domain mappings

To edit the domain mappings of existing DNS providers, perform the following steps:

1. Navigate to **SSL dashboard > Third party integration > ACME > DNS Providers**.
2. Select a DNS provider and click **Edit**.
3. Navigate to **Domain mapping**, and add or remove domains as required.
4. Click **Save**.

> **Important:**
>
> If a domain is unmapped, its certificate renewal stops. Always remap domains to a valid DNS provider to ensure that renewals continue.

Limitations

- Certificate renewal happens only for the DNS providers that are supported by `acme.sh`.

Troubleshoot issues related to automatic certificate renewal

A few common error messages that might occur and their associated root cause are listed in this section:

- **Certificate has invalid domain - ADCD** error is reported when the domain name in the certificate is not valid as per ACME requirements.
- **Invalid identifiers requested :: Cannot issue for "testdomain": Domain name needs at least one dot** is reported when the requested domain name is missing a dot (such as "example"instead of "example.com").
- **Could not get nonce from the CA server. Please check the CA server configuration.** is reported when the ACME client fails to obtain a nonce from the CA, often due to network or server issues.
- **Cannot initialize API for the CA server. Please check the CA server configuration.** is reported when the ACME client cannot initialize communication with the CA server, possibly due to misconfiguration.
- **Invalid domain name provided. Please check the domain name and try again.** is reported when the domain name format is invalid or not allowed by the ACME protocol.
- **Domains not changed. Certificate with same configuration already exists.** is reported when a certificate request is made with no changes to the domain list and the certificate already exists.

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

- **Error adding TXT record for domain validation. Please check the DNS configuration and try again.** is reported when the ACME client fails to add the required DNS TXT record for domain validation.
- **Signature does not match. Please check the server time as it may not be in sync.** is reported when there is a signature mismatch, often due to time synchronization issues between client and server.
- **Certificate is missing a DNS provider name.** is reported when no DNS provider is specified for DNS-based domain validation.
- **Renewal skipped as no active DNS providers are configured.** is reported when certificate renewal is attempted but no active DNS providers are configured.
- **Error validating contact(s) :: unable to parse email address** is reported when the contact email address provided is invalid or cannot be parsed.
- **Unable to process finalize order request. (For invalid ACME Directory URL)** is reported when the ACME client cannot finalize the order, often due to an invalid or unreachable ACME Directory URL.
- **DNS Provider - TestDNS does not exist or is not active.** is reported when the specified DNS provider is not found or is inactive in the system.
- **Config CA ID is empty/does not exist.** is reported when the CA configuration ID is missing or does not match any existing configuration.

Zero-touch certificate management

September 27, 2025

In NetScaler Console, you can configure zero-touch certificate management on the managed NetScaler instances running build **14.1-34.x** and later. With zero-touch certificate management, you eliminate manual interventions and build an in-memory zero-touch certificate store to serve the application requests. Navigate to **Infrastructure > SSL Dashboard > Zero-Touch Certificate Management** to upload all the certificates and keys on NetScaler Console, and enable it on the managed NetScaler instances. NetScaler periodically polls the certificate repository and delivers the necessary certificates as required.

With zero-touch certificate management, the following processes are automatically done by NetScaler®:

- Adding, binding, and linking the certificates
- Providing the certificates and keys in a specific order or together

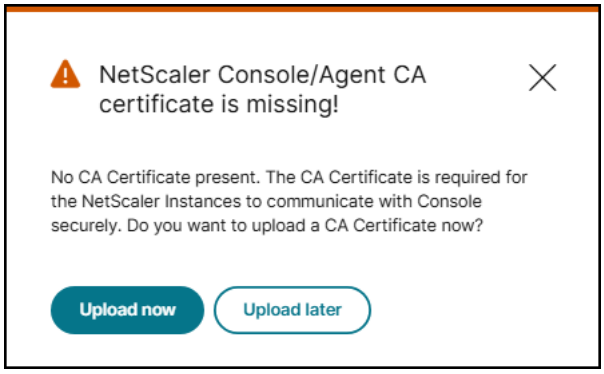
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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:

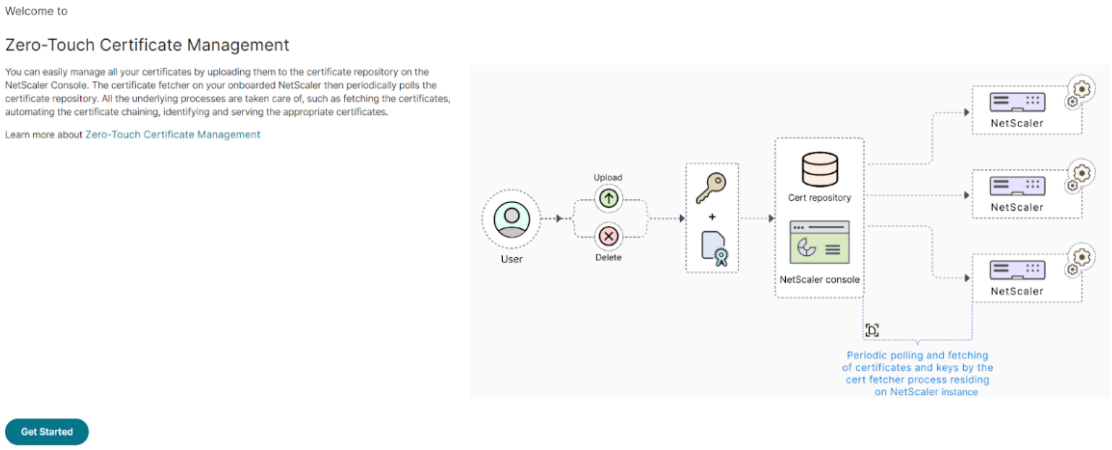
- NetScaler instances are running build 14.1-34.x or later and they are managed in NetScaler Console.
- Upload the certificates (in any format) and keys. Then, enable zero-touch on the managed NetScaler instances.
- Ensure that a valid CA certificate is present on NetScaler Console. If you have an updated 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.



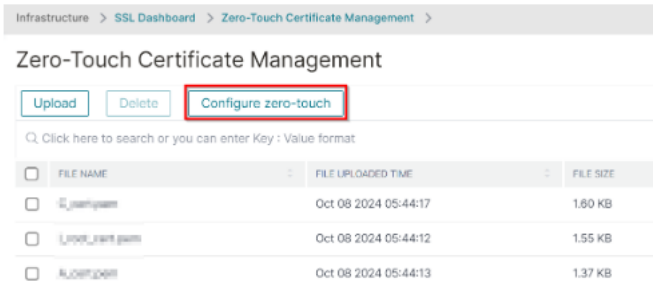
3. NetScaler instances running build 14.1-34.x or later are listed. You can either click **Configure zero-touch** to enable zero-touch or click **Skip** to proceed the next step.
4. Click **Upload** to upload all the certificates (can be in any format, such as .pem, .cer, and .crt).

> **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

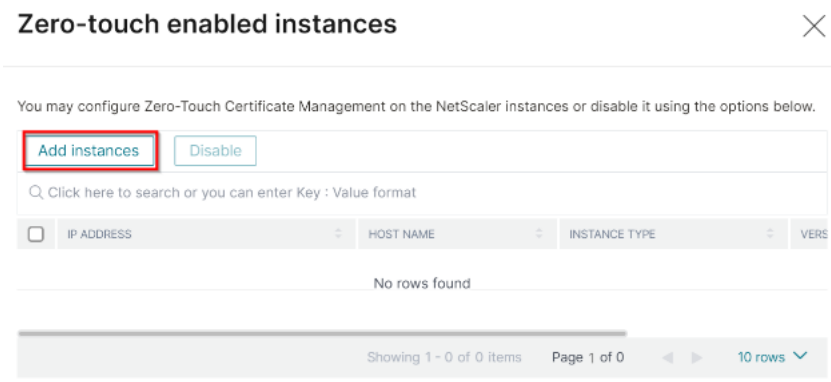
After you upload the certificates, you must enable zero-touch on the managed NetScaler instances.

1. From the **Zero-Touch Certificate Management** page, click **Configure zero-touch**.



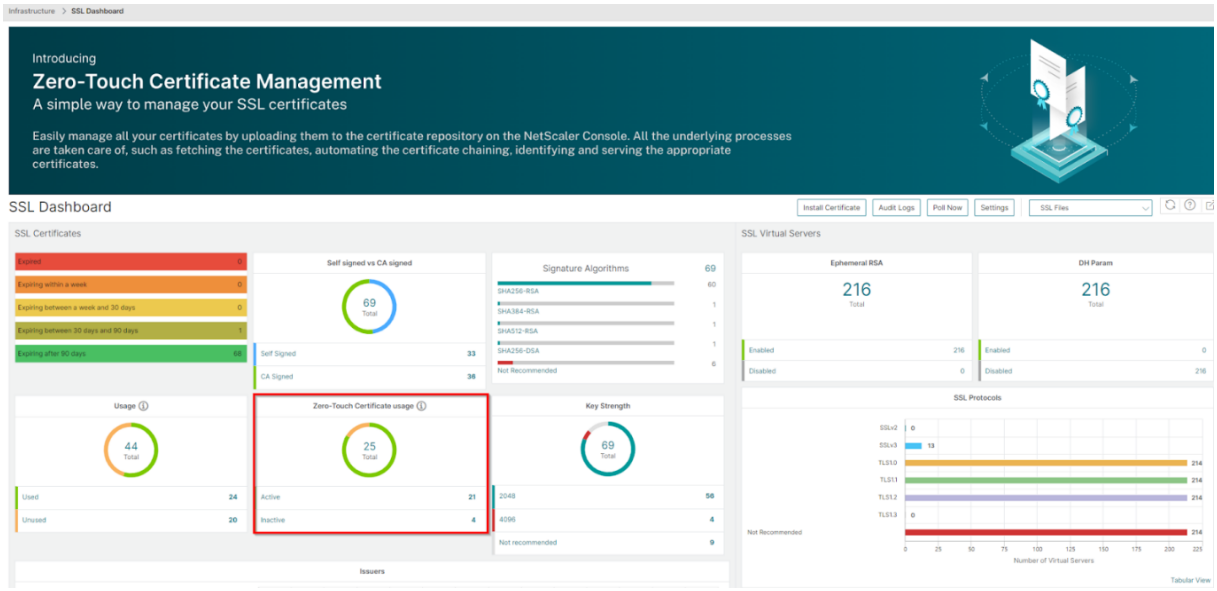
2. Click **Add instances**, select the instances, and then click **Enable**.

© 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 27, 2025

You can use the SSL certificate dashboard in NetScaler Console to view graphs that help you track 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.

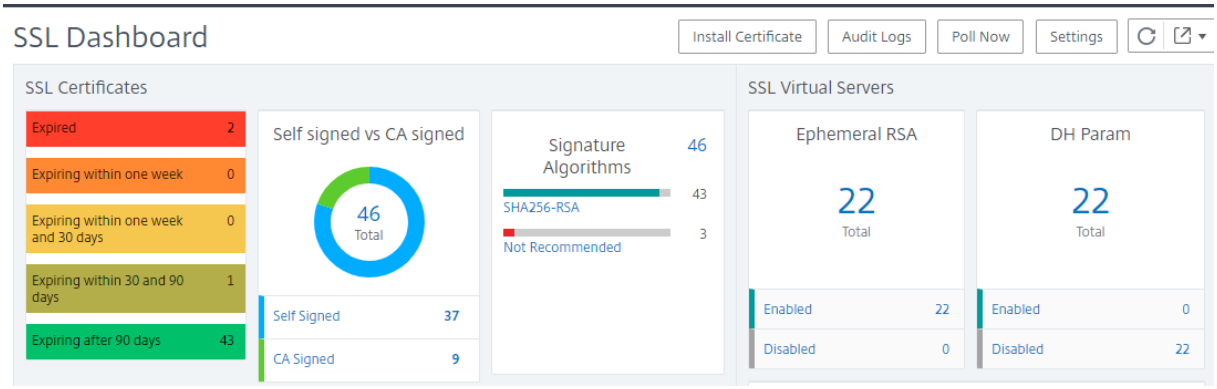
- Number of self-signed and CA-signed certificates
- Number of issuers
- Signature algorithms
- SSL protocols
- Top 10 instances by number of certificates in use

To monitor SSL certificates

You might use the SSL dashboard on NetScaler Console to monitor your certificates if your company has 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 might 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,

1. Navigate to **Infrasturcture > SSL Dashboard**.
2. Click **Poll Now**.

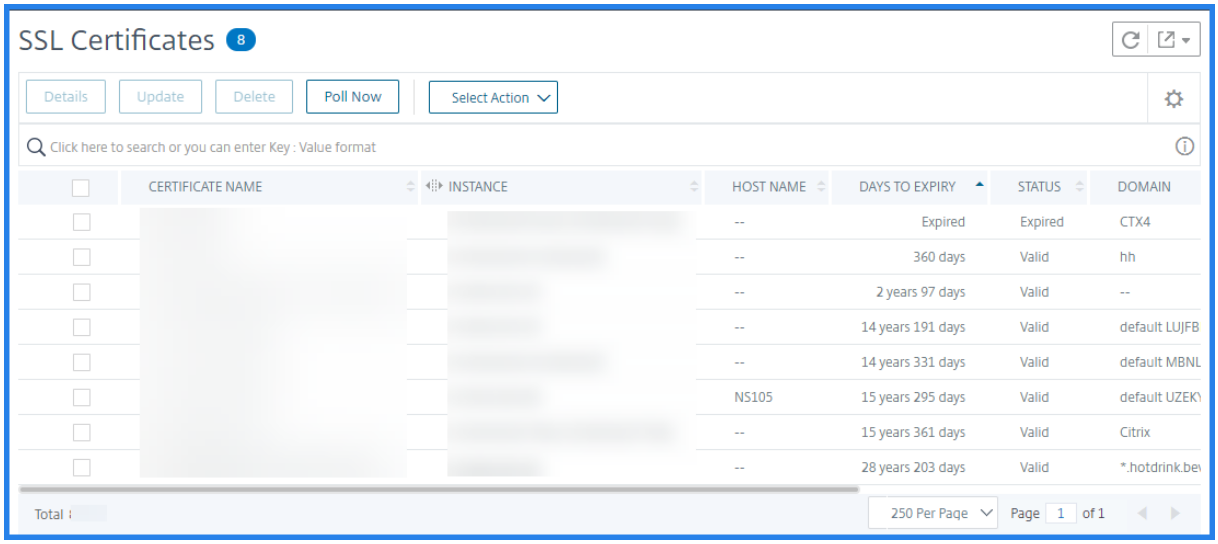
   On the **Poll Now** page, you can either poll all managed NetScaler instances or select specific instances.
3. Click **Start Polling**.

In **SSL Dashboard**, you can monitor the NetScaler SSL certificates, SSL virtual servers, and SSL protocols.

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

You can click the metrics on the dashboard to view details related to SSL certificates, SSL Virtual Servers, or SSL protocols.

For example, when you click the number under **Self signed vs CA signed** on the dashboard, the NetScaler Console GUI displays all the SSL certificates on the NetScaler instances.



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, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. 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.

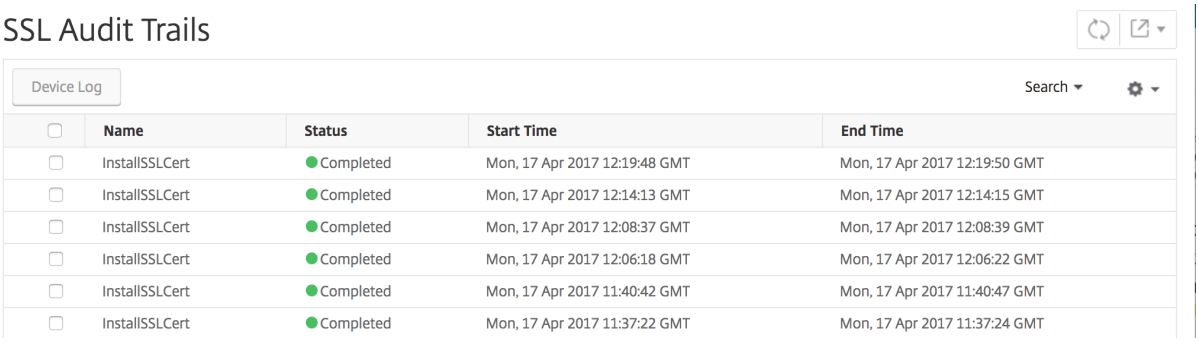
A donut chart appears after Diffie-Hellman (DH) or Ephemeral RSA keys are enabled or disabled on the SSL dashboard. These keys enable secure communication with export clients even if the server certificate does not support export clients, as in the case of a 1024-bit certificate. Clicking the appropriate chart displays a list of the virtual servers on which DH or Ephemeral RSA keys are enabled.

To view audit trails for SSL certificates

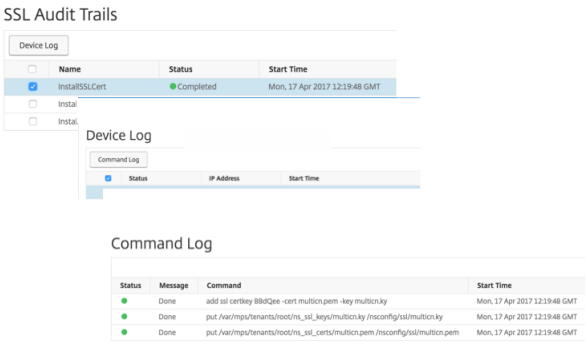
You can now view log details of SSL certificates on NetScaler Console. The log details display operations performed using SSL certificates on NetScaler Console such as: installing SSL certificates, linking and unlinking SSL certificates, updating SSL certificates, and deleting SSL certificates. Audit trail information is useful while monitoring SSL certificate changes done on an application with multiple owners.

To view an audit log for a particular operation performed on NetScaler Console using SSL certificates, navigate to **Infrastructure > SSL Dashboard** > and click **Audit Logs**.

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



For a particular operation performed using 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.

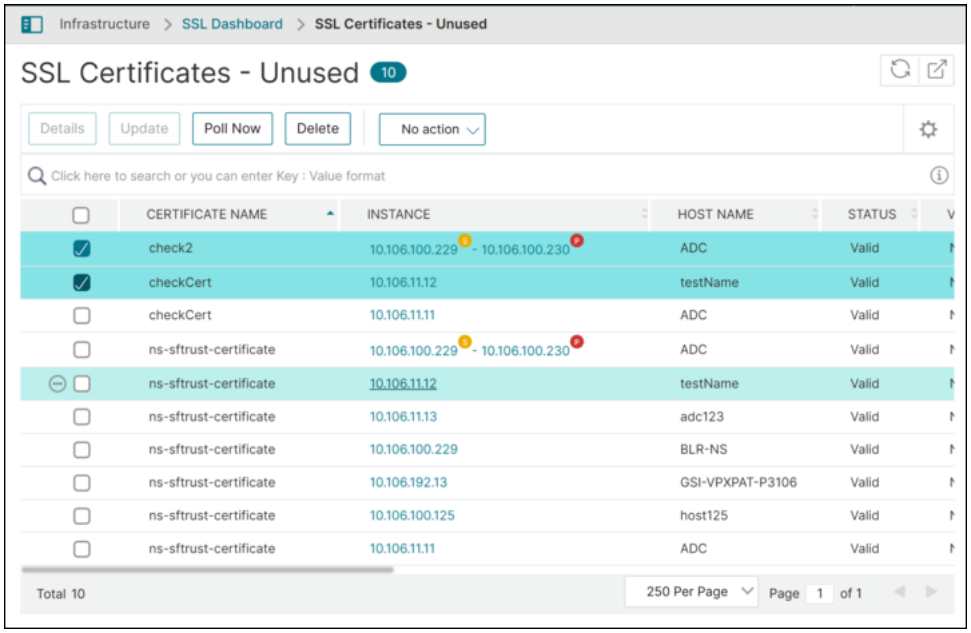


To delete the SSL certificate on the SSL Dashboard

NetScaler 14.1-38.x and later provides an option to delete the associated SSL certificate files from NetScaler while deleting the selected configuration of an 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**.
3. A page with a list of unused certificates is displayed.
4. Choose one or more unused certificates you wish to delete.

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



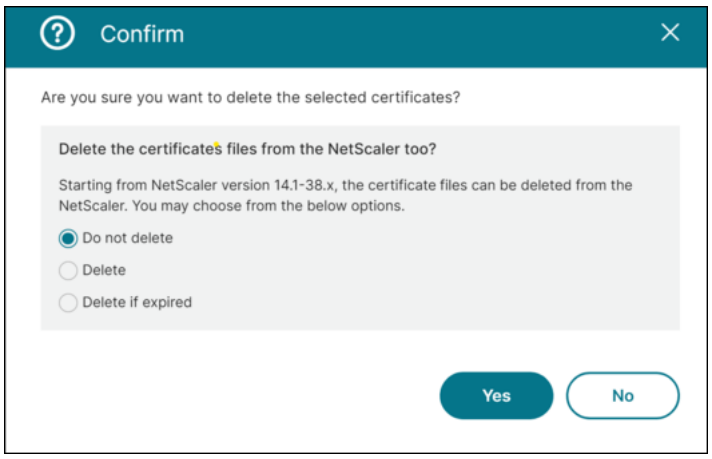
5. Click **Delete**.
6. A **Confirm** dialogue box appears, providing the following options to delete the certificate files from NetScaler® as well:

   - **Do Not Delete**: Skips the deletion of certificate files from NetScaler.
   - **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.

7. Select the appropriate option based on your needs.
8. Click **Yes** to delete the certificate or click **No** to exit the workflow without making any changes.

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

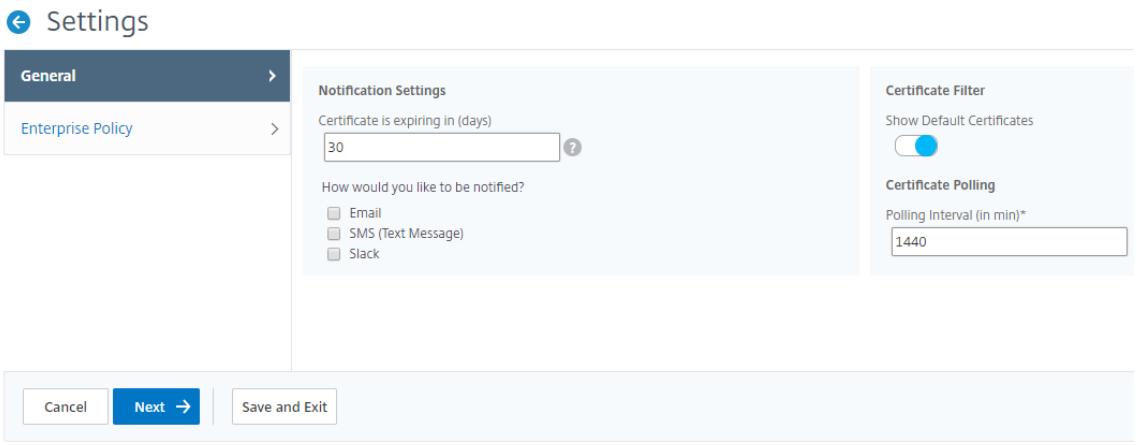


To exclude default NetScaler certificates on the SSL Dashboard

NetScaler Console allows you to show or hide default NetScaler 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. Type the number of days when the certificate expires to receive notification about certificate expiry.
5. Select the method of notification and create the respective profiles.
6. In the **Certificate Filter** section, clear the **Show Default Certificates** checkbox and click **Save and Exit**.



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

View, upload, and download SSL files

To view SSL files on NetScaler Console, navigate to **Infrastructure > SSL Dashboard > SSL Files on NetScaler Console**.

You can view, upload, and download the following files on NetScaler Console:

- SSL certificates
- SSL keys
- SSL CSRs

To view and download SSL files on a NetScaler instance, navigate to **Infrastructure > SSL Dashboard > SSL Files on NetScaler**.

You can access the SSL files only after the NetScaler instances have been backed up, either manually or through a scheduled backup process.

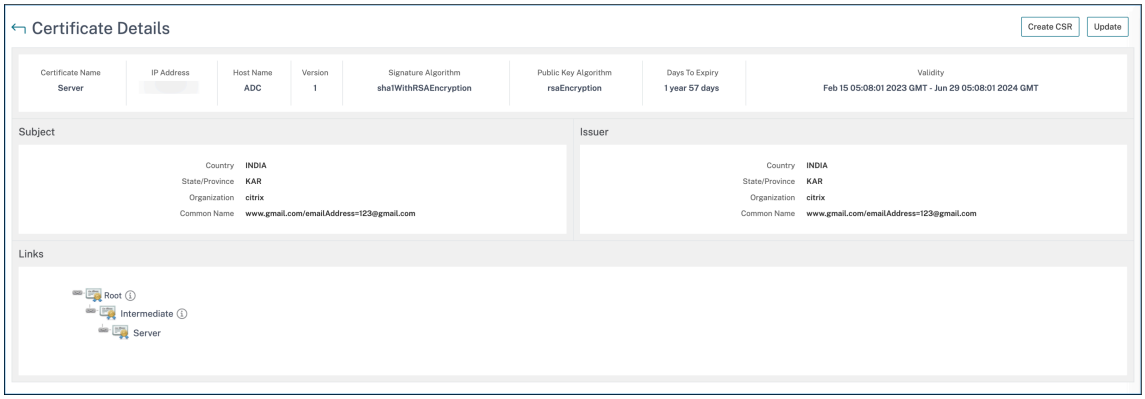
> **Important:**
>
> To enable the SSL files download from NetScaler instances, enable the **Instance SSL certificates** feature. For more information, see Enable or disable NetScaler Console features.

View SSL certificate chain

You can view the complete certificate chain from 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

September 27, 2025

As a security administrator, you can set up notifications to inform you when certificates are about to expire and to include information about which Citrix 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.

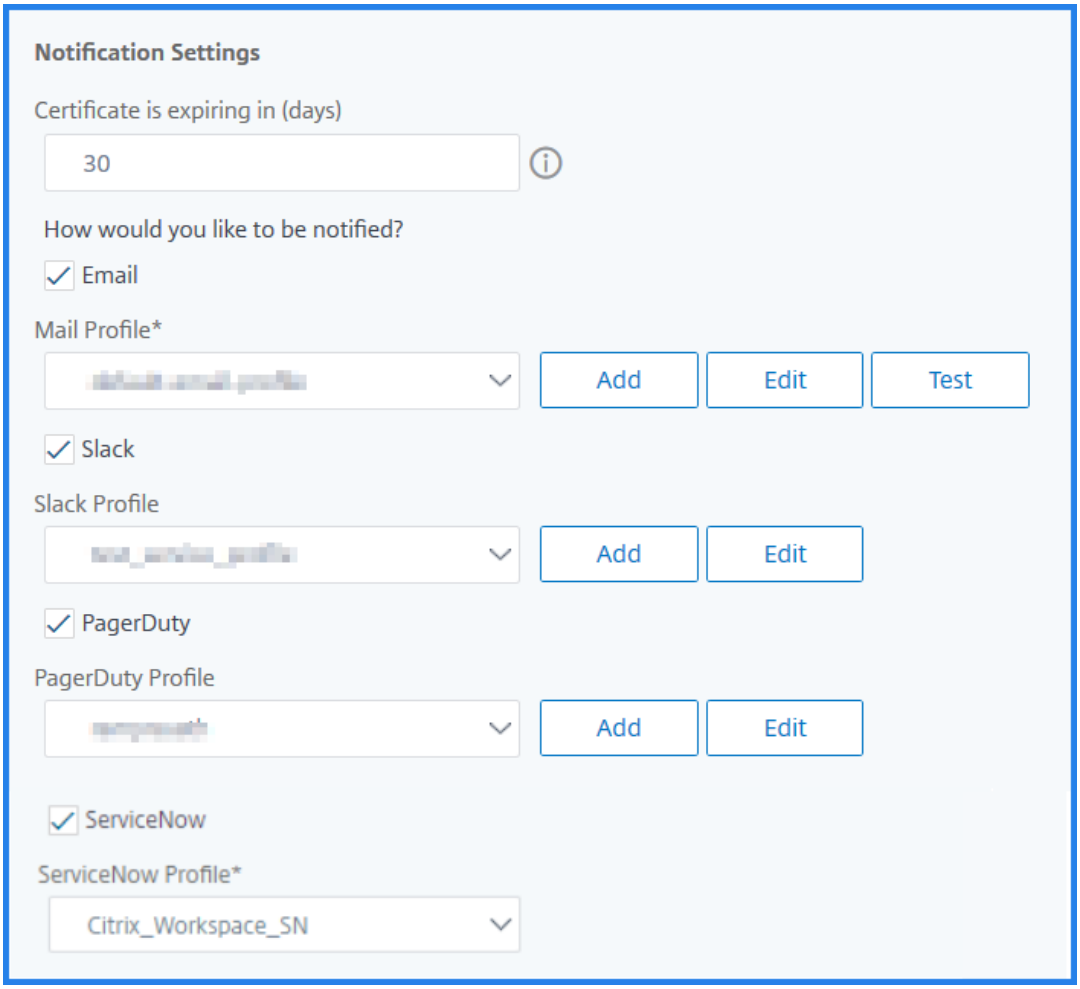
To set up notifications from NetScaler Console:

1. In NetScaler Console, navigate to **Infrastructure > SSL Dashboard**.
2. On the **SSL Dashboard** page, click **Settings**.
3. On the **SSL Settings** page, click the **Edit** icon .
4. In the **Notification Settings** section, specify when you want 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 drop-down 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.
    - **SMS** –Specify a Short Message Service (SMS) server and profile details. An SMS message is triggered when your certificates are about to expire.
    - **Slack** - Specify Slack profile details.
    - **PagerDuty alerts** - Specify a PagerDuty profile. Based on the notification settings configured in your PagerDuty portal, a notification is sent when your certificates are about to expire.
    - **ServiceNow** - A notification is sent to the default ServiceNow profile when your certificates are about to expire.

        > **Important**
        >
        > Ensure Citrix Cloud ITSM Adapter is configured for ServiceNow and integrated with NetScaler Console. For more information, see Integrate NetScaler Console with ServiceNow instance.

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



6. Click **Save and Exit**.

NetScaler Console now sends SSL certificate expiry trap to external trap destination server when your SSL certificates are due for expiry. NetScaler Console sends a trap when the following two conditions are satisfied:

- You have configured the number of days for the certificate expire in SSL dashboard settings page.
- You have added the trap destination.

You can set trap destinations by navigating to **Settings > SNMP > Trap Destinations**. Type the IP address of the destination SNMP server where the traps are sent. Enter the port number and type "public"(without quotes) as the community string.

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

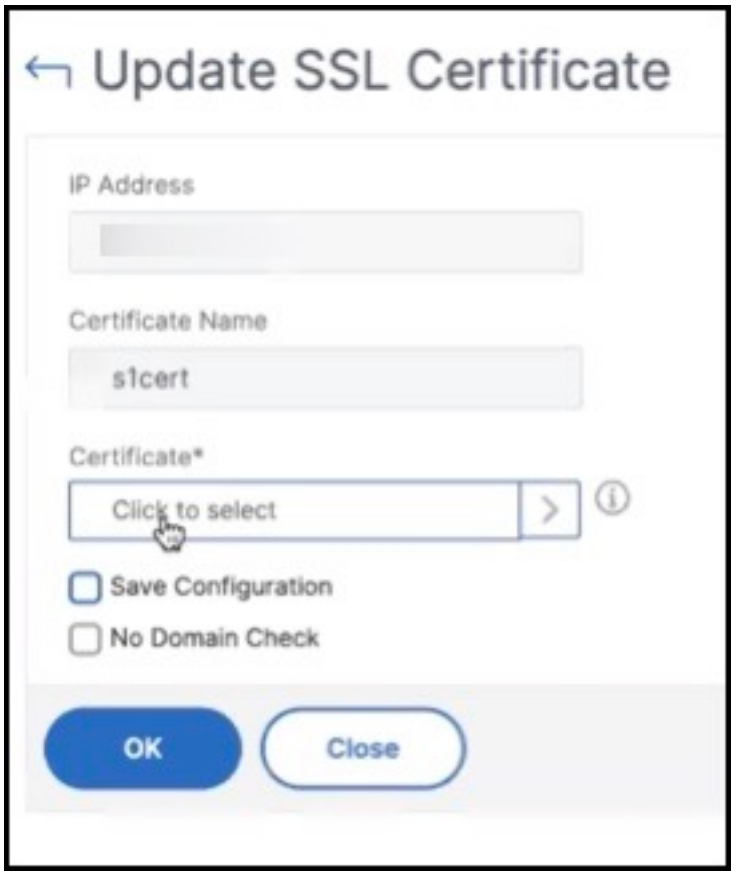
Update an installed certificate

September 27, 2025

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.

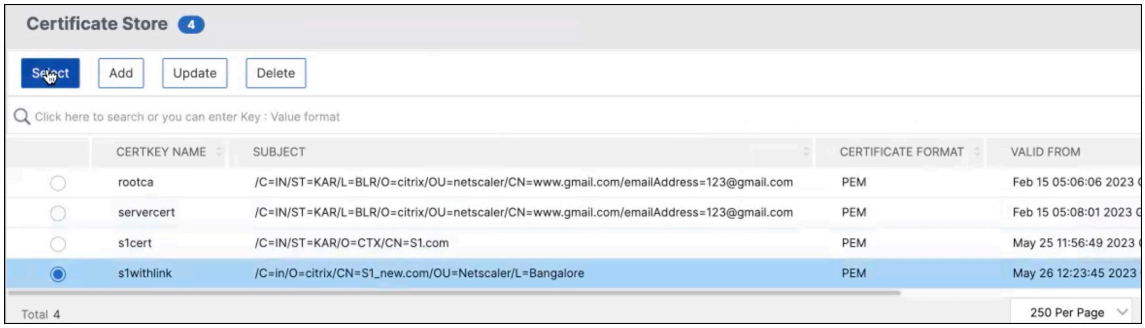
To update an SSL certificate from NetScaler Console:

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 view the **Certificate Store** page.

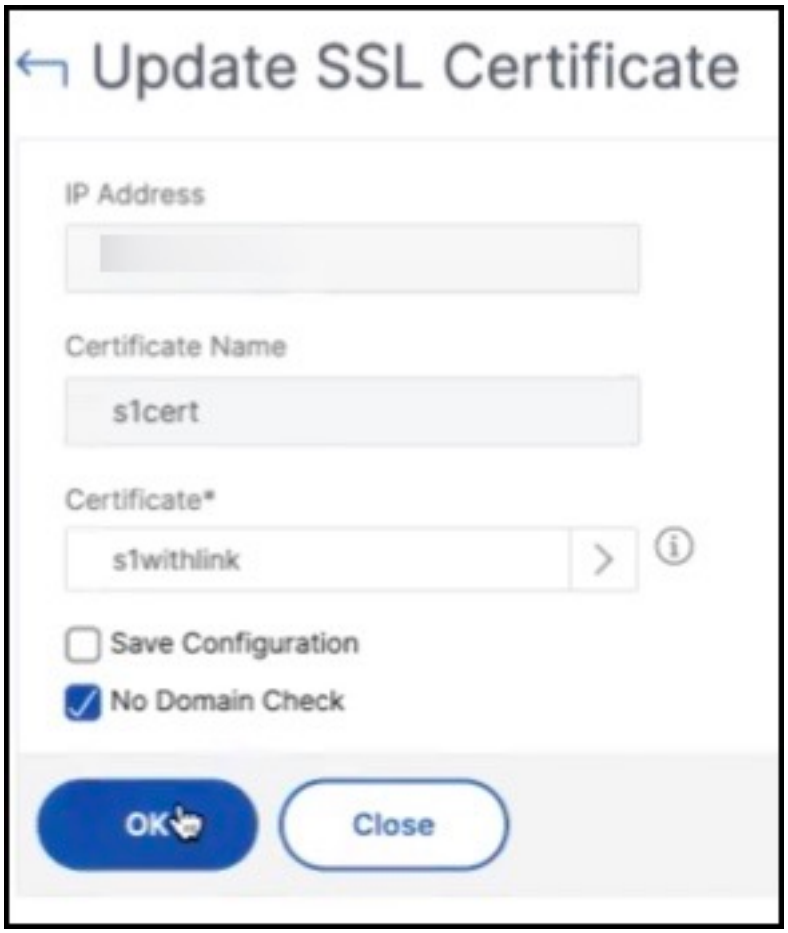


5. In the **Certificate Store** page, select the certificate file you want to add. Click **Select**.

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



6. If the domain name of the new certificate does not match the old certificate, select **No Domain Check** if you want the server to host the new domain.



Click **OK**. All the SSL virtual servers to which this certificate is bound are automatically updated.

> **Note:**
>
> 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

September 27, 2025

Before installing SSL certificates on Citrix NetScaler instances, ensure that the certificates are issued by trusted CAs. Also, ensure that the key strength of the certificate keys is 2048 bits or higher and that the keys are signed with secure signature algorithms.

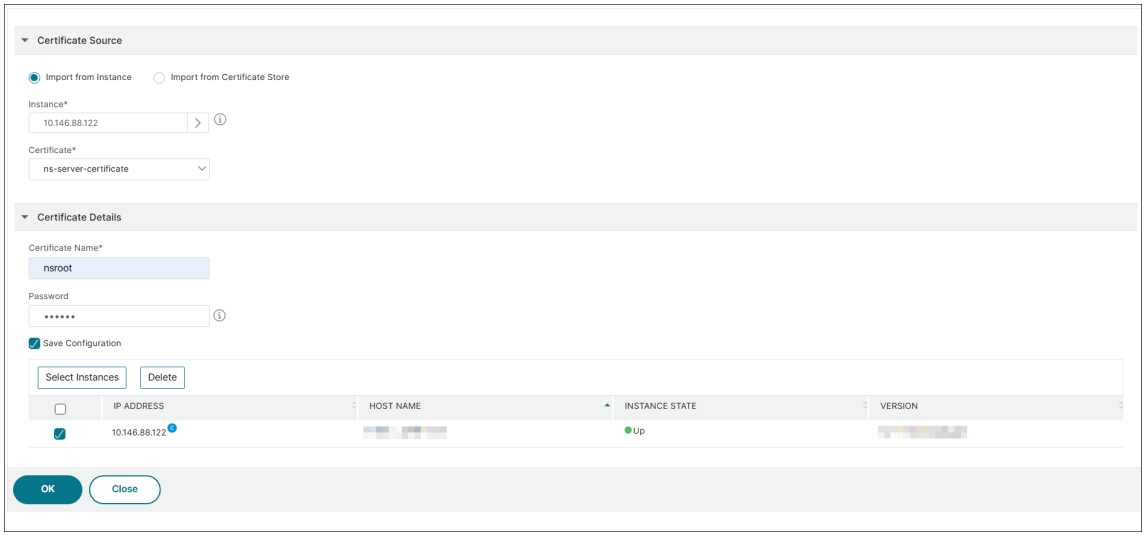
To install an SSL certificate from another NetScaler Instance:

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. Click **Install Certificate**.
3. On the **Install SSL Certificate on NetScaler Instances** page, specify the following parameters:
   a) **Certificate Source**
   Select the option to **Import from Instance**.
      - Choose the **Instance** that you want to import the certificate from.
      - Choose the **Certificate** from the list of all SSL certificate files on the instance.

   b) **Certificate Details**
      - **Certificate Name**. Specify a name for the certificate key.
      - **Password**. Password to encrypt the private key. You can use this option to upload encrypted private keys.
4. Click **Select Instances** to select the NetScaler instances on which you want to install your certificates.
5. To save the configuration for future use, select the **Save Configuration** check box.
6. Click **OK**.

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



To install an SSL certificate from NetScaler Console:

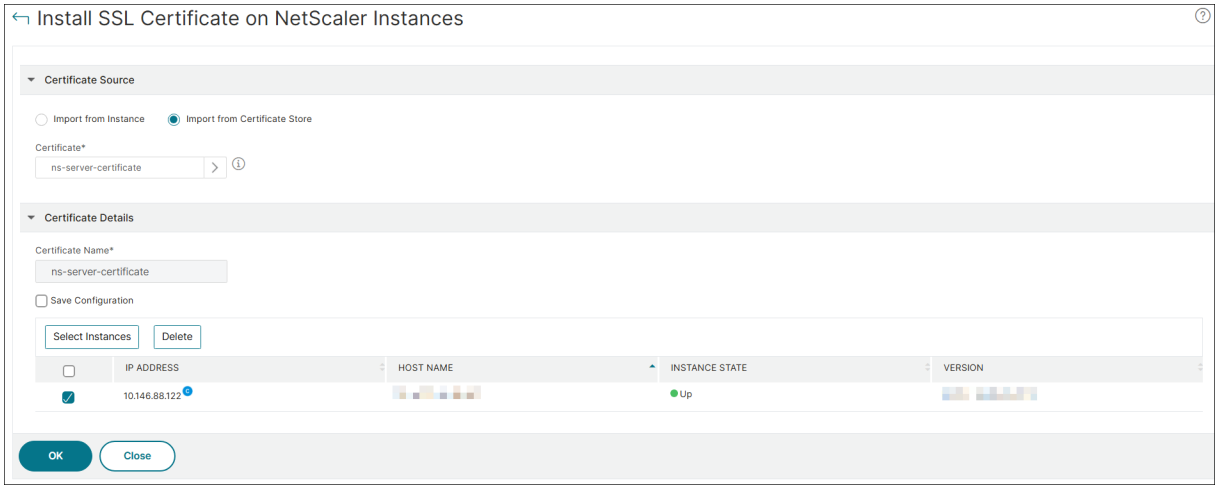
1. In NetScaler Console, navigate to **Infrastructure > SSL Dashboard**.
2. Click **Install Certificate**.
3. On the **Install SSL Certificate on NetScaler Instances** page, specify the following parameters:

   a) **Certificate Source**
   Select the option to **Import from Certificate Store**.
   - **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 Console virtual instance).

   b) **Certificate Details**
   - **Certificate Name** –Specify a name for the certificate key.

4. Click **Select Instances** to select the NetScaler Console instances on which you want to install your certificates.
5. To save the configuration for future use, select the **Save Configuration** check box.
6. Click **OK**.

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



Create a Certificate Signing Request (CSR)

September 27, 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 will be 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** list.
3. On the **Create Certificate Signing Request (CSR)** page, specify a name for the CSR.
4. Do one of the following:
    - **Upload a key** - Select the **I have a Key** option. To upload your key file, select either **Local** (your local machine) or **Appliance** (the key file must be present on the NetScaler Console virtual instance).
    - **Create a key** - Select the I do not have a Key option, and then specify the following parameters:

Encryption Algorithm	Type of key. For example, RSA.
Key File Name	Name for your file in which the RSA key is stored.

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

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'll need to provide a PEM Passphrase.
PEM Passphrase	If you've chosen the PEM Encoding Algorithm, enter a passphrase.
Confirm PEM Passphrase	Confirm your PEM passphrase.

5. Click **Continue**.
6. On the following page, provide more details.

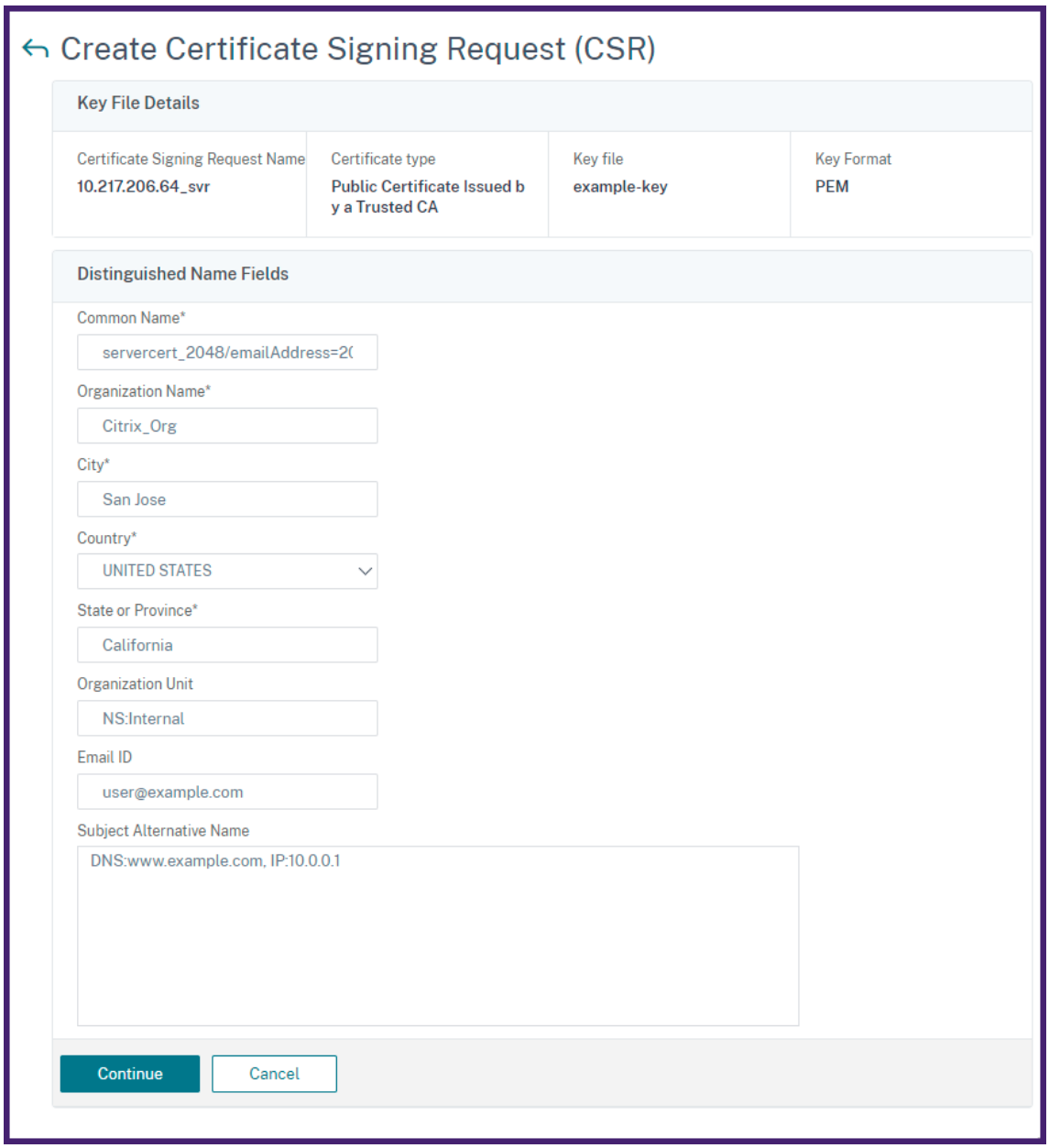
   Most fields have default values extracted from the subject of the selected certificate. The subject contains details such as the common name, organization name, state, and country.

   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:

   ```
   1 DNS:<Domain name>, IP:<IP address>
   ```

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



In this example, it secures `10.0.0.1` and `www.example.com`.

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.

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

Link and unlink SSL certificates

September 27, 2025

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 **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 **Action** drop-down list.
4. Click **OK**.

> **Note**
>
> If the selected certificate is not linked to another certificate, the following message is displayed: Certificate does not have any CA link.

Configure an enterprise policy

September 27, 2025

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

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 Citrix 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 SSL Settings page, click the **Edit** 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 **Save** to save your enterprise policy.

> **Note**
>
> The SSL dashboard displays only the **Signature Algorithms** that are selected through the **Settings** option and others are displayed as **Not Recommended**.

Poll SSL certificates from NetScaler instances

September 27, 2025

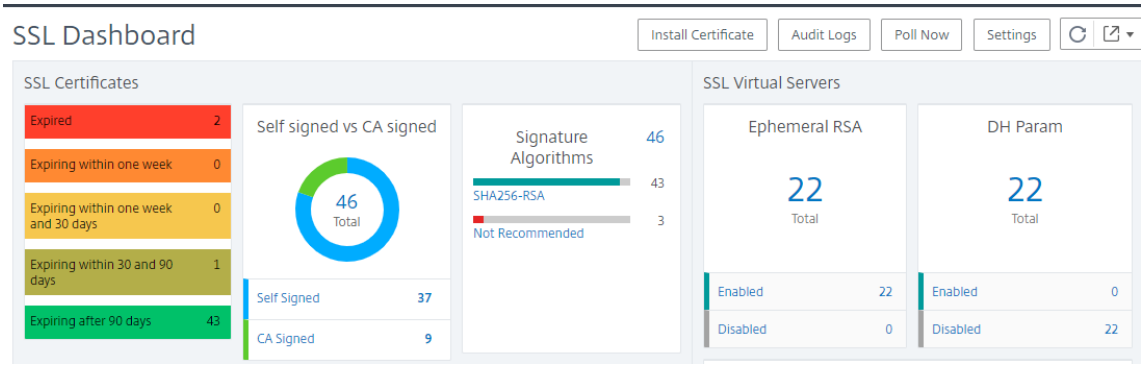
NetScaler Console automatically polls SSL certificates once every 24 hours by using NITRO calls and the Secure Copy (SCP) protocol. You can also manually poll the SSL certificates to discover newly added SSL certificates on the Citrix NetScaler instances. Polling all the NetScaler instances SSL certificates 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.

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

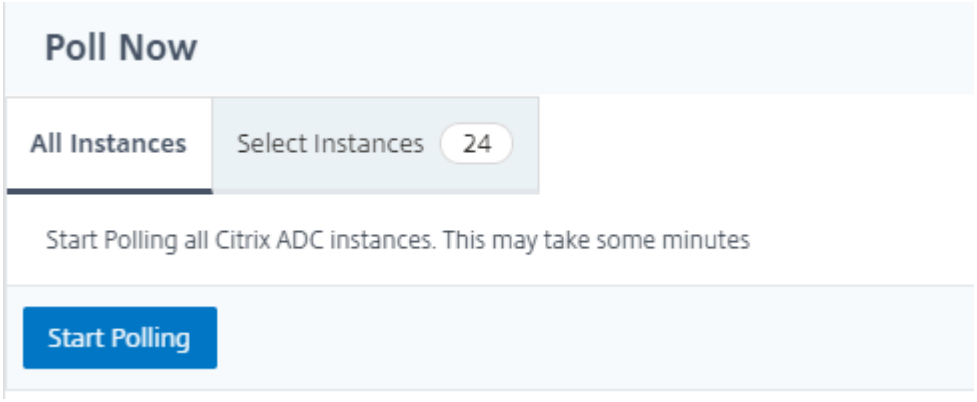
To poll SSL certificates on NetScaler instances:

1. In NetScaler Console, navigate to **Infrastructure > SSL Dashboard**.
2. On **SSL Dashboard** page, in the top right-hand corner, click **Poll Now**.

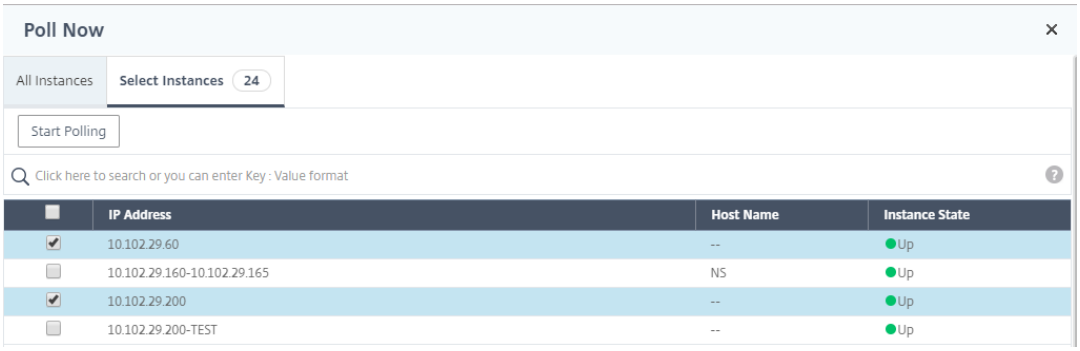


3. The **Poll Now** page pops up, giving you the option to poll all NetScaler instances in the network or to poll the selected instances.

   a) To poll the SSL certificates of all the NetScaler instances, select the **All Instances** tab and click **Start Polling**.



   b) To poll specific instances, select the **Select Instances** tab, select the instances from the list, and click **Poll Now**.



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

Use the NetScaler Console certificate store to manage SSL certificates

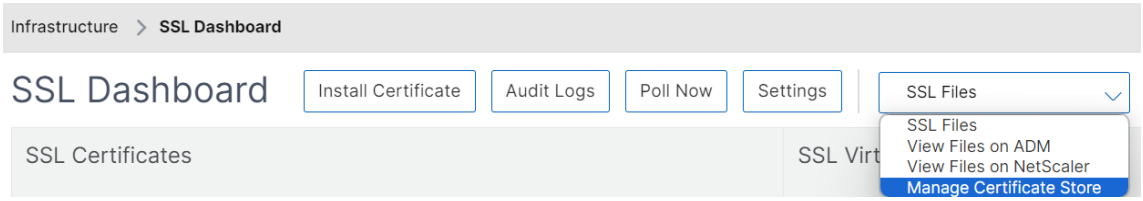
September 27, 2025

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** and select **Manage Certificate Store** from the list.



2. Click **Add**.
3. On the **Add Certificate** page, enter the following details:
    - **Certkey Name** - Enter a name for the certificate. The name must have only ASCII alphanumeric, underscore, and hyphen characters and must be fewer than 30 characters. You cannot change the name after the certificate is created.
    - **Certificate File** - Browse to your local drive and upload the certificate file.
    - **Key File** - Upload the key file from your local computer.
    - **Password** - If you have an encrypted private key in PEM format, type the passphrase that was used to encrypt the private key.
    - **Add Certificate Chain** - Select this option to add the certificate in a certificate chain.
    - **Certificate Chain** - Browse to your local drive and upload the certificate file.
    - Click **Create**.

Update SSL certificates in the certificate store

1. Navigate to **Infrastructure > SSL Dashboard** and select **Manage Certificate Store** from the list.
2. Select the certificate that you want to update and click **Update**.

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

3. 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** and select **Manage Certificate Store** from the list.
2. Select the certificate and click **Delete**.
3. When prompted, click **Yes** to delete the certificate.

Install SSL certificates on NetScaler® instances

1. Navigate to **Infrastructure > SSL Dashboard** and select **Manage Certificate Store** from the list.
2. Select the certificate and click **Install**.
3. 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.

4. Click **Select Instances** to select the NetScaler instances on which you want to install your certificates.

Click **OK**.

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

Import certificates from NetScaler instances

1. Navigate to **Infrastructure > SSL Dashboard** and select **Manage Certificate Store** from the list.
2. Click **Import NetScaler Certificates**.
3. 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.

Manage database custom certificates and ciphers in a high-availability deployment

September 27, 2025

NetScaler Console allows you to replace the default inbuilt database certificates with your own certificates from a trusted certificate authority. You can also configure your own cipher suites in the NetScaler Console database. This feature provides greater flexibility and security for your certificate management needs, and secures all communication between your HA nodes with trusted SSL certificates.

Install your database certificates on NetScaler Console

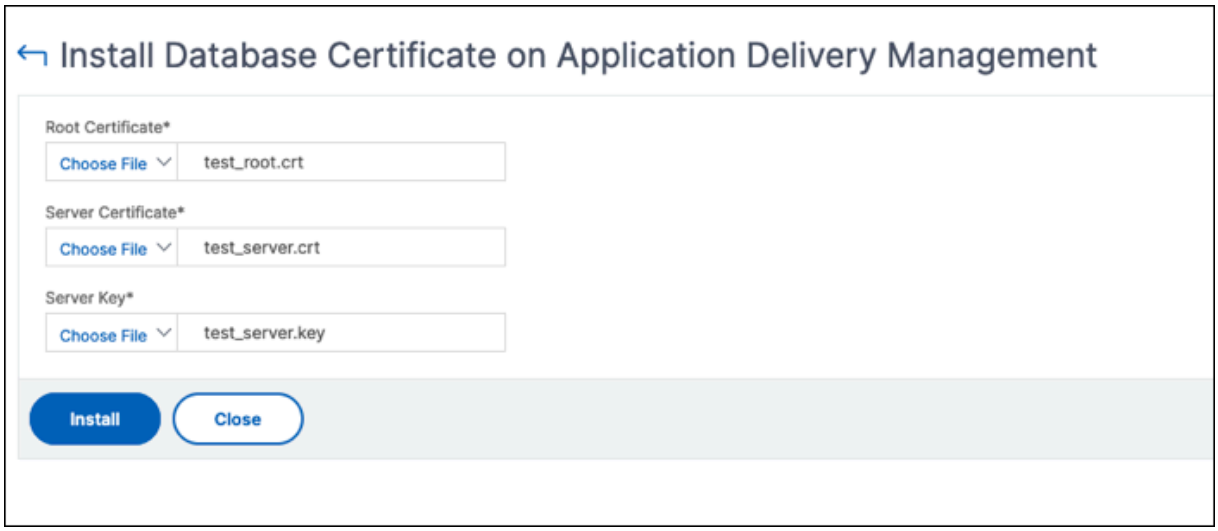
To install your certificates in an HA setup:

1. Navigate to **Settings > HA Deployment** and click **Database Certificates**.
2. Click the **Installed Certificate** tab and click **Install New Certificate**.
3. In the **Install Database Certificate on Application Delivery Management** page, upload a root certificate, server certificate, and server key. You can do one of the following:
    - **Choose File > Local** to upload a certificate or key file from your local machine.

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

- **Choose File > Appliance** to upload a certificate or key file that is present on NetScaler Console.

4. Click **Install**.



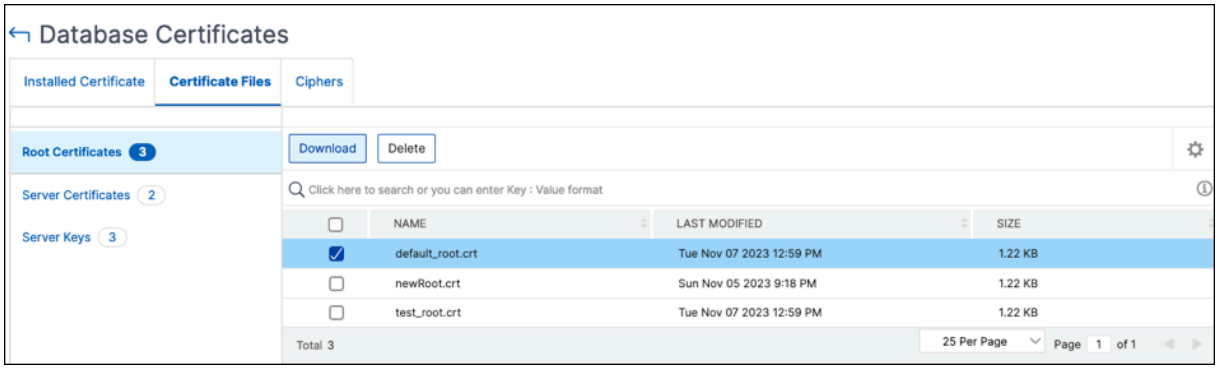
> **Note:**
>
> If there are multiple chain certificates, you must combine them into a single file. Make sure that the order of concatenation is correct, with the intermediate certificates first, followed by the root certificate. This order is essential for the certificate chain to be recognized correctly.
>
> For example, the following command appends the content of each certificate file (intermediate_certificate1.crt, intermediate_certificate2.crt, and root_certificate.crt) to the file named combined_certs.crt:
>
> ```
> cat intermediate_certificate1.crt >> combined_certs.crt
> cat intermediate_certificate2.crt >> combined_certs.crt
> cat root_certificate.crt >> combined_certs.crt
> ```

Manage your installed database certificates

To view, download, and delete your installed certificates:

1. Navigate to **Settings > HA Deployment** and click **Database Certificates**.
2. Click the **Certificate Files** tab and select **Root Certificates, Server Certificates**, or **Server Keys** to see the corresponding files.
3. To download a file to your local machine, click **Download**.
4. To delete a certificate file, select the file and click **Delete**. In the confirmation dialog box that appears, click **OK**.

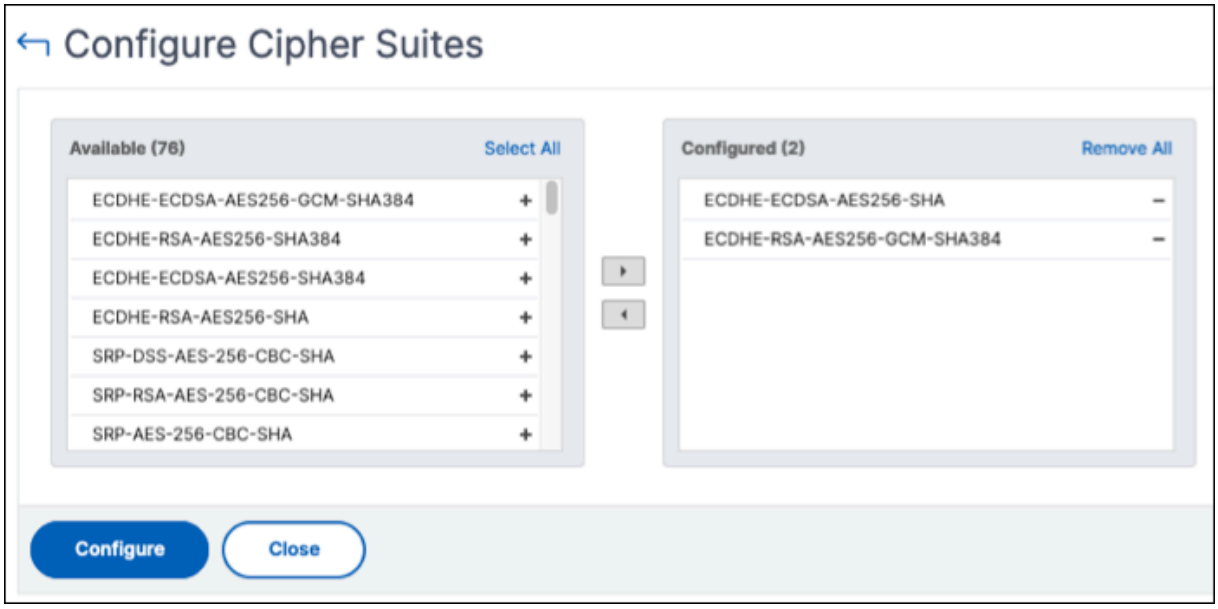
© 1997–2025 Citrix Systems, Inc. All rights reserved.



Configure database cipher suites

To configure cipher suites for an HA deployment:

1. Navigate to **Settings > HA Deployment** and click **Database Certificates**.
2. Click the **Ciphers** tab and then click **Configure Cipher**.
3. In the **Configure Cipher Suites** page, select one or more ciphers from the available list of ciphers.
4. Click **Configure**. In the confirmation dialog box that appears, click **Yes** to change the cipher settings.



> **Note:**
>
> Changing the cipher settings restarts the NetScaler Console secondary and disaster recovery nodes.

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

Events

September 27, 2025

When the IP address of a Citrix 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 the events generated on instances to form alarms of different severity levels. These alarms are then displayed as messages, some of which might require immediate attention. For example, system failure can be categorized as a "Critical"event severity and would need to be addressed immediately.

You can configure rules to monitor specific events. Rules make it easier to monitor the events, which can be many, 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 multiple notifications are triggered for an event for a specific time interval, until the event is cleared. As an extra measure, you can customize your email with a specific subject line and user message, and upload an attachment.

Use events dashboard

September 27, 2025

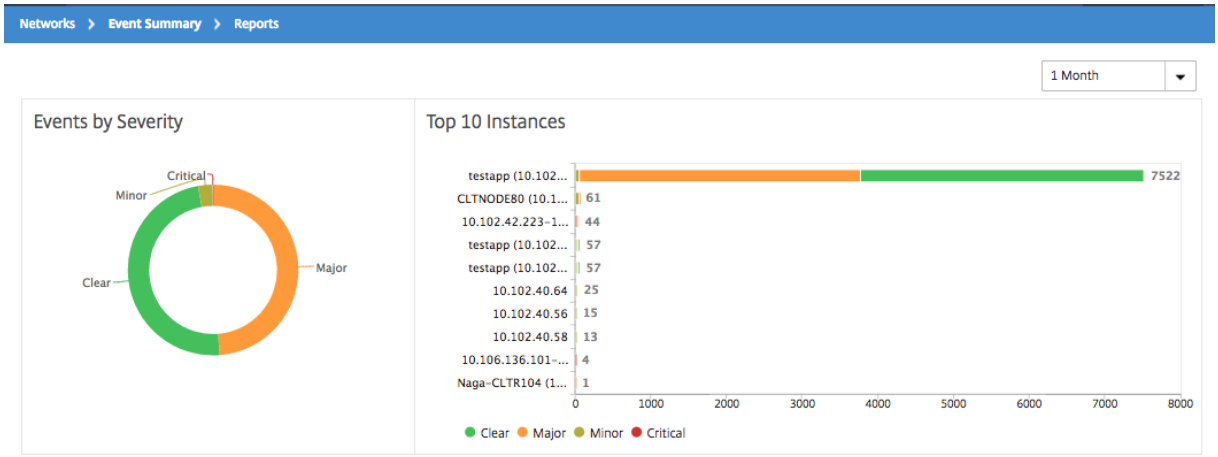
As a network administrator, you can view details such as configuration changes, login conditions, hardware failures, threshold violations, and entity state changes on your NetScaler instances, along with events and their severity on specific instances. You can use the NetScaler Console's events dashboard to view reports generated for critical event severity details on all your NetScaler instances.

To view the details on the events dashboard:

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

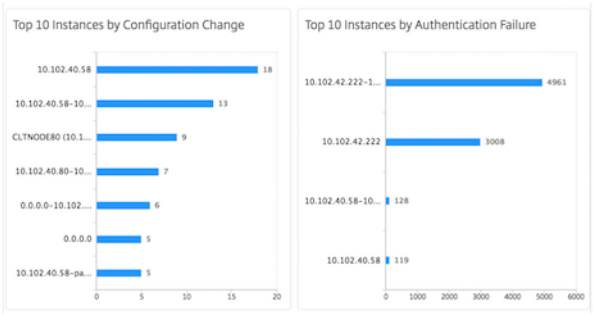
Navigate to **Infrastructure > Events > Reports**.

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.



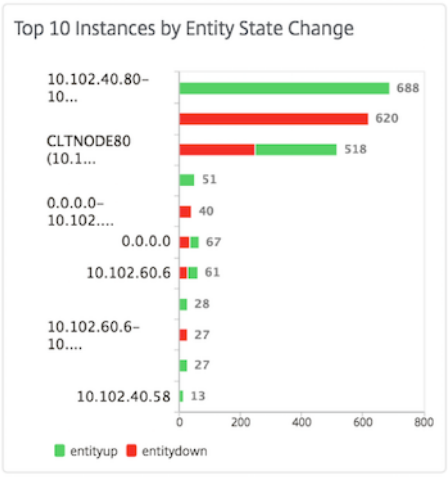
You can view more details by navigating to the NetScaler instance type (**Infrastructure > Events > Reports** > **NetScaler/ NetScaler SDX**) to view the following:

- Top 10 devices by hardware failure
- Top 10 devices by configuration change
- Top 10 devices by authentication failure

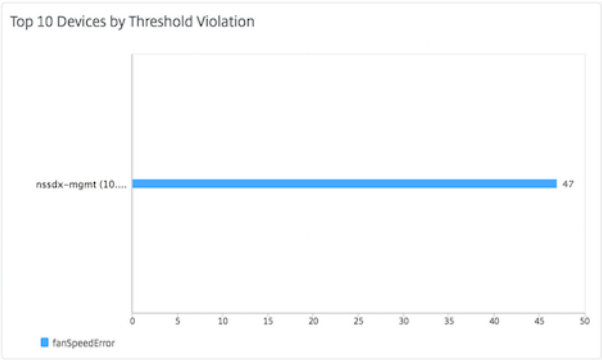


- Top 10 devices by entity state changes

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



- Top 10 devices by threshold violation



Set event age for events

September 27, 2025

You can set the event age option to specify the time interval (in seconds). NetScaler Console monitors the appliances until the set duration and generates an event only if the event age exceeds the set duration.

> Note:
>
> 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 is occurred.

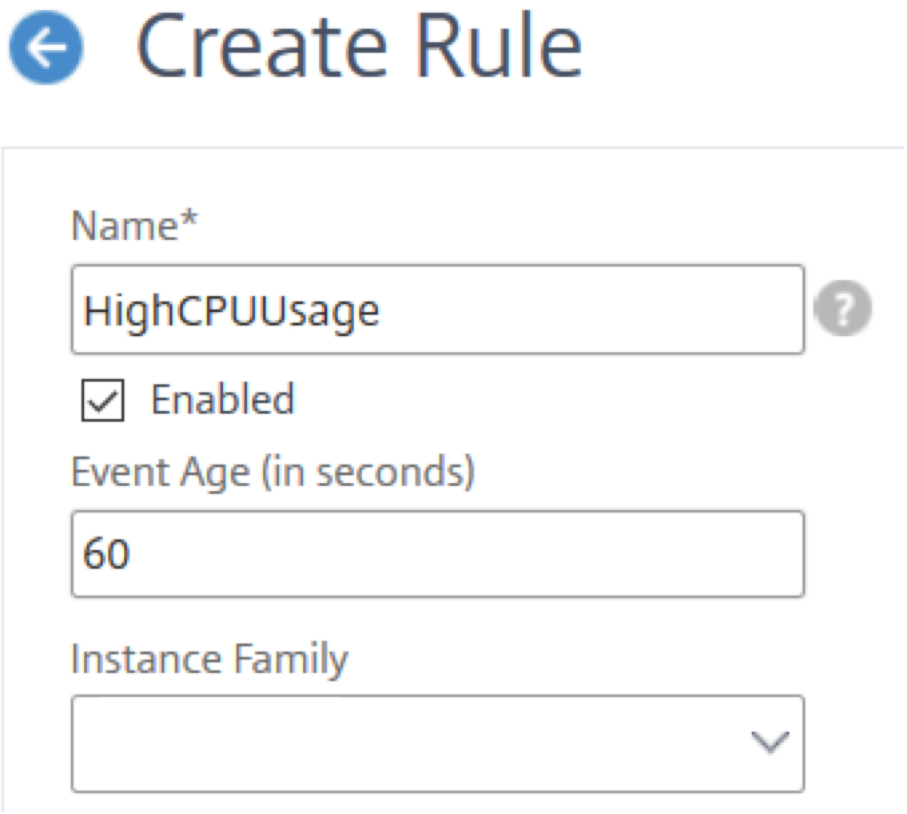
For example, consider that you want to manage various NetScaler appliances and get notified by email when any of your virtual servers goes down for 60 seconds or longer. You can create an event rule with the necessary filters and set the rule's event age to 60 seconds. Then, whenever a virtual server

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

remains down for 60 or more seconds, you receive an email notification with details such as entity name, status change, and time.

To set event age in NetScaler Console:

1. In NetScaler Console, navigate to **Infrastructure > Events > Rules**, and click **Add**.
2. On the **Create Rule** page, set the rule parameters.
3. Specify the event age in seconds.



Ensure to set all the co-related traps in the **Category** section and also set the respective severity in the **Severity** section when you set event age. In the preceding example, select the `entityup`, `entitydown`, and `entityofs` traps.

Schedule an event filter

September 27, 2025

After creating a filter for your rule, if you do not want the NetScaler Console server 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.

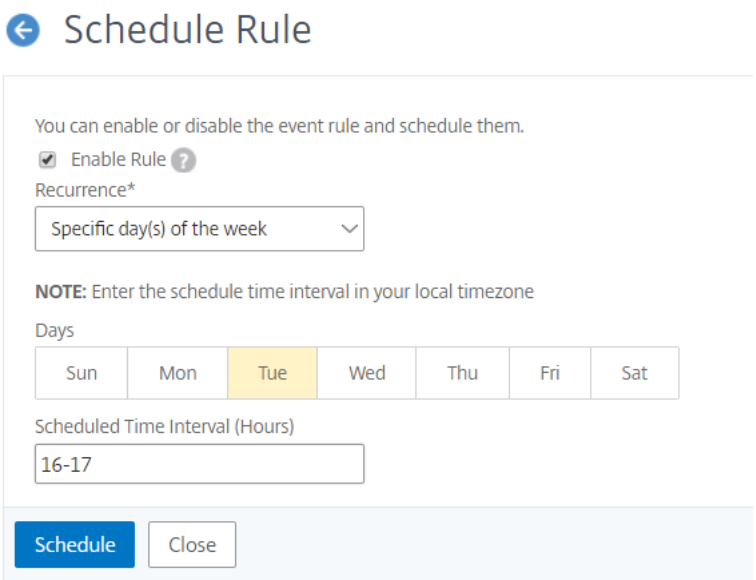
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 a large number of email notifications when NetScaler Console receives these traps. If you want the server to send these email notifications during a specific time period only, you can do so by scheduling a filter.

To schedule a filter using NetScaler Console:

1. In the NetScaler Console, navigate to **Infrastructure > Events > Rules**.
2. Select the rule you want to schedule a filter for, and click **View Schedule**.
3. On the **Scheduled Rule** page, click **Schedule** and specify the following parameters:
    - **Enable Rule** –Select this check box to enable the scheduled event rule.
    - **Recurrence** - Interval at which to schedule the rule. Select either a specific day of the week or a specific date in a month.
    - **Days**: Select the day of the week to run the rule. You can select multiple days.
    - **Dates**: Type in the dates. You can type multiple dates as comma-separated values.
    - **Scheduled Time Interval (Hours)** –Hours, at which to schedule the rule (use the 24-hour format).
4. Click **Schedule**.



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

Set repeated email notifications for events

September 27, 2025

To ensure that all critical events are addressed and no important email notifications are missed, you can opt to send repeated email notifications for event rules that meet the criteria you've selected. For example, if you've created an event rule for instances that involve disk failures, and you want to be notified until the issue is resolved, you can opt to receive repeated email notifications about those events.

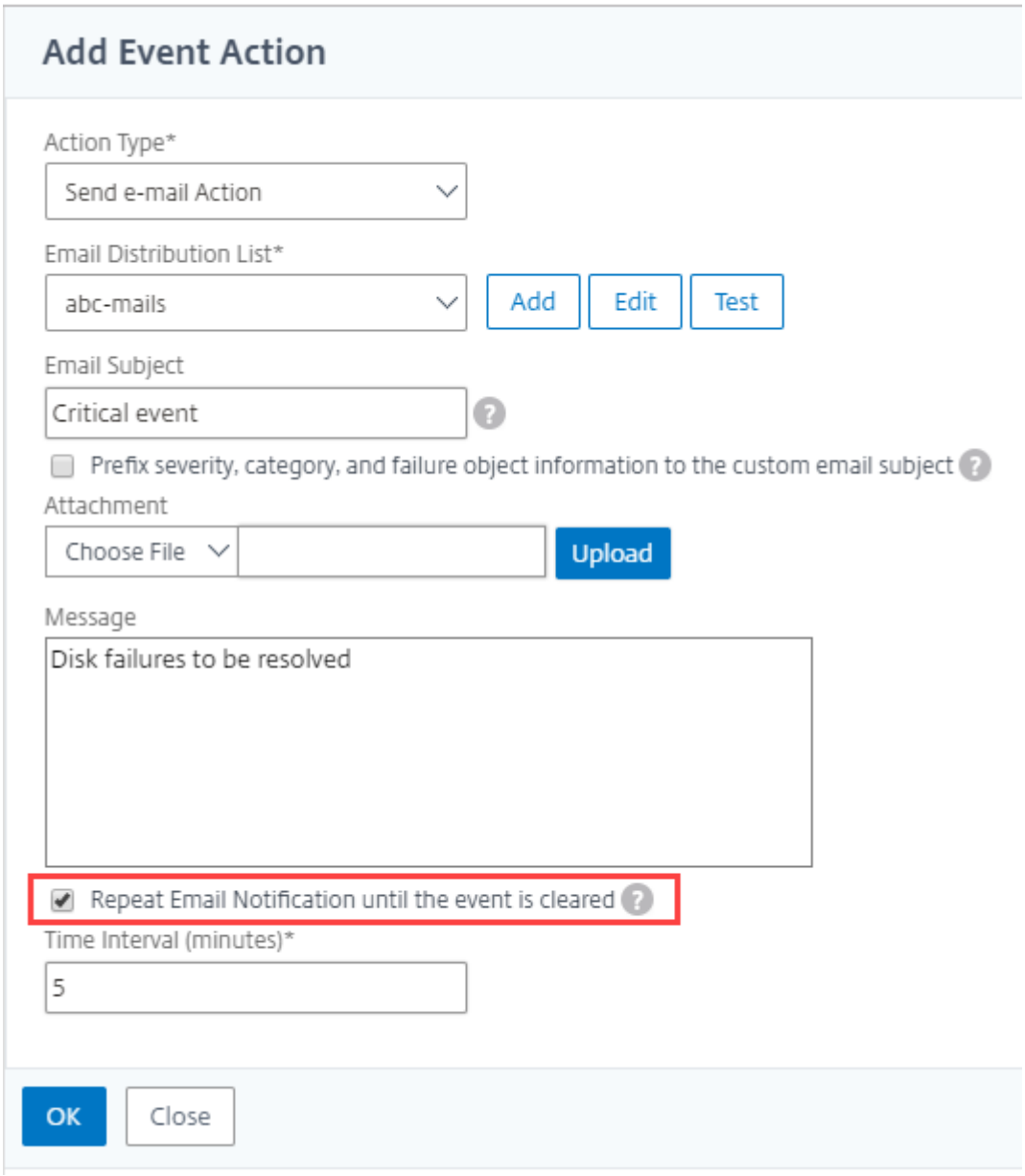
These email notifications are sent repeatedly, at pre-defined intervals, until the recipient acknowledges having seen the notification or the event rule is cleared.

> **Note**
>
> Events can only be cleared automatically if there is an equivalent "clear"trap set and sent from your NetScaler instance.
>
> To clear an event manually, you can do the following:
>
> - Navigate to **Infrastructure > Events > Event Summary**, choose a **Category** and select an event in the category and click **Clear**.
> - Or, navigate to **Infrastructure > Events > Event Messages**. Choose an instance type and then, select an event from the grid below and click **Clear**.

To set repeated email notifications from NetScaler Console:

1. In NetScaler Console, navigate to **Infrastructure > Events > Rules**, and click **Add** to create a rule.
2. On the **Create Rule** page, set the rule parameters.
3. Under **Event Rule** Actions, click **Add Action**. Then, select **Send e-mail Action** from the **Action Type** drop-down list and select an **Email Distribution List**.
4. You can also add a customized subject line and user message, and upload an attachment to your email when an incoming event matches the configured rule.
5. Select the **Repeat Email Notification until the event is cleared** check box.

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



Suppress events

September 27, 2025

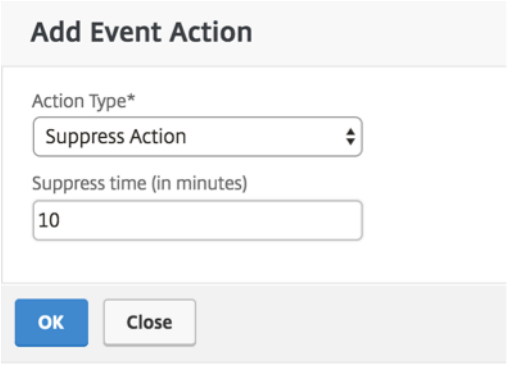
When you choose the **Suppress Action** event action, you can configure a time period, in minutes, for which an event is suppressed or dropped. You can suppress the event for a minimum of 1 minute.

© 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.

To suppress events by using NetScaler Console:

1. In NetScaler Console, navigate to **Infrastructure > Events > Rules**. Click **Add**.
2. Specify all the parameters required to create a rule.
3. Under **Event Rule Actions**, click **Add Action** to assign notification actions for the event.
4. On the **Add Event Action** page, select **Suppress Action** from the **Action Type** drop-down list and specify the time period, in minutes, for which an event must be suppressed.
5. Click **OK**.



Create event rules

September 27, 2025

You can configure rules to monitor specific events. Rules make it easier to monitor a large number of 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. The conditions for which you can create filters are: severity, Citrix Application Delivery Controller (NetScaler) instances, category, failure objects, configuration commands, and messages.

You can assign the following actions to the events:

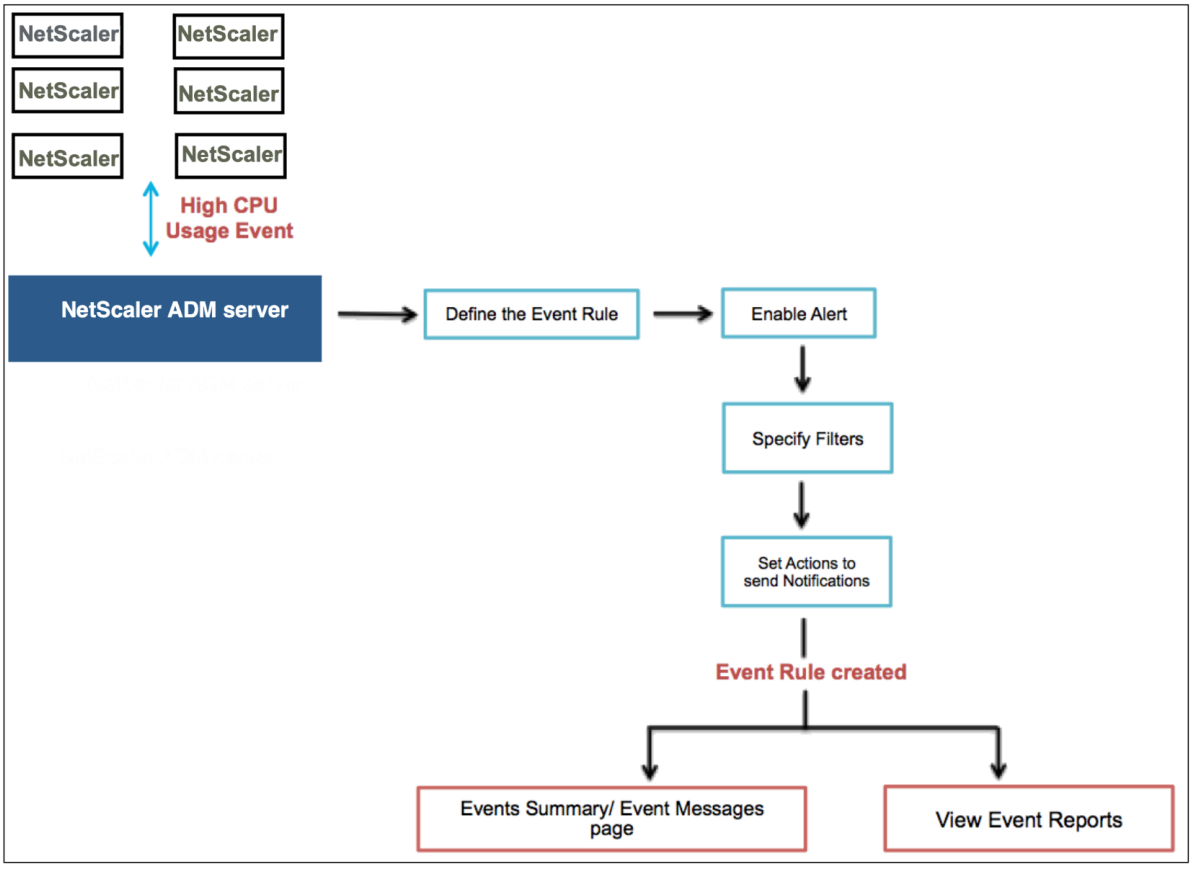
- **Send e-mail Action**: Send an email for the events that match the filter criteria.

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

- **Send Trap Action**: Send or forward SNMP traps to an external trap destination
- **Run Command Action**: Run a command when an incoming event meets the configured rule.
- **Execute Job Action**: Run a job is for events that match the filter criteria that you've specified.
- **Suppress Action**: Suppresses drop an event for a specific time period.
- **Send Slack Notifications**: Send notifications on the configured Slack channel for the events that match the filter criteria.
- **Send PagerDuty Notifications**: Send event notifications based on the PagerDuty configurations for the events that match the filter criteria.
- **Send ServiceNow Notifications**: Auto-generate ServiceNow incidents for an event that match the filter criteria.

For more information, see Add event rule actions

You can also have notifications resent at a specified interval until an event is cleared. And you can customize the email with a specific subject line, user message, and attachment.



For example, as an administrator you might want to monitor "high CPU usage"events for specific NetScaler instances if those events can lead to an outage of your NetScaler instances. You can:

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

- Create a rule to monitor the instances and specify an action that sends you an email notification when an event in the “high CPU usage”category occurs.
- Schedule the rule to run at a specific time, such as between 11 AM to 11 PM, so that you are not notified every time there is an event generated.

Configuring an event rule involves the following tasks:

1. Define the rule
2. Choose the severity of the event that the rule detects
3. Specify the category of the event
4. Specify NetScaler instances to which the rule applies
5. Select failure objects
6. Specify advanced filters
7. Specify actions to be taken when the rule detects an event

Step 1 - Define an event rule

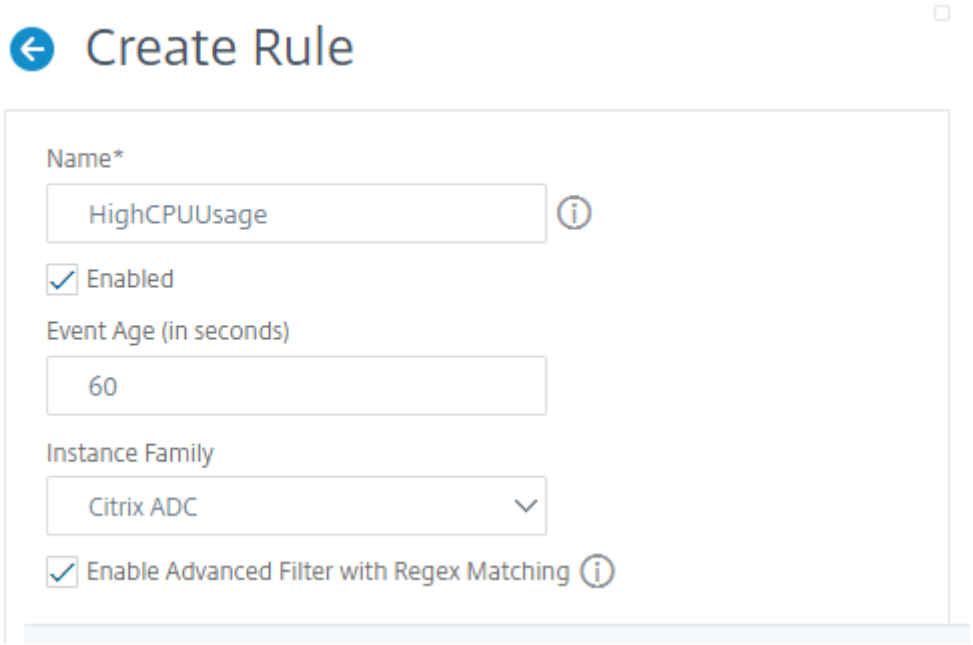
Navigate to **Infrastructure > Events > Rules**, and click **Add**. If you want to enable your rule, select the **Enable Rule** check box.

You can set the **Event Age** option to specify the time interval (in seconds) after which NetScaler Console refreshes an event rule.

> Note:
>
> 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 is occurred.

Based on the example above, you may want to be notified by email every time your NetScaler instance has a “high CPU usage”event for 60 seconds or longer. You can set the event age as 60 seconds, so that every time your NetScaler instance has a “high CPU usage”event for 60 seconds or more, you receive an email notification with details of the event.

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



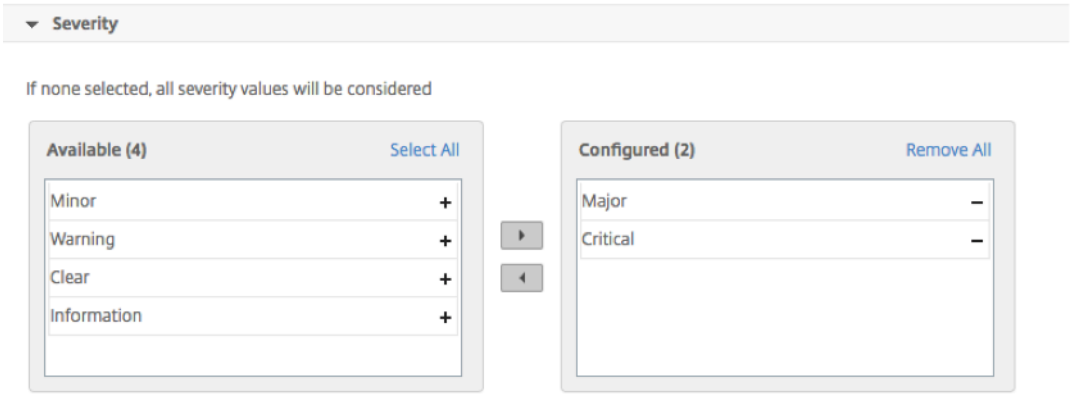
You can also filter event rules by **Instance Family** to track the NetScaler instance from which NetScaler Console receives an event.

If you want to include a regular expression other than asterisk (*) pattern matching, select **Enable Advanced Filter with Regex Matching**.

Step 2 - Choose the severity of the event

You can create event rules that use the default severity settings. Severity specifies the current severity of the events you which you want to add the event rule.

You can define the following levels of severity: Critical, Major, Minor, Warning, Clear, and Information.



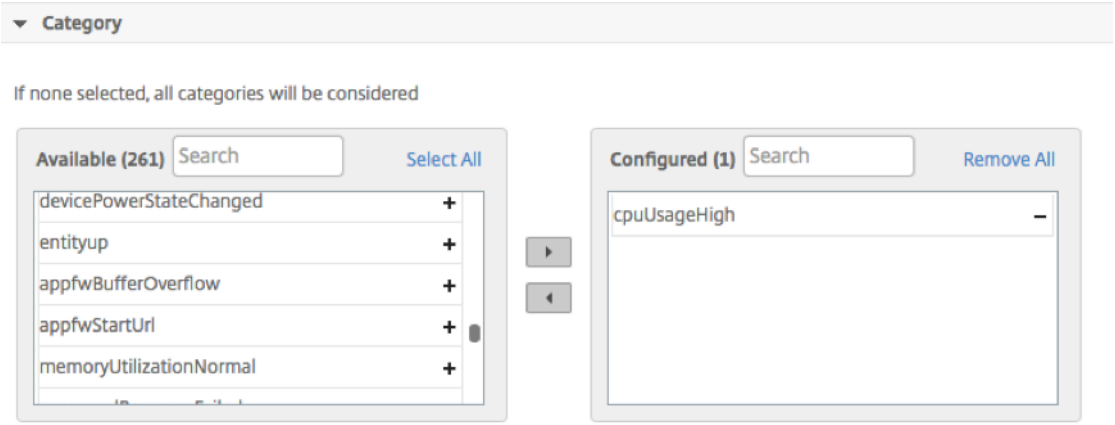
© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Note**
>
> You can configure severity for both generic and Advanced-specific events. To modify event severity for NetScaler instances managed on NetScaler Console, navigate to **Infrastructure > Events > Event Settings**. Choose the **Category** for which you want to configure event severity and click **Configure Severity**. Assign a new severity level and click **OK**.

Step 3 - Specify the event category

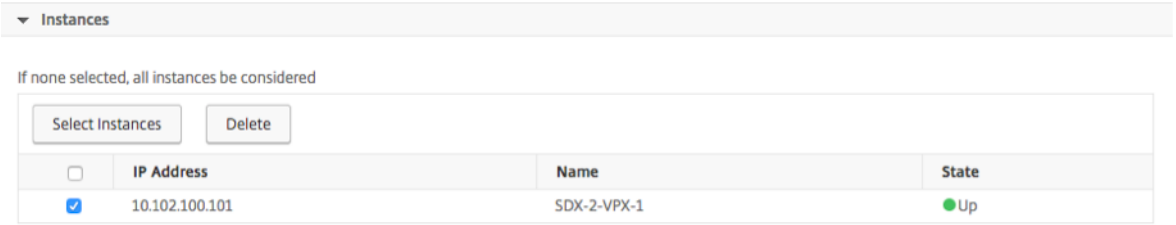
You can specify the category or categories of the events generated by your NetScaler instances. All categories are created on NetScaler instances. These categories are then mapped with NetScaler Console that can be used to define event rules. Select the category you want to consider and move it from the **Available** table to the **Configured** table.

In the example above, you must choose "cpuUsageHigh"as the event category from the table displayed.



Step 4 - Specify NetScaler instances

Select the IP addresses of the NetScaler instances for which you want to define the event rule. In the **Instances** section, click **Select Instances**. In the **Select Instances** page, choose your instances, and click **Select**.



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

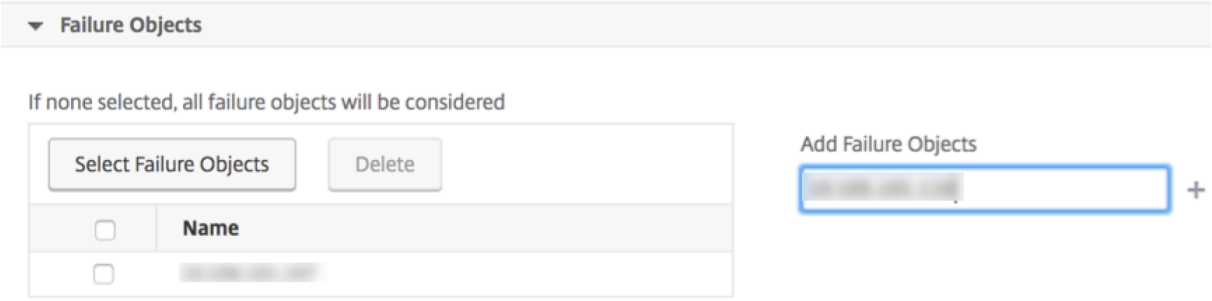
Step 5 - Select failure objects

You can either select a failure object from the list provided or add a failure object for which an event has been generated. You can also specify a regular expression to add failure objects. Depending on the specified regular expression, the failure objects are automatically added to the list. Failure objects are entity instances or counters for which an event has been generated.

> **Important**
>
> To list failure objects using regular expression, select **Enable Advanced Filter with Regex Matching** in Step 1.

The failure object affects the way that an event is processed and ensures it reflects the exact problem as notified. With this filter, you can 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 here is the user name or password, such as `nsroot`.

This list can contain counter names for all threshold-related events, entity names for all entity-related events, certificate names for certificate-related events, and so on.



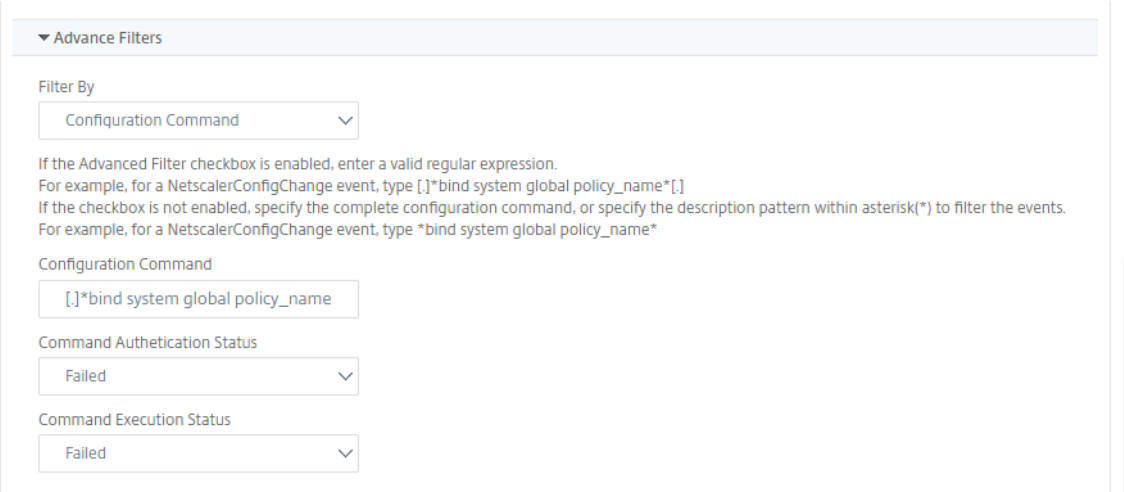
Step 6 - Specify advanced filters

You can further filter an event rule by:

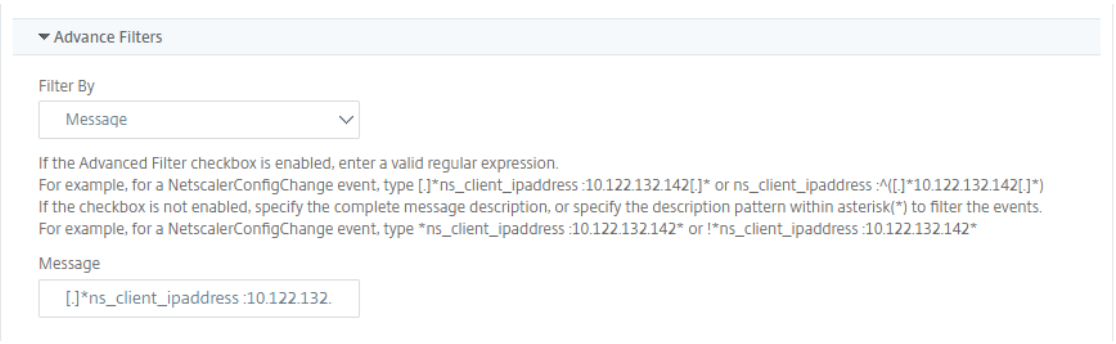
- **Configuration Commands** - You can specify the complete configuration command, or specify a regular expression to filter events.

  You can further filter the event rule by the command's authentication status and/ or its execution status. For example, for a `NetscalerConfigChange event`, type `[.]*bind system global policy_name[.]*`.

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



- **Messages** - You can 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[.]*)`
  .



Step 7 - Add event rule actions

You can add event rule actions to assign notification actions for an event. These notifications are sent or performed when an event meets the defined filter criteria that you've set above. You can add the following event actions:

- Send email Action
- Send Trap Action
- Run Command Action
- Run Job Action
- Suppress Action
- Send Slack Notifications

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

- Send PagerDuty Notifications
- Send ServiceNow Notifications

To set email Event Rule Action

When you choose the Send email Action event action type, an email is triggered when the events meet the defined filter criteria. You must either create an email distribution list by providing mail server or mail profile details or you can select an email distribution list that you've previously created.

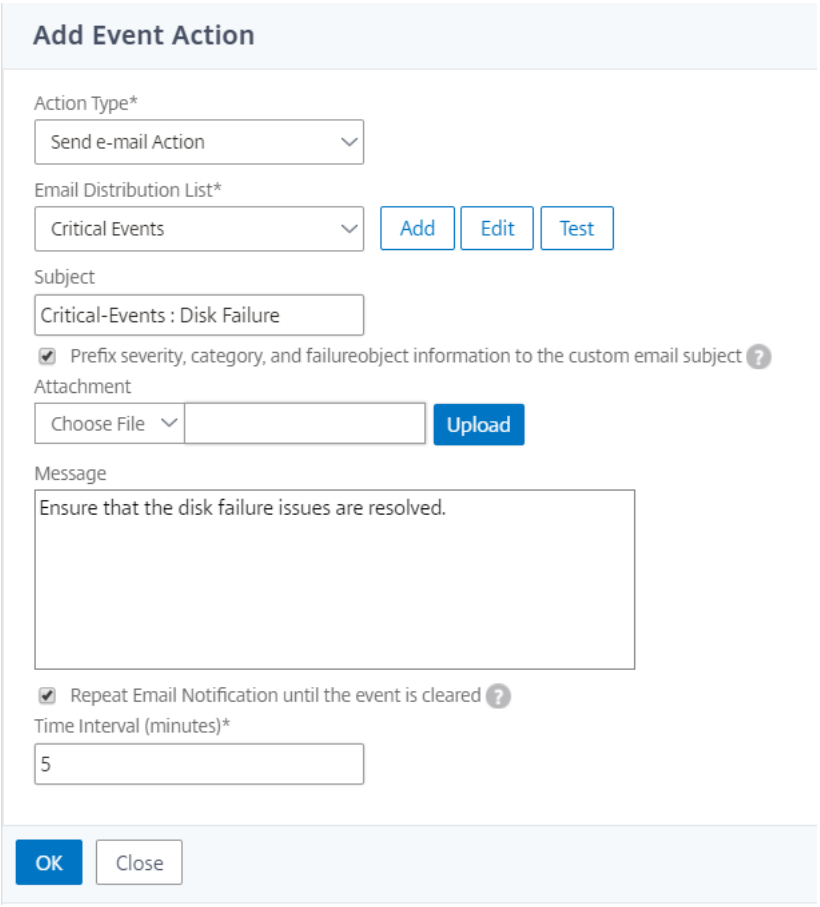
Due to a high number of virtual servers being configured in NetScaler Console, you might receive a high number of emails every day. The emails have a default subject line that provides information about the severity of the event, the category of the event and the failure object. But the subject line does not carry any information about the name of the virtual server where these events originate from. You now have an option to include some additional information like the name of the affected entity, name of the failure object.

You can also add a customized subject line and a user message, and upload an attachment to your email when an incoming event matches the configured rule.

While sending emails for event notifications, you might want to send a test email to test the configured settings. The "Test"button now allows you to send a test email after configuring an email server, associated distributed lists, and other settings. This feature ensures that settings are working fine.

You can also ensure that all critical events are addressed and no important email notifications are missed, by selecting the **Repeat Email Notification until the event is cleared** check box to send repeated email notifications for event rules that meet the criteria you've selected. For example, if you've created an event rule for instances that involve disk failures, and you want to be notified until the issue is resolved, you can opt to receive repeated email notifications about those events.

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



To set Trap Event Rule Action

When you choose the **Send Trap Action** event action type, SNMP traps are sent or forwarded to an external trap destination. By defining a trap distribution list (or a trap destination and trap profile details), trap messages are sent to specific trap listeners when events meet the defined filter criteria.

To set the 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 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 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 consider providing 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 NetScaler agent. For example, /var.
- Provide the .sh file location in NetScaler Console to run when the rule criteria are met.

To set the **Run Command** action for creating a new virtual server:

1. Define the rule
2. Select the severity of the event
3. Select the event category **entitydown**
4. Select the instance that has the virtual server configured
5. Select or create a failure object for the virtual server
6. Under **Event Rule Actions**, click **Add Action** and select **Run Command Action** from the **Action Type** list.
7. Under **Command Execution List**, click **Add**.

   The Create Command Distribution List page is displayed.

   a) In **Profile Name**, specify a name of your choice

   b) In **Run Command**, specify the NetScaler agent location, where the script must be run. For example: /sh/var/demo.sh $source $failureobj.

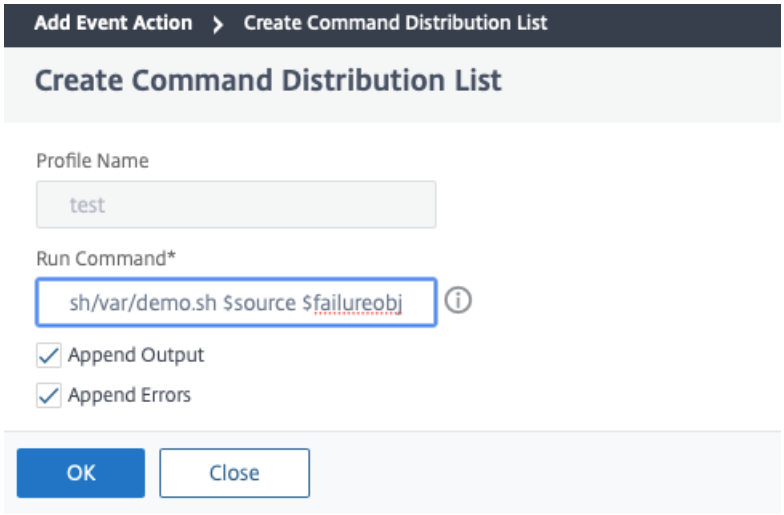
   c) Select **Append Output** and **Append Errors**

   > **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**.

8. In the **Add Event Action** page, click **OK**.

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



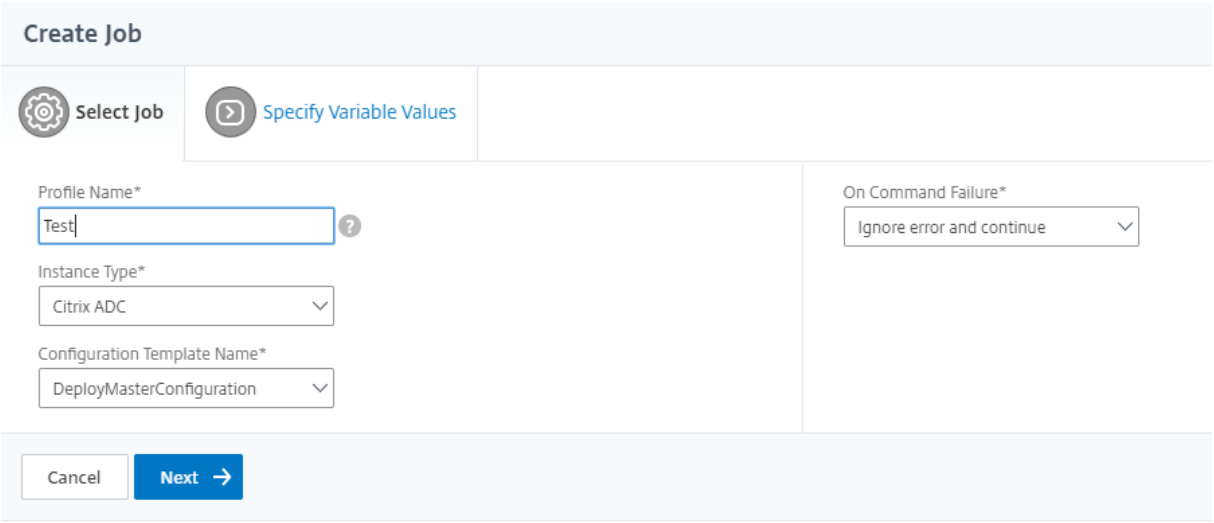
> **Note**
>
> You can enable the **Append Output** and **Append Errors** options if you want to store the output and errors generated (if any) when you run a command script in the NetScaler Console server log files. If you do not enable these options, NetScaler Console discards all outputs and errors generated while running the command script.

To set the `Execute` Job Action

By creating 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.

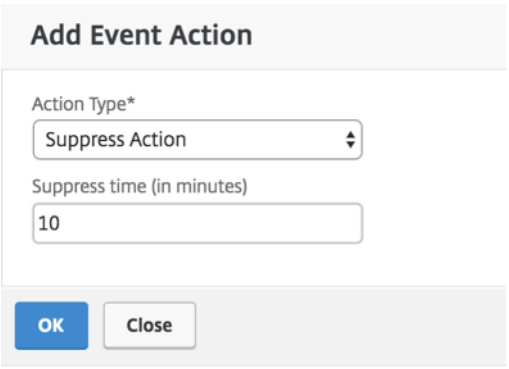
1. Under **Event Rule Actions**, click **Add Action** and select **Execute Job Action** from the **Action Type** drop-down list.
2. Create a profile with a job that you want to run when the events meet the defined filter criteria.
3. While creating a job, specify a profile name, the instance type, the configuration template, and what action you'd like to perform if the commands on the job fail.
4. Based on the instance type selected and the configuration template chosen, specify your variables values and click **Finish** to create the job.

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



To set the Suppress Action

When you choose the **Suppress Action** event action, you can configure a time period, in minutes, for which an event is suppressed or dropped. You can suppress the event for a minimum of 1 minute.



To set Slack notifications from NetScaler Console

Configure the required Slack channel by providing the profile name and the webhook URL in NetScaler Console GUI. The event notifications are then sent to this channel. You can configure multiple Slack channels to receive these notifications

1. In NetScaler Console, navigate to **Infrasturcture > Events > Rules**, and click **Add** to create a rule.
2. On the **Create Rule** page, set the rule parameters such as severity and category. Select instances and also failure objects that must be monitored.
3. Under **Event Rule Actions**, click **Add Action**. Then, select **Send Slack Notifications** from the **Action Type** list and select **Slack Profile List.**

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

4. You can also add a Slack profile list by clicking **Add** next to the **Slack Profile List** field.
5. Type the following parameters to create a profile list:
    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 have entered earlier. 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 to be posted on the designated Slack channel. An example of a webhook is as follows: https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK
6. Click **Create** and click **OK** in the **Add Event Action** window.

> **Note:**
>
> You can also add the Slack profiles by navigating to **System** > **Notifications** > **Slack Profiles**. Click **Add** and create the profile as described in the earlier section.

You can view the status of the Slack profiles that you have created.

Your event rule is now created with appropriate filters and well defined event rule actions.

To set PagerDuty notifications from NetScaler Console

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 registered number.

Before you add a PagerDuty profile in NetScaler Console, ensure you have completed the required configurations in PagerDuty. For more information, see 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.

To add a PagerDuty profile in NetScaler Console:

1. Log on to NetScaler Console using administrator credentials.
2. Navigate to **Settings > Notifications > PagerDuty Profiles**.

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

3. Click **Add** to create a new profile.
4. In the Create PagerDuty Profile page:
   a) Provide a profile name of your choice.
   b) Enter the **Integration Key**.
      You can get the Integration Key from your PagerDuty portal.
   c) Click **Create**.

   Use case:

   Consider a scenario that you:

   - want to send notifications to your PagerDuty profile.
   - have configured phone call as an option in PagerDuty to receive notifications.
   - want to get phone call alerts for NetScaler events.

   To configure:

   a) Navigate to **Events** > **Rules**
   b) On the **Create Rule** page, configure all other parameters to create a rule.
   c) Under **Create Rule Actions**, click **Add Action**.
      The **Add Event Action** page is displayed.
      i. Under **Action Type**, select **Send PagerDuty Notifications**.
      ii. Select your PagerDuty profile and click **OK**.

   After the configuration is complete, whenever a new event is generated for NetScaler instance, you will receive a phone call. From the phone call, you can decide to:

   - Acknowledge the event
   - Mark it as resolved
   - Escalate to another team member

To auto-generate ServiceNow incidents from NetScaler Console

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 NetScaler Console with a ServiceNow instance. For more information, see Configure ITSM adapter for ServiceNow.

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

To configure an event rule, navigate to **Events** > **Rules**.

1. On the **Create Rule** page, configure all other parameters to create a rule.
2. Under **Create Rule Actions**, click **Add Action**.

   The **Add Event Action** page is displayed.

   a) In **Action Type**, select **Send ServiceNow Notifications**.

   b) In **ServiceNow Profile**, select the **Citrix_Workspace_SN** profile from the list.

   c) Click **OK**.

Modify the reported severity of events that occur on NetScaler instances

September 27, 2025

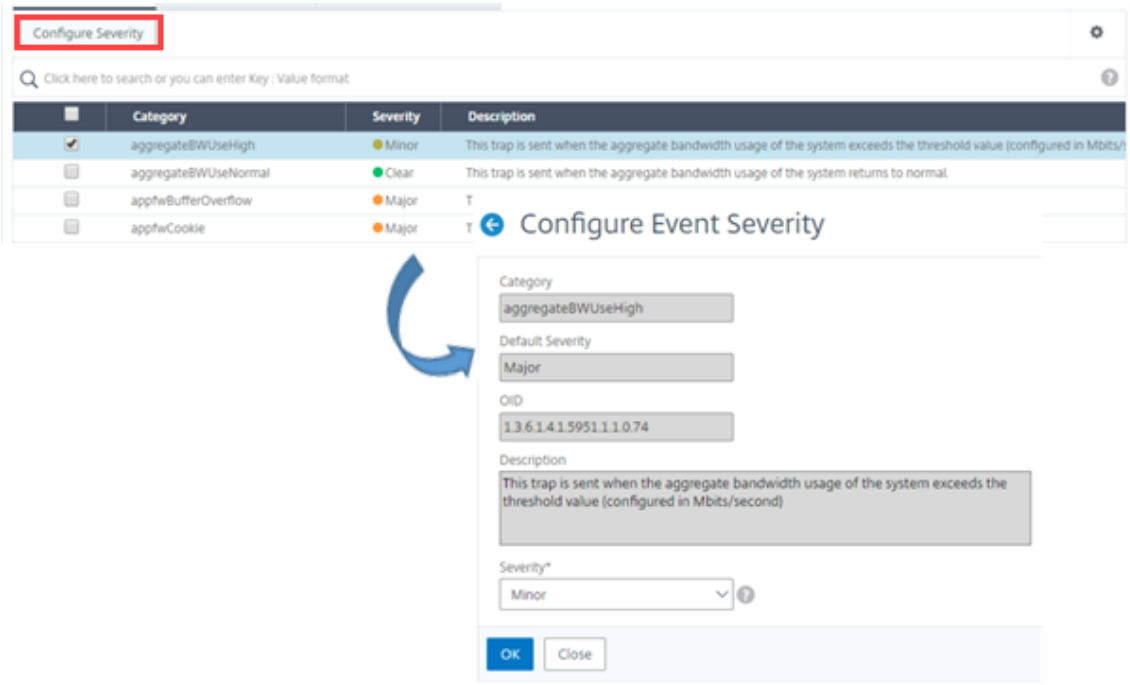
You can manage the reporting of events generated on all your devices, so that you can view event details regarding a particular event on a particular instance and view reports on the basis of event severity. You can create event rules that use the default severity settings, and you can change the severity 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.



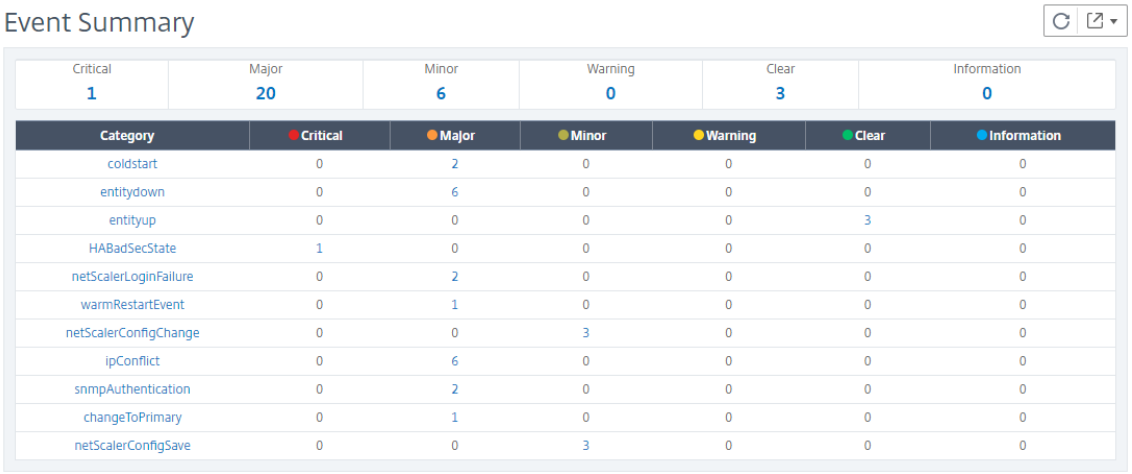
View events summary

September 27, 2025

You can now view an Events Summary page to monitor the events and traps received on your NetScaler Console server. Navigate to **Infrastructure > Events**. The Events Summary page displays the following information in a tabular format:

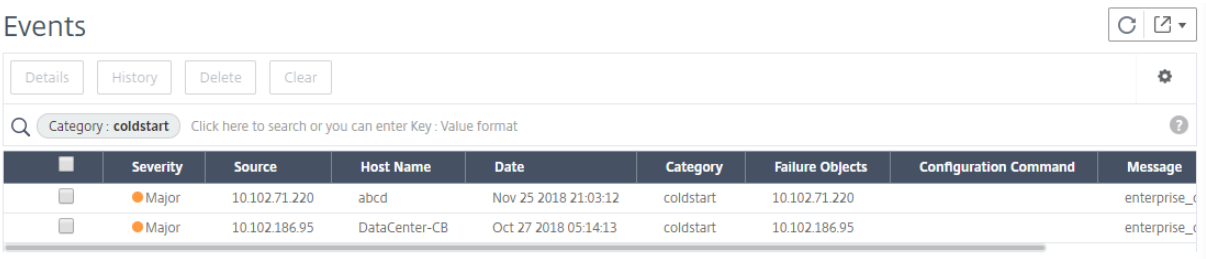
- **Summary of all the events received by NetScaler Console**. The events are listed by category, and the different severities are displayed in different columns: Critical, Major, Minor, Warning, Clear, and Information. For example, a Critical event would occur when a NetScaler instance goes down and stops sending information to the NetScaler Console server. During the event, a notification is sent to an administrator, explaining the reason 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 a summary and access the details of the event.

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



- **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 NetScaler instance's IP address and host name, date on which the trap was received, category, failure objects, configuration command run, and the message notification.



Display event severities and SNMP trap details

September 27, 2025

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 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

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

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.

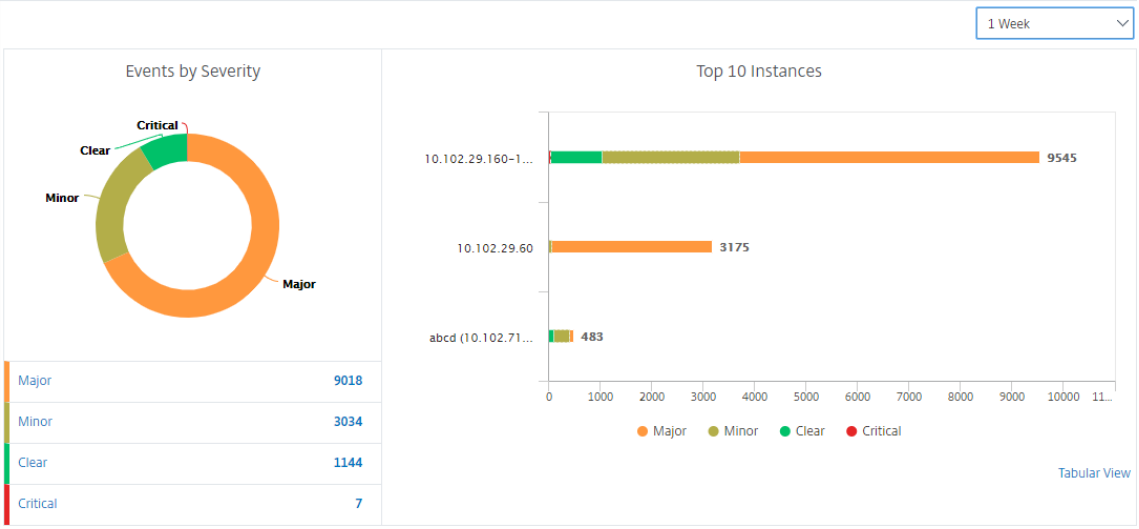
Similarly, you can view the health of a NetScaler VPX instance on the Dashboard. You can mask the time during which the instance was up and running, and display only the times the instance was out of service. By clicking on the graph, you are taken to that instance's page, where the *out of service* filter is already applied, and see details such as host name, the number of HTTP requests it received per second, CPU usage, and so on. You can also select the instance and see the particular Citrix instance's 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 > Dashboard**.

   Or,

   Navigate to **Infrastructure > Events > Reports**.
3. From the menu 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

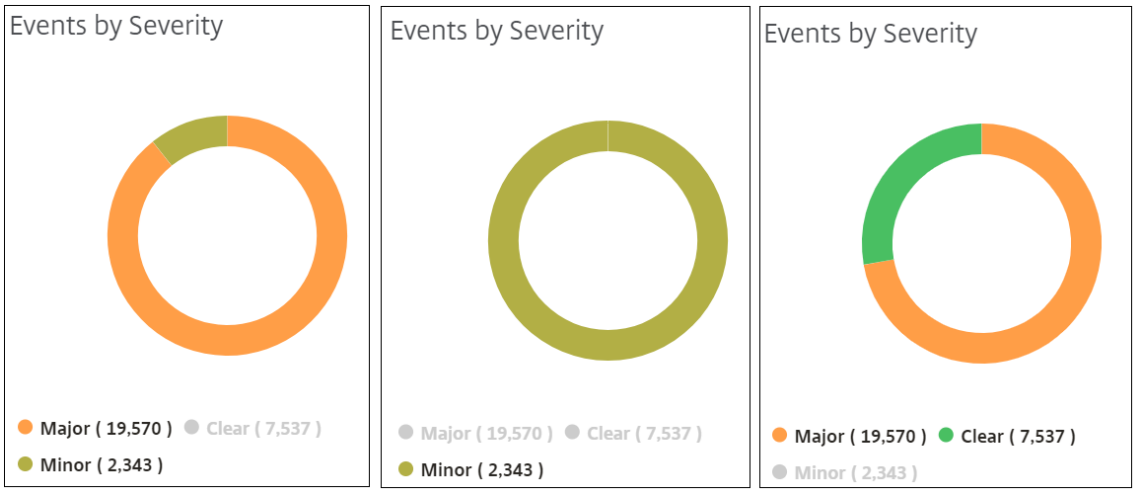
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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. You can toggle the severity types to more easily view and monitor your chosen severity.



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 server 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.

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

For example, an event with the trap category **monRespTimeoutBelowThresh**, the description of the trap is displayed as "This trap is sent when the response timeout for a monitor probe comes back to normal, less than the threshold set."

View and export NetScaler syslog messages

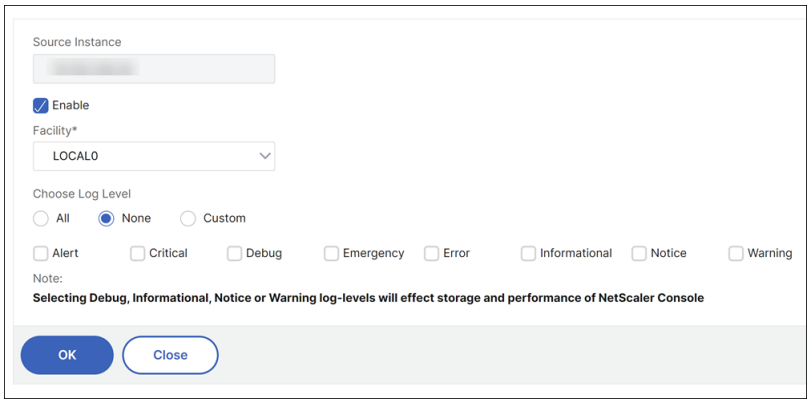
February 9, 2024

From your NetScaler Console, you can monitor the syslog events generated on your Citrix NetScaler instances. For that, you must configure NetScaler Console as the syslog server for your NetScaler instances. After you've configured NetScaler Console, all syslog messages are redirected from the NetScaler instances 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.
6. Select the required log level for the syslog messages.
7. Click **OK**.



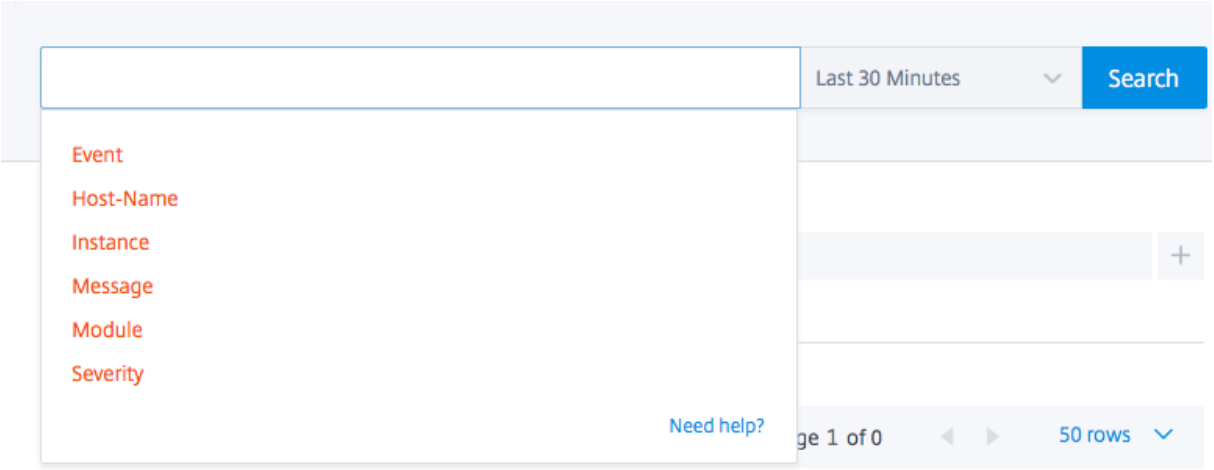
These steps configure all the syslog commands in the NetScaler instance, and NetScaler Console starts receiving the syslog messages.

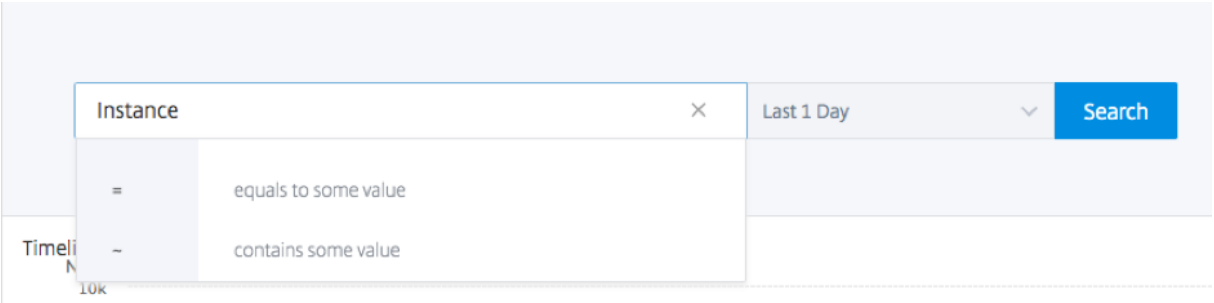
© 1997–2025 Citrix Systems, Inc. All rights reserved.

View and search syslog messages

You can view all your syslog messages generated on your managed NetScaler instances. The syslog messages are stored in the database centrally and are available under **Infrastructure > Events > Syslog Messages** for auditing purposes. You can combine this logging information and derive reports for analytics from the collected data.

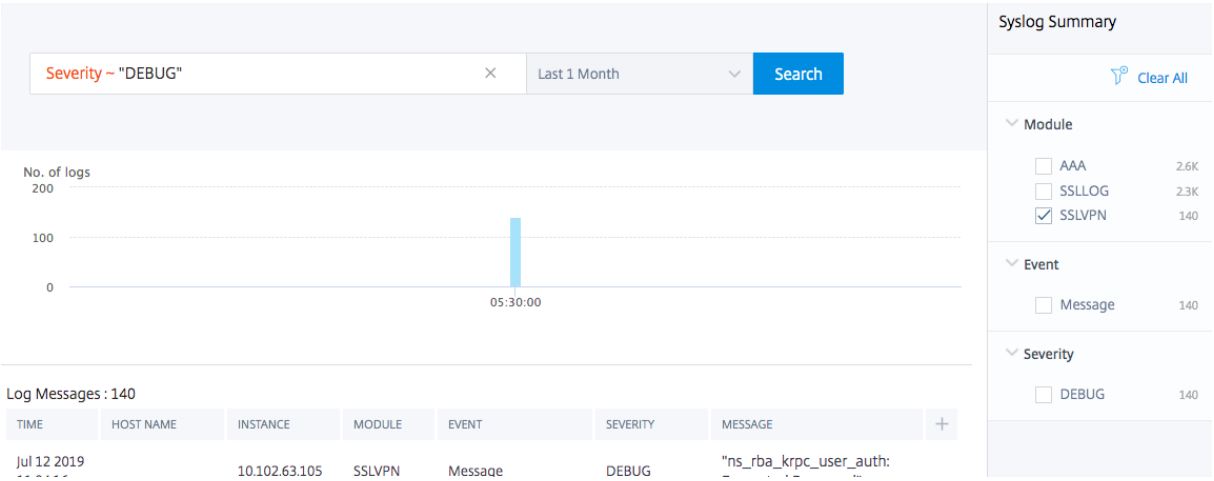
Further, you can use filters to narrow down the search results of syslog messages and find exactly what you are looking for and in real time. Click **Need Help?** to open the built-in search help.





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** pane.

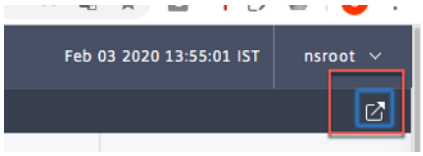
© 1997–2025 Citrix Systems, Inc. All rights reserved.



Export and schedule syslog messages

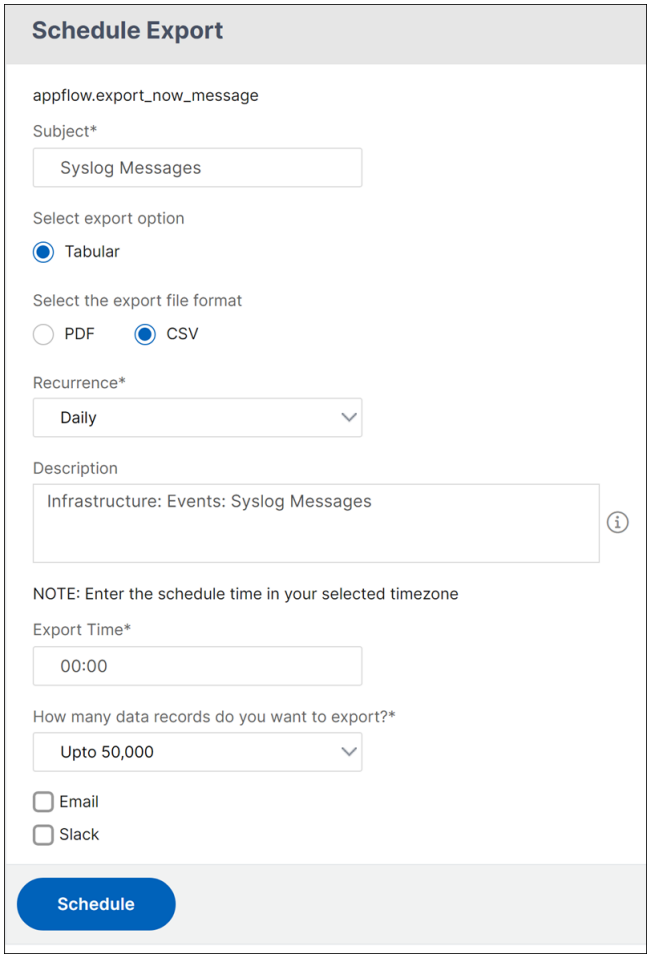
You can view syslog messages without logging into NetScaler Console, by scheduling an export of all syslog messages received on the server. You can export syslog messages that are generated on your NetScaler instances in PDF, CSV, PNG, and JPEG formats. You can schedule the export of these reports to specified email addresses or Slack account at various intervals.

To export and schedule the log messages, click the arrow icon on the upper right corner.



- To export the log messages, click **Export Reports > Export Now**, select the required format, and then click **Export**.
- To schedule the export of syslog messages, click **Export Reports > Schedule Report**, and set the required parameters. You can receive the report through email or Slack.

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



Suppress syslog messages

September 27, 2025

When configured as a syslog server, NetScaler Console receives all syslog messages sent to it by the configured NetScaler instances. There might be a large number of messages that you might not want to see. For example, you might not be interested in seeing all 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 matches 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

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

Console drops all messages that matches 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)

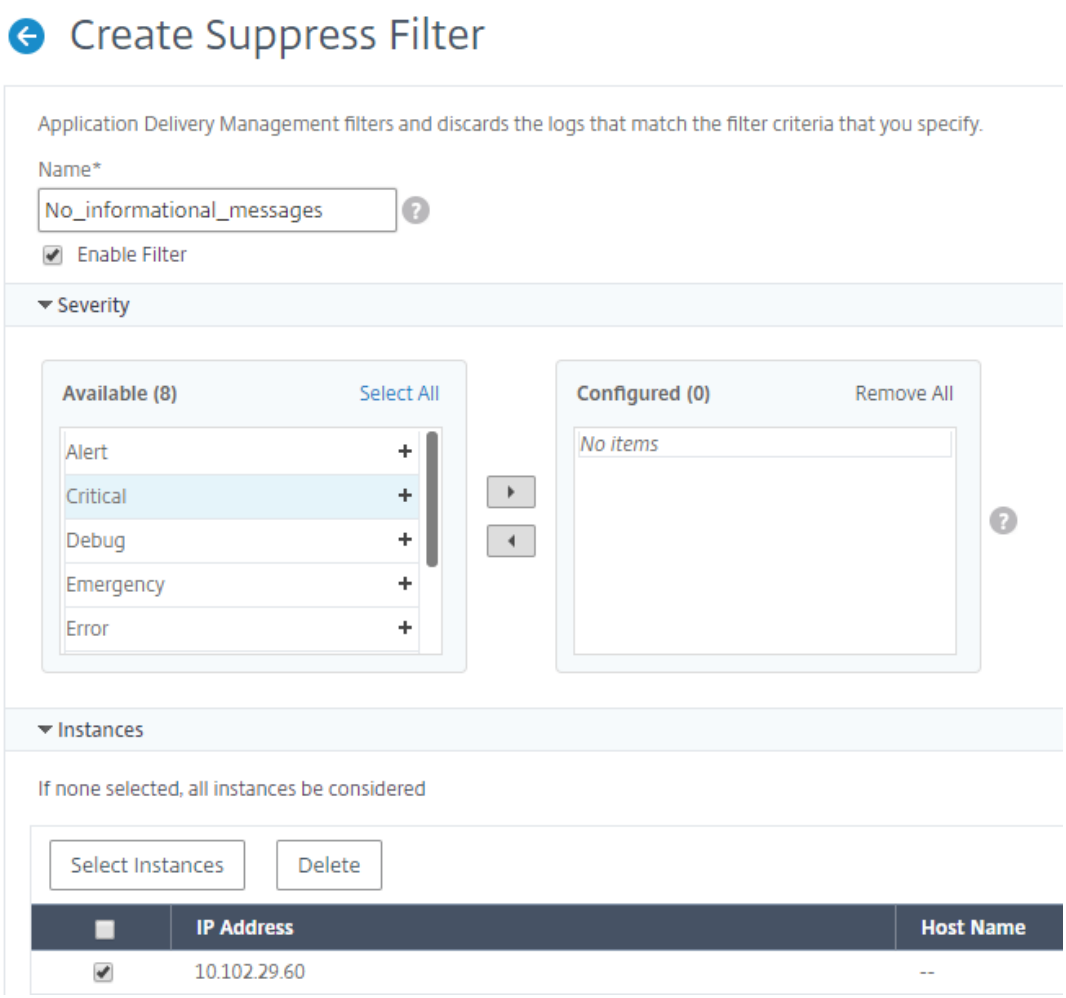
Suppressing syslog messages by creating filters

1. In NetScaler Console, navigate to **Infrastructure > Events > Syslog Messages** > **Suppress Filter**.
2. On **Create Suppress Filter** page, 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 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.

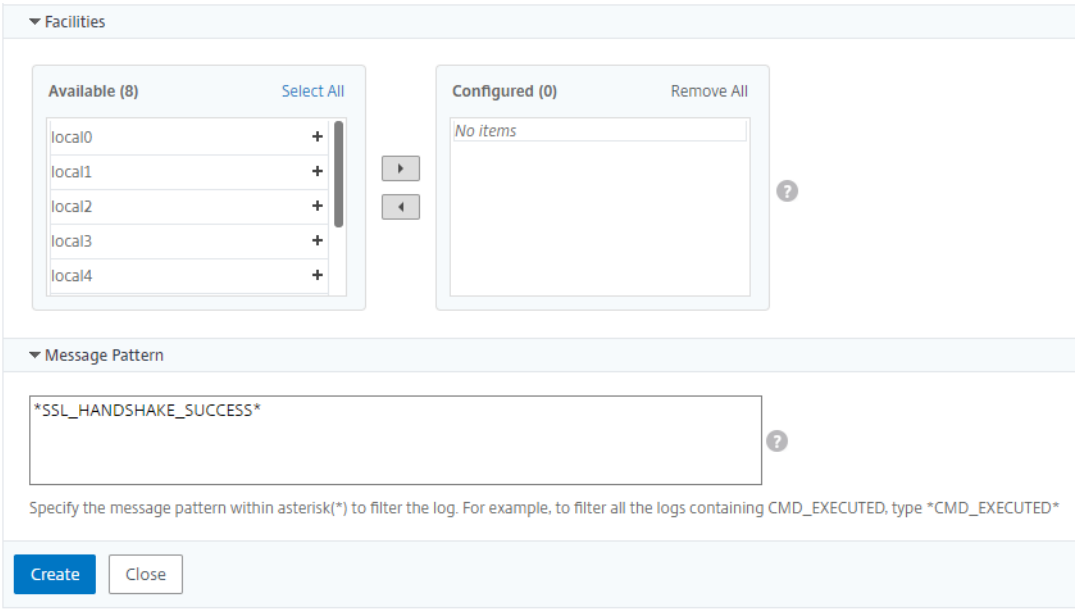
© 1997–2025 Citrix Systems, Inc. All rights reserved.



d) **Facilities** - Select the facility to suppress messages on the basis of the source that generates them.

e) **Message Pattern** - You can also type a text pattern surrounded by asterisk (*) to suppress the messages. The messages are searched for the text pattern string and those messages that contain this pattern are suppressed.

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



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** > **Suppress Filter**, and on **Suppress Filter** page, select the filter and click **Edit**.
2. On **Configure Suppress Filter** page, clear **Enable Filter** check box to disable the filter.

Configure prune settings for instance events

September 27, 2025

Citrix NetScaler instances managed by your NetScaler Console server send event messages data continuously to be stored on NetScaler Console. You can specify the interval for which you want NetScaler Console to retain network reporting data, events, audit logs, and task logs. By default, this data is pruned every 24 hours (at 00.00 hours).

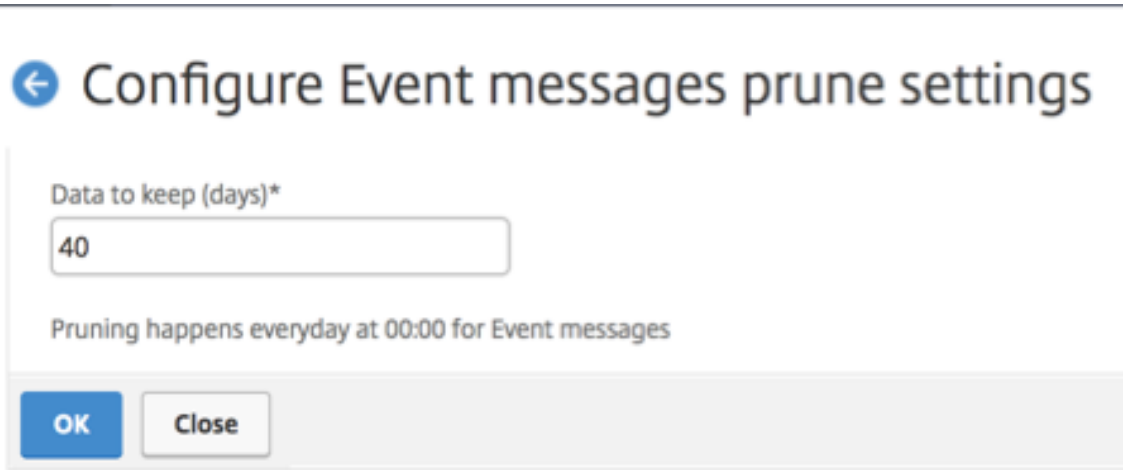
> **Note**
>
> The value you can specify cannot exceed 40 days or be less than 1 day.

To configure prune settings for instance events:

1. Navigate to **System** > **System Administration**.

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

2. Under **Prune Settings**, click **Instance Events Prune Settings**.
3. Enter the time interval, in days, for which you want to retain data on the NetScaler Console server and click **OK**.



Network functions

September 27, 2025

Using the Network Functions feature, you can monitor the state of the entities configured on your managed Citrix 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

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

Generate reports for load balancing entities

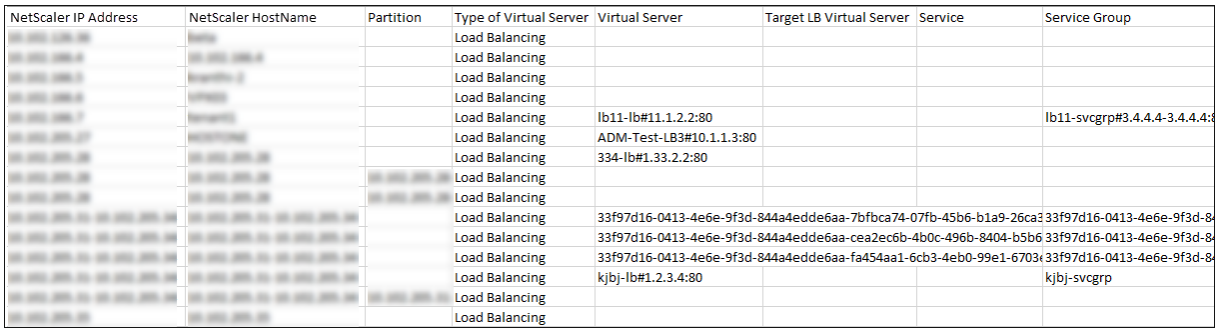
September 27, 2025

NetScaler Console allows you to view the reports of Citrix 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]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing	lb11-lb#11.1.2.2:80			lb11-svcgrp#3.4.4.4-3.4.4.4:
[redacted]	[redacted]		Load Balancing	ADM-Test-LB3#10.1.1.3:80			
[redacted]	[redacted]		Load Balancing	334-lb#1.33.2.2:80			
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-7bfbca74-07fb-45b6-b1a9-26ca3			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-cea2ec6b-4b0c-496b-8404-b5b6			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-fa454aa1-6cb3-4eb0-99e1-6703			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	kjbj-lb#1.2.3.4:80			kjbj-svcgrp
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]		Load Balancing				

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.

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

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 **Infrasturcture > Network Funtions > Load Balancing.**
2. On **Load Balancing** page, click  .
3. On the **Export** page that opens, you have two options to view the report:
   a) Select **Export Now** tab and click **OK**.

      The consolidated report downloads to your system.

   b) Select **Schedule Report** tab to schedule generating and exporting of the report at regular intervals. Specify the report generation recurrence settings and create an email profile to which the report is exported.

      i. **Recurrence** - select **Daily**, **Weekly**, or **Monthly** from the drop-down list box.

      ii. **Recurrence time** - Enter the time as Hour:Minute in 24-hour format.

      iii. **Email Profile** - Select a profile from the drop-down list box, or click **+** to create an email profile.

> **Note**
>
> If you select **Weekly** recurrence, ensure that you select the weekdays on which you want the report to be scheduled.



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

> **Note**
>
> If you select **Monthly** recurrence, ensure that you enter all the days that you want the report to be scheduled separated by commas.

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 **Infrasturcture > Network Funtions > Load Balancing > Services.**
2. On **Services** page, click the **Export** button at the top right-hand corner.
   a) Select **Export Now** tab if you want to generate and view the report at this instant.
   b) Select **Schedule Export** to schedule generating and exporting of the report at regular intervals.

> **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

September 27, 2025

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 NetScaler 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

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

- Virtual Server name
- Type of virtual server
- Virtual server
- 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.

> **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.
> - You cannot generate a network functions report for HAProxy.

To export and schedule network functions reports:

1. Navigate to **Infrastructure > Network Functions**.
2. On the **Network Functions** page, in the right pane, click **Generate Report** at the top right corner of the page.
3. On the **Generate Report** page, you have the following 2 options:

   a) Select **Export Now** tab and click **OK**. The report downloads to your system.

   The following image shows an example of a network functions report.

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

NetScaler IP Address	NetScaler HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing	lb11-lb#11.1.2.2:80			lb11-svcgrp#3.4.4.4-3.4.4.4:
[redacted]	[redacted]		Load Balancing	ADM-Test-LB3#10.1.1.3:80			
[redacted]	[redacted]		Load Balancing	334-lb#1.33.2.2:80			
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-7bfbca74-07fb-45b6-b1a9-26ca3			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-cea2ec6b-4b0c-496b-8404-b5b6			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-fa454aa1-6cb3-4eb0-99e1-6703			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	kjbj-lb#1.2.3.4:80			kjbj-svcgrp
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]		Load Balancing				

b) Select **Schedule Report** tab to schedule generating and exporting of the report at regular intervals. Specify the report generation recurrence settings and create an email profile to which the report is exported.

   i. **Recurrence** - select **Daily**, **Weekly**, or **Monthly** from the drop-down list box.

   ii. **Recurrence time**- Enter the time as Hour: Minute in 24-hour format.

   iii. **Email Profile** - Select a profile from the drop-down list box, or click **+** 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

September 27, 2025

You can optimize resource usage by monitoring your network reporting on NetScaler Application Delivery Management (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 all resources are used optimally.

NetScaler Console now allows you to generate reports not only for instances at a global level but also for entities such as the virtual servers and network interfaces. The instance family comprises NetScaler instances. 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

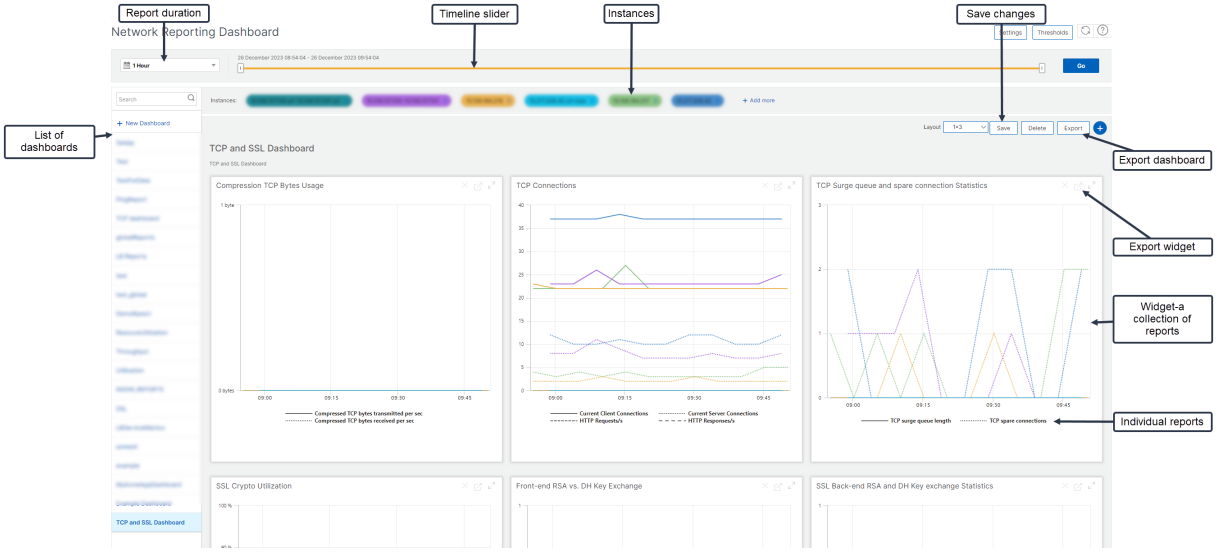
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- NetScaler Gateway

The network reporting dashboard in NetScaler Console is a highly customizable. You can now create multiple dashboards for various instances, virtual servers, and other entities.

Network reporting dashboard

The following image calls out the various features in the dashboard:



- The left side panel lists all the custom dashboards that are created in NetScaler Console. You can click one of them to view the various reports that the dashboard is composed of. For example, a TCP and SSL dashboard contains various reports related to TCP and SSL protocols.
- You can customize each dashboard with multiple widgets to display various reports. A widget represents a report on the dashboard, that is a collection of more related reports. For example, a compression TCP Bytes Usage report contains 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. In addition, you can now 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 the report must be generated. You can also configure an email distribution list to which the reports must be sent.
- The Instances section at the top of the dashboard lists the IP addresses of all the instances for which the report is generated.
- You can either remove instances by clicking “X”or add more instances to the reports. But, currently NetScaler Console allows you to view reports for 10 instances.

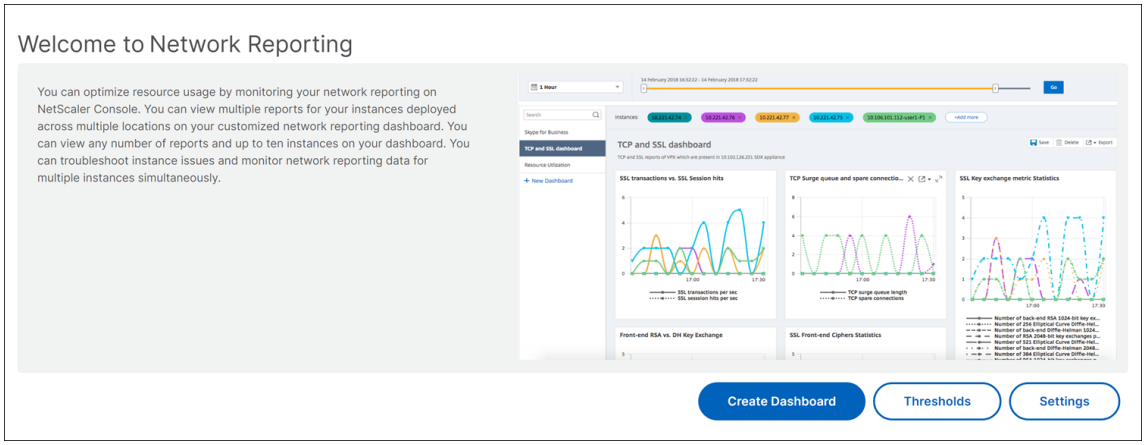
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- You can also export the entire dashboard as a .pdf, .jpeg, .png, or .csv format to your system. Any changes made to the dashboard must be saved. Click Save to save the changes.

The following section explains in detail the tasks to create a dashboard, generate reports, and to export reports.

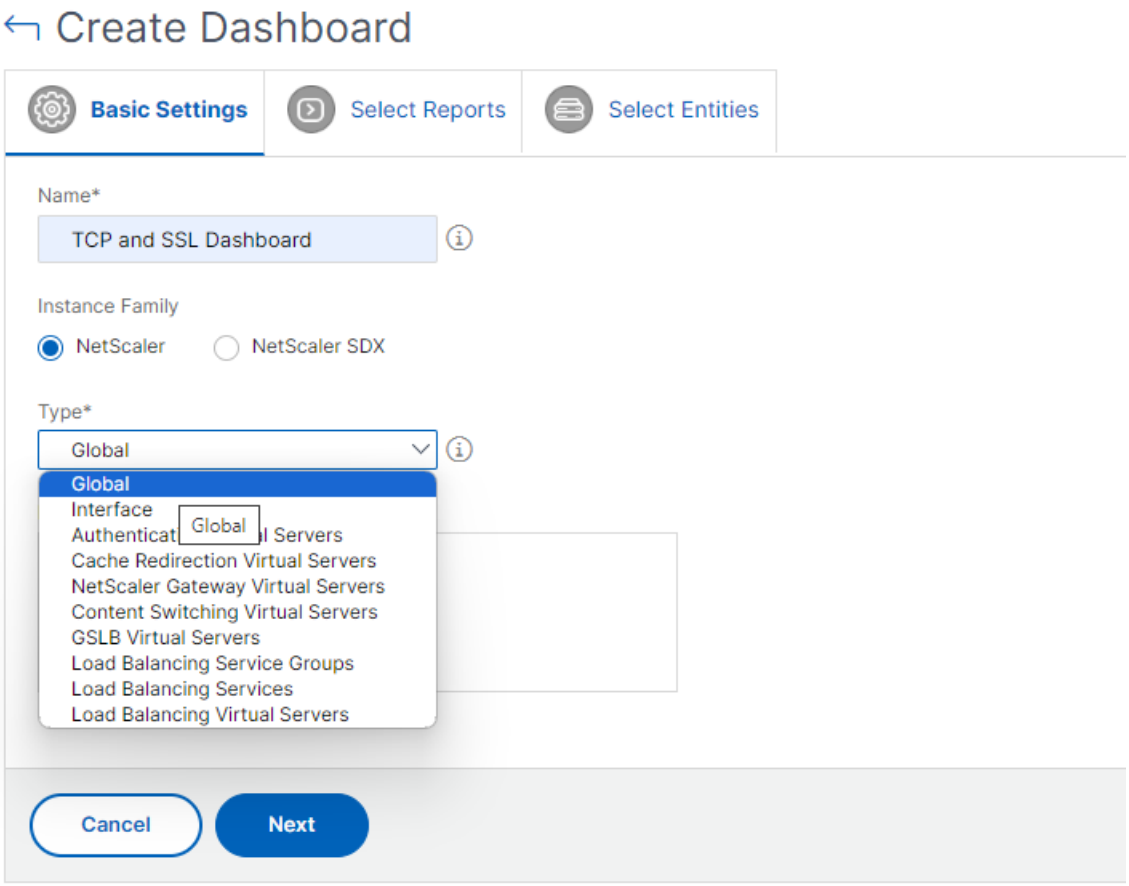
To view or to create a dashboard:

1. In NetScaler Console, navigate to **Infrastructure > Network Reporting**.



2. To view the existing dashboards, click **View Dashboard**. The Network Reporting **Dashboard** page opens where you can view all your dashboards and report widgets.
3. To create a dashboard, click **New Dashboard**. The Create Dashboard page opens.

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



4. In the Basic Settings tab, enter the following details:

   a) **Name**. Type the name of the dashboard.

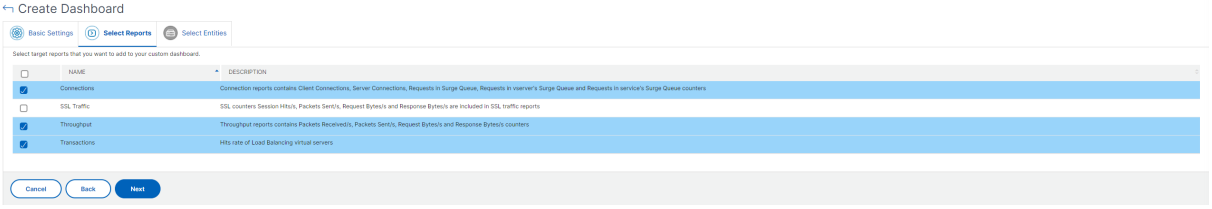
   b) **Instance Family**. Select the type of instance - NetScaler or NetScaler SDX.

   c) **Type**. Select the entity type for which you want to generate reports. In this example, select load balancing virtual servers.

   d) **Description**. Type a meaningful description for the dashboard.

5. Click **Next**. All the supported reports for the instance and the specific entity appear.

6. In the **Select Reports** tab, select the reports required. In this example, you can select transactions, connections, and throughput. Click **Next**.

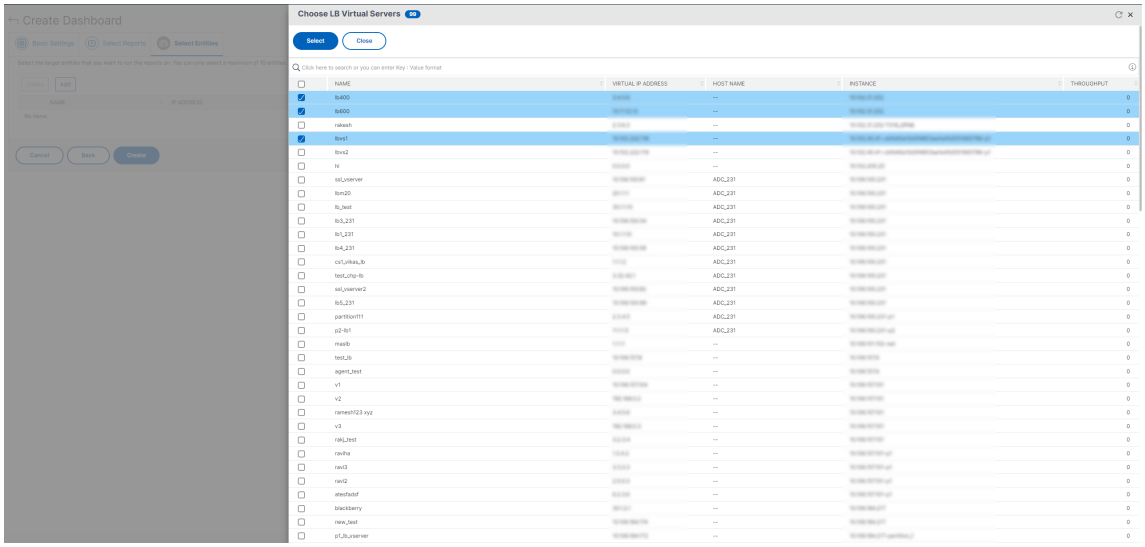


© 1997–2025 Citrix Systems, Inc. All rights reserved.

1. 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, **Choose LB Virtual Servers** window appears.

2. Select the entities that you want to monitor.



3. 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.

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 be able to create a file in NetScaler Console and to be able 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 have 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.

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

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, 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.

While scheduling network reports, you can customize the heading of the report by entering a text string in the **Subject** field. The report created at the scheduled time has this string as its name.

For example, for network reports originating from a particular virtual server, you can type in the subject as "authentication-reports-10.106.118.120,"where 10.106.118.120 is the IP address of the monitored virtual server.

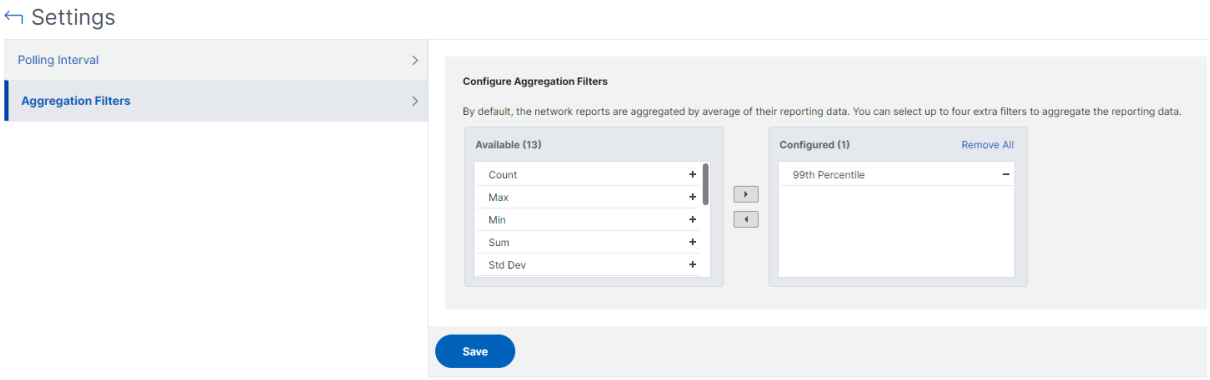
> **Note**
>
> Currently, this option is available only when you schedule the export of reports. You cannot add a heading to the report when you export them instantly.

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 ensure if all resources are used optimally. Navigate to **Network > Network Reporting** and select the time duration 1 day or later to get the **View By** option.

In the existing average data, you can apply aggregations by selecting the option from the **View By** list. When you apply aggregation, the data is updated for each metric in the dashboard. Click **Settings** and select **Aggregation Filters**.

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



The following are the aggregations that you can add:

- Count
- Max
- Min
- Sum
- Std Dev
- Variance
- Mode
- Median
- 25th Percentile
- 75th Percentile
- 95th Percentile
- 99th Percentile
- First
- Last

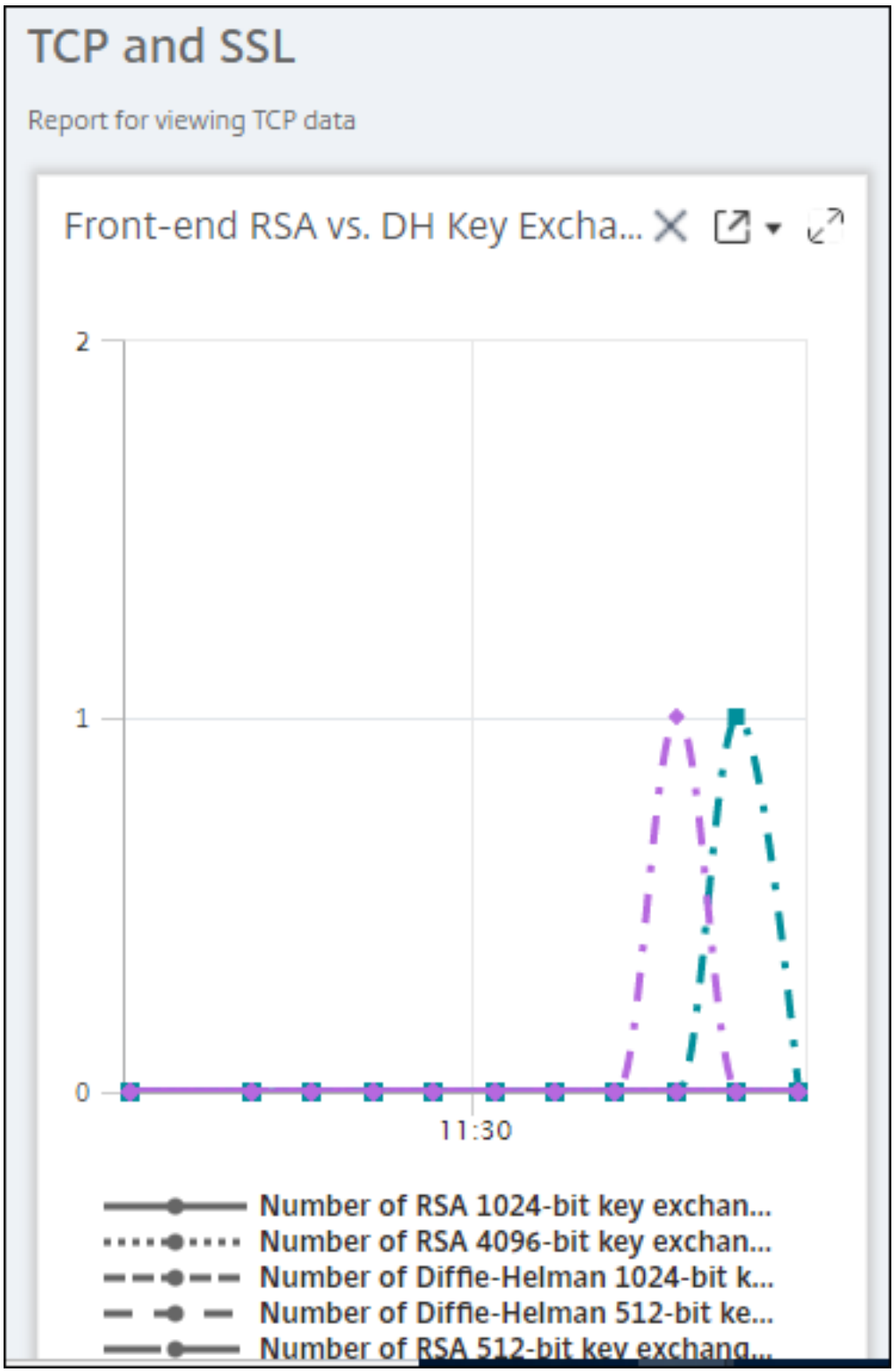
You can add up to 4 aggregation options to the dashboard. After you add the aggregation options, NetScaler Console takes approximately 1 hour to generate reports for the selected aggregation options.

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**.

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

4. Select a widget. For example, select **Load Balancing Virtual Server Transactions**.
5. Click the export button at the top right corner of the page
6. Under the **Export Now** tab, select the required format, and then click **Export**.



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

How to manage Thresholds for Network Reports on NetScaler Console

To monitor the state of a NetScaler instance, you can set thresholds on counters and receive notifications when a threshold is exceeded. On NetScaler Console, you can configure thresholds and view, edit, and delete them.

For example, you can receive an email notification when the Connections counter for a content switching virtual server reaches a specified value. You can define a threshold for a specific instance type. You can also choose the reports you want to generate for specific counter metrics from your chosen instance.

When the value of a counter exceeds or falls below (as specified by the rule) the threshold value, an event of the specified severity is generated to signify a performance-related issue. When the counter value returns to a value that you consider normal, the event is cleared. These events can be viewed by navigating to **Infrastructure > Events > Reports**. On the Reports page, you can click the **Events by Severity** donut to view events by their severity.

You can also associate an action with a threshold such as sending an email or SMS message when the threshold is breached.

To create a threshold:

1. In NetScaler Console, navigate to **Infrastructure > Network Reporting > Thresholds**. Under **Thresholds**, click **Add**.
2. On the **Create Threshold** page, specify the following details:
    - **Name**. Name of the threshold.
    - **Instance Type**. Choose NetScaler.
    - **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.

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

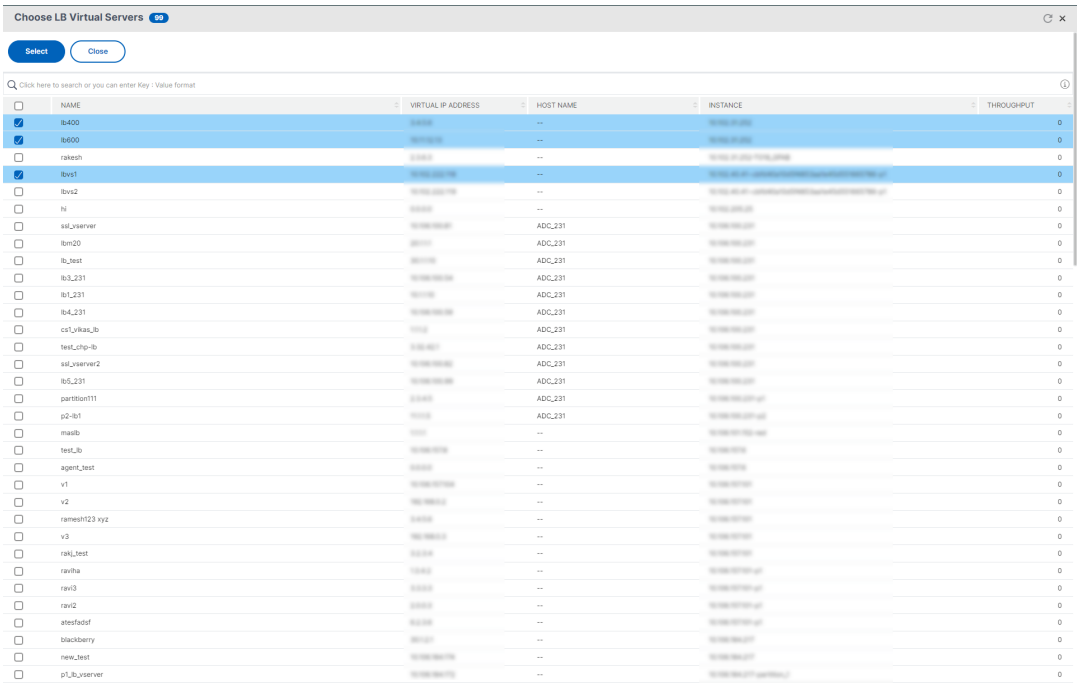
- **Clear Value**. Type the value that indicates when to clear the value. For example, you might want to clear the Current Client Connections threshold when the monitored value reaches 50 percent. In this case, type 50 as the clear value.
- **Event Severity**. Select the security level that you want to set for the threshold value.

4. You can choose instances and entities to be set with the threshold value. In the **Instances** section, choose one of the following options:

   - **All Instances**. The threshold is set for all the instances.
   - **Specific Instances**. The threshold is set for specific instances. Use the right arrow to move instances from the **Available** list to the **Configured** list. The threshold is set for the instances in the **Configured** list.
   - **Specific Entities**. The threshold is set for specific entities.

     Click **Add** to select the entities.

     A window appears with the entities list depending on the selected report type in the **Report Name** field. In this example, the **Choose LB Virtual Servers** window appears.



     Select the entities for which you want to set a threshold. Click **Select**. The selected entities appear in the **Instances** section.

     > **Note**
     >
     > The **Specific Entities** option appear only if you select vserver based reports in **Report Name**. For example, if you select **LB Service Statistics**

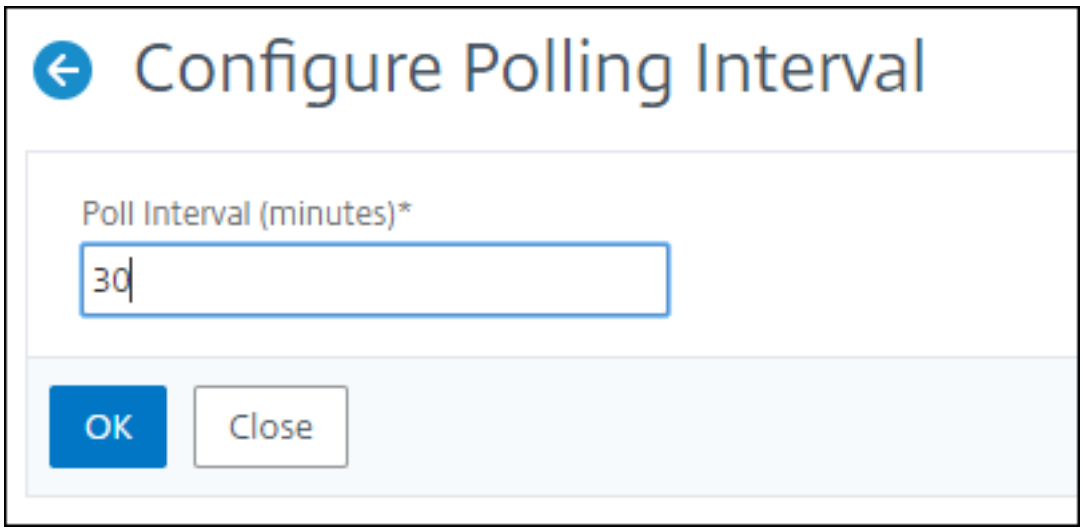
© 1997–2025 Citrix Systems, Inc. All rights reserved.

5. You can also add an **Event Message**. Type a message that you want to appear when the threshold is reached. NetScaler Console appends the monitored value and the threshold value to this message.
6. Select **Enable** to enable the threshold to generate alarms.
7. Optionally, you can configure **Actions** such as email or Slack notifications or both email and Slack notifications.
8. Click **Create**.

Set Performance Polling Interval for Network Reports

By default, every 5 minutes, NITRO calls collect performance data for network reporting. NetScaler Console retrieves instance statistics such as counter information and aggregates them based on per minute, per hour, per day, or per week. You can view this aggregated data in predefined reports.

To set the performance polling interval, navigate to **Infrasturcture > 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 setting 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 30 days or be less than 1 day.

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

Configuration jobs

September 27, 2025

NetScaler Application Delivery Management (NetScaler Console) configuration management process ensures the proper replication of configuration changes, system upgrades, and other maintenance activities across multiple Citrix NetScaler instances in the network.

NetScaler Console allows you to create configuration jobs that help you to perform all these activities with ease on several devices as a single task. Configuration jobs and templates simplify the most repetitive administrative tasks to a single task on NetScaler Console. A configuration job contains a set of configuration commands that you can run on one or multiple managed devices.

Configuration Jobs can either use SSH commands to do configuration commands or use SCP to do file copy from either locally or to another appliance, for example, we can schedule a HA-failover or HA-upgrade.

You can create a configuration job by using one of the following four options in NetScaler Console. Use one of these to create a reusable source of commands and instructions to the system to run a configuration job.

1. Configuration Template
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.

> **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.

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

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.

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 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.

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

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

- How to Use Configuration Templates to Create Audit Templates
- How to Use Record-and-Play to Create Configuration Jobs
- How to Use the Master Configuration Template on NetScaler Console

Create a configuration job

September 27, 2025

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, replicate configurations on multiple instances on your network, and record-and-play configuration tasks using the NetScaler Console GUI and convert it into CLI commands.

You can use the Configuration Jobs feature of NetScaler Console to create a configuration job, send email notifications, and check execution logs of the jobs created.

To create a configuration job on NetScaler Console:

1. Navigate to the **Infrastructure > Configuration > Configuration Jobs**.
2. Click **Create Job**.
3. On the **Create Job** page, under the **Select Configuration** tab, specify the Job Name and select the **Instance Type** from the list.
4. In the **Configuration Source** list, select the configuration job template that you want to create. Add the commands for the selected template.
    - You can either enter the commands or import the existing commands from the saved configuration templates.
    - You can also add multiple templates of different types in the Configuration editor while creating a job in the Configuration Jobs.
    - From the **Configuration Source** list, select the different templates and then drag the templates into the configuration editor. The template types can be **Configuration Template**, **In built Template**, **Master Configuration**, **Record and Play**, **Instance** and **File**.

    > **Note**
    >
    > If you add the `Deploy Master Configuration Job` template for the first time, add a template of different type, then the whole job template becomes a `Master Configuration` type.

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

You can also rearrange and reorder the commands in the configuration editor. You can move the command from one line to another by dragging and dropping the command line. You can also move or rearrange the command line from one line to any target line by simply changing the command line number in the text box. You can also rearrange and reorder the command line while editing the configuration job.

You can define variables that enable you to assign different values for these parameters or run a job across multiple instances. You can review all the variables that you have defined while creating or editing a configuration job in a single consolidated view. Click the **Preview Variables** tab to preview the variables in a single consolidated view that you have defined while creating or editing a configuration job.

You can customize rollback commands for every command on the configuration editor. To specify your customized commands, Enable the custom rollback option.

> **Important**
>
> For custom rollback to take effect, complete the **Create Job** wizard. And in the **Execute** tab, select the **Rollback Successful Commands** option from the **On Command Failure** list.

5. In the **Select Instances** tab, select the instances on which you want to run the configuration audit.

   a) In a NetScaler high-availability pair, you can run a configuration job local to a primary or a secondary node. Select on which node you want to run the job.

      - **Execute on primary nodes** - Select this option to run the job only on primary nodes.
      - **Execute on secondary nodes** - Select this option to run the job only on secondary nodes.

      You can also choose both primary and secondary node to run the same configuration job. If you do not select either primary or secondary node, automatically the configuration job runs on the primary node.

6. In the **Specify Variable Values** tab, you have two options:

   a) Download the input file to enter the values for the variables that you have defined in your commands, and then upload the file to the NetScaler Console server.

   b) Enter common values for the variables that you have defined for all instances

   c) Click **Next**.

To send an email and Slack notification for a job:

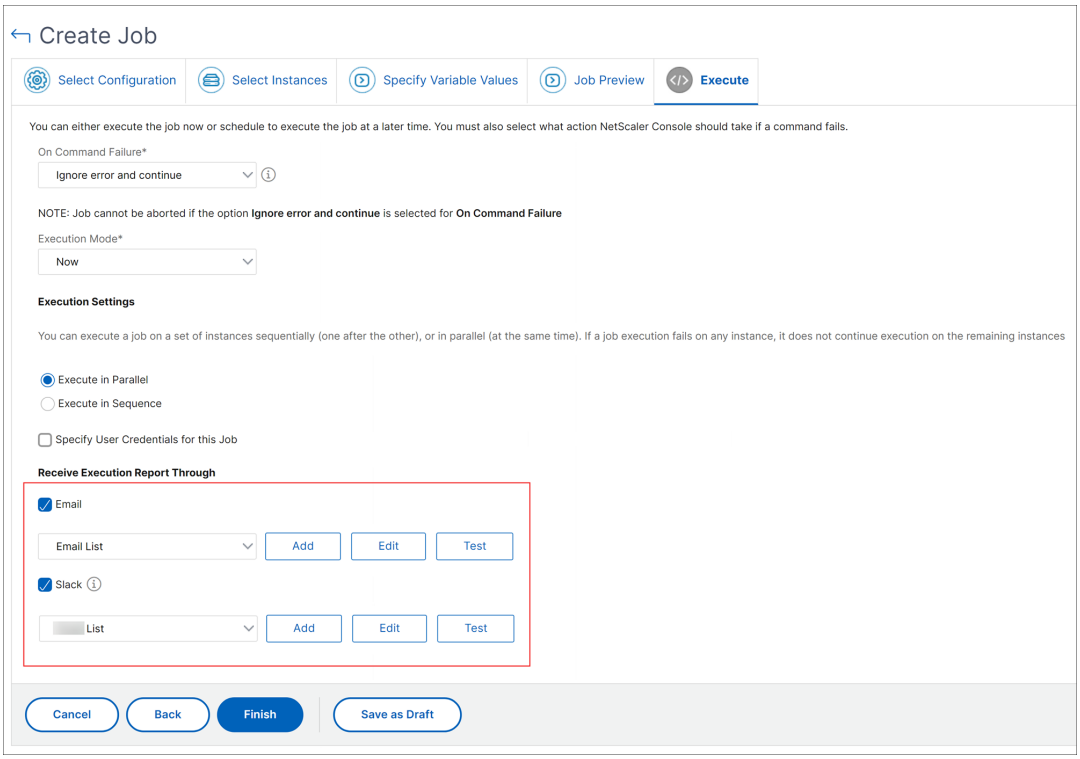
An email and Slack notification is now sent every time a job is run or scheduled. The notification includes details such as the success or failure of the job along with the relevant details.

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

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.
   - 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 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:

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

- 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.

- Select the **Slack** check box and choose the slack channel to which you want to send the execution report.

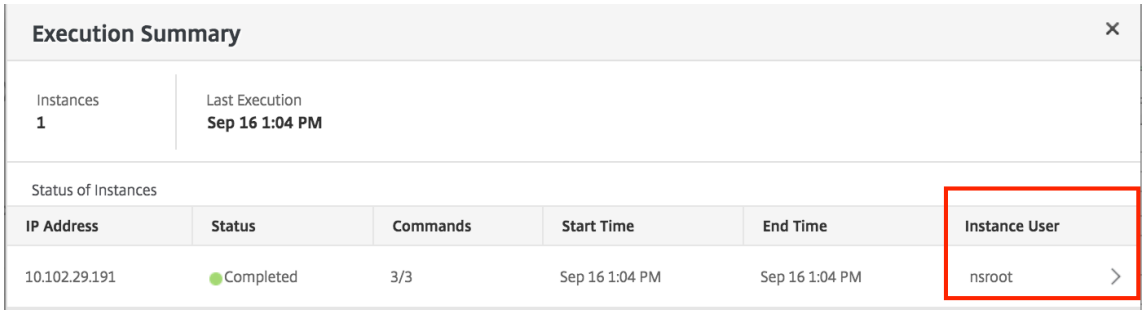
  If you want to add a Slack profile, click **Add** and specify the **Profile Name**, **Channel Name**, and **Token** of the required Slack channel.

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 that run the job
   - The commands run on the job
   - The start and end time of the job, and
   - The instance user's name



View audit reports

September 27, 2025

(NetScaler Console) allows you to view and download the configuration audit diff report in the configuration audit section. The configuration audit section allows you to export the:

- Summary report across all instances per instance
- Granular differential (diff) report for each instance-template pair

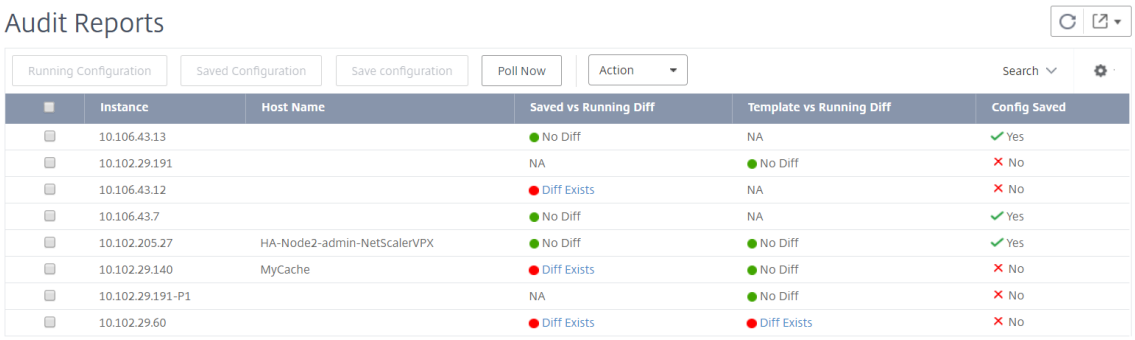
© 1997–2025 Citrix Systems, Inc. All rights reserved.

The audit templates in **Audit Templates** run at the scheduled time against the configurations in the specified instances. The **NetScaler Config Drift** chart on the **Configuration Audit** dashboard displays high-level details about configuration changes in saved against unsaved configurations. When you click the **NetScaler Config Drift** chart, the ensuing **Audit Reports** page displays a list of instances that shows both "Diff Exists"and No Diff." You can download the diff reports displayed by NetScaler Console.

NetScaler Console also provides an option to schedule automatic export of a diff report as a mail attachment.

To export configuration audit reports:

1. In NetScaler Console, navigate to **Infrastructure > Configuration > Configuration Audit**.
2. On the **Configuration Audit** page, click inside the **NetScaler® Config Drift** chart.
3. The **Audit Reports** page lists instances that have a difference. The page also displays a list of instances that does not have any difference in their running configurations.



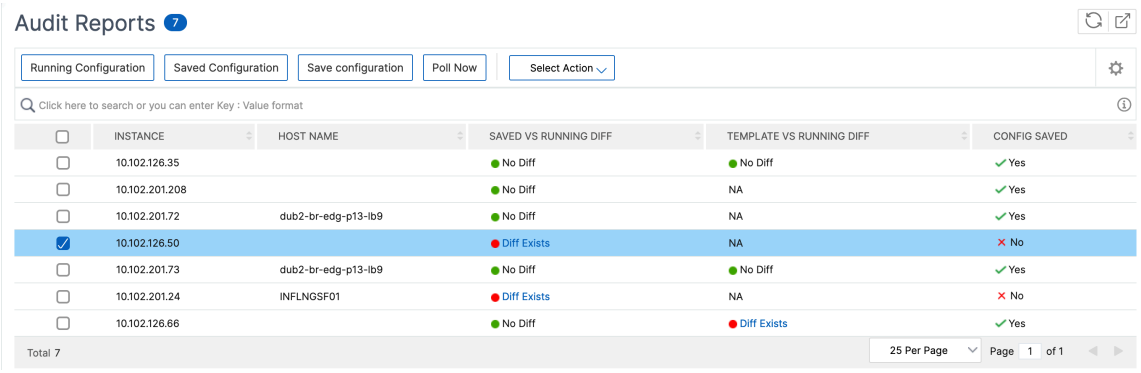
In the image you can see that for some instances a diff is present only in **Saved Vs Running Diff** and for some instances, a diff is present only in **Template vs Running Diff**. For some instances, differences exist in both **Saved Vs Running Diff** and **Template vs Running Diff.**

Saved Vs Running Diff

You can view a report of the diff between the configuration saved on the instance and the configuration that is currently running on the instance.

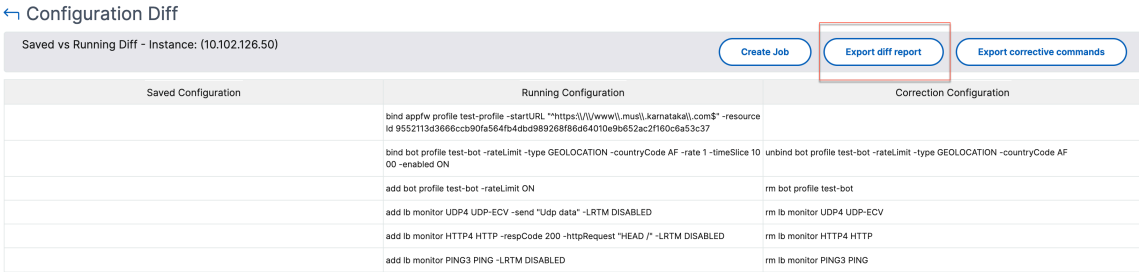
1. Click **Diff Exists** for an instance under **Saved Vs Running Diff.**

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



You can view the report for saved configuration against running configuration diff for that instance.

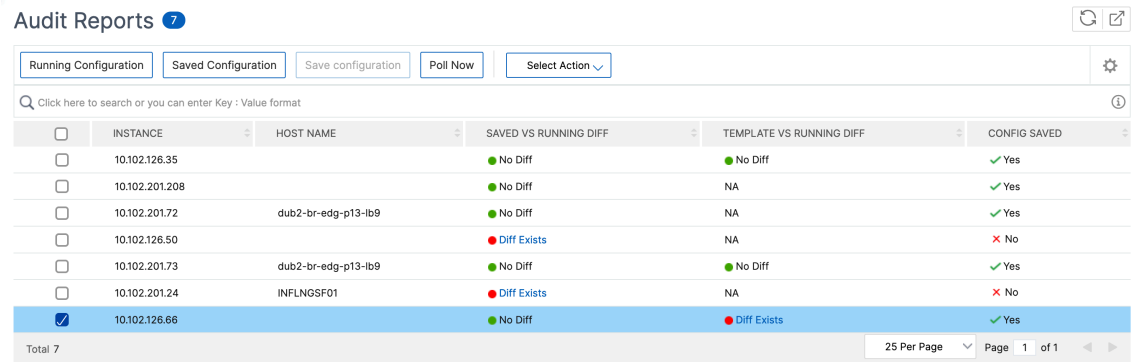
2. Click **Export diff report** to download a .csv file of the diff report. You can also click **Export corrective commands** to export the commands to a .txt file. You can then run the commands on the associated NetScaler Console instance from Configuration Jobs to correct the configuration in that instance.



Template vs Running Diff

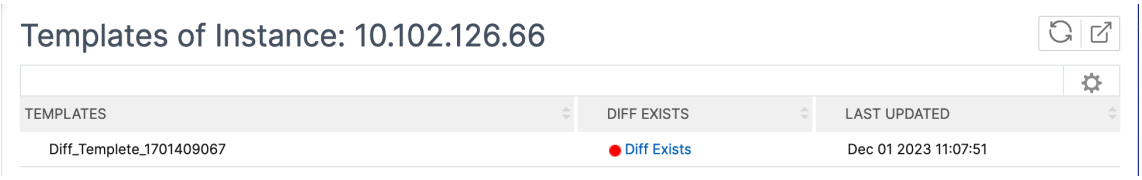
The **Template vs Running Diff** includes all templates other than **Saved Vs Running Diff** which is the default template. You can view the difference that exists between the template and the running configuration.

1. Click **Diff Exists** for one of the instances under **Template vs Running Diff.**

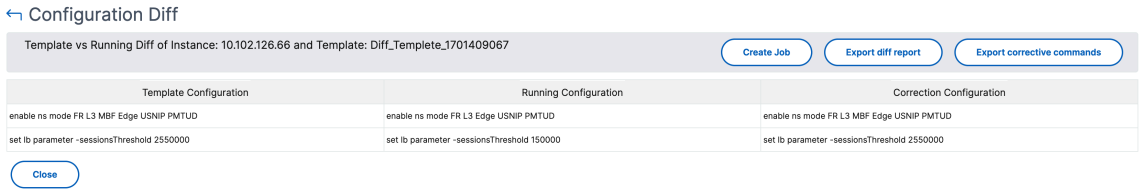


© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. The templates reveal the differences when the NetScaler Console instance deviates from the configuration specified by the template.



3. Click **Diff Exists** again. The following image shows the configuration that the template is looking for, the running configurations, and the correction configurations or the commands to run to correct the configuration. If the **Running Configuration** is blank, it means either that commands are not configured or are removed.



4. Click **Export diff report** to download a .csv file of the diff report. You can also click **Export corrective commands** to export the commands to a .txt file. You can then run the commands in CLI to correct the configuration in the instance.

Template_vs_Running_Diff_of_Instance _10.102.126.66_and_Template _Diff_Templete_1701409067

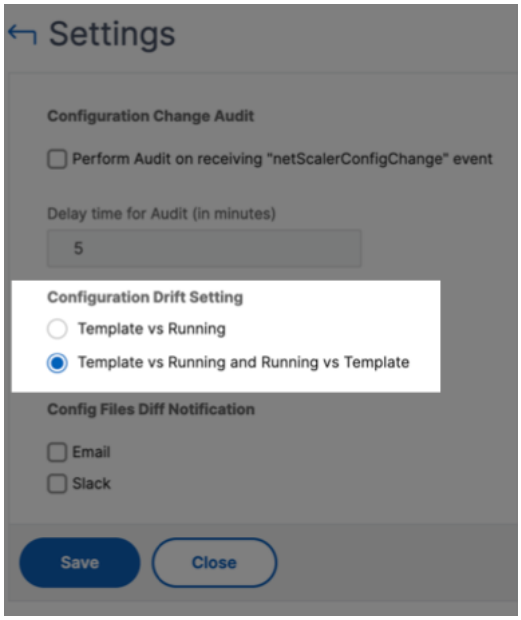
Template Configuration	Running Configuration	Correction Configuration	
enable ns mode FR L3 MBF Edge USNIP PMTUD	enable ns mode FR L3 Edge USNIP PMTUD	enable ns mode FR L3 MBF Edge USNIP PMTUD	
set lb parameter -sessionsThreshold 2550000	set lb parameter -sessionsThreshold 150000	set lb parameter -sessionsThreshold 2550000	

You can also use Template vs Running and Running vs template drift setting, to compare the configuration from both ways:

- Compares the audit template configuration with the running configuration on the instance.
- Compares the running configuration on the instance with the audit template.

By default, the Template vs. Running drift setting is selected. To modify the drift setting, select **Settings** in the **Configuration Audit** page.

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



View the file status audit reports

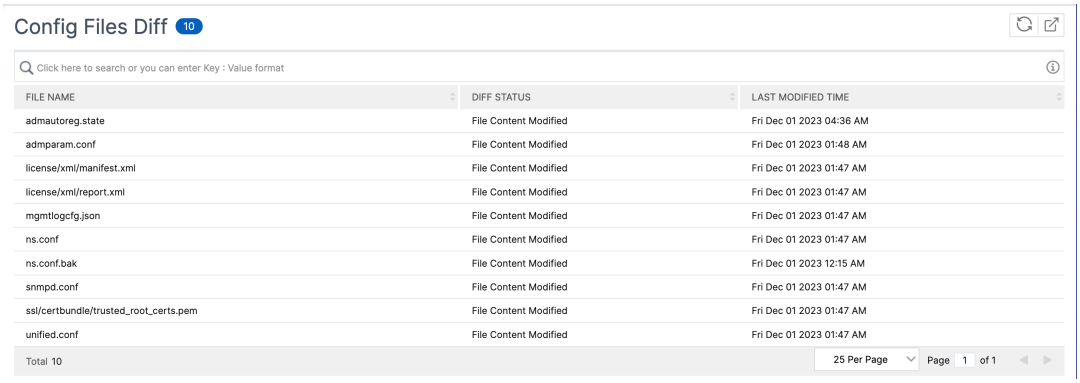
Use the **NetScaler File Status** chart to monitor if any files are added to, modified, or removed from the `nsconfig` folder. For example, if the license file is updated on an NetScaler instance, you can check when this file was last updated and take the required actions.

1. Navigate to **Infrastructure > Configuration > Configuration Audit**.
2. In the **Configuration Audit** page, click the **NetScaler Config File Status** chart.

   The **Audit Reports** page lists instances with the Diff status.

   The **Diff Status** is calculated for the interval between the **Previous Polled Time** to the **Latest Polled Time**. The **Diff Status** can be one of the following:

   - **Diff exists** - This status indicates that the files have changed in the `nsconfig` folder of an instance since the **Previous Polled Time**. To view what has changed on the file, click **Diff Exists**.



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

- **No Diff** - This status indicates the files in the `nsconfig` folder hasn't changed since the previous polled time.
- **NA** - This status indicates that monitoring the file status is not applicable. This status appears when the NetScaler Console doesn't poll the instance. For example, when an instance is added newly or an instance state is inactive the polling of the instance doesn't occur.

Audit configuration changes across instances

September 27, 2025

You want to make sure that certain configurations are running on specific instances for optimal performance of your network. You also want to monitor configuration changes across managed NetScaler instances, troubleshoot configuration errors, and recover unsaved configurations after a sudden system shutdown.

You can create audit templates with specific configurations to audit on certain instances. NetScaler Console compares these instances with the audit template and reports if there is a mismatch in the configuration. The configuration diff report enables you to troubleshoot and rectify unwanted configuration changes.

You can automate the running of the audit template by:

- Scheduling the time at which the template must be run.
- Setting the frequency at which NetScaler Console must run the template. You can run the template daily, on a specific day in a week, or on a specific date in a month.

You also have an option to send the diff report generated by NetScaler Console to specified email addresses that you can configure. With this option, users can receive the report as a mail attachment or a Slack notification. They don't have to log on to NetScaler Console to export the reports manually.

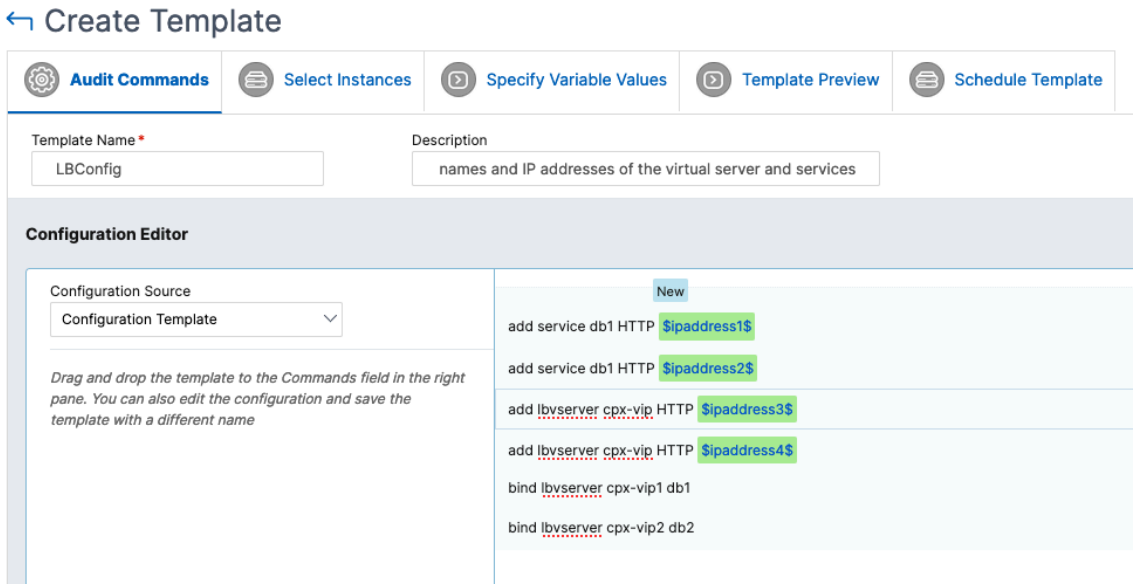
> **Note:**
>
> The **Rename** option is disabled for the default configuration templates. However, you can rename custom configuration templates.

To create audit templates:

1. Navigate to **Infrastructure > Configuration > Configuration Audit > Audit Templates**, and click **Add**.
2. In the **Create Template** page, and in the **Audit Commands** tab, specify the template name and its description.

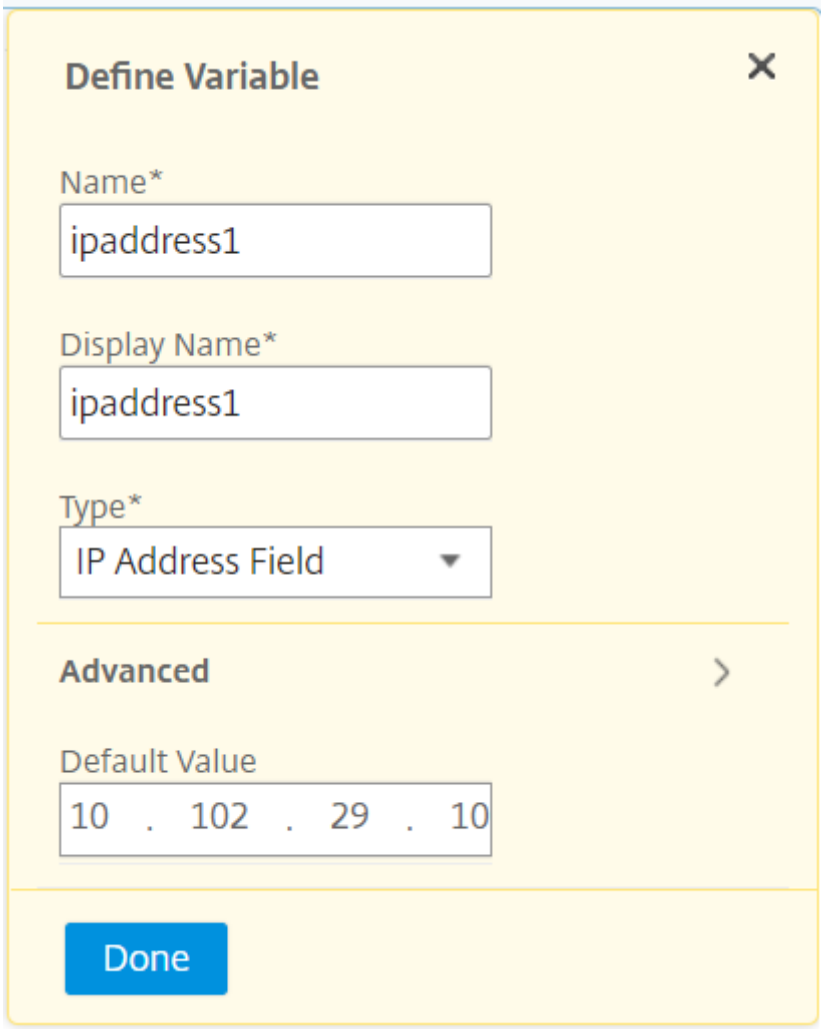
© 1997–2025 Citrix Systems, Inc. All rights reserved.

3. In the **Configuration Editor** page, type in your commands and save the commands as a configuration template. You can also drag an existing template from the left pane to the editor.
4. Select the values that you want to convert to a variable, and then click **Convert to Variable**. For example, select the IP address of the load balancing server ”ipaddress1,”and click **Convert to Variable**. The variable is now enclosed with “$”.

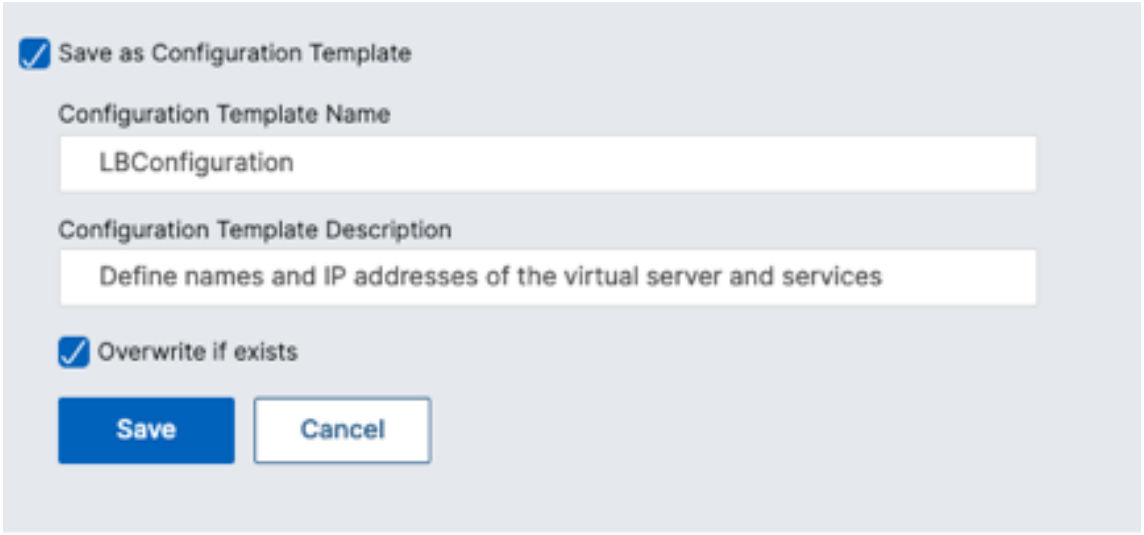


In the **Define Variable** window, set the properties for this variable - name, display name, and the type of the variable. Click the **Advanced** option if you want to further specify a default value for your variable.

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



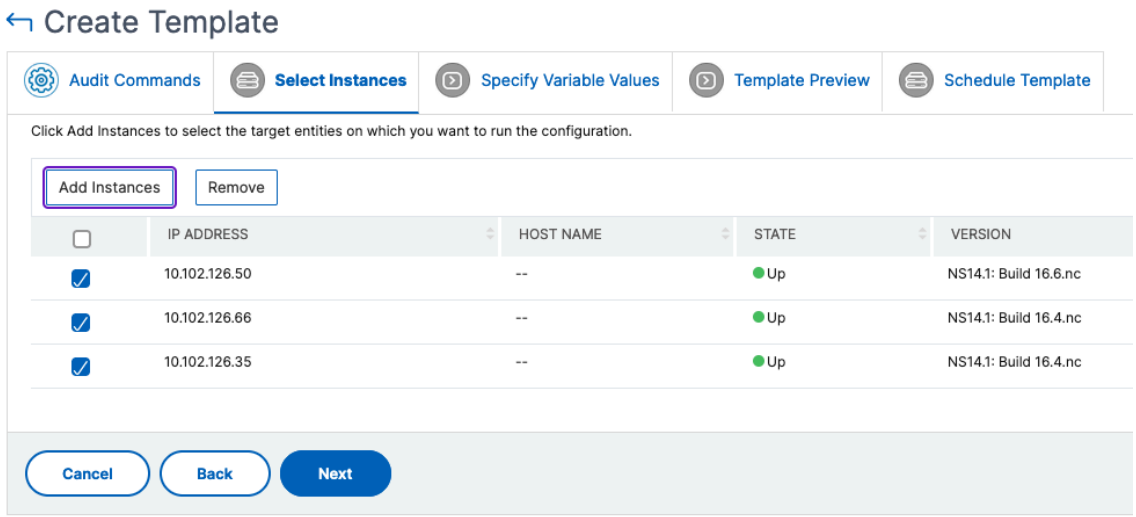
You can also save the commands as a configuration template.



5. Click **Save** and then, click **Next**.

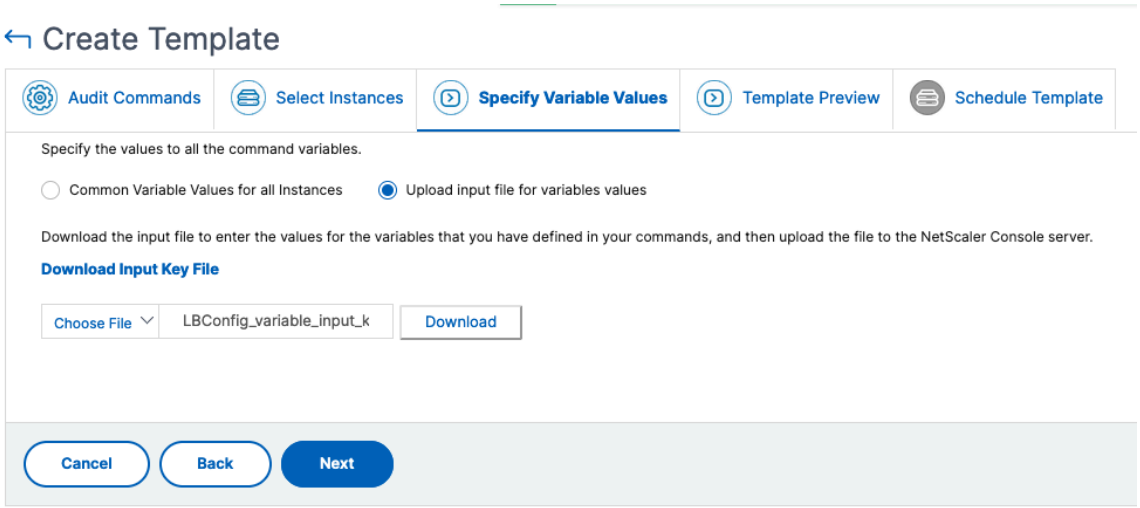
© 1997–2025 Citrix Systems, Inc. All rights reserved.

6. In the **Select Instances** tab, select the instances you want to run the configuration audit on and click **Next**.



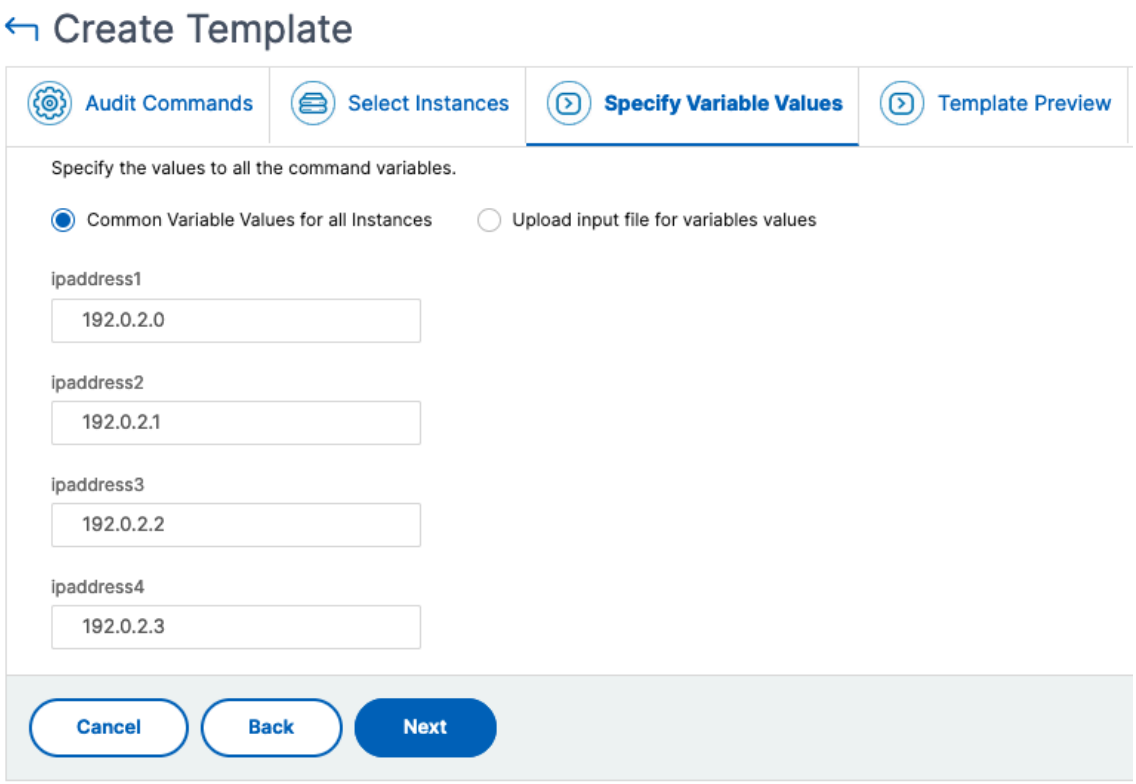
7. In the **Specify Variable Values** tab, you have two options:

   a) Download the input file to enter the values for the variables that you have defined in your commands. After entering the variables, upload the file to the NetScaler Console server.



   a) Enter common values for the variables that you have defined for all instances.

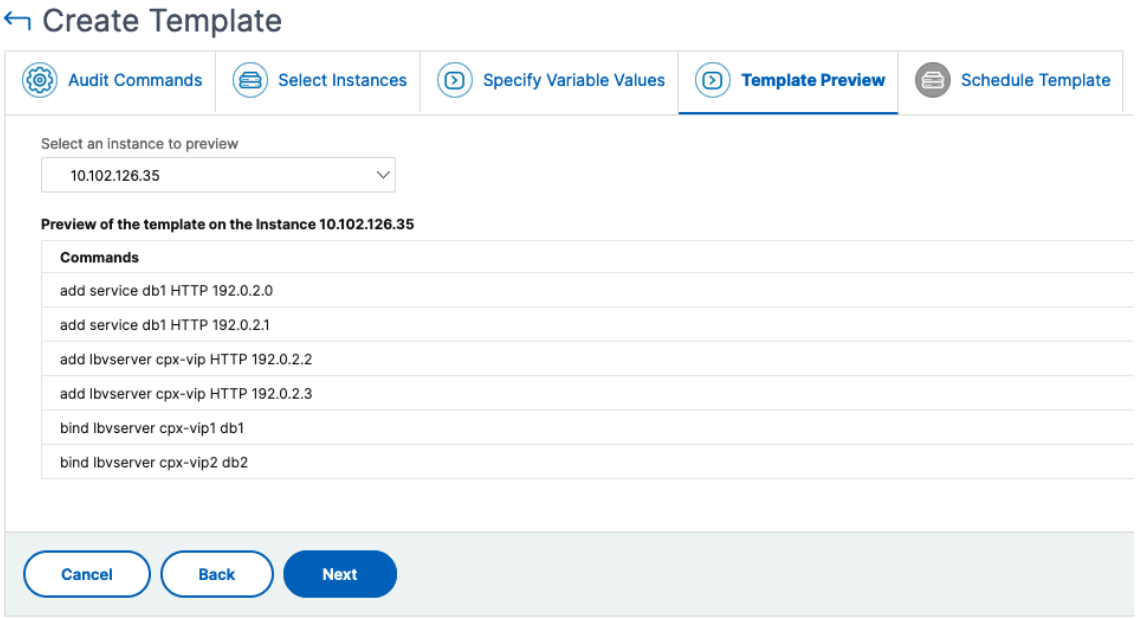
© 1997–2025 Citrix Systems, Inc. All rights reserved.



> **Note:**
>
> If you want to audit each instance with different values, you must create separate variables in the input file for each instance.

8. Click **Next**.
9. In the **Template Preview** tab, you can evaluate and verify the commands to be run on each instance or instance group. Click **Next**.

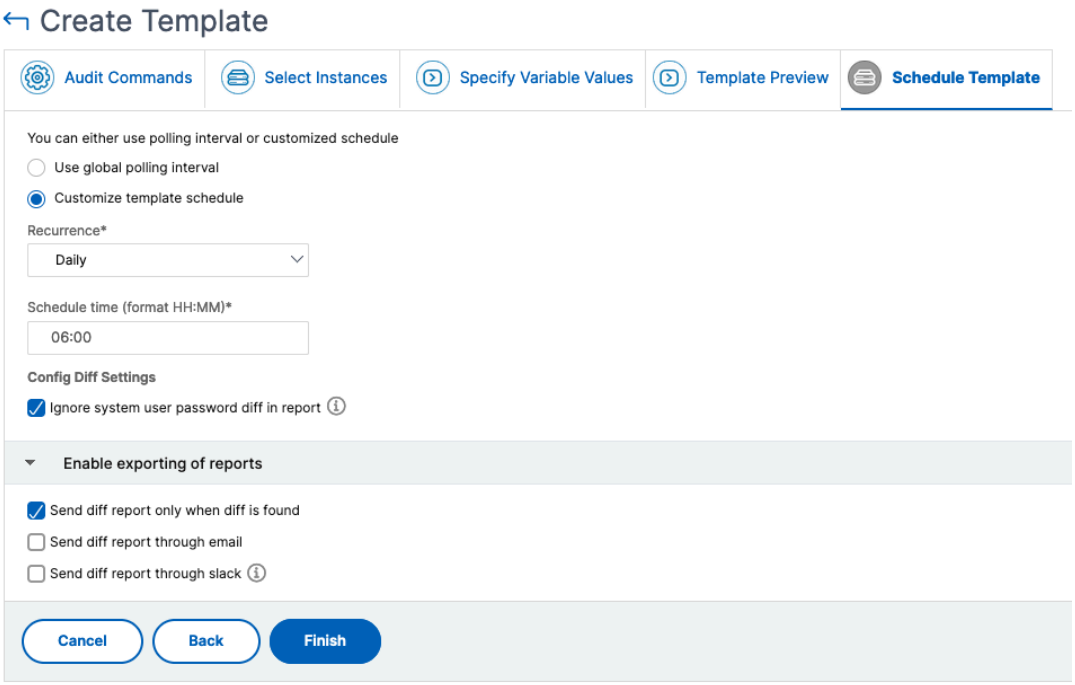
© 1997–2025 Citrix Systems, Inc. All rights reserved.



10. In the **Schedule Template** tab, you have the following options to schedule the running of the template and configuring the mail address to send the diff report.

    - **Use global polling interval**. Select this option to run the template on the instances at a time configured globally on NetScaler Console.
    - **Customize template schedule**. Use this option to configure the time and the frequency at which the templates must be run.
        - Specify the frequency and the timing for the execution of the audit templates.
    - **Enable exporting of reports**. Use this option to:
        - **Send diff report only diff is found**
        - **Send diff report through email**. Configure the mail profile to which the diff report must be sent as a mail attachment.
        - **Send diff report through slack**. Configure the Slack channel to which the diff report must be sent as a notification.

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



11. Click **Finish**.

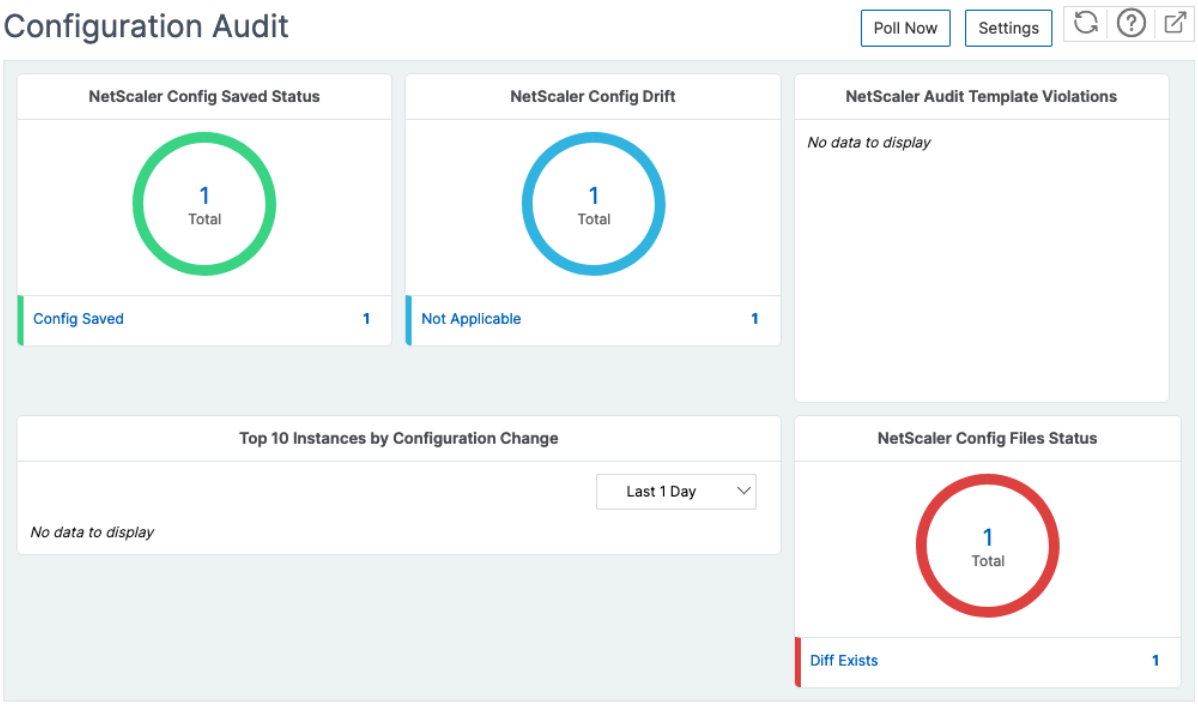
The audit template appears in the **Audit Templates** list and is run at the scheduled time against the configurations in the specified instances.

View configuration changes

You can also use the **Configuration Audit** dashboard to view high-level details about configuration changes such as:

- The top 10 instances by configuration change
- The number of saved and unsaved configurations
- The file added, removed, or modified in the `nsconfig` folder

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

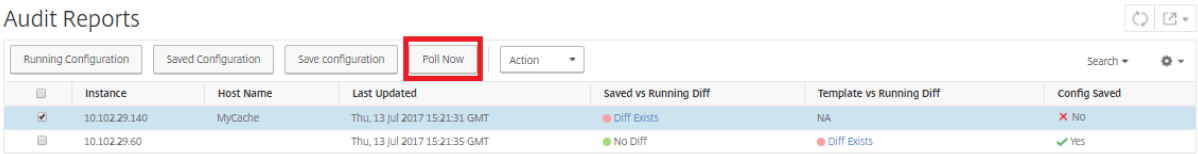


NetScaler Console also allows you to poll configuration audits manually and adds all the configuration audits of the instances immediately to the NetScaler Console. To do so, navigate to **Infrastructure > Configuration > Configuration Audit**, click **Poll Now,** the pop-up page **Poll Now** provides you an option to poll all NetScaler instances in the network, or poll the selected instances.

You can also force an audit on an instance. To do so, click any of the following charts:

- **NetScaler Config Saved Status**
- **NetScaler Config Drift**

On the **Audit Reports** page, select the instance and, in the **Action** list, select **Poll Now**.



The **NetScaler Config File Status** chart provides you the status of the NetScaler files present in the `nsconfig` folder. The NetScaler Console records and compares changes in files within the `nsconfig` folder and displays the differences. See, View the file status audit reports.

Set configuration audit notifications

1. Navigate to **Infrastructure > Configuration > Configuration Audit**.
2. In the **Configuration Audit** page, click **Settings**.

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

3. In the **Notification Settings** page, click the **Edit** icon to enable the notification settings.
4. Select the **Enabled** checkbox. Choose an email distribution list from the drop-down list. You can also create an email distribution list by clicking the **+** icon and specifying email server details.

Get configuration advice on network configuration

September 27, 2025

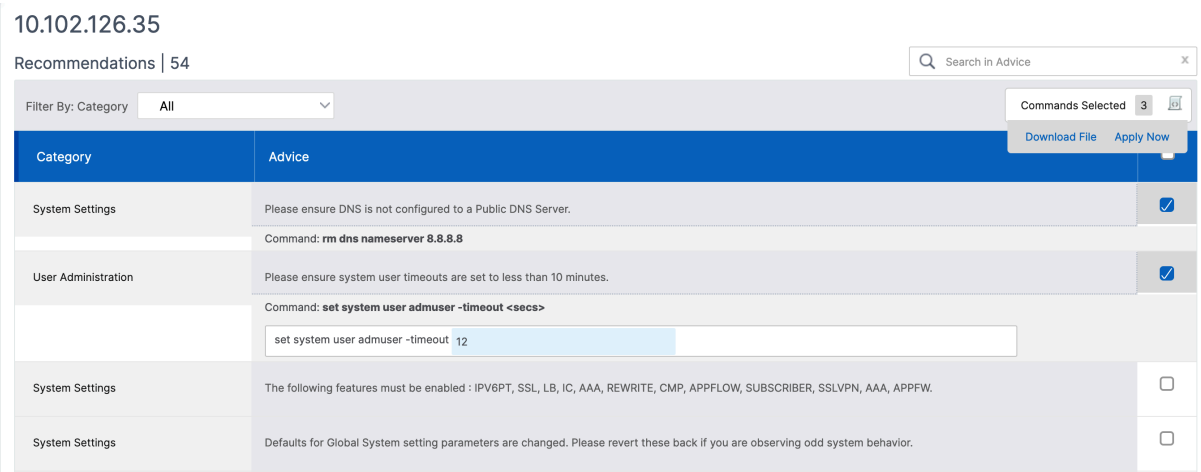
You set up your NetScaler instances with optimal configurations so that you can achieve optimal performance on your applications. However, some configurations might not be standard configurations, which might affect your applications' performance.

To help you optimize your application performance, NetScaler Console analyzes the NetScaler instance configuration and provides you with recommendations. You can apply the recommended configurations from NetScaler Console.

To analyze the NetScaler instance:

1. Navigate to **Infrastructure > Configuration > Configuration Audit > Configuration Advice**.
2. Do one of the following:
   - Click **Upload Configuration File** and upload the configuration file of your network instance.
   - Click **Select Device** and select the NetScaler instance that you want to analyze.

NetScaler Console analyzes the configuration on your instance and provides a list of configuration recommendations as shown in the following image. Click the checkbox next to a configuration advice to view the corrective commands.

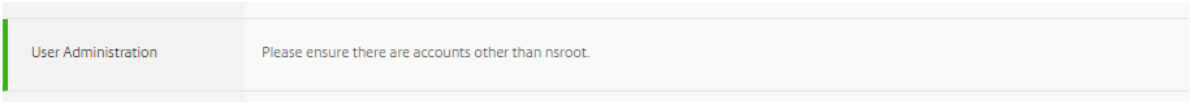


If you want to update your configuration, specify the values for the variables in the corrective commands and click **Apply Now**.

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

> **Note:**
>
> The commands listed here are only recommendations. A user with read and write access can edit any command using this feature. Ensure that you grant a limited privileged access to users whom you think must not edit the commands.

When the command is successfully run on the network instance, the checkbox next to the advice disappears.



If you want to view the details of the commands run on your network instance, navigate to **Infrastructure > Instances > <Instance_Type\>**, select the IP address of the instance, and then click **Show Events** from the **Actions** drop-down list.

On the **Events** page, view the details of the configuration change.

Poll configuration audit of NetScaler® instances

September 27, 2025

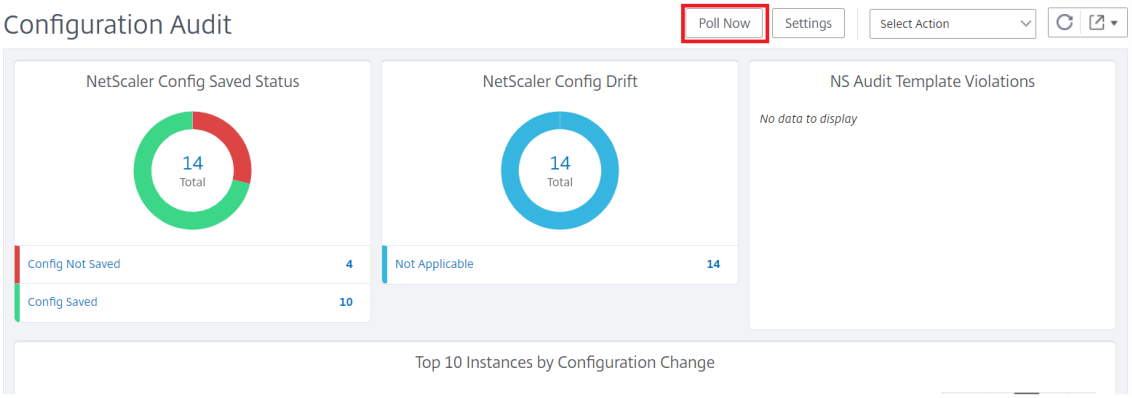
NetScaler Console automatically polls the configuration audits every 10 hours to look for configuration changes that occur on NetScaler instances. You can also manually poll the configuration audits to discover recent changes, but polling all the NetScaler instances configuration places a heavy load on the network.

Instead of polling the entire NetScaler instance configuration audit, you can manually poll only the configuration audits of a selected instance or instances.

To poll configuration audits of NetScaler instances:

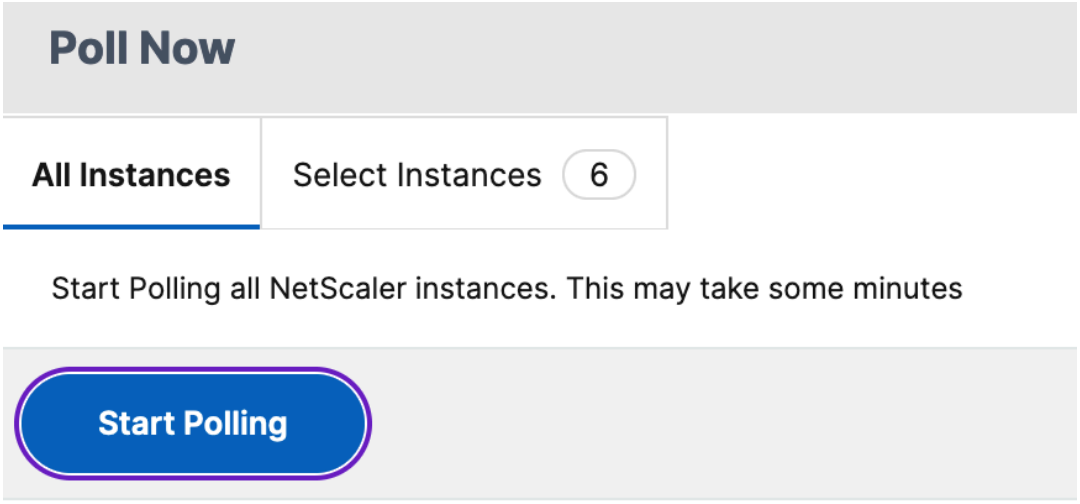
1. In NetScaler Console, navigate to **Infrastructure > Configuration > Configuration Audit**.
2. In **Configuration Audit**, click **Poll Now**.

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

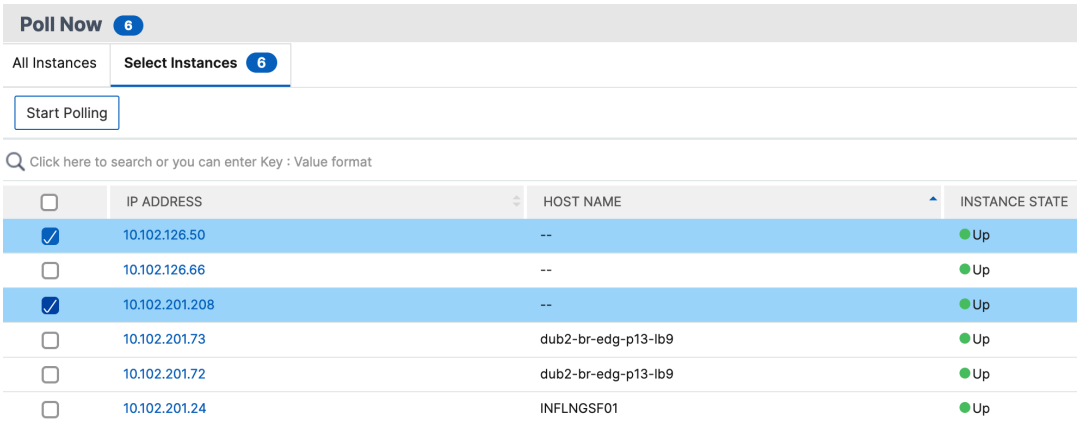


3. The **Poll Now** page pops up, giving you the option to poll all NetScaler instances in the network or poll selected instances.

   a) To poll all NetScaler instances, select the **All Instances** tab and click **Start Polling**.



   b) To poll specific instances, select the **Select Instances** tab, select the instances from the list, and click **Poll Now**.



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

Generate configuration audit diff for ConfigChange SNMP Traps

September 27, 2025

Whenever there is a configuration change in a NetScaler instance in the network, the configuration file is updated. The instance sends a ConfigChange SNMP trap to NetScaler Console. You can enable NetScaler Console to do a configuration audit on that instance when the instance sends a ConfigChange SNMP trap.

If there is a difference between the audit template configuration and the running configuration, a Diff Exists status message appears on the **Audit Report** page. Click the **Diff Exists** link takes to go to the **Configuration Diff** page, where you can view the corrective command. You can use these corrective commands to create a configuration job and run that on the specific NetScaler instances. When you run the configuration job, the instances are brought back to the desired configuration.

For more information on how to create configuration jobs from corrective commands, see How to Create Configuration Jobs from Corrective Commands on NetScaler Console.

To run configuration audit templates on receiving ConfigChange SNMP trap:

NetScaler Console allows you to enable the option to run the configuration audit template in NetScaler Console.

1. In NetScaler Console, navigate to **Infrastructure > Configuration > Configuration Audit**.
2. Click **Settings** on the **Configuration Audit** page.
3. Select **Perform Audit on recieving "netScalerConfigChange"event**.

> **Note:**
>
> NetScaler Console performs a configuration audit for every instance that receives the netScalerConfigChange SNMP traps in the future.

1. In the **Time delay to run the Audit Template** (in minutes) field, type the minutes. NetScaler Console runs the configuration audit template on the NetScaler instance after this time delay when it receives the ConfigChange SNMP trap by that instance.

Configuration audit

September 27, 2025

This document includes topics on how to:

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

- View audit reports
- Audit configuration changes across instances
- Get configuration advice on network configuration
- Poll configuration audit of NetScaler instances
- Generate configuration audit diff for ConfigChange SNMP traps

Upgrade jobs

November 30, 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.

You can create the following maintenance tasks using NetScaler Console. You can then schedule the maintenance tasks at a specific date and time.

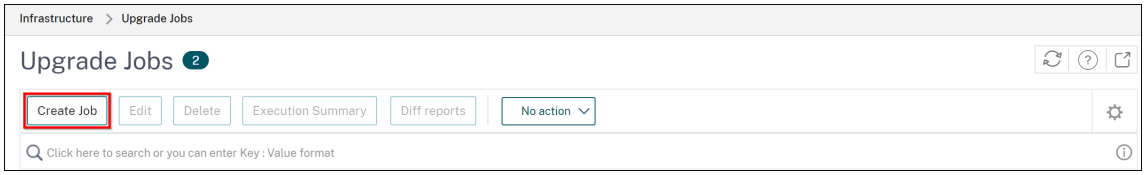
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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

> **Notes:**
>
> - If an upgrade job fails, NetScaler Console removes the build files and other extracted files to ensure that NetScaler instances have sufficient disk space for the next upgrade attempt.
> - While you can select any number of NetScaler instances for upgrade, NetScaler Console on-prem supports a maximum of 10 concurrent upgrade threads. This means that only 10 instances can be upgraded simultaneously.

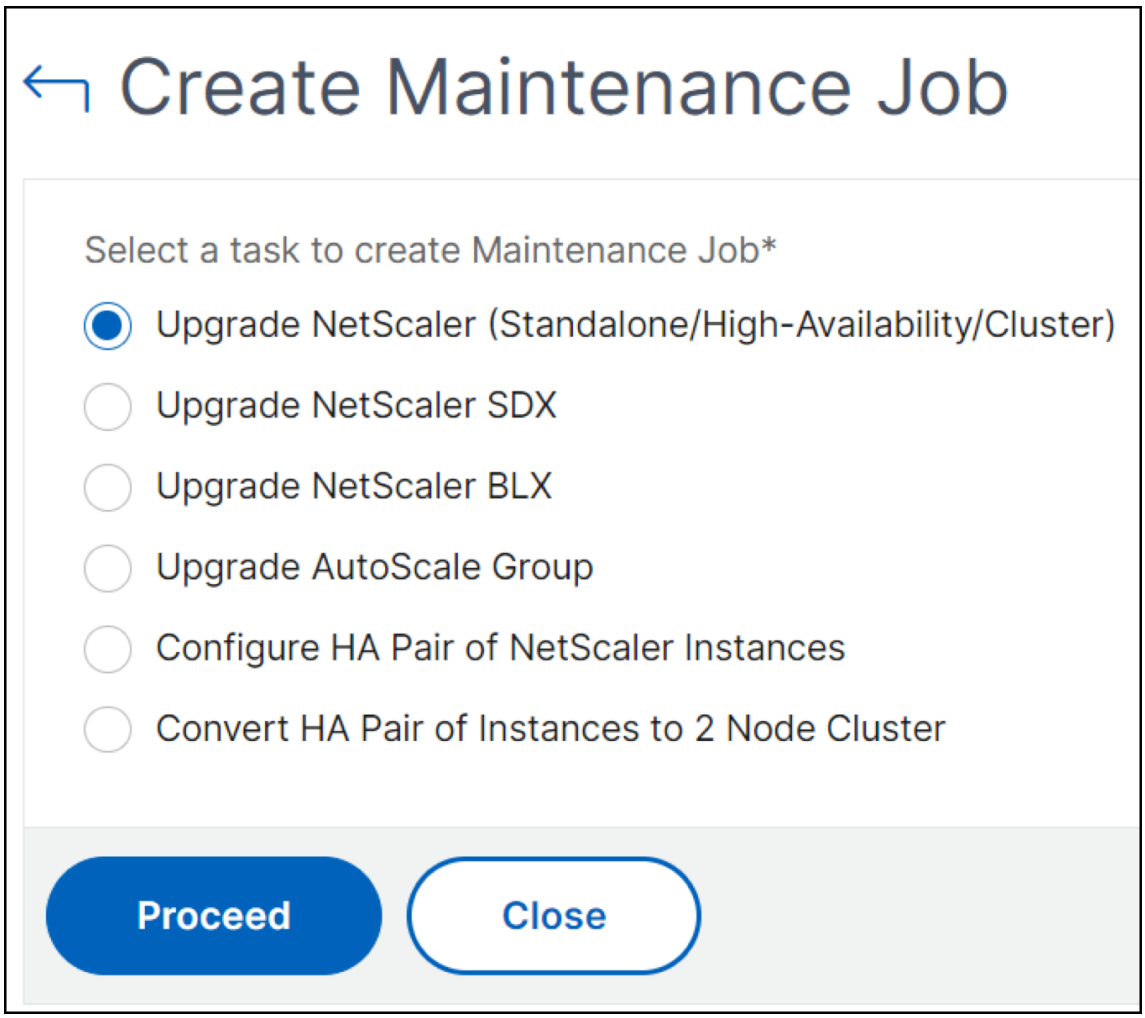
Schedule upgrading of NetScaler instances

1. Navigate to **Infrastructure > Upgrade Jobs**. Click **Create Job**.

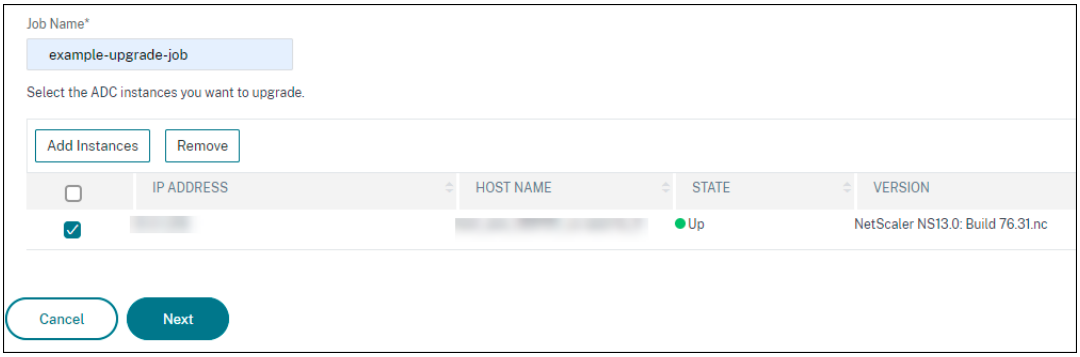


2. In **Create Maintenance Jobs**, select **Upgrade NetScaler (Standalone/High-Availability/Cluster)** and click **Proceed**.

© 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. Select one of the following options from the **Software Image**

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

list:

- **Local** - Select the instance upgrade file from your local machine.
- **Appliance** - Select the instance upgrade file from 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.

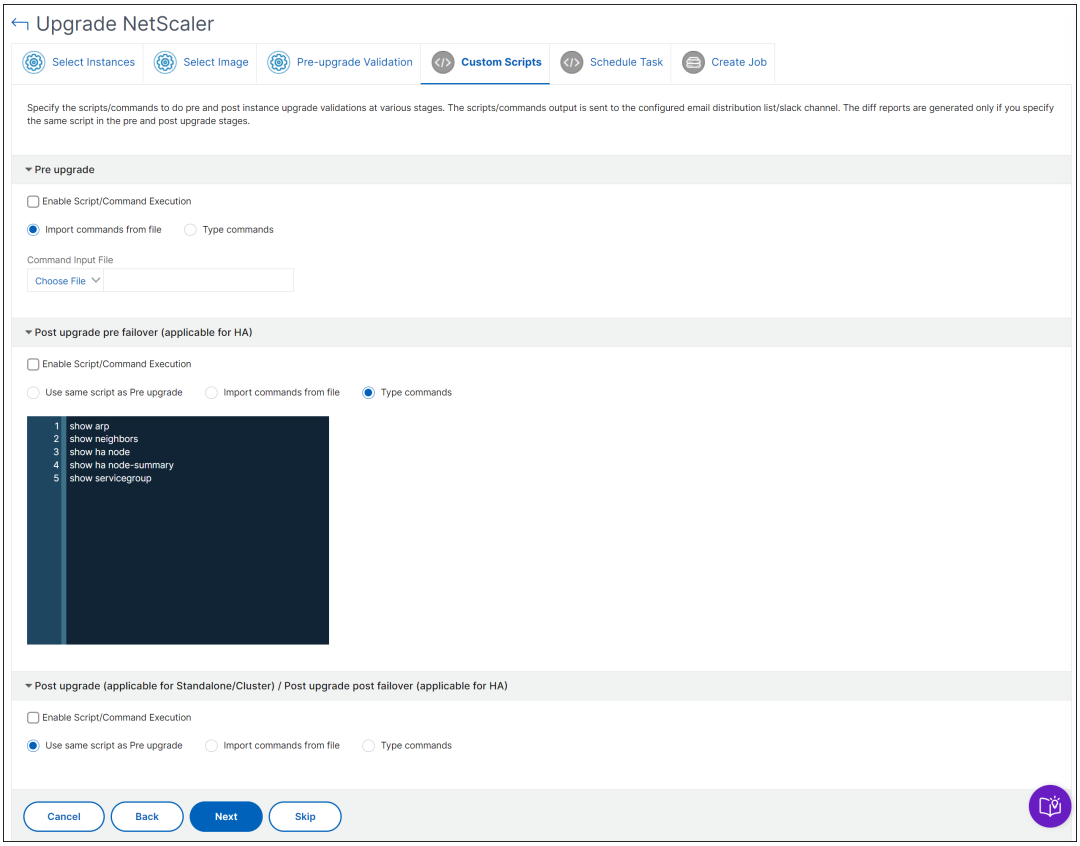
6. Click **Next** to start the pre-upgrade validation on the selected instances.

   The **Pre-upgrade validation** tab displays the failed instances. Remove the failed instances and click **Next**.

   > **Important**
   >
   > If you specify cluster IP address, NetScaler Console does pre-upgrade validation only on the specified instance not on the other cluster nodes.

7. Optional, in **Custom scripts**, specify the scripts to run before and after an instance upgrade. Use one of the following ways to run the commands:
   - **Import commands from file** - Select the command input file from your local computer.
   - **Type commands** - Enter commands directly on the GUI.

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



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**.

     Specify the **Execution Date** and **Start Time** when you want to upgrade another instance in the HA pair.

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

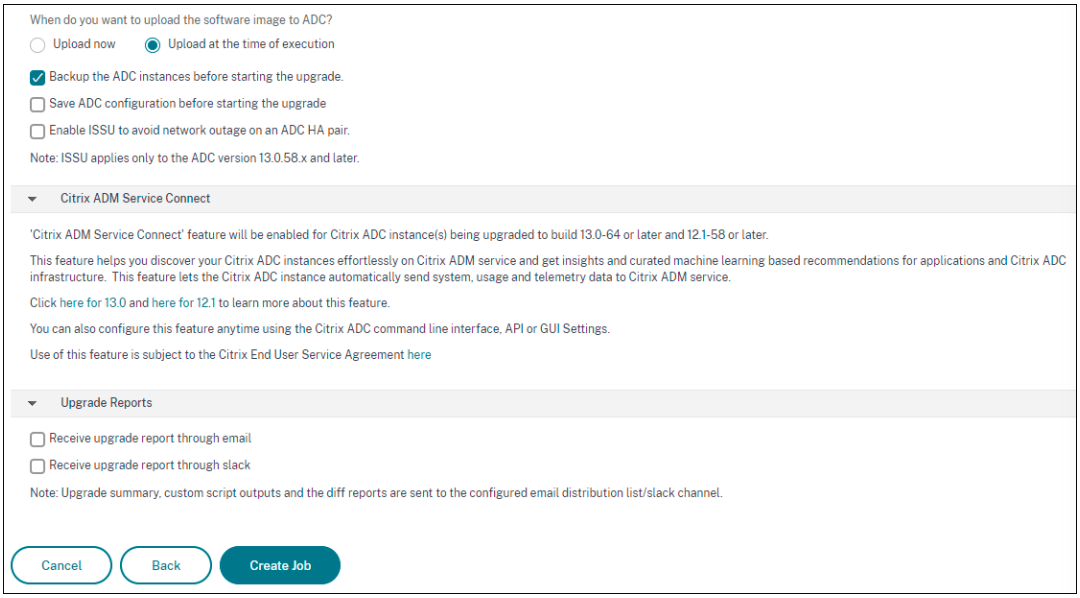
9. Click **Next**. In **Create Job**, specify the following details:

    a) Specify when you want to upload the image to an instance:

    - **Upload now** - Select this option to upload the image immediately. However, the upgrade job runs at the scheduled time.
    - **Upload at the time of execution** - Select this option to upload the image at the time of upgrade job execution.
    - **Backup the NetScaler instances before starting the upgrade.** - Creates a backup of the selected NetScaler instances.
    - **Saves NetScaler Configuration before starting the upgrade** - Saves the configuration jobs that are configured on the instance before the upgrade.
    - **Enable ISSU to avoid network outage on NetScaler HA pair** - Enabling In-Service Software Upgrade (ISSU) allows you to upgrade a NetScaler high-availability (HA) pair without causing network downtime. ISSU ensures that the existing connections are honoured during the upgrade by migrating the active sessions seamlessly between the nodes. After enabling ISSU in the upgrade workflow, the system can also trigger ISSU migration completion after the delay time defined by the customer. NetScaler Console triggering a complete ISSU migration completion ensures that the upgrade completes even if connections persist. Specify the ISSU migration timeout in minutes to set the wait time before NetScaler Console completes the migration.

- **NetScaler Console Service Connect** - If you are upgrading to build **13.0-64 or later** and **12.1-58 or later**, NetScaler Console Service 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. 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 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**
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** checkbox and **Receive Execution Report through slack** checkbox to enable the notifications.

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

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. 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. 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 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.

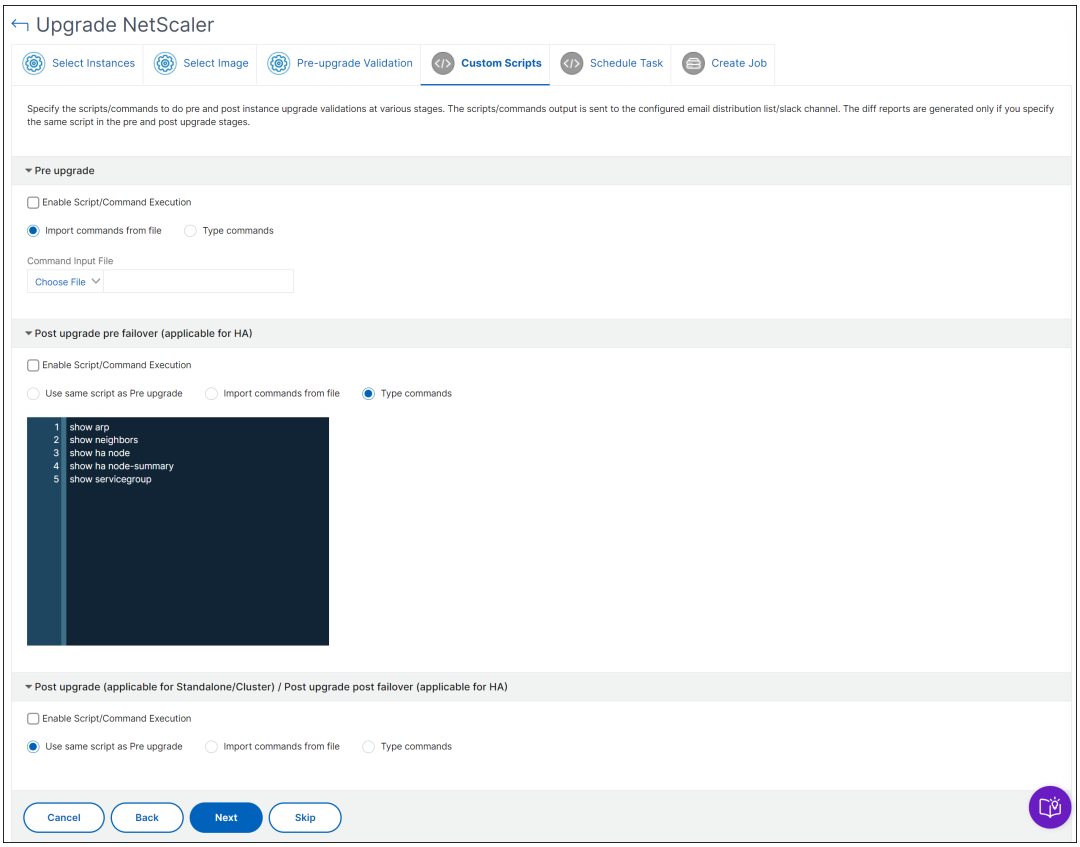
   The **Pre-upgrade validation** tab displays the failed instances. Remove the failed instances and click **Next**.

   > **Important**
   >
   > If you specify cluster IP address, NetScaler Console does pre-upgrade validation only on the specified instance not on the other cluster nodes.

7. Optional, in **Custom scripts**, specify the scripts to run before and after an instance upgrade. Use one of the following ways to run the commands:
    - **Import commands from file** - Select the command input file from your local computer.

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

- **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**.

     Specify the **Execution Date** and **Start Time** when you want to upgrade another instance in the HA pair.

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

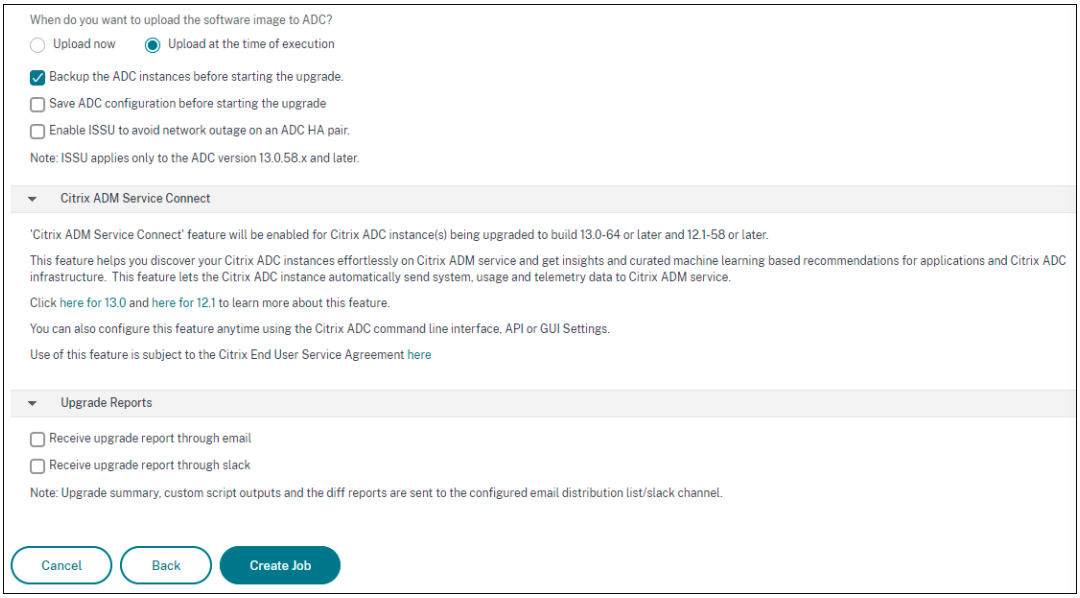
9. Click **Next**. In **Create Job**, specify the following details:

    a) Specify when you want to upload the image to an instance:

    - **Upload now** - Select this option to upload the image immediately. However, the upgrade job runs at the scheduled time.
    - **Upload at the time of execution** - Select this option to upload the image at the time of upgrade job execution.
    - **Backup the NetScaler instances before starting the upgrade** - Creates a backup of the selected NetScaler instances.
    - **Save NetScaler Configuration before starting the upgrade** - Saves the configuration jobs that are configured on the instance before the upgrade.
    - **Enable ISSU to avoid network outage on NetScaler HA pair** - Enabling In-Service Software Upgrade (ISSU) allows you to upgrade a NetScaler high-availability (HA) pair without causing network downtime. ISSU ensures that the existing connections are honoured during the upgrade by migrating the active sessions seamlessly between the nodes. After enabling ISSU in the upgrade workflow, the system can also trigger ISSU migration completion after the delay time defined by the customer. NetScaler Console triggering a complete ISSU migration completion ensures that the upgrade completes even if connections persist. Specify the ISSU migration timeout in minutes to set the wait time before NetScaler Console completes the migration.

    - **NetScaler Console Service Connect** - If you are upgrading to build **13.0-64 or later** and **12.1-58 or later**, NetScaler Console Service 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 Autoscale™ group

Perform the following steps to upgrade all the instances in the cloud services that are part of the Autoscale group:

1. Navigate to **Infrastructure > Upgrade Jobs**. Click **Create Job**.
2. Select **Upgrade Autoscale Group** and click **Proceed**.
3. In the **Upgrade Settings** tab:
   a) Select the **Autoscale Group** that you want to upgrade.
   b) In **Image**, select the NetScaler version. This image is the existing version of NetScaler instances in the Autoscale group.
   c) In **NetScaler Image**, browse the NetScaler version file to which you want to upgrade.

      If you check **Graceful Upgrade**, the upgrade task waits until the specified drain connection period to expire.
   d) Click **Next**.
4. In the **Schedule Task** tab:
   a) Select one of the following from the Execution Mode list:
      - **Now:** To start the NetScaler instances upgrade immediately.
      - **Later:** To start the NetScaler instances upgrade at later time.

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

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** checkbox and **Receive Execution Report through slack** checkbox to enable the notifications.

5. Click **Finish**.

Schedule configuring HA pair of NetScaler instances

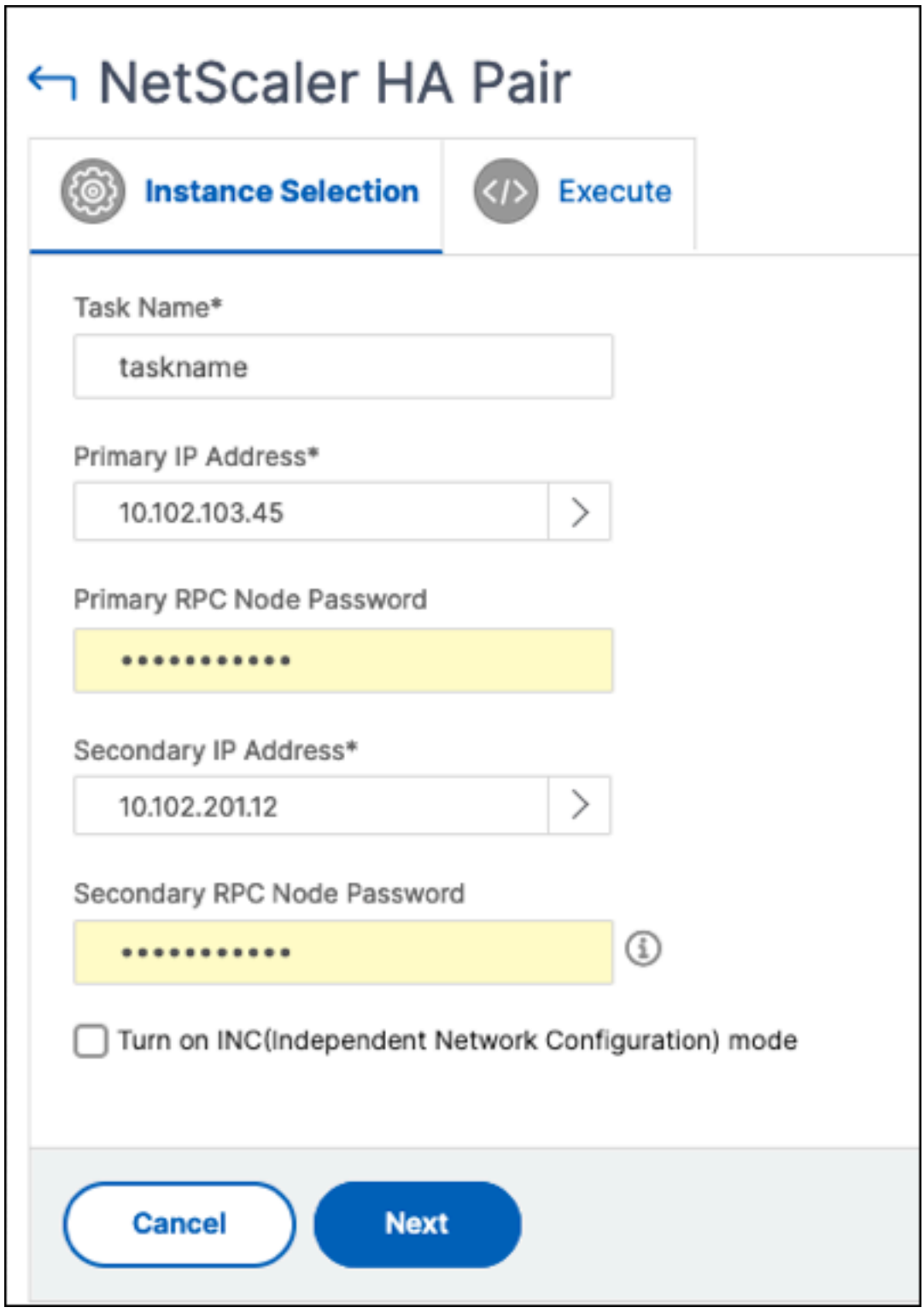
1. Navigate to **Infrastructure > Upgrade Jobs**. Click **Create Job**.
2. Select **Configure HA Pair of NetScaler Instances** and click **Proceed**.
3. On the **NetScaler HA Pair** page, in the **Instance Selection** tab:
   a) Add a **Task Name**.
   b) Select the primary IP address. Click **OK**.
   c) Enter the primary RPC node password.
   d) Select the secondary IP address. Click **OK**.

      Note:

      The RPC node password fields are available in NetScaler release 14.1 and later.

   e) Enter the secondary RPC node password.
   f) Click to enable **Turn on INC(Independent Network Configuration) mode** if you have the HA pair instances in two subnets.
   g) Click **Next**.

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



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 a NetScaler HA pair later, select **Later** from the **Execution Mode** list. You can then

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

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** checkbox and **Receive Execution Report through slack** checkbox 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. 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** checkbox and **Receive Execution Report through slack** checkbox 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 27, 2025

You can use NetScaler Console to upgrade one or more NetScaler instances. You must know the licensing framework and types of licenses before you upgrade an instance.

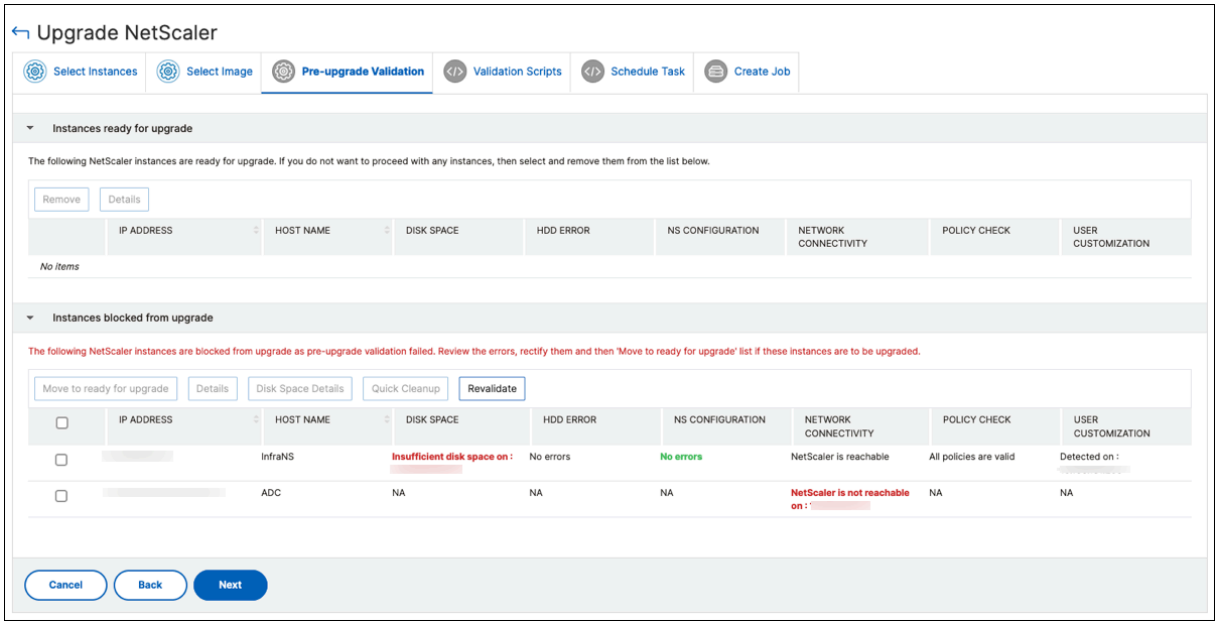
NOTE: If you want to upgrade an instance that has classic policies, we recommend that you convert the classic policies to advanced policies before upgrading the instance, using the NSPEPI tool. This is applicable for the features that are supported by the NSPEPI tool. For more information, see Upgrade considerations for configurations with classic policies.

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

When you upgrade your NetScaler instance by creating a maintenance job, perform the pre-validation check on the instances that you want to upgrade.

Pre-validation checks

1. **Check for customizations** - Back up your customizations and delete them from the instances. You can reapply the backed-up customizations after the instance upgrade.
2. **Check the disk usage** - If the `/var` folder has less than 6 GB space and the `/flash` folder has less than 200 MB space, clean up the disk space. Check the following folder paths to clean the disk space:
   - `/var/nstrace`
   - `/var/log`
   - `/var/nslog`
   - `/var/tmp/support`
   - `/var/core`
   - `/var/crash`
   - `/var/nsinstall`
   - `/var/netscaler/nsbackup`
3. **Check for disk hardware issues** - Resolve the hardware issues if any.
4. **Check for STAYPRIMARY and STAYSECONDARY nodes** - For a NetScaler HA, the upgrade is blocked for the nodes in STAYPRIMARY and STAYSECONDARY states. These nodes are identified in the pre-validation check and listed under **Instances blocked from upgrade**.



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

NetScaler high-availability pair

When you upgrade a NetScaler HA pair, note the following:

- The secondary node is upgraded first.
- Synchronization and propagation of the nodes are disabled until both nodes are upgraded successfully.
- After the successful HA pair upgrade, an error message appears in the execution history. This message appears if your nodes in the HA pair are on different builds or versions. This message indicates that synchronization between primary and secondary node is disabled.

You can upgrade a NetScaler HA pair in two stages:

1. Create an upgrade job and run on one of the nodes immediately or schedule it later.
2. Schedule the upgrade job to run on the remaining node later. Ensure to schedule this job after the initial node's upgrade.

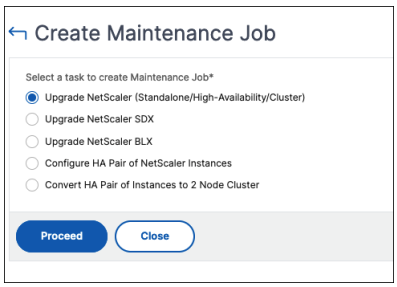
NetScaler clusters

When you upgrade a NetScaler cluster, the NetScaler Console does pre-upgrade validation on the specified instance only. Before you upgrade, check and resolve customization, disk usage, and hardware issues on the cluster nodes.

Create an upgrade maintenance job to upgrade NetScaler instances

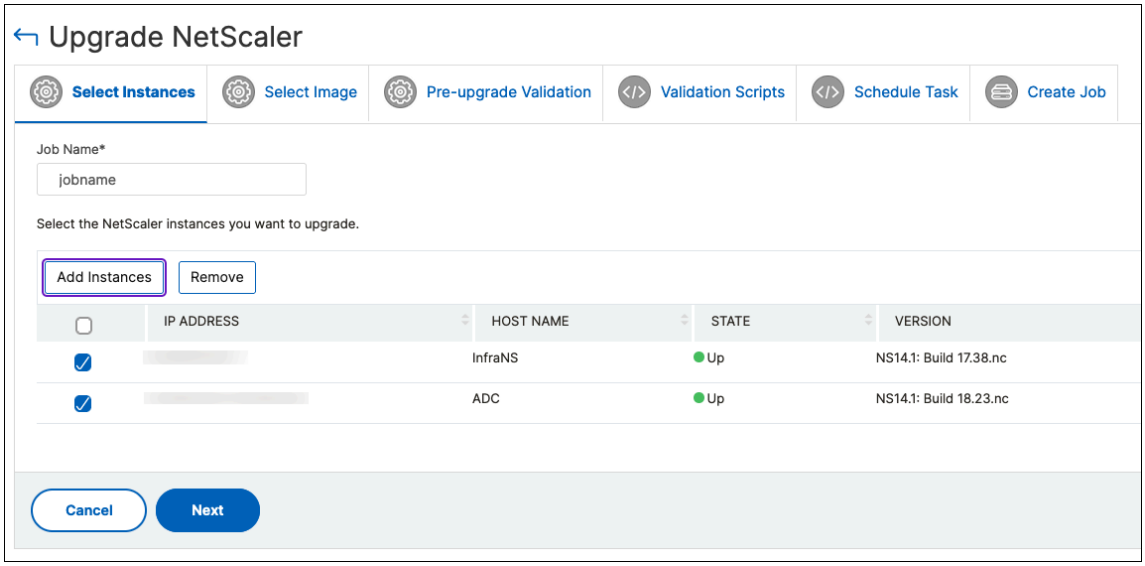
> **Note**
>
> NetScaler upgrade from a higher version to a lower version is not supported. For example, if your NetScaler instance is 13.0 82.x, you cannot downgrade the NetScaler instance to 13.0 79.x or any other earlier versions.

1. In NetScaler Console, navigate to **Infrastructure > Upgrade Jobs**. Click the **Create Job** button.
2. In **Create Maintenance Jobs**, select **Upgrade NetScaler (Standalone/High-Availability/Cluster)** and click **Proceed**.

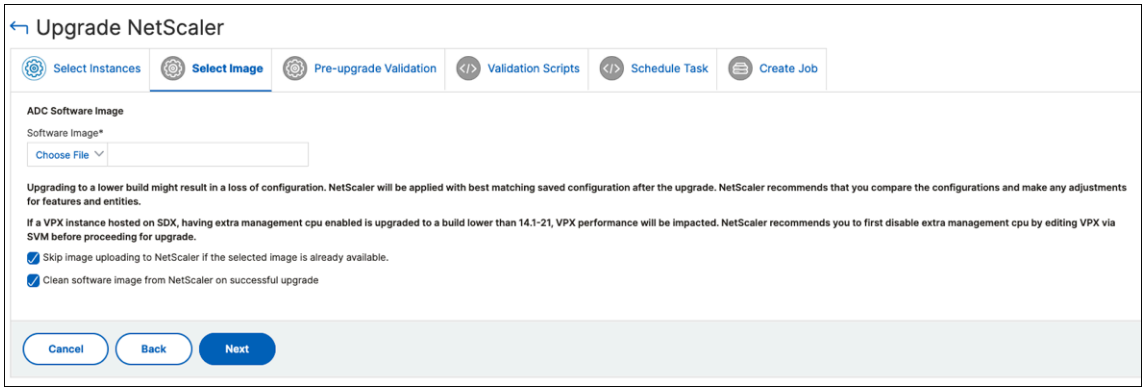


© 1997–2025 Citrix Systems, Inc. All rights reserved.

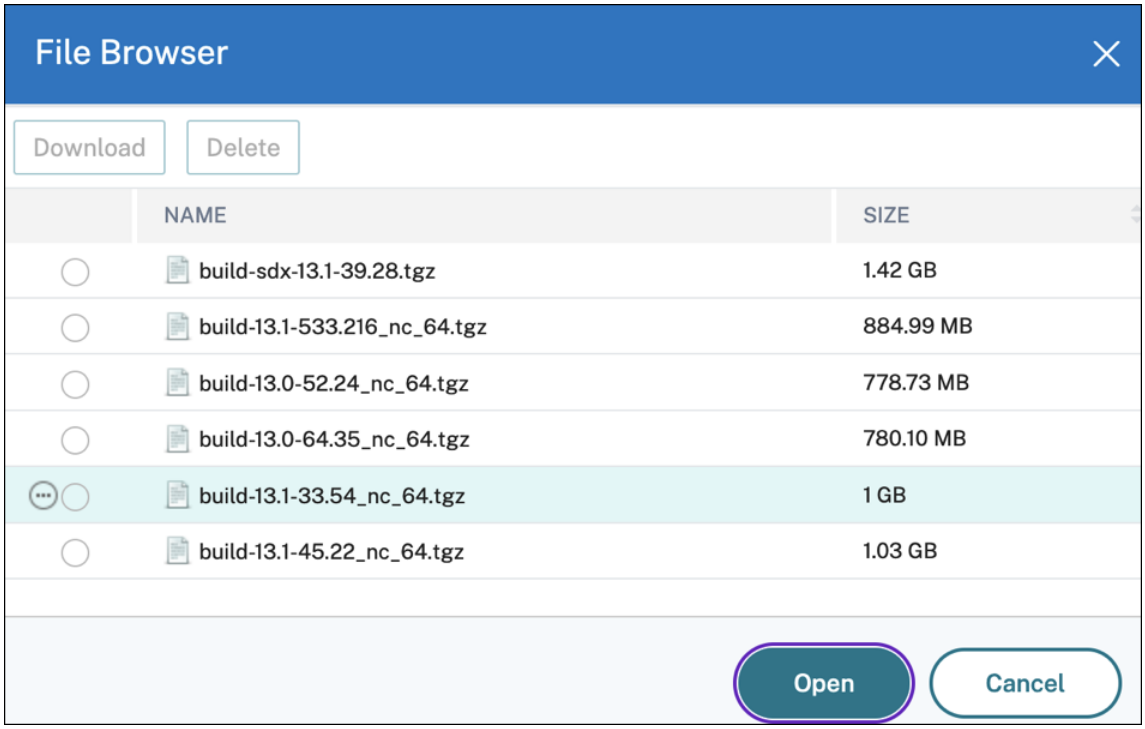
3. In **Select Instance**, type a name of your choice for **Job Name**.
4. Click **Add Instances** to add NetScaler instances that you want to upgrade.
   - To upgrade a NetScaler high-availability pair, select the IP addresses of the high-availability pair (denoted by the superscript of 'S'and 'P').
   - To upgrade a cluster, select the cluster IP address (denoted by the superscript of 'C').



5. In the **Select Image** tab, select an NetScaler image from your local drive or the build images.
   - **Local** - Select the instance upgrade file from your local machine.
   - **Appliance** - Select the instance upgrade file from a NetScaler Console file browser. The NetScaler Console GUI displays the instance files that are present at `/var/mps/ns_images`.



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



- **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.

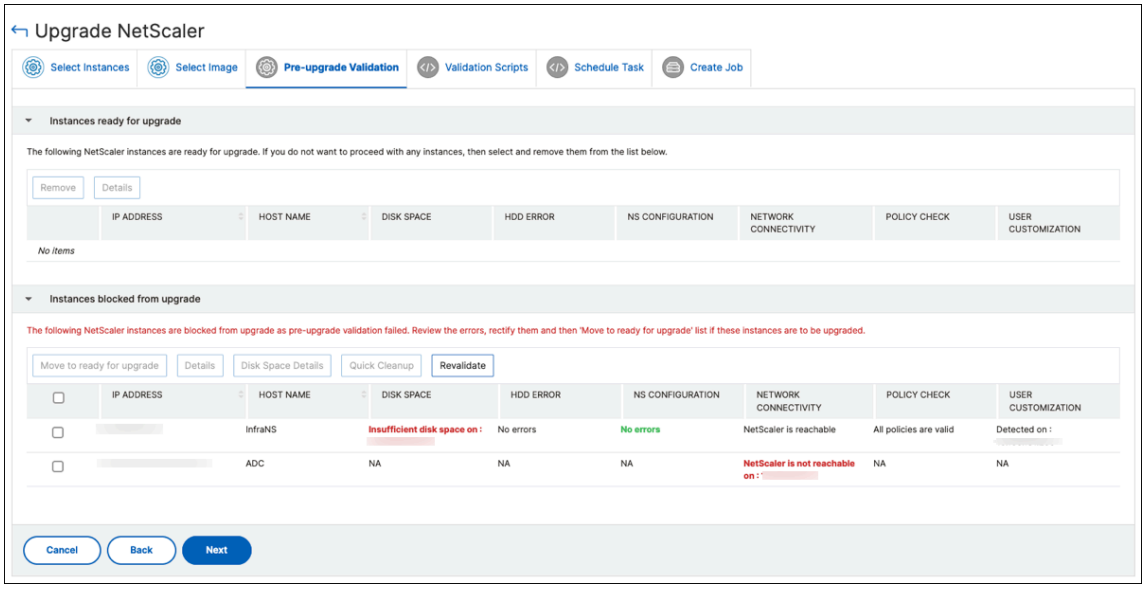
Click **Next** to start the pre-upgrade validation on the selected instances.

> **Note:**
>
> - The downloaded NetScaler images are stored in the NetScaler Console 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 NetScaler Console agent at a time.

6. 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.

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

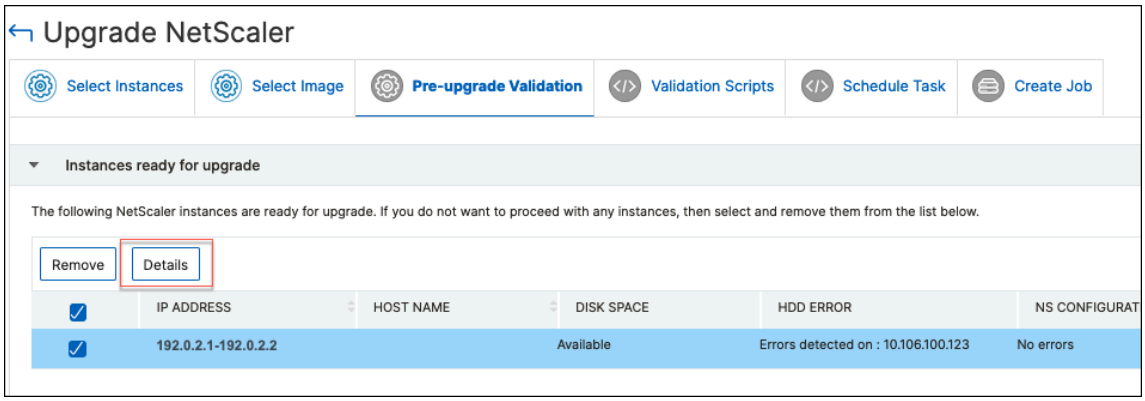
You can review, rectify the errors, and then click **Move to ready for upgrade** to upgrade them. If you face insufficient disk space on an instance, you can check and clean up the disk space. See, Clean up NetScaler disk space.



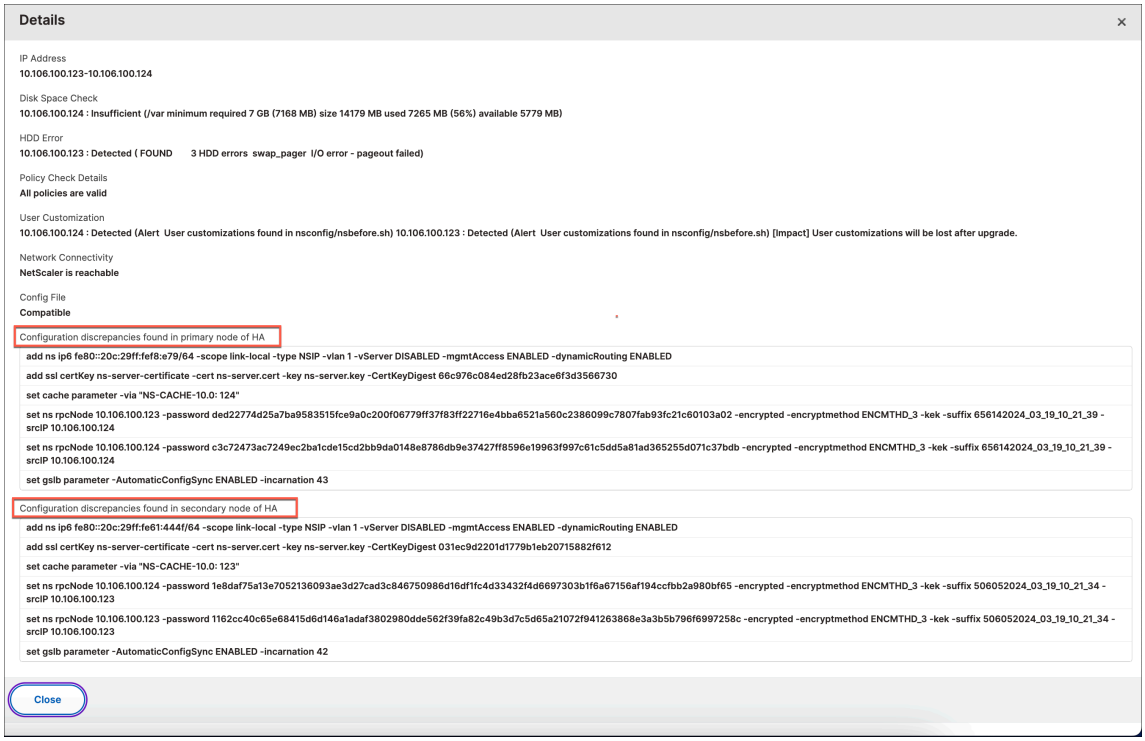
- **Policy Check**: If NetScaler Console finds unsupported classic policies, you can remove such policies to create an upgrade job.

> **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.

To view discrepancies between primary and secondary nodes during an upgrade, select the high-availability node, and click **Details**.



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



- **Configuration discrepancies found in primary node of HA** - Displays all the configurations found in the secondary node of the NetScaler high-availability pair but missing in the primary node.
- **Configuration discrepancies found in secondary node of HA** - Displays all the configurations found in the primary node of the NetScaler high-availability pair but missing in the secondary node.

> **Note:**
>
> You can ignore the following discrepancies that may appear in the configuration discrepancies sections:
>
> - Device-specific configurations like IP addresses.
> - Encrypted passwords or certificates, which may differ between nodes, even if the password is the same.
>
> You can review the discrepancies and choose to ignore them if they are not relevant.

7. In **Validation Scripts**, specify the scripts to run before and after an instance upgrade. You can do either of the following:

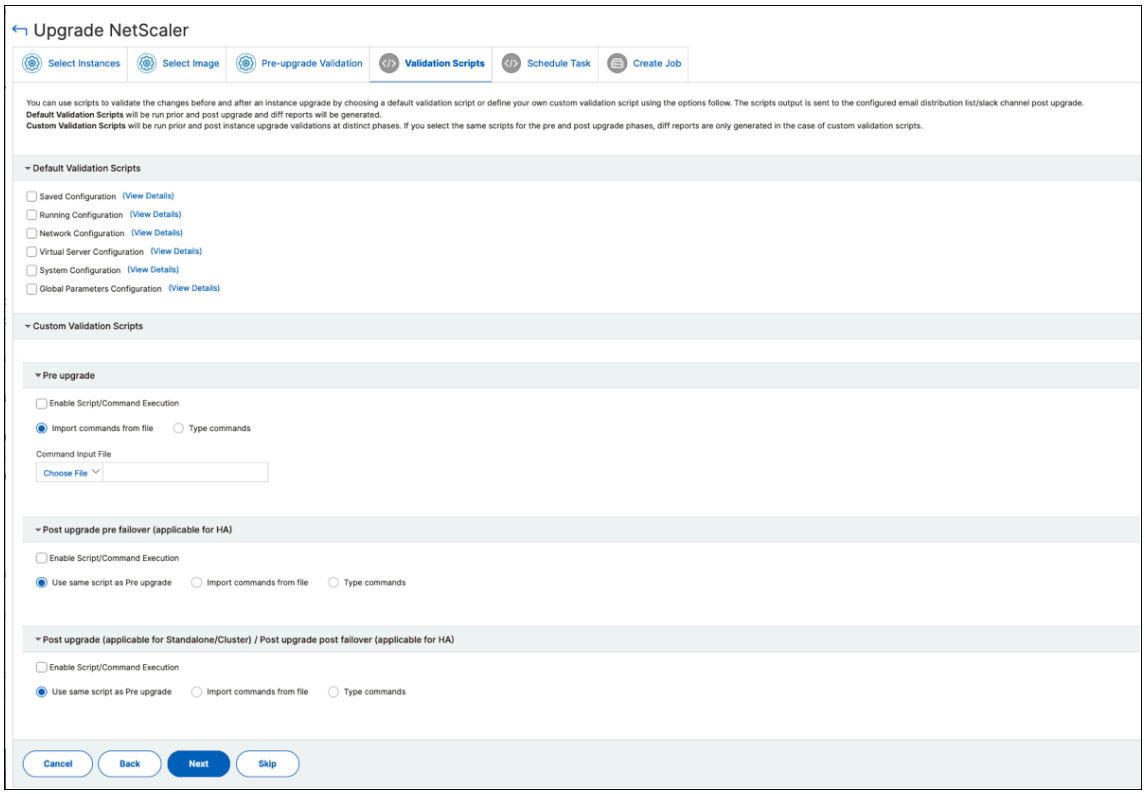
   - **Default Validation Scripts** - Choose this option to run the predefined validation scripts. These scripts are run both before and after the upgrade job, generating a difference report for the validation script.

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

> **Note:**
>
> You cannot change or edit this predefined set of commands.

- **Custom Validation Scripts** - Choose this option to run your validation script. You can specify if you want the scripts to be run before or after the upgrade. A diff report is generated only if the same scripts are selected before and after the upgrade.

To know the set of commands in each configuration, click **View Details**.



In **Custom Validation scripts**, specify the scripts to run before and after an instance upgrade. Use one of the following ways to run the NetScaler CLI commands:

The custom scripts are used to check the changes before and after an 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.

An instance upgrade has multiple stages. You can now specify these scripts to run in the following stages:

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

- **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 execution at the required stages. Otherwise, the specified scripts do not run.

You can import a script file or type NetScaler CLI commands directly in the NetScaler Console GUI.

- **Use same script as Pre upgrade**: Use the same custom script for pre-upgrade, pre-failover, and post-upgrade.
- **Import commands from file**: Select the NetScaler CLI command input file from your local computer.
- **Type commands**: Enter the NetScaler CLI commands directly on the GUI.

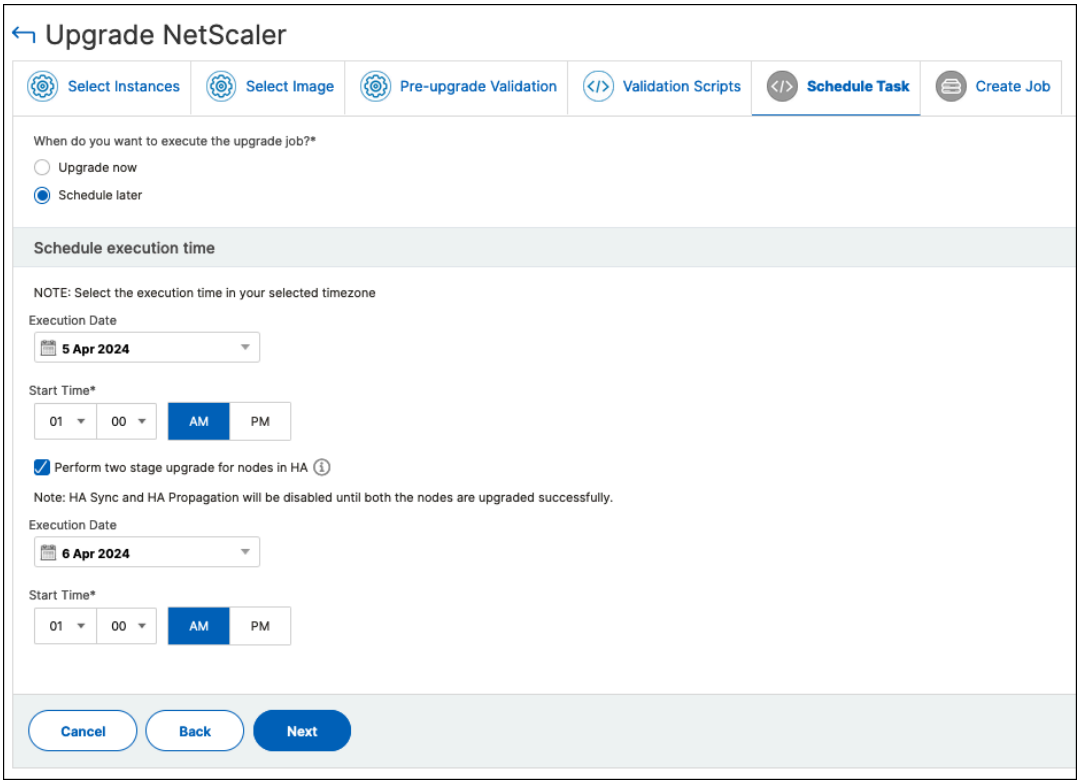
8. In **Schedule Task**, select one of the following options:

   - **Upgrade now** - The upgrade job runs immediately.
   - **Schedule Later** - Select this option to run this upgrade job later. Specify the **Execution Date** and **Start Time** when you want to upgrade the instances.

     If you want to upgrade a NetScaler HA pair in two stages, select **Perform two stage upgrade for nodes in HA**.

     Specify the **Execution Date** and **Start Time** when you want to upgrade another instance in the HA pair.

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



9. In **Create Job**, specify the following details:

   a) 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 a file browser. The NetScaler Console GUI displays the instance files that are present at `/var/mps/mps_images`.

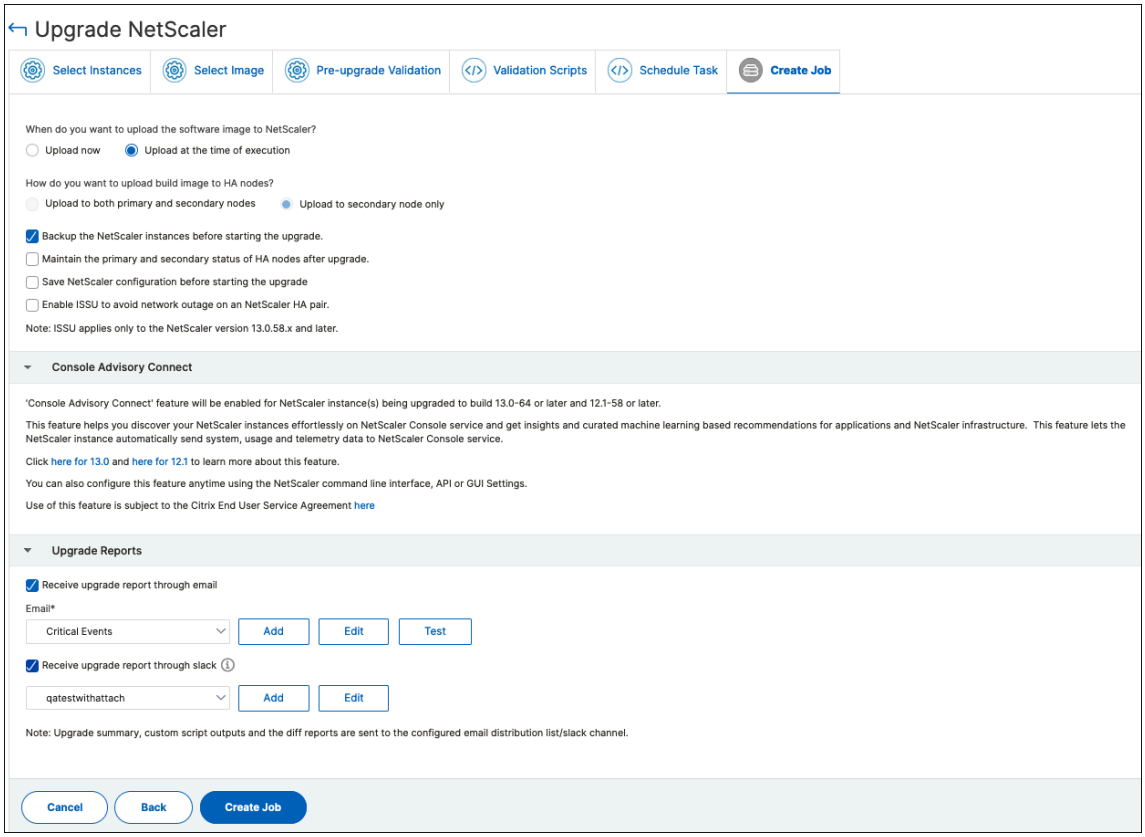
   b) Specify when you want to upload the image to an instance:

   - **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 a high-availability pair, you can specify the nodes on which you want to upload the image:

   - **Upload to both primary and secondary nodes**: Upload the build image file to both the primary and secondary nodes.
   - **Upload to secondary node only**: Upload the build image file to only the secondary node. After the secondary node is upgraded, a failover occurs and the build image file is uploaded to the new secondary node which was previously, the primary node.

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



For more information on the available scheduling scenarios for high-availability pair, see Scheduling upgrade jobs for high-availability pair.

- **Clean software image from NetScaler on successful upgrade** - Select this option to clear the uploaded image in the NetScaler instance after the instance upgrade.
- **Backup the NetScaler instances before starting the upgrade.** - Creates a backup of the selected NetScaler instances.
- **Maintain the primary and secondary status of HA 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 an NetScaler high-availability pair. This option provides a migration functionality that honors the existing connections during the upgrade. So, you can upgrade a NetScaler HA pair without downtime. Specify the ISSU migration timeout in minutes.
- **Receive Execution Report through email** - Sends the execution report in email. To add an email distribution list, see Create an email distribution list.

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

- **Receive Execution Report through slack** - Sends the execution report in slack. To add a Slack profile, see Create a Slack profile.

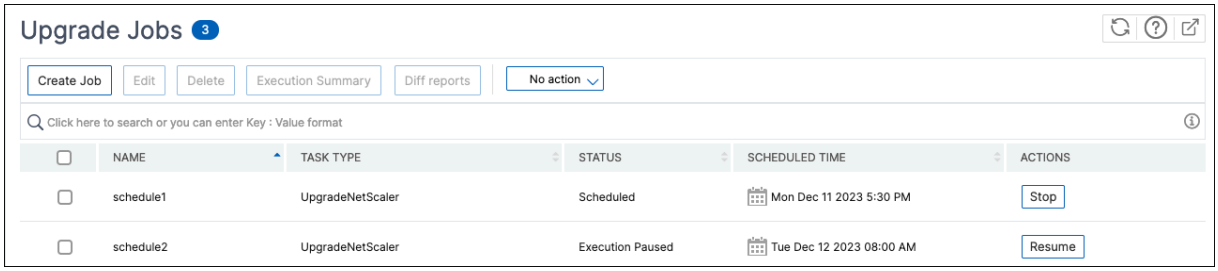
Click **Create Job**.

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.

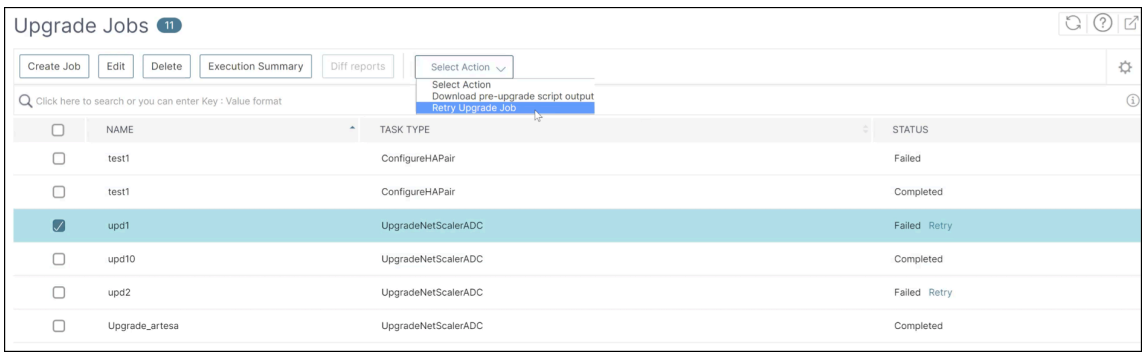
To use this feature, navigate to **Infrastructure > Upgrade Jobs**, select an existing scheduled upgrade job, and click **Stop** to pause the job. To resume the scheduled upgrade job, click **Resume**.



> **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.

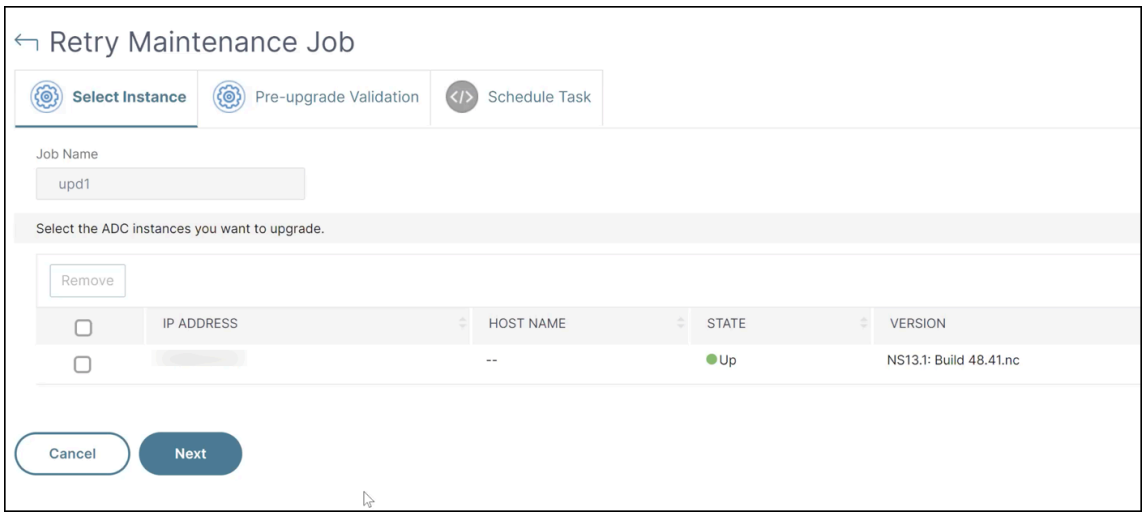


2. In **Select Instance**, specify the following details:

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

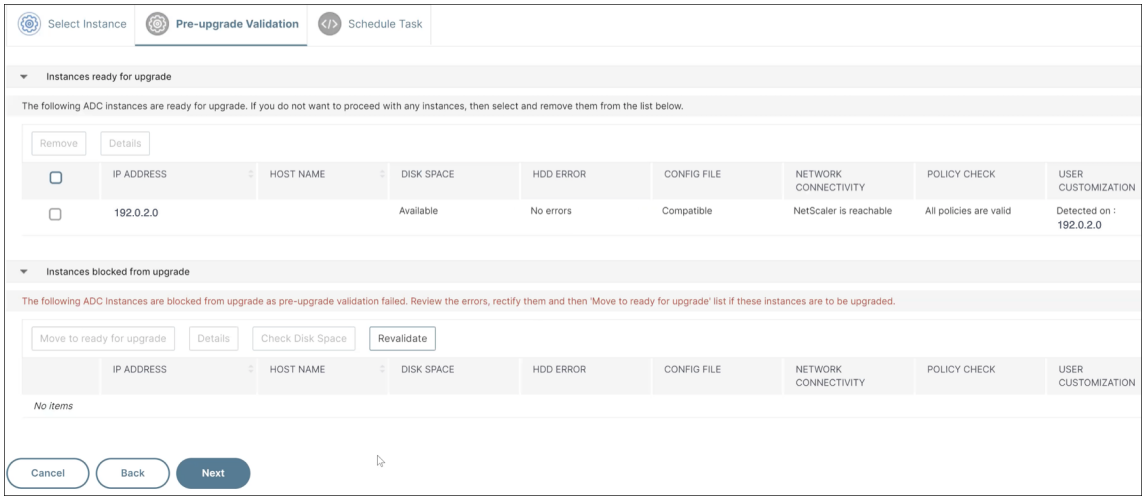
- **Job Name** - Enter a name for the upgrade.
- Select the NetScaler instances that you want to upgrade from the list. To delete any instances, click **Remove**.

Click **Next** to begin the validation process.



3. The **Pre-upgrade validation** tab displays the following sections:
   - **Instances ready for upgrade**. You can continue with the upgrade of these instances.
   - **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 the NetScaler disk space.
   - **Policy Check**: If NetScaler Console finds unsupported classic policies, you can remove such policies to create an upgrade job.

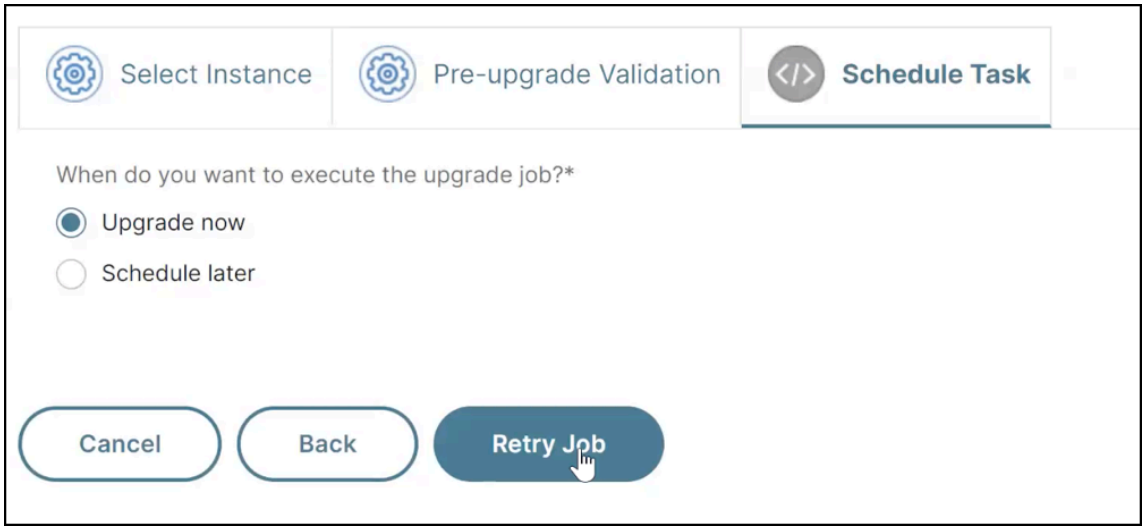


© 1997–2025 Citrix Systems, Inc. All rights reserved.

Click **Next**.

4. In **Schedule Task**, select one of the following options:

   - **Upgrade now**: The upgrade job runs immediately.
   - **Schedule Later**: Select this option to run this upgrade job later. Specify the **Execution Date** and **Start Time** when you want to upgrade the instances.



Click **Retry**.

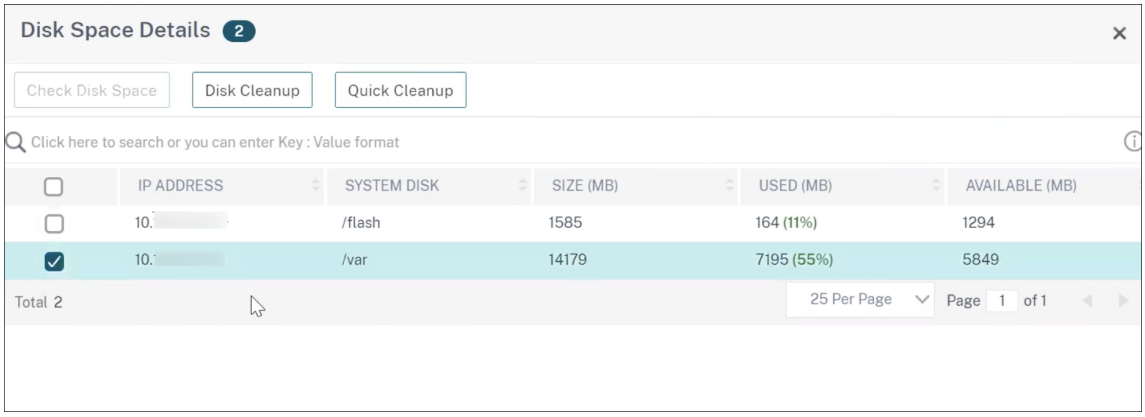
Clean up the NetScaler disk space

If you face the insufficient disk space issue while upgrading an 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** page appears. This page displays the instances, used memory, and available memory.

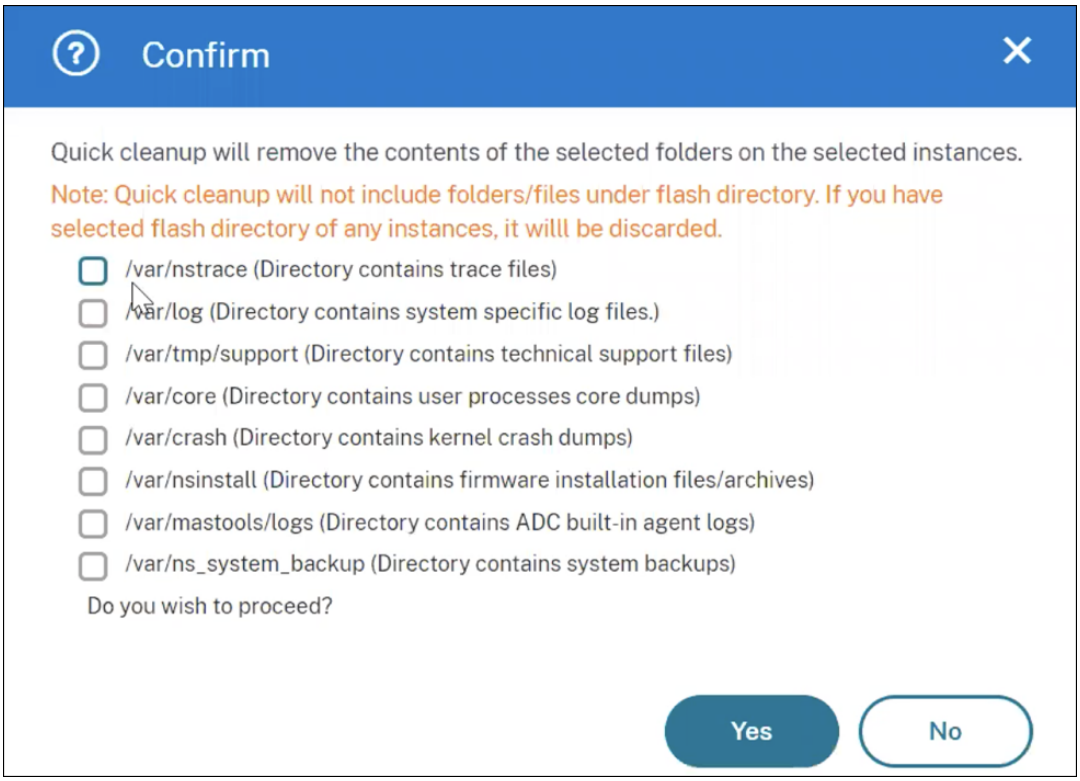
© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. In the **Disk Space Details** pane, select the instance that requires clean up and do one of the following:

   a) **Disk Cleanup** - Navigate to the required folders or directories and delete them to free up disk space.

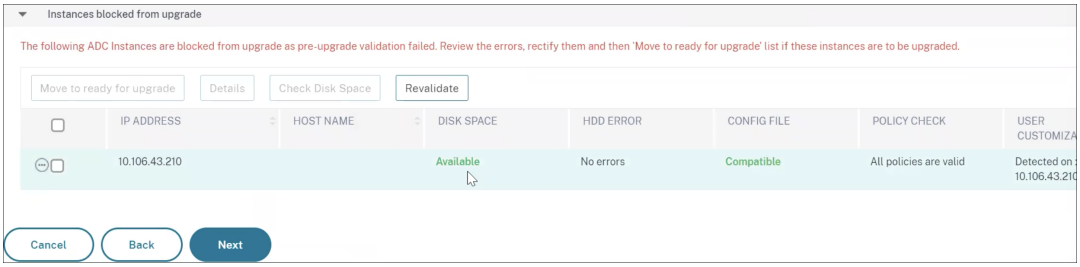
   b) **Quick Cleanup** - Quickly clear up disk space by deleting multiple folders. In the **Confirm** pane that appears, select the folders you want to delete and click **Yes**.



   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.



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)
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 combined diff report of a NetScaler upgrade job

You can download a difference report of an NetScaler upgrade job if custom scripts are specified. A diff report contains the differences between the outputs of the pre-upgrade and post-upgrade scripts. With this report, you can determine what changes occurred on the NetScaler instance post upgrade.

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

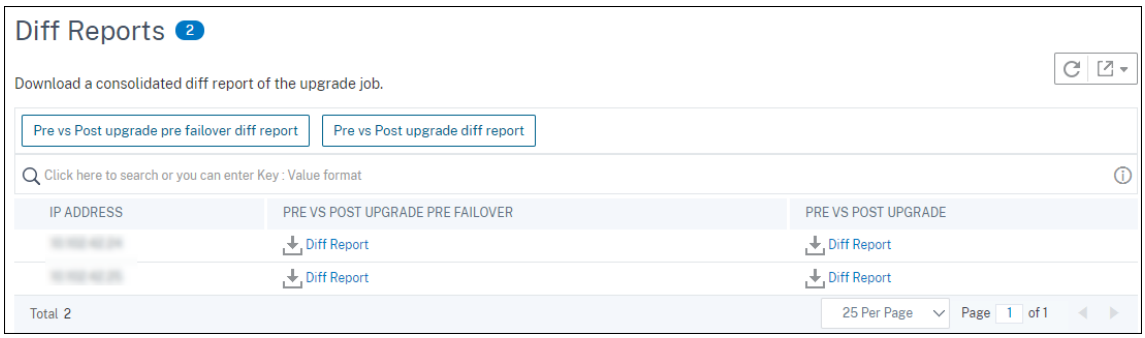
> **Note**
>
> The diff report is generated only if you specify the same script in the pre-upgrade and post-upgrade stages.

To download a diff report of an upgrade job, do the following:

1. Navigate to **Infrastructure > Upgrade 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:

   - **Pre vs Post upgrade pre failover diff report**
   - **Pre vs Post upgrade diff report**



Security Advisory

October 14, 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:

- 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.

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

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.
  - **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.

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

- **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.

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:

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

1. Click **Scan Now**.
2. Select the types of scans that you want to run.
    - Security Config Recommendations
    - CVE Detection
    - File Integrity Monitoring
3. Click **Scan Now**. Once the scanning is completed, the revised security details appear in the security advisory dashboard.

Scan History

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

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

NetScalers impacted

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

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

Settings

As an admin, you can receive Citrix Cloud notifications, which tell how many NetScaler instances are vulnerable with CVEs. To configure when and how you want to receive notifications, click the settings icon on the upper-right corner of the security advisory page.

You can perform the following actions:

- Select the type of events for which you must receive the notification.
- Select how you want to be notified. For example, through email, Slack, PagerDuty.
- Select the type of scan that must be included in system scans. By default, only CVE scan is enabled for system scan.
- Opt out of security advisory custom scan.

You can also configure the type of scans that must be included in the system scans.

© 1997–2025 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 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

October 14, 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.

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

- **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.

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.

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.

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

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.

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.
    - **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

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

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 streamlines the implementation process. Recommendations that require input demand careful data gathering and validation from the user, while those not requiring input can often be applied as standard security baselines or through automated deployment mechanisms.

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

For instance, here's an example of a configuration recommendation that requires user input. One can

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

enter configuration values one by one or choose to upload a file containing the configuration values as shown in the following image.

CVE Detection

October 14, 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

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.

The impacted instances are categorized based on the following form factors:

- MPX and VPX

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

- 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
- 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.

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

> **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.

- **CVE ID**: The ID of the CVE that impacts the instances.
- **Publication date**: The date the security bulletin was released for that CVE.
- **Severity score**: The severity type (high/medium/critical) and score. To see the score, hover over the severity type.
- **Vulnerability type**: The type of vulnerability for this CVE.
- **Affected NetScaler instances**: The instance count that the CVE ID is impacting. On hover over, the list of NetScaler instances appears.
- **Remediation**: The available remediations, which are upgrading the instance (usually) or applying configuration packs.

The same instance can be impacted by multiple CVEs. This table helps you see how many instances one particular CVE or multiple selected CVEs are impacting. To check the IP address of the impacted instance, hover over NetScaler Details under **Affected NetScaler Instances**. To check the details of the impacted instance, click **View Affected Instances** at the bottom of the table.
You can also add or remove columns in the table by clicking the plus sign.

CVE repository

Both instance view and CVE view contain the **CVE Repository** tab. This tab gives a detailed view of all the NetScaler related CVEs that Citrix has announced since Dec 2019, that might impact your NetScaler infrastructure.

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

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

You can use this view to understand the CVEs in the security advisory scope and to learn more about the CVE. For information on CVEs that are not supported, see Unsupported CVEs in Security Advisory.

Points to note

- Security Advisory does not support NetScaler builds that have reached End of Life (EOL). We recommend you upgrade to the NetScaler supported builds or versions.
- Instances supported for CVE detection: all NetScaler (SDX, MPX, VPX) and Gateway.
- Instances supported for File Integrity Monitoring: MPX, VPX instances, and Gateway.
- CVEs supported: All CVEs after Dec 2019.

  > **Note:**
  >
  > The detection and remediation of vulnerabilities impacting the NetScaler Gateway plug-in for Windows is not supported by the NetScaler Console Security Advisory. For information on CVEs that are not supported, see Unsupported CVEs in Security Advisory.

- NetScaler Console security advisory doesn't account for any kind of feature misconfiguration while identifying the vulnerability.
- NetScaler Console security advisory only supports the identification and remediation of the CVEs. It does not support identification and remediation of the security concerns that are highlighted in the Security article.
- Scope of NetScaler, Gateway releases: The feature is limited to main builds. Security advisory does not include any special build in its scope.
  - Security advisory is not supported in the Admin partition.
- The following types of scan are available for CVEs:
  - **Version scan**: This scan needs NetScaler Console to compare the version of an NetScaler instance with the versions and builds on which the fix is available. This version comparison helps NetScaler Console security advisory identify whether the NetScaler is vulnerable to the CVE. For example, if a CVE is fixed on an NetScaler release and build xx.yy, the security

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

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

October 14, 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:

- 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

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

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.
- 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

Supported CVEs through Security Advisory

November 11, 2025

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

In your NetScaler Console on-prem, the full version of Security Advisory is supported if you have enabled Security Advisory through Cloud Connect or auto-enabled channel. For more information, see Security Advisory.

Latest supported CVEs

The following table provides the latest supported CVE details that you can identify and remediate in Security Advisory:

Release date	CVE ID	Identification	Remediation	Resource link
11 Nov 2025	CVE-2025-12101	Requires version scan.	Upgrade to the recommended build mentioned in the security bulletin.	Security Bulletin

> **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.

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

Supported CVEs

The following are the existing CVEs supported in Security Advisory:

Release date	CVE ID	Resource link
Nov 11, 2025	CVE-2025-12101	Security Bulletin
Aug 26, 2025	CVE-2025-8424	Security Bulletin
Aug 26, 2025	CVE-2025-7776	Security Bulletin

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

Release date	CVE ID	Resource link
Aug 26, 2025	CVE-2025-7775	Security Bulletin
Jun 25, 2025	CVE-2025-6543	Security Bulletin
Jun 17, 2025	CVE-2025-5349	Security Bulletin
Jun 17, 2025	CVE-2025-5777	Security Bulletin
Nov 12, 2024	CVE-2024-8535	Security Bulletin
Jul 09, 2024	CVE-2024-5491	Security Bulletin
Jul 09, 2024	CVE-2024-5492	Security Bulletin
Jan 16, 2024	CVE-2023-6549	Security bulletin
Jan 16, 2024	CVE-2023-6548	Security bulletin
Oct 10, 2023	CVE-2023-4967	Security bulletin
Oct 10, 2023	CVE-2023-4966	Security bulletin
Jul 18, 2023	CVE-2023-3519	Security bulletin
Jul 18, 2023	CVE-2023-3467	Security bulletin
Jul 18, 2023	CVE-2023-3466	Security bulletin
May 09, 2023	CVE-2023-24488	Security bulletin
May 09, 2023	CVE-2023-24487	Security bulletin
Dec 13, 2022	CVE-2022-27518	Security bulletin
Nov 08, 2022	CVE-2022-27516	Security bulletin
Nov 08, 2022	CVE-2022-27513	Security bulletin
Nov 08, 2022	CVE-2022-27510	Security bulletin
Jul 26, 2022	CVE-2022-27509	Security bulletin
May 25, 2022	CVE-2022-27508	Security bulletin
May 25, 2022	CVE-2022-27507	Security bulletin
Nov 09, 2021	CVE-2021-22956	Security bulletin
Nov 09, 2021	CVE-2021-22955	Security bulletin
Jul 19, 2021	CVE-2021-22927	Security bulletin
Jul 19, 2021	CVE-2021-22920	Security bulletin
Jul 19, 2021	CVE-2021-22919	Security bulletin
Jun 08, 2021	CVE-2020-8300	Security bulletin

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

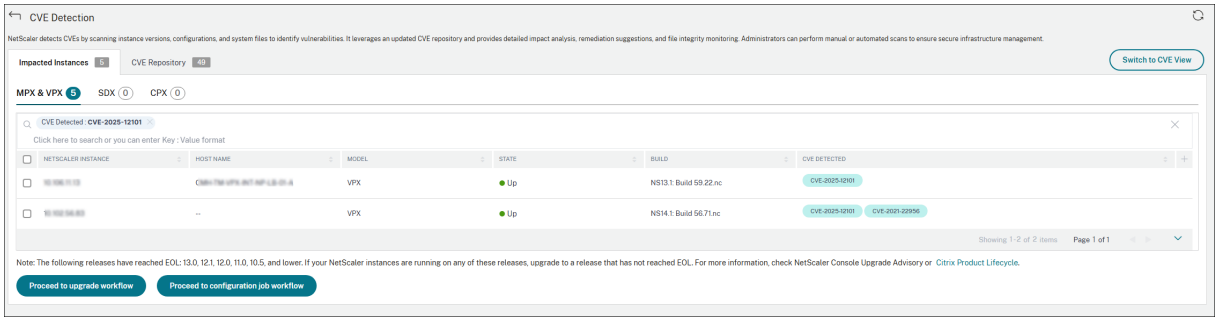
Release date	CVE ID	Resource link
Jun 08, 2021	CVE-2020-8299	Security bulletin
Sep 17, 2020	CVE-2020-8247	Security bulletin
Sep 17, 2020	CVE-2020-8246	Security bulletin
Sep 17, 2020	CVE-2020-8245	Security bulletin
Jul 07, 2020	CVE-2020-8197	Security bulletin
Jul 07, 2020	CVE-2020-8199	Security bulletin
Jul 07, 2020	CVE-2020-8195	Security bulletin
Jul 07, 2020	CVE-2020-8196	Security bulletin
Jul 07, 2020	CVE-2020-8193	Security bulletin
Jul 07, 2020	CVE-2020-8187	Security bulletin
Jul 07, 2020	CVE-2020-8191	Security bulletin
Jul 07, 2020	CVE-2020-8190	Security bulletin
Jul 07, 2020	CVE-2019-18177	Security bulletin
Jul 07, 2020	CVE-2020-8194	Security bulletin
Jul 07, 2020	CVE-2020-8198	Security bulletin
Dec 17, 2019	CVE-2019-19781	Security bulletin

Identify and remediate vulnerabilities for CVE-2025-12101

November 11, 2025

In the NetScaler Console® security advisory dashboard, click **CVE Detection**. On the **Impacted Instances** tab, search for CVE-2025-12101. The list of NetScaler instances that are impacted by CVE-2025-12101 is displayed.

© 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-2025-12101 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

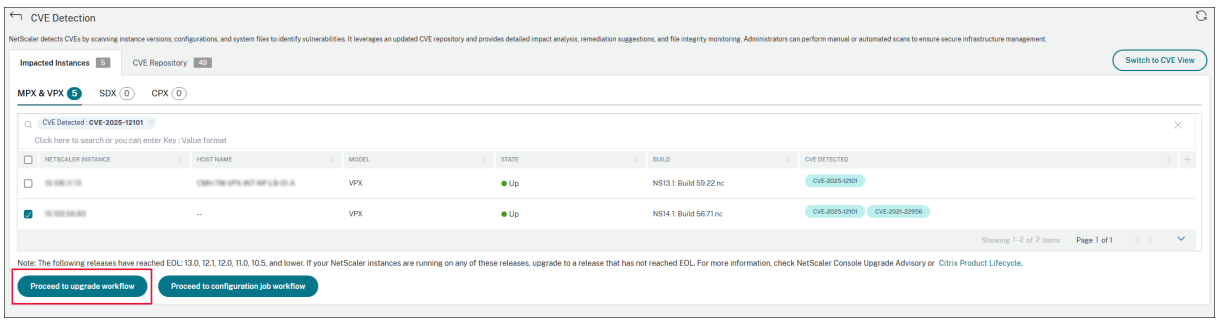
Remediate CVE-2025-12101

For CVE-2025-12101 impacted NetScaler instances, the remediation is a single-step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix.

In the GUI, under **CVE Detection > Impacted Instances**, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

> **IMPORTANT**
>
> If your vulnerable NetScaler instances have the /etc/httpd.conf file copied to the /nsconfig directory, see Upgrade considerations for customized NetScaler configurations before planning NetScaler upgrade.

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

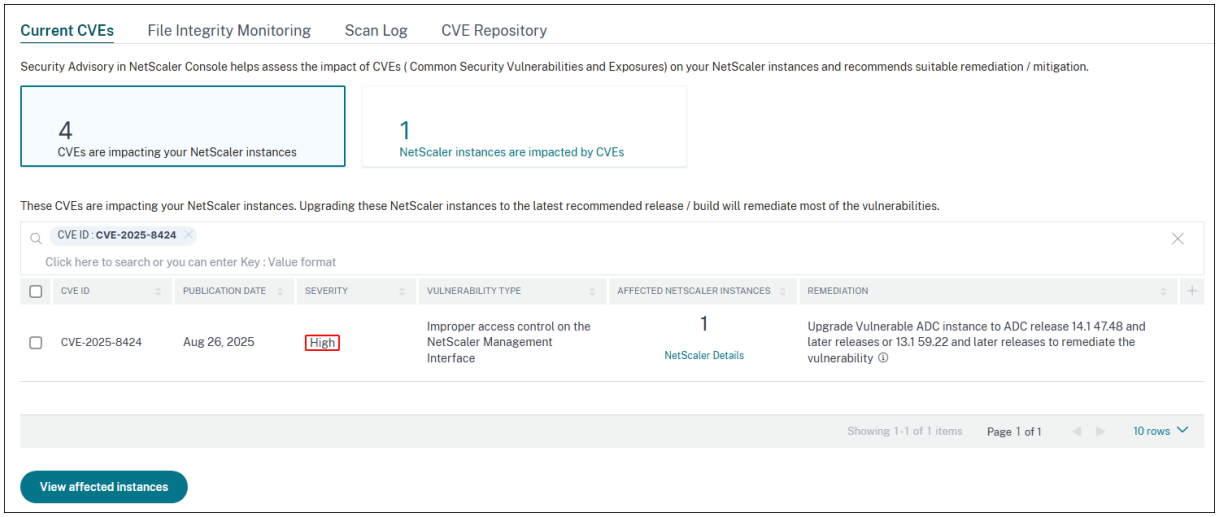


© 1997–2025 Citrix Systems, Inc. All rights reserved.

Identify and remediate vulnerabilities for CVE-2025-8424

September 27, 2025

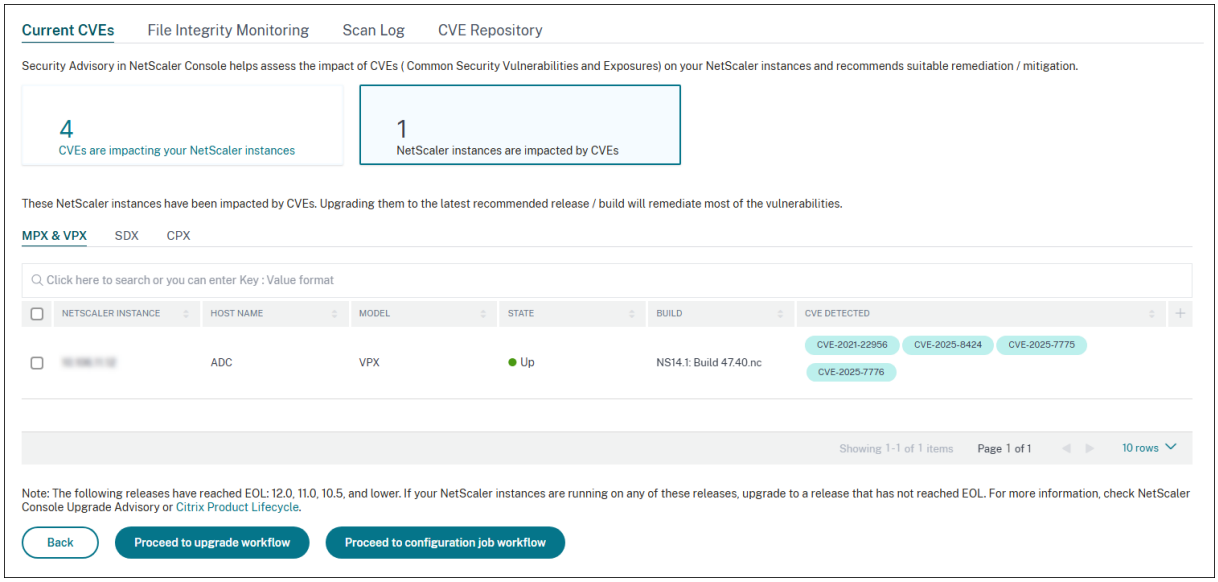
In the NetScaler Console security advisory dashboard, under **Current CVEs <number of> NetScaler instances are impacted by CVEs**, you can see all the instances vulnerable due to CVE-2025-8424. To check the details of the instances impacted by the CVEs, select CVE-2025-8424 and click **View Affected 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-2025-8424.

© 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 **Current CVEs > NetScaler instances are impacted by CVEs**, you can see the step to remediate.

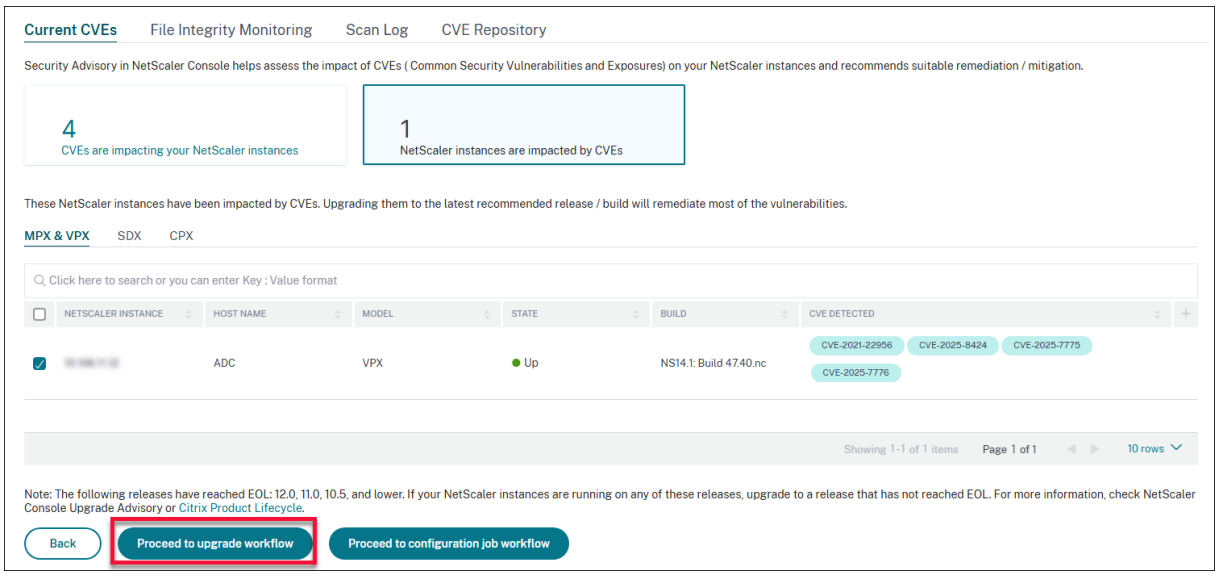
Under **Current CVEs> NetScaler instances impacted by CVEs**, you see the following workflow for this single step remediation process, which is **Proceed to upgrade workflow**.

To upgrade the vulnerable instances, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

> **IMPORTANT**
>
> If your vulnerable NetScaler instances have the /etc/httpd.conf file copied to the /nsconfig directory, see Upgrade considerations for customized NetScaler configurations before planning NetScaler upgrade.

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

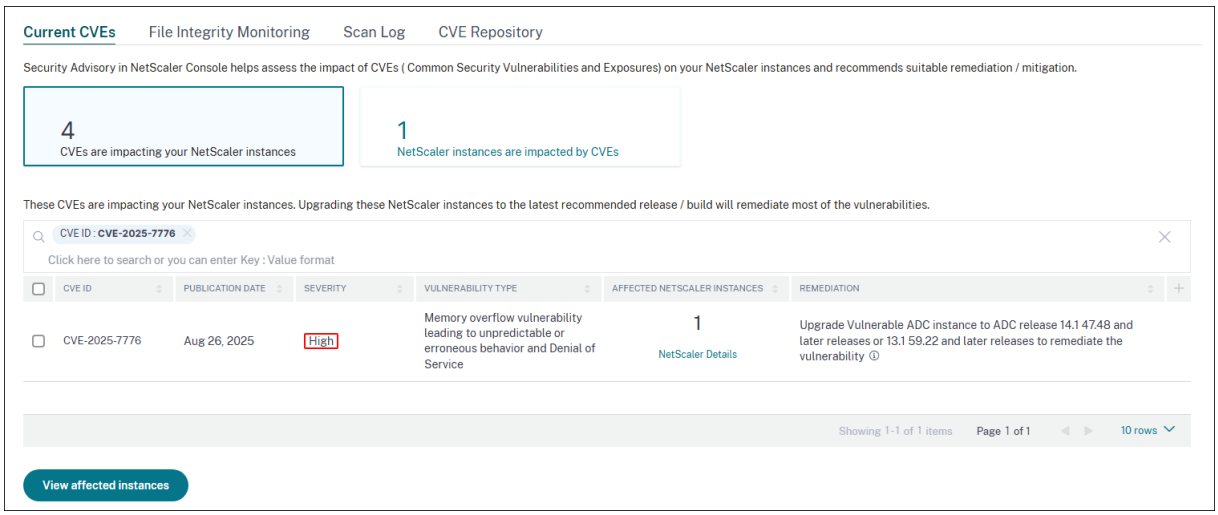
© 1997–2025 Citrix Systems, Inc. All rights reserved.



Identify and remediate vulnerabilities for CVE-2025-7776

September 27, 2025

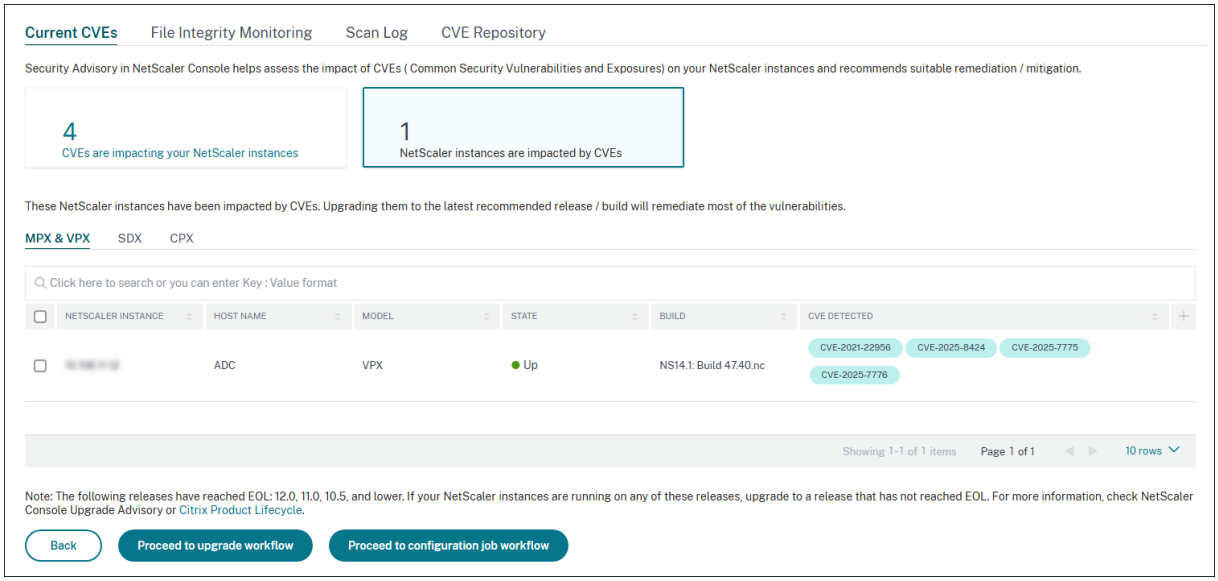
In the NetScaler Console security advisory dashboard, under **Current CVEs <number of> NetScaler instances are impacted by CVEs**, you can see all the instances vulnerable due to CVE-2025-7776. To check the details of the instances impacted by the CVEs, select CVE-2025-7776 and click **View Affected Instances**.



> **Note:**
>
> To understand the reason for NetScaler vulnerability, download the CSV report in **Scan logs** tab in Security Advisory.

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

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-2025-7776.



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 **Current CVEs > NetScaler instances are impacted by CVEs**, you can see the step to remediate.

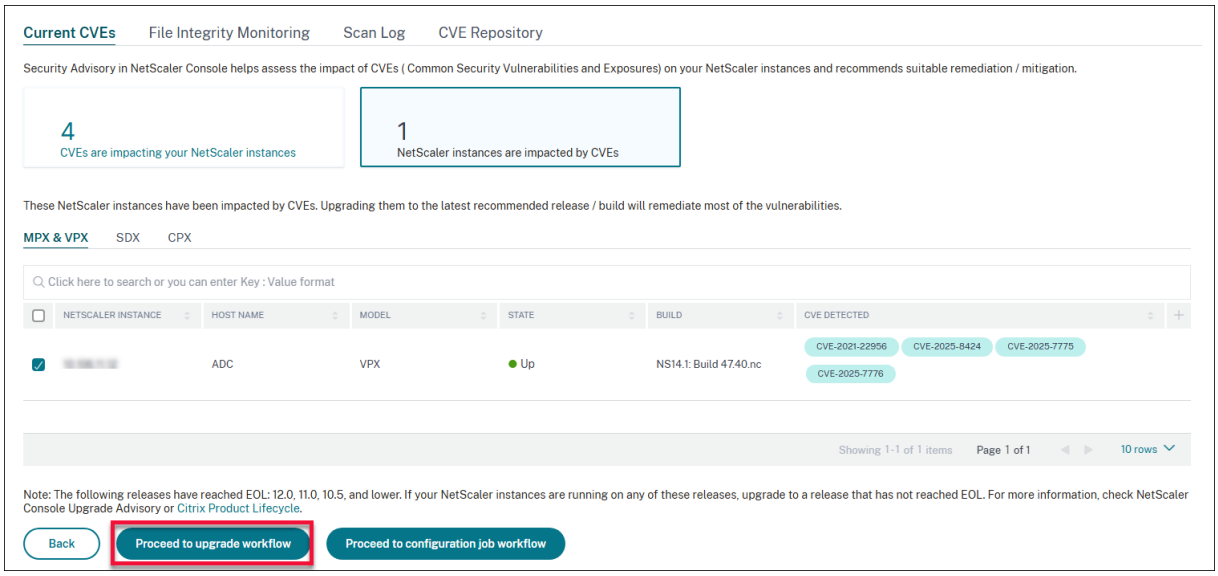
Under **Current CVEs> NetScaler instances impacted by CVEs**, you see the following workflow for this single step remediation process, which is **Proceed to upgrade workflow**.

To upgrade the vulnerable instances, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

> **IMPORTANT**
>
> If your vulnerable NetScaler instances have the /etc/httpd.conf file copied to the /nsconfig directory, see Upgrade considerations for customized NetScaler configurations before planning NetScaler upgrade.

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

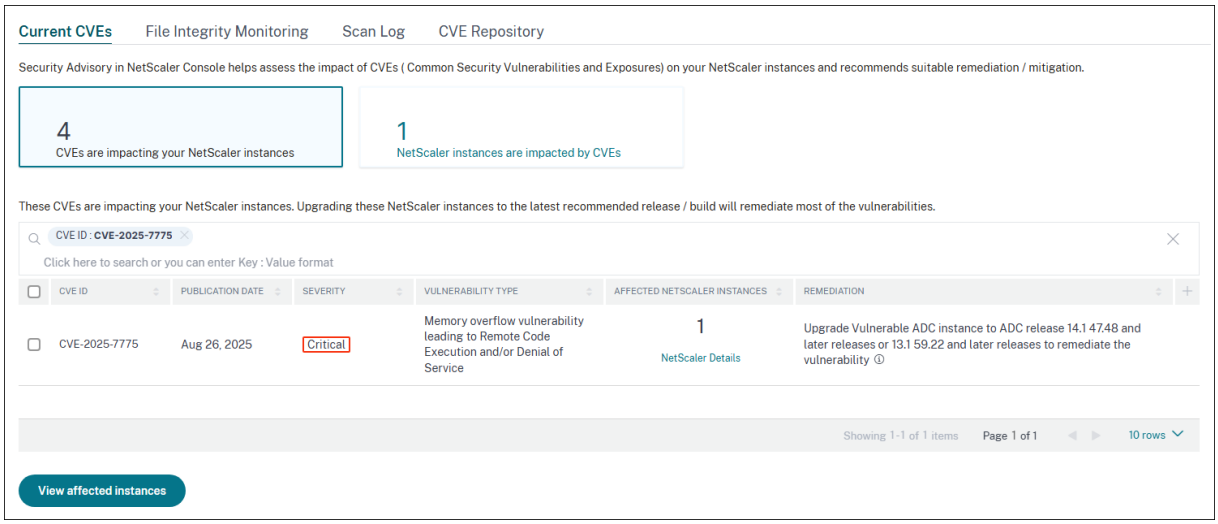
For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.



Identify and remediate vulnerabilities for CVE-2025-7775

September 27, 2025

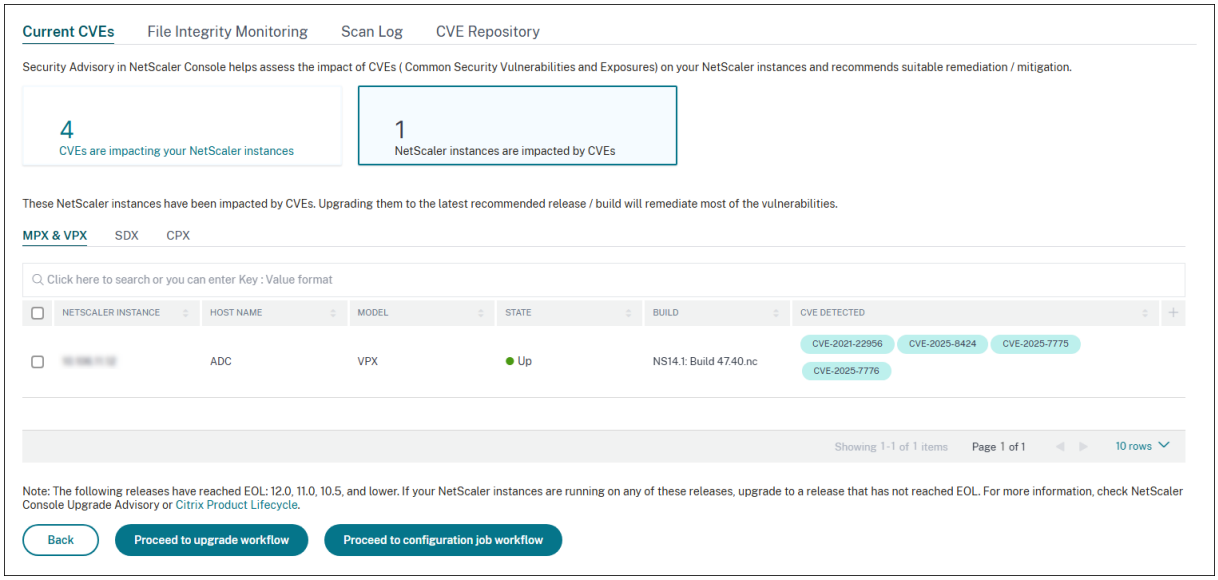
In the NetScaler Console security advisory dashboard, under **Current CVEs <number of> NetScaler instances are impacted by CVEs**, you can see all the instances vulnerable due to CVE-2025-7775. To check the details of the instances impacted by the CVEs, select CVE-2025-7775 and click **View Affected 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-2025-7775.



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

> **Note:**
>
> It might take a couple of hours for the security advisory system scan to conclude and reflect the impact of CVE-2025-7775 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2025-7775

For CVE-2025-7775 impacted NetScaler instances, the remediation is a single step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix. In the GUI, under **Current CVEs > NetScaler instances are impacted by CVEs**, you can see the step to remediate.

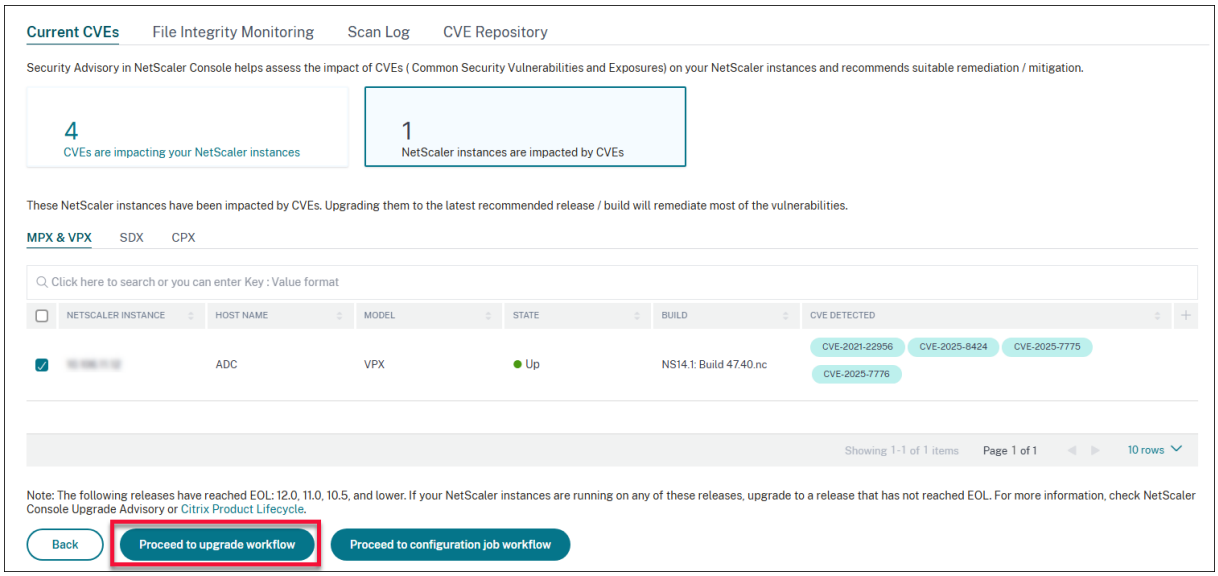
Under **Current CVEs> NetScaler instances impacted by CVEs**, you see the following workflow for this single step remediation process, which is **Proceed to upgrade workflow**.

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.

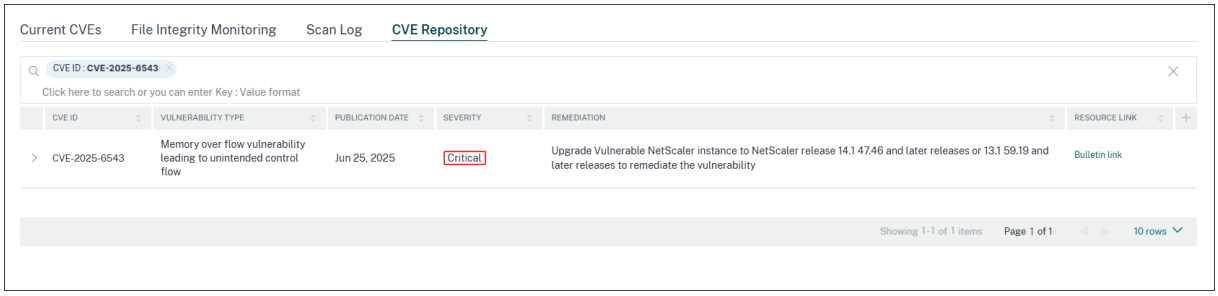
For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.



Identify and remediate vulnerabilities for CVE-2025-6543

September 27, 2025

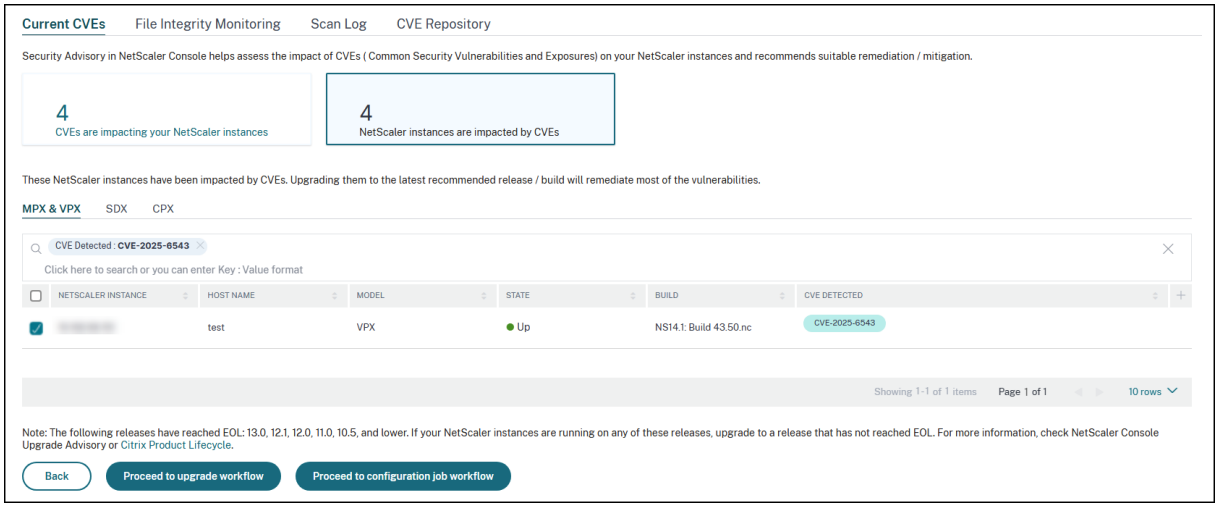
In the NetScaler Console security advisory dashboard, under **Current CVEs <number of> NetScaler instances are impacted by CVEs**, you can see all the instances vulnerable due to CVE-2025-6543. To check the details of the instances impacted by the CVEs, select CVE-2025-6543 and click **View Affected 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-2025-6543.



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**.

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.

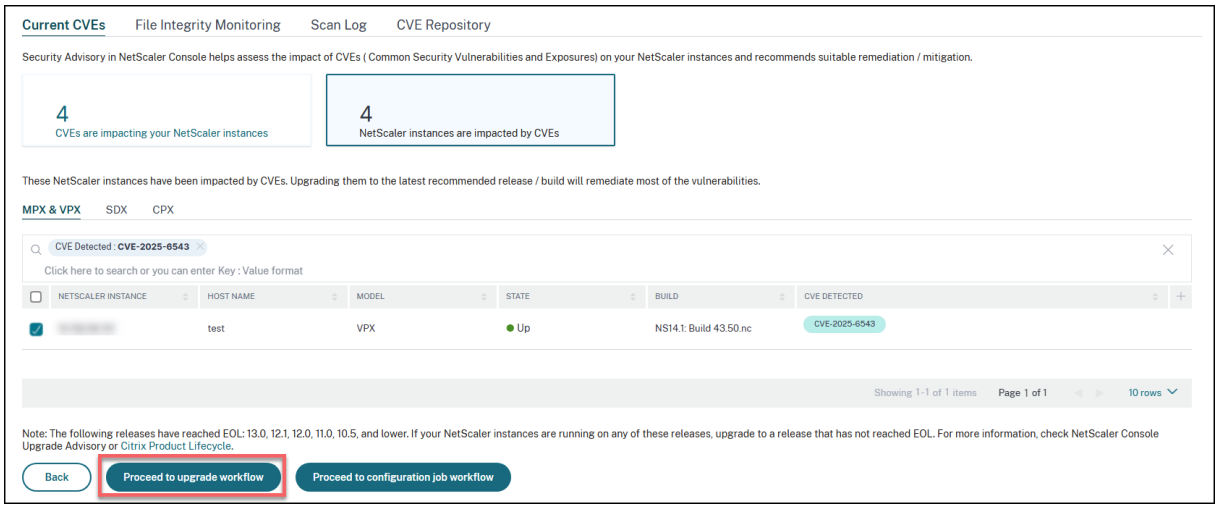
Under **Current CVEs> NetScaler instances impacted by CVEs**, you see the following workflow for this single step remediation process, which is **Proceed to upgrade workflow**.

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.

© 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.



Identify and remediate vulnerabilities for CVE-2025-5349

December 22, 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**.

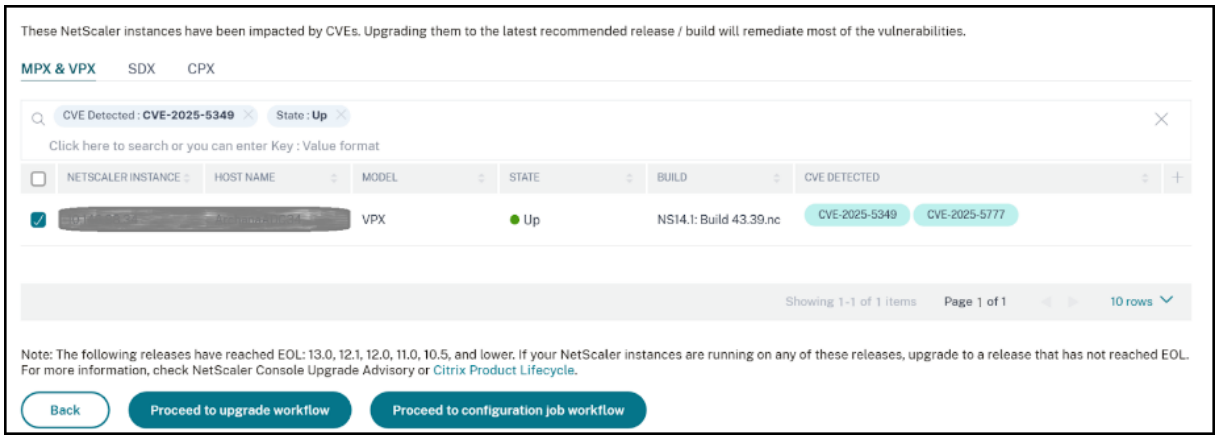


> **Note:**
>
> To understand the reason for NetScaler vulnerability, download the CSV report in **Scan logs** tab

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

> 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.

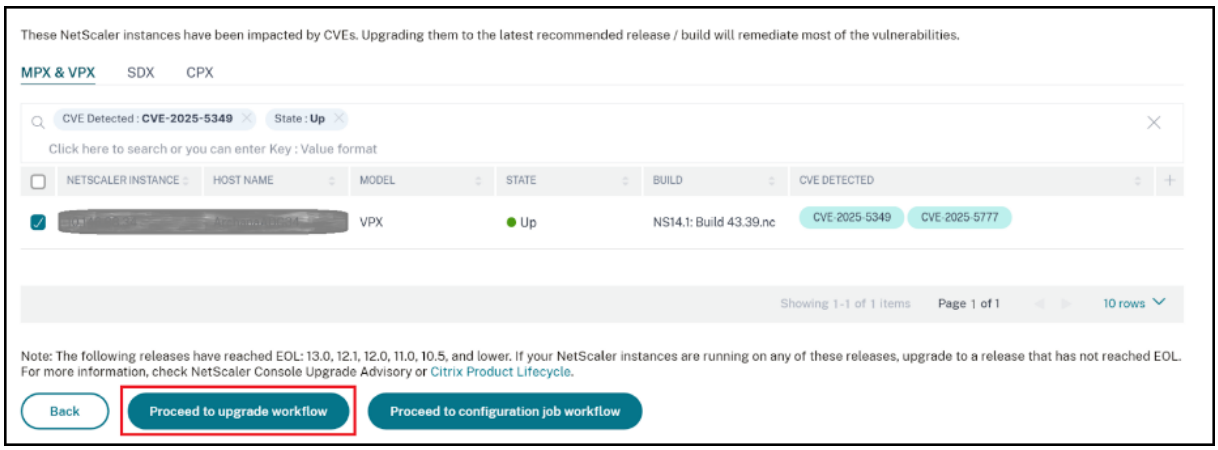
Under **Current CVEs> NetScaler instances impacted by CVEs**, you see the following workflow for this single step remediation process, which is **Proceed to upgrade workflow**.

To upgrade the vulnerable instances, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

> **IMPORTANT**
>
> If your vulnerable NetScaler instances have the /etc/httpd.conf file copied to the /nsconfig directory, see Upgrade considerations for customized NetScaler configurations before planning NetScaler upgrade.

For more information on how to use NetScaler Console to upgrade NetScaler instances, see Create a NetScaler upgrade job.

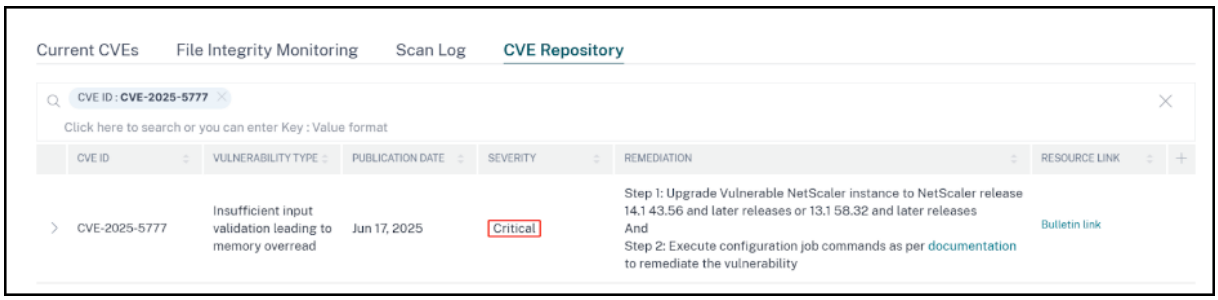
© 1997–2025 Citrix Systems, Inc. All rights reserved.



Remediate vulnerabilities for CVE-2025-5777

December 22, 2025

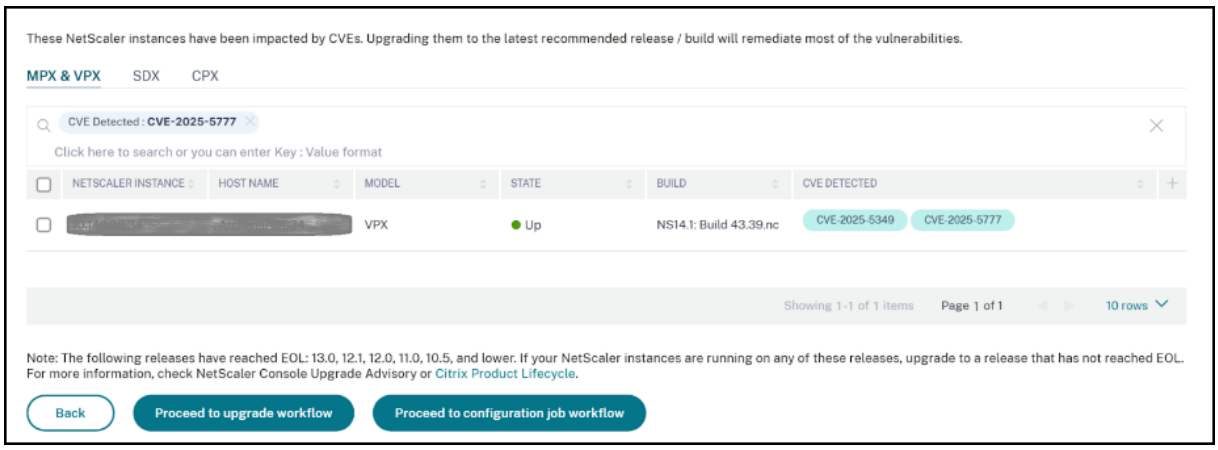
In the NetScaler Console security advisory dashboard, under **Current CVEs <number of> NetScaler instances are impacted by CVEs**, you can see all the instances vulnerable due to CVE-2025-5777. To check the details of the instances impacted by the CVEs, select CVE-2025-5777 and click **View Affected Instances**.



> **Note:**
>
> To understand the reason for NetScaler vulnerability, download the CSV report in **Scan logs** tab in Security Advisory.

The **<number of> NetScaler instances impacted by CVEs** window appears. In the following screen capture, you can see the count and details of the NetScaler instances impacted by CVE-2025-5777.

© 1997–2025 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-2025-5777 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.

Remediate CVE-2025-5777

For CVE-2025-5777 -impacted NetScaler instances, the remediation is a two-step process. In the GUI, under **Current CVEs > NetScaler instances are impacted by CVEs**, you can see step 1 and 2.



The two steps include:

1. Upgrading the vulnerable NetScaler instances to a release and build that has the fix.
2. Applying the required configuration commands using the customizable built-in configuration template in configuration jobs.

Under **Current CVEs> NetScaler instances impacted by CVEs**, you see two separate workflows for this 2-step remediation process: which are **Proceed to upgrade workflow** and **Proceed to configuration job workflow**.

© 1997–2025 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.

> **Note:**
>
> This step can be done at once for all the vulnerable NetScaler instances.

Step 2: Apply configuration commands

After you've upgraded the impacted instances, in the **<number of> NetScaler instances impacted by CVEs** window, select the instance impacted by CVE-2025-5777 and click **Proceed to configuration job workflow**. The workflow includes the following steps.

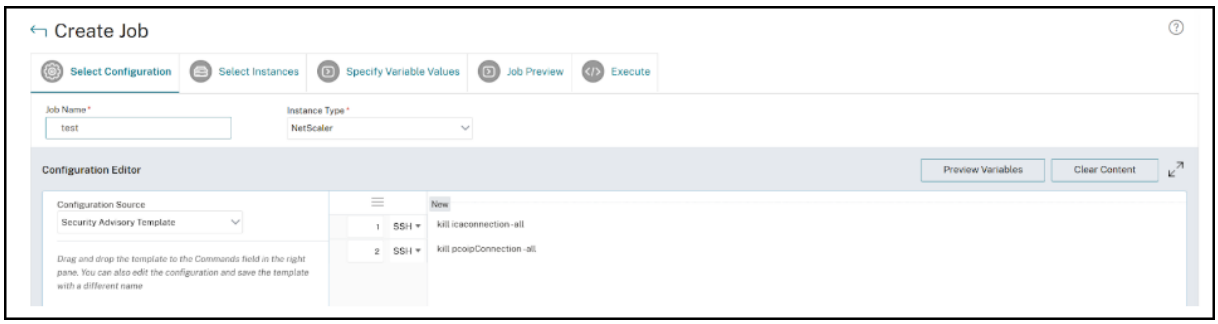
1. Customizing the configuration.
2. Reviewing the auto-populated impacted instances.
3. Running the job.

Keep the following points in mind before you select an instance and click **Proceed to configuration job workflow**:

- For a NetScaler instance impacted by multiple CVEs (such as CVE-2020-8300, CVE-2021-22927, CVE-2021-22920, CVE-2021-22956, and CVE-2025-5777): when you select the instance and click **Proceed to configuration job workflow**, the built-in configuration template does not auto-populate under **Select configuration**. You must Drag and drop the appropriate config job template under **Security Advisory Template** manually to the config job pane on the right side.
- For multiple NetScaler instances that are impacted by CVE-2025-5777 only: you can run config jobs on all instances at once. For example, you've NetScaler 1, NetScaler 2, and NetScaler 3, and all of them are impacted only by CVE-2025-5777. Select all these instances and click **Proceed to configuration job workflow**, and the built-in configuration template auto-populates under **Select configuration**.
- For multiple NetScaler instances impacted by CVE-2025-5777 and one or more other CVEs (such as CVE-2020-8300, CVE-2021-22927, and CVE-2021-22920), which require remediation to be applied to each NetScaler at a time: when you select these instances and click **Proceed to configuration job workflow**, an error message appears telling you to run the config job on each NetScaler at a time.

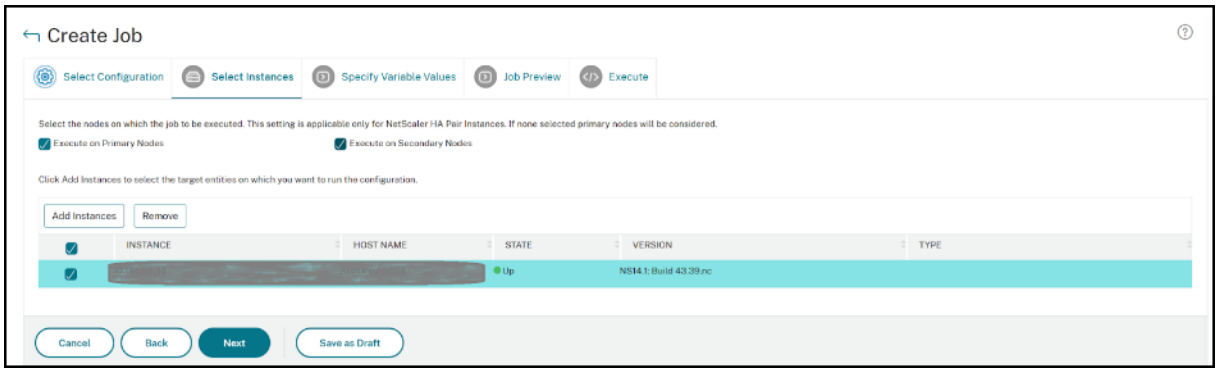
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

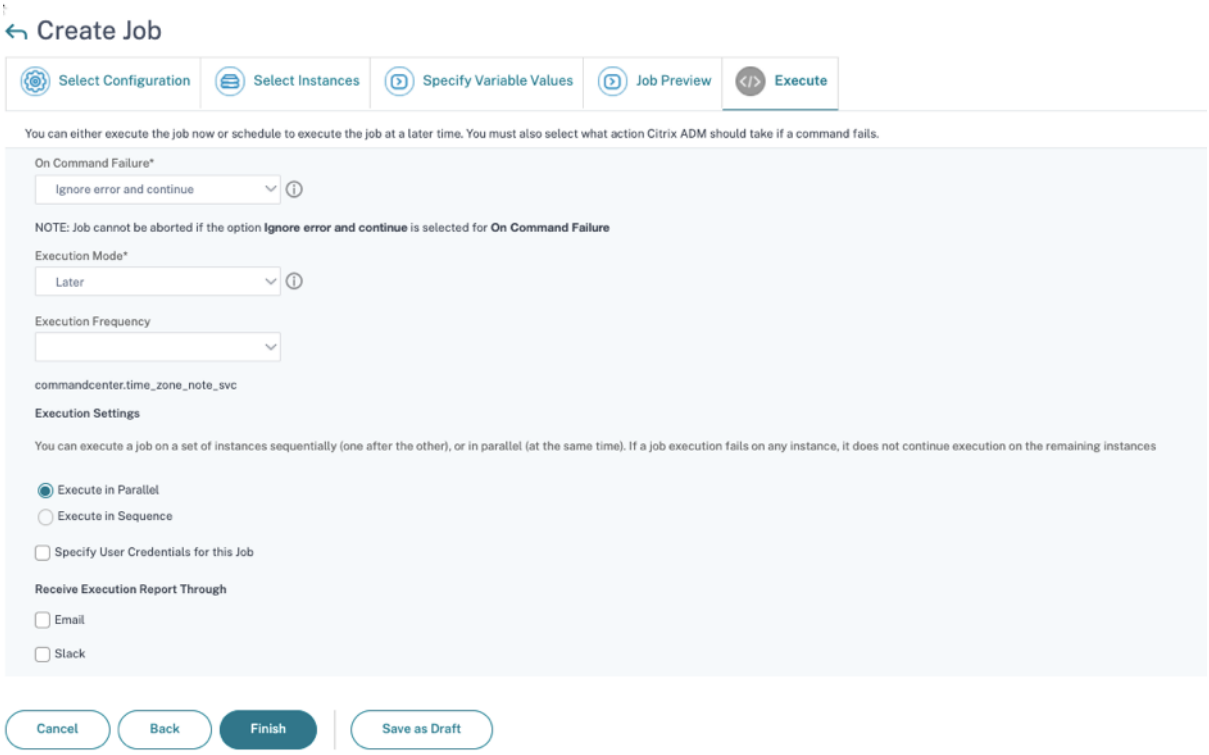
The impacted instance is auto-populated under **Select Instances**. Select the instance. If this instance is part of an HA pair, select **Execute on Secondary Nodes**. Click **Next**.



> **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**.

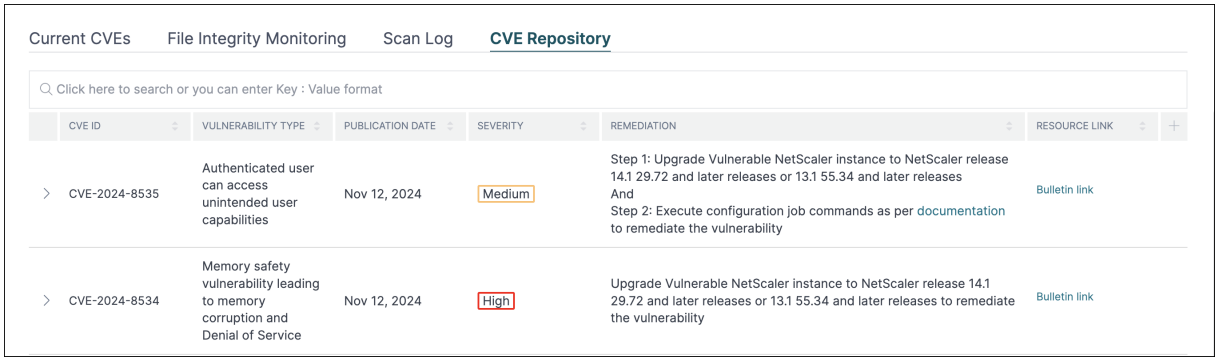
After completing the two remediation steps for all vulnerable NetScaler instances, you can run an on-demand scan to see the revised security posture.

Remediate vulnerabilities for CVE-2024-8535

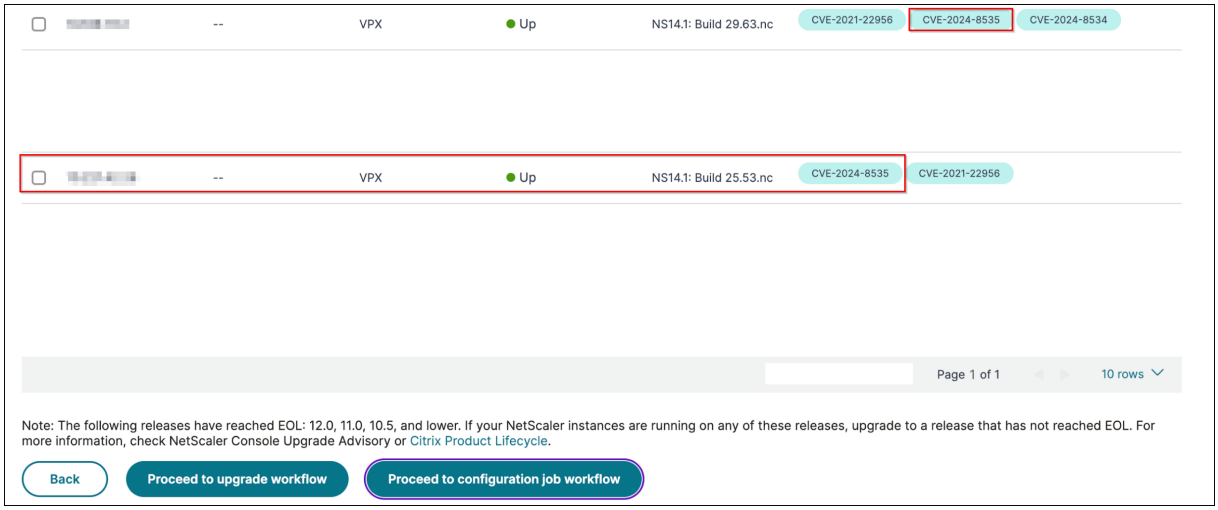
September 27, 2025

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-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

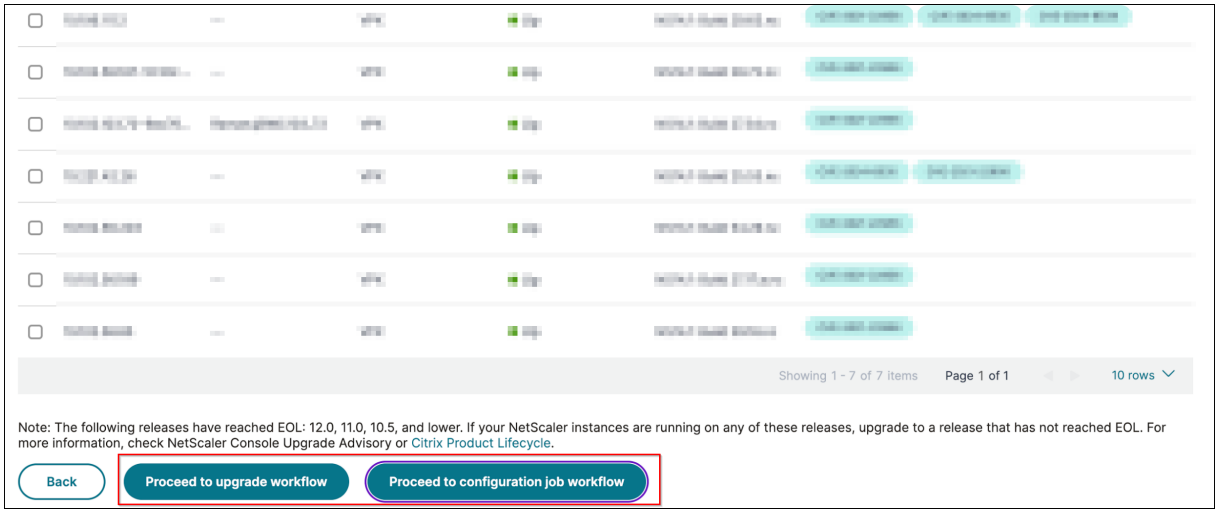
For CVE-2024-8535 -impacted NetScaler instances, the remediation is a two-step process. In the GUI, under **Current CVEs > NetScaler instances are impacted by CVEs**, you can see step 1 and 2.

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.

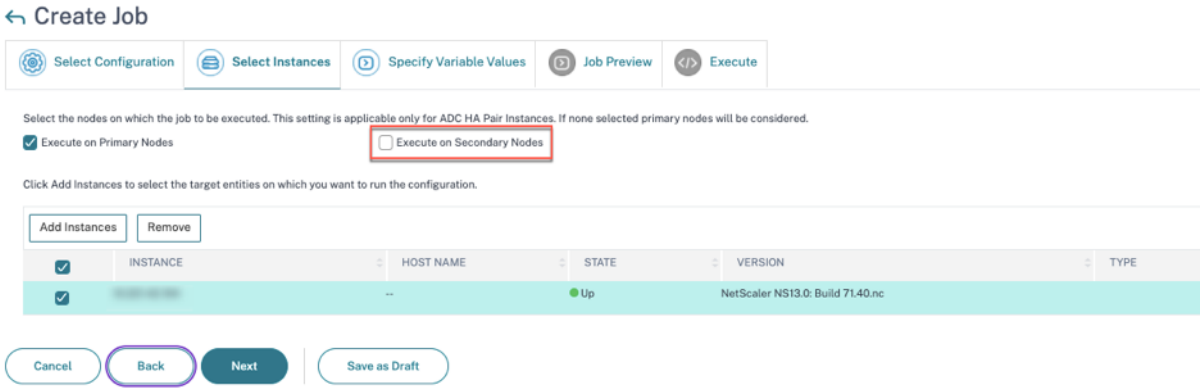
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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**.

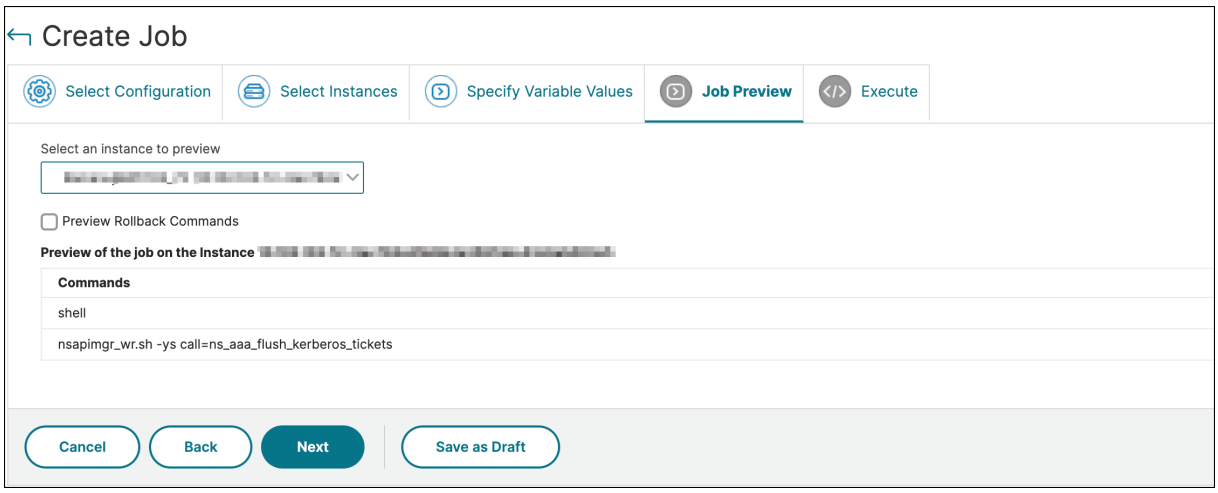


> **Note:**
>
> For NetScaler instances in cluster mode, using security advisory, the NetScaler Console supports running the config job only on the cluster configuration coordinator (CCO) node. Run the commands on non-CCO nodes separately.

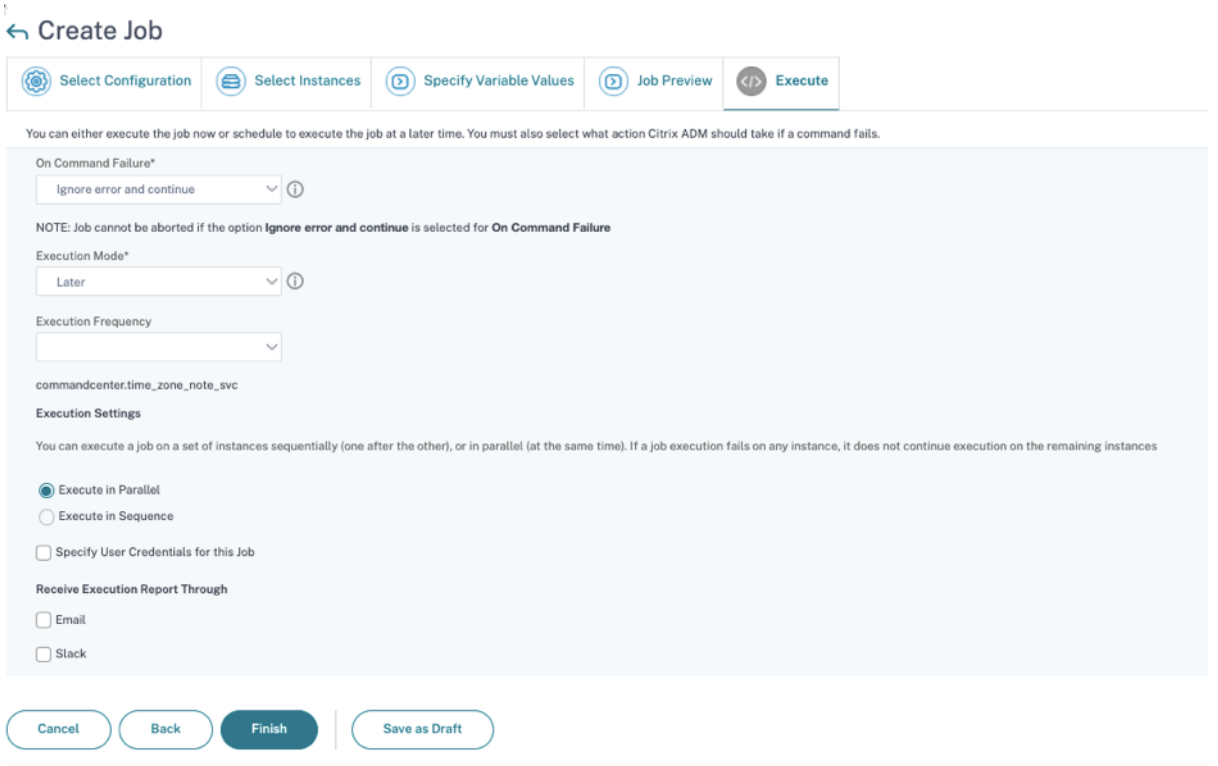
Step 3: Specify variable values No variable is required to specify in this step. Select **Common Variable Values for all instances** and click **Next**.

© 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**.

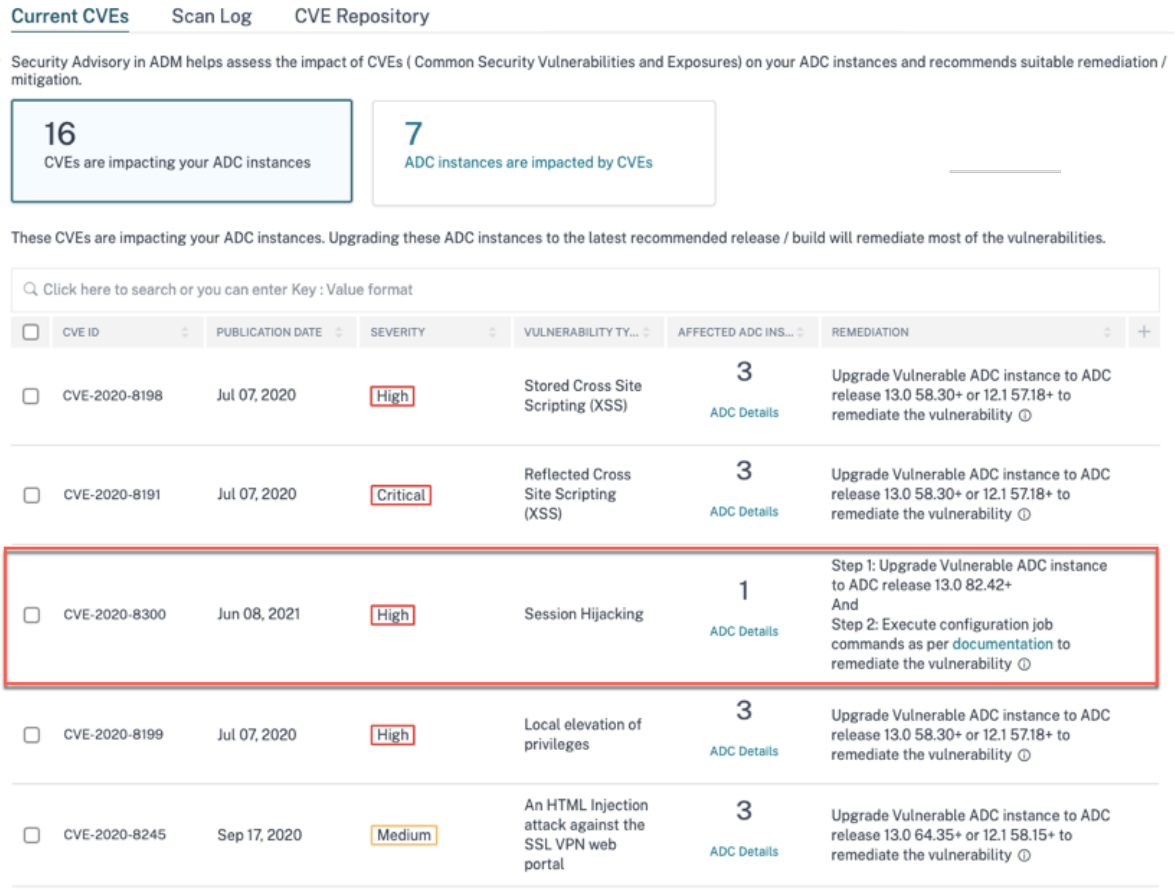
After completing the two remediation steps for all vulnerable NetScaler instances, you can run an on-demand scan to see the revised security posture.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Remediate vulnerabilities for CVE-2020-8300

February 9, 2024

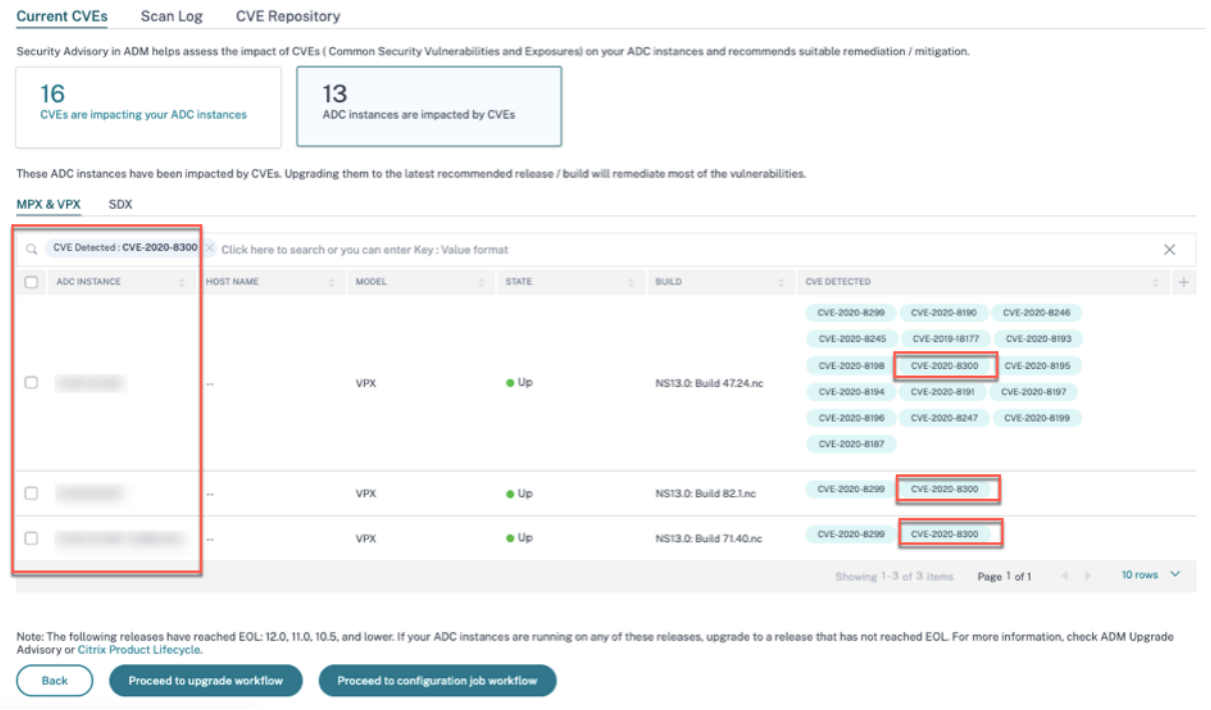
In the NetScaler Console security advisory dashboard, under **Current CVEs > <number of> NetScaler instances are impacted by CVEs**, you can see all the instances vulnerable due to this specific CVE. To check the details of the CVE-2020-8300 impacted instances, select **CVE-2020-8300** and click **View Affected Instances**.



> **Note**
>
> For more information about the security advisory dashboard see, Security Advisory.

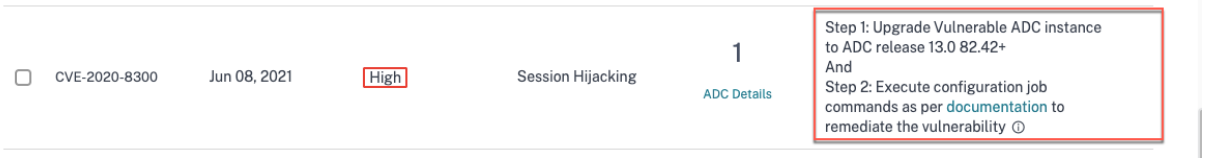
The **<number of> NetScaler instances impacted by CVEs** window appears. Here you see the count and details of the NetScaler instances impacted by CVE-2020-8300.

© 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.

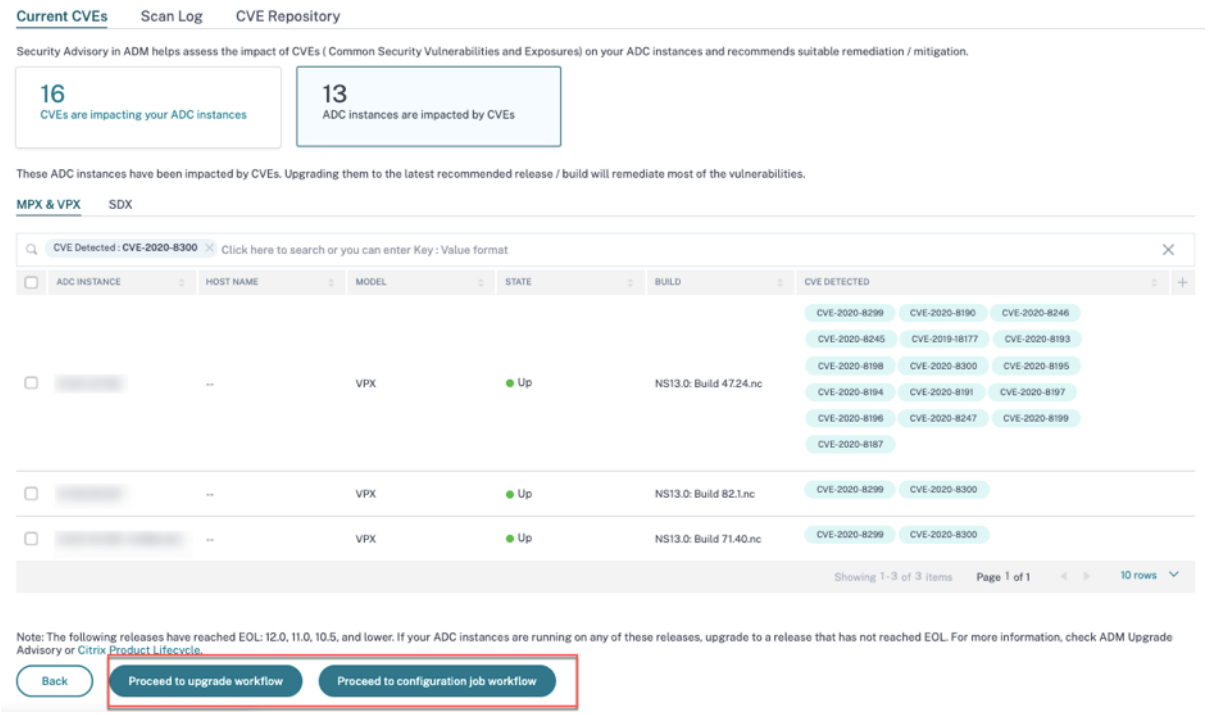


The two steps include:

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.

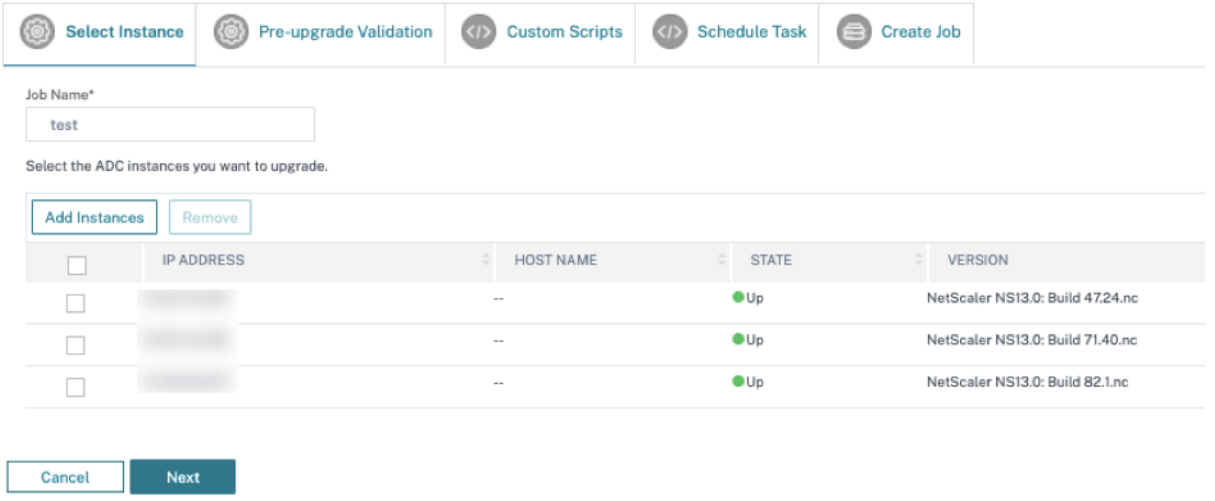
Under **Current CVEs> NetScaler instances impacted by CVEs**, you see two separate workflows for this 2-step remediation process: which are **Proceed to upgrade workflow** and **Proceed to configuration job workflow**.

© 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.

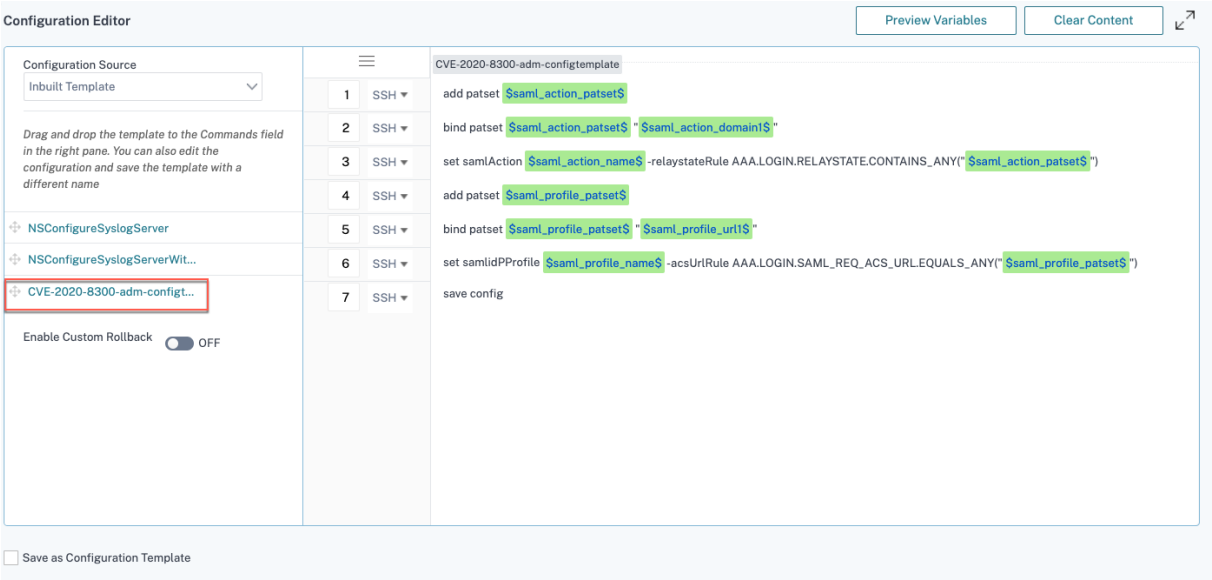
1. Customizing the configuration.
2. Reviewing the auto-populated impacted instances.
3. Specifying inputs for variables for the job.
4. Reviewing the final config with variable inputs populated.
5. Running the job.

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**.
- 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.



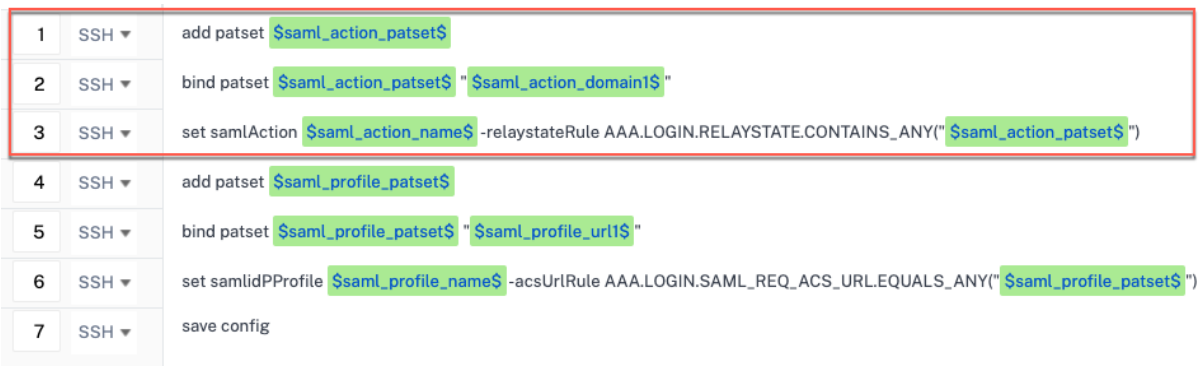
Run a separate configuration job for each impacted NetScaler instance, one at a time, and include all SAML actions and SAML profiles for that NetScaler. For example, if you have two vulnerable NetScaler instances each having two SAML actions and two SAML profiles, you must run this configuration job 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`.

```
> show samlaction -summary
-------------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------
      Name            Username field  Decryption key       Encryption key       Url to be redirected to
                      Reject unsigned assertions Issuer name          Two factor Smart Group
-------------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------
1     SamlSPAct1                      idp_private_public   sp_private_public    https://<IP3>/saml/login
                ON          http://<IP1>          OFF
2     SamlSPAct2                      idp_private_public   sp_private_public    https://[redacted]/saml/login
                ON          http://[redacted]     OFF
 Done
```

b. **SAML profiles and their associated URLs**

Depending on the number of SAML profiles you have in your deployment, replicate lines 4–6. Customize the URLs for each SAML profile.

```
1  SSH  add patset $saml_action_patset$
2  SSH  bind patset $saml_action_patset$ "$saml_action_domain1$"
3  SSH  set samlAction $saml_action_name$ -relaystateRule AAA.LOGIN.RELAYSTATE.CONTAINS_ANY("$saml_action_patset$")
4  SSH  add patset $saml_profile_patset$
5  SSH  bind patset $saml_profile_patset$ "$saml_profile_url1$"
6  SSH  set samlidPProfile $saml_profile_name$ -acsUrlRule AAA.LOGIN.SAML_REQ_ACS_URL.EQUALS_ANY("$saml_profile_patset$")
7  SSH  save config
```

For example, if you have two SAML 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.

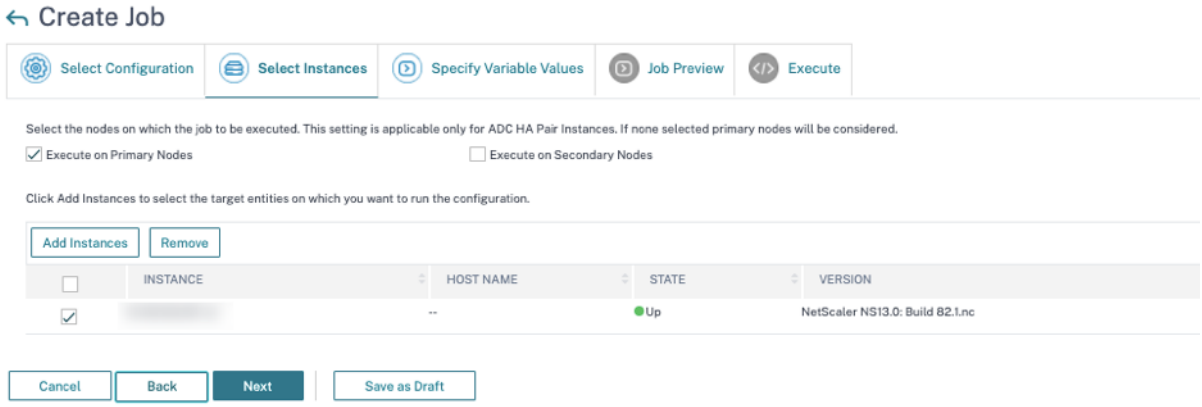
- `saml_profile_patset`: is the config template variable, and it represents the value of the name of the pattern set (patset) for the SAML profile. You can specify the real value in step 3, of the config job workflow. See the section Step 3: Specify variable values in this document.
- `saml_profile_url1`: 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**.



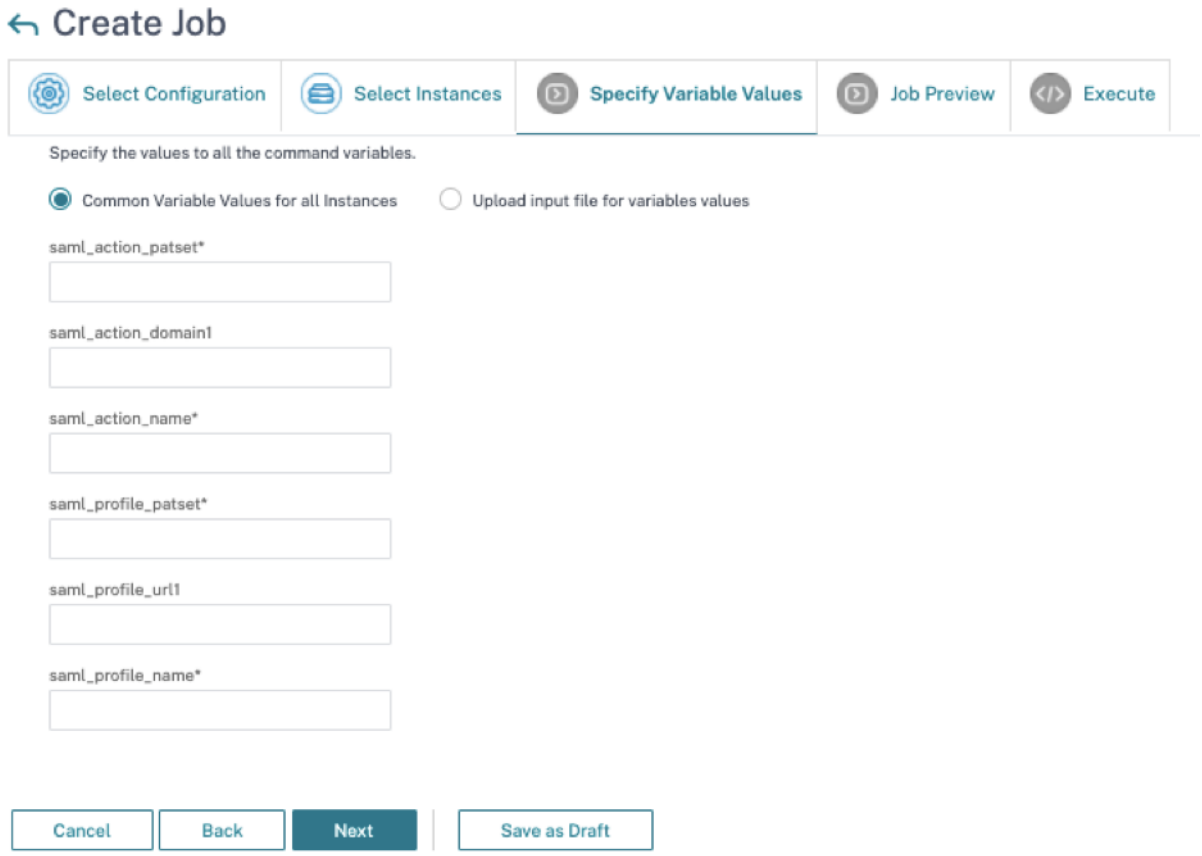
Step 3: Specify variable values Enter the variable values.

- `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

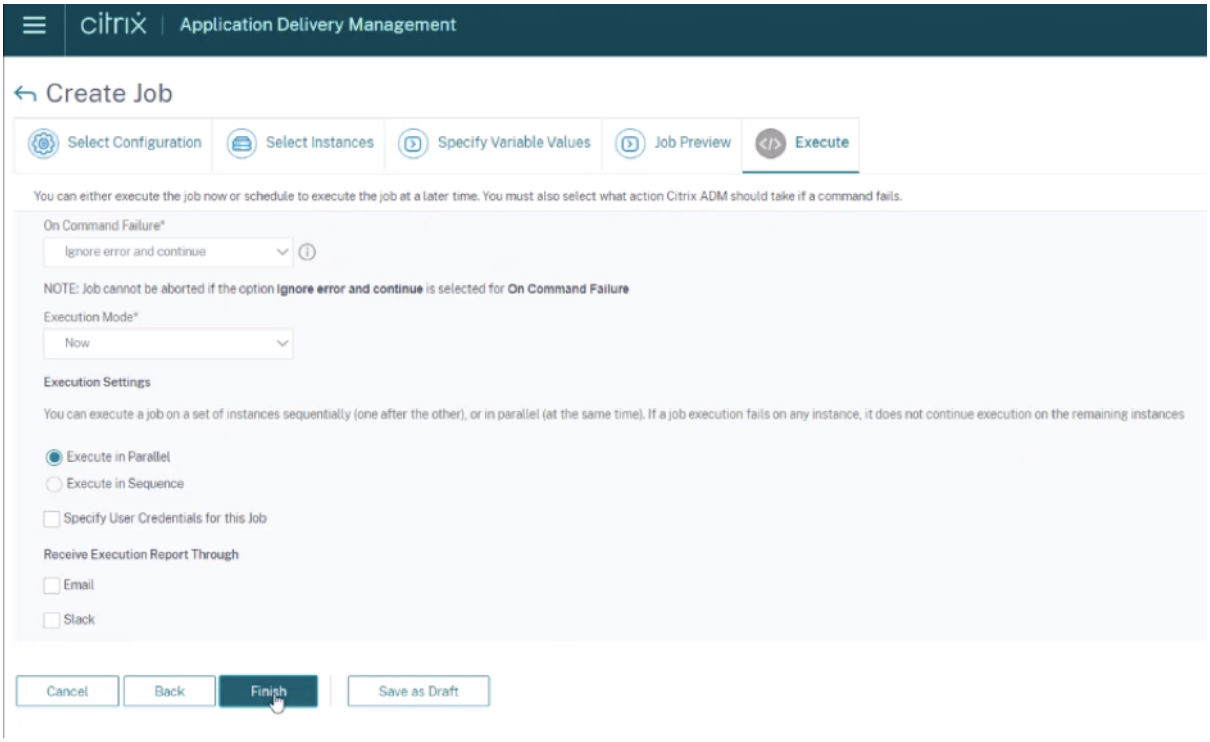
> **Note**
>
> For URLs, the extension is not always `cgi/samlauth`. It depends on what third-party authorization you have, and accordingly you must put the extension.



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.

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.

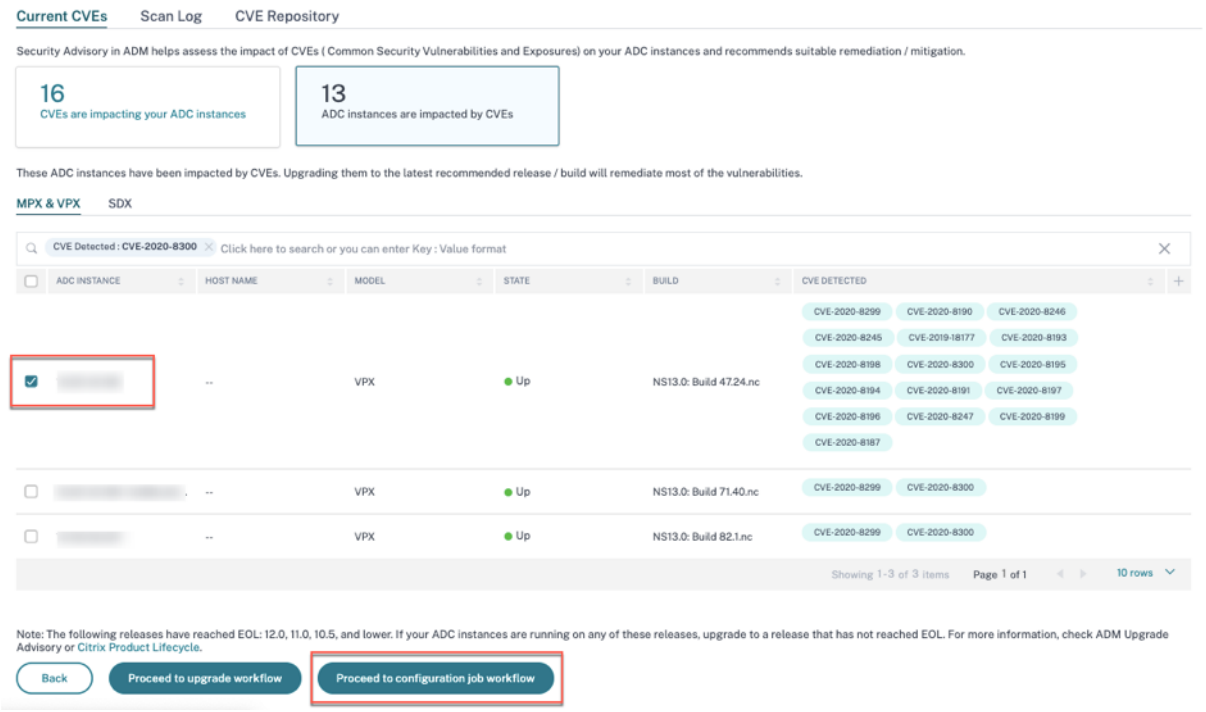
Scenario

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.

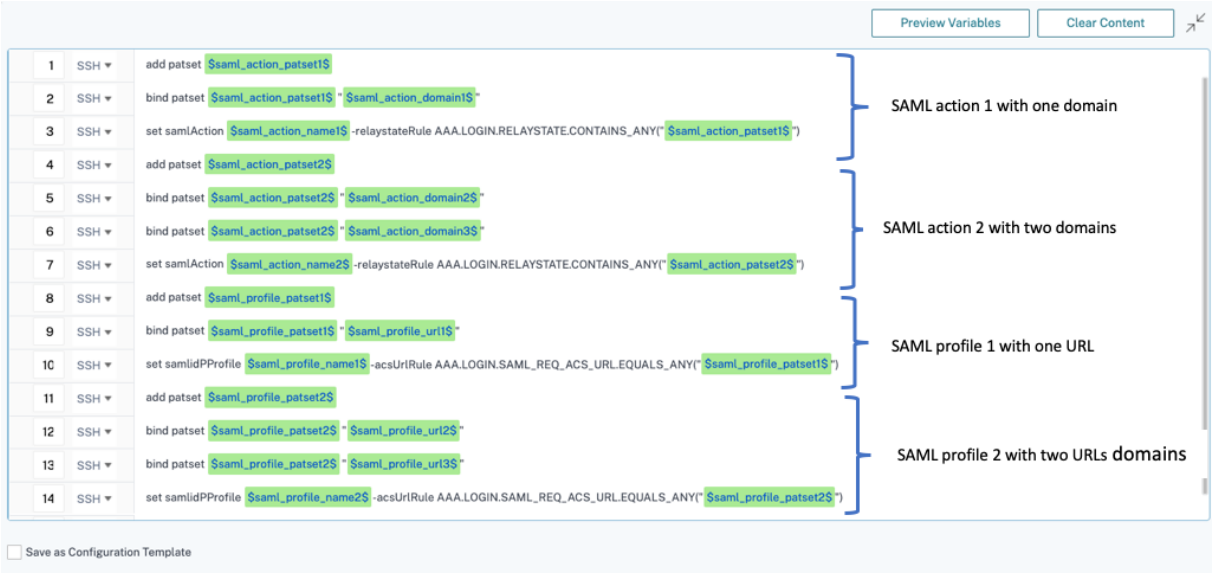
The vulnerable NetScaler 1 has the following configuration:

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.

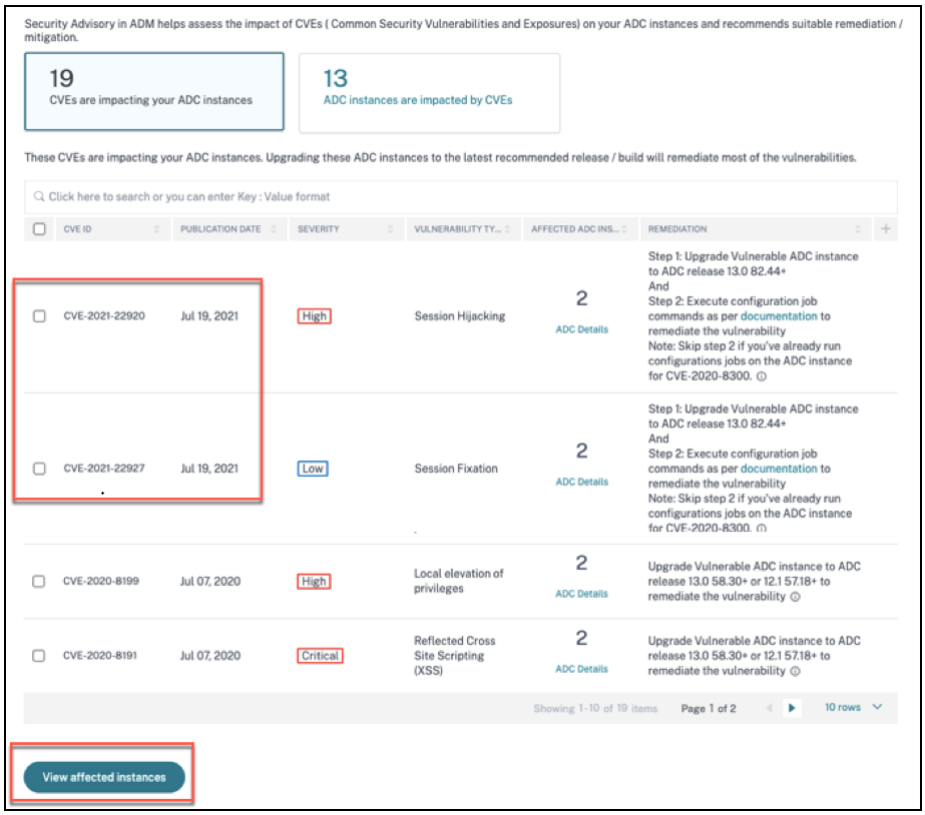
After the job is run, it appears under **Infrastructure > Configuration > Configuration Jobs**.

After completing the two remediation steps for NetScaler1, 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

September 27, 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-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**.

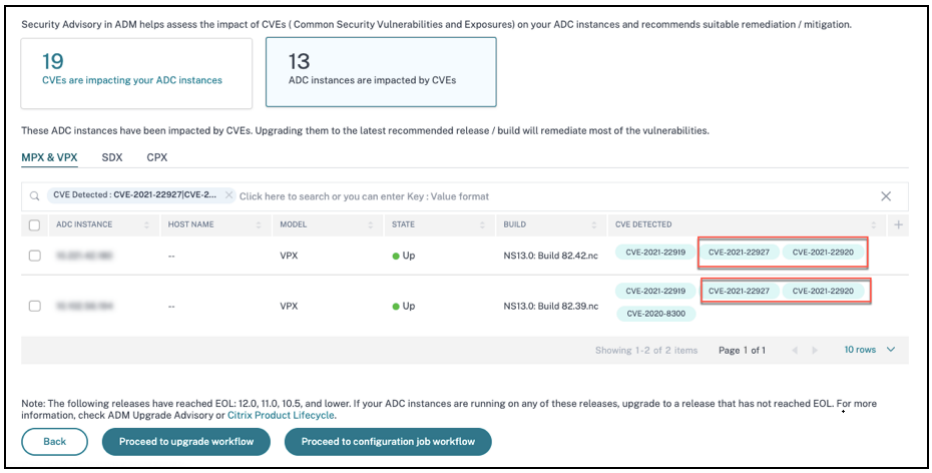


> **Note**
>
> It might take a couple of hours for the security advisory system scan to conclude and reflect

© 1997–2025 Citrix Systems, Inc. All rights reserved.

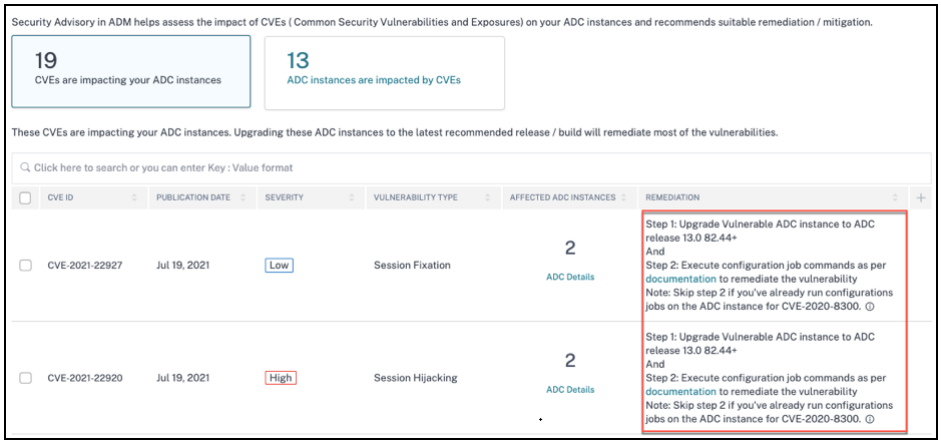
> the impact of CVE-2021-22927 and CVE-2021-22920 in the security advisory module. To see the impact sooner, start an on-demand scan by clicking **Scan-Now**.
>
> For more information about the security advisory dashboard see, Security Advisory.

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.



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:

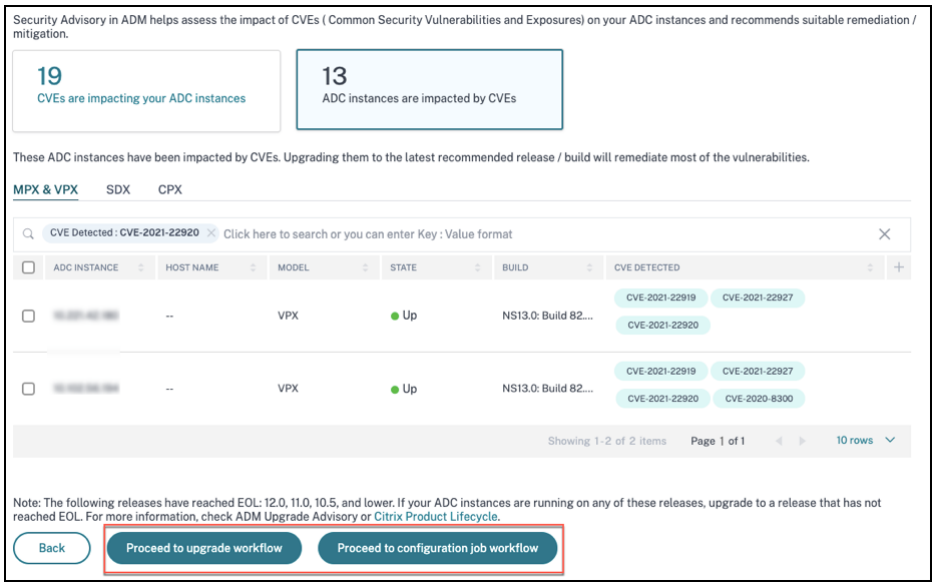
1. Upgrading the vulnerable NetScaler instances to a release and build that has the fix.

© 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.

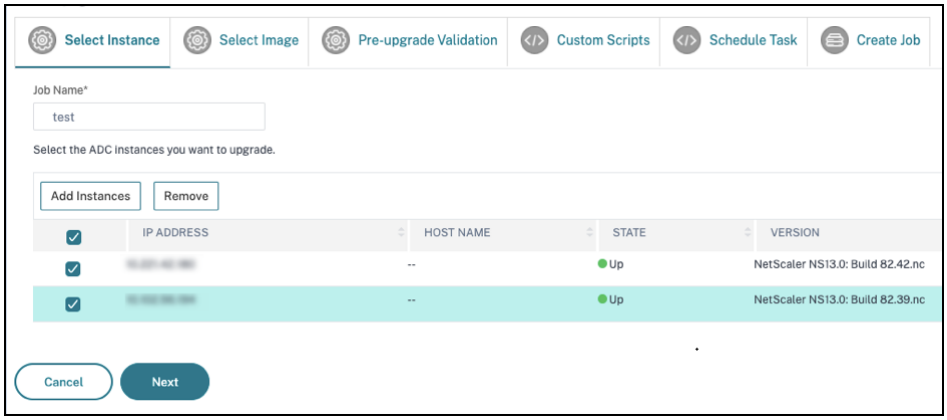
> **Note**
>
> Skip step 2 if you've already run configuration jobs on the NetScaler instance for CVE-2020-8300.

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.

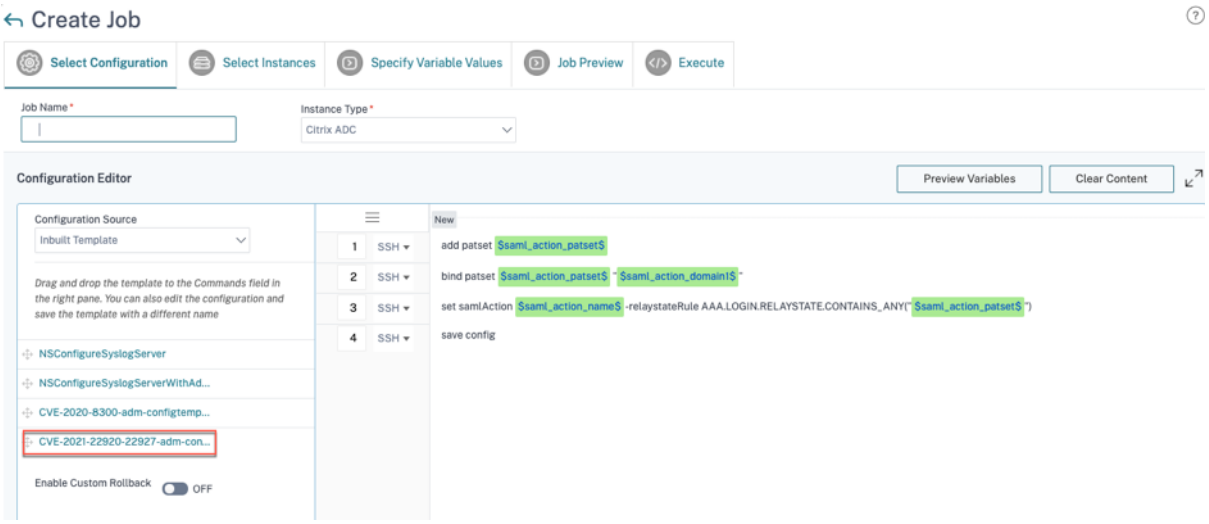
Keep the following points in mind before you select an instance and click **Proceed to configuration job workflow**:

- For a NetScaler instance impacted by multiple CVEs (such as CVE-2020-8300, CVE-2021-22927, CVE-2021-22920, and CVE-2021-22956): when you select the instance and click **Proceed to configuration job workflow**, the built-in configuration template does not auto-populate under Select configuration. Drag and drop the appropriate config job template under **Security Advisory Template** manually to the config job pane on the right side.
- For multiple NetScaler instances that are impacted by CVE-2021-22956 only: you can run config jobs on all instances at once. For example, you've NetScaler 1, NetScaler 2, and NetScaler 3, and all of them are impacted only by CVE-2021-22956. Select all these instances and click **Proceed to configuration job workflow**, and the built-in configuration template auto-populates under **Select configuration**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- For multiple NetScaler instances impacted by CVE-2021-22956 and one or more other CVEs (such as CVE-2020-8300, CVE-2021-22927, and CVE-2021-22920), which require remediation to be applied to each NetScaler at a time: when you select these instances and click **Proceed to configuration job workflow**, an error message appears telling you to run the config job on each NetScaler at a time.

Step 1: Select configuration In the configuration job workflow, the built-in configuration base template auto-populates under **Select configuration**.



> **Note**
>
> If the NetScaler instance selected in step 2 for applying configuration commands, is vulnerable to CVE-2021-22927, CVE-2021-22920, and also CVE-2020-8300, the base template for CVE-2020-8300 is auto-populated. The CVE-2020-8300 template is a super set of the config commands required for all the three CVEs. Customize this base template according to your NetScaler instance deployment and requirement.

You must run a separate configuration job for each impacted NetScaler instance, one at a time, and include all SAML actions for that NetScaler. For example, if you have two vulnerable NetScaler instances each having two SAML actions, you must run this configuration job two times. One time per NetScaler covering all its SAML actions.

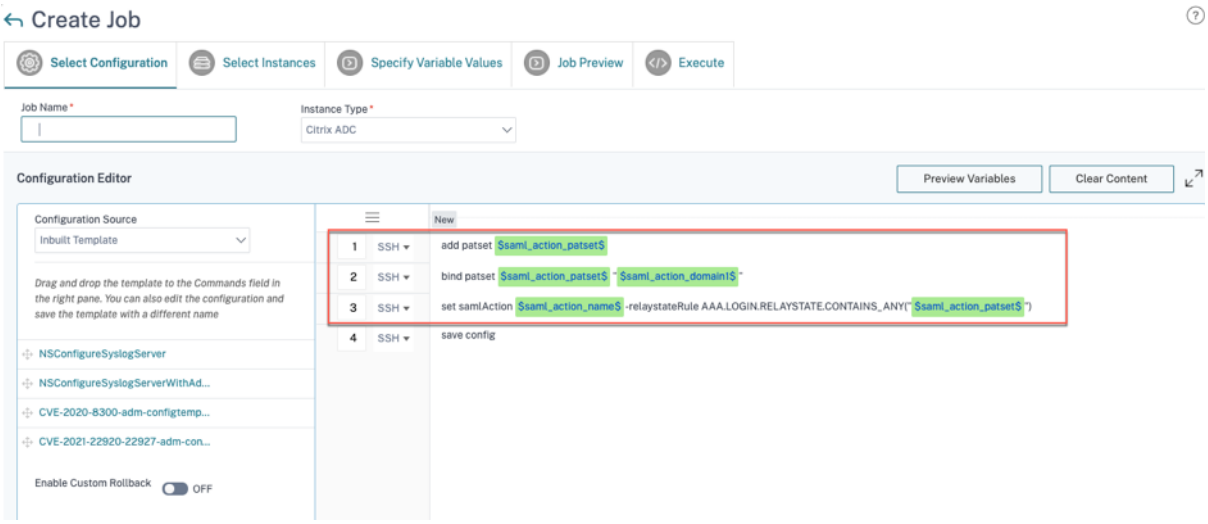
NetScaler 1	NetScaler 2
Job 1: two SAML actions	Job 2: two SAML actions

Give the job a name and customize the template for the following specifications. The built-in configuration template is only an outline or base template. Customize the template based on your deployment for the following requirements:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.
- `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.

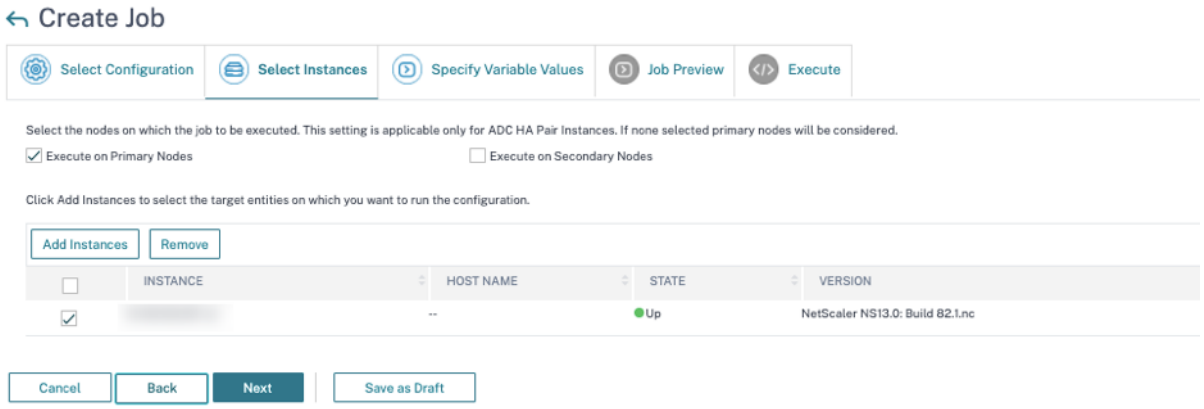
To find all the SAML actions for a device, run the command `show samlaction`.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

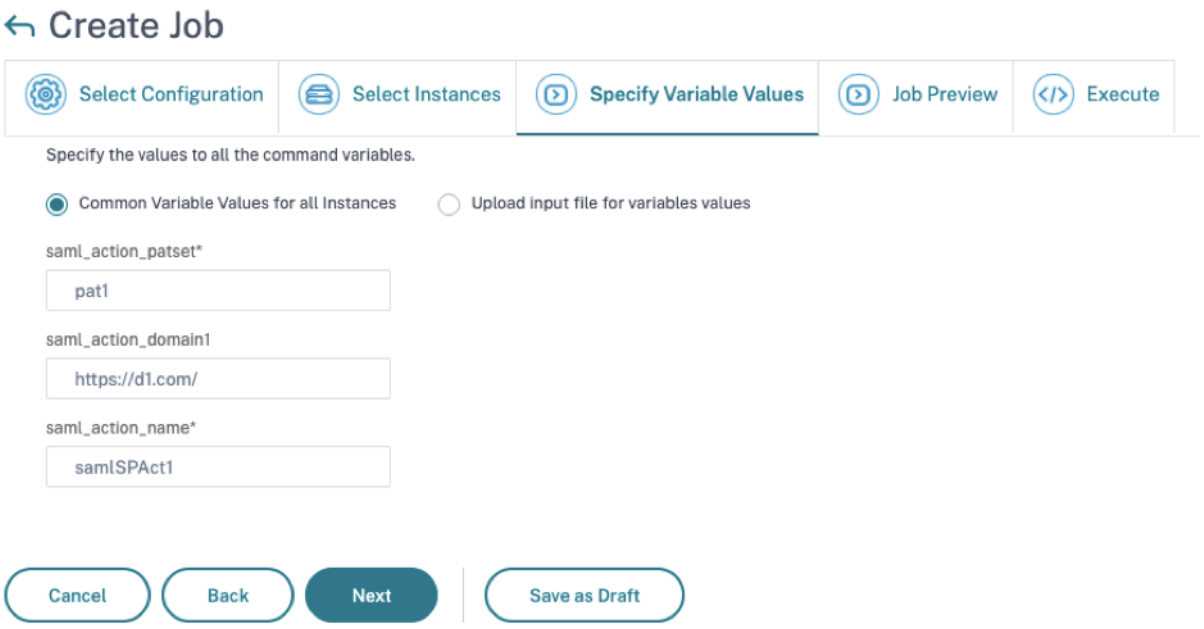
Step 2: Select the instance

The impacted instance is auto-populated under **Select Instances**. Select the instance and click **Next**.



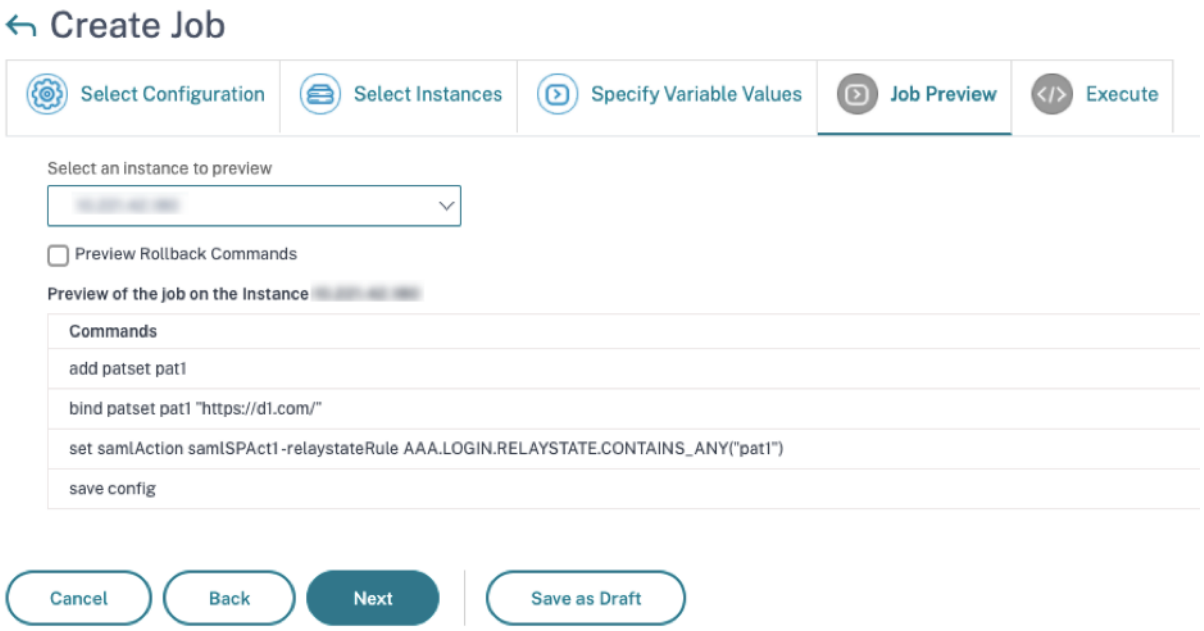
Step 3: Specify variable values Enter the variable values.

- `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

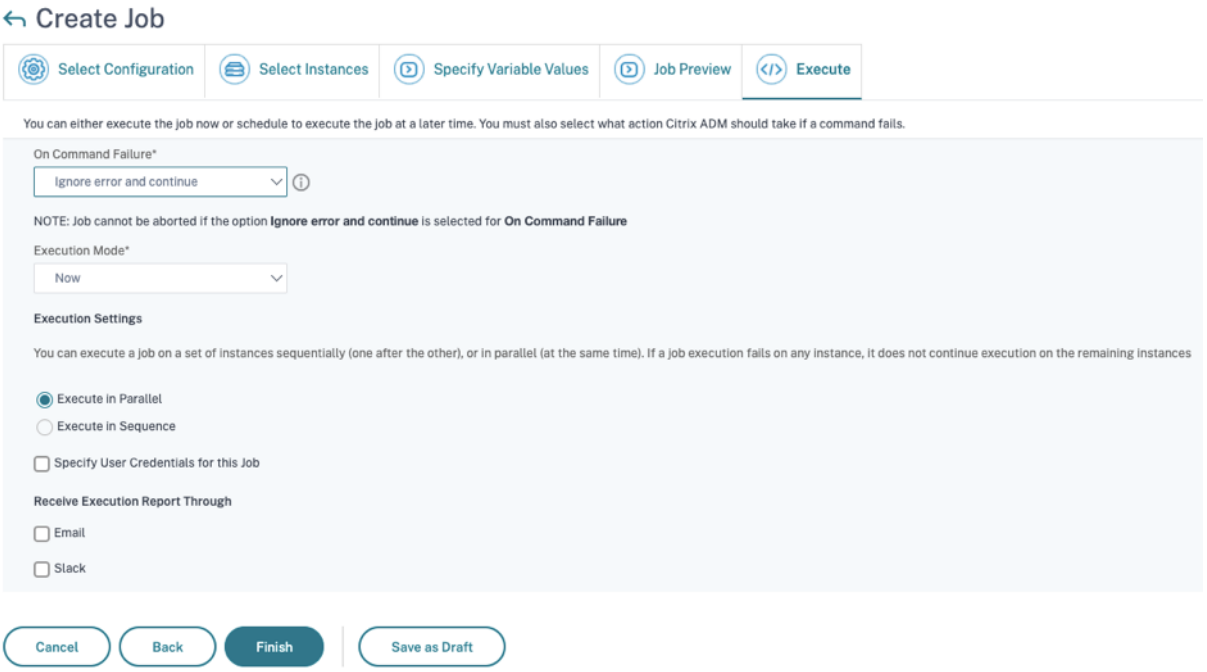


© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.



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.

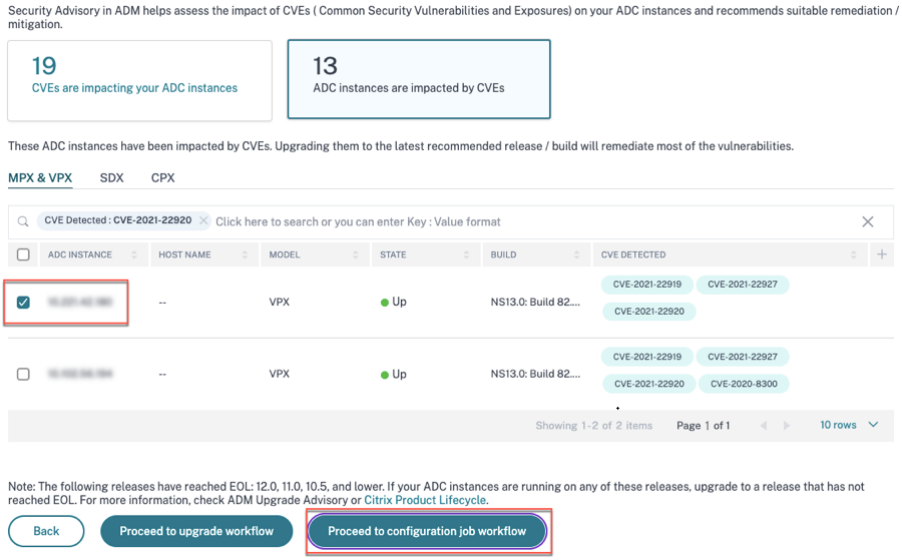
Scenario

In this scenario, two NetScaler instances are vulnerable to CVE-2021-22920, and you need to remediate all the instances. Follow these steps:

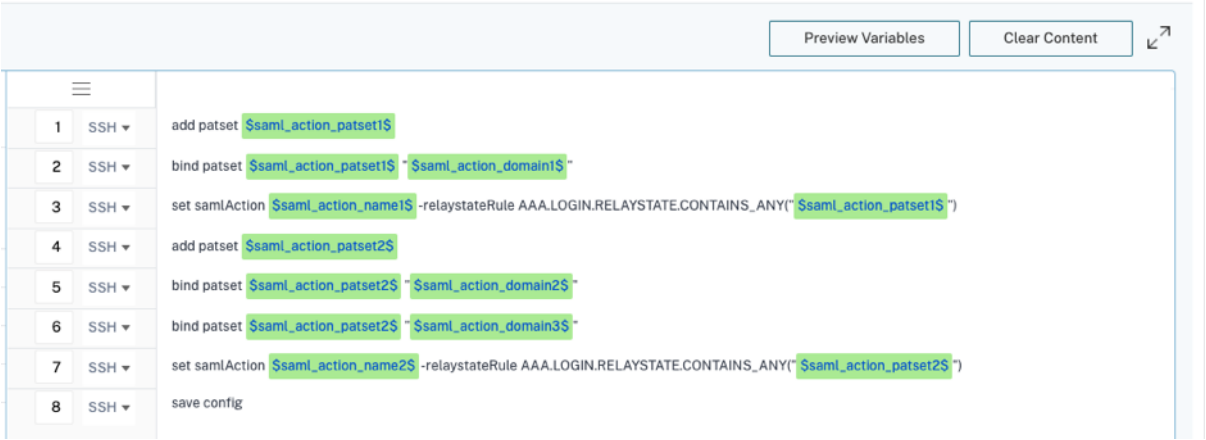
1. Upgrade all the three NetScaler instances by following the steps given in the “Upgrade an instance”section in this document.
2. Apply the config patch to one NetScaler at a time, using the configuration job workflow. See the steps given in the “Apply configuration commands”section in this document.

The vulnerable NetScaler 1 has two SAML actions:

- SAML action 1 has one domain
- SAML action 2 has two domains



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.



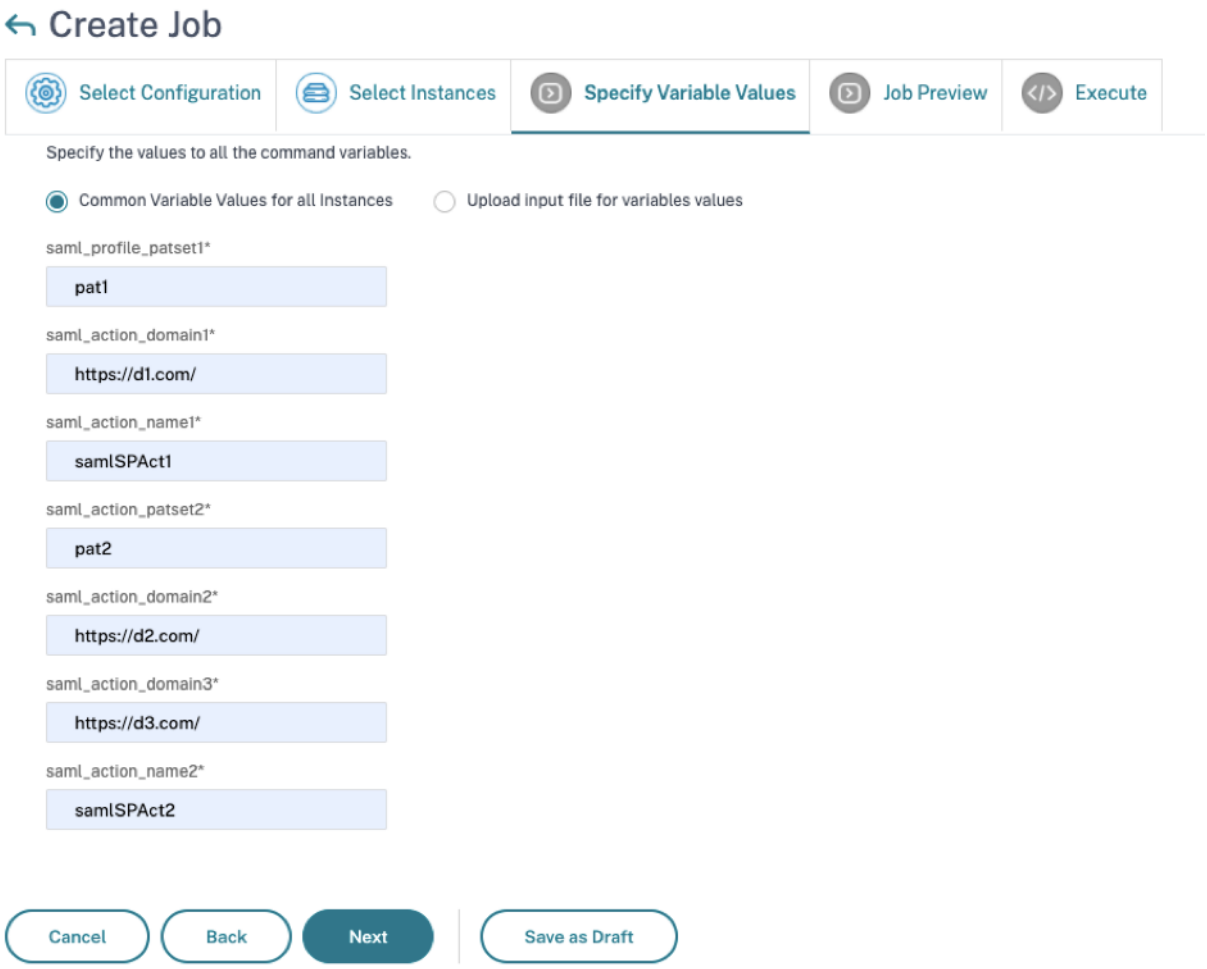
© 1997–2025 Citrix Systems, Inc. All rights reserved.

The following table lists the variable definitions for customized parameters.

Table. Variable definitions for SAML action

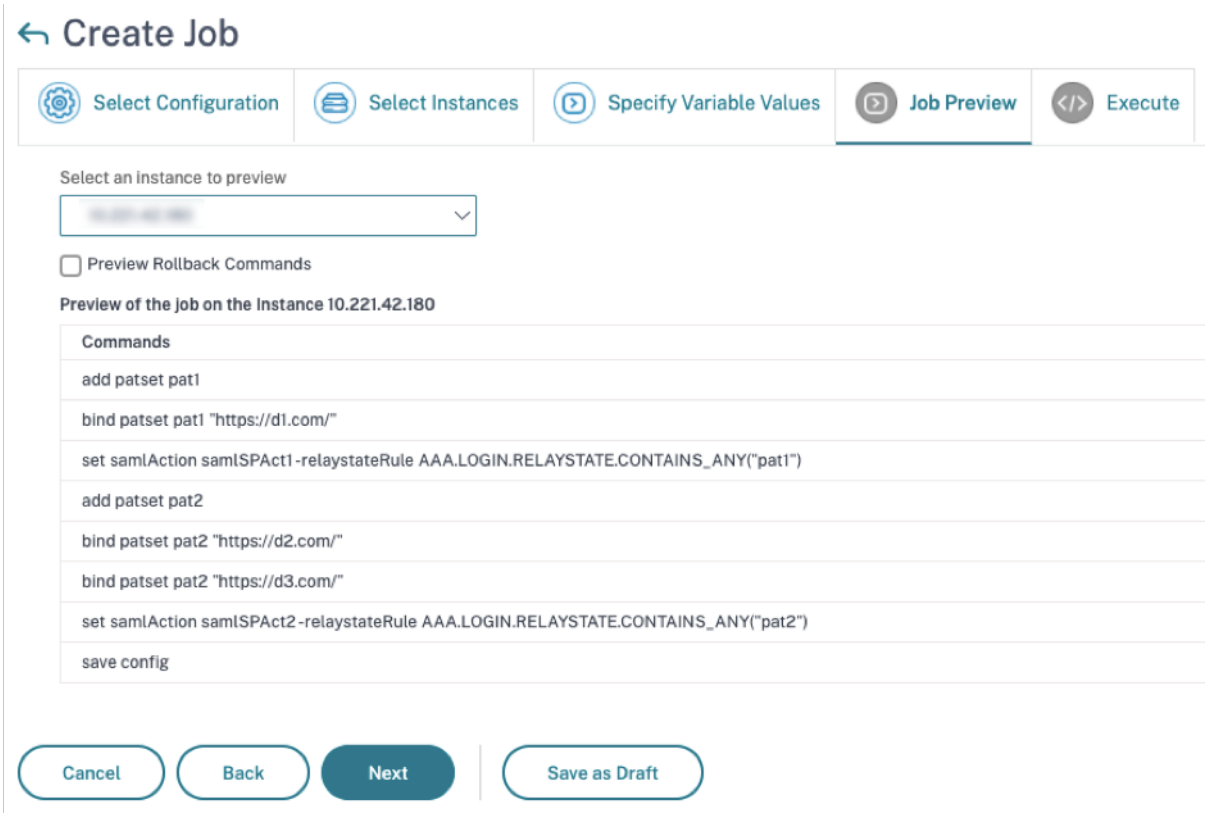
NetScaler configuration	Variable definition for patset	Variable definition for SAML action name	Variable definition for domain
SAML action 1 has one domain	saml_action_patset1	saml_action_name1	saml_action_domain1
SAML action 2 has two domains	saml_action_patset2	saml_action_name2	saml_action_domain2, 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**.

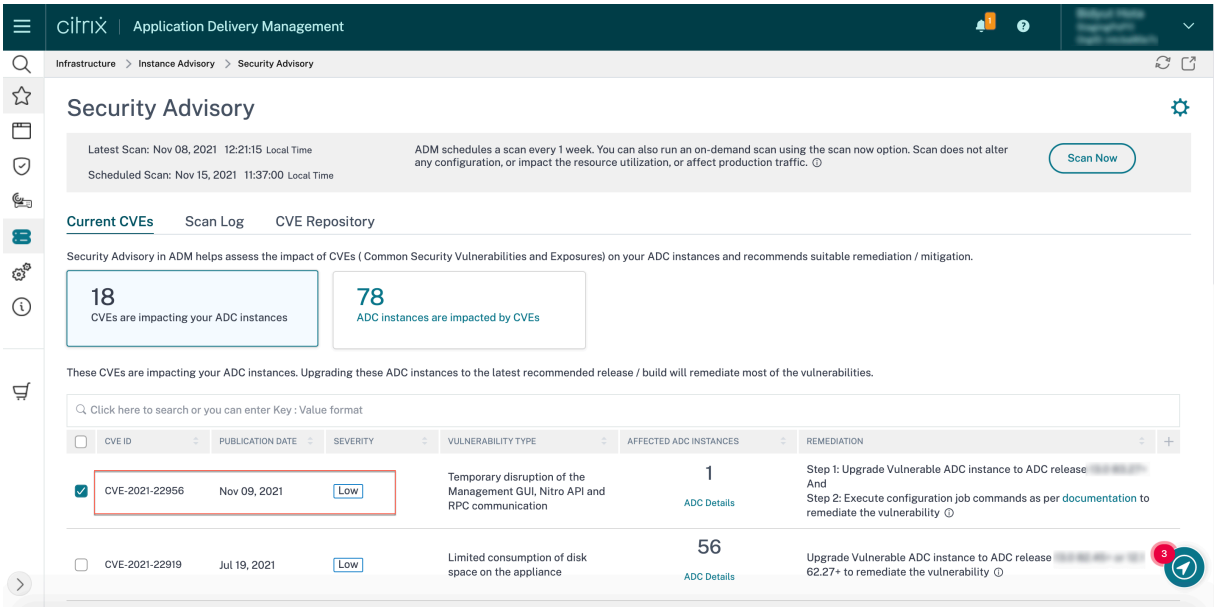
After completing the two remediation steps for NetScaler1, follow the same steps to remediate NetScaler 2 and NetScaler 3. After remediation is complete, you can run an on-demand scan to see the revised security posture.

Identify and remediate vulnerabilities for CVE-2021-22956

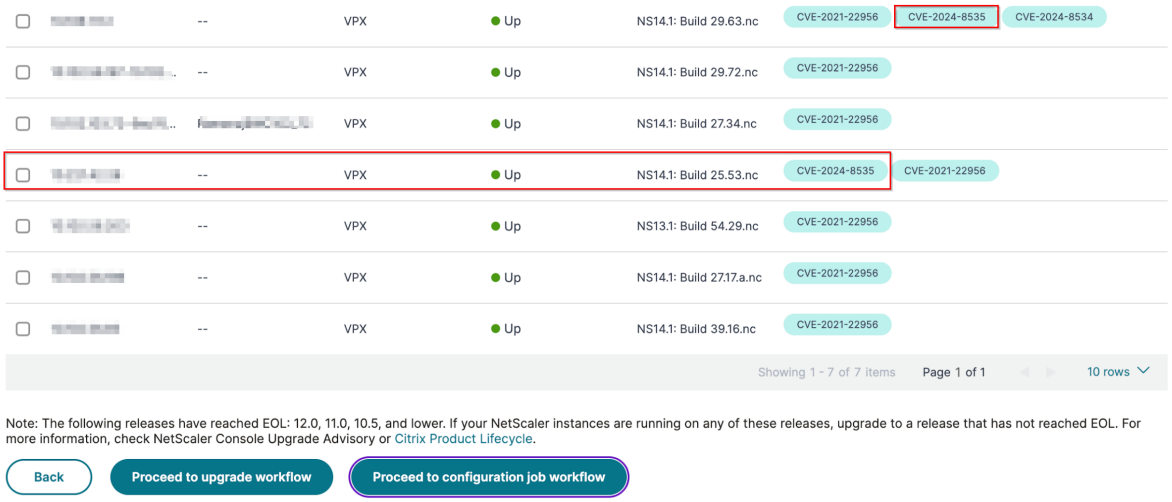
September 27, 2025

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 NetScaler Console service connects with the managed NetScaler instance, pushes a script to the instance. The script runs on the NetScaler instance

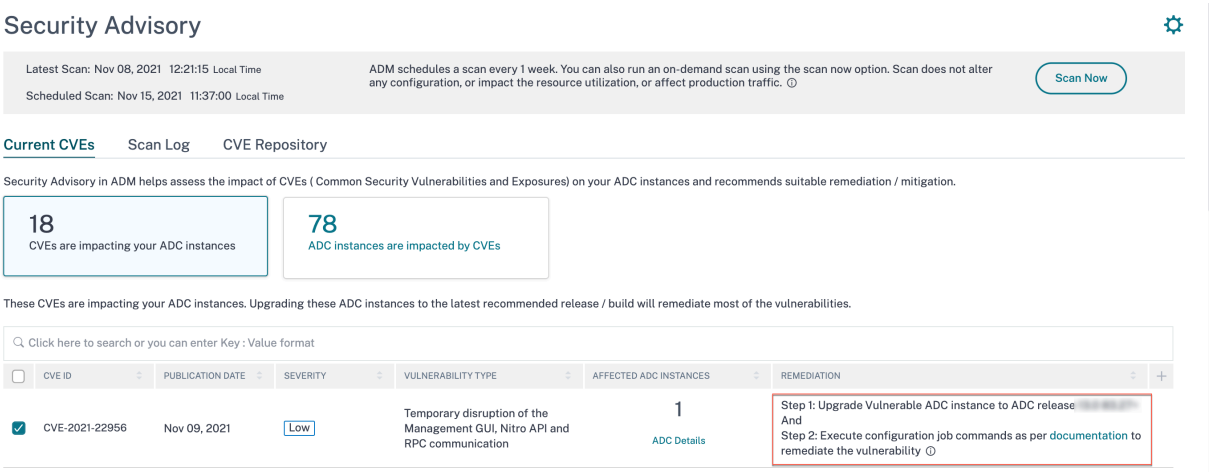
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 service is the vulnerability status in Boolean (true or false). The script also gives back to NetScaler Console service a list of counts for max_clients for different network interfaces, for example local host, NSIP, and SNIP with management access.

This script runs every time your scheduled on on-demand scans run. After the scan is completed, the script is deleted from the NetScaler instance.

Remediate CVE-2021-22956

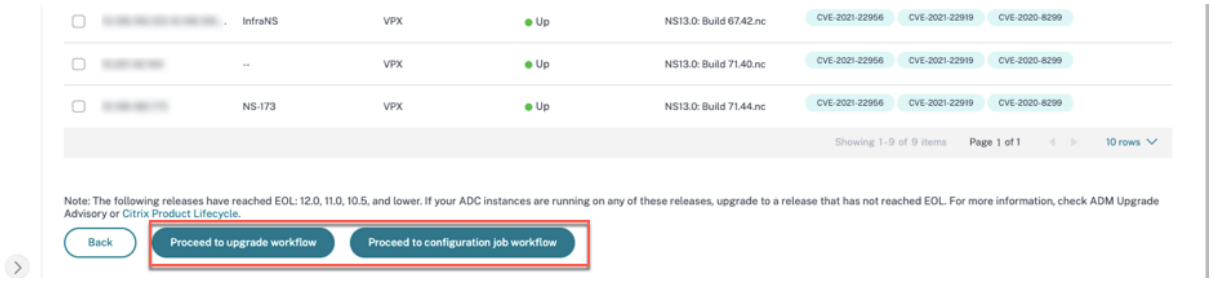
For CVE-2021-22956 -impacted NetScaler instances, the remediation is a two-step process. In the GUI, under **Current CVEs > NetScaler instances are impacted by CVEs**, you can see step 1 and 2.



The two steps include:

1. Upgrading the vulnerable NetScaler instances to a release and build that has the fix.
2. Applying the required configuration commands using the customizable built-in configuration template in configuration jobs.

Under Current CVEs> NetScaler instances impacted by CVEs, you see two separate workflows for this 2-step remediation process: which are Proceed to upgrade workflow and Proceed to configuration job workflow.



© 1997–2025 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.

> **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-2021-2295 and click **Proceed to configuration job workflow**. The workflow includes the following steps.

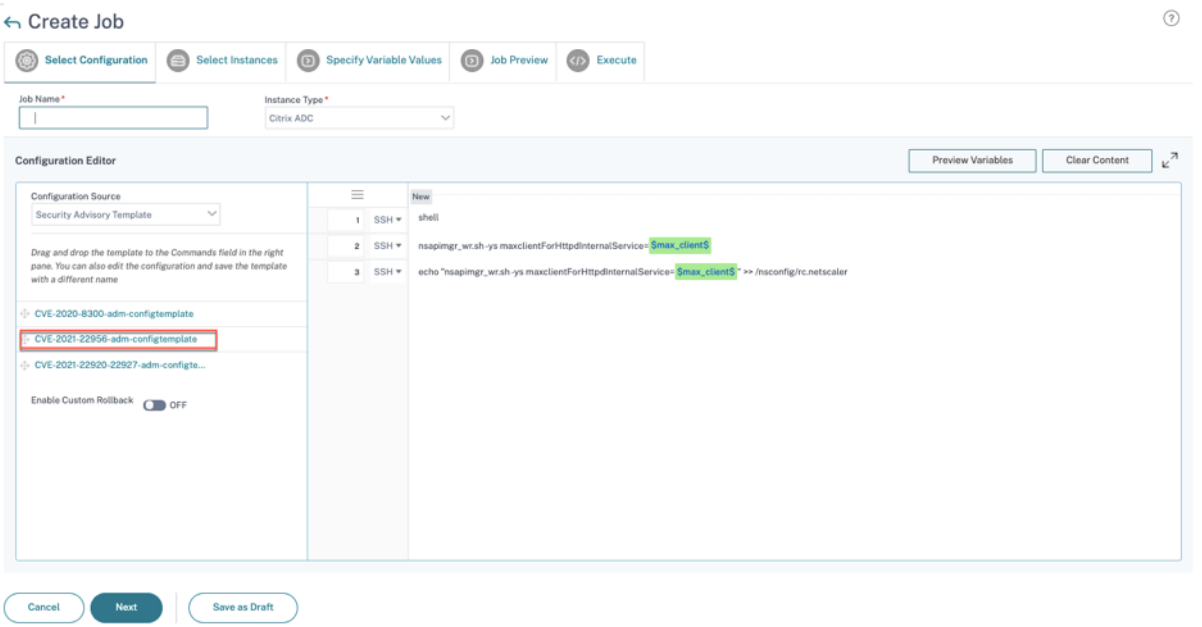
1. Customizing the configuration.
2. Reviewing the auto-populated impacted instances.
3. Specifying inputs for variables for the job.
4. Reviewing the final config with variable inputs populated.
5. Running the job.

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.

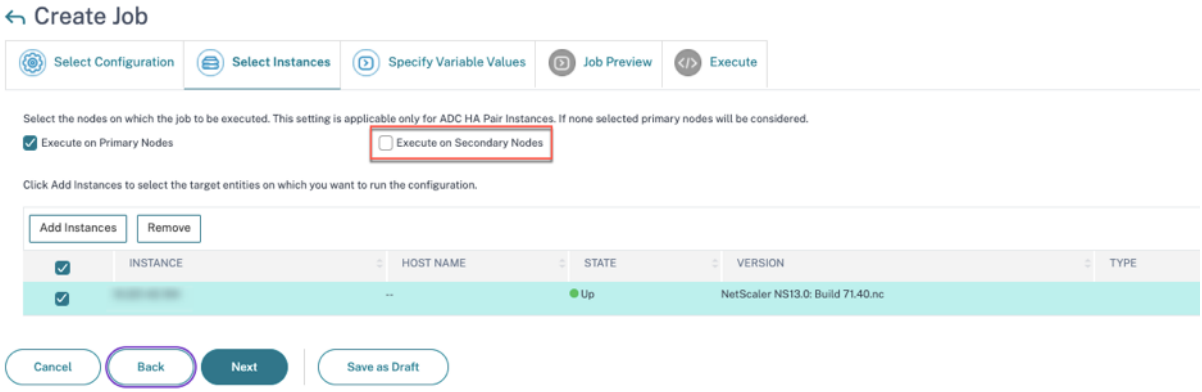
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.

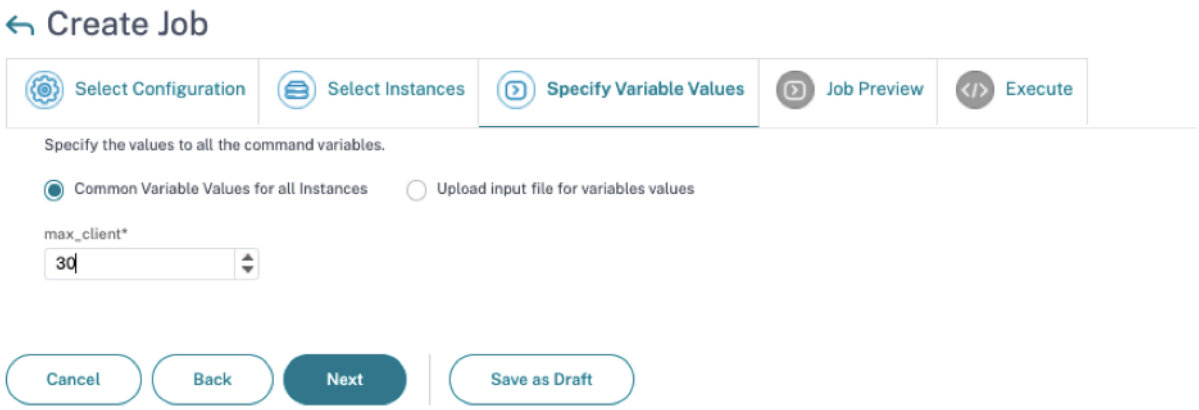


> **Note**
>
> For NetScaler instances in cluster mode, using NetScaler Console security advisory, NetScaler Console supports running the config job only on the cluster configuration coordinator (CCO) node. Run the commands on non-CCO nodes separately.

`rc.netscaler` is synced across all HA and cluster nodes, making the remediation persistent after each restart.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Step 3: Specify variable values Enter the variable values.



Select one of the following options to specify variables for your instances:

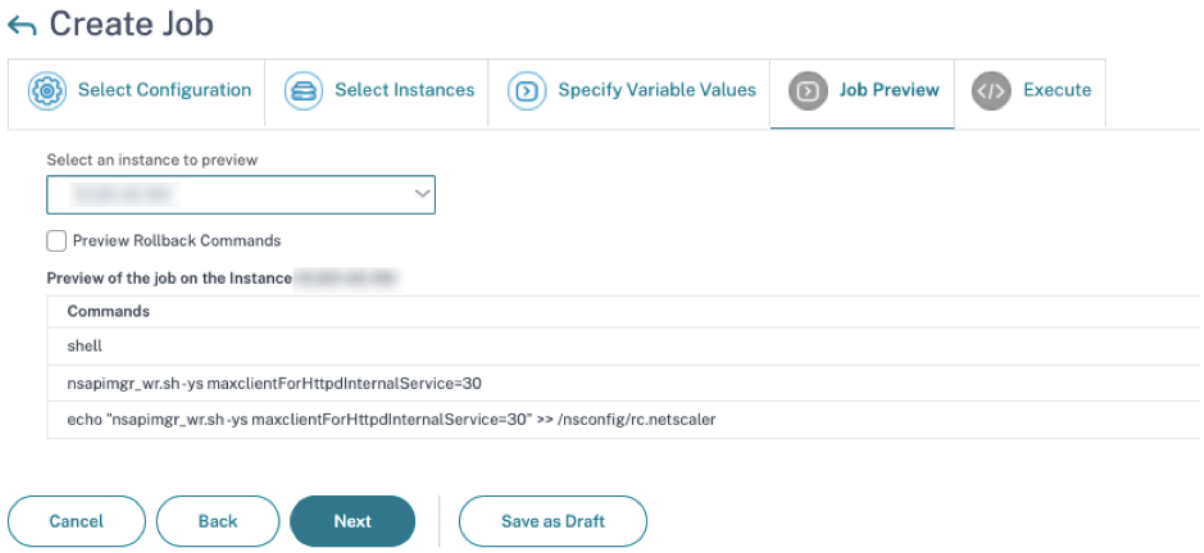
Common variable values for all instances: Enter a common value for the variable `max_client`.

Upload input file for variables values: Click **Download Input Key File** to download an input file. In the input file, enter values for the variable `max_client` and then upload the file to the NetScaler Console server.

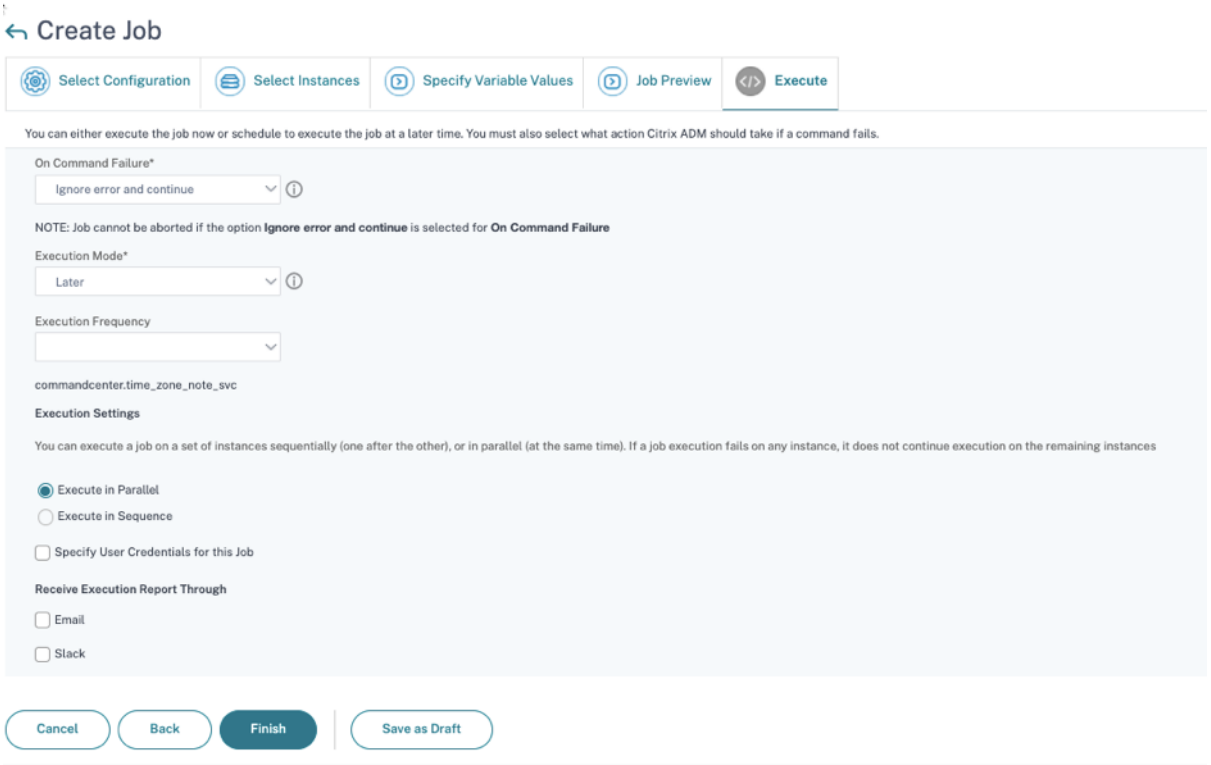
> **Note**
>
> For both options mentioned above, the recommended `max_client` value is 30. You can set the value according to your present value. However, it should not be zero, and it should be less than or equal to the max_client set in the `/etc/httpd.conf` file. You can check the present value set in the Apache HTTP Server configuration file `/etc/httpd.conf` by searching the string `MaxClients`, in the NetScaler instance

Step 4: Preview the configuration Previews the variable values having been inserted in the config and click **Next**.

© 1997–2025 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**.

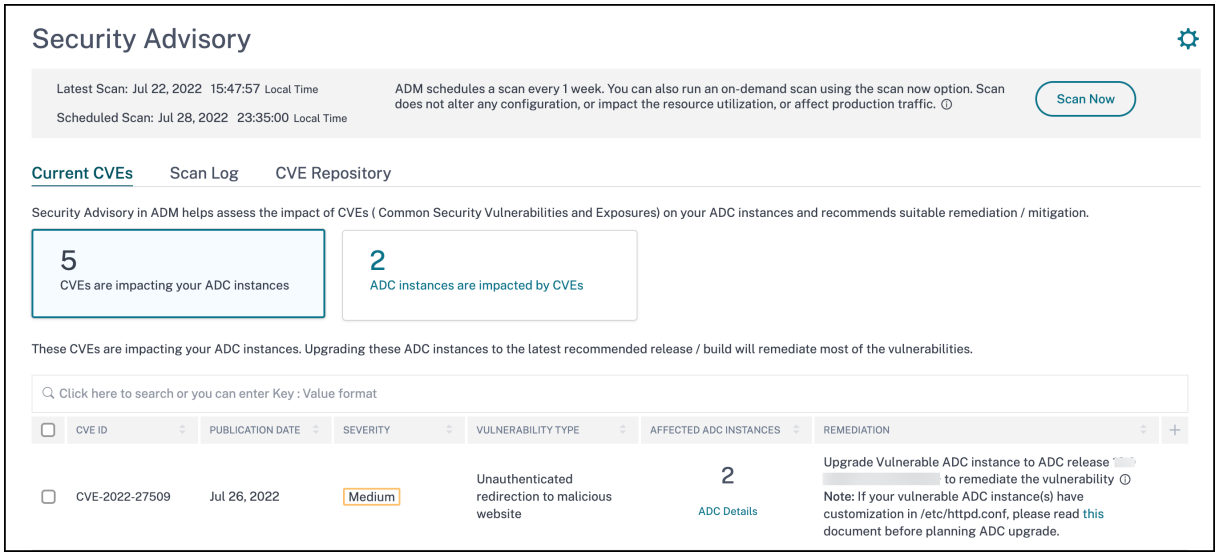
After completing the two remediation steps for all vulnerable NetScaler instances, you can run an on-demand scan to see the revised security posture.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Identify and remediate vulnerabilities for CVE-2022-27509

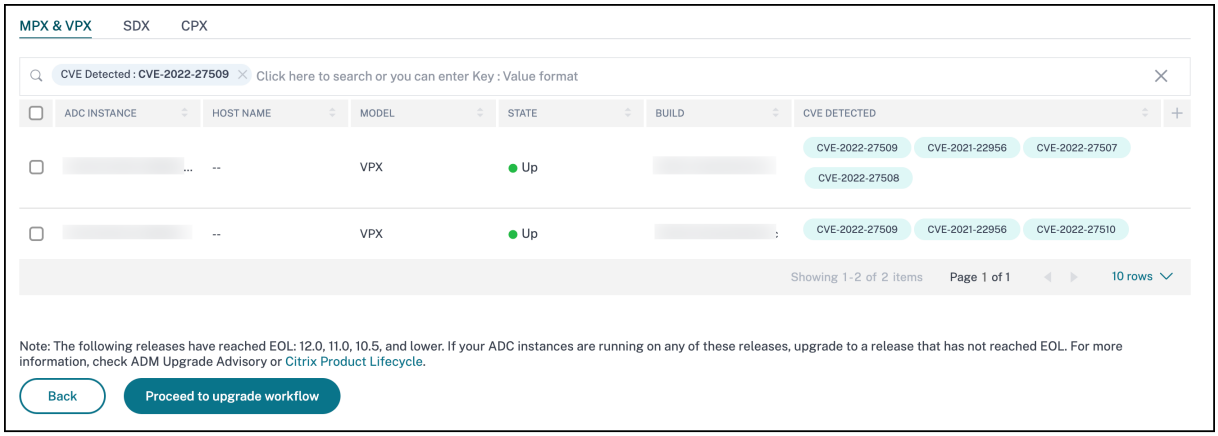
February 9, 2024

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.



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-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, NetScaler Console service connects with the managed NetScaler instance and pushes a script to the instance. The script runs on the NetScaler instance and determines if the instance is vulnerable. This script runs every time your scheduled or on-demand scan runs.

After the scan is completed, the script is deleted from the NetScaler instance.

You can also opt out of these Security Advisory Custom scans. For more information on Custom Scan Settings and opting out of custom scans, see the **Configure Custom Scan settings** section on the **Security Advisory** page.

Remediate CVE-2022-27509

For CVE-2022-27509 impacted NetScaler instances, the remediation is a single step process and you need to upgrade the vulnerable NetScaler instances to a release and build that has the fix. In the GUI, under **Current CVEs > NetScaler instances are impacted by CVEs**, you can see the step to remediate.

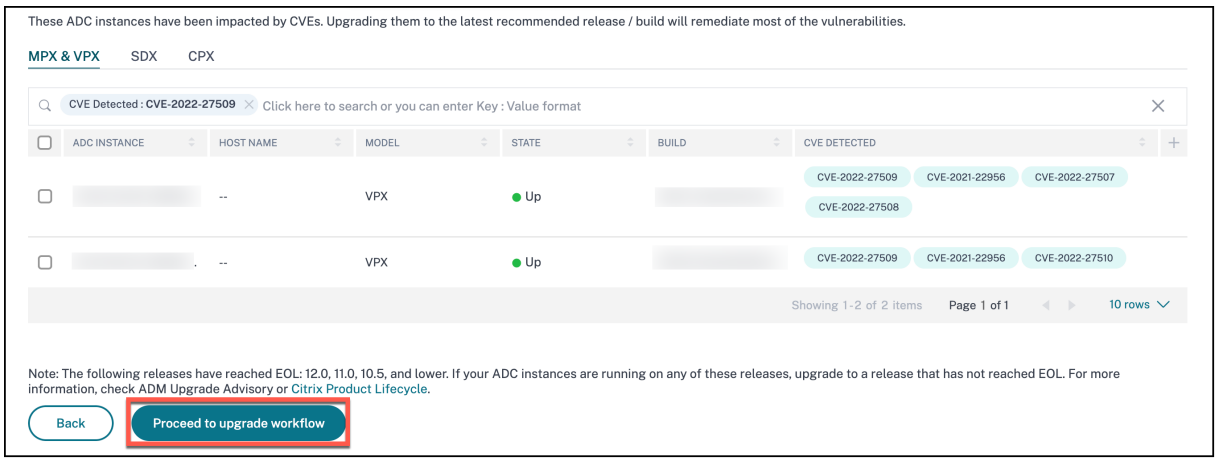
Under **Current CVEs> NetScaler instances impacted by CVEs**, you see the following workflow for this single step remediation process, which is **Proceed to upgrade workflow**.

To upgrade the vulnerable instances, select the instances and click **Proceed to upgrade workflow**. The upgrade workflow opens with the vulnerable NetScaler instances already populated.

> **IMPORTANT**
>
> If your vulnerable NetScaler instance(s) 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.



Unsupported CVEs in Security Advisory

September 27, 2025

NetScaler Console security advisory tracks all the new Common Vulnerabilities and Exposures (CVEs) and assesses the impact of CVEs on the infrastructure. You can review the recommendations and take appropriate actions. However, there are a few CVEs that are not supported and the detection and remediation of the vulnerabilities are out of NetScaler Console Security Advisory scope.

- **CVE-2022-21827**:

  CVE-2022-21827 impacts NetScaler Gateway plug-in for Windows supported versions prior to 21.9.1.2.

  The detection and remediation of vulnerabilities impacting the NetScaler Gateway plug-in for Windows is not supported by the NetScaler Console. Also, NetScaler Gateway plug-in vulnerabilities cannot be assessed by performing any checks on NetScaler side, verifying the NetScaler version, or by checking the NetScaler configuration. The detection & remediation for this CVE can only be assessed based on the version of the NetScaler Gateway plug-in for Windows deployed on the client.

  As a result, the detection and remediation of this vulnerability is out of NetScaler Console Security Advisory scope.

Upgrade Advisory (Preview)

October 7, 2025

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Upgrade Advisory is no longer supported starting from **14.1-25.x** build.

As a network administrator, you might manage many NetScaler instances running on different NetScaler builds 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 have reached the End of Life (EOL) or End of Maintenance (EOM). Then, plan their upgrade.

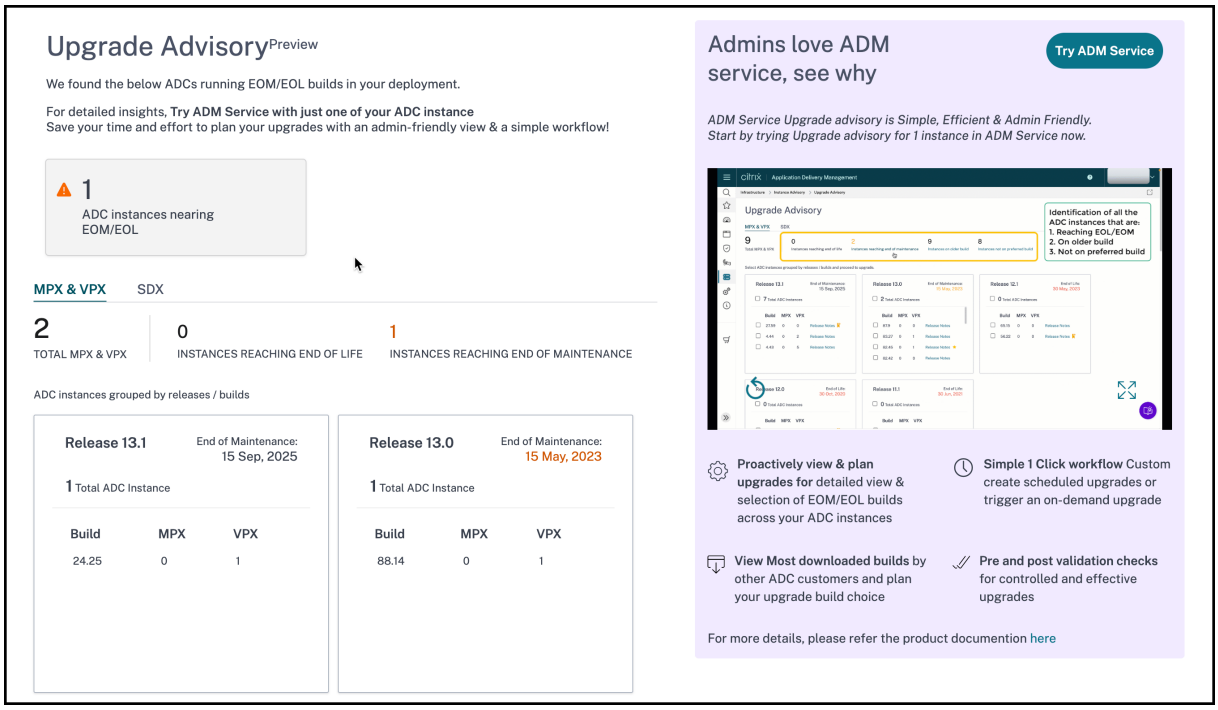
NetScaler Console on-premises Upgrade Advisory performs a version scan on the NetScaler instances and provides a view of the EOM/EOL builds across your NetScaler instances.

> **IMPORTANT**
>
> For detailed insights, and the workflow to upgrade the NetScaler instances, **try NetScaler Console Service**.

View upgrade advisory

Navigate to **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.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

The **Upgrade Advisory** page groups the NetScaler instances by their releases.

NetScaler Console on-premises upgrade advisory also allows you to select one of the NetScaler instances, and onboard the NetScaler instance to NetScaler Console service. Click **Try NetScaler Console service** and onboard the NetScaler instance to NetScaler Console service. NetScaler Console service Upgrade Advisory provides you the workflow to upgrade by selected NetScaler instance.

For more information on the NetScaler Console service Upgrade Advisory, view the gif animation on the **Upgrade advisory** page.

Orchestration

September 27, 2025

In Software Defined Networking (SDN), a software application controller manages a network and its activities instead of hardware that supports the network. That is, SDN allows the network administrators to virtualize a physical network connectivity into a logical network connectivity and manage network services using a software based centralized management tool. SDN allows network engineers and administrators to respond to rapidly changing business requirements.

While the better known advantages of SDN are traffic programmability, greater agility, the ability to create policy driven network supervision, and implementing network automation, some of the specific advantages of SDN are listed below:

- Centralized network provisioning
- Increased network security at granular level
- Reduced operating costs
- Increased levels of cloud abstraction
- Guaranteed content delivery
- Reduced network downtime

NetScaler Console supports SDN in enterprises network by integrating with SDN controllers of different vendors. NetScaler Console supports both VMware NSX Manager and Cisco Application Policy Infrastructure Controller (APIC).

VMware NSX Manager

NetScaler Console integrates with VMware network virtualization platform to automate the deployment, configuration, and management of NetScaler services. This integration abstracts away the tra-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

ditional complexities associated with physical network topology, enabling vSphere/vCenter administrators to programmatically deploy NetScaler services faster.

VMware NSX Manager exposes logical firewalls, switches, routers, ports, and other networking elements to allow virtual networking among diverse hypervisors, cloud management systems, and associated network hardware. It also supports external networking, and security services.

The Cloud Orchestration feature of NetScaler Console enables the integration of NetScaler products with VMware NSX, and provides the following capabilities:

- Ability to allocate a pre-provisioned VPX on-demand to a certain Edge gateway as part of service insertion.
- Ability to configure advanced features of NetScaler such as SSL and CS along with basic load balancing through application templates on the instances that are running inside NSX environment.
- Ability to de-allocate a VPX from a certain Edge gateway as part of service deletion and reallocate the same VPX for another Edge gateway.
- Ability to rapidly deploy NetScaler functions from the vCenter console as part of the deployment workflow of all the infrastructure required for an application.

Benefits:

- Automated, on-demand allocation of new NetScaler services as part of an application deployment workflow
- Simplified configuration of application specific, advanced NetScaler functionality through application templates
- Multitenant separation-of-duties and a self-service consumption model while providing cloud administrators a single point of control
- Easier integration with NetScaler Console API's, which help to support unanticipated future uses.

For more information on how to configure VMware NSX Manager on NetScaler Console, see Integrating NetScaler Appliances with VMware NSX Manager.

OpenStack: Integrating NetScaler instances

September 27, 2025

The Cloud Orchestration feature of NetScaler Console enables integration of NetScaler products with OpenStack platform. By using this feature with OpenStack platform, the OpenStack users are able to

© 1997–2025 Citrix Systems, Inc. All rights reserved.

avail the load balancing feature (LBaaS) of the NetScaler. After this, the OpenStack users can deploy their load balancer configurations from OpenStack in NetScaler instance.

The following sections provide a brief description of the features in NetScaler Console and OpenStack integration workflow.

NetScaler Driver for OpenStack Neutron LBaaS

OpenStack Neutron LBaaS plug-in includes a NetScaler driver that enables OpenStack to communicate with the NetScaler Console. OpenStack uses this driver to forward any load balancing configuration done through LBaaS APIs, to the NetScaler Console, which creates the load balancer configuration on the desired NetScaler instances. OpenStack also uses the driver to call NetScaler Console at regular intervals to retrieve the status of different entities (such as VIPs and Pools) of all load balancing configurations from the NetScalers. NetScaler driver software for OpenStack platform is bundled along with the NetScaler Console. To download and install the drivers, you have to first install NetScaler Console and launch the application.

Registering NetScaler Console and OpenStack with each other

You have to first register OpenStack information on the NetScaler Console. Specify the OpenStack controller IP address and cloud administrative user credentials, and also the OpenStack NetScaler driver user credentials. You can later specify the same login credentials in the NetScaler_driver section of the Neutron configuration file (neutron.conf) so that NetScaler driver in OpenStack can connect to NetScaler Console during LB configurations.

After OpenStack and NetScaler Console are registered with each other, both can talk to each other. Also, OpenStack users can use their existing credentials in OpenStack to log on to the NetScaler Console user interface to check how their LB configurations are performing in NetScalers.

Tenants in OpenStack

In OpenStack a tenant is also called a project. A tenant is a group of users; a tenant or a project can also be defined as a set of resources (compute, network, storage, and so on) assigned to an isolated group of users.

Placement policies

Placement policies provide the flexibility to decide on the NetScaler instance that is used in each load balancer configuration created by users. Alternatively, the NetScaler Console also provides an option to assign a NetScaler instance based on OpenStack tenants.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Service packages

Service packages are bundles that tie together policies/SLAs, devices or auto-provision configuration specifications, and tenants/placement-policies. A service package is usually defined in terms of the isolation policies that are provided to the tenant.

The following are some points related to service packages:

- A tenant cannot be part of more than one service package.
- Multiple tenants can be associated with the same service package.
- In a service package that is set for auto-provisioning, virtual NetScaler instances can be created from only one platform type (on SDX platform or on OpenStack Compute platform).

Features Supported on LBaaS V1 and LBaaS V2

While LBaaS V1 driver in OpenStack supports operations from OpenStack Horizon user interface, LBaaS V2 driver supports only command line operations.

The following list shows the features supported on both LBaaS V1 and LBaaS V2 on OpenStack:

- LBaaS V1
    - Load Balancing
- LBaaS V2
    - Load Balancing
    - SSL Offload with certificates managed by **Barbican**, the Key Manager in OpenStack
    - Certificate Bundles (includes intermediary Certification Authorities)
    - SNI support

This document provides information about:

- Use Case Scenario
- NetScaler Console Integration with OpenStack Workflow
- Prerequisites
- Pre-configuration Tasks in NetScaler Console and OpenStack
- Configuration Steps for LBaaS V1 using Horizon
- Configuration Steps for LBaaS V2 using Command Line
- Manual Provisioning of NetScaler VPX Instance on OpenStack

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Integrating NetScaler Console with OpenStack Heat Services
- Monitoring OpenStack Applications in NetScaler Console

Use Case Scenario

The following use-case scenario explains the workflow of integrating NetScaler Console with the OpenStack platform:

An enterprise, Example-Cloud-Provider, has used OpenStack components to set up a cloud to provide infrastructure to its tenants. Steve is the administrator of this cloud provider, while Tom is a tenant of the Example-Cloud-Provider's cloud infrastructure. Tom's organization, Example-SportsOnline.com, requires two servers S1 and S1, and Tom also requires a dedicated NetScaler device to load balance the traffic between servers S1 and S2 on OpenStack platform.

To meet this requirement, Steve has to install and configure both OpenStack and NetScaler Console, and prepare them to compatible with each other. Steve has to create a tenant account named Example-SportsOnline in OpenStack, and then allocate resources to the tenant account. Steve also has to create different log-on credentials (users) for Example-SportsOnline for managing its resources and configuration. Tom can now create the two servers S1 and S2 on OpenStack to manage the traffic in his organization.

Steve has to register OpenStack details with NetScaler Console, and configure the NetScaler LBaaS driver in OpenStack networking component, Neutron. After the registration is complete, NetScaler Console displays the details of all tenants from the OpenStack. Steve can select Example-SportsOnline from the list who wants the NetScaler LBaaS features and configure Tom to get a dedicated NetScaler allotted for his load balancer configurations in NetScaler Console.

For this, Steve can either provision a NetScaler VPX instance on the computing layer (Nova) of OpenStack using NetScaler Console user interface or enable MAS to auto-provision a NetScaler VPX instance on demand, when Tom does his LB configuration in OpenStack. In either case, NetScaler Console manages the VPX instance. For achieving this, Steve creates a service package in NetScaler Console, and defines the conditions in the service package that were agreed in the SLA with Tom. For example, Steve selects the 'dedicated'isolation policy to provide a dedicated instance for providing load balancer configurations to Tom. That is, Steve selects a non-shared instance for Tom in the service package. He then assigns many NetScaler VPX instances to the service package, and associates Example-SportsOnline, along with other tenants, who require a dedicated NetScaler with the service package. As a result, when Tom performs his first load balancer configuration, NetScaler Console allots one of the NetScaler VPX instances in the service package to Example-SportsOnline and also deploys his configuration in that NetScaler.

Tom can now create load balancing configurations, by creating pools, virtual IPs (VIP), and health monitors using OpenStack LBaaS/UI. Pools and the VIPs in OpenStack get deployed as service groups and

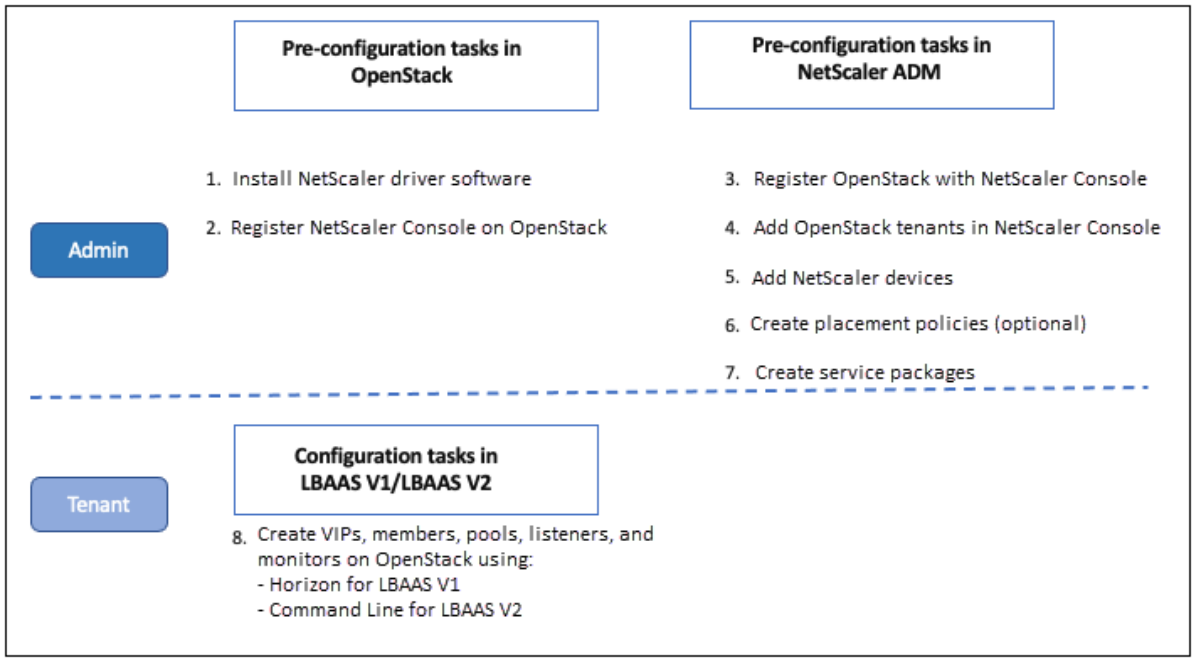
© 1997–2025 Citrix Systems, Inc. All rights reserved.

virtual servers on the NetScaler instance. Tom can also create health monitors to monitor the servers, and send application traffic to only those servers which are UP at any point of time and reachable from NetScaler.

The load balancing configuration created in OpenStack is now implemented on the NetScaler instance. Once fully configured, the NetScaler VPX instance then takes over the load balancing functionality and starts accepting application traffic and load balances the traffic between the servers S1 and S2 created by Tom.

NetScaler Console Integration with OpenStack Workflow

The following flowchart depicts the workflow that you need to follow when you are configuring LBaaS V1 and LBaaS V2.



NSX Manager: manual provisioning of NetScaler instances

September 27, 2025

NetScaler Console integrates with VMware network virtualization platform to automate the deployment, configuration, and management of NetScaler services. This integration abstracts away the traditional complexities associated with physical network topology, enabling vSphere/vCenter admins to programmatically deploy NetScaler services faster.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

This article provides you with a list of tasks that you have to perform on both VMware NSX Manager and on NetScaler Console.

> **Note**
>
> Ensure that VMware NSX for vSphere 6.2 and above is installed and configured, and the edge gateways, DLR, and virtual machines that have to be load balanced are already created.

Prerequisites

- Install VMware ESXi version 4.1 or later with hardware that meets the minimum requirements.
- Install VMware Client on a management workstation that meets the minimum system requirements.
- Install VMware OVF Tool (required for VMware ESXi version 4.1) on a management workstation that meets the minimum system requirements.
- Install NetScaler Console on any of the supported hypervisors.

  For tasks to install NetScaler Console build 13.1, on any of the supported hypervisors, see Deploying NetScaler Console.

VMware ESXi Hardware Requirements

The following table lists the virtual computing resources that you require on your VMware ESXi server to install a NetScaler Console virtual appliance.

Component	Requirement
RAM	8 GB
Virtual CPU	8
Storage space	500 GB
Virtual Network Interfaces	1
Throughput	1 Gbps

> **Note**
>
> The memory and hard disk requirements specified above are for deploying NetScaler Console on VMware ESXi server, considering that there are no other virtual machines running on the host. The hardware requirements for VMware ESXi server depends on the number of virtual machines

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> running on it.

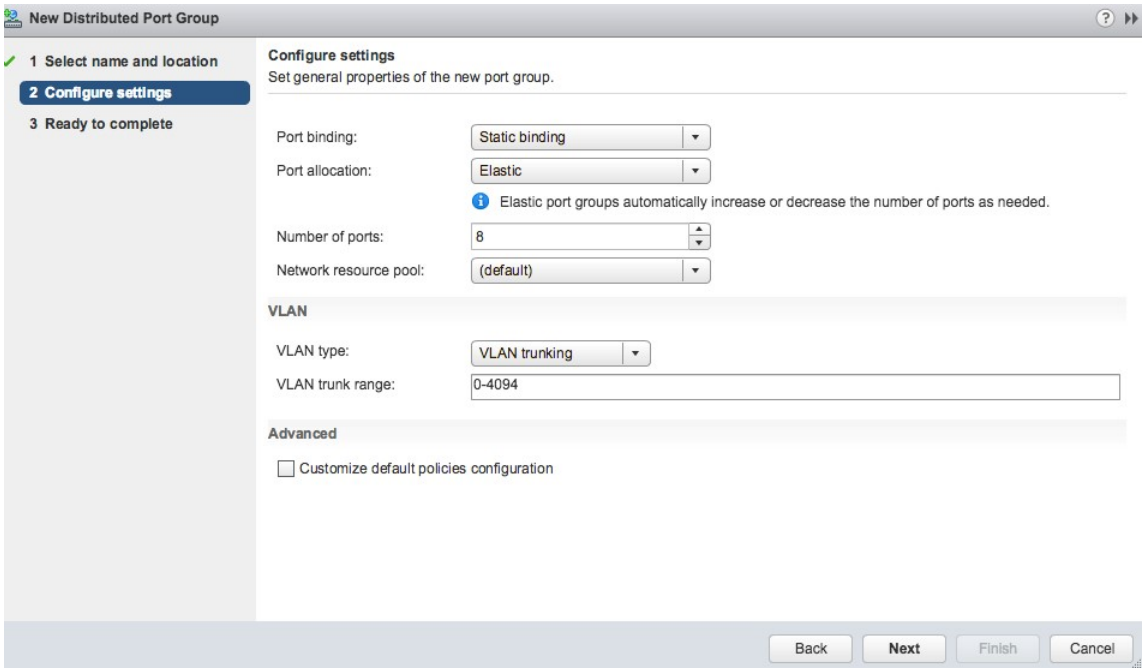
Configuring VMware NSX

- Create a pool of NetScaler VPX instances of different capacities, which are added to the different service packages.

For example:

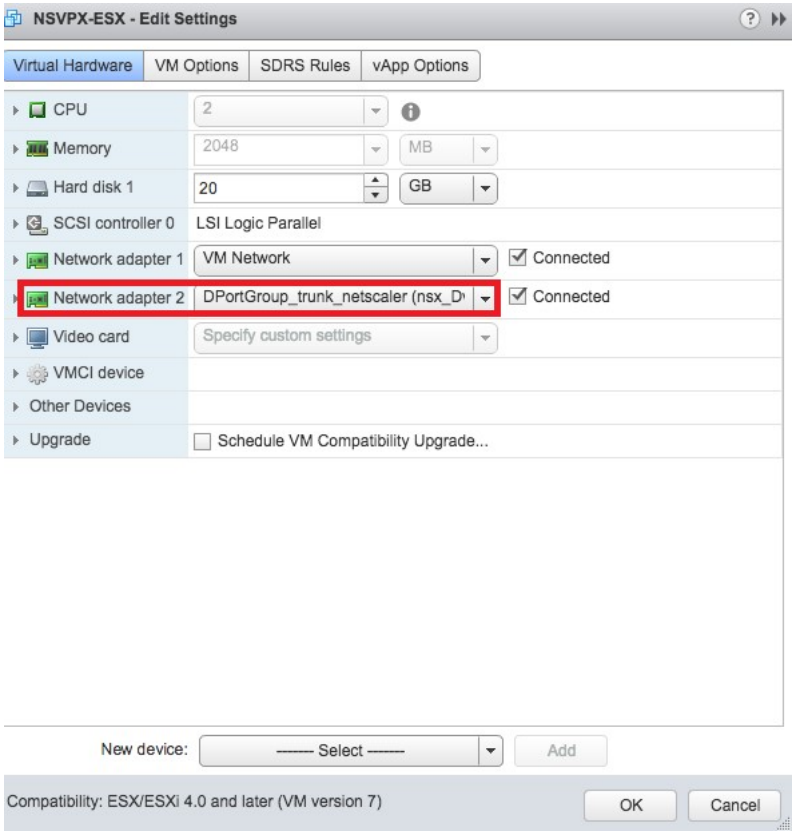
- Create five NetScaler VPX instances of VPX1000 (1 Gbps). These instances are added to the Gold service package.
- Create five NetScaler VPX instances of VPX10 (10 Mbps). These instances are added to the Bronze service package.

1. In vSphere client, navigate to **Networking**, and create a port group of type VLAN trunking with range, for example, 101-105 (you can even provide the full range, but create port group of type VLAN for only the required VLANs).



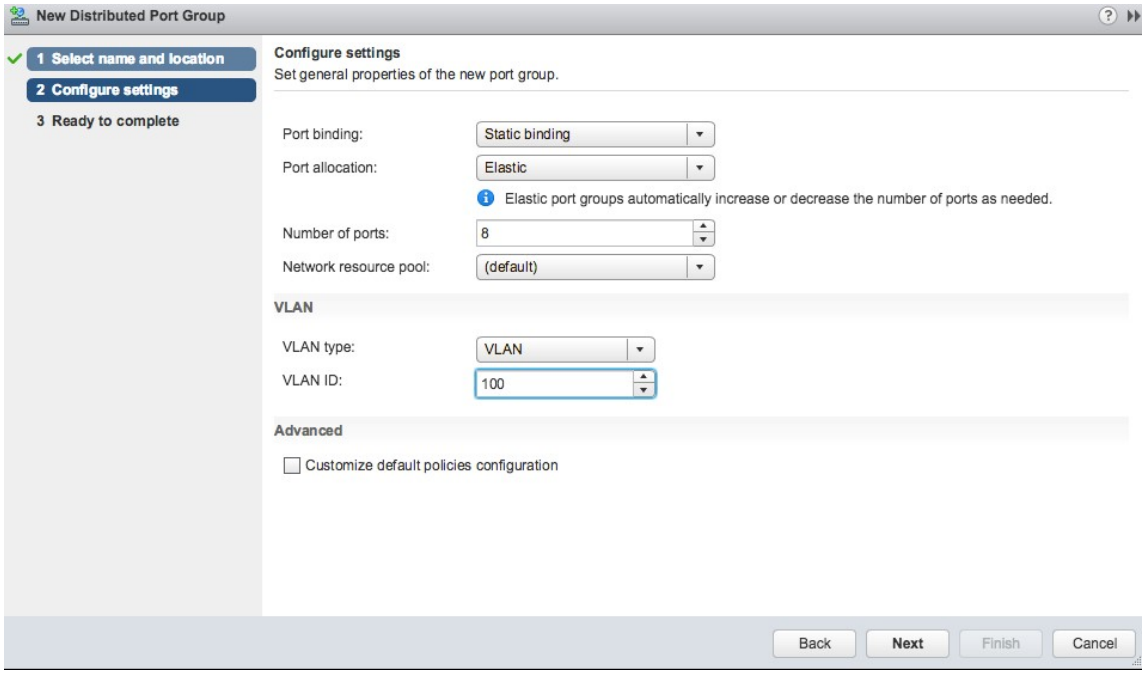
2. Create a new interface for each NetScaler VPX instance, and attach it to the VLAN range trunk port group that was created above.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. In vSphere client, navigate to **Networking**, and create a port group of type VLAN.

   For example, If the initial trunked port group was created with range 101-105, create five VLAN port groups one per VLAN, that is a port group with VLAN 101, another with VLAN102, and so on, until VLAN 105.

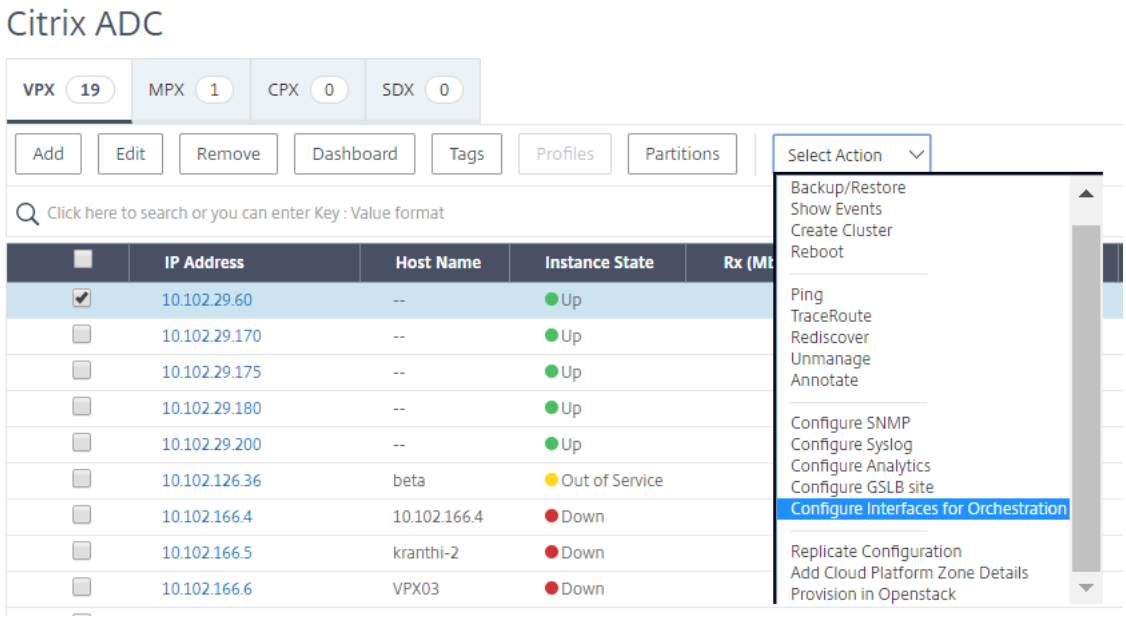


© 1997–2025 Citrix Systems, Inc. All rights reserved.

Adding NetScaler VPX Instance in NetScaler Console

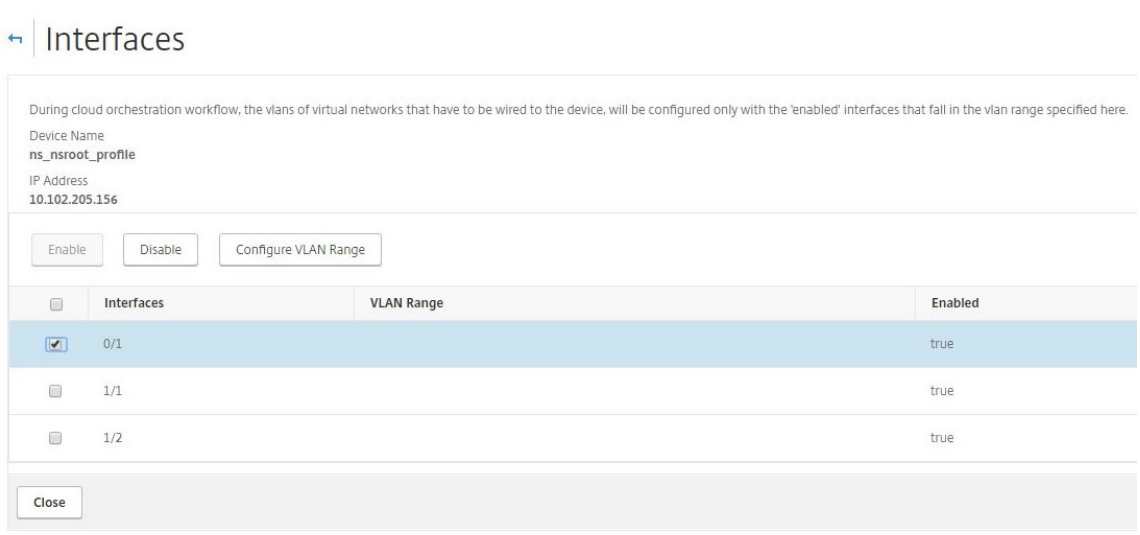
Add NetScaler VPX instances in NetScaler Console and specify the VLAN range of the trunked group for each device.

1. In NetScaler Console, navigate to **Infrastructure** > **Instances** > **NetScaler VPX**, and click **Add**.
2. On the **Add NetScaler VPX** page, specify either the host names of the instances, the IP address of each instance, or a range of IP addresses, and then select an instance profile from the P**rofile Name** list. You can also create a new instance profile by clicking the + icon.
3. Click **OK**.
4. Select the newly added NetScaler VPX instance from the list on the **NetScaler VPX** page, and click the down arrow button in **Action** field. Select **Configure Interfaces for Orchestration**.

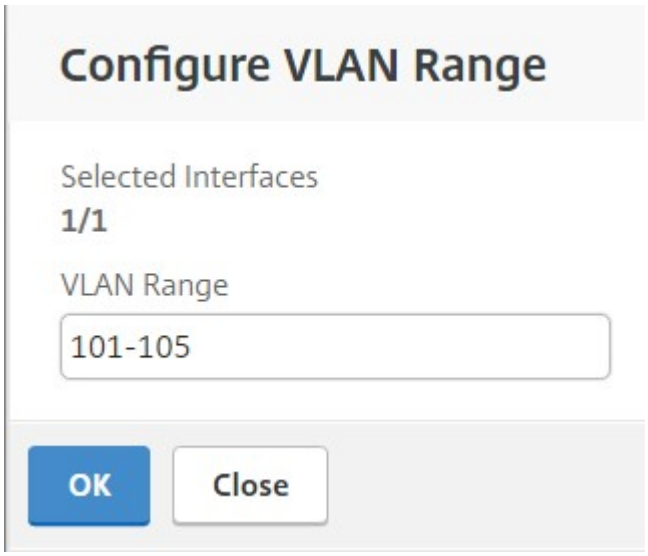


5. On the **Interfaces** page, select the management interface, and click **Disable** to disable VLAN from binding to the management interface.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



6. On the **Interfaces** page, select the required interface, and click **Configure VLAN Range**.
7. Enter the VLAN range configured in NSX Manager, click **OK**, and then click **Close**.



Registering VMware NSX Manager with NetScaler Console

Register VMware NSX manager with NetScaler Console to create a communication channel between them.

1. In NetScaler Console, navigate to **Orchestration** > **SDN Orchestration** > **VMware NSX Manager** from the drop-down list, and click **Configure NSX Manager Settings**.
2. On **Configure NSX Manager Settings** page, set the following parameters:

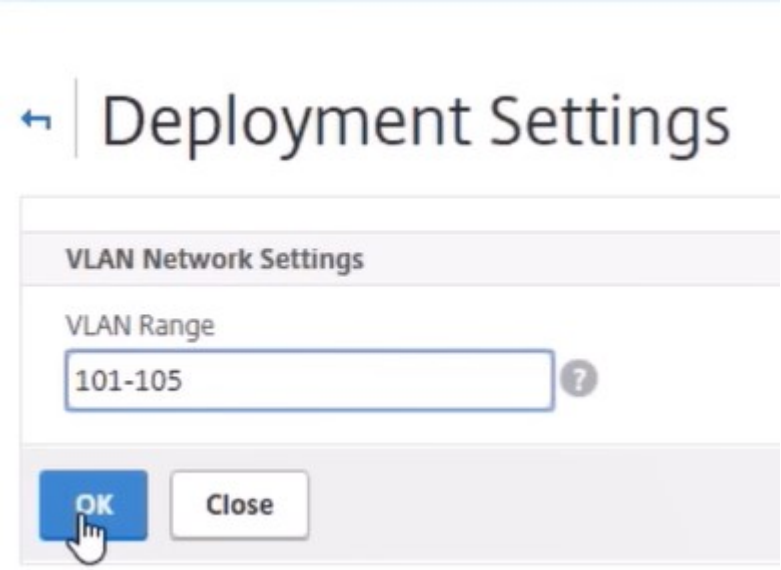
    a) NSX Manager IP Address - IP address of NSX Manager.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

b) NSX Manager user name - Administrative user name of NSX Manager.

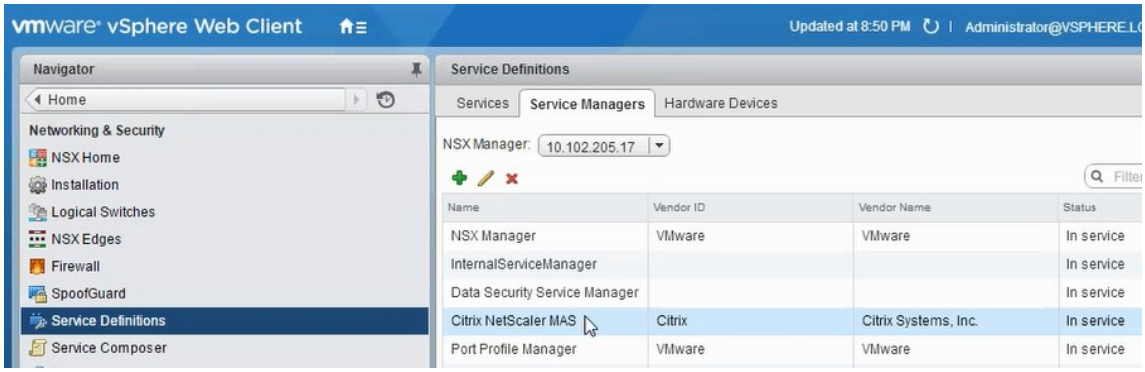
c) Password - Password of the administrative user of NSX Manager.

3. In **NetScaler Console account used by NSX Manager** section, set the NetScaler Driver user name and Password for the NSX Manager. NetScaler Console authenticates load balancer configuration requests from the NSX Manager by using these logon credentials.
4. Click **OK**.
5. Navigate to **Orchestration** > **System** > **Deployment Settings**. Provide the VLAN range which was configured in trunked port group.



6. Log on to the NSX Manager on vSphere Web Client, and navigate to **Service Definitions** > **Service Managers**.

   You can view Citrix NetScaler Console as one of the service managers. This indicates that the registration is successful and a communication channel is established between the NSX manager and NetScaler Console.



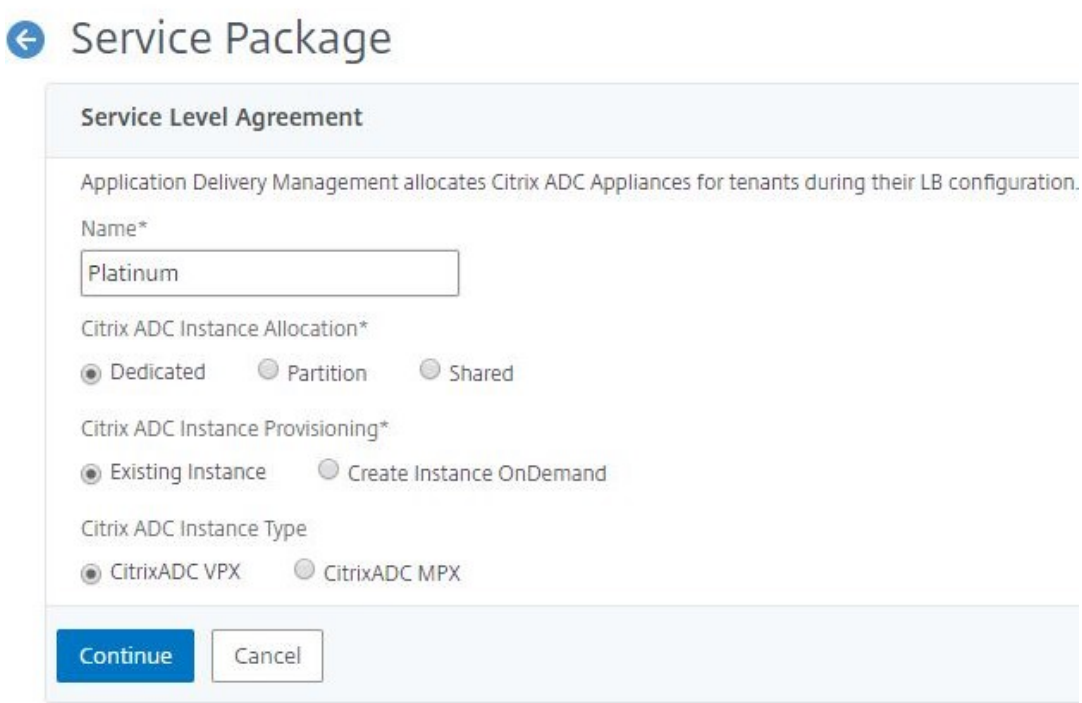
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Creating a Service Package in NetScaler Console

1. In NetScaler Console, navigate to **Orchestration** > **SDN Orchestration** > **VMware NSX Manager** > **Service Packages**, and click **Add** to add a new service package.
2. On **Service Package** page, in **Basic Settings** section, set the following parameters:
   a) Name –type the name of a service package
   b) Isolation Policy –by default, the isolation policy is set to Dedicated
   c) Device Type –by default, the device type is set to NetScaler VPX

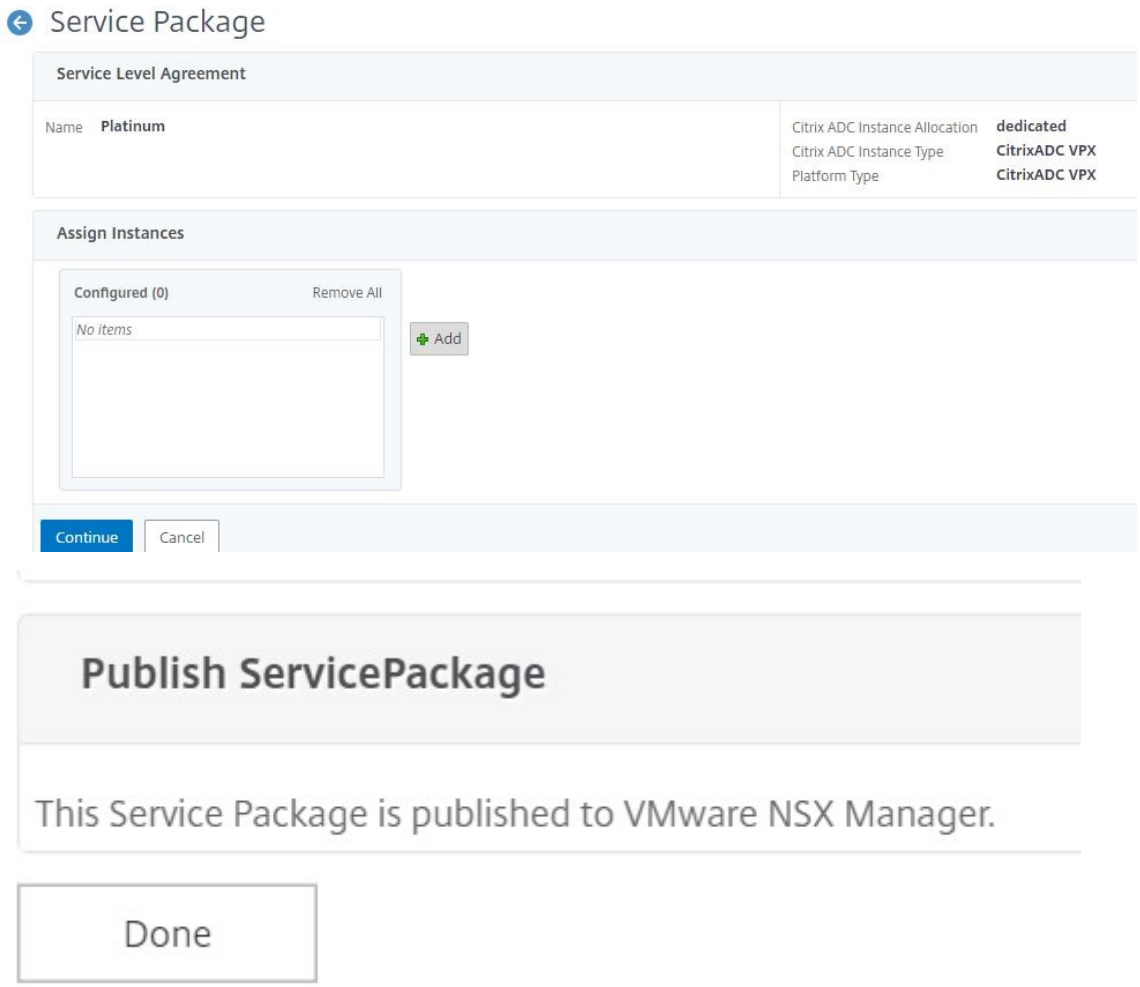
      > **Note**
      >
      > These values are set by default in this version, and you cannot modify them.

   d) Click **Continue**.



3. In **Assign Devices** section, select the pre-provisioned VPX for this package, and click **Continue**.
4. In **Publish Service Package** section, click **Continue** to publish the service package to VMware NSX, and then click **Done**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



This procedure configures a service package in the NSX Manager. A service can have multiple devices added to it and multiple edges can use the same service package to offload the NetScaler VPX instance to NetScaler Console.

5. Log on to the NSX Manager on vSphere Web Client, and navigate to **Service Definitions** > **Services**.

   You can see that the NetScaler Console service package is registered.

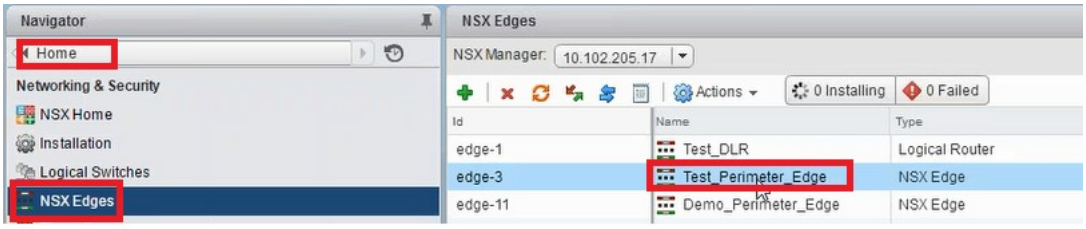


© 1997–2025 Citrix Systems, Inc. All rights reserved.

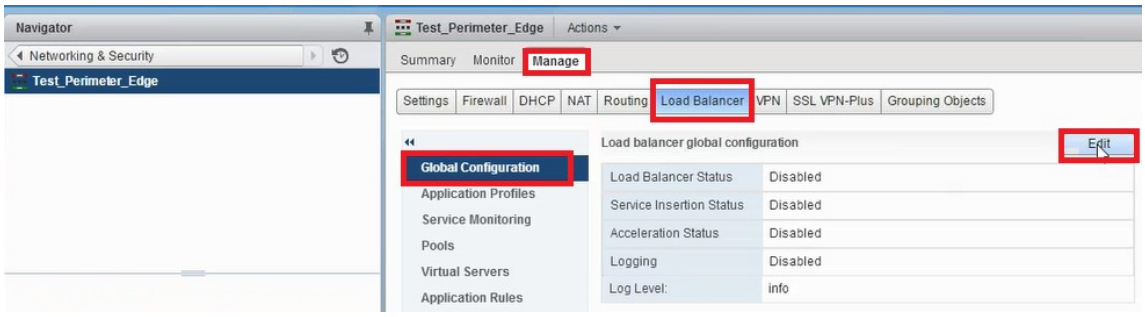
Performing Load Balancer Service Insertion for Edge

Perform load balancer service insertion on the previously created NSX Edge gateway (offload the load balancing function from NSX LB to NetScaler).

1. In NSX Manager, navigate to **Home** > **NSX Edges**, and select the edge gateway that you have configured.

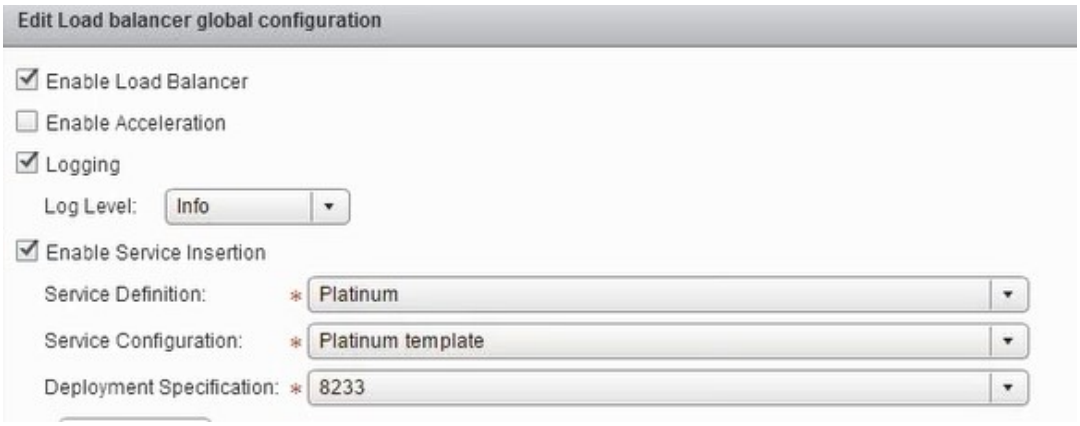


2. Click **Manage**, and on the **Load Balancer** tab, select **Global Configuration**, and click **Edit**.



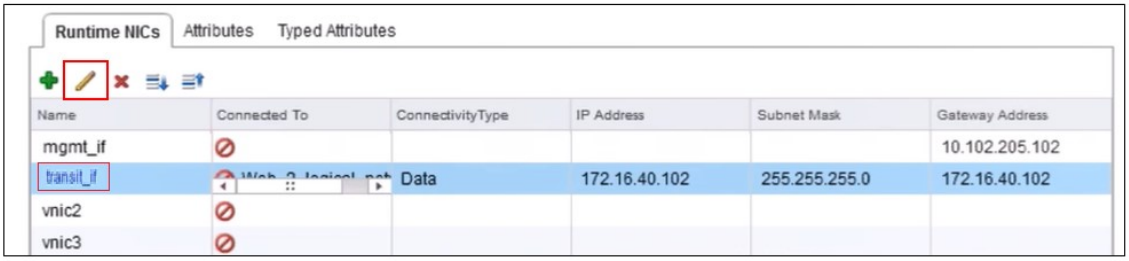
3. Select **Enable Load Balancer**, **Logging**, **Enable Service Insertion** to enable them.

   a) In **Service Definition,** select the service package that was created in NetScaler Console and published to NSX Manager.

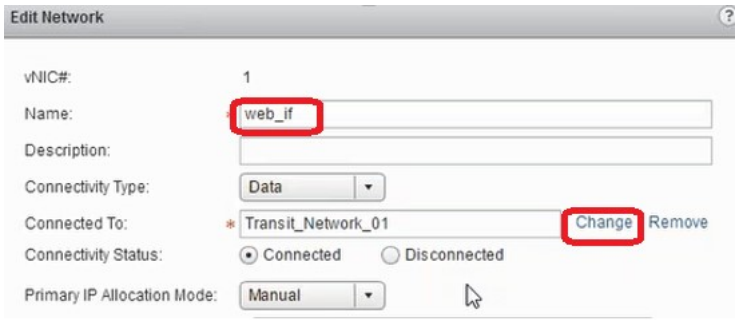


4. Select the existing runtime NICs and click the Edit icon to edit runtime NICs that have to be connected when NetScaler VPX is allocated.

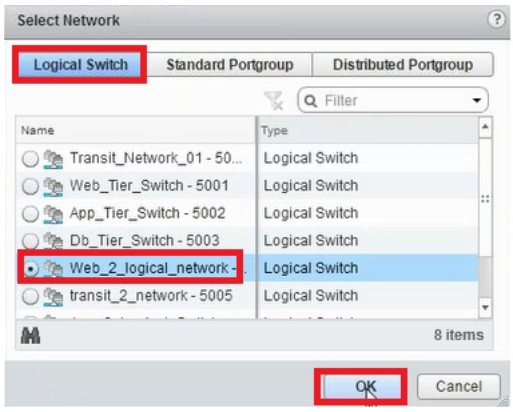
© 1997–2025 Citrix Systems, Inc. All rights reserved.



5. Edit the name of the NIC, specify Connectivity Type as **Data**, and click **Change**.



6. Select the appropriate web logical switch.

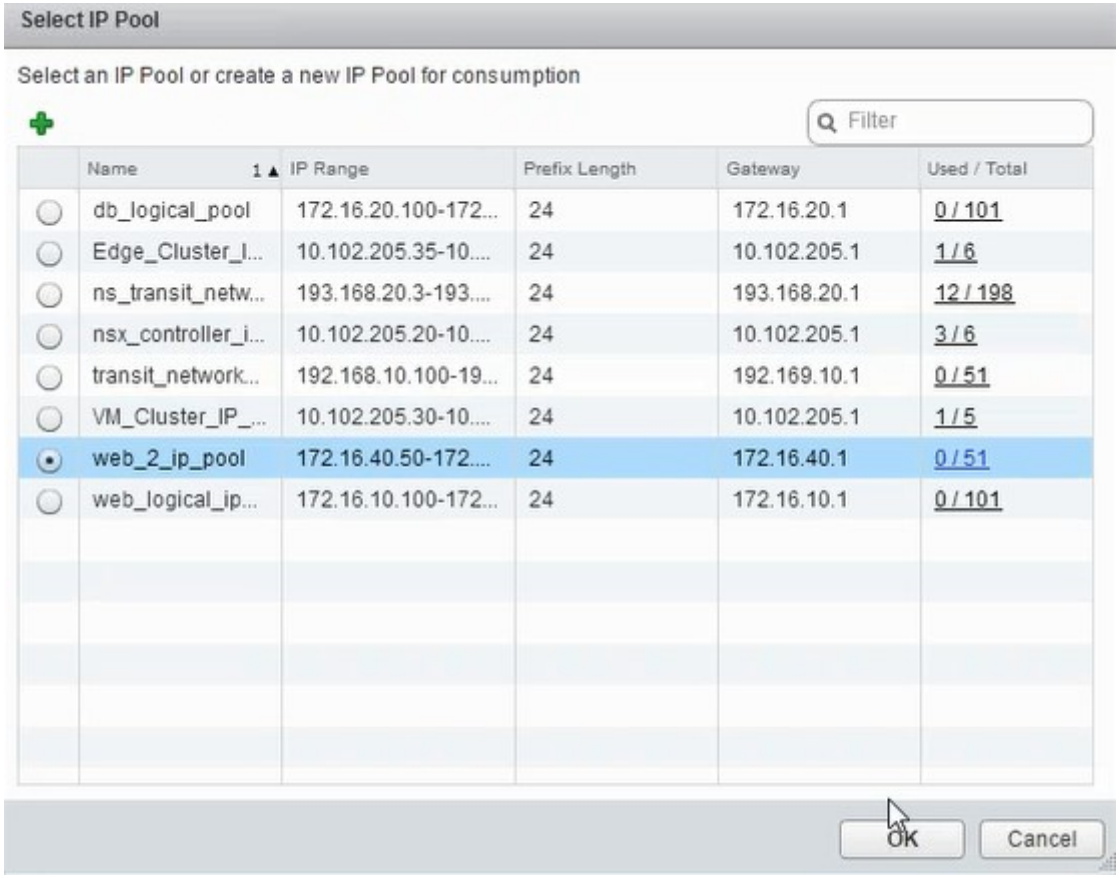


7. In **Primary IP Allocation Mode**, select IP Pool from the drop-down list, and click the down-arrow button on IP Pool field.



8. In the **Select IP Pool** window, select the appropriate IP pool, and click **OK**.

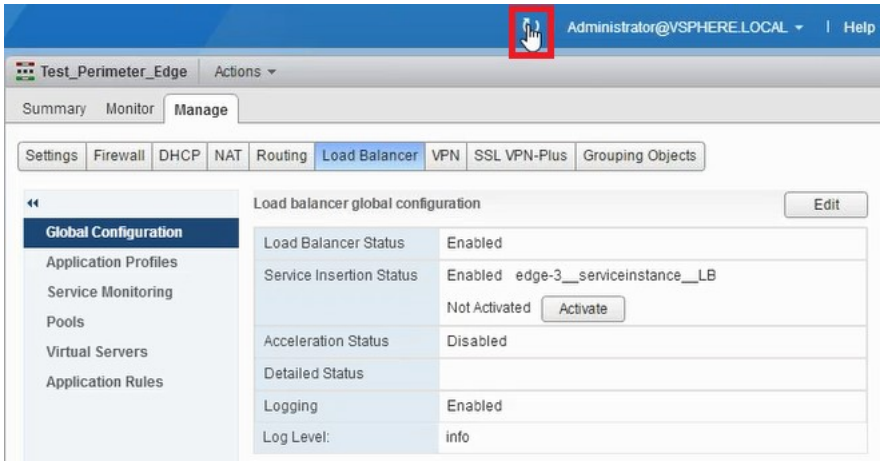
© 1997–2025 Citrix Systems, Inc. All rights reserved.



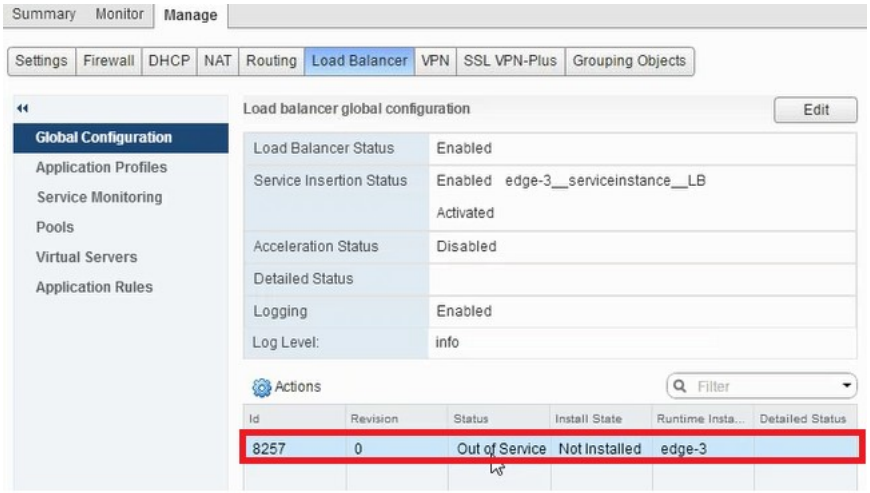
The IP address is acquired and is set as the source net IP address in the NetScaler VPX appliance. A L2 gateway is created in the NSX Manager to map the VXLAN to VLAN.

> **Note**
>
> All data interfaces are connected as run-time NICs, and they are part of interfaces for DLR.

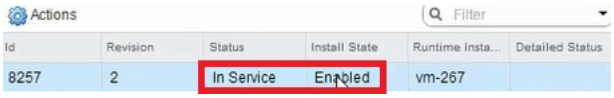
9. Refresh the view to see the creation of the run time.



© 1997–2025 Citrix Systems, Inc. All rights reserved.



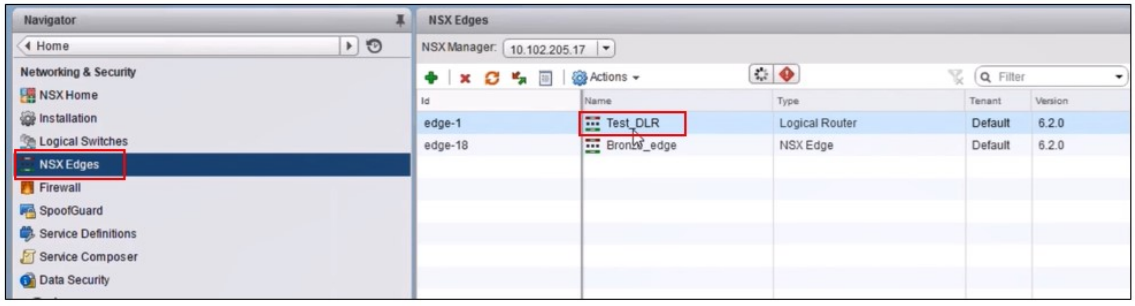
10. After the VM has started, the value of Status changes to **In Service** and that of Install State changes to **Enabled**.



> **Note**
>
> In NetScaler Console, navigate to **Orchestration** > **Requests** to see progress details of completion of LB service insertion.

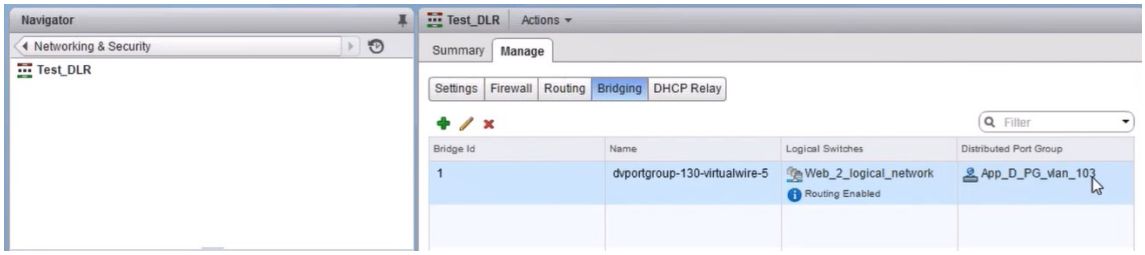
Viewing L2 Gateway on NSX Manager

1. Log on to the NSX Manager on vSphere Web Client, navigate to **NSX Edges**, and select the DLR created.



2. In the DLR page, navigate to **Manage** > **Bridging**. You can see the L2 gateway displayed in the list.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



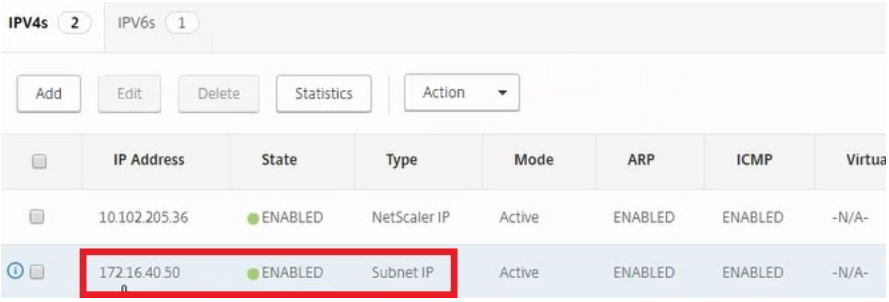
> **Note**
>
> An L2 gateway gets created for each data interface.

Viewing Allotted NetScaler

1. Log on to the NetScaler VPX instance using the IP address displayed in NetScaler Console. Then, navigate to **Configuration** > **System** > **Networking**. In the right pane, you can see that the two IP address are added. Click the IP address hyperlink to see the details.



   The subnet IP address is same as the IP address of the web interface added in the NSX.



2. Navigate to **Configuration** > **System** > **Licenses** to view the licenses that are applied to this instance.

Configuring NetScaler VPX Instance Using StyleBook

1. In NetScaler Console, navigate to **Orchestration** > **SDN Orchestration** > **Configure NSX Manager** > **Edge Gateways**.

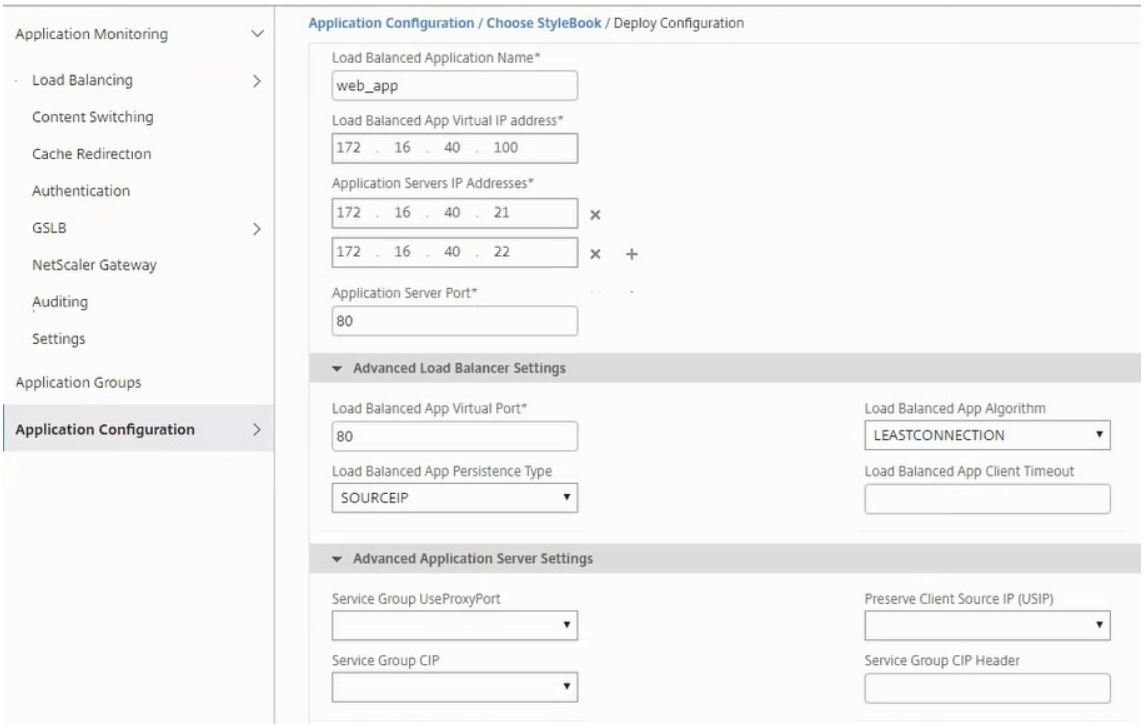
   Make a note of the NetScaler instance IP that is allotted to the respective Edge Gateway on which Load Balancing configuration through StyleBooks has to be applied.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

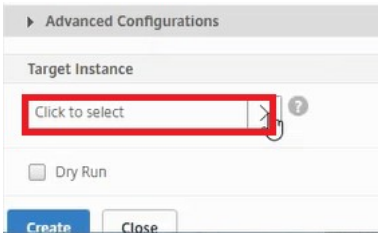
2. Create a new StyleBook. Navigate to **Applications** > **Configuration**, import the StyleBook, and select the StyleBook from the list.

   To create a new StyleBook, see Create Your Own StyleBook.

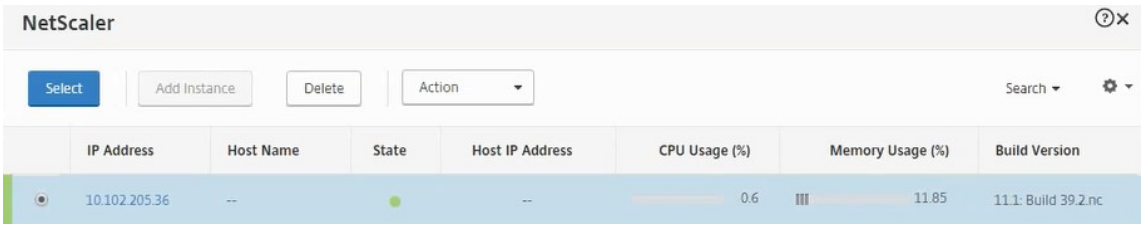
3. Specify values for all the required parameters.



4. Specify the NetScaler VPX instance on which you want to run these configuration settings.

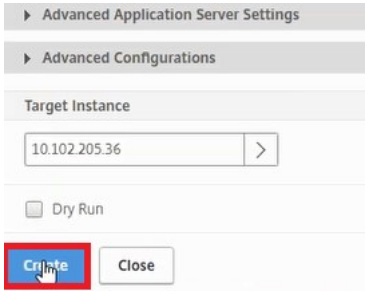


5. Select the IP instance noted earlier, and click **Select**.



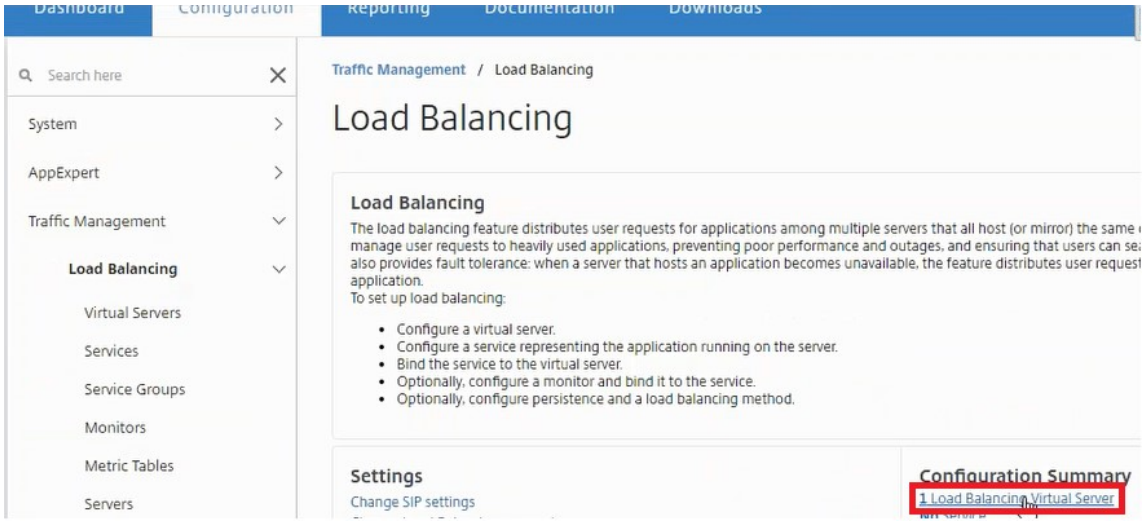
6. Click **Create** to apply the configuration on the selected device.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

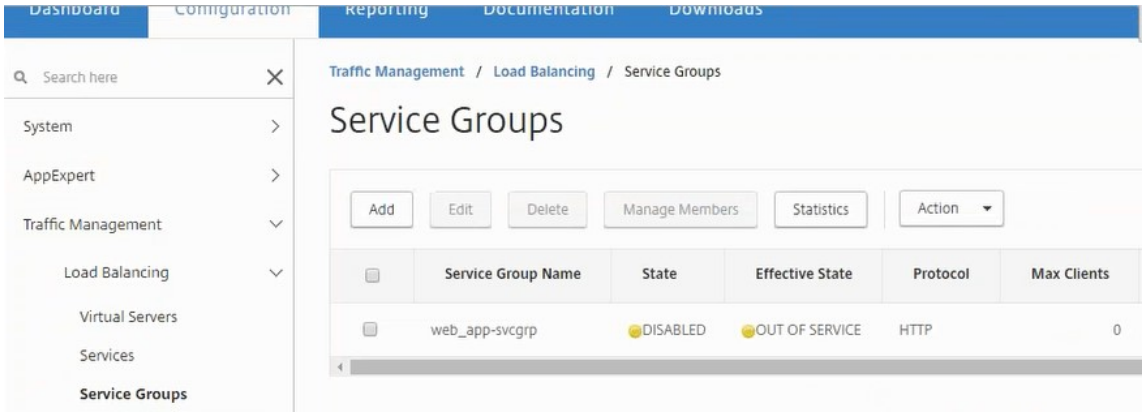


Viewing Load Balancer Configuration

1. Log on to the NetScaler VPX instance, navigate to **Configuration** > **Traffic Management** > **Load Balancing** to view the load balancing virtual server that is created.

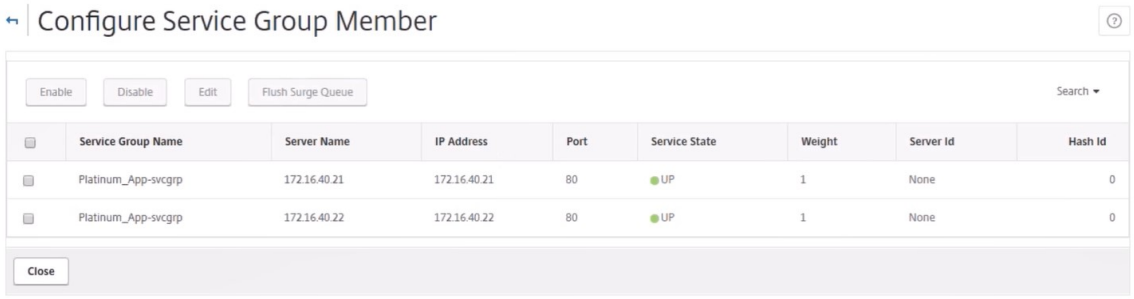


You can also view the service groups that are created.



2. Select the service group, and click **Manage Members**. The **Configure Service Group Member** page displays the members associated with the service group.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

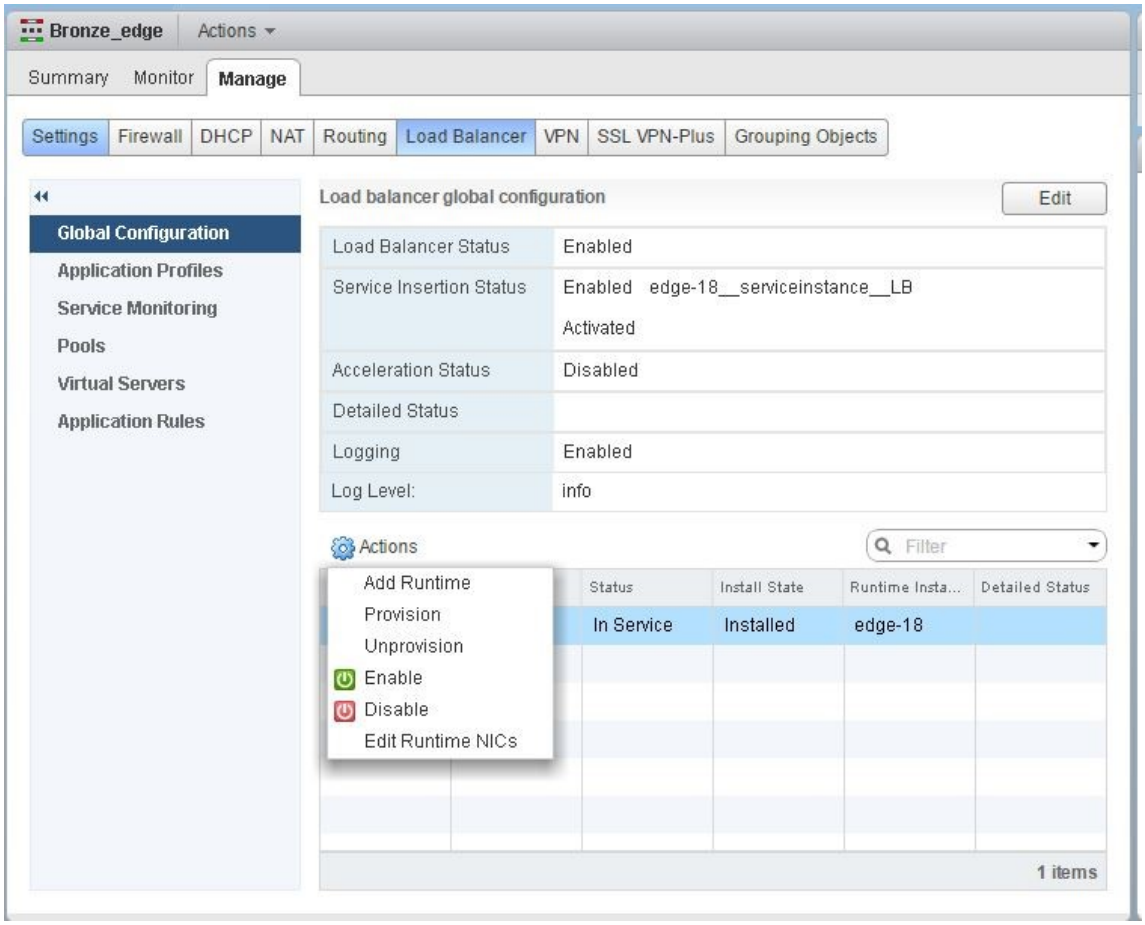


Deleting Load Balancer Service

1. In NetScaler Console, navigate to **Applications** > **Configuration**, and click **X** icon to delete the application configuration.
2. Log on to the NSX Manager on vSphere Web Client and navigate to the edge gateway to which the NetScaler VPX instance is connected.
3. Navigate to the **Manage** > **Load Balancer** > **Global Configuration**, right-click on the runtime entry, and click **Unprovision**.

> **Note**
>
> Edge Gateways in NetScaler Console corresponds to runtime entries in NSX manager.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



The NetScaler VPX instance is rendered out of service.

4. In NetScaler Console, navigate to **Orchestration** > **SDN Orchestration** > **Configure NSX Manager** > **Edge Gateways**. Verify that the respective mapping of Edge Gateway to the deleted instance is not present.

NSX Manager: auto provisioning of NetScaler instances

September 27, 2025

Overview

NetScaler Console integrates with VMware network virtualization platform to automate the deployment, configuration, and management of NetScaler services. This integration abstracts away the traditional complexities associated with physical network topology, enabling vSphere/vCenter admins to programmatically deploy NetScaler services faster.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

During load-balancing service insertion and deletion on VMware NSX Manager, NetScaler Console dynamically provisions and destroys the NetScaler instances. This dynamic provisioning requires the NetScaler VPX license assignments to be automated in NetScaler Console. When the NetScaler licenses are uploaded to the NetScaler Console, NetScaler Console performs the role of license server.

Prerequisites

> **Note**
>
> This integration is supported only for **VMware NSX for vSphere 6.1 or earlier**.

- NetScaler Console, version 13.0 setup in high availability and installed on ESX.
- NetScaler VPX, version 13.0
- NetScaler VPX licenses for NetScaler VPX instances, version 13.0
- Install VMware ESXi version 4.1 or later with hardware that meets the minimum requirements.
- Install VMware Client on a management workstation that meets the minimum system requirements.
- Install VMware OVF Tool (required for VMware ESXi version 4.1) on a management workstation that meets the minimum system requirements.

High-Availability Deployment of NetScaler Console and NetScaler Instances

To provision the NetScaler Console HA setup, install the NetScaler Console image file that you have downloaded from the NetScaler site. For more information on how to provision NetScaler Console HA setup, see Deploying NetScaler Console in High Availability.

Setting up NetScaler Console HA Endpoint Details

To integrate VMware NSX manager with NetScaler Console that is deployed in a HA mode, you must first enter the virtual IP address of the load balancing NetScaler instance. You must also upload the certificate file that is present on the NetScaler load balancing virtual server to the NetScaler Console file system.

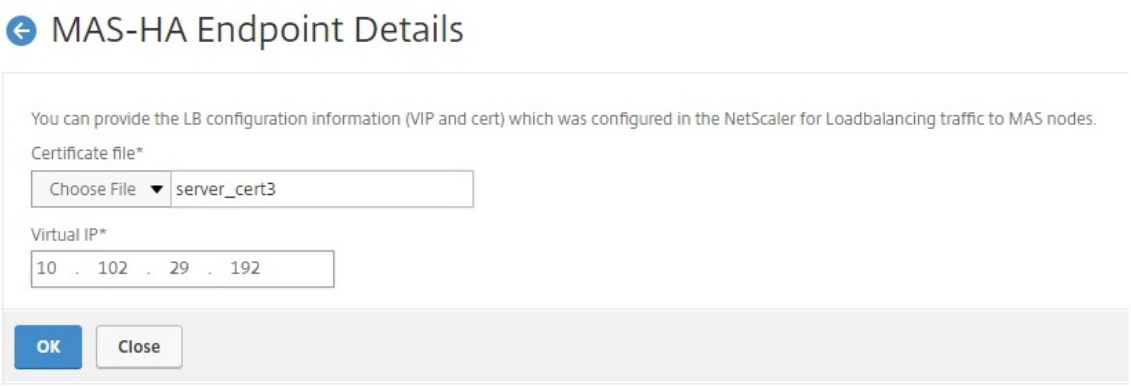
To provide load balancing configuration information in NetScaler Console:

1. In NetScaler Console HA node, navigate to **System** > **Deployment**.
2. Click **HA Settings** in the top-right corner, and in **MAS-HA Settings** page, click **MAS-HA Endpoint Details**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. On **MAS-HA Endpoint Details** page, upload the same certificate that is already present on the load balancing NetScaler instance.
4. Enter the virtual IP address of the load balancing NetScaler instance and click **OK**.



Registering VMware NSX Manager with NetScaler Console

When you set up two NetScaler Console servers in high availability, the two server nodes are in active-passive mode. Log on to the primary NetScaler Console server node to register VMware NSX manager with NetScaler Console in HA, to create a communication channel between them.

To register VMware NSX manager with NetScaler Console in HA:

1. In the primary NetScaler Console server node, navigate to **Orchestration** > **SDN Orchestration** > **VMware NSX Manager**.
2. Click **Configure NSX Manager Settings**.
3. On **Configure NSX Manager Settings** page, set the following parameters:
    a) NSX Manager IP Address - IP address of NSX Manager.
    b) NSX Manager user name - Administrative user name of NSX Manager.
    c) Password - Password of the administrative user of NSX Manager.
4. In NetScaler Console account used by NSX Manager section, set the NetScaler Driver Password for the NSX Manager.
5. Click **OK**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

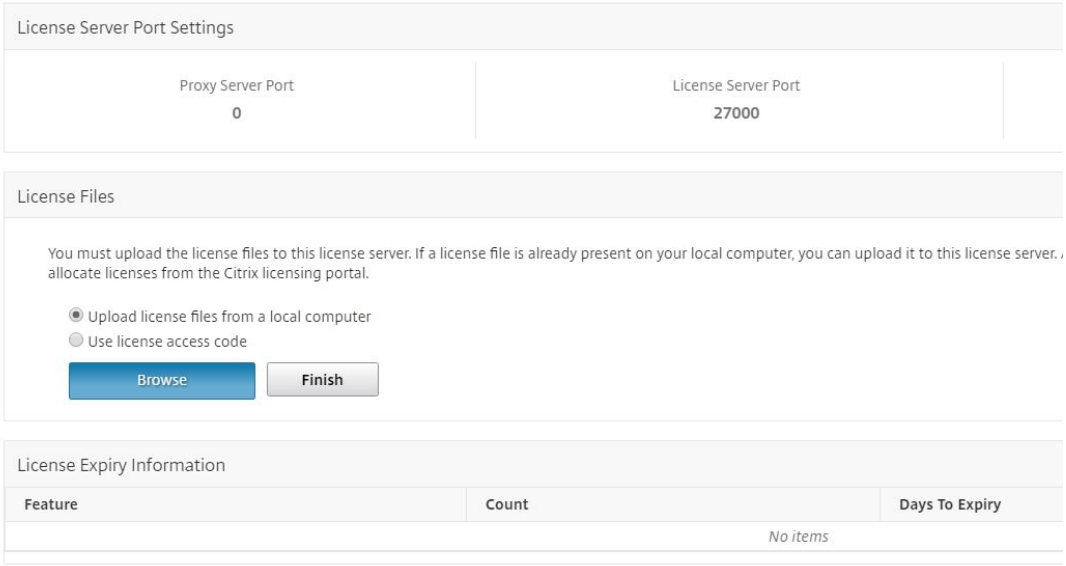
Uploading Licenses in NetScaler Console

Upload the NetScaler VPX licenses to NetScaler Console, so that NetScaler Console can automatically allocate licenses to the instances during orchestration with NSX.

To install license files on NetScaler Console:

1. In NetScaler Console, navigate to **Infrastructure > Pooled Licensing**.
2. In **License Files** section, select one of the following options:
   a) **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. To add license files, click **Browse** and select the license file (.lic) that you want to add. Then click **Finish**.
   b) **Use License Access Code** - Citrix emails the License Access Code for the licenses that you purchase. To add license files, enter the license access code in the text box and then click **Get Licenses**.

> **Note**
>
> At any time, you can add more licenses to the NetScaler Console from the License Settings.



Uploading NetScaler VPX Images in NetScaler Console

Add the NetScaler images to NetScaler Console, so that the NetScaler Console uses these images as defined in the service package.

To upload NetScaler VPX Images in NetScaler Console:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

1. In NetScaler Console, navigate to **Orchestration** > **SDN Orchestration** > **VMware NSX Manager** > **ESX NSVPX Images**.
2. Click **Upload**, and select the NetScaler VPX zip package from the local storage folder.

Creating Service Packages in NetScaler Console

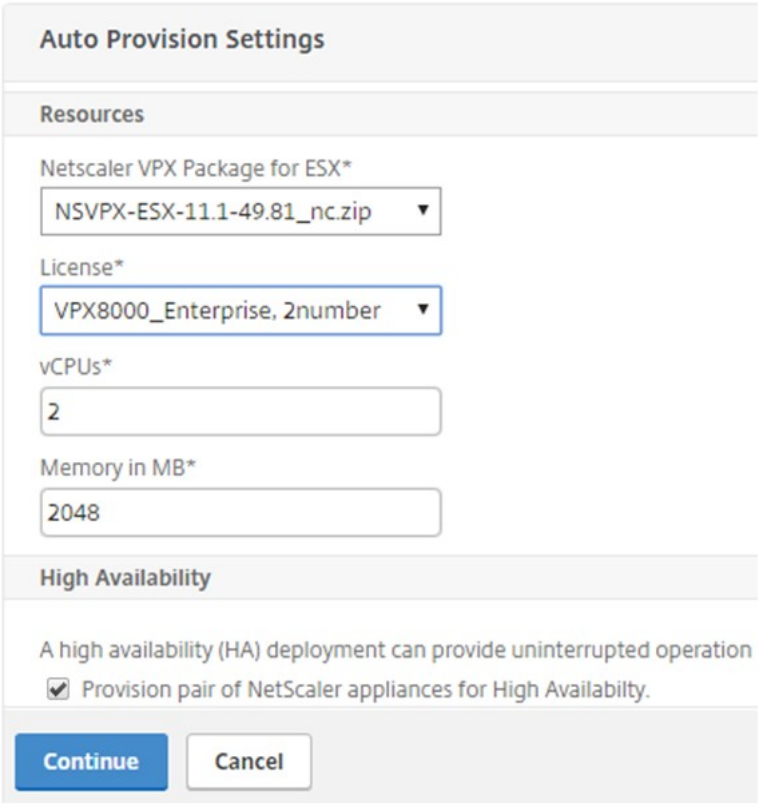
Create service packages in NetScaler Console to define the set of SLAs, which states how the NetScaler resources are allocated.

To create service packages in NetScaler Console:

1. In NetScaler Console, navigate to **Orchestration** > **SDN Orchestration** > **VMware NSX Manager** > **Service Packages**, and click **Add** to add a new service package.
2. On **Service Package** page, in **Basic Settings** section, set the following parameters:
   a) Name - name of a service package
   b) Isolation Policy - select **Dedicated**
   c) NetScaler Instance Provisioning - select **Create Instance OnDemand**
   d) Auto Provision Platform - select **CitrixNetScaler SDX**
   e) Click **Continue**
3. In the **Auto Provision Settings** section, select the recently uploaded NetScaler VPX zip package for deploying it on NSX platform, select the corresponding license, and click **Continue**.

   > **Note**
   >
   > In **High Availability** section, check the box to provision NetScaler instances for HA.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



> **Note**
>
> The name of license displayed in the list box shown in the figure above, VPX8000_Advanced, 2 number is an example and is explained as below:
>
> - VPX - the license is to deploy NetScaler VPX instances
> - 8000 - consumable bandwidth is 8GB
> - Advanced - NetScaler® provides three types of licenses - Standard, Advanced, and Premium
> - 2 number - two NetScaler VPX instances can be deployed by using this license
>
> The name of license displayed in the **License** list box depends on the license that you have purchased from Citrix.

4. Click **Continue**.
5. The service package is published to NSX Manager. In NSX Manager, navigate to **Service Definitions** > **Service Managers**. You can view NetScaler Console as one of the service managers. This indicates that the registration is successful and bi-directional communication is established between the NSX manager and NetScaler Console.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Note**
>
> For NetScaler Console in high availability deployment, the licenses are uploaded only in the NetScaler Console license server node. The NetScaler Console nodes are in an active-passive mode.

Performing Load Balancer Service Insertion for Edge

Perform load balancer service insertion on the existing NSX Edge Gateway, that is, offload the load balancing function from NSX load balancer to NetScaler.

To insert load balancing service on NSX Edge Gateway:

1. In NSX Manager, navigate to **Home** > **Networking and Security** > **NSX Edges**, and double-click to select the edge gateway that you have configured.
2. Click **Manage**, and on the **Load Balancer** tab, select **Global Configuration**, and click **Edit**.
3. Select **Enable Load Balancer** and **Enable Service Insertion** to enable them.
4. In **Service Definition**, select the service package that was published to NSX Manager.
5. Configure one virtual NIC for management interface, and one or more virtual NICs for data interfaces. Select the networks for management and data accordingly.

   > **Note**
   >
   > Select IP Pool option in Primary IP Allocation mode. NetScaler Console does not support manual or DHCP allocation of IP addresses.

6. Click the refresh icon to see the creation of the run time.

   > **Note**
   >
   > Because you are deploying two NetScaler VPX instances in HA deployment, two run times are created in the NSX manager.
   >
   > You might have to refresh the screen to view the run times displayed on the screen.

7. Select the run time, click **Actions**, and select **Install** from the pop-up menu. For HA, repeat this for the other run time also.
8. When both the virtual machines start, the value of Status changes to “In Service”and that of Install State changes to “Enabled.”

   > **Note**
   >
   > You might have to refresh the screen to view the change in status.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

9. In NetScaler Console, navigate to **Orchestration** > **Requests** to see progress details of completion of service insertion. You can see that a request to create and update the run time has come in to NetScaler Console. When the run time has been updated, select the request and click the **Tasks** button to view that NetScaler Console has been added in NSX Manager.

   For HA, there will be two requests to create and update two run times in NetScaler Console. When both run times have been updated, select both requests and click the **Tasks** button to view that two NetScaler Console HA nodes have been added in NSX Manager.

10. In NetScaler Console, navigate to **Orchestration** > **SDN Orchestration** > **VMware NSX Manager** > **Edge Gateways**. In the right-hand side panel, you can view that the NetScaler VPX has been added to the NSX Edge Gateway.

    For HA, you can see that two NetScaler VPX instances in HA mode have been added to the NSX Edge Gateway.

11. In NetScaler Console, navigate to **Infrastructure > Pooled Licensing > VPX Licenses**. Select the NetScaler VPX license and the edition that you have installed.

    The NetScaler VPX instances that are in HA mode consume two licenses and the status is displayed on your screen as below.



When the service insertion is complete, you can use StyleBooks to configure the NetScaler instances in one of the following two methods:

- Configuring Load Balancing Services on NetScaler VPX in VMware NSX Manager GUI

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Configuring Load Balancing Services on NetScaler VPX in NetScaler Console GUI

Configuring Load Balancing Services on NetScaler VPX in VMware NSX Manager GUI

Perform the following task to enable configuration of load balancing services on the NSX Edge gateway device using built-in StyleBooks.

In NSX Manager, navigate to **Home** > **Networking and Security** > **NSX Edges**, and double-click to select the edge gateway that you have configured.

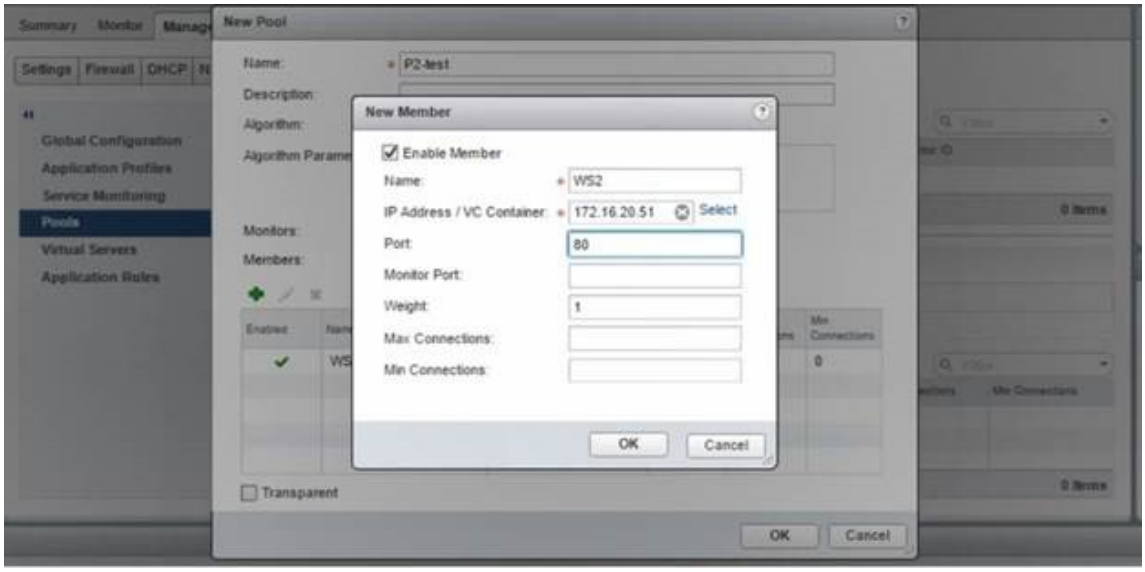
Creating pools and pool members

Create a pool of servers and members of different capacities.

1. Click **Manage**, and on the **Load Balancer** tab, select **Pools**, and click "**+**"icon to add a new pool, and set the following parameters:
    a) Name - Name of the new pool
    b) Algorithm - Select an algorithm from the drop-down list base on which the pool will be selected.
    c) Monitors - Make sure the service monitor is set to default_http_monitor
    d) Members - Click "+"to add members to the pool and enter the required parameters in the New Member window.
        i. Name - Name of the member
        ii. IP Address/ VC Container - Click Select to select the object from the available list or enter the IP address of the object.
2. Click **OK**.

    Add as many members as required.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Creating virtual servers

Create a set of virtual servers and assign a pool to each virtual server.

1. Click **Manage**, and on the Load Balancer tab, select **Virtual Servers**, and click "**+**"icon to add a virtual server, and set the following parameters:

    a) Application profile - By default, the service profile that you created in NetScaler Console is displayed.

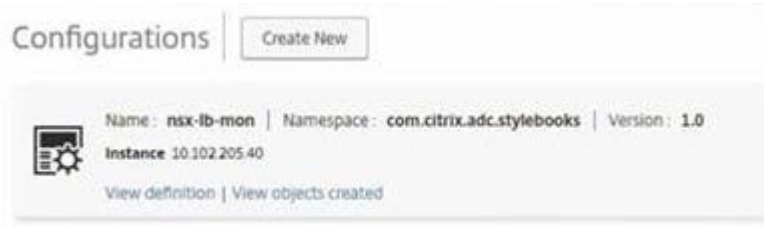
    b) Name - Name of the virtual server.

    c) IP Address - Click Select to select an existing pool of IP addresses or create a new pool of IP addresses.

    d) Default pool - Select the default pool from the drop-down list.

2. Click **OK**.
3. In NetScaler Console, navigate to **Orchestration** > **Requests** to see progress details of completion of service creation on one or more selected NetScaler instances.
4. In NetScaler Console, navigate to **Applications** > **Configuration**, and check that the `nsx-lb-mon` config pack has been created.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Configuring Load Balancing Services on NetScaler VPX in NetScaler Console GUI

Deploy load balancer configurations on the NetScaler instance using NetScaler Console StyleBooks. For HA, the configuration is deployed on both NetScaler instances that are in HA.

To create config packs through StyleBooks:

1. In NetScaler Console, navigate to **Applications** > **Configuration** > **Create New**, and select the **HTTP/SSL LoadBalancing (with Monitors) StyleBook** from the list. The StyleBook opens as a user interface page on which you enter the values for all the parameters defined in this StyleBook.
2. Specify values for all the required parameters.
3. Select the target NetScaler VPX instance that is provisioned in the NSX environment, and click **Create** to apply the configuration on the selected device. For HA deployment, select the instances that are in HA mode.

Verifying Creation of Virtual Servers and Service Groups in NetScaler VPX Instances

You can view that the service groups and virtual servers are created by login on to the NetScaler VPX instance.

To view the service groups and virtual servers:

1. Log on to the NetScaler VPX instance. For HA deployment, you must log on to both NetScaler instances that are in HA.
2. Navigate to **Configuration** > **System** > **Networking**. In the right pane, you can view the IP addresses that are added. Click the IP address hyperlink to see the details. You can see that the subnet IP address is same as the IP address of the web interface that was added in NSX.
3. Next, navigate to **Traffic Management** > **Load Balancing** > **Virtual Servers** and view the virtual server details.
4. Next, navigate to **Service Groups** and view the service group details.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

5. Finally, navigate to **Configuration** > **System** > **Licenses** to view the licenses that are applied to this instance.

Deleting Load Balancing Services

When the load balancing services are no longer required on the NetScaler VPX instances deployed on the NSX manager, you can delete the service insertions that were performed earlier.

To delete configuration and service insertion:

1. In NetScaler Console, Navigate to **Applications** > **Configuration**, select the application configuration created, and then delete the configuration by clicking the "X"icon.
2. In NSX Manager, navigate to the edge gateway to which the NetScaler VPX instance is connected. Navigate to **Manage** > **Load Balancer** > G**lobal Configuration**, right-click on the runtime entry, and then click **Unprovision**. The virtual machine is rendered out of service.
3. In NetScaler Console, navigate to **Orchestration** > **Cloud Orchestration** > **Edge Gateways**. Ensure there is no respective mapping of Edge gateway to deleted instance.

Manage the Kubernetes Ingress configuration in NetScaler Console

July 5, 2024

Kubernetes (K8s) is an open source container orchestration platform that automates the deployment, scaling, and management of cloud-native applications.

Kubernetes provides the Ingress feature which allows client traffic outside the cluster to access microservices of an application running inside the Kubernetes cluster. NetScaler instances can act as the Ingress to applications running inside a Kubernetes cluster. NetScaler instances can load balance and content route North-South traffic from the clients to any microservices inside the Kubernetes cluster.

> **Note**
>
> - NetScaler Console supports the Ingress feature on the clusters with Kubernetes version 1.14–1.21.
> - NetScaler Console supports NetScaler VPX and MPX appliances as Ingress devices.
> - In the Kubernetes environment, the NetScaler instance load balances only the "NodePort" service type.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

You can configure multiple NetScaler instances to act as Ingress devices on the same cluster or different clusters or namespaces. After you configure the instances, you can assign each instance to different applications based on the Ingress policy.

You can create and deploy an Ingress configuration using Kubernetes `kubectl` or APIs. You can also configure and deploy an Ingress from NetScaler Console.

You can specify the following aspects of Kubernetes integration in NetScaler Console:

- **Cluster** –You can register or unregister Kubernetes clusters for which NetScaler Console can deploy Ingress configurations. When you register a cluster in NetScaler Console, specify the Kubernetes API server information. Then, select an agent that can reach the Kubernetes cluster and deploy Ingress configurations.
- **Policies** –Ingress policies are used to select the NetScaler instance based on cluster or namespace to deploy an Ingress configuration. Specify the cluster, site, and instance information when you add a policy.

Before you begin

To use NetScaler instances as Ingress devices on Kubernetes clusters, ensure you have:

- Kubernetes cluster in place.
- Kubernetes cluster registered in NetScaler Console.

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 service account. This binding grants a `ClusterRole` across the cluster to a service account. The following is an example command to bind a `cluster-admin` role to the service account.

   ```
   kubectl create clusterrolebinding citrixadm-sa-admin --clusterrole
       =cluster-admin --serviceaccount=default:citrixadm-sa
   ```

   After binding the NetScaler Console service 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:

   ```
   1 kubectl describe sa citrixadm-sa
   ```

4. Run the following command to obtain the secret string of the token:

   ```
   1 kubectl describe secret <token-name>
   ```

Add the Kubernetes cluster in NetScaler Console

After you configure a NetScaler agent and configure static routes, you must register the Kubernetes cluster in NetScaler Console.

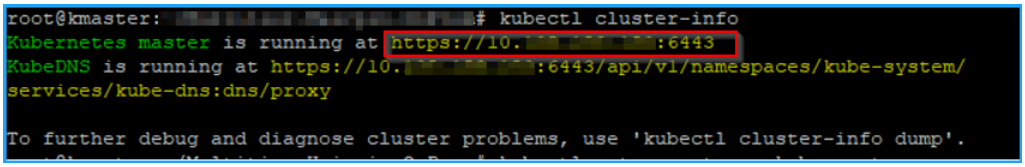
To register the Kubernetes cluster:

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 main node.

      i. On the Kubernetes main 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 the Kubernetes cluster and NetScaler Console. To generate an authentication token:

      i. On the Kubernetes main node, run the following commands:

      ```
      1 kubectl describe secret <token-name>
      ```

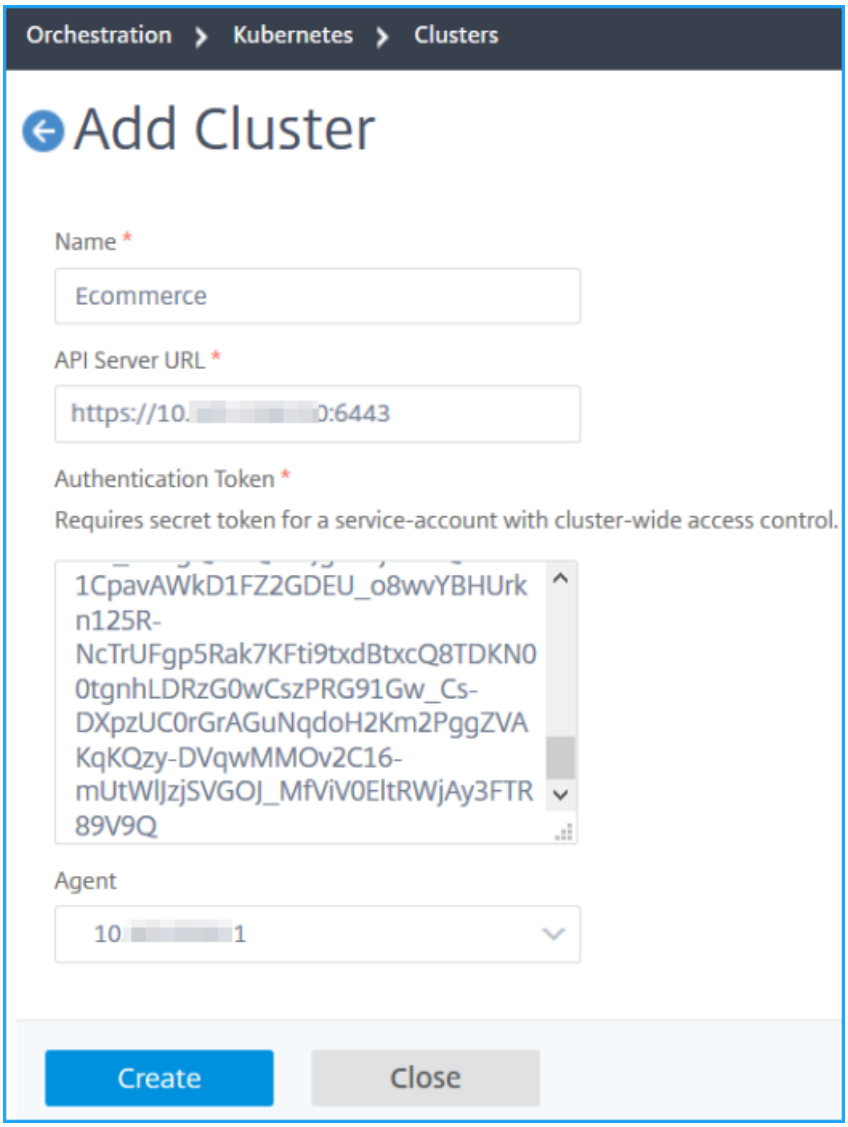
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.



Configure IP address management (IPAM)

September 27, 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

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`
   - **Is it a private endpoint?** - If the Infoblox DDI is privately hosted, select this checkbox and then select an Agent.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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 NetScaler Console, you're only registering the use of Infoblox network within Console. 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 NetScaler Console.

Similarily, If you delete the NetScaler Console IPAM network, NetScaler Console de-registers the Infoblox network. This means that 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

For more information on the Infoblox APIs, see the Infoblox REST API reference guide available at Infoblox DDI.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:

     ```
     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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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 config 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**.

Configure an action policy to receive application event notifications

September 27, 2025

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:

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Event Categories	Event sub categories	Events
		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 laretency 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**.
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 –.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

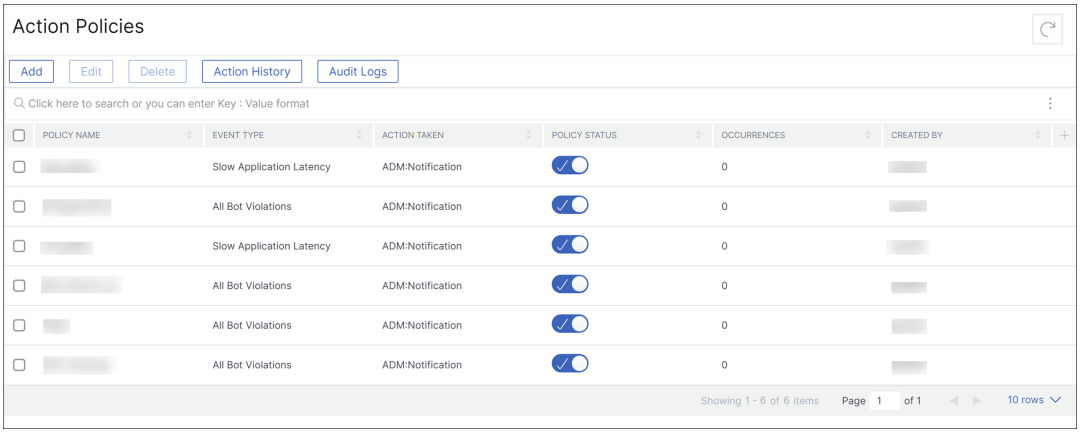
e) **Then Do the Following** –Select **Notify**. After you select **Notify**, the Notification Type option is displayed.

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.
	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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Violation name	Condition	Description
	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.
	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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Violation name	Condition	Description
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.
	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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Violation name	Condition	Description
	Total Attacks	The total attacks for which you want to get notified.
	Violation Type	Select the bot violation from the list.
	Request URL	The URL that you want to configure to block. Specify the URL.
	Vserver name	The associated applications configured for custom applications. Select the application from the list. If you do not add this condition, then all applications from the NetScaler instance are considered.
WAF Violations per Client	Application Name	The custom application name. Select the application from the list. If you do not add this condition, then all applications from the NetScaler instance are considered.
	Instance IP	IP address of the NetScaler instance. Select the IP address from the list.
	Client IP	The source from where the Bot originates. Specify the IP address.
	Total Attacks	The total attacks for which you want to get notified.
	Violation Type	Select the WAF violation from the list.
	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.
App Score Violation	Performance Indicator	The app score components and their threshold values. Select the app score component from the list. For more information, see Select App Score components and set thresholds.
	Breach Count	The breach count for which you want to get notified. For example, if you configure breach count Equal to 5 for response time, you will get notified when the response time threshold is breached 5 times.
	Application Name	Click **Select Applications** to select the applications that you want to get the violation notified.
Client Network Latency	Client Network Average Latency	Specify the client latency (client to NetScaler) value in 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Violation name	Condition	Description
Server Network Latency	Server Network Average Latency	Specify the server latency (server to NetScaler) value in milliseconds for which you want to get notified.
	Server Network Latency Anomalies	Specify the anomaly count for the network latency that you want to get notified.
	Application Name	Click **Select Applications** to select the applications that you want to get the violation notified.
Response Time	Response Avg Time	Specify the value (in milliseconds) for which you want to get notified.
	Response Avg Time Anomalies	Specify the anomaly counts for which you want to get notified.
	Application Name	Click **Select Applications** to select the applications that you want to get notified. If you do not select any application, then it is applied in all applications.
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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Violation name	Condition	Description
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.
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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Violation name	Condition	Description
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.
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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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, 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.

Observability Integration

April 29, 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.
- Configure NetScaler instances for the export of insights to Prometheus using the default schema.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Integration with Splunk

September 27, 2025

You can now integrate NetScaler Console with Splunk to view analytics for:

- WAF violations
- Bot violations
- SSL Certificate Insights
- Gateway insights
- Events and metrics
- HDX™ 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 events, and sends to Splunk periodically. The Splunk Common Information Model (CIM) add-on converts the events to CIM compatible data. As an administrator, using the CIM compatible data, you can view the events in the Splunk dashboard.

For a successful integration, you must:

- Configure Splunk to receive data from NetScaler Console
- Configure NetScaler Console to export data to Splunk
- View dashboards in Splunk

Configure Splunk to receive data from NetScaler Console on-prem

In Splunk, you must:

1. Setup the Splunk HTTP event collector endpoint and generate a token
2. Install the Splunk Common Information Model (CIM) add-on
3. Install the CIM normalizer (applicable only for WAF and bot insights)
4. Prepare a sample dashboard in Splunk

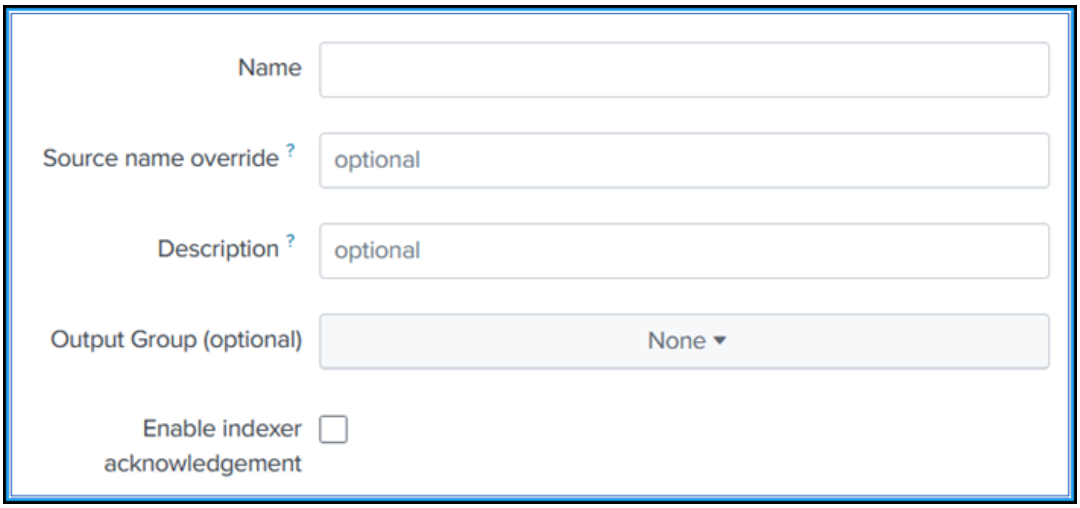
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Setup the Splunk HTTP event collector endpoint and generate a token

You must first setup the HTTP event collector in Splunk. This setup enables the integration between the NetScaler Console and Splunk to send the data. Next, you must generate a token in Splunk to:

- Enable authentication between NetScaler Console and Splunk.
- Receive data through the event collector endpoint.

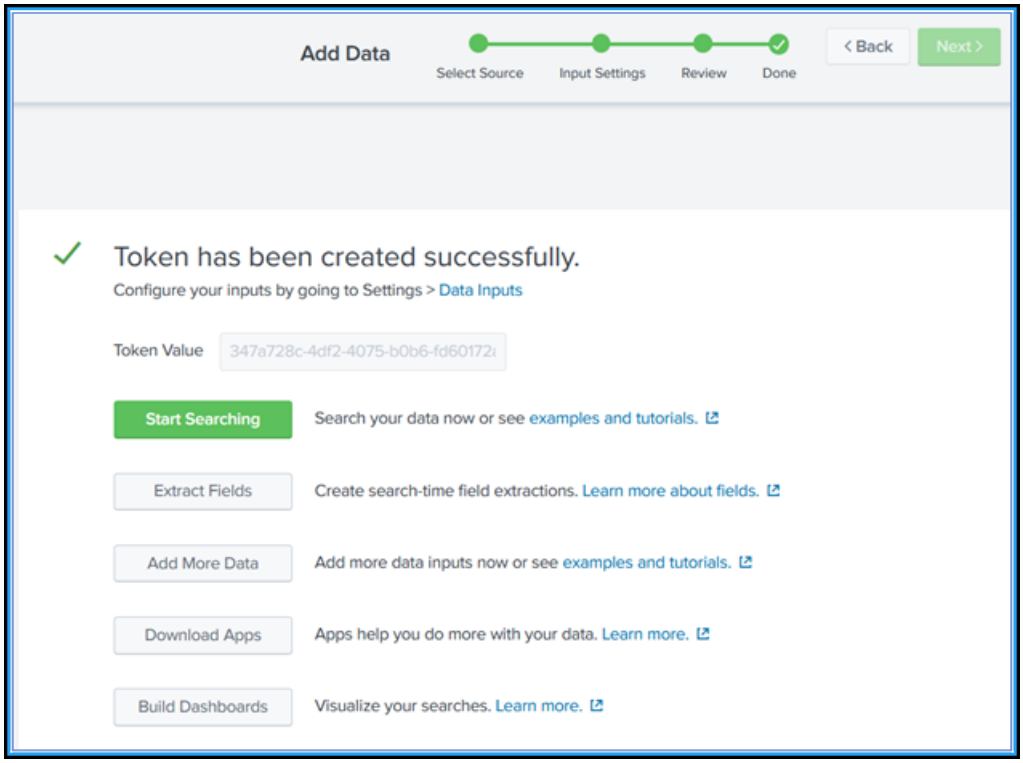
1. Log on to Splunk.
2. Navigate to **Settings > Data Inputs > HTTP event collector** and click **Add new**.
3. Specify the following parameters:
    a) **Name**: Specify a name of your choice.
    b) **Source name override (optional)**: If you set a value, it overrides the source value for HTTP event collector.
    c) **Description (optional)**: Specify a description.
    d) **Output Group (optional)**: By default, this option is selected as None.
    e) **Enable indexer acknowledgement**: NetScaler Console does not support this option. We recommend not to select this option.



4. Click **Next**.
5. Optionally, you can set additional input parameters in the **Input Settings** page.
6. Click **Review** to verify the entries and then click **Submit**.

    A token gets generated. You must use this token when you add details in NetScaler Console.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

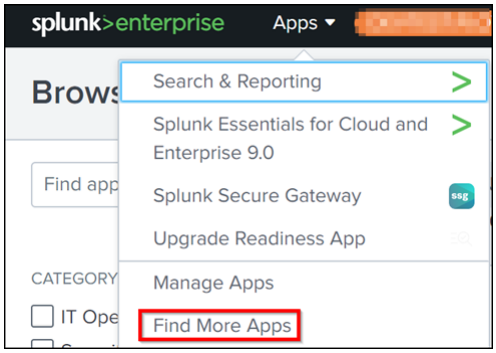


Install the Splunk Common Information Model

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.

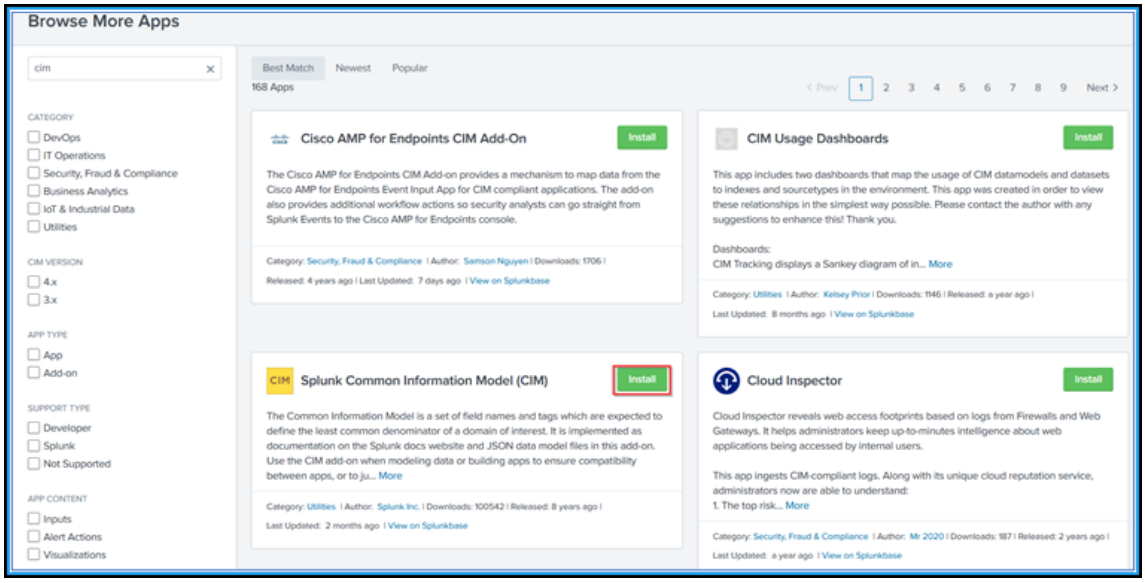
> **Note**
>
> You can ignore this step if you have already installed the Splunk CIM add-on.

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**.

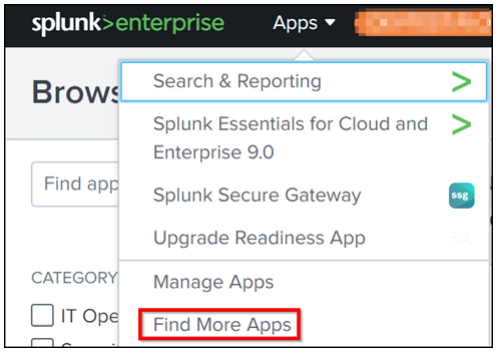
© 1997–2025 Citrix Systems, Inc. All rights reserved.



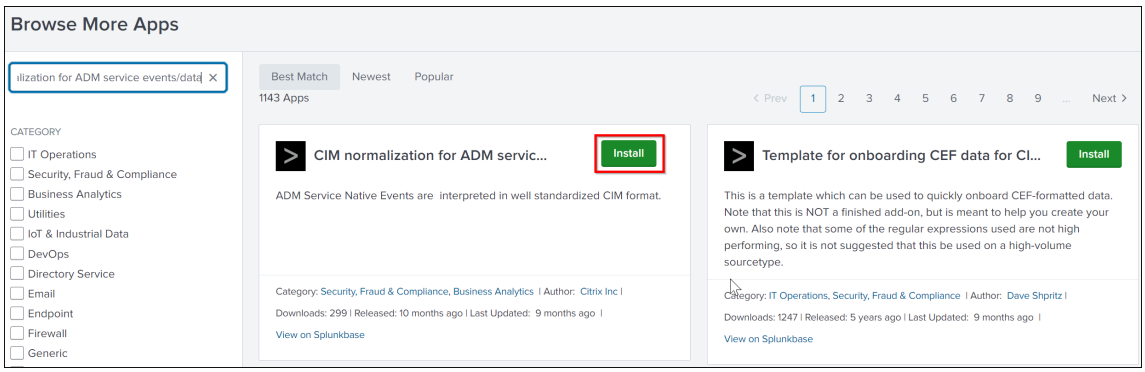
Install the CIM normalizer

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 NetScaler Console service events/data** in the search bar and press **Enter** to get the add-on, and click **Install**.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Prepare a sample dashboard in Splunk

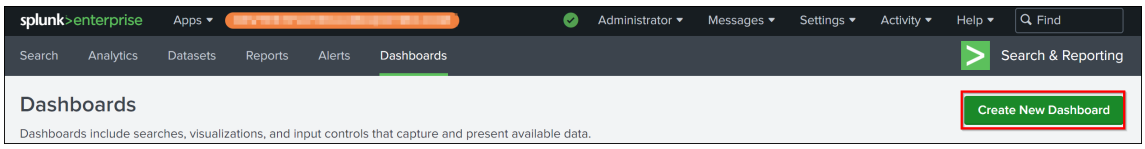
After you install the Splunk CIM, you must prepare a sample dashboard using a template for WAF and Bot, SSL Certificate insights, and events and metrics. You can download the dashboard template (`.tgz`) file, use any editor (for example, notepad) to copy its contents, and create a dashboard by pasting the data in Splunk.

> **Note:**
>
> The following procedure to create a sample dashboard is applicable for all use cases. You must use the required `json` file.

1. Log on to Citrix downloads page and download the sample dashboard available under Sample Dashboards for 3rd party Endpoints.
2. Extract the file, open the `json` file using any editor, and copy the data from the file.

   After you extract, you get three `json` files. Use the:

   - `adm_splunk_security_violations.json` file to create WAF and Bot sample dashboard.
   - `adm_splunk_ssl_certificate.json` file to create SSL certificate insight sample dashboard.
   - `adm_splunk_events_and_metrics_history.json` file to create NetScaler Console events and metrics 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.

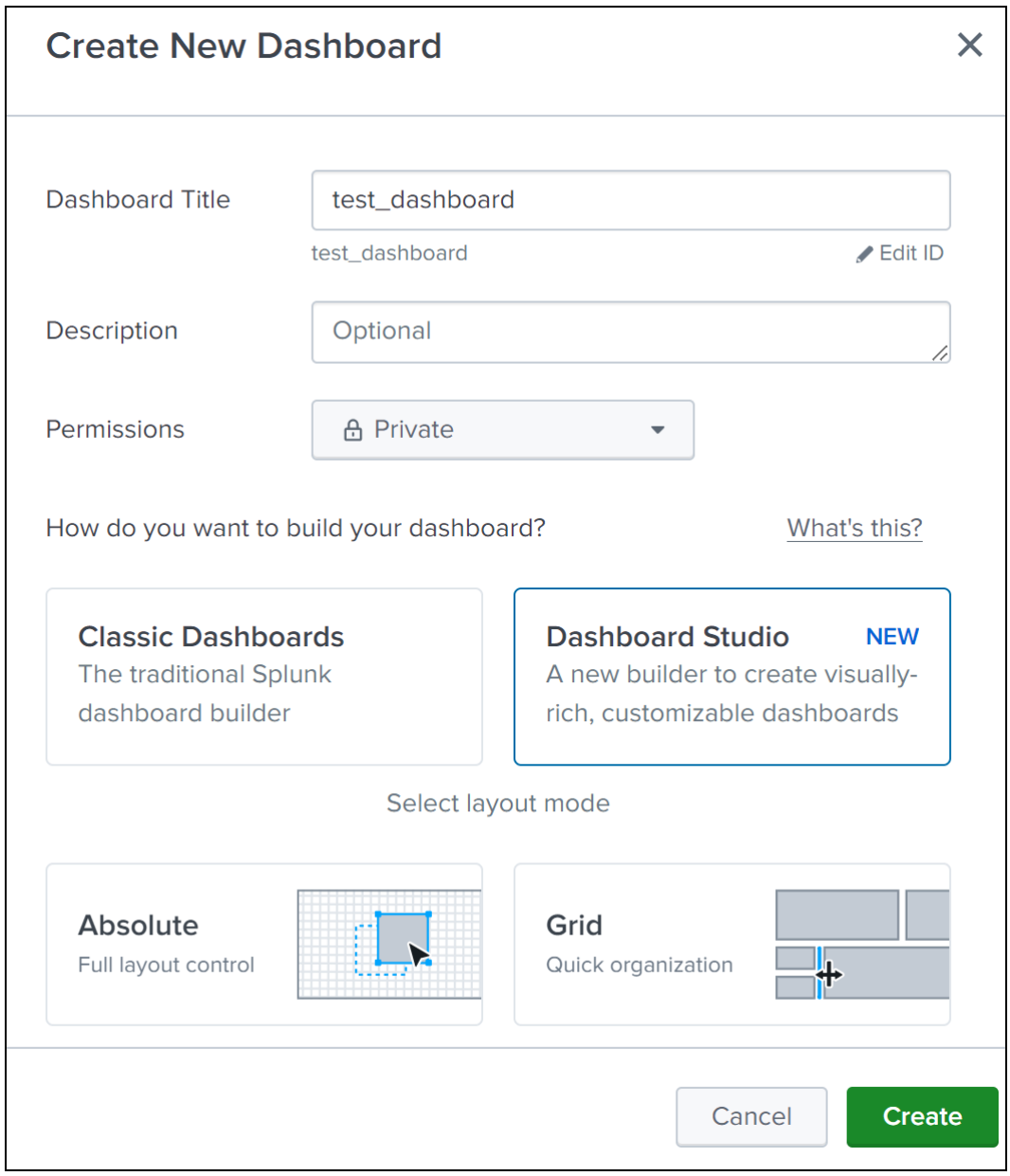
   b) **Description** - Optionally, you can provide a description for your reference.

   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.

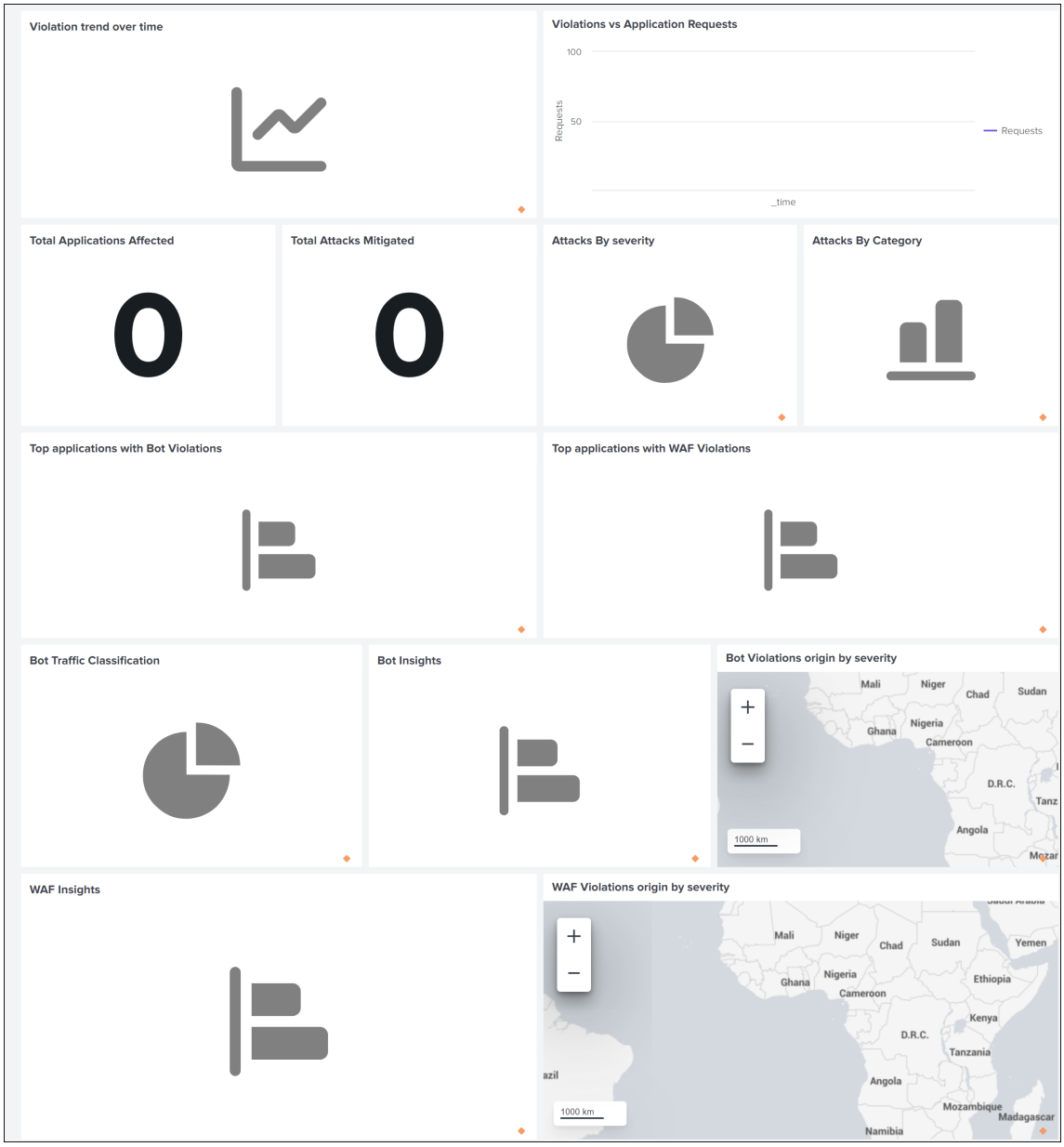


5. Delete the existing data, paste the data that you copied in step 2, and click **Back**.
6. Click **Save**.

   You can view the sample dashboard.

   The following is an example sample dashboard for WAF and bot.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Configure NetScaler Console on-prem 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

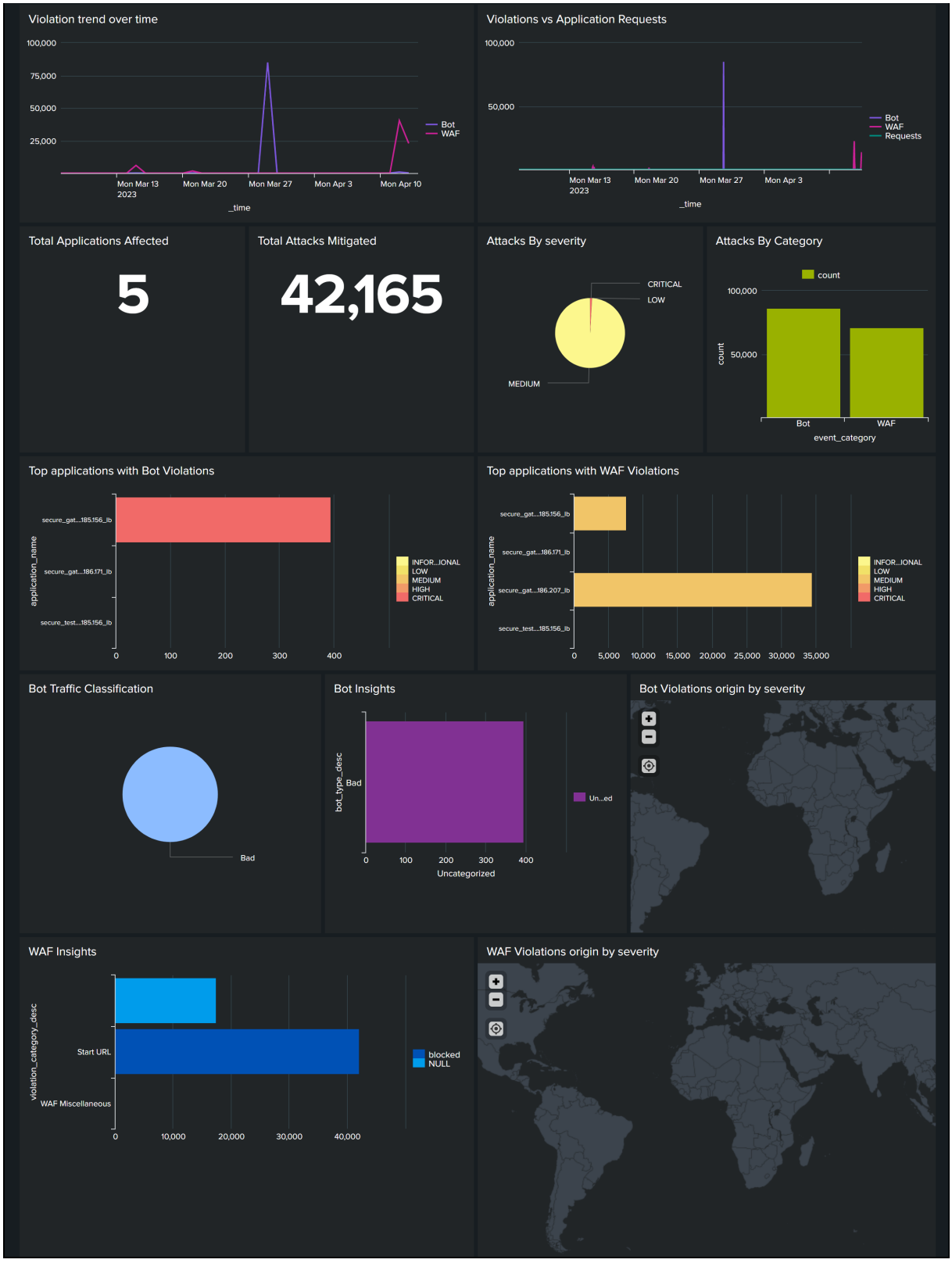
After you complete the configuration in NetScaler Console, the data gets exported from NetScaler Console and the events appear in Splunk.

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.

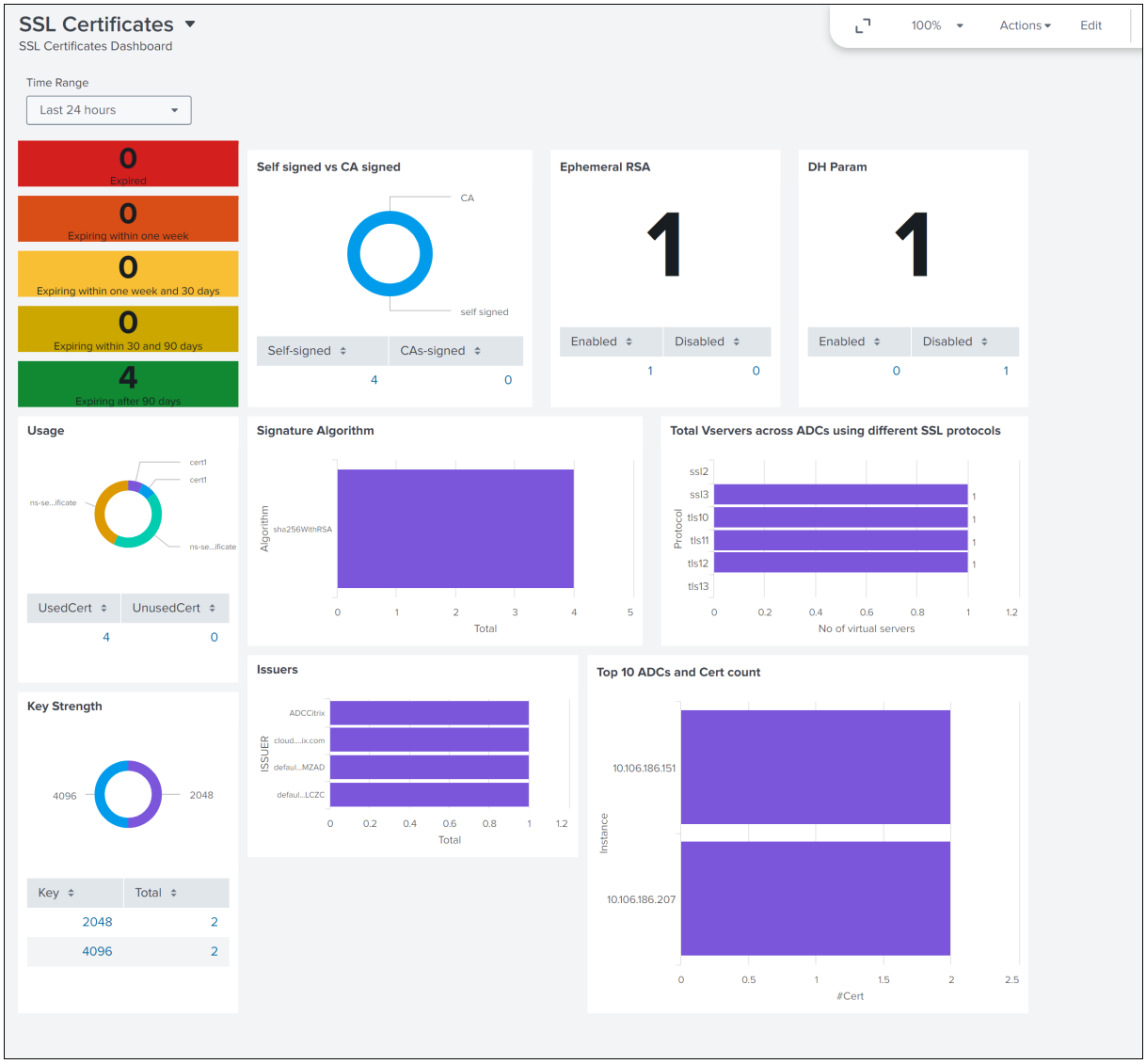
The following is an example for the updated WAF and Bot dashboard:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



The following dashboard is an example for the updated SSL Certificate insights dashboard.

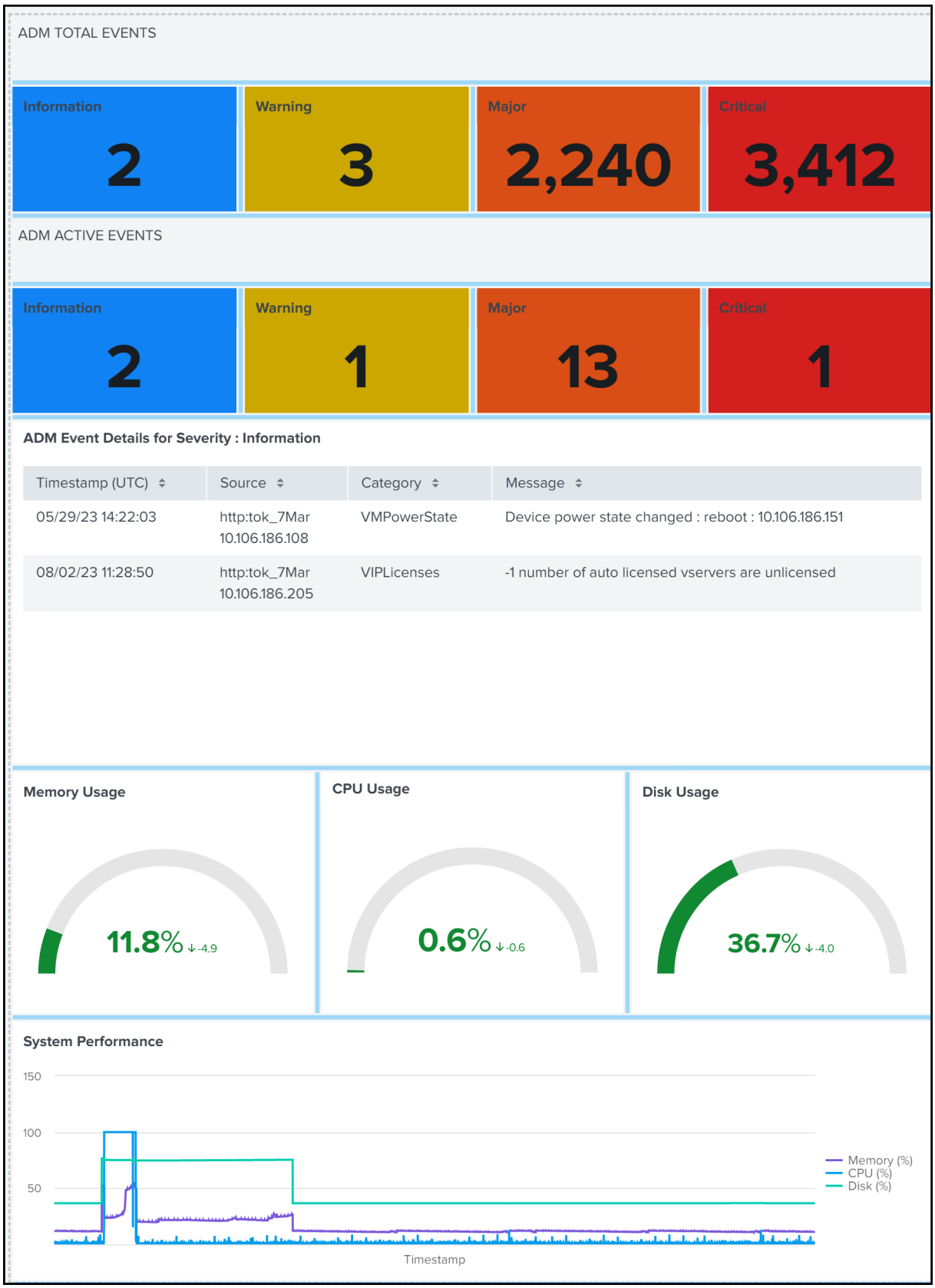
© 1997–2025 Citrix Systems, Inc. All rights reserved.



The following dashboard is an example for the updated events and metrics dashboard.

> **Note:**
>
> The usage data for Memory, CPU, and Disk shows the current value from the NetScaler Console. The up and down trend of these values are shown based on the comparison of the previous value for every 5 minutes.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Apart from 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="metrics"` and select the duration from the list to view the NetScaler Console metrics data.
    - Type `sourcetype="event"` and select the duration from the list to view the NetScaler Console events data.
    - 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="hdx_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.

Integration with New Relic

September 27, 2025

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 and WAF events, and sends them to New Relic either in real time or periodically based on your choice. As an administrator, you can also view the Bot and WAF events in your New Relic dashboard.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Prerequisites

For a successful integration, you must:

- Obtain a New Relic event endpoint in the following format:

  `https://insights-collector.newrelic.com/v1/accounts/<account_id>/events`

  For more information on configuring an event endpoint, see New Relic documentation.

  For more information on getting an account ID, see New Relic documentation.
- Obtain a New Relic key. For more information, see New Relic documentation.
- Add the key details in NetScaler Console

Add the key details in NetScaler Console

After you generate a token, you must add details in NetScaler Console to integrate with New Relic.

1. Log on to NetScaler Console.
2. Navigate to **Settings > Observability Integration**.
3. In the **Integrations** page, click **Add**.
4. In the **Create Subscription** page, specify the following details:
   a) Specify a name of your choice in the **Subscription Name** field.
   b) Select **NetScaler® Console** as the **Source** and click **Next**.
   c) Select **New Relic** and click **Configure**. In the **Configure Endpoint** page:
      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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

g) Click **Next**.

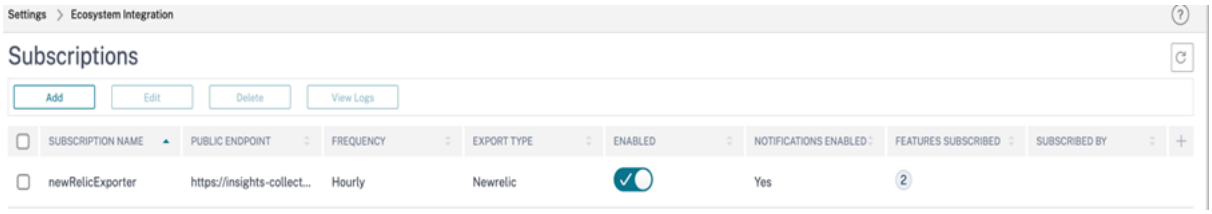
h) In the **Select Instance** tab, you can either choose **Select All Instances** or **Custom select**, and then click **Next**.

- **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.



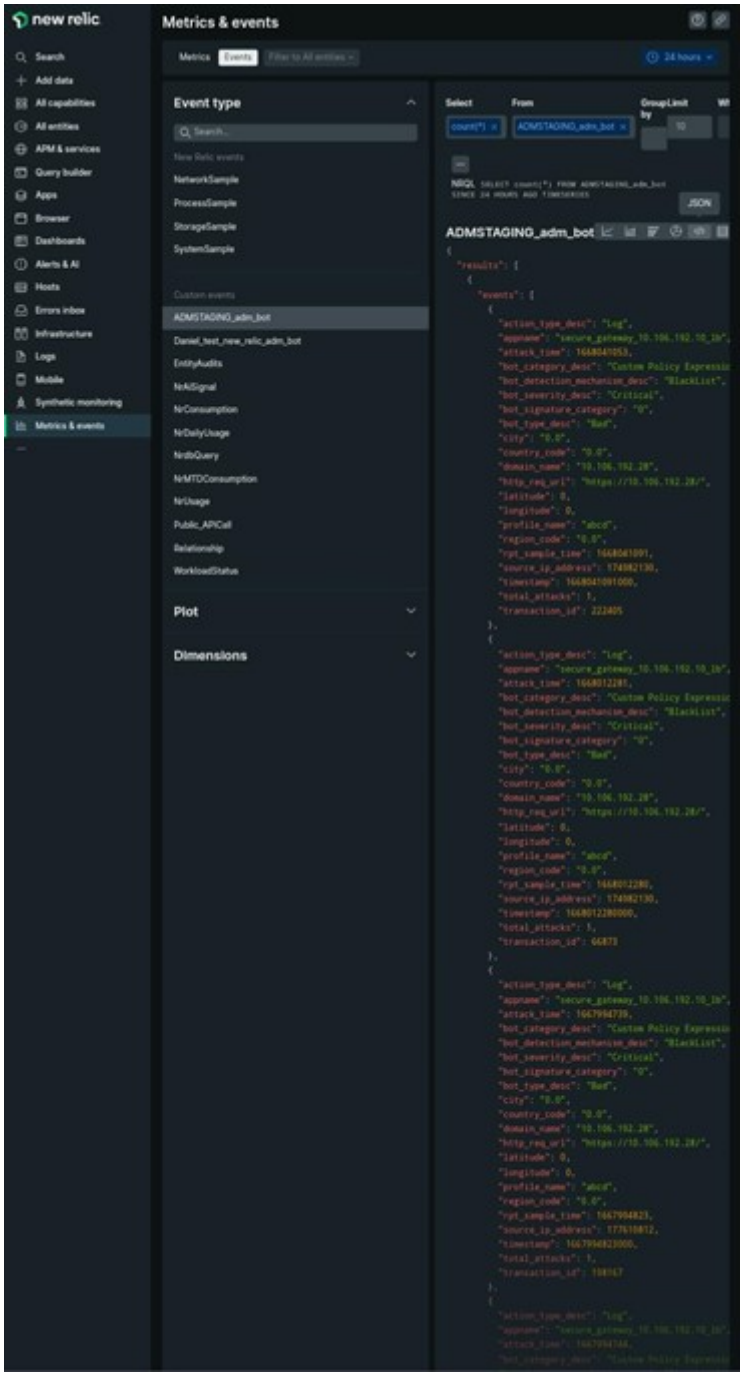
New Relic dashboard

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>.

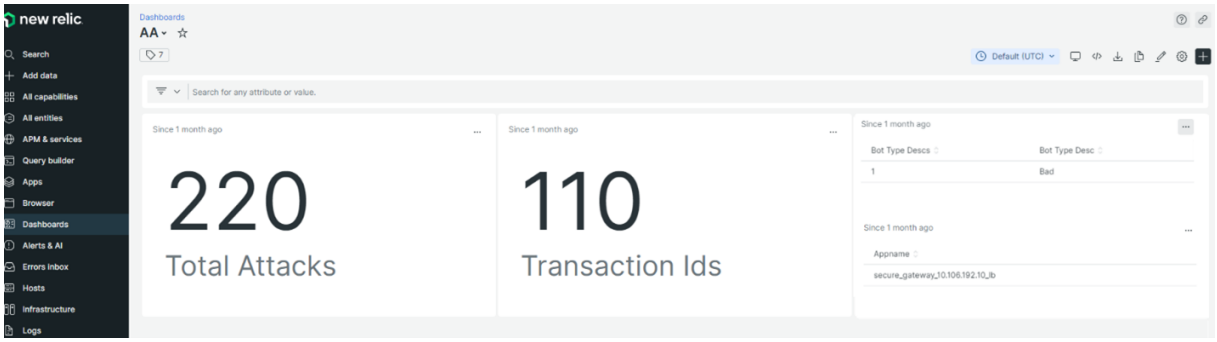
© 1997–2025 Citrix Systems, Inc. All rights reserved.



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 27, 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
- Metrics and events
- NetScaler® Console audit logs

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Microsoft Sentinel provides centralized data collection that gathers data from various sources such as applications, servers, and so on. As an administrator, you can view data and make decisions after the insights or violations are reported in Microsoft Sentinel.

For a successful integration, ensure that you have an active Azure subscription and then follow the procedure under each section:

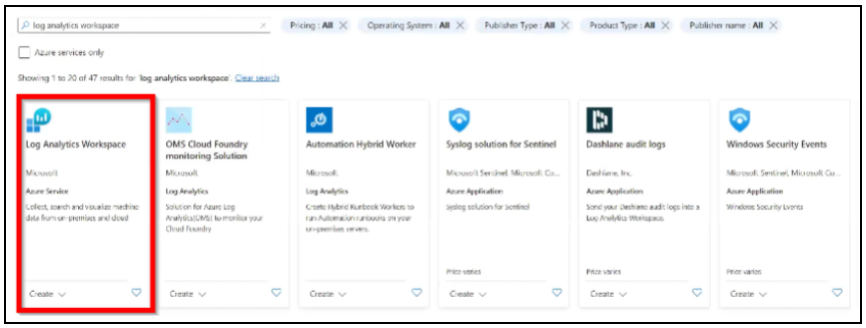
Configure the Log Analytics Workspace

A Log Analytics Workspace is required to store and analyze the collected data.

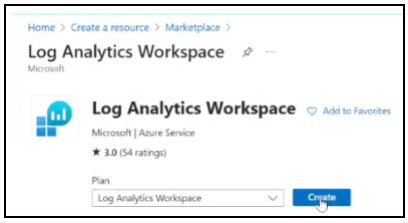
1. Login to Azure.
2. Click **Create a resource**.



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.

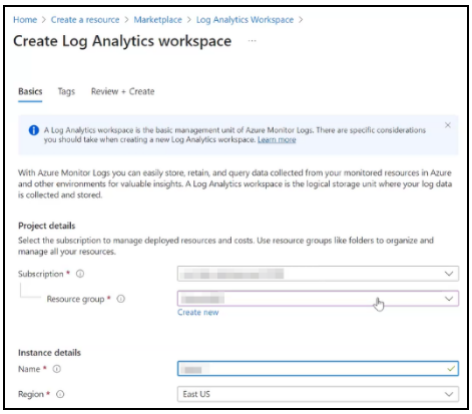
> **Note:**
>
> You can also click **Create new** to add a resource group if you have the privilege.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

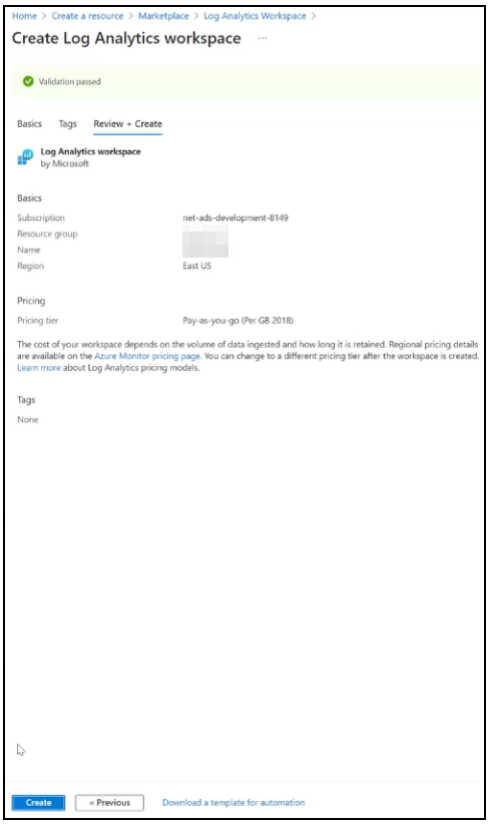
b) Specify a name of your choice.

c) Select your region from the list.

d) Click **Review + Create**.



e) A validation passed message appears. Click **Create** to deploy the workspace.



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.

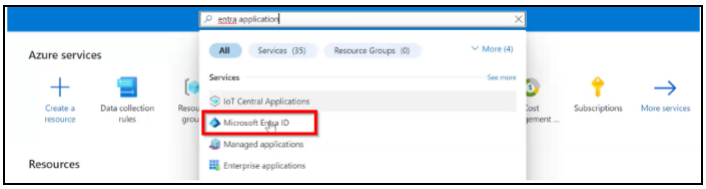


The workspace is successfully created.

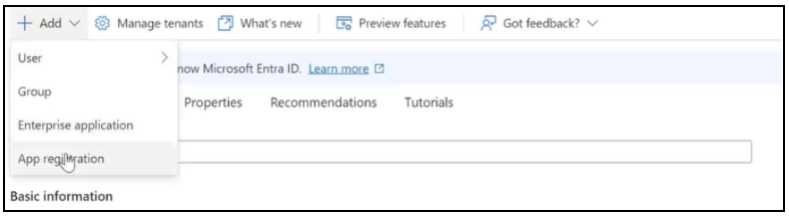
Create a Microsoft Entra application

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**.

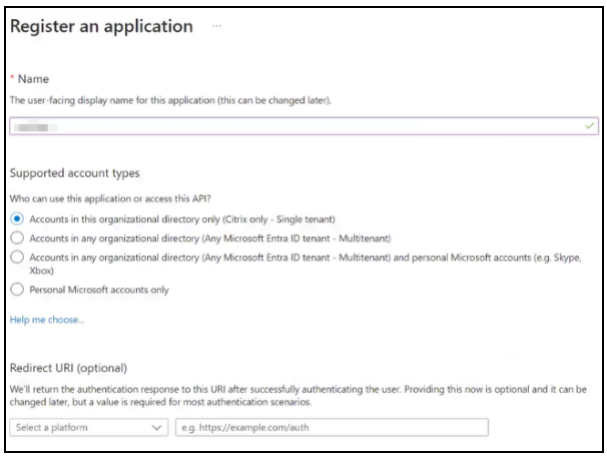


3. Click **Add** and select **App registration**.



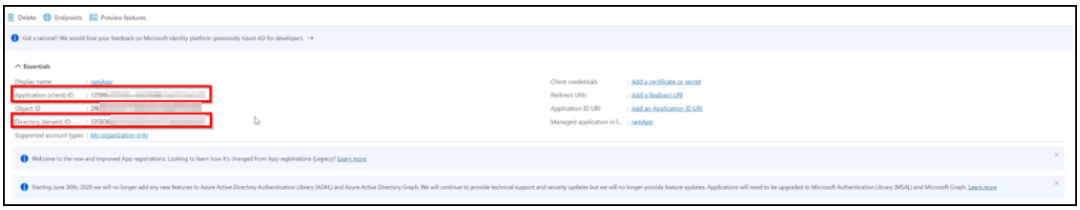
4. Specify a name for the app, select the default option under **Supported account types**, and then click **Register**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



5. After you register the application:

   a) Make a note of **Client ID** and **Tenant ID**.

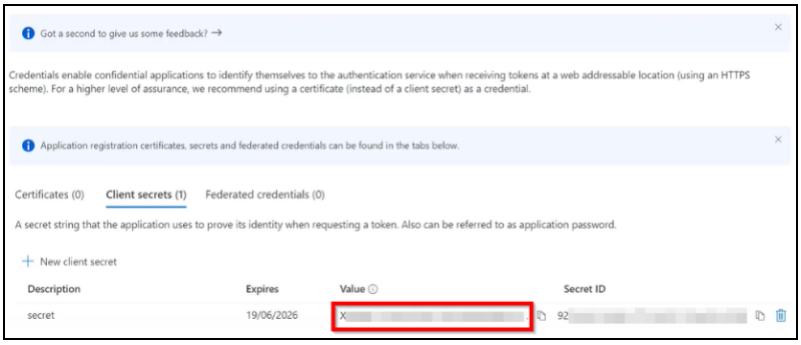


   b) Create a Secret ID for your application. Click **Certificates & secrets** and under **Client secrets**, click **New client secret**. Provide a description, validity, and then click **Add** to create a secret ID for your application.



   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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



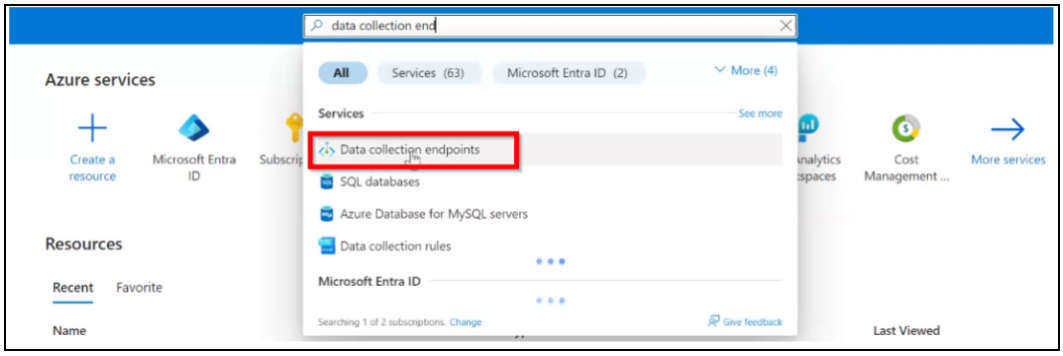
Send data to Microsoft Sentinel by using the Microsoft Entra ID data connector

Microsoft Entra ID logs provide comprehensive information about users, applications, and networks accessing your Entra tenant. For more information, see Send data to Microsoft Sentinel using the Microsoft Entra ID data connector.

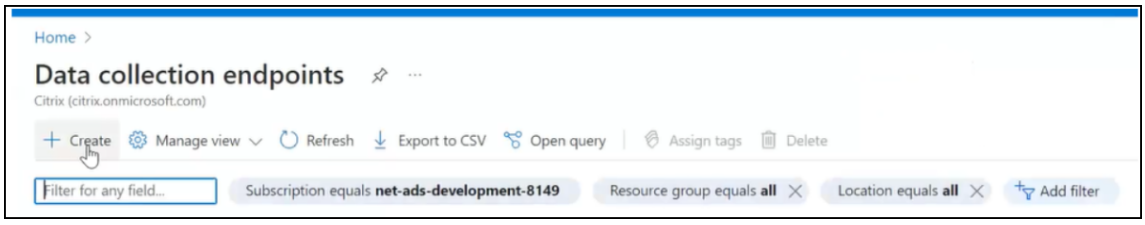
Configure data collection endpoint

You must create a data collection endpoint to get the endpoint URL. This is required when you create a subscription in NetScaler Console.

1. In your Azure portal, under **Azure services**, select **Data collection endpoints** or type the keyword in the search bar.



2. Click **Create** in the **Data collection endpoints** page.



3. In **Create data collection endpoint**:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

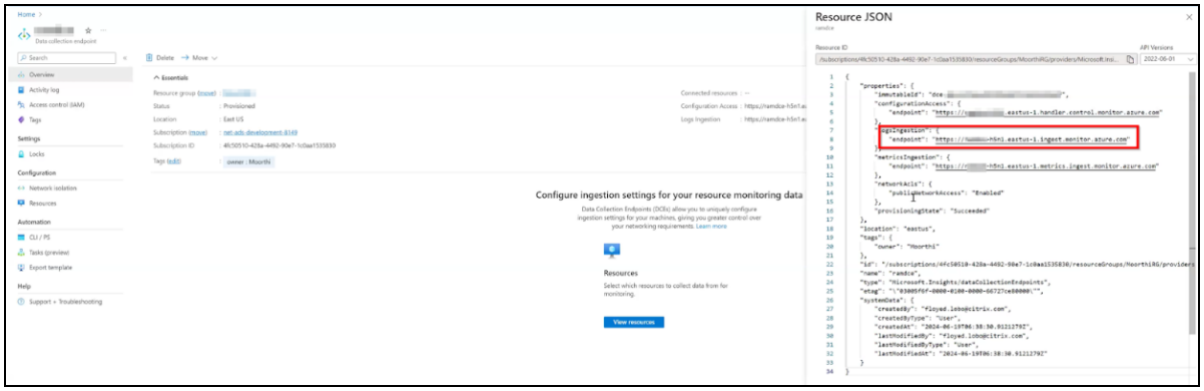
a) Specify an endpoint name of your choice

b) Select the **Subscription, Resource Group**, and **Region**.

c) Click **Review + Create**.

d) After you see the validation passed message, click **Create**.

You must make a note of the endpoint URL. In the **Data collection endpoint** main page, select the created endpoint, click **JSON view**, and make a note of the endpoint ID.



Create tables to export data

You must create a table and provide the JSON information for each insight that you want to export from NetScaler Console to Microsoft Sentinel. You can refer to the following details on the table requirements for each insight:

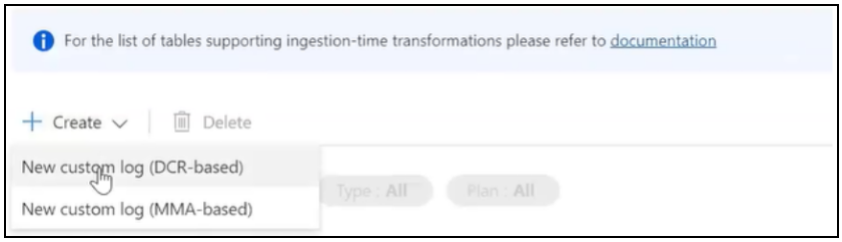
Insights	Total number of tables required
SSL insights	3
WAF	1
Bot	1
Gateway insights	5
Events	1
Metrics	1
Audit logs	1

You can create a maximum of 10 tables for each Data Collection Rule (DCR). Beyond 10 tables, you must create another DCR.

1. Navigate to your workspace in the Azure portal and click **Tables** under **Settings**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. Click **Create** and select **New custom log (DCR-based)**



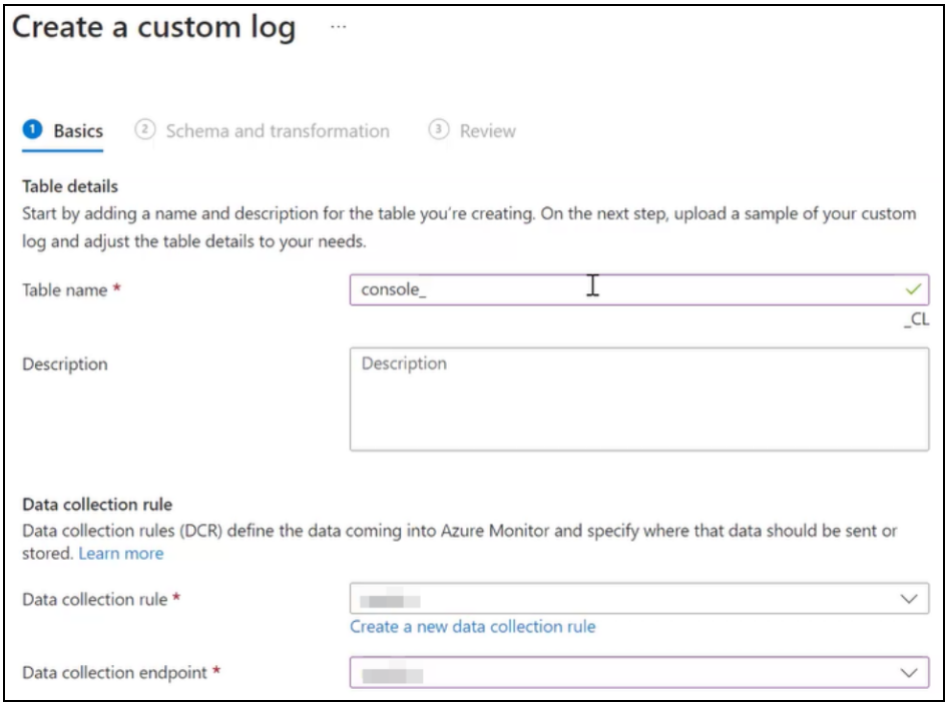
3. In **Create a custom log**:

   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.



   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
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
Events	{ "rpt_sample_time": -1, "category": " HealthMonitoring", " entity": " 10.106.186.148: HealthMonitoring: System Disk Usage", " counter_threshold_value ": "", "id": "0 f2607cf-f97d-4f71 -9162-11e580262e93", "timestamp": 1712927472, "message" : "Disk Usage High: 63.24%", "severity": "Critical", " user_name": "", " device_entity_type": "", "device_type": "" , " counter_actual_value" : "", " cmd_auth_status": "", "source": " 10.106.186.148", " history": "Update Time= Fri, 12 Apr 2024 06:32:49 UTC , Previous Severity= Critical ,New Severity= Critical, Source= 10.106.186.148\ nUpdate Time= Fri, 12 Apr 2024 06:27:46 UTC ,Previous Severity= Critical , New Severity= Critical, Source= 10.106.186.148\ nUpdate Time= Fri, 12 Apr 2024 06:22:44 UTC ,Previous Severity= Critical ,	console_event

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Insights	JSON	Table name to be used
Metrics	{ "memory_free": 28830060544.0, "disk_used": 81248694272.0, "disk_free": 29632114688.0, "node_type": "", "memory_total": 34355544064.0, "cpu_usage": 0.49, "disk_total": 120522616832.0, "disk_usage": 73.28, "node_id": "", "id": "1be15a09-d078-469c-868a-bfbfcffe5ef1", "disk_total_capacity": 0.0, "page_size": 4096.0, "memory_usage": 16.08, "table_name": "mps_health"}	console_mps_health
Audit logs	{ "system_gmt_time":1721868291, "source":"X.X.X.X", "severity":"INFO", "module":"DEVICECONFIG", "event_type":"CMD_EXECUTED", "message":"Sample Mesage", "instance_ip":"X.X.X.X", "app_name":""}	console_syslog_messages

After uploading the JSON, you can view the following details:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Click **Transformation editor**, enter the following query that is applicable for the appropriate insight, and click **Run** to accept the data starting from the poll time in NetScaler Console.

- **SSL** - `source | extend TimeGenerated = todatetime(poll_time)| project-rename sslvserver_id = id`
- **WAF** and **Bot** - `source | extend TimeGenerated = todatetime(rpt_sample_time)`
- **Gateway Insight** - `source | extend TimeGenerated = todatetime(rpt_sample_time)`



5. Click **Next** and click **Create** to complete.
6. Navigate to **Data collection rules**, click the DCR that you have created.
7. Under **Configuration**, click **Data sources** to view the created table.

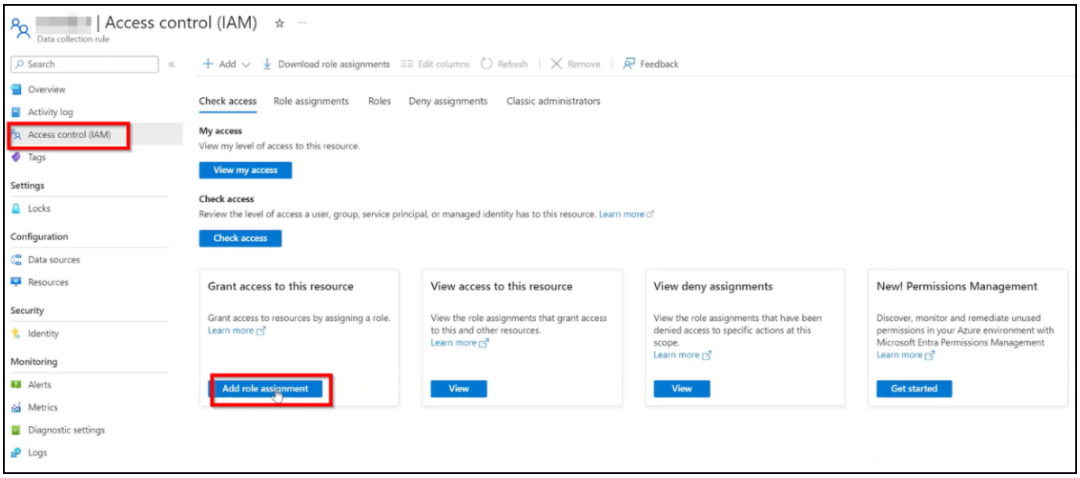


The DCR (Data collection rule) requires access to the **Monitoring Metrics Publisher** role.

a) Navigate to your DCR that you can access from your Azure portal under **Recents**.

b) Click **Access control (IAM)** from your DCR page and click **Add role assignment**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



c) In the search bar, type the keyword monitor to select **Monitoring Metrics Publisher** and click **Next**.

d) In the **Members** tab, click **Select Members** and select the Entra app that you created.

e) Click **Review + assign**.

You must make a note of the Data collection rules ID. Navigate to the Data collection rules page, select your DCR, and click the JSON view to make a note of the ID.



Create a subscription in NetScaler Console

You now have everything ready. The final step is to configure NetScaler Console by creating a subscription and adding the required details. To create a subscription in NetScaler Console, you need the following details that you have noted:

- Endpoint URL
- Data collection rules ID
- Tenant ID
- Client ID

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Client secret

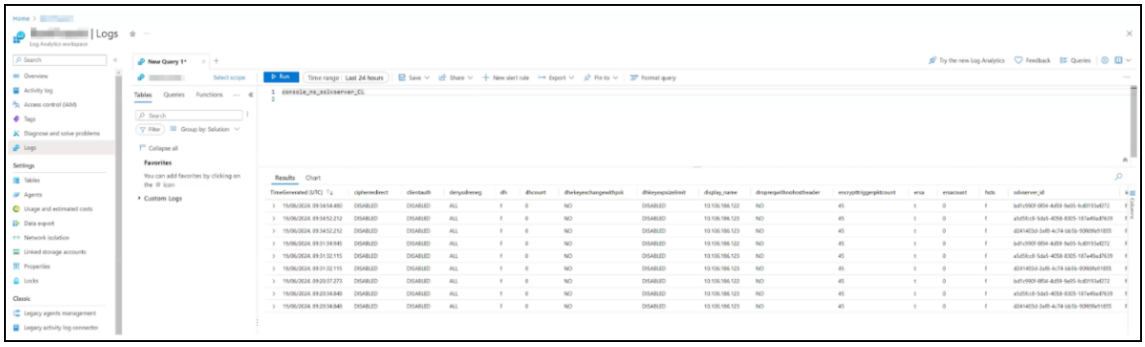
1. Login to NetScaler Console.
2. Navigate to **Settings > Observability Integration**.
3. In the **Integrations** page, click **Add**.
4. In the **Create Subscription** page, specify the following details:
    a) Specify a name of your choice in the Subscription Name field.
    b) Select **NetScaler Console** as the **Source** and click **Next**.
    c) Select **Microsoft Sentinel** and click **Configure**. In the **Configure Endpoint** page, enter all details, and click **Submit**.
    d) Click **Next**.
5. Click **Add Insights** and in the **Select Feature** tab, depending upon the tables that you have added in Microsoft Azure, select the features that you want to export and click **Add Selected**, and click **Next**.
6. In the **Select Instance** tab, you can either choose **Select All Instances** or **Custom select**, and then click **Next**.
    - **Select All Instances** - Exports data to Microsoft Sentinel from all the NetScaler instances.
    - **Custom select** - Enables you to select the NetScaler instances from the list. If you select specific instances from the list, then the data is exported to Microsoft Sentinel only from the selected NetScaler instances.
7. Click **Submit**.

View logs in Microsoft Azure

After you configure everything, we recommend that you wait until 30 minutes to view details in Microsoft Azure.

1. In your Azure portal, navigate to your **Log Analytics Workspace**.
2. Click **Logs**, provide the table name, and click **Run** to view results.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

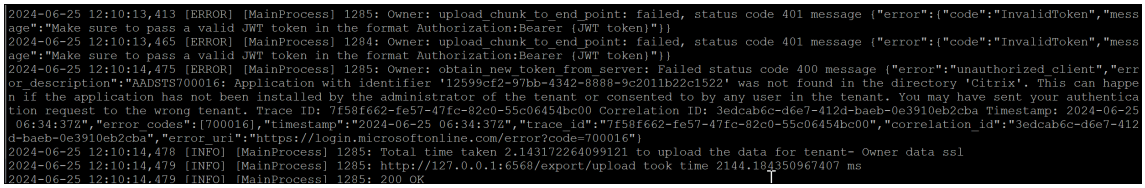


You can also troubleshoot and use the logs to verify the configurations. For example, use the Poll Now option in NetScaler Console GUI for the configured insight and:

1. Login to your NetScaler Console using an SSH client.
2. Type shell to enter bash mode.
3. Use the following command to view logs:

   ```
   tail -f /var/mps/log/nbs/nbs_api.log
   ```

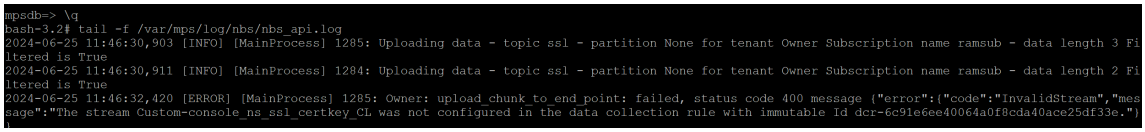
The following examples help you analyze the possible errors for troubleshooting:

1. 

   ```
   2024-06-25 12:10:13,413 [ERROR] [MainProcess] 1285: Owner: upload_chunk_to_end_point: failed, status code 401 message {"error":{"code":"InvalidToken","mess
   age":"Make sure to pass a valid JWT token in the format Authorization:Bearer {JWT token}"}}
   2024-06-25 12:10:13,465 [ERROR] [MainProcess] 1284: Owner: upload_chunk_to_end_point: failed, status code 401 message {"error":{"code":"InvalidToken","mess
   age":"Make sure to pass a valid JWT token in the format Authorization:Bearer {JWT token}"}}
   2024-06-25 12:10:14,475 [ERROR] [MainProcess] 1285: Owner: obtain_new_token_from_server: Failed status code 400 message {"error":"unauthorized_client","err
   or_description":"AADSTS700016: Application with identifier '12599cf2-97bb-4342-8888-9c2011b22c1522' was not found in the directory 'Citrix'. This can happe
   n if the application has not been installed by the administrator of the tenant or consented to by any user in the tenant. You may have sent your authentica
   tion request to the wrong tenant. Trace ID: 7f58f662-fe57-47fc-82c0-55c06454bc00 Correlation ID: 3edcab6c-d6e7-412d-baeb-0e3910eb2cba Timestamp: 2024-06-25
    06:34:37Z","error_codes":[700016],"timestamp":"2024-06-25 06:34:37Z","trace_id":"7f58f662-fe57-47fc-82c0-55c06454bc00","correlation_id":"3edcab6c-d6e7-412
   d-baeb-0e3910eb2cba","error_uri":"https://login.microsoftonline.com/error?code=700016"}
   2024-06-25 12:10:14,478 [INFO] [MainProcess] 1285: Total time taken 2.143172264099121 to upload the data for tenant- Owner data ssl
   2024-06-25 12:10:14,479 [INFO] [MainProcess] 1285: http://127.0.0.1:6568/export/upload took time 2144.184350967407 ms
   2024-06-25 12:10:14,479 [INFO] [MainProcess] 1285: 200 OK
   ```

   This log indicates that you have provided an invalid Client ID for the Microsoft Sentinel subscription in NetScaler Console (**Settings > Observability Integrations**).

   Workaround: Ensure that you have copied the right Client ID and edit the subscription by providing the right Client ID. For more information, see Create a Microsoft Entra application.

2. 

   ```
   mpsdb=> \q
   bash-3.2# tail -f /var/mps/log/nbs/nbs_api.log
   2024-06-25 11:46:30,903 [INFO] [MainProcess] 1285: Uploading data - topic ssl - partition None for tenant Owner Subscription name ramsub - data length 3 Fi
   ltered is True
   2024-06-25 11:46:30,911 [INFO] [MainProcess] 1284: Uploading data - topic ssl - partition None for tenant Owner Subscription name ramsub - data length 2 Fi
   ltered is True
   2024-06-25 11:46:32,420 [ERROR] [MainProcess] 1285: Owner: upload_chunk_to_end_point: failed, status code 400 message {"error":{"code":"InvalidStream","mes
   sage":"The stream Custom-console_ns_ssl_certkey_CL was not configured in the data collection rule with immutable Id dcr-6c91e6ee40064a0f8cda40ace25df33e."}
   ```

   This log indicates that you have not configured the required ssl_certkey table in your Microsoft Azure.

   Workaround: Configure a table for ssl_certkey in Microsoft Azure. For more information, see Create tables to export data.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Configure NetScaler® instances for the export of insights to Prometheus using the default schema

September 27, 2025

NetScaler supports directly exporting metrics to Prometheus. You can use the rich set of metrics provided by NetScaler instance to monitor NetScaler health and application health. For example, you can gather metrics on CPU and memory usage to know the NetScaler health. Similarly, you can use metrics like the number of HTTP requests received per second or the number of active clients to monitor application health.

To export the metrics to Prometheus, you must configure an analytics profile with type as time series. For more information, see Monitor NetScaler, applications, and application security using Prometheus.

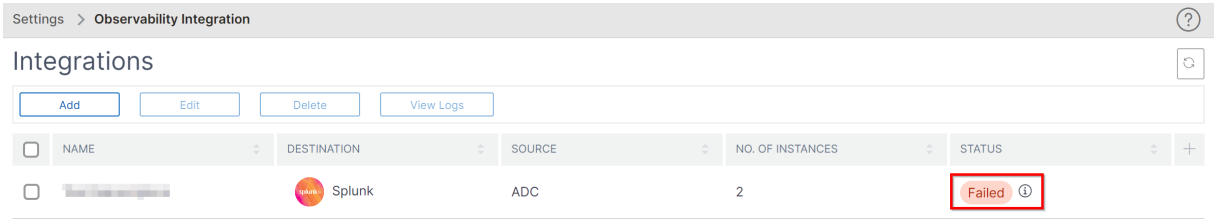
With the Observability Integration feature in NetScaler Console, you can configure the export of insights to Prometheus using the default schema.

1. Navigate to **Settings > Observability Integration**.
2. In the **Integrations** page, click **Add**.
3. In the **Create Subscription** page, specify the following details:
    a) Specify a name of your choice in the **Subscription Name** field.
    b) Select **NetScaler** as the **Source** and click **Next**.
    c) Select **Prometheus** as the Destination.
    d) Select **Default** for the default insights to the exported.
    e) Click **Add Instances** and select the instances for which you want to export insights to Prometheus.
    f) Click **Submit**.

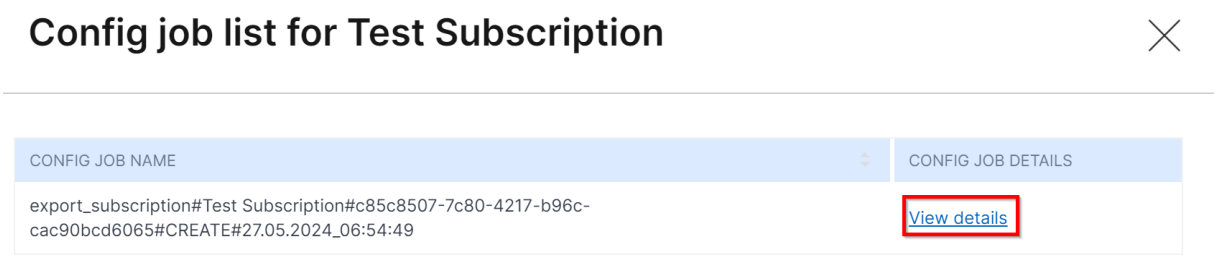
View logs for failed configurations

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.

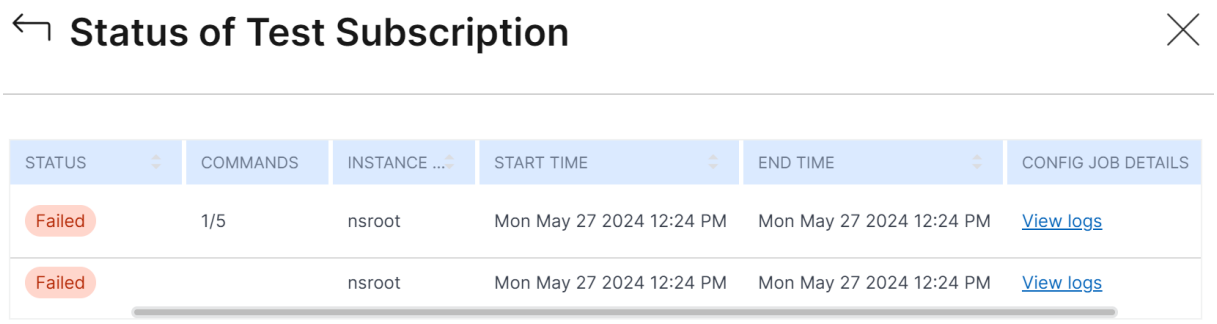
© 1997–2025 Citrix Systems, Inc. All rights reserved.



Click **View details** under **Config job details**.



Click **View logs** to view details of the issue.



Configure the export of NetScaler® metrics and audit logs to Splunk

September 27, 2025

NetScaler supports direct export of metrics to Splunk in the JSON format. NetScaler provides rich metrics to monitor your application health and application security health. By exporting the metrics provided by NetScaler to Splunk, you can visualize the metrics and get meaningful insights.

Audit logging enables you to log the NetScaler states and status information collected by various modules in NetScaler. By reviewing the logs, you can troubleshoot problems or errors and fix them.

For more information, see:

- Export audit logs directly from NetScaler to Splunk
- Export metrics directly from NetScaler to Splunk

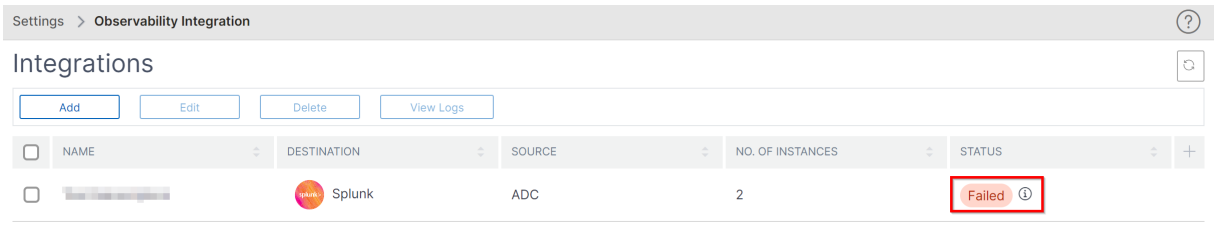
© 1997–2025 Citrix Systems, Inc. All rights reserved.

To configure the export of metrics and audit logs to Splunk through NetScaler Console:

1. Navigate to **Settings > Observability Integration**.
2. In the **Integrations** page, click **Add**.
3. In the **Create Subscription** page, specify the following details:
    a) Specify a name of your choice in the **Subscription Name** field.
    b) Select **NetScaler** as the **Source** and click **Next**.
    c) Select **Splunk** as the **Destination** and click **Configure**. In Configure Endpoint:
        - **Endpoint URL** - Specify the Splunk endpoint details. The end point must be in the `https://SPLUNK_PUBLIC_IP:SPLUNK_HEC_PORT/services/collector/event`‘ format.
        - **Authentication Token** - Copy and paste the authentication token from Splunk.
        - Click **Submit**.
    d) Click **Next**.
    e) Click **Add Insights** and select **NetScaler Metrics** and **NetScaler Audit Logs**, and then click **Add Selected**.
    f) Click **Next**.
    g) Click **Add Instances** and select the instances.
    h) Click **Submit**.

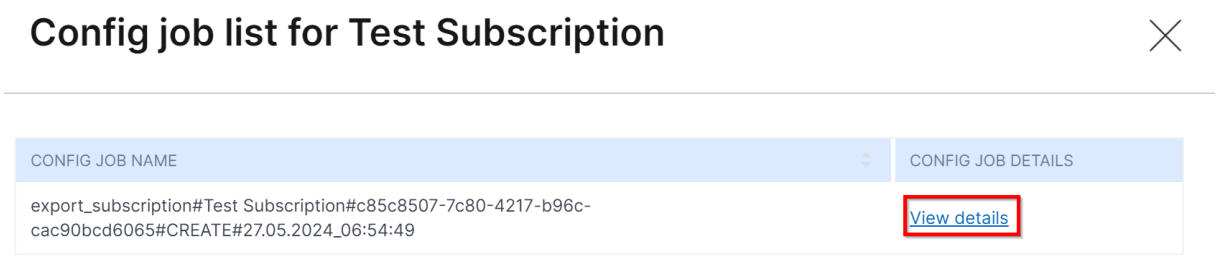
View logs for failed configurations

After you create a subscription, you can view the status of the created subscription at **Settings > Observability Integration**. If the status shows **Failed**, click to view details.

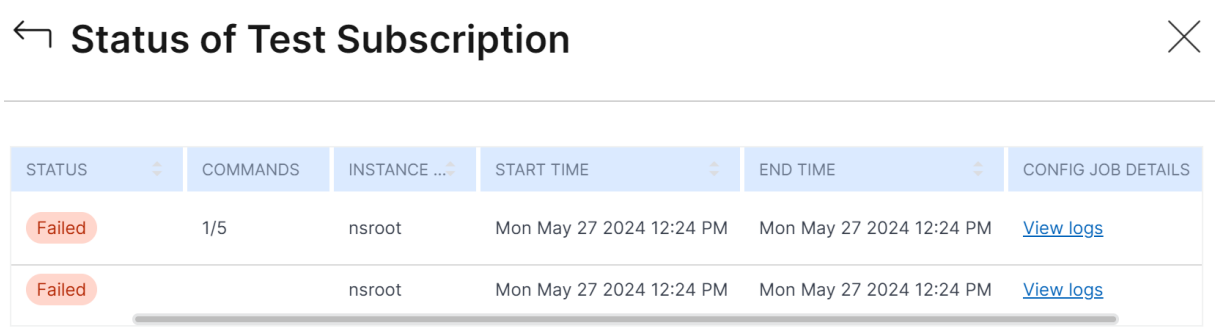


Click **View details** under **Config job details**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Click **View logs** to view details of the issue.



Access control lists

September 27, 2025

An access control list (ACL) is a set of conditions that you can apply to a network appliance to filter IP traffic and secure your appliance from any unauthorized access.

You can configure ACL in NetScaler Console GUI to limit and control access to NetScaler Console. ACL on NetScaler Console is supported from 14.1-29.x build.

Usage guidelines

- When you upgrade NetScaler Console to 14.1-29.x build, the ACL feature is disabled by default.
- As an administrator, you can control only inbound packets through ACL on NetScaler Console.
- Any configurations on NetScaler Console do not require any changes in the existing ACL configuration.

How to Configure an ACL

Configuring an ACL involves:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Enable the ACL feature
- Create an ACL rule
- Enable the ACL rule

Enable the ACL feature

1. Log on to NetScaler Console GUI and navigate to **Settings > Access Control List (ACL)**
2. By using the toggle button, turn on the ACL feature.



Create an ACL rule

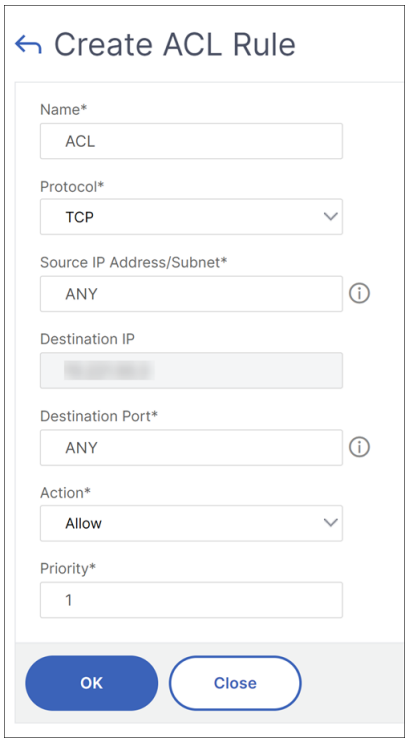
1. On the ACL page, click **Create Rule**.
2. In the **Create Rule** window, add the details listed in the following table:

Options	Description
Name	Specify a name of your choice.
Protocol	Select a protocol from the menu. By default, TCP is selected. You can select ANY to allow all protocols.
Source IP Address/Subnet	Specify the source IP address or source subnet to which the rule applies. Select ANY if the rule must be applied to all incoming traffic.
Destination IP	The NetScaler Console IP address is autopopulated as the destination IP. This field cannot be edited.
Destination port	Specify the destination port to which the rule applies. Select ANY if the rule applies to all destination ports.
Action	Select the action for the rule, which is Allow or Deny.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Options	Description
Priority	Assign priority to specify the order in which the rule is to be evaluated. Priority numbers determine the order in which ACL rules are matched against an incoming packet. A lower priority number has a higher priority. For example, priority number 1 has a higher priority than priority number 2. If none of the rules match with the incoming packet, then the packet is blocked.

3. Click **OK** to create the rule.



After the rule is created, it is in the disabled state. To make the rule effective, you must enable the rule.

> **Note:**
>
> To enable a rule, the ACL feature must be enabled. If the feature is disabled, and you attempt to enable an ACL rule, a message “ACL is not running”appears.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Enable an ACL rule

1. Hover your mouse over the rule that you want to enable and click the circle with three dots.
2. From the menu, select **Enable**.
3. Alternatively, select the radio button for that rule and click the Enable tab.
4. At the prompt, click **Yes** to confirm.

Other actions for ACL rules

You can apply the following actions to the ACL rules:

- Disable an ACL rule
- Edit an ACL rule
- Delete an ACL rule
- Renumber the priority of ACL rules

Disable an ACL rule

1. Hover the mouse over the rule that you want to disable and select the circle with three dots.
2. Click **Disable** from the list.
3. Alternatively, select the radio button for that rule and click the **Disable** button.
4. Click **Yes** to confirm.

> **Note:**
>
> When you disable a rule, the rule no longer applies to incoming traffic. However, the rule configuration remains under ACL settings.

Edit an ACL rule

1. Hover the mouse over the rule that you want to edit and select the circle with three dots.
2. Click **Edit Rule** from the list.
3. Alternatively, select the radio button for that rule and click the **Edit Rule** button.
4. Make the edits and click **OK**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> You can edit a rule in both enabled and disabled state. If you edit a rule that is already enabled, the edits get applied immediately. For a rule in the disabled state, the edits get applied when you enable the rule.

Delete an ACL rule

1. Ensure that the rule is in the disabled state. You cannot delete a rule in the enabled state.
2. Hover the mouse over the rule that you want to delete and select the circle with three dots.
3. Click **Delete Rule** from the list.
4. Alternatively, select the radio button for that rule and click the **Delete Rule** button.
5. Click **Yes** to confirm.

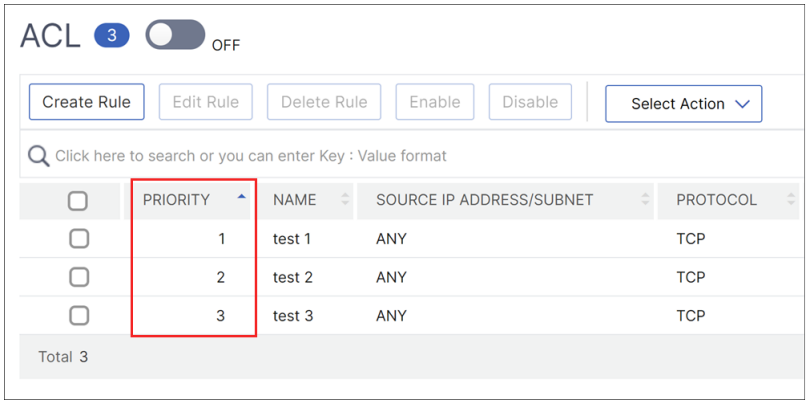
Renumber priorities of ACL rules

1. Hover the mouse over the rule that you want to renumber the priorities for and select the circle with three dots. Click **Renumber Priority** from the list.
2. Alternatively, select the radio button for that rule and from the **Select Action** list, select **Renumber Priority**.

NetScaler® automatically assigns new priority numbers, which are multiples of 10, to all the existing rules.

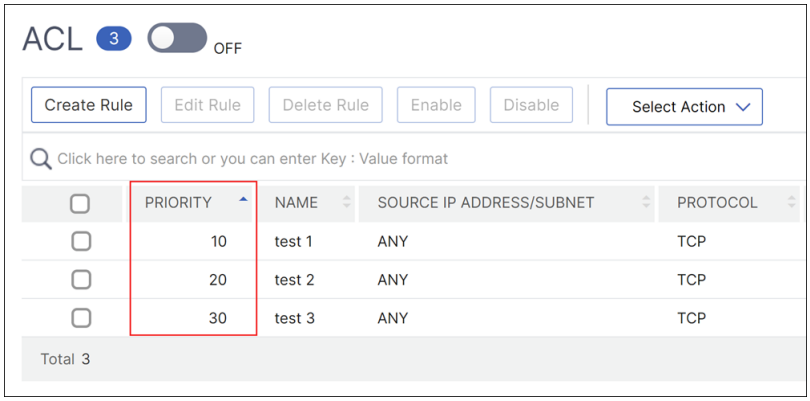
Edit the rules to assign priority numbers according to your requirement. See the "To edit an ACL rule" section for more information about how to edit a rule.

Example for existing priority numbers:



Example for the renumbered priority by NetScaler Console:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Troubleshooting

If ACL rules are improperly set up, all user accounts can be denied access. If you inadvertently lose all network access to NetScaler Console because of improper ACL setup, follow these steps to gain access:

1. Log on to NetScaler Console by using an SSH client.
2. Run the command `pfctl –d`.
3. Log on to NetScaler Console GUI and reconfigure the ACL accordingly.

Use NetScaler Console audit logs for managing and monitoring your infrastructure

September 27, 2025

You can use the NetScaler Console service to track all events on NetScaler Console and syslog events generated on NetScaler Console-managed 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- NetScaler Console related audit logs
- Application audit logs

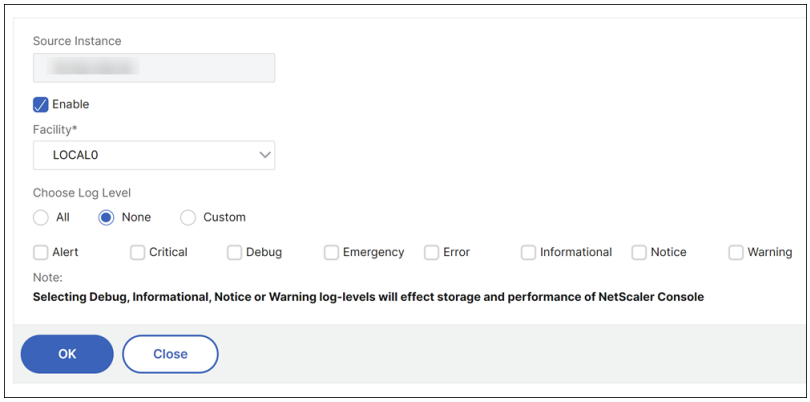
NetScaler instance related audit logs

Before you can view NetScaler instance-related syslog messages from NetScaler Console, configure the NetScaler Console service 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 the NetScaler Console service as a syslog server

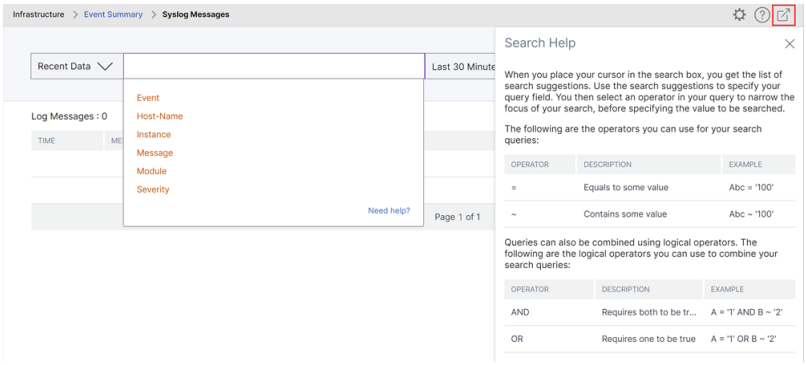
Follow these steps to configure NetScaler Console as the syslog server:

1. From the NetScaler Console GUI, navigate to **Infrastructure > Instances**.
2. Select the NetScaler instance from which you want the syslog messages to be collected and displayed in NetScaler Console.
3. In the **Select Action** list, select **Configure Syslog**.
4. Click **Enable**.
5. In the **Facility** drop-down list, select a local or user-level facility.
6. Select the required log level for the syslog messages.
7. Click **OK**.



These steps configure all the syslog commands in the NetScaler instance, and NetScaler Console starts receiving the syslog messages. You can view the messages by navigating to **Infrastructure > Events > Syslog Messages**. Click **Need Help?** to open the built-in search help. For more information, see View and export syslog messages.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



To export the log messages, click the arrow icon on the upper right corner.

Next, click **Export Now** or **Schedule Export**. For more information, see View and export syslog messages.

NetScaler Console related audit logs

Based on preconfigured rules, NetScaler Console generates audit log messages for the corresponding events, helping you monitor the health of your infrastructure.

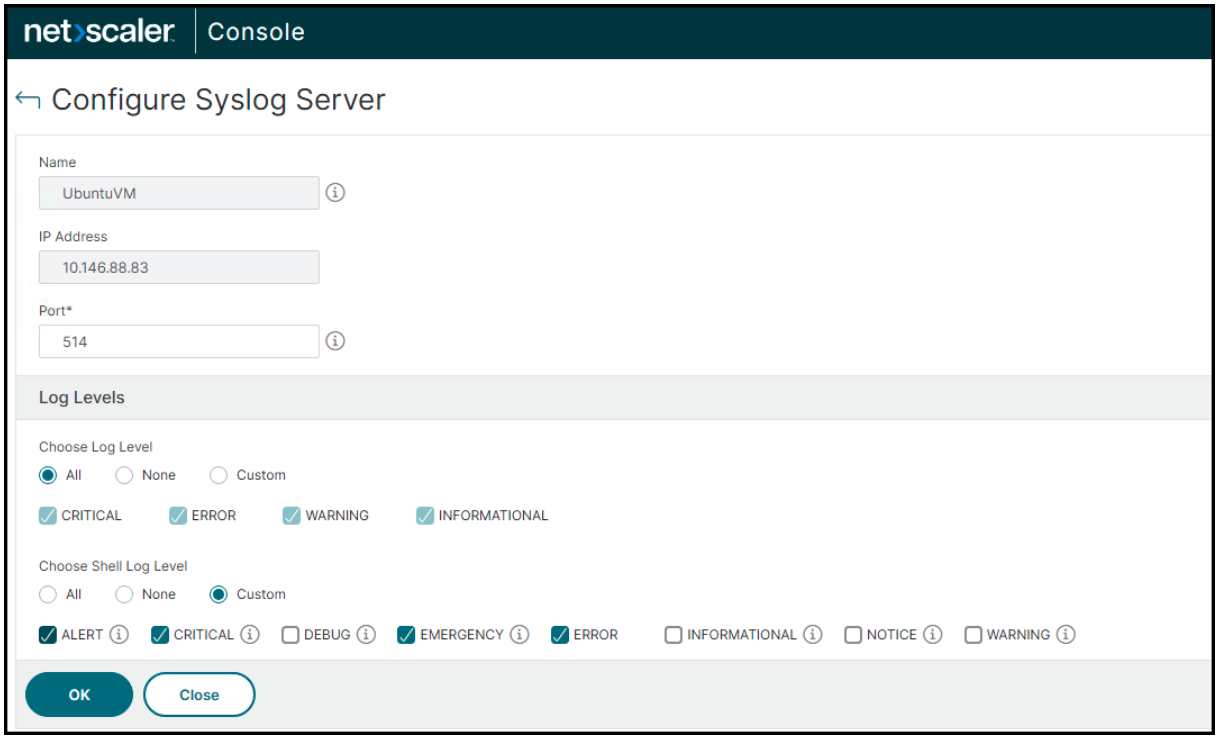
Configuring a syslog server to monitor audit and shell logs

You can configure an external syslog server to monitor audit and shell log events for your NetScaler Console deployments. For versions 14.1-34.x and later, you can configure a syslog server to also receive shell log events. This is an addition to the existing audit log configuration. Similar to audit logs, shell logs can be configured for different log levels.

Follow these steps to configure a syslog server on NetScaler Console:

1. Navigate to **UI Settings > Audit logs > Syslog servers**.
2. Choose the log levels for audit logs, shell logs, or for both.
    - **All**: Selects all listed log levels for audit or shell related events.
    - **None**: Clears all the selection and no logging level is selected.
    - **Custom**: Allows you to select specific log levels from the available list presented as check boxes.
3. Click **OK** to continue with the selected configuration. This enables NetScaler Console to send audit and/or shell related events to the configured syslog server.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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**, click a virtual server and select **Audit Log**.

License Activation Service

December 18, 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: 14.1-51.80, 13.1-60.29, 13.1-37.247 (FIPS)
- NetScaler SVM: 14.1-51.83, 13.1-60.30
- NetScaler Console Service: Supported from early September 2025.
- NetScaler Console on-prem: 14.1-51.83

  Note: LAS support for Console on-prem is from release 14.1-51.83 onwards. However, file-based licensing is deprecated from Console on-prem releases 14.1-51.83 onwards and 13.1-60.26 onwards, and goes EOL on April 15th, 2026. That is, even if you upgrade to Console on-prem release 14.1-51.83 or release 13.1-60.26 or later, you can continue using file-based licensing. However you must upgrade to Console on-prem release 14.1-51.83 or later, and switch to LAS before 15th April 2026 because file-based licensing reaches EOL.

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 new cloud-based licensing solution that provides an alternative to traditional file-based licensing. LAS introduces new modules for activating Citrix and NetScaler products, ensuring a seamless and modern approach to license management.

Notes:

- LAS is a licensing mechanism, not a license type.
- File-based licensing refers to the older method of licensing using manual entitlements. In

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 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 as proxy for licensing communication is optional.
- LAS eliminates the need for Z-Cap software license files on the NetScaler MPX™ and SDX instances.

NetScaler version compatibility for LAS

To use LAS, your NetScaler instances must be running one of the following minimum versions:

- NetScaler ADCs: 14.1 51.80, 13.1 60.29, 13.1 37.247 (FIPS)
- NetScaler SVM: 14.1 51.83, 13.1 60.30
- NetScaler Console Service: Supported from early September 2025.
- NetScaler Console on-prem: 14.1-51.83

> **Note:**
>
> - To use LAS, ensure that you have completed the following prerequisites:
>   - The NetScaler instance is running a LAS-compatible version.
>   - The NetScaler instance is added as a managed instance in NetScaler Console.
> - 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.

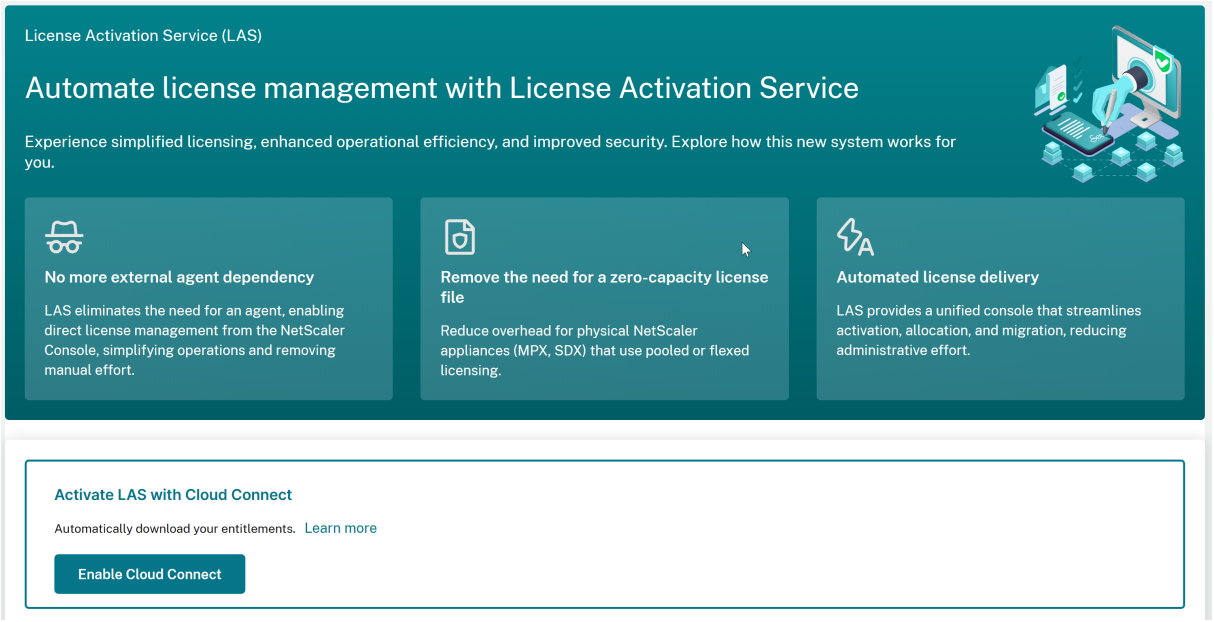
Transitioning to LAS

Activating LAS

Activating LAS involves obtaining a license entitlement file or blob on NetScaler Console on-prem. When you navigate to **NetScaler Licensing > License Management > LAS**, an introduction to the License Activation Service (LAS) is displayed.

The supported deployment option is **Activate LAS with Cloud Connect**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Activate LAS with Cloud Connect The Activate LAS with Cloud Connect option is for cloud-connected Console on-prem deployments. This deployment simplifies license management by automatically downloading entitlements and handling timely renewals directly from the Console service.

Using its cloud-connect feature, Console on-prem connects to the Console Service, which retrieves the license entitlement file or blob from LAS.

This entitlement file or blob is valid for 30 days. To ensure continuous licensing, the cloud-connected Console automatically refreshes this entitlement blob every day with LAS.

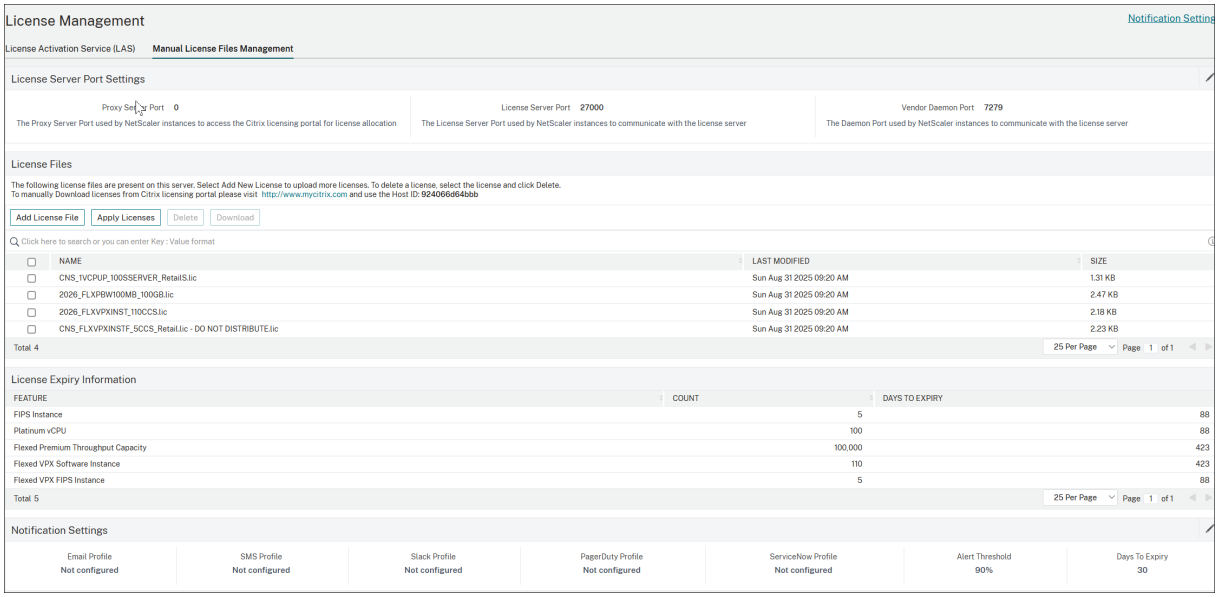
> **Notes:**
>
> - Ensure that the **Enable Cloud Connect** option is enabled to use **Activate LAS with the Cloud Connect** deployment method. To enable the option, see Enable Cloud Connect.
> - LAS is automatically enabled once Cloud Connect is enabled.

You can verify that Cloud Connect is enabled by checking the top-right corner of the Console GUI. Once you connect to the NetScaler Console Service, you are directed to the **LAS** tab under **License Management**. Here, you can view the last and next renewal dates, but no manual action is needed.

Once LAS is enabled on your Console on-prem, all your NetScaler Flexed and Pooled license entitlements appear in the **NetScaler Licenses > License management > License Activation Service (LAS)** section.

With file-based licensing, your applied entitlements and configurations are visible under **NetScaler Licenses > License management> Manual License File management** tab.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



License or Migrate NetScaler Instances to LAS

When you navigate to **NetScaler Licenses > License management > License Activation Service (LAS)**, the GUI dynamically updates based on the compatibility of your NetScaler instances.
If you do not have any NetScaler instances on a LAS-compatible version, a message is displayed in the screen directing you to upgrade or add a NetScaler.

> **Note:**
>
> If some of your NetScaler instances are upgraded to a compatible version, you can use LAS for those specific instances.

If one or more of your NetScaler instances are compatible with LAS, they are organized into two categories:

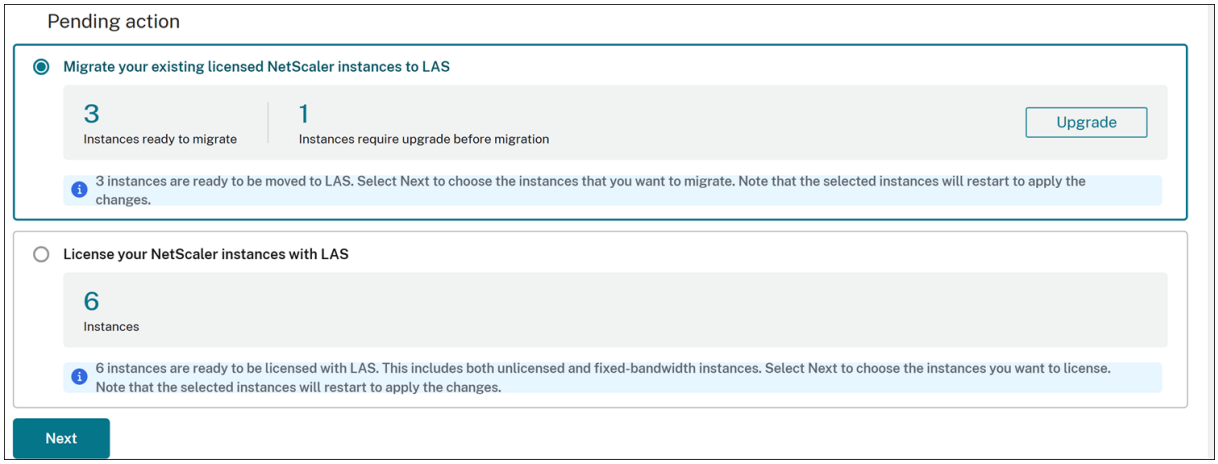
License NetScaler instances with LAS: These are instances that are not yet using LAS but are compatible.

Migrate the licensed NetScaler instances to LAS: These are instances that are already licensed through a different method and are eligible to be migrated to LAS.

The NetScaler GUI adjusts dynamically depending on whether you are a first-time LAS user (with zero instances on LAS) or an existing user (already have instances on LAS and are now adding more).

First Time User The following image is displayed for the first-time user:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Licensing 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 the instances with LAS perform the following steps :

1. Select **License with License Activation Service (LAS)**, click **Next**.
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.

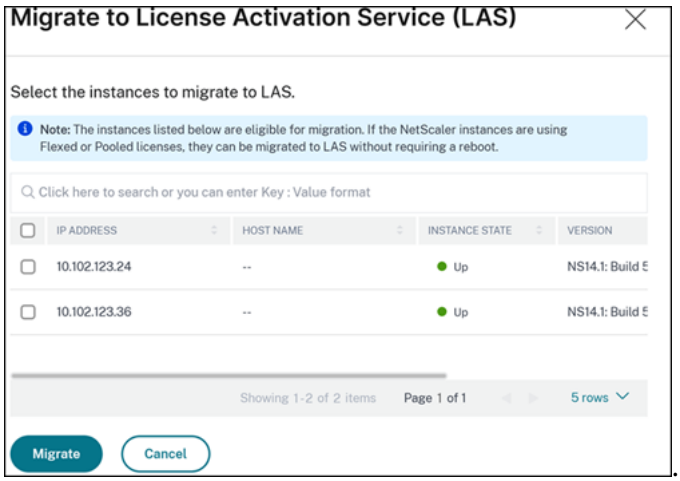
> **Note:**
>
> The selected instances restart for the license to take effect, except for SDX instances.

Migrating existing licensed NetScaler instances to LAS The **Migrate 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. In **Migrate to License Activation Service (LAS)**, select one or more NetScaler instances, and click **Migrate**.

> **Note:**
>
> Applying these changes restarts the selected instances, except for SDX instances.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



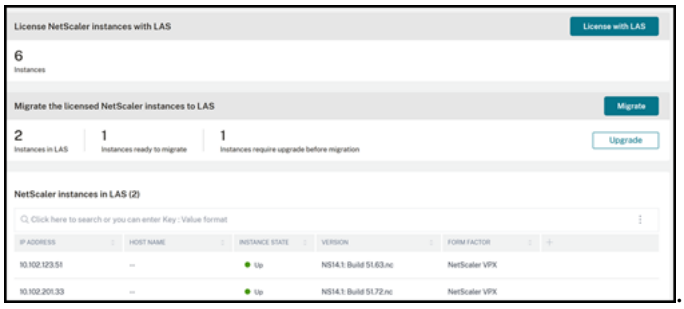
- **Instances require upgrade before migration:** List the instances that are to be upgraded to a compatible version or builds before migration. To upgrade, perform the following steps:

  Prerequisite:

  To use LAS-based licensing, the edition of your NetScaler instance must match the edition of your Pooled or Flexed 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 LAS user, you see the following GUI.



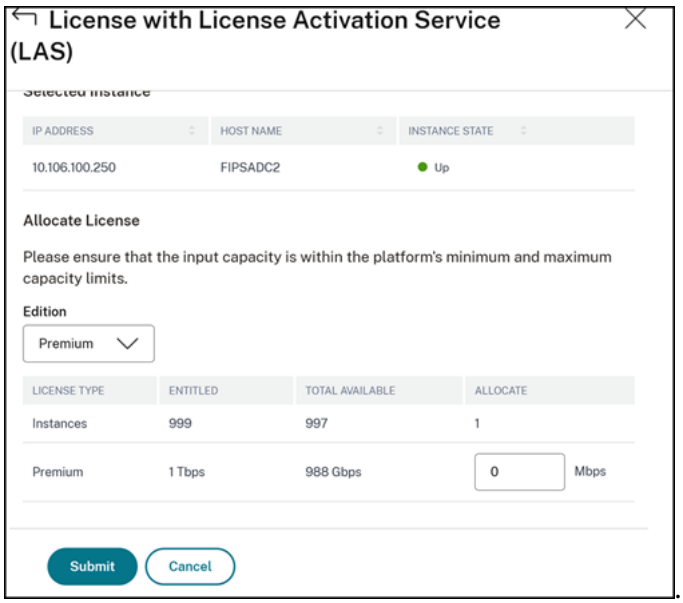
Note: To view the CPX instances licensed with LAS, see the Flexed Dashboard GUI. CPX instances are not listed here under NetScaler instance with LAS.

License NetScaler Instances with LAS The **License NetScaler instances with LAS** section lists NetScaler instances that are currently unlicensed or use any license other than a Flexed bandwidth or Pooled bandwidth file-based license.

To license the instances with LAS, perform the following steps:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

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 click **Migrate**.
     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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

1. Select **Instances require upgrade before migration**, click **Upgrade**.
2. Select one or more NetScaler instances, and click **Upgrade**.
3. Enter the details and click **Submit**.

License Activation Blob Behavior

The license activation blobs that NetScaler instances get from Console on-prem as part of **License with LAS or Migrate to LAS** are valid for 30 days. If a NetScaler loses and then regains connectivity with Console on-prem, the license activation blob is immediately restored.

When a NetScaler is unable to connect back to Console on-prem for up to 24 hours, it enters a grace period.
By default, license activation blobs refresh every 8 hours. If three consecutive 8-hour refresh attempts fail over 24 hours, the NetScaler enters a grace period.

License grace period alert

The following are the touch points for the license grace period alert:

- On the Flexed dashboard, a warning icon appears that the instance is in the grace period and the remaining days before the license activation blob expires.
- Every time an admin logs in to the NetScaler instance GUI, a pop-up message appears indicating that the instance is in the grace period and the remaining days before the license activation blob expires.
- Email notifications are sent to the email address configured. For more information, see Configure email settings.

  Note: Ensure to select **Licenses** for System Event Category to receive license-related email notifications.

Information sent to LAS during LAS licensing workflow

This section details all information sent as part of the request for an activation blob to LAS during every initial request and each LAS activation blob refresh request.
The following table summarizes the parameters sent to LAS during the licensing workflow:

Parameter	Description	Need for it in LAS workflow
lsguid	Unique ID of Console on-prem in UUID format	LAS binding parameter

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Parameter	Description	Need for it in LAS workflow
lsid	Unique ID of Console on-prem in SHA256	LAS binding parameter
pubkey	Public key of Console on-prem used for NetScaler token distribution	Ensures that LAS has authorized this Console
ccid	Citrix Cloud ID that is used to onboard the Console on-prem	LAS binding parameter
lsbuild	Build version of Console on-prem	LAS activation requirement
Console IP and hostname	Hostname of Console on-prem in the IP_hostname format	LAS activation requirement
activated_clients	List of NetScalers with LAS licenses, features, and request times. Note: NSIPs are not shared; only the LPEID (unique ID) is provided.	List of NetScalers with LAS activation blobs generated by this Console.
lastactivationid	Previous LAS activation ID, provided during renewal	For LAS side tracking

License management

October 3, 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: 14.1-51.80, 13.1-60.29, 13.1-37.247 (FIPS)

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> - NetScaler SVM: 14.1-51.83, 13.1-60.30
> - NetScaler Console Service: Supported from early September 2025.
> - NetScaler Console on-prem: 14.1-51.83
>
> **Note:** LAS support for Console on-prem is from release 14.1-51.83 onwards. However, file-based licensing is deprecated from Console on-prem releases 14.1-51.83 onwards and 13.1-60.26 onwards, and goes EOL on April 15th, 2026. That is, even if you upgrade to Console on-prem release 14.1-51.83 or release 13.1-60.26 or later, you can continue using file-based licensing. However you must upgrade to Console on-prem release 14.1-51.83 or later, and switch to LAS before 15th April 2026 because file-based licensing reaches EOL.
>
> All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
>
> LAS-based licenses may not be available to customers where prohibited by law or regulations.
>
> If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don't apply where prohibited by law or regulation.

Read the following note before proceeding further.

> **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.

Flexed licenses are supported in NetScaler Console on-prem 14.1 and 13.1 releases. For a better product experience showcasing Flexed GUI and offering bundled entitlement, we recommend upgrading your NetScaler Console on-prem to release 14.1–12.34 or later.

In NetScaler Console on-prem release 14.1–12.34 and later:

- You can manage Flexed licenses through the Flexed dashboard UI (NetScaler® **Licensing > Flexed Licensing)**.
- Bundled entitlement of unlimited NetScaler Console VIPs for analytics is available if you apply Flexed licenses.

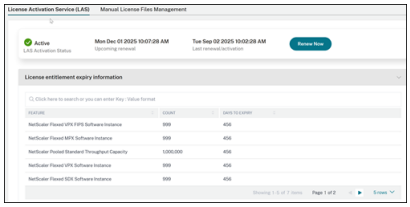
For NetScaler Console on-prem release 13.1 and 14.1 builds earlier than 14.1-12.34:

- When you apply Flexed licenses, NetScaler Console treats them the same as Pooled licenses and shows the details in the Pooled dashboard UI (**Infrastructure > Pooled Licensing**).
- When the Flexed license is applied, the bundled entitlement of unlimited NetScaler Console VIPs for analytics is not available in these releases.-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

LAS-based license

Your entitlements appear in the **Console UI > License Management > License Activation Service (LAS)** section after you enable LAS.



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).

Once you have enabled LAs and established a cloud connection, the initial entitlements for Pooled or Flexed licenses are fetched within one hour. Any subsequent new or renewed Pooled or Flexed licenses are fetched within 24 hours.

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 (License contract 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 the email notification is configured in **Notifications settings**. A notification email is sent in the frequency of 30, 20, and 10 days before the license end date.

Notifications 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.
4. Select a notification type and click **Add** to add details. You can also test each notification system before saving your settings.
5. Specify the Days to Expiry, which is the number of days before which you would like to be notified about the license expiry.
6. 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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.
- Click **Create**.

Create a Slack profile Perform the following steps to create a Slack profile:

1. In Slack, click **Add**.
2. In **Create Slack Profile**, specify the following details:

   - **Notifications** - When enabled, sends alerts and event notifications directly to a designated Slack channel.
   - **Notifications with attachments** - When enabled, detailed information about triggered alerts and events is sent as an email attachment or a JSON payload within a webhook.
   - **Profile Name** - Specify the profile name. This name appears in the Slack profile list.
   - **Channel Name** - Specify the Slack channel name to which the NetScaler Console sends the notification.
   - **Webhook URL** - Specify the Webhook URL of the channel. Incoming Webhooks are a simple way to post messages from external sources into Slack. The URL is internally linked to the channel name. All event notifications that are sent to this URL are posted on the designated Slack channel. An example of a webhook is as follows: https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK

Create a PagerDuty profile PagerDuty enables you to configure notifications through email, push notifications, and phone calls on a registered number. Before you add a PagerDuty profile in NetScaler Console, ensure that you have completed the required configurations in PagerDuty. To get started with PagerDuty, see the PagerDuty documentation.

Perform the following steps to create a PagerDuty profile:

1. In PagerDuty, click **Add**.
2. In **Create PagerDuty Profile**, specify the following details:

   - **Profile Name** - Specify a profile name. This name is used by different modules, such as event rules and SSL notifications to send PagerDuty alerts.
   - **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.
   - Click **Create**.

For more information, see Services and Integrations in the PagerDuty documentation.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

View the ServiceNow profile To enable ServiceNow notifications for the NetScaler events, you must integrate the 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).

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

File name contains	Description	Download information	Where to upload/apply the license
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
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

1. If you are a Pooled licensing customer transitioning to Flexed licensing and your MPX and SDX hardware already has Z-Cap Perpetual licenses, then you don't need to apply the Z-Cap licenses received with Flexed. However, if the current Z-Cap licenses that are applied on NetScaler MPX/NetScaler SDX are valid for a specific period, then you must apply the Z-Cap licenses received with the Flexed license. Flexed software license includes NetScaler Flexed MPX/SDX/VPX/VPX FIPS software instance and NetScaler Flexed Platinum bandwidth licenses.
2. 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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

License File	Apply on
NetScaler Flexed MPX SW Instance	NetScaler Console
NetScaler Flexed Platinum BW	NetScaler Console
ADC Zero Capacity MPX-Z Platform	NetScaler MPX

Apply the following licenses if you are using NetScaler VPX, NetScaler BLX, or NetScaler CPX form factor:

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

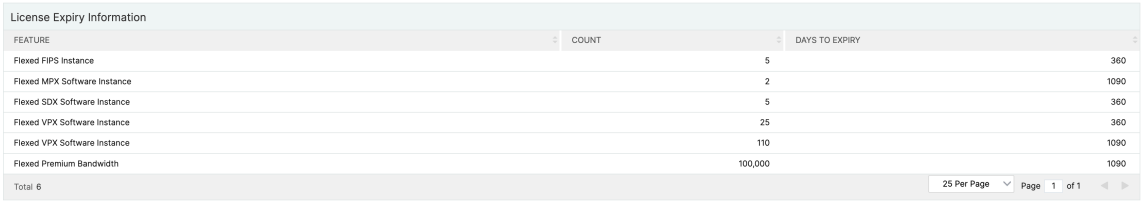
License File	Apply on
NetScaler Flexed VPX FIPS SW Instance	NetScaler Console
NetScaler Flexed Platinum BW	NetScaler Console

Apply a license file You can add, delete, and download licenses. You must apply licenses before they can be used.

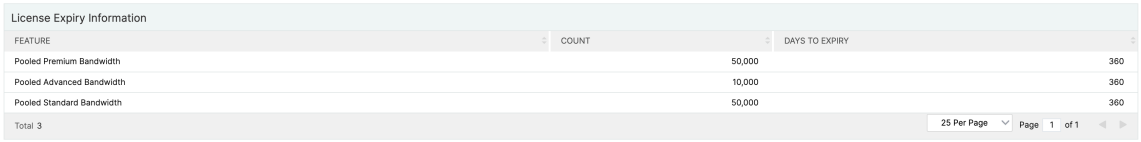
1. Navigate to **NetScaler Licensing > License Management**.
2. In the **License Files** section, click **Add License File** and select one of the following options:
   - **Upload license files from a local computer**: If a license file is already present on your local computer, you can upload it to 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

The following screenshot shows the number of Flexed NetScaler VPX, NetScaler MPX, NetScaler SDX, and NetScaler VPX FIPS software instance licenses, Flexed premium bandwidth capacity present and the days to expiry (contract end date).



The following screenshot shows the Pooled Standard, Advanced, and Premium bandwidth available and the days to expiry (contract end date).



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.
- **Proxy Server Port**: NetScaler Console can be used as a forward HTTP proxy for NetScaler instances to access the MyCitrix Portal for automated license retrieval. To enable this feature, specify a TCP port the proxy listens on.

License expiry information

You can now configure the license expiry threshold for Flexed or Pooled capacity licenses. When the threshold is set, NetScaler Console sends notifications using email or SMS when a license is due to

© 1997–2025 Citrix Systems, Inc. All rights reserved.

expire. An SNMP trap and a notification are also sent when the license has expired on NetScaler Console.

An event is generated when a license expiry notification is sent and this event can be viewed on NetScaler Console from **Infrastructure > Events**.

View license expiry

1. Navigate to **NetScaler Licensing > License Management**.
2. In the **License Settings** page, under the **License Expiry Information** section, you can find the details of the licenses that are going to expire:

    - **Feature**: Type of license that is going to expire.
    - **Count**: Number of virtual servers or instances that are affected.
    - **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 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 going to expire by selecting the appropriate checkbox. The notification types are as follows. Select a notification type and click **Add** to add details. You can also test that each notification is delivered before saving your settings.

    - **Email**: Email profile or distribution list for sending notifications. For more information, see Create an email distribution list.
    - **SMS**: SMS profile or distribution list for sending notifications.
    - **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 option available currently.
      For more information about creating these profiles, see Configure notifications

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 an 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 send 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 an SMS distribution list Perform the following steps to configure SMS notification settings:

1. In **SMS**, click **Add**.
2. In **Create SMS Distribution List**, specify the following details:

    - **Name** - Specify the distribution list name.
    - **SMS Server** - Select the SMS server that sends SMS notifications. To add an SMS server, click **Add**. Specify the server details and click **Create**.
    - **To** - Specify the phone number to which the NetScaler Console sends 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.

© 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, SMS, 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.
3. Click **Create**.

For more information, see Services and Integrations in the PagerDuty documentation.

View the ServiceNow profile To enable ServiceNow notifications for NetScaler events and the 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. 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 Flexed and Pooled licensing

October 3, 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: 14.1-51.80, 13.1-60.29, 13.1-37.247 (FIPS)
- NetScaler SVM: 14.1-51.83, 13.1-60.30
- NetScaler Console Service: Supported from early September 2025.
- NetScaler Console on-prem: 14.1-51.83

  Note: LAS support for Console on-prem is from release 14.1-51.83 onwards. However, file-based licensing is deprecated from Console on-prem releases 14.1-51.83 onwards and 13.1-60.26 onwards, and goes EOL on April 15th, 2026. That is, even if you upgrade to Console on-prem release 14.1-51.83 or release 13.1-60.26 or later, you can continue using file-based licensing. However you must upgrade to Console on-prem release 14.1-51.83 or later, and switch to LAS before 15th April 2026 because file-based licensing reaches EOL.

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 the 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- The maximum bandwidth and the number of instances that a NetScaler can check out.
- The minimum bandwidth unit for each bandwidth check out. The minimum bandwidth unit is the smallest unit of bandwidth that a NetScaler has to check out from a pool. Any check-out must be an integer multiple of the minimum bandwidth unit. For example, if the minimum bandwidth unit of a NetScaler is 1 Gbps, 1000 Mbps can be checked out, but not 200 Mbps or 150.5 Gbps. The minimum bandwidth unit is different from the minimum bandwidth requirement. A NetScaler instance can only operate after it is licensed with at least the minimum bandwidth. Once the minimum bandwidth is met, the instance can check out more bandwidth in multiples of the 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Product line	Minimum bandwidth (Gbps)	Maximum bandwidth (Gbps)	Minimum bandwidth unit
MPX 16000Z	30	250	1 Gbps
MPX 22000Z	40	120	1 Gbps
MPX 24000Z	100	150	1 Gbps
MPX 25000Z	100	160	1 Gbps
MPX 25000Z-40G	100	200	1 Gbps
MPX 26000Z	100	200	1 Gbps
MPX 26000Z-50S	100	200	1 Gbps
MPX 26000Z-100G	100	200	1 Gbps

Table 2A. Supported Flexed capacity for NetScaler SDX version earlier than build 13.0-47.x

Product line	Minimum bandwidth (Gbps)	Maximum bandwidth (Gbps)	Minimum instances	Maximum instances	Minimum bandwidth unit
SDX 8900Z	10	30	2	7	1 Gbps
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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Product line	Minimum bandwidth (Gbps)	Maximum bandwidth (Gbps)	Minimum instances	Maximum instances	Minimum bandwidth unit
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)

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Table 2C. Supported Flexed capacity for NetScaler SDX version 13.1 (build 51.x and later), and version 14.1 (build 12.x and later)

Product line	Minimum bandwidth (Gbps)	Maximum bandwidth (Gbps)	Minimum instances	Maximum instances	Minimum bandwidth unit
SDX 8900Z	5	30	1	7	1 Gbps
SDX 9100Z	10	95	1	7	1 Gbps
SDX 14000Z	10	100	1	25	1 Gbps
SDX 14000Z-40G	20	100	1	25	1 Gbps
SDX 15000Z	10	120	1	55	1 Gbps
SDX 15000Z-50G	10	120	1	55	1 Gbps
SDX 16000Z	15	250	1	55	1 Gbps
SDX 22000Z	20	120	1	80	1 Gbps
SDX 24000Z	50	150	1	80	1 Gbps
SDX 25000Z	50	200	1	115	1 Gbps
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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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
VPX	-
CPX	-
BLX	-

Flexed capacity license

October 3, 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: 14.1-51.80, 13.1-60.29, 13.1-37.247 (FIPS)
> - NetScaler SVM: 14.1-51.83, 13.1-60.30
> - NetScaler Console Service: Supported from early September 2025.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> - NetScaler Console on-prem: 14.1-51.83
>
> **Note:** LAS support for Console on-prem is from release 14.1-51.83 onwards. However, file-based licensing is deprecated from Console on-prem releases 14.1-51.83 onwards and 13.1-60.26 onwards, and goes EOL on April 15th, 2026. That is, even if you upgrade to Console on-prem release 14.1-51.83 or release 13.1-60.26 or later, you can continue using file-based licensing. However you must upgrade to Console on-prem release 14.1-51.83 or later, and switch to LAS before 15th April 2026 because file-based licensing reaches EOL.
>
> 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.

License Activation Service (LAS) - Activate LAS with Cloud Connect deployment to make your Flexed entitlements visible in NetScaler Console On-prem. Later, allocate them to any NetScaler form factor in the NetScaler Console On-prem.

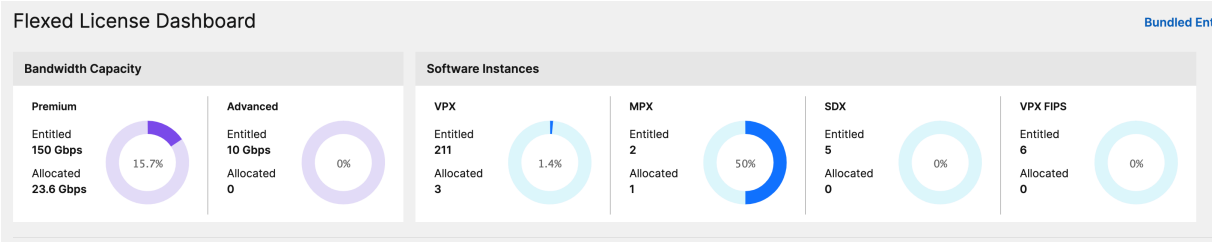
Manually managed entitlement (File-Based Licensing) - Apply the Flexed license directly on the NetScaler Console on-prem. Also, you must apply the MPX Z-Cap and SDX Z-Cap licenses to the respective NetScaler MPX and NetScaler SDX hardware. You can then allocate these entitlements to all NetScaler form factors, in both cloud and on-prem deployments.

A Flexed license also offers analytics for unlimited virtual servers.

If you have a Pooled license and have now 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



For more details, see Flexed license dashboard.

You can use Flexed licensing to maximize bandwidth utilization by ensuring the necessary bandwidth allocation to an instance and not more than its need. Increase or decrease the bandwidth allocated to an instance at run time without affecting the traffic.

Zero-capacity hardware

When managed through NetScaler® Flexed licensing, MPX and SDX instances are referred to as "zero-capacity hardware"because these instances cannot function until they check resources out of the bandwidth pool. Thus, these platforms are also referred to as MPX-Z, and SDX-Z appliances.

Zero-capacity hardware requires a Z-cap license to check out bandwidth from the common pool.

> **Note:**
>
> - The zero capacity license installation works the same way as other NetScaler local licenses. For more information about how to obtain and install a zero capacity license, see Licensing guide for NetScaler.

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.

> **Note:**
>
> When using LAS-based licensing, you do not need to apply Z-Cap licenses.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Standalone NetScaler VPX instances

NetScaler VPX instances running NetScaler software release 11.1 Build 54.14 and later on the following hypervisors support Flexed licensing:

- VMware ESX 6.0
- Citrix Hypervisor™
- Linux KVM

NetScaler VPX instances running NetScaler software release 12.0 Build 51.24 and later on the following hypervisors and cloud platforms support Flexed licensing:

- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

NetScaler VPX instances running NetScaler software release 13.0 and 13.1 (all versions) on the following hypervisors and cloud platforms support Flexed licensing:

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM
- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

> **Note:**
>
> To enable communication between NetScaler Console and Microsoft Azure or AWS, an IPSEC tunnel has to be configured. For more information, see Add NetScaler VPX Instances Deployed in Cloud to NetScaler Console. Unlike zero-capacity hardware, NetScaler VPX does not require a zero capacity license. To process traffic, it must check out bandwidth and an instance license from the pool.

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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:

- 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

November 27, 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: 14.1-51.80, 13.1-60.29, 13.1-37.247 (FIPS)
> - NetScaler SVM: 14.1-51.83, 13.1-60.30
> - NetScaler Console Service: Supported from early September 2025.
> - NetScaler Console on-prem: 14.1-51.83
>
> **Note:** LAS support for Console on-prem is from release 14.1-51.83 onwards. However, file-based licensing is deprecated from Console on-prem releases 14.1-51.83 onwards and 13.1-60.26 onwards, and goes EOL on April 15th, 2026. That is, even if you upgrade to Console on-prem release 14.1-51.83 or release 13.1-60.26 or later, you can continue using file-based licensing. However you must upgrade to Console on-prem release 14.1-51.83 or later, and switch to LAS before 15th April 2026 because file-based licensing reaches EOL.
>
> All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
>
> LAS-based licenses may not be available to customers where prohibited by law or regulations.
>
> If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don't apply where prohibited by law or regulation.

Read the following note before proceeding further.

> **Note:**
>
> If you have pooled licenses, and have now purchased and applied Flexed licenses, the combined entitlement appears in the Flexed license dashboard.

NetScaler Flexed licensing allows you to share bandwidth or instance licenses across different NetScaler form factors. Use this Flexed capacity for the instances that are in the data center or public

© 1997–2025 Citrix Systems, Inc. All rights reserved.

clouds. When an instance no longer requires the resources, it checks the allocated capacity back into the common pool. Reuse the released capacity on other NetScaler instances that need resources.

You can use Flexed 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.

You can perform the following tasks in NetScaler Console:

- **For LAS:**
  1. Activate the License Activation Service (LAS) using Cloud Connect.
  2. Once the license entitlements appear on the Console on-prem license server, check out licenses for NetScaler instances.
  3. Ensure that the licenses are based on the minimum and maximum capacity of each instance.
- **For file-based licensing:**
  1. Upload your Flexed licenses, which include bandwidth and software instance pools, to the NetScaler Console on-prem license server.
  2. Upload the SDX or MPX zero-capacity licenses directly to their respective hardware.
  3. Allocate licenses from the license pool to your NetScaler instances on demand. When checking out licenses, ensure that they are based on the minimum and maximum capacity of the instance.

  You can download all Flexed licenses, including bandwidth, instance, and zero-capacity (Z-cap) licenses, from the citrix.com website. For more information, see Licensing guide for NetScaler®.

LAS-based licensing

When using LAS, an external agent is optional. Ensure port 443 is available for instances to check out licenses from NetScaler Console. For more information, see System requirements.

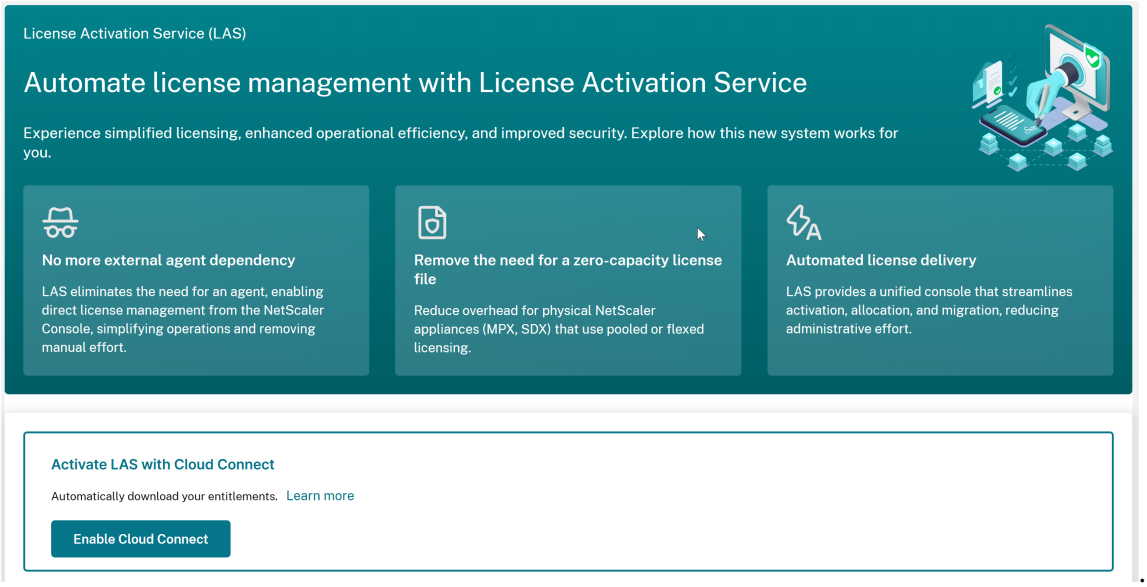
Step 1: Activate LAS and fetch entitlements

1. Activate LAS using **Cloud Connect**.

   For more information, see Activate License Activation Service.

   Once activated, your Flexed and Pooled license entitlements appear in the **License Management > LAS**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Step 2: Add NetScaler Instances to NetScaler Console On-prem

Ensure that you add your NetScaler instances to NetScaler Console On-prem so they can receive licenses. For more information about adding instances, see Add NetScaler instances to NetScaler Console On-prem.

Step 3: License or Migrate NetScaler Instances

1. Navigate to **Licensing management > LAS**.
2. Click **License with LAS or Migrate to LAS**.

   For more information, see License Activation Service.

Step 4: Edit Flexed Throughput Capacity

After licensing an instance, modify its allocated throughput capacity.

1. Navigate to **NetScaler Licensing > Flexed Licensing > Dashboard**.
2. Select the **LAS managed entitlements** tab.
3. In the **Licensed NetScalers** section, select an instance and click **Edit Throughput Capacity**.
4. Enter the new capacity in the **Allocate** column and click **Submit**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Special Licensing for Unlicensed MPX Appliances

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. Log in to the NetScaler GUI.
2. Navigate to **System > Licenses > ADC License > Manage Licenses > Add New License**.
3. In the **Licenses** page, select the **Use remote licensing** radio button, and choose **LAS** mode from **Remote Licensing Mode**.
4. In the **Server Name/IP address** field, enter the IP address of the NetScaler Console external agent.
5. Enter your credentials to register the instance with NetScaler Console, then click **Continue**.

   Note: Select the Validate Certificate checkbox if you have a digital certificate for validation.
6. 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 define a custom instance profile name.
7. Under **Allocate licenses**, 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.
8. Click **Get Licenses**.

> **Note:**
>
> Perform a warm restart of the instance after changing the license edition for the changes to take effect.

License Activation Blob Behavior

The license activation blobs that NetScaler instances get from Console on-prem as part of **License with LAS or Migrate to LAS** are valid for 30 days. If a NetScaler loses and then regains connectivity with Console on-prem, the license activation blob is immediately restored.

When a NetScaler is unable to connect back to Console on-prem for up to 24 hours, it enters a grace period.
By default, license activation blobs refresh every 8 hours. If three consecutive 8-hour refresh attempts fail over 24 hours, the NetScaler enters a grace period.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

License grace period alert

The following are the touch points for the license grace period alert:

- On the Flexed dashboard, a warning icon appears that the instance is in the grace period and the remaining days before the license activation blob expires.
- Every time an admin logs in to the NetScaler instance GUI, a pop-up message appears indicating that the instance is in the grace period and the remaining days before the license activation blob expires.
- Email notifications are sent to the email address configured. For more information, see Configure email settings.

Note: Ensure to select **Licenses** for System Event Category to receive license-related email notifications.

Manually managed entitlement (File-Based licensing)

Before you begin

Ensure that the following prerequisite is met before you configure Flexed licensing:

- The `27000` and `7279` ports are reachable from NetScaler to NetScaler Console, to check out licenses. 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

4. In **License Files**, select a license file that you want to apply and click **Apply licenses**.

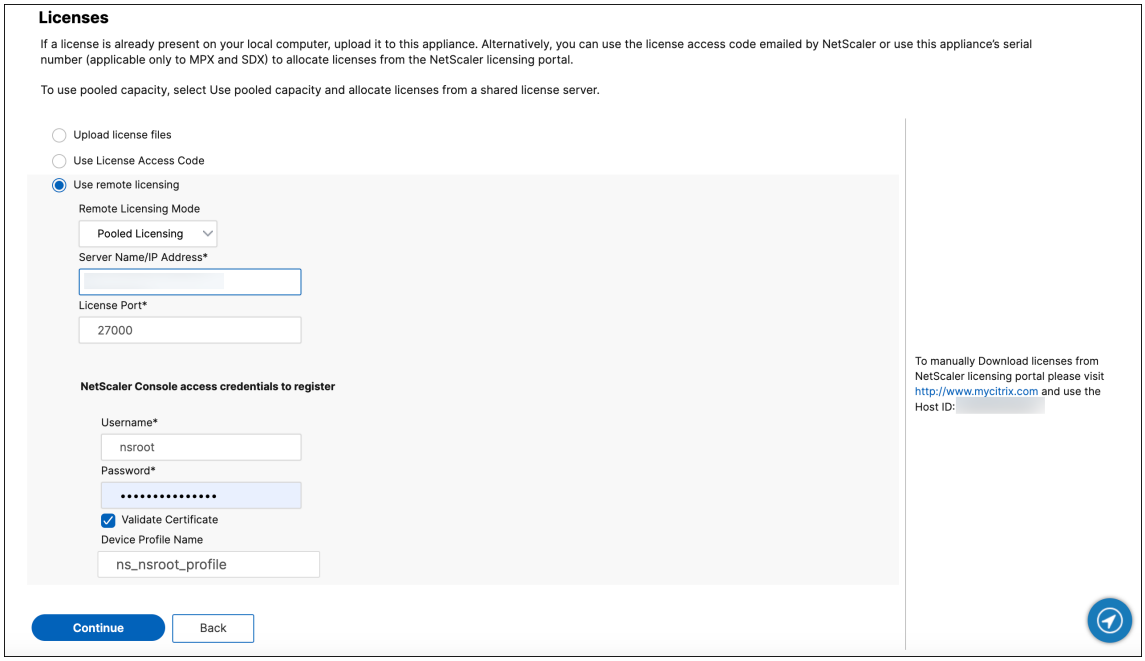
   This action enables NetScaler instances to use the selected license as a Flexed license.

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.

Register a NetScaler Console server using the GUI In the NetScaler Console GUI, register the NetScaler Console server associated with a 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 NetScaler Console server IP address.
6. The default license port is 27000.
7. Enter your NetScaler Console server credentials to register an instance with NetScaler Console and click **Continue**. In NetScaler Console, one of the servers is the license server.

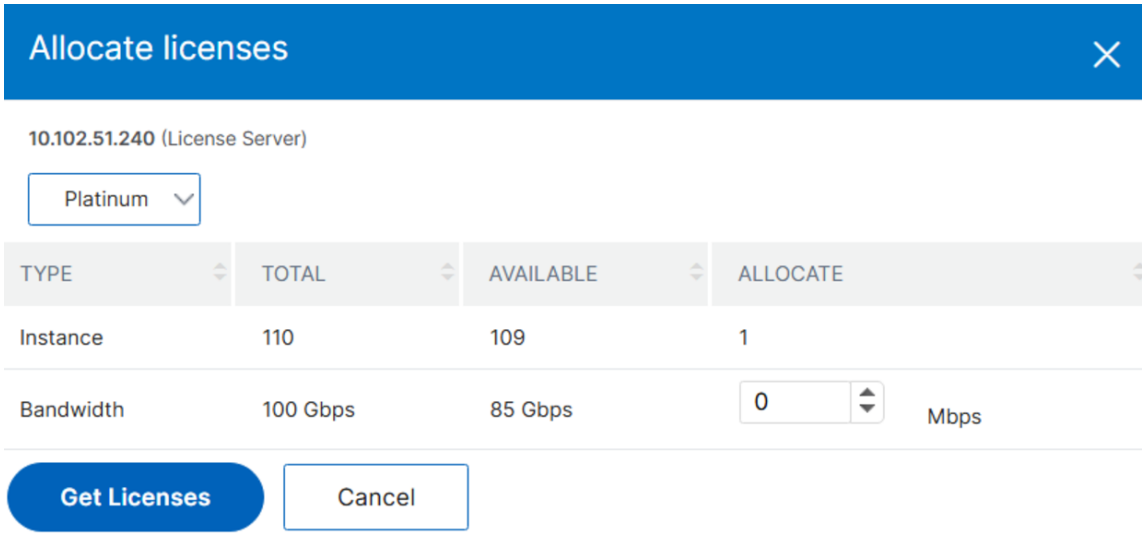


© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Select the **Validate Certificate** checkbox only if you have a digital Certificate Authority (CA) certificate for validation.

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.

   For the first time, allocate licenses in NetScaler. You can later change or release the license allocation from the NetScaler Console GUI.



   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 a NetScaler Console server using the CLI If a NetScaler instance has no GUI, use the following CLI commands to add a NetScaler Console server associated with an instance:

1. Log in to the NetScaler console.
2. Add the associated NetScaler Console server's IP address that is registered with NetScaler Console. The default license port is 27000.

```
> add ns licenseserver <adm-server-IP-address> -port <adm-server-license-port-number>
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

Step 3 - 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**.

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 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

NetScaler SDX-Z

SDX-Z is the Flexed-capacity enabled NetScaler SDX appliance. SDX-Z supports bandwidth and instance pool for the Premium edition licenses.

SDX-Z requires a license before it can connect to the License Server. You can install the SDX-Z license by using one of the following ways:

- Uploading the license file from a local computer.
- Using the instance's hardware serial number.
- The License Access Code from the **System** > **Licenses** section of the instance's GUI.

If you remove the SDX-Z license, SDX becomes unlicensed. The licenses are released to the license server.

You can dynamically modify the bandwidth of an SDX-Z instance without a restart.

> **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)

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 a 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 a NetScaler instance. The NetScaler instances configured with Flexed licensing display one of the following states:

- **Allocated**: Instance is running with proper license capacity.
- **Grace**: The instance is running in a grace period. The grace period is of 30 days, after which the instance becomes unlicensed.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Flexed license dashboard

October 3, 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: 14.1-51.80, 13.1-60.29, 13.1-37.247 (FIPS)
> - NetScaler SVM: 14.1-51.83, 13.1-60.30
> - NetScaler Console Service: Supported from early September 2025.
> - NetScaler Console on-prem: 14.1-51.83
>
> **Note:** LAS support for Console on-prem is from release 14.1-51.83 onwards. However, file-based licensing is deprecated from Console on-prem releases 14.1-51.83 onwards and 13.1-60.26 onwards, and goes EOL on April 15th, 2026. That is, even if you upgrade to Console on-prem release 14.1-51.83 or release 13.1-60.26 or later, you can continue using file-based licensing. However you must upgrade to Console on-prem release 14.1-51.83 or later, and switch to LAS before 15th April 2026 because file-based licensing reaches EOL.
>
> All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
>
> LAS-based licenses may not be available to customers where prohibited by law or regulations.
>
> If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don't apply where prohibited by law or regulation.

Read the following note before proceeding further.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Notes:

- If you had pooled licenses earlier, and now purchased and applied Flexed licenses, the combined entitlement now appears in the Flexed license dashboard.
- If you have only pooled licenses, check the Pooled license dashboard.
- If you have only Flexed licenses, or both Flexed and Pooled licenses, check the Flexed license dashboard.
- **Point to note based on licensing method:**
  - To view LAS-based licensing licenses, navigate to **NetScaler® licenses > Flexed Licensing > Dashboard > LAS managed entitlements** tab
  - To view manually managed entitlements (file-based licensing) licenses, navigate to **NetScaler® licenses > Flexed Licensing > Dashboard > Manually managed entitlements** tab
  - If you use both license mechanism refer to both tabs.
    The Flexed license dashboard gives you a comprehensive view of the throughput capacity and instances purchased by you.

Throughput capacity across editions and instance details for different form factors, such as MPX, VPX, and SDX are displayed on this page. NetScaler MPX and NetScaler MPX FIPS have the same license file. Similarly, NetScaler SDX and NetScaler SDX FIPS have the same license file. However, NetScaler VPX FIPS has a different file from NetScaler VPX and is displayed separately. Also, NetScaler VPX (including VPX on SDX), NetScaler BLX, and NetScaler CPX require NetScaler 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 throughput capacity
  - Premium
  - Advanced
  - Standard

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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.

Flexed license reporting

October 3, 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: 14.1-51.80, 13.1-60.29, 13.1-37.247 (FIPS)
> - NetScaler SVM: 14.1-51.83, 13.1-60.30
> - NetScaler Console Service: Supported from early September 2025.
> - NetScaler Console on-prem: 14.1-51.83
>
> **Note:** LAS support for Console on-prem is from release 14.1-51.83 onwards. However, file-based licensing is deprecated from Console on-prem releases 14.1-51.83 onwards and 13.1-60.26 onwards, and goes EOL on April 15th, 2026. That is, even if you upgrade to Console on-prem release 14.1-51.83 or release 13.1-60.26 or later, you can continue using file-based licensing. However you must upgrade to Console on-prem release 14.1-51.83 or later, and switch to LAS before 15th April 2026 because file-based licensing reaches EOL.
>
> 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:

- 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.

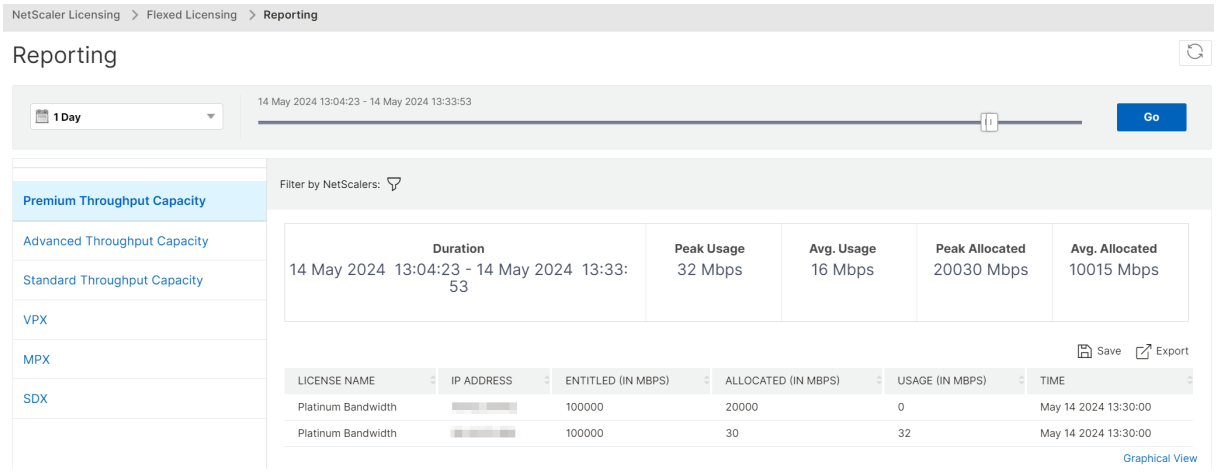
- **Peak usage** = The sum of the highest datapoint (Mbps) from the 24 hours of all NetScaler instances. For example, if the highest datapoint from the 24-hour duration for NetScaler A is 30 Mbps, NetScaler B is 45 Mbps, and NetScaler C is 120 Mbps, then the peak usage is displayed as 195 Mbps (30 + 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):

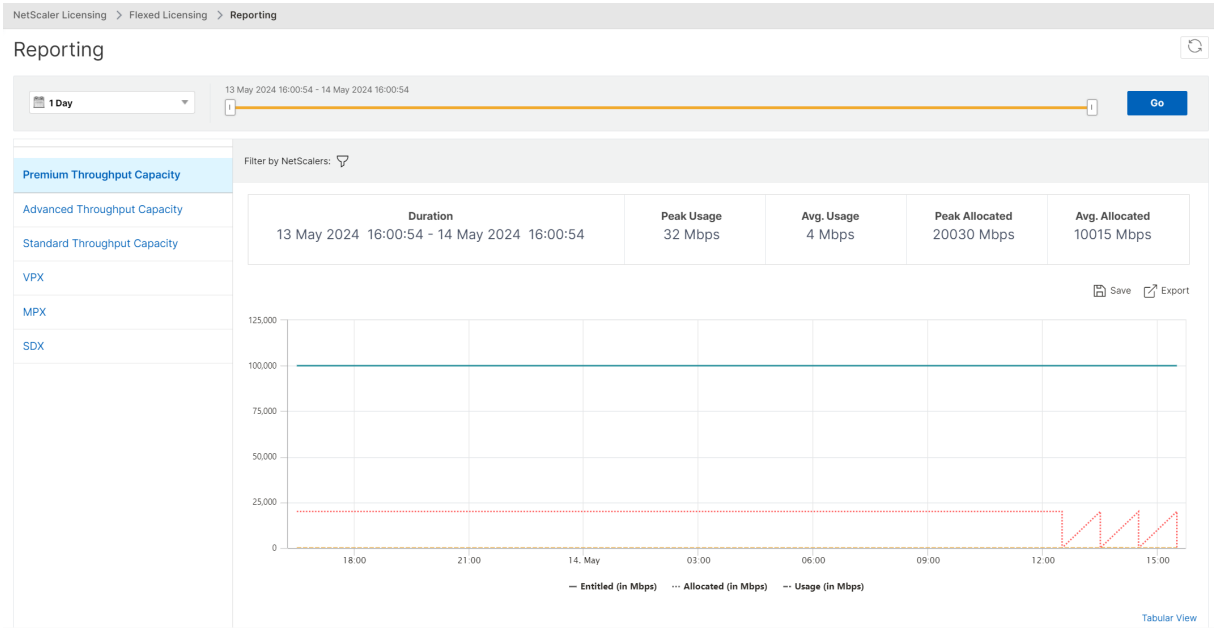


The following details appear on the dashboard:

- **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

October 3, 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: 14.1-51.80, 13.1-60.29, 13.1-37.247 (FIPS)
> - NetScaler SVM: 14.1-51.83, 13.1-60.30
> - NetScaler Console Service: Supported from early September 2025.
> - NetScaler Console on-prem: 14.1-51.83
>
> **Note:** LAS support for Console on-prem is from release 14.1-51.83 onwards. However, file-based licensing is deprecated from Console on-prem releases 14.1-51.83 onwards and 13.1-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 60.26 onwards, and goes EOL on April 15th, 2026. That is, even if you upgrade to Console on-prem release 14.1-51.83 or release 13.1-60.26 or later, you can continue using file-based licensing. However you must upgrade to Console on-prem release 14.1-51.83 or later, and switch to LAS before 15th April 2026 because file-based licensing reaches EOL.
>
> All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
>
> LAS-based licenses may not be available to customers where prohibited by law or regulations.
>
> If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don't apply where prohibited by law or regulation.

Read the following note before proceeding further.

LAS-based licenses

> **Note:**
>
> Ensure your NetScaler (ADC and SDX) instances are on LAS-compatible versions.

Information related to migration for the following license, refer to the **Migrate existing licensed instances** section at License Activation Service.

- 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, refer to the **Transition to LAS** section at 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)

Manually managed entitlements (file-based licenses)

> **Note:**
>
> You must switch to the Flexed licensing before the expiry of your current license. While planning

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> the transition keep the following steps in mind, and plan a maintenance window if the steps involve a license reconfiguration or NetScaler® reboot.

Pooled bandwidth license to Flexed license

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 software licenses on NetScaler Console. See License files.
2. If you have a Z-Cap software license 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 license before the expiry of your current license.

The following additional steps are needed:

1. Check out the required instance and bandwidth license from Flexed license 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 bandwidth capacity

For VPX

1. Upload and apply Flexed software Licenses on NetScaler Console. See License files.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

For CPX

1. Upload and apply flexed licenses on NetScaler Console. See License files.
2. Update the CPX YAML or HELM manifest file with bandwidth requirements. See CPX bandwidth-based licensing.
3. Deploy CPX instance using `kubectl apply -f cpx.yaml` command or using the HELM chart.

Fixed subscription or Perpetual license to Flexed license

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. Upload and apply Flexed software licenses on NetScaler Console. See License files.
3. 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 license 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

CICO to Flexed bandwidth capacity

For VPX

1. Upload and apply Flexed software 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

October 3, 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: 14.1-51.80, 13.1-60.29, 13.1-37.247 (FIPS)
> - NetScaler SVM: 14.1-51.83, 13.1-60.30
> - NetScaler Console Service: Supported from early September 2025.
> - NetScaler Console on-prem: 14.1-51.83
>
> **Note:** LAS support for Console on-prem is from release 14.1-51.83 onwards. However, file-based licensing is deprecated from Console on-prem releases 14.1-51.83 onwards and 13.1-60.26 onwards, and goes EOL on April 15th, 2026. That is, even if you upgrade to Console on-prem release 14.1-51.83 or release 13.1-60.26 or later, you can continue using file-based licensing. However you must upgrade to Console on-prem release 14.1-51.83 or later, and switch to LAS before 15th April 2026 because file-based licensing reaches EOL.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
>
> LAS-based licenses may not be available to customers where prohibited by law or regulations.
>
> If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don't apply where prohibited by law or regulation.

LAS-based licenses

Before the term expires

- The license must be renewed before its term expires.
- For NetScaler Console on-prem (cloud-connected), the license entitlement is renewed automatically if the license contract has been renewed within 24 hours.
- If the license is renewed before the term expires, the NetScaler will seamlessly switch to the new license after the old one expires, as long as the device is up and running.
- A restart is not required.
- NetScaler does not require 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

The license activation blobs that NetScaler instances receive from Console on-prem as part of the **License with LAS** or **Migrate to LAS** processes are valid for 30 days.

If the NetScaler loses connectivity with Console on-prem and then reconnects, it immediately receives the license activation blob without any delay.

If a NetScaler cannot reconnect to Console on-prem for up to 24 hours, it enters a grace period.

By default, license activation blobs are refreshed every 8 hours. If a refresh attempt fails three consecutive times within 24 hours, the NetScaler enters a grace period.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Grace period:

- NetScaler enters a 30-day grace period.
- All licensing functionality continues to work. However, on the thirty-first day:
    - NetScaler VPX, NetScaler CPX, NetScaler BLX, and NetScaler MPX instances undergoes a forced reboot and become unlicensed.
    - The throughput on all VPX instances on a NetScaler SDX is reduced to 1 Mbps.

License grace period alert On the Flexed dashboard, a warning icon appears that the instance is in the grace period and the remaining days before the license activation blob expires. Everytime an admin logs in to the NetScaler instance GUI, a pop-up message appears indicating that the instance is in the grace period and the remaining days before the license activation blob expires.

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.

Types of Flexed licenses

- Software instance (VPX/BLX/CPX, SDX, MPX, VPX FIPS)
- Bandwidth capacity

Scenario: MPX form factor

You are using Flexed/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/Pooled license seamlessly after the old license expires.
- Restart is not required.
- NetScaler does not require a manual capacity reconfiguration.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

After the term expires NetScaler instance stops its normal operations after the license expiry, including configuration loss and complete shutdown of traffic processing.

Scenario: SDX form factor

You are using Flexed/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/Pooled license seamlessly after the old license expires.
- 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.

Scenario: VPX/BLX/CPX form factor

You are using Flexed/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/Pooled license seamlessly after the old license expires.
- 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Scenarios for connectivity issues behavior

If connectivity breaks between NetScaler and NetScaler Console on-prem server, the behavior is as follows:

- NetScaler goes into grace for 30 days.
- During this grace period, licensing functionality continues to work until the thirtieth day.
- On the thirty-first day,
  - NetScaler VPX/NetScaler CPX/NetScaler BLX and NetScaler MPX undergo a forced reboot and become unlicensed.
  - The throughput on all the VPX on NetScaler SDX is decreased to 1 Mbps.

Configure NetScaler Console server as the Flexed or Pooled license server

October 3, 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: 14.1-51.80, 13.1-60.29, 13.1-37.247 (FIPS)
> - NetScaler SVM: 14.1-51.83, 13.1-60.30
> - NetScaler Console Service: Supported from early September 2025.
> - NetScaler Console on-prem: 14.1-51.83
>
>   **Note:** LAS support for Console on-prem is from release 14.1-51.83 onwards. However, file-based licensing is deprecated from Console on-prem releases 14.1-51.83 onwards and 13.1-60.26 onwards, and goes EOL on April 15th, 2026. That is, even if you upgrade to Console on-prem release 14.1-51.83 or release 13.1-60.26 or later, you can continue using file-based

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> licensing. However you must upgrade to Console on-prem release 14.1-51.83 or later, and switch to LAS before 15th April 2026 because file-based licensing reaches EOL.
>
> 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 NetScaler Console server only as the Flexed or Pooled license server. With this configuration, NetScaler Console server 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 the NetScaler Console on-prem server in your regulatory zone to use management, monitoring, and analytics capabilities. When you follow the same approach to use the Flexed or Pooled licenses feature, you have to split Flexed or Pooled licenses across various NetScaler Console license servers. This approach does not provide you the flexibility to allocate Flexed or Pooled licenses across your globally deployed NetScaler instances.

Therefore, configure NetScaler Console server only as the Flexed or Pooled license server. NetScaler Console server receives only licensing data from all NetScaler instances. So, you can adhere to the regulatory mandate and dynamically allocate Flexed or Pooled capacity licenses across globally deployed NetScaler instances.

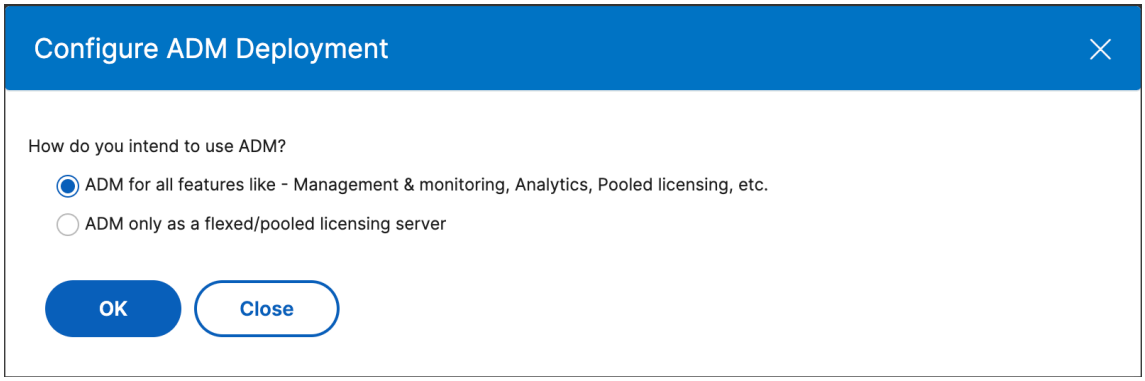
How to configure NetScaler Console server only as the Flexed or Pooled license server

Before you begin, ensure that no NetScaler instances are added to NetScaler Console server. Add NetScaler instances only after you complete step 4.

Do the following to configure NetScaler Console server only for the Flexed or Pooled license server:

1. Navigate to **Settings > Administration**.
2. In the **System Configurations** section, select **System Deployment**.
3. In **ADM Deployment**, select **NetScaler Console only as a flexed/pooled licensing server**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



4. Click **OK**.

   This action keeps only the Flexed or 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 Flexed or Pooled licensing feature. And, the remaining features do not appear.

5. 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 one or more NetScaler Console servers. When you change the password of such NetScaler instances, ensure to update the password on all NetScaler Console servers where the instance is discovered.
> - A user can still do some operations of the disabled features in the NetScaler Console GUI. For example, event polling and NetScaler backup. As a super administrator, If you want to restrict such operations, disable user access for other administrators using an appropriate access policy. For more information, see Configure Access Policies on NetScaler Console.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

You can also deploy NetScaler Console server only for Flexed or Pooled license server with the following lower specifications:

Component	Requirement
RAM	8 GB
Virtual CPU	4
Storage	120 GB

NetScaler Pooled capacity

October 3, 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: 14.1-51.80, 13.1-60.29, 13.1-37.247 (FIPS)
> - NetScaler SVM: 14.1-51.83, 13.1-60.30
> - NetScaler Console Service: Supported from early September 2025.
> - NetScaler Console on-prem: 14.1-51.83
>
> **Note:** LAS support for Console on-prem is from release 14.1-51.83 onwards. However, file-based licensing is deprecated from Console on-prem releases 14.1-51.83 onwards and 13.1-60.26 onwards, and goes EOL on April 15th, 2026. That is, even if you upgrade to Console on-prem release 14.1-51.83 or release 13.1-60.26 or later, you can continue using file-based licensing. However you must upgrade to Console on-prem release 14.1-51.83 or later, and switch to LAS before 15th April 2026 because file-based licensing reaches EOL.
>
> All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 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 Pooled capacity allows you to share bandwidth or instance licenses across different NetScaler form factors. For virtual CPU subscription-based instances, you can share virtual CPU license across instances. Use this Pooled capacity for the instances that are in the data center or public clouds. When an instance no longer requires the resources, it checks the allocated capacity back into the common pool. Reuse the released capacity to other NetScaler instances that need resources.

You can use 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.

How NetScaler Pooled capacity licensing works

NetScaler Pooled capacity has the following components:

- NetScaler instances, which can be categorized into:
  - Zero-capacity hardware
  - Standalone NetScaler VPX instances or NetScaler CPX instances or NetScaler BLX instances
- Bandwidth pool
- Instance pool
- NetScaler Console configured as a license server

Zero-capacity hardware

When managed through NetScaler Pooled capacity, MPX and SDX instances are referred to as "zero-capacity hardware"because these instances cannot function until they check resources out of the bandwidth and instance pools. Thus, these platforms are also referred to as MPX-Z, and SDX-Z appliances.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Zero-capacity hardware requires a platform license to be able to check out bandwidth and an instance license from the common pool.

> **Note**
>
> - Instance license subscription is not required for MPX instances. See table 1 in this page for supported Pooled capacity for MPX and SDX instances. See table 5 for license requirements for different MPX and SDX form factors.
> - 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.

Manage and install platform licenses

You must install a platform license manually, by using the hardware serial number or the license access code. After a platform 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 platform 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 Pooled capacity. For more information, see **Table 1. Supported Pooled capacity for MPX and SDX instances**.

Standalone NetScaler VPX instances

NetScaler VPX instances running NetScaler software release 11.1 Build 54.14 and later on the following hypervisors supports Pooled capacity:

- 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 supports Pooled capacity:

- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

© 1997–2025 Citrix Systems, Inc. All rights reserved.

NetScaler VPX instances running NetScaler software release 13.0 and 13.1 (all versions) on the following hypervisors and cloud platforms support Pooled capacity:

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM
- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

> **Note**
>
> To enable communication between NetScaler Console and Microsoft Azure or AWS, an IPSEC tunnel has to be configured. For more information, see Add NetScaler VPX Instances Deployed in Cloud to NetScaler Console.
> Unlike zero-capacity hardware, NetScaler VPX does not require a platform license. To process traffic, it must check out bandwidth and an instance license from the pool.

Standalone NetScaler CPX instances

NetScaler CPX instances deployed on a Docker host support Pooled capacity. Unlike zero-capacity hardware, NetScaler CPX does not require a platform 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 pool licensing, you can add more bandwidth only in multiples of 10 Mbps.

Standalone NetScaler BLX instances

NetScaler BLX instances support Pooled capacity licenses. A NetScaler BLX instance does not require a platform license. To process traffic, a NetScaler BLX instance must check out bandwidth and an instance license from the pool.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Bandwidth Pool

The bandwidth pool is the total bandwidth that can be shared by NetScaler instances, both physical and virtual. The bandwidth pool comprises separate pools for each software edition (Standard, Advanced, and Premium). A given NetScaler 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

The instance pool defines the number of NetScaler VPX instances or NetScaler CPX instances or NetScaler BLX instances that can be managed through NetScaler Pooled capacity or the number of NetScaler VPX instances in an SDX-Z instance.

When checked out from the pool, a license unlocks the MPX-Z, SDX-Z, VPX, NetScaler CPX, and NetScaler BLX instance's resources, including CPUs/PEs, SSL cores, packets per second, and bandwidth.

> **Note**
>
> The Management Service of an SDX-Z does not consume an instance.

NetScaler Console license server

NetScaler Pooled capacity uses NetScaler Console configured as a license server to manage Pooled capacity licenses: bandwidth pool licenses and instance pool licenses. You can use the NetScaler Console software to manage Pooled capacity licenses without an NetScaler Console license.

When checking out licenses from bandwidth and instance pool, NetScaler form factor and hardware model number on a zero-capacity hardware determines

- The minimum bandwidth and the number of instances that a NetScaler instance must check out before being functional.
- The maximum bandwidth and the number of instances that a NetScaler can check out.
- The minimum bandwidth unit for each bandwidth check-out. The minimum bandwidth unit is the smallest unit of bandwidth that a NetScaler has to check out from a pool. Any check-out must be an integer multiple of the minimum bandwidth unit. For example, if the minimum bandwidth unit of a NetScaler is 1 Gbps, 1000 Mbps can be checked out, but not 200 Mbps or 150.5 Gbps. The minimum bandwidth unit is different from the minimum bandwidth requirement. A NetScaler instance can only operate after it is licensed with at least the minimum bandwidth. Once the minimum bandwidth is met, the instance can check out more bandwidth with the minimum bandwidth unit.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Tables 1, 2, 3, and 4 summarize the maximum bandwidth/instances, minimum bandwidth/instances, and minimum bandwidth unit for all supported NetScaler instances. Table 5 summarizes the license requirement for different form factors for all supported NetScaler instances:

Table 1. Supported Pooled capacity for MPX and SDX instances

Product line	Maximum bandwidth (Gbps)	Minimum bandwidth (Gbps)	Minimum instances	Maximum instances	Minimum bandwidth unit
MPX 5900Z	10	1	N/A	N/A	1 Gbps
MPX 8900Z	30	5	NA	NA	1 Gbps
MPX 9100Z	30	10	NA	NA	1 Gbps
MPX 8900Z FIPS	33	5	NA	NA	1 Gbps
MPX 14000Z series	100	20	NA	NA	1 Gbps
MPX 14000Z 40G series	100	20	N/A	N/A	1 Gbps
MPX 14000Z FIPS series	100	20	N/A	N/A	1 Gbps
MPX 14000Z 40S series	100	20	N/A	N/A	1 Gbps
MPX 15000Z series	120	20	N/A	N/A	1 Gbps
MPX 15000Z FIPS series	120	20	N/A	N/A	1 Gbps
MPX 15000Z 50G series	120	20	N/A	N/A	1 Gbps
MPX 16000Z series	200	30	N/A	N/A	1 Gbps
MPX 22000Z series	120	40	N/A	N/A	1 Gbps
MPX 24000Z series	150	100	N/A	N/A	1 Gbps

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Product line	Maximum bandwidth (Gbps)	Minimum bandwidth (Gbps)	Minimum instances	Maximum instances	Minimum bandwidth unit
MPX 25000Z 40G	200	100	N/A	N/A	1 Gbps
MPX 25000ZA	200	100	N/A	N/A	1 Gbps
MPX 26000Z series	200	100	N/A	N/A	1 Gbps
MPX 26000Z 100G series	200	100	N/A	N/A	1 Gbps
MPX 26000Z 50S series	200	100	N/A	N/A	1 Gbps
SDX 8900Z	30	10	1	7	1 Gbps
SDX 9100Z	95	20	1	7	1 Gbps
SDX 14000Z series	100	10	1	25	1 Gbps
SDX 14000Z 40G series	100	1	2	25	1 Gbps
SDX 14000Z 40S series	100	20	1	25	1 Gbps
SDX 14000Z FIPS series	100	10	1	25	1 Gbps
SDX 15000Z 50G	120	10	1	55	1 Gbps
SDX 15000Z	120	10	1	55	1 Gbps
SDX 16000Z series	200	15	1	55	1 Gbps
SDX 22000Z series	120	20	1	80	1 Gbps
SDX 25000Z 40G	200	50	1	115	1 Gbps
SDX 25000ZA	200	50	1	115	1 Gbps
SDX 26000Z 100G	200	50	1	115	1 Gbps

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Product line	Maximum bandwidth (Gbps)	Minimum bandwidth (Gbps)	Minimum instances	Maximum instances	Minimum bandwidth unit
SDX 26000Z	200	50	1	115	1 Gbps
SDX 26000Z 50S	200	50	1	115	1 Gbps
SDX 24000Z series	150	50	1	80	1 Gbps

> Note
>
> The minimum bandwidth and instances are applicable to SDX instances running the following releases and higher: 11.1 64.x, 12.0 63.x, 12.1 54.x, and 13.0 41.x.
>
> The minimum purchase quantity is different from the minimum system requirement.

Table 2. Supported Pooled capacity 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

Table 3. Supported Pooled capacity 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Hypervisor/Cloud Service	Maximum bandwidth (Gbps)	Minimum bandwidth (Mbps)	Minimum instances	Maximum instances	Minimum bandwidth unit
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 4. Supported Pooled capacity 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 5. License requirement for different form factors

Product line	Zero Capacity Hardware Purchase	Bandwidth and Edition Subscription	Instance Subscription
MPX	License required	License required	-
SDX	License required	License required	License required
VPX	-	License required	License required
CPX	-	-	License required
BLX	-	License required	License required

Configure NetScaler Pooled capacity

November 28, 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: 14.1-51.80, 13.1-60.29, 13.1-37.247 (FIPS)
- NetScaler SVM: 14.1-51.83, 13.1-60.30
- NetScaler Console Service: Supported from early September 2025.
- NetScaler Console on-prem: 14.1-51.83

  Note: LAS support for Console on-prem is from release 14.1-51.83 onwards. However, file-based licensing is deprecated from Console on-prem releases 14.1-51.83 onwards and 13.1-60.26 onwards, and goes EOL on April 15th, 2026. That is, even if you upgrade to Console on-prem release 14.1-51.83 or release 13.1-60.26 or later, you can continue using file-based licensing. However you must upgrade to Console on-prem release 14.1-51.83 or later, and switch to LAS before 15th April 2026 because file-based licensing reaches EOL.

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.

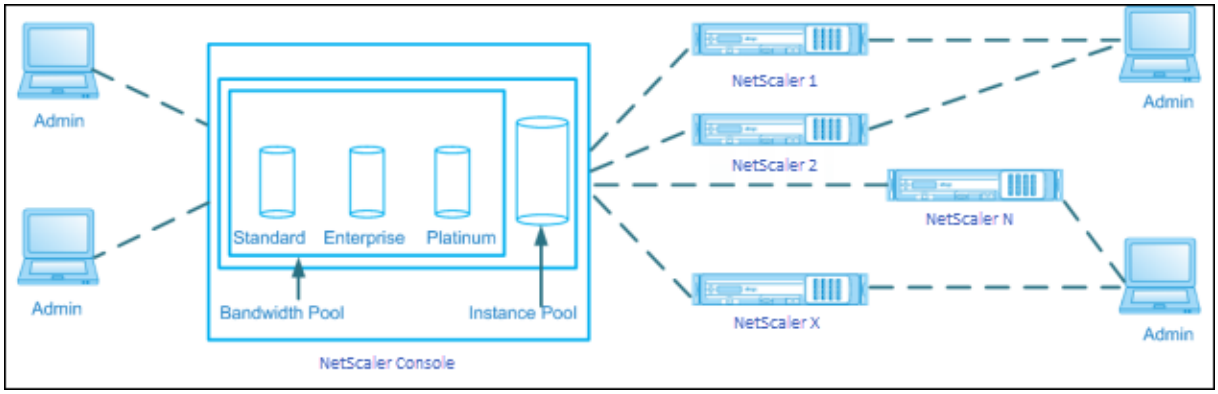
To use NetScaler Pooled capacity, configure NetScaler Console as a license server to the required NetScaler instances. NetScaler instances check in and check out licenses from the NetScaler Console. You can perform the following tasks in the NetScaler Console GUI:

- Upload the Pooled capacity license files (bandwidth and instance pool) to the license server.
- 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 min-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

imum and maximum capacity of the instance.

- Configure Pooled capacity for NetScaler FIPS instances to check in or check out licenses.



Supported hardware and software versions

For supported hardware and software versions for Pooled capacity, see NetScaler Pooled capacity.

NetScaler Pooled capacity states

The Pooled capacity states indicate the license requirement on an NetScaler instance. The NetScaler instances configured with Pooled capacity display one of the following states:

- **Optimum**: Instance is running with proper license capacity.
- **Capacity mismatch**: Instance is running with a capacity less than the user configured.
- **Grace**: Instance is running on a grace license.
- **Grace & Mismatch**: Instance is running on grace but with a capacity less than the user configured.
- **Not available**: Instance is not registered with NetScaler Console for management, or NITRO communication from NetScaler Console to the instances is not working.
- **Not allocated**: License is not allocated in the instance.

Step 1 - Apply licenses in NetScaler Console

1. In NetScaler Console, navigate to **NetScaler Licensing > Pooled Licensing**.
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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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** tab lists the licenses present in 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 Pooled capacity.

Step 2 - Register NetScaler Console as a license server

To register NetScaler Console as a license server to a NetScaler instance, follow one of the procedures:

- Use GUI
- Use CLI

Use the GUI to register NetScaler Console as a license server

In the NetScaler GUI, register the NetScaler Console server as a license server.

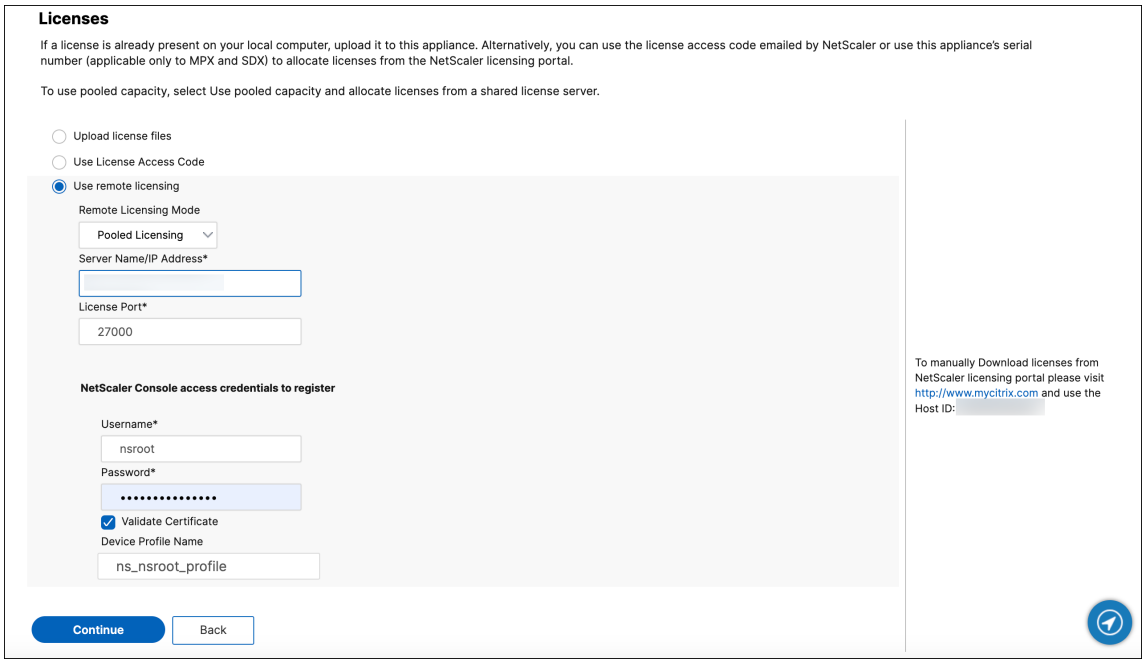
1. Log in to NetScaler GUI.
2. Navigate to **System** > **Licenses** > **Manage Licenses**.
3. Click **Add New License**.
4. Select **Use remote licensing** and under **Remote Licensing Mode**, select **Pooled Licensing** from the list.
5. In the **Server Name/IP address** field, specify the NetScaler Console server IP address.

> For a HA deployment, use a floating IP. For more information on configuration, see Configure High Availability Deployment.
>
> For a deployment which uses a standalone NetScaler Console or an agent, see Licensing overview

6. The default license port is 27000.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

7. Enter your NetScaler Console server credentials to register an instance with NetScaler Console and click **Continue**. In NetScaler Console, one of the servers is the license server.



> **Notes:**
>
> - Select the **Validate Certificate** checkbox only if NetScaler Console has a valid digital Certificate issued by a Certificate Authority (CA) (under **Settings > Administration > SSL Settings**).
> - 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.

   For the first time, allocate licenses in NetScaler. You can later change or release the license allocation from the NetScaler Console GUI.

   a) Click **Get Licenses**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Important:**
>
> Warm restart the instance if you change the license edition. The configuration changes do not take effect until you restart the instance.

Use CLI to add NetScaler Console as a license server

If an NetScaler instance has no GUI, use the following CLI commands to add the NetScaler Console server as a license server:

1. Log in to the NetScaler console.
2. Add the NetScaler Console server IP address:

   ```
   > add ns licenseserver <adm-server-IP-address> -port <adm-server-port-number> -licensemode <license-mode>
   ```

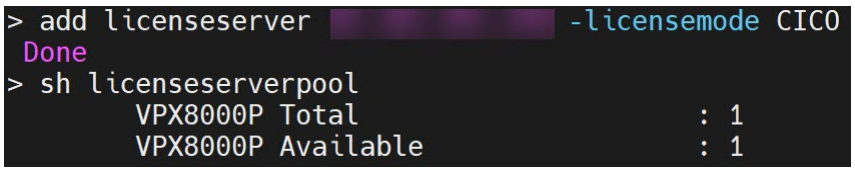
   For more information, see Licensing overview.
3. View the license bandwidth available in the license server.

   ```
   > sh ns licenseserverpool
   ```

   This command lists the licenses based on the specified license mode while adding the license server.

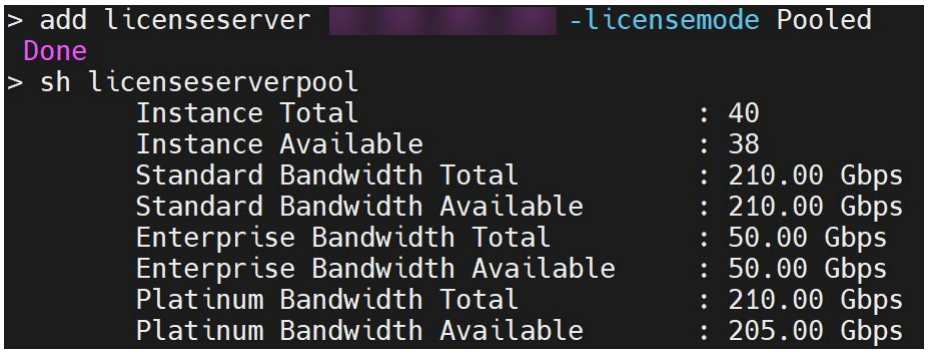
   Example-1:

   If the specified license mode is `CICO`, the output contains only CICO licenses.

   Example-2:

   If the specified license mode is `Pooled`, the output contains only Pooled capacity licenses.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Example-3:

If the specified license mode is vCPU, the output contains only virtual CPU licenses.

```
> add licenseserver [redacted] -licensemode vCPU
 Done
> sh licenseserverpool
        Standard CPU Total                  : 100
        Standard CPU Available              : 100
        Enterprise CPU Total                : 100
        Enterprise CPU Available            : 100
        Platinum CPU Total                  : 25
        Platinum CPU Available              : 20
```

To view all the licenses together, run the following command:

```
1  > sh ns licenseserverpool -getallLicenses
```

Example output:

```
> sh licenseserverpool -getallLicenses
        Instance Total                      : 40
        Instance Available                  : 33
        Standard Bandwidth Total            : 210.00 Gbps
        Standard Bandwidth Available        : 210.00 Gbps
        Enterprise Bandwidth Total          : 50.00 Gbps
        Enterprise Bandwidth Available      : 50.00 Gbps
        Platinum Bandwidth Total            : 210.00 Gbps
        Platinum Bandwidth Available        : 205.00 Gbps
        VPX8000P Total                      : 1
        VPX8000P Available                  : 1
        Standard CPU Total                  : 100
        Standard CPU Available              : 100
        Enterprise CPU Total                : 100
        Enterprise CPU Available            : 100
        Platinum CPU Total                  : 25
        Platinum CPU Available              : 20
```

4. Allocate the license bandwidth from the required license edition:

```
1  > set ns capacity -unit <specify-mbps-or-gbps> -bandwidth <specify
       -amount-license-bandwidth> -edition <specify-license-edition>
```

The license edition can be **Standard** or **Enterprise** or **Platinum**.

> **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 - Allocate Pooled licenses to NetScaler instances

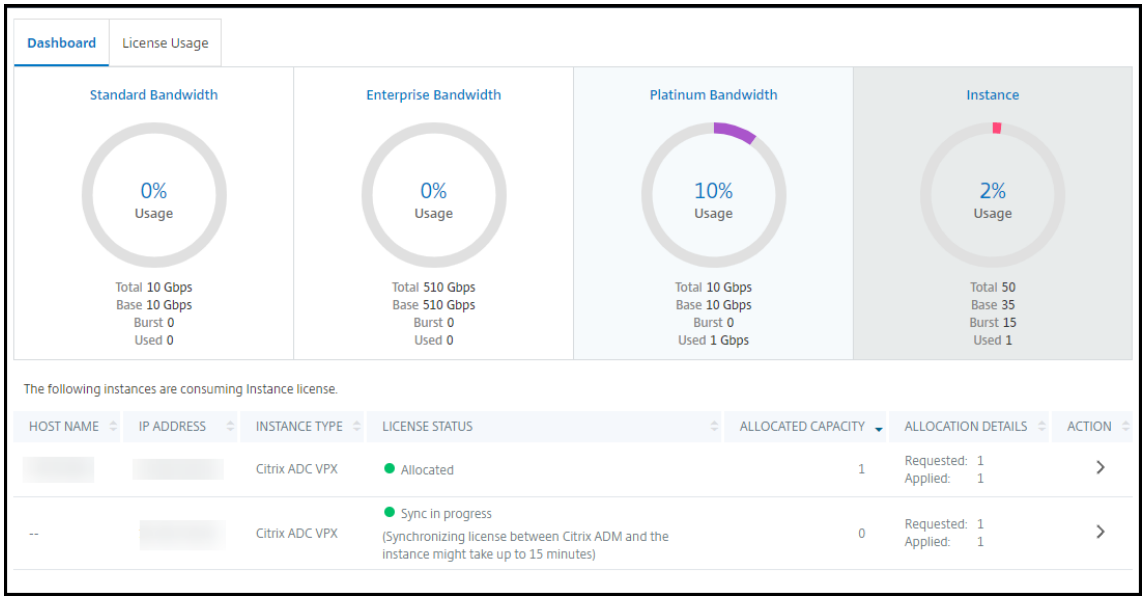
To allocate Pooled capacity licenses from the NetScaler Console GUI:

1. Log in to NetScaler Console.
2. Navigate to **Infrastructure > Licenses > 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 an NetScaler instance from the list of available instances by clicking the **>** button.



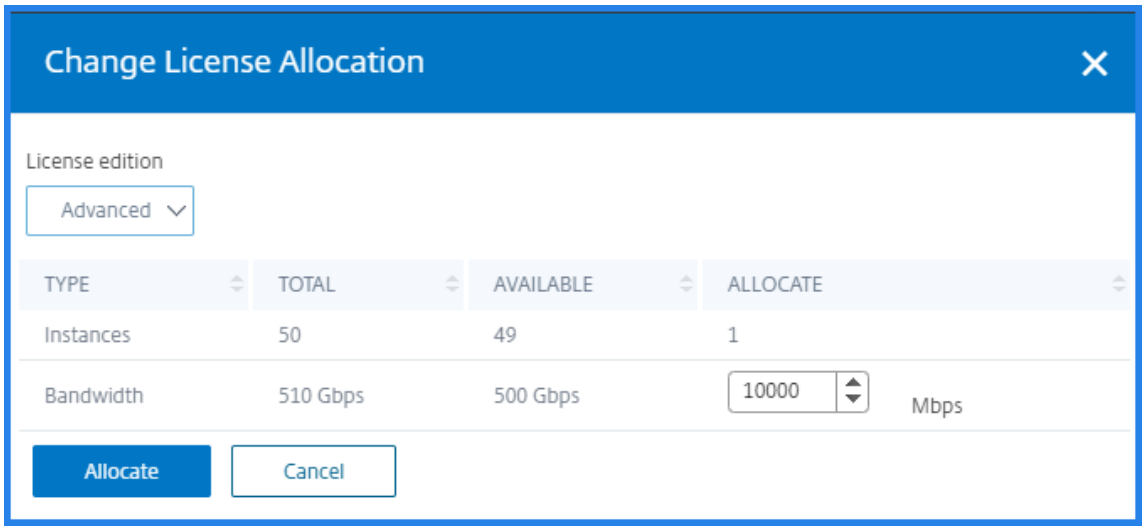
   The **LICENSE STATUS** column displays corresponding license allocation status messages.

   > **Note:**
   >
   > The **Unmanaged Instances** tab displays the instances that are discovered but not managed in NetScaler Console.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



5. Click **Change allocation** or **Release allocation** to modify the license allocation.
6. A pop-up window with the available licenses in the License Server appears.
7. You can choose the bandwidth or instance allocation to the instance by setting the **Allocate** list options. After making your selections, click **Allocate**.
8. You can also change the allocated license edition from the list options in the **Change License Allocation window**.



> **Note**
>
> Warm restart an instance if you change the license edition.

For more information on how to change the bandwidth allocation, see the related video:

This is an embedded video. Click the link to watch the video

Configure Pooled capacity on NetScaler instances

You can configure Pooled capacity licenses on the following NetScaler instances:

- NetScaler instances
- NetScaler VPX™ instances
- NetScaler high-availability pair

© 1997–2025 Citrix Systems, Inc. All rights reserved.

NetScaler MPX™ instances

MPX-Z is the Pooled capacity enabled NetScaler MPX appliance. MPX-Z supports bandwidth pooling for Premium, Advanced, or Standard edition licenses.

MPX-Z requires platform licenses before it can connect to the License Server. You can install the MPX-Z platform license by either of the following:

- 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 platform license, the Pooled capacity feature is disabled. 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 Pooled licenses required for its configured capacity.

NetScaler VPX instances

A Pooled capacity enabled NetScaler VPX instance can check out licenses from a bandwidth pool (Premium/Advanced/Standard editions). You can use the NetScaler GUI to check out licenses from the License Server.

You can dynamically modify the bandwidth of a VPX instance without a restart. A restart is required only if you want to change the license edition.

> **Note:**
>
> When you restart the instance, the configured Pooled capacity licenses are automatically checked out from the NetScaler Console server.

NetScaler high-availability pair

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.

For NetScaler instances configured in a high availability mode, you have to configure Pooled capacity on each node of the high availability pair. For both the primary and secondary nodes, you need to allocate licenses of the same capacity. For example, if you want 1 Gbps capacity from each instance

© 1997–2025 Citrix Systems, Inc. All rights reserved.

in the HA pair, you need twice the capacity (2 Gbps) from the common pool. Then you can allocate 1 Gbps capacity to each node.

To allocate pool license to each node in the pair, follow the steps given in Allocate Pooled licenses to NetScaler instances. First allocate license to the first node and then repeat the same steps to allocate license to the second node.

Upgrade a perpetual license in NetScaler VPX to NetScaler Pooled capacity

November 28, 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: 14.1-51.80, 13.1-60.29, 13.1-37.247 (FIPS)
> - NetScaler SVM: 14.1-51.83, 13.1-60.30
> - NetScaler Console Service: Supported from early September 2025.
> - NetScaler Console on-prem: 14.1-51.83
>
> **Note:** LAS support for Console on-prem is from release 14.1-51.83 onwards. However, file-based licensing is deprecated from Console on-prem releases 14.1-51.83 onwards and 13.1-60.26 onwards, and goes EOL on April 15th, 2026. That is, even if you upgrade to Console on-prem release 14.1-51.83 or release 13.1-60.26 or later, you can continue using file-based licensing. However you must upgrade to Console on-prem release 14.1-51.83 or later, and switch to LAS before 15th April 2026 because file-based licensing reaches EOL.
>
> 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.

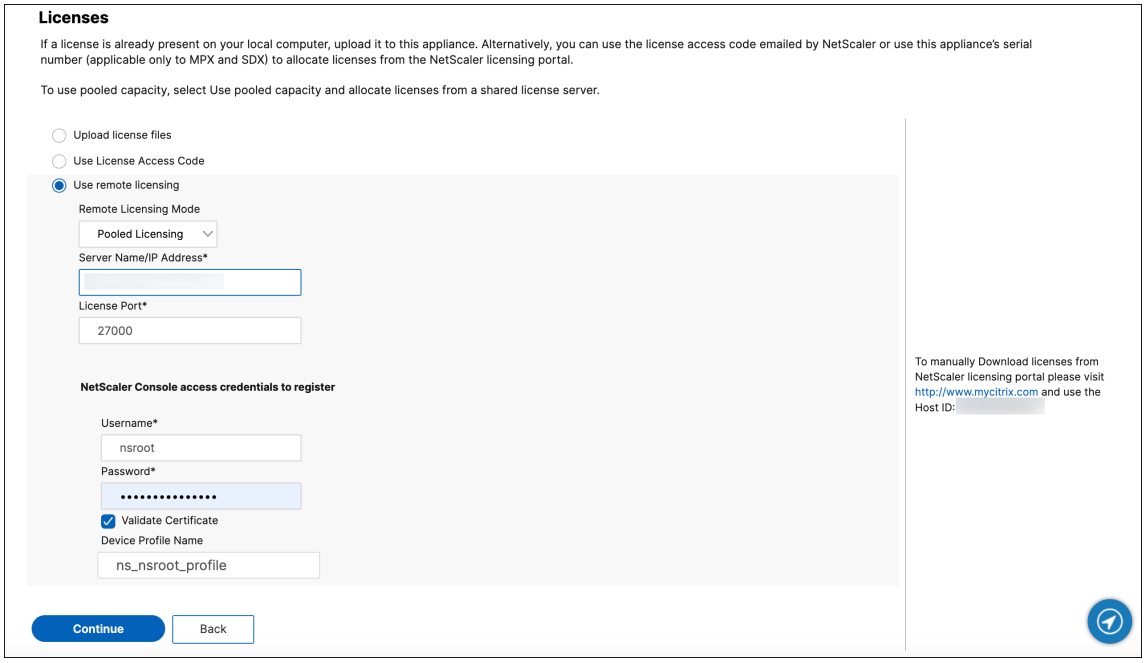
> LAS-based licenses may not be available to customers where prohibited by law or regulations.
>
> If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don't apply where prohibited by law or regulation.

NetScaler VPX instances with perpetual license can be upgraded to NetScaler Pooled capacity license. Upgrading to Pooled capacity license enables you to allocate licenses from the license pool to the VPX instances on demand. You can also configure Pooled capacity license for NetScaler instances configured in a high availability mode. To configure Pooled capacity license for VPX instances in high availability mode, see Upgrading the Perpetual License in NetScaler VPX High Availability Pair to NetScaler Pooled Capacity.

Prerequisites

To upgrade to NetScaler Pooled capacity:

1. In a Web browser, type the IP address of the VPX instance, such as http://192.168.100.1.
2. In **User Name** and **Password**, type the administrator credentials.
3. On the **Welcome** page, click **Continue**.
4. On the **Configuration tab**, navigate to **System > Licenses** and click **Manage Licenses**.
5. On the **Licenses** page, click **Add New License**.
6. On the **Licenses** page, choose **Use remote licensing** and do the following:



© 1997–2025 Citrix Systems, Inc. All rights reserved.

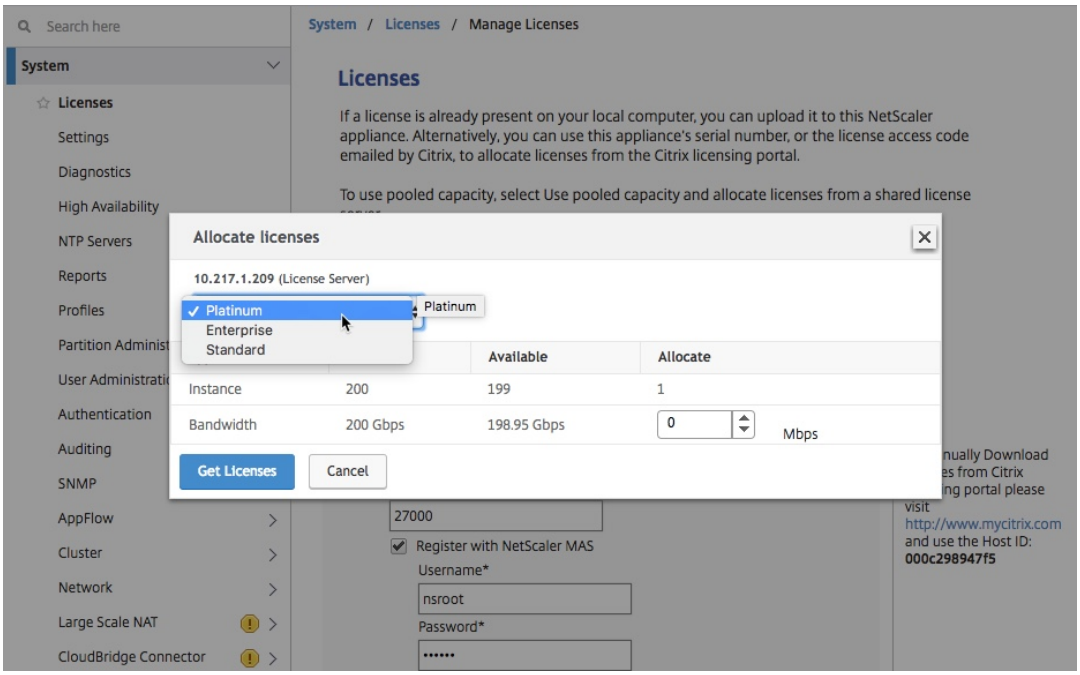
a) In the **Remote Licensing mode** drop-down list, choose **Pooled Licensing**.

b) In the **Server Name/IP Address** field, Enter the details of the license server.

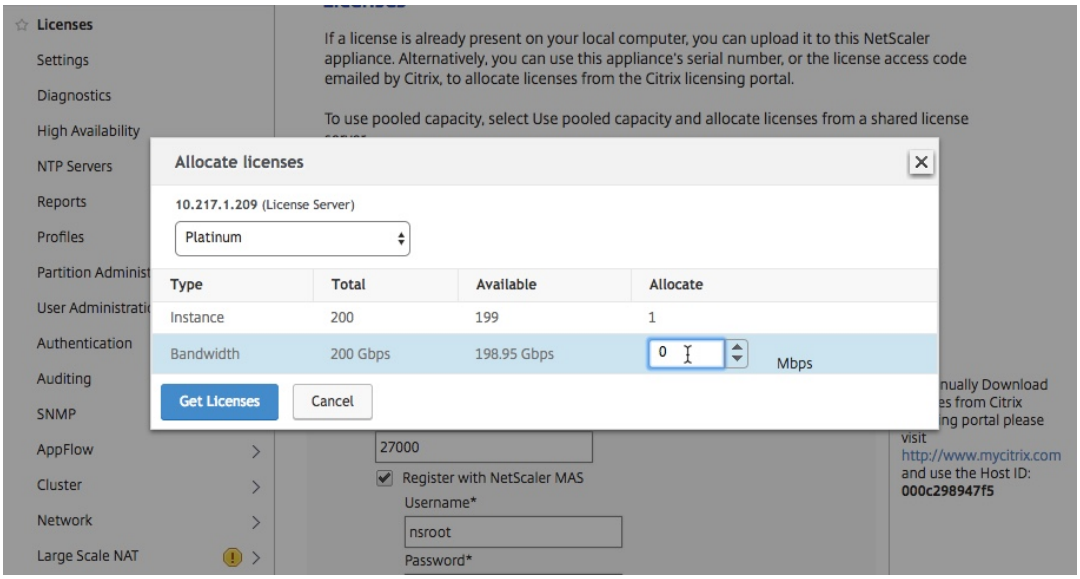
c) Click **Continue**.

7. In **Allocate licenses**, do the following:

a) Select the license edition from the drop-down list.

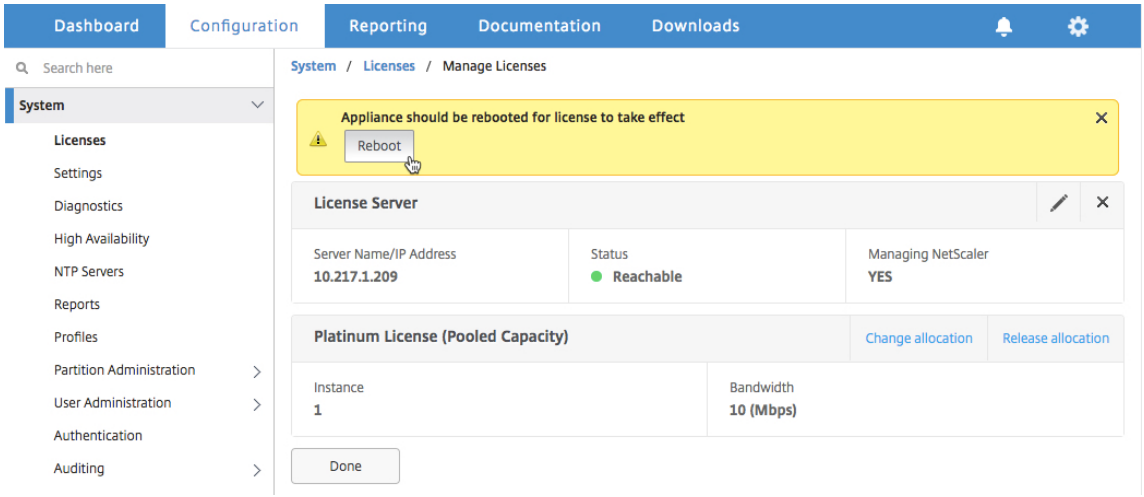


b) Allocate the bandwidth to the NetScaler appliance from the **Allocate** menu and click **Get Licenses**.



8. When prompted, click **Reboot** to reboot the appliance.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



9. In the Confirm dialog box, click **Yes**.
10. After the VPX instance restarts, log on to the instance. On the **Welcome** page, click **Continue**.

    The **Licenses** page displays all the features that are licensed on the NetScaler VPX appliance. Click **X**.
11. Navigate to **System > Licenses** and click **Manage Licenses**.

    On the **Manage Licenses** page, you can view the details of the license server, license edition, and the allocated bandwidth.

Upgrade the perpetual License in NetScaler VPX high availability pair to NetScaler Pooled capacity

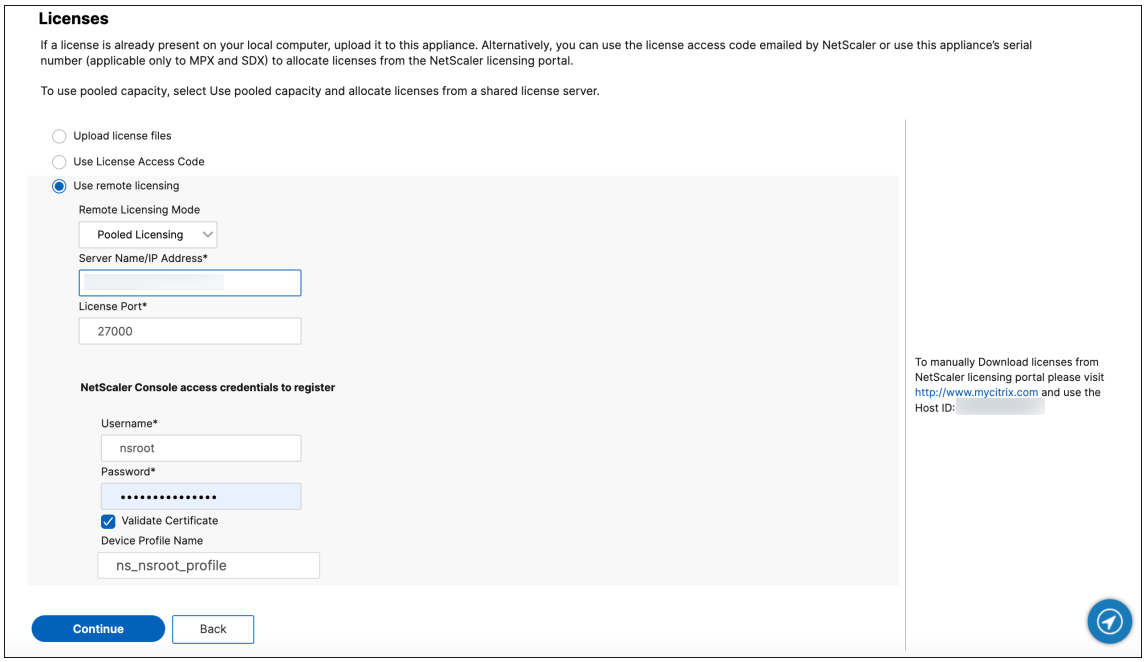
For VPX instances configured in a high availability mode, you have to configure Pooled capacity on both the primary and secondary instances in the HA pair. For both the primary and secondary instances, you need to allocate licenses of the same capacity. For example, if you want 1 Gbps capacity from each instance in the HA pair, you need twice the capacity (2 Gbps) from the common pool. Then you can allocate 1 Gbps capacity each to the primary and secondary instances in the HA pair.

To upgrade an exisiting NetScaler VPX HA setup to NetScaler Pooled Capacity:

1. Log on to the secondary VPX (node 2) 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**, type the administrator credentials.
3. On the **Welcome** page, click **Continue**.
4. On the Configuration tab, navigate to **System > Licenses** and click **Manage Licenses**.
5. On the **Licenses** page, click **Add New License**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

6. Choose **Use remote licensing** and do the following:



   a) In the **Remote Licensing mode** drop-down list, choose **Pooled Licensing**.

   b) In the **Server Name/IP Address** field, Enter the details of the license server.

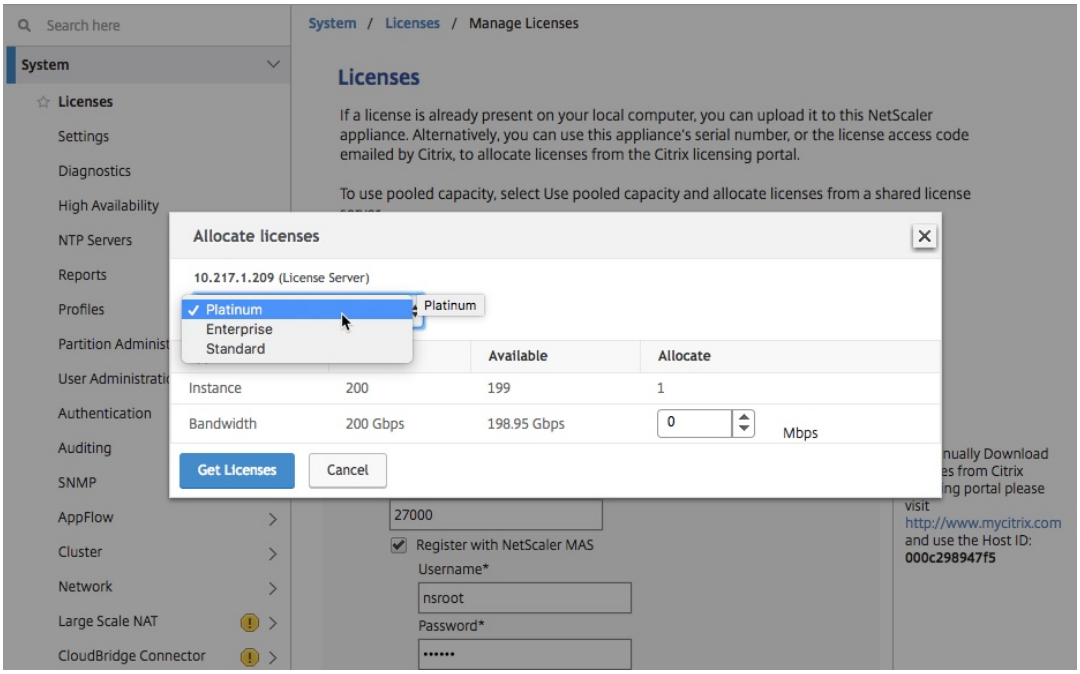
   c) Make sure that the **Register with NetScaler Console** checkbox is selected and enter the NetScaler Console credentials, if you want to manage your instance's pool licenses through NetScaler Console.

   d) Click **Continue**.

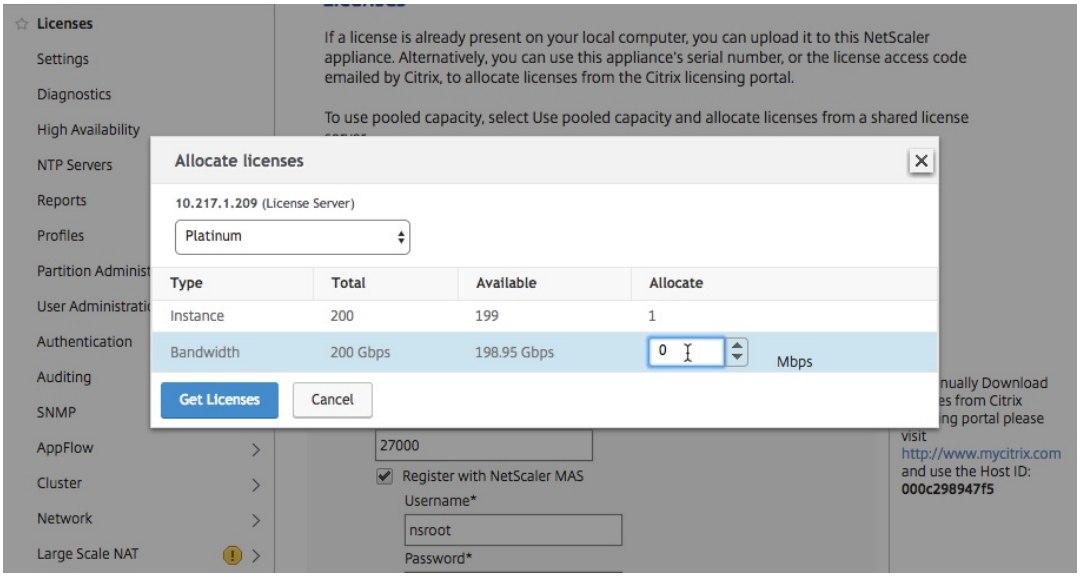
7. In **Allocate licenses**, do the following:

   a) Select the license edition from the drop-down list.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

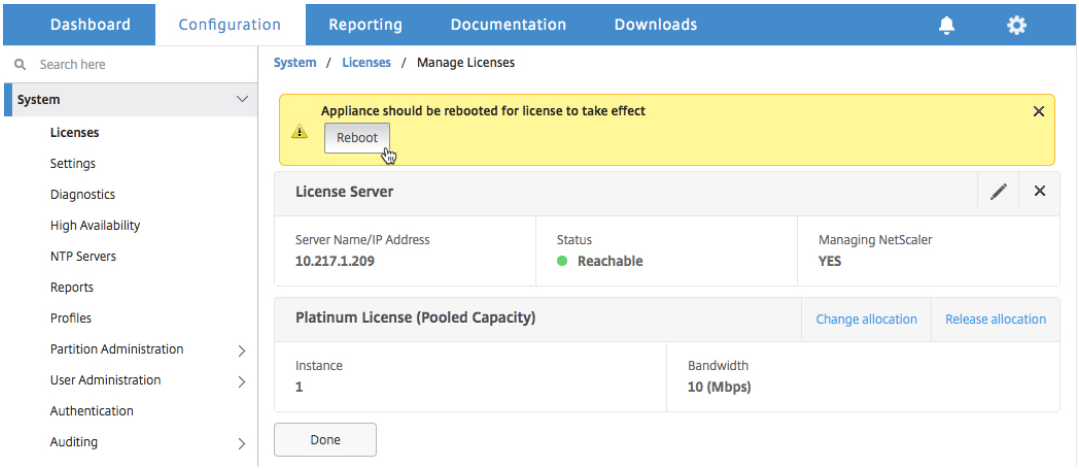


b) Allocate the bandwidth to the NetScaler appliance from the **Allocate** menu and click **Get Licenses**.



c) When prompted, click **Reboot** to warm restart the instance.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



8. In the **Confirm** dialog box, click **Yes**.

   The VPX instance reboots.

   When prompted, click **Reboot** to restart the appliance. After the appliance is up and running with the new license, force a failover by typing `force ha failover`. This failover ensures that the HA pair is in good health.

9. After the failover, log on to the new secondary VPX instance (node 1) and repeat the same process to add the new secondary to the pool.

   If you want to change the primary and secondary instances in the HA pair to your original HA pair configuration, force a failover. Run the following command on any instance in the HA pair:

   ```
   1   > force ha failover
   ```

10. To verify that the VPX instance is upgraded to Pooled capacity license, log on to the primary and secondary instances and complete the following steps.

    a) On the **Welcome** page, click **Continue**.

    b) On the Configuration tab, navigate to **System > Licenses** and click **Manage Licenses**. On the **Manage Licenses** page, you can view the details of the license server, license edition, and the allocated bandwidth.

Upgrading a perpetual license in NetScaler MPX to NetScaler Pooled capacity

November 28, 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: 14.1-51.80, 13.1-60.29, 13.1-37.247 (FIPS)
> - NetScaler SVM: 14.1-51.83, 13.1-60.30
> - NetScaler Console Service: Supported from early September 2025.
> - NetScaler Console on-prem: 14.1-51.83
>
> **Note:** LAS support for Console on-prem is from release 14.1-51.83 onwards. However, file-based licensing is deprecated from Console on-prem releases 14.1-51.83 onwards and 13.1-60.26 onwards, and goes EOL on April 15th, 2026. That is, even if you upgrade to Console on-prem release 14.1-51.83 or release 13.1-60.26 or later, you can continue using file-based licensing. However you must upgrade to Console on-prem release 14.1-51.83 or later, and switch to LAS before 15th April 2026 because file-based licensing reaches EOL.
>
> All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
>
> LAS-based licenses may not be available to customers where prohibited by law or regulations.
>
> If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don't apply where prohibited by law or regulation.

Read the following note before proceeding further.

NetScaler MPX 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. You can also configure 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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Note**
>
> Conversion from a perpetual license to a Pooled capacity license is a one-way process for license entitlement. You can't revert the Pooled capacity license to perpetual.
> **Important**
>
> For upgrading NetScaler MPX to NetScaler Pooled capacity license, you need to upload the MPX-Z license to the appliance.

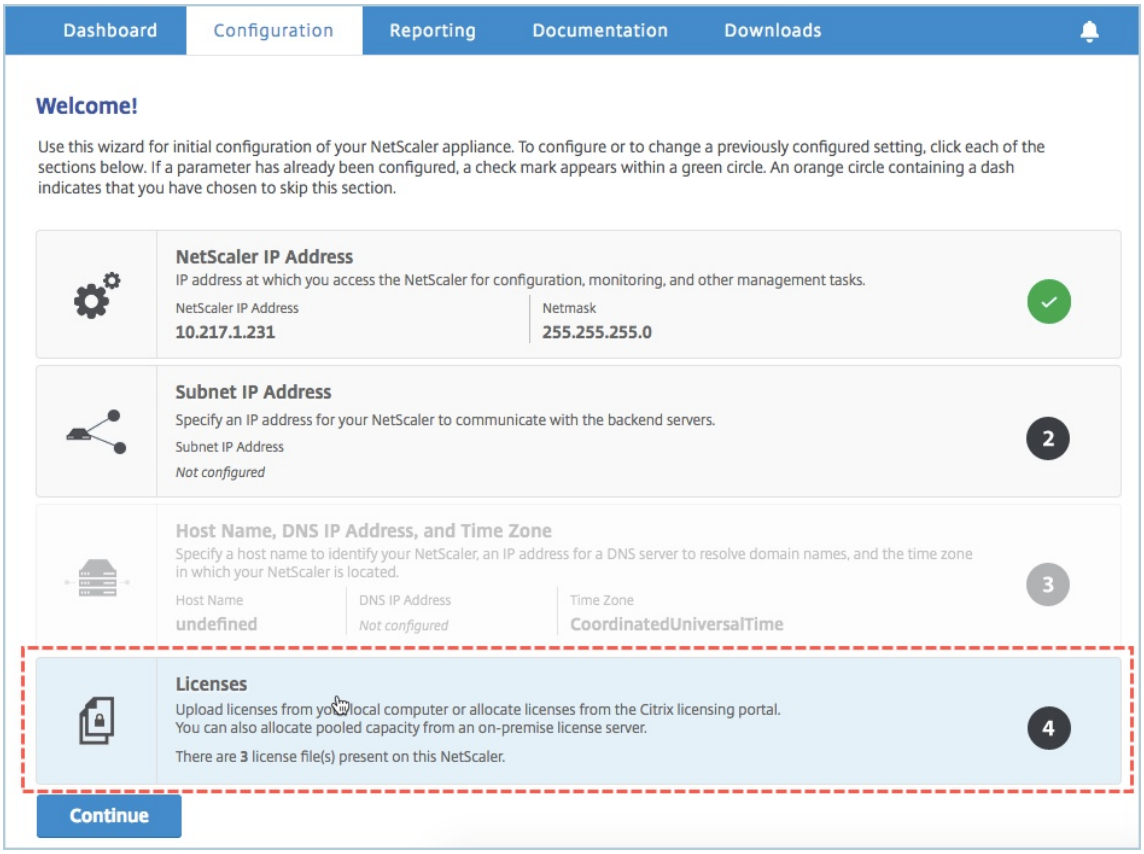
To upgrade to NetScaler Pooled capacity:

1. In a Web browser, type the IP address of the NetScaler, such as http://192.168.100.1.
2. In **User Name** and **Password**, 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.
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 can't connect to the appliance through the NetScaler Console GUI, by using HTTPS.

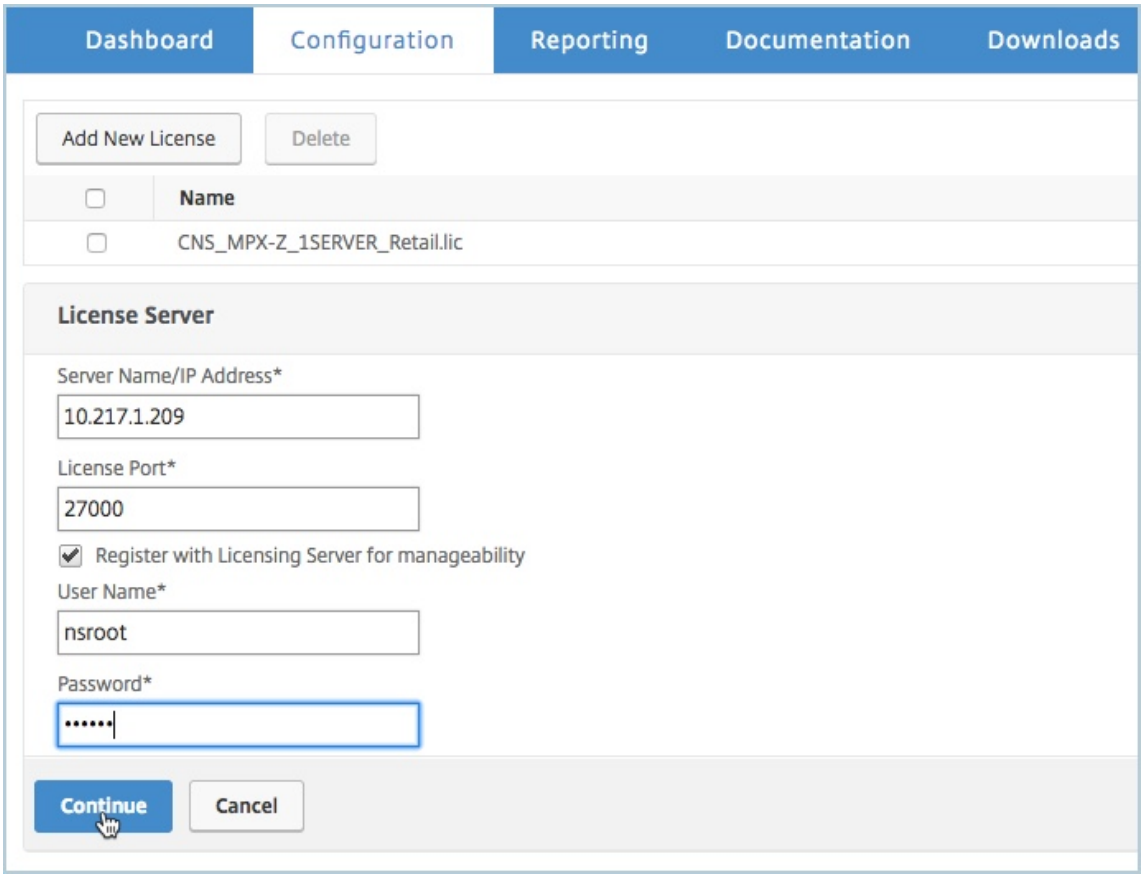
8. On the **Confirm** page, click **Yes**.
9. After the appliance reboots, logon to the appliance.
10. On the Welcome page, click the **Licenses** section.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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.

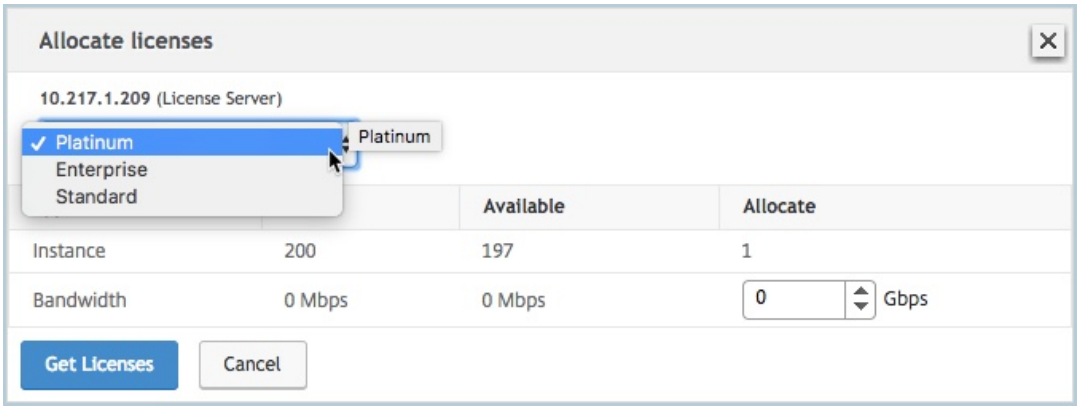
c) If you want to manage your instance's pool licenses through NetScaler Console, select the **Register with Licensing Server for manageability** checkbox and enter NetScaler Console credentials.

d) Click **Continue**.

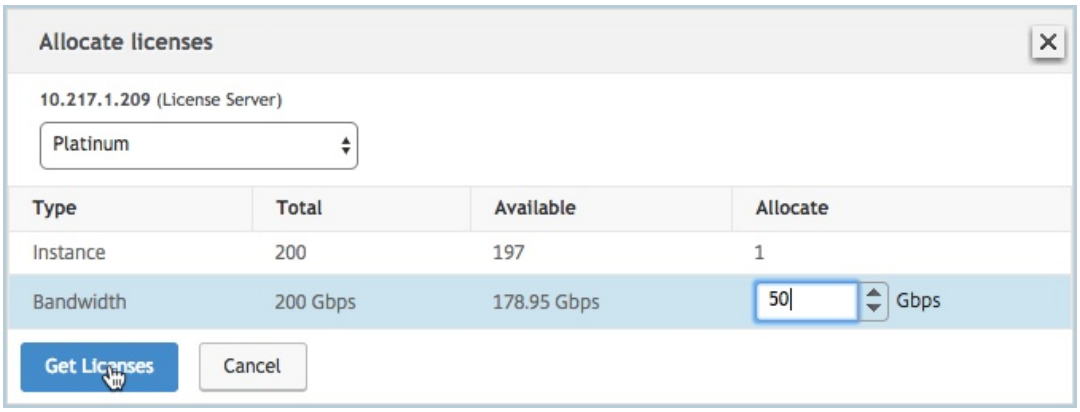
12. In **Allocate licenses**, do the following:

a) Select the license edition from the drop-down list.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



b) Allocate the bandwidth to NetScaler from the **Allocate** menu and click **Get Licenses**.



c) When prompted, click **Reboot** to reboot the appliance.

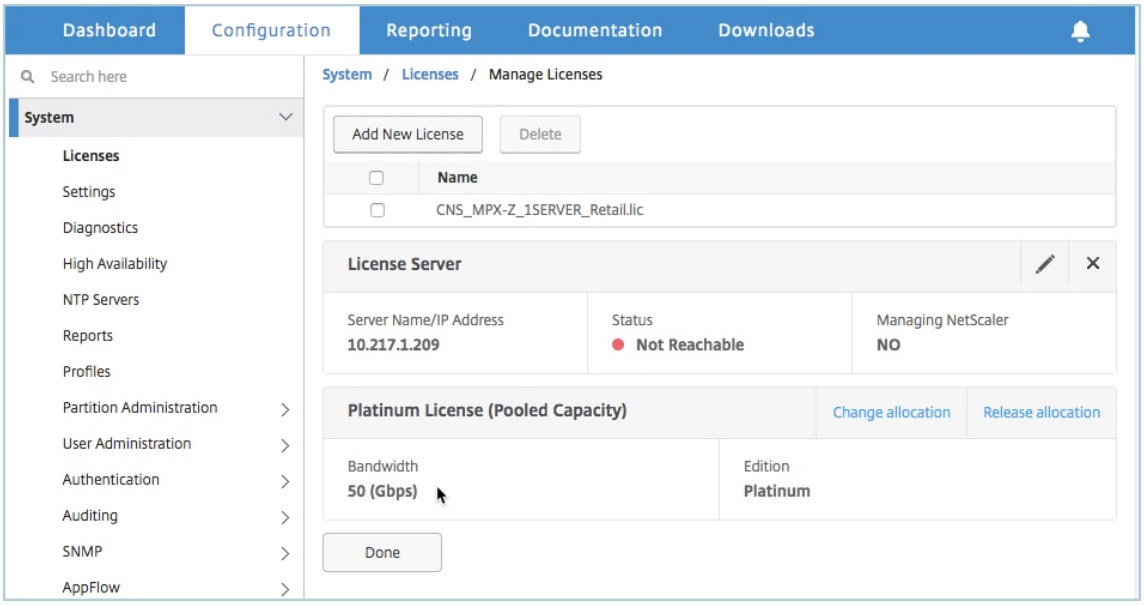
13. Once NetScaler MPX reboots, logon to the NetScaler MPX. On the **Welcome** page, click **Continue**.

    The **Licenses** page lists all the licensed features.

14. Navigate to **System > Licenses** 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 MPX appliances configured in high availability mode, you have to configure Pooled capacity on both the primary and secondary NetScaler instances in the HA pair. 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. With 2 Gbps capacity, you can allocate 1 Gbps each to the primary and secondary NetScaler instances in the HA pair.

> **Important**
>
> For upgrading NetScaler MPX 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**, type the administrator credentials.
3. On the **Welcome** page, click **Continue**.

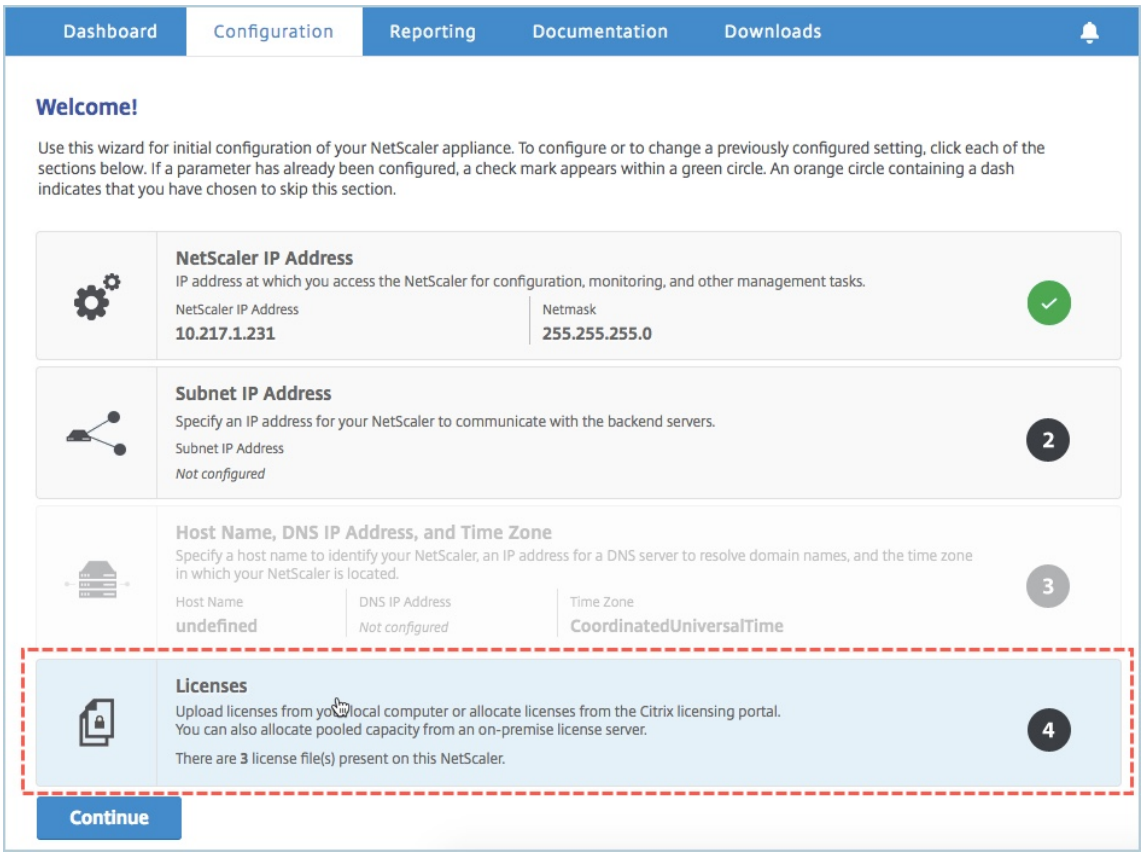
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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**.

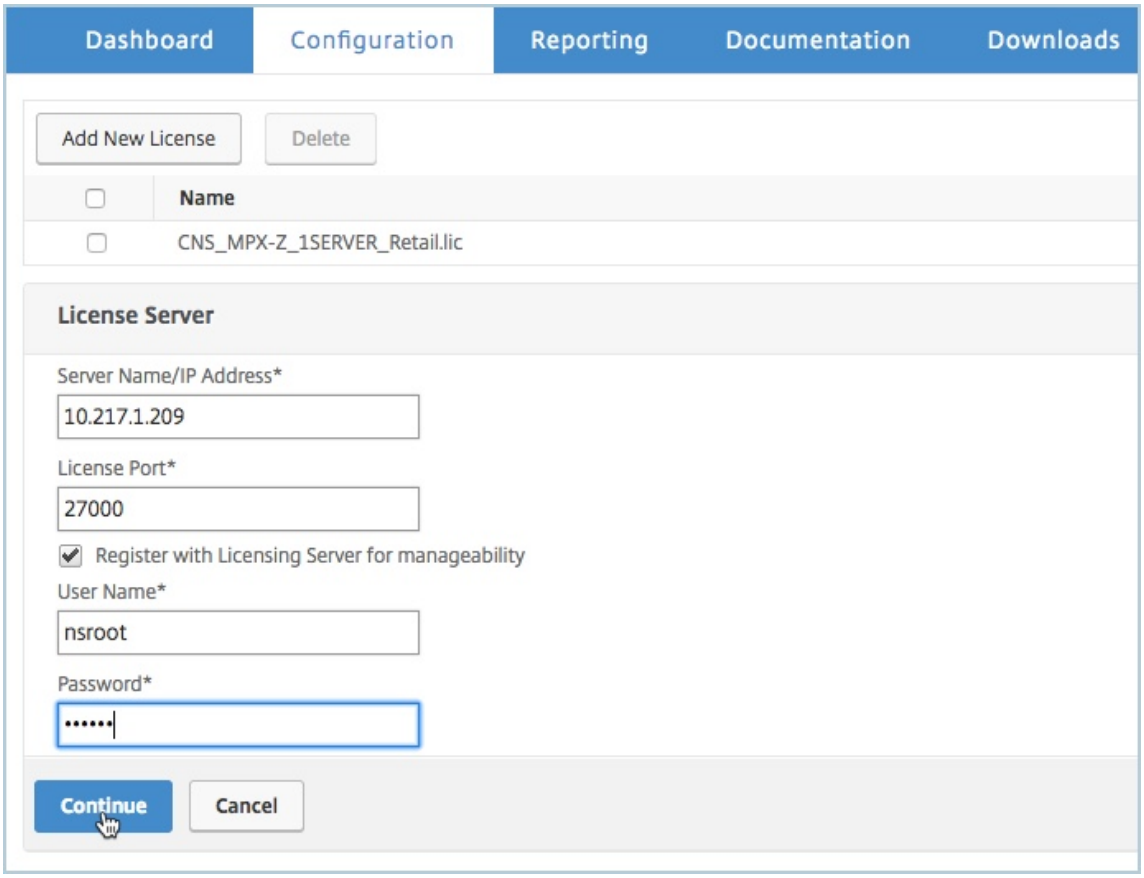
To upgrade an exisiting HA setup to NetScaler Pooled Capacity:

1. Log on to the secondary NetScaler MPX Instance. In a Web browser, type the IP address of NetScaler, such as http://192.168.100.1.
2. In **User Name** and **Password**, 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.

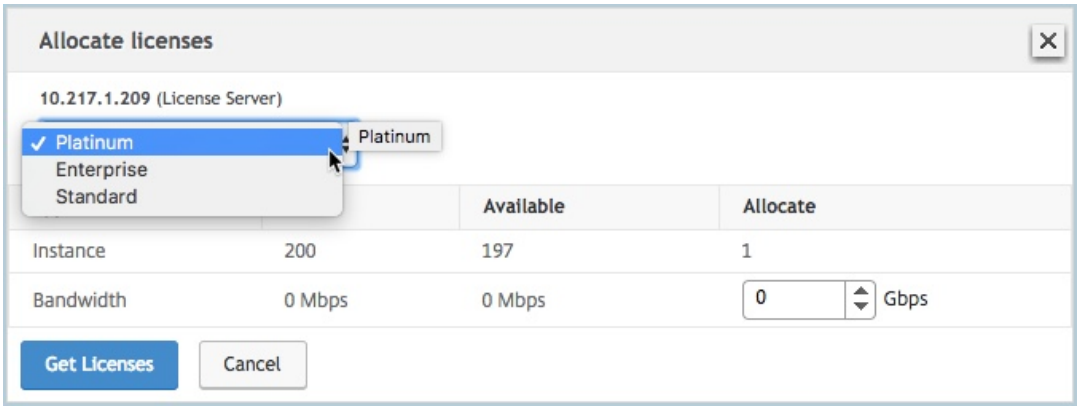
c) If you want to manage your instance's pool licenses through NetScaler Console, select the **Register with Licensing Server for manageability** checkbox and enter NetScaler Console credentials.

d) Click **Continue**.

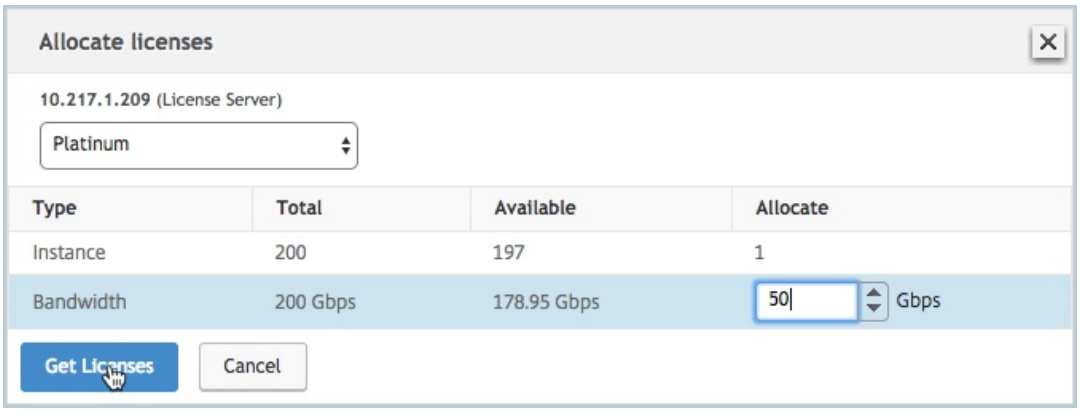
5. In **Allocate licenses**, do the following:

a) Select the license edition from the drop-down list.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



b) Allocate the bandwidth to NetScaler from the **Allocate** menu and click **Get Licenses**.



c) When prompted, click **Reboot** to restart the appliance. After the appliance is up and running with the new license, force a failover by typing `force ha failover`. This failover ensures that the HA pair is in good health.

6. Log on to the existing primary NetScaler MPX and reboot the appliance. Perform the following:

   a) In a Web browser, type the IP address of the NetScaler, such as http://192.168.100.1.

   b) In **User Name** and **Password**, type the administrator credentials.

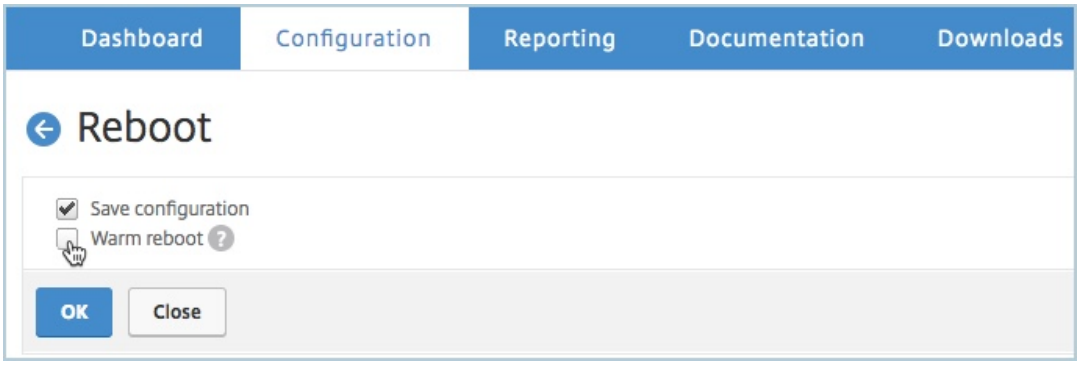
   c) On the **Welcome** page, click **Continue**.

   d) On the **Configuration** tab, click **System**.

   e) On the **System** page, click **Reboot**.

   f) On the **Reboot** page, select **Warm reboot** and click **OK**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



After the primary NetScaler MPX reboots, it becomes the secondary NetScaler MPX in the HA pair. If you want to change the primary and secondary instances in the HA pair to your original HA pair configuration, force a failover. Run 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

October 3, 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: 14.1-51.80, 13.1-60.29, 13.1-37.247 (FIPS)
> - NetScaler SVM: 14.1-51.83, 13.1-60.30
> - NetScaler Console Service: Supported from early September 2025.
> - NetScaler Console on-prem: 14.1-51.83
>
> **Note:** LAS support for Console on-prem is from release 14.1-51.83 onwards. However, file-

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> based licensing is deprecated from Console on-prem releases 14.1-51.83 onwards and 13.1-60.26 onwards, and goes EOL on April 15th, 2026. That is, even if you upgrade to Console on-prem release 14.1-51.83 or release 13.1-60.26 or later, you can continue using file-based licensing. However you must upgrade to Console on-prem release 14.1-51.83 or later, and switch to LAS before 15th April 2026 because file-based licensing reaches EOL.
>
> 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.

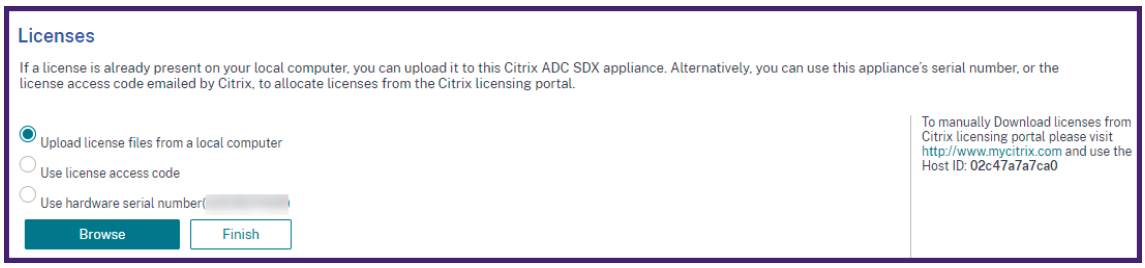
NetScaler SDX with perpetual license can be upgraded to NetScaler Pooled capacity license. Upgrading to NetScaler Pooled Capacity license enables you to allocate licenses from the license pool to NetScaler on demand. You can also configure NetScaler Pooled capacity license for NetScaler instances configured in high availability mode.

> **Important**
>
> 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.
>
> - For upgrading NetScaler SDX 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 ensure that there is no impact on the current licenses, the customer has to allocate the same number of instances and bandwidth that is available as part of the perpetual license.

To upgrade to NetScaler Pooled capacity:

1. In a Web browser, type the IP address of NetScaler SDX, such as http://192.168.100.1.
2. In **User Name** and **Password**, type the administrator credentials.
3. On the **Welcome** page, click **Continue**.
4. Upload the zero-capacity license. On the Configuration tab, navigate to **System** > **Licenses**.
5. On the **Manage Licenses** page, click **Add License File**.
6. In the **Licenses** page, select **Upload license files from a local computer** and click **Browse** to select the zero-capacity license from your local machine. Then, click **Finish**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Once the zero-capacity license is applied successfully, the **Pooled Licenses** section appears on the **Licenses** page.

> **Note**
>
> To remove the old license file, you don't have to reboot your NetScaler SDX and therefore downtime is avoided. For more help, contact NetScaler support.

7. In the **Pooled licenses** section, do the following:

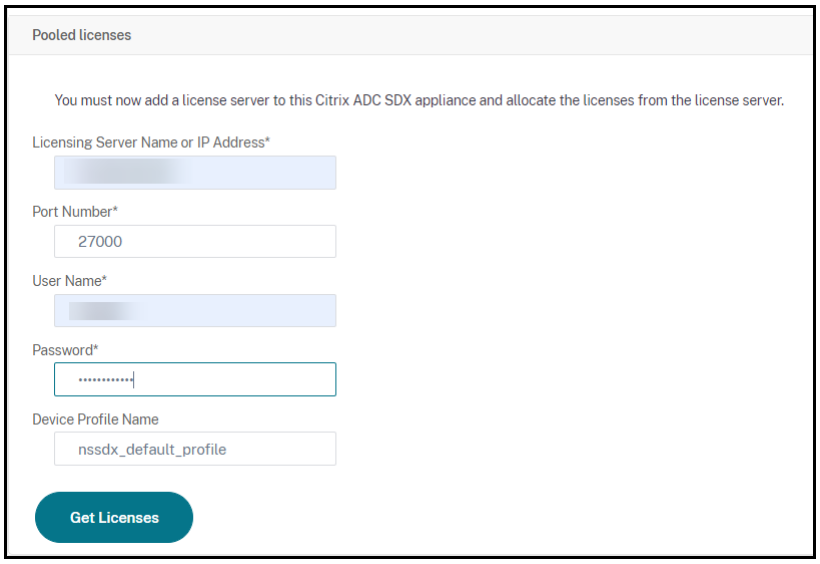
   a) In the **Licensing Server Name or IP Address** field, enter the license server details. If you want to configure the NetScaler Console server as a license server, specify the NetScaler Console server's IP address.

   b) In the **Port Number** field, enter the license server port. Default value: 27000.

   c) Specify **User Name** and **Password** of the licensing server.

      - For the NetScaler Console server, enter the administrator credentials.
      - For the NetScaler Console agent, enter the agent credentials.

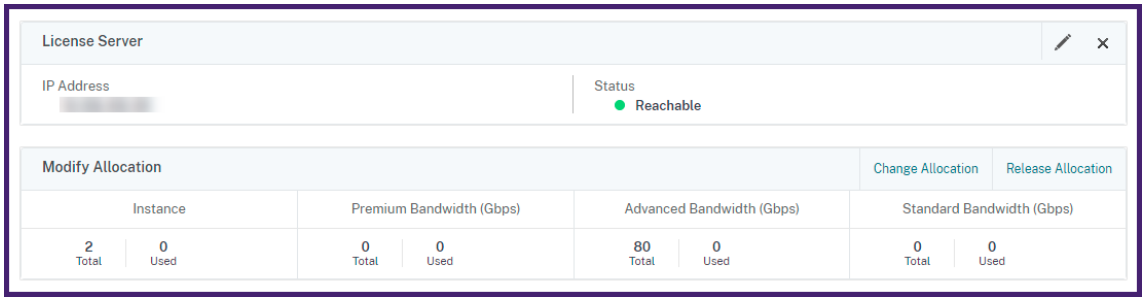
   d) Click **Get Licenses**.



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 Pooled capacity on NetScaler instances in cluster mode

October 3, 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: 14.1-51.80, 13.1-60.29, 13.1-37.247 (FIPS)
> - NetScaler SVM: 14.1-51.83, 13.1-60.30
> - NetScaler Console Service: Supported from early September 2025.
> - NetScaler Console on-prem: 14.1-51.83
>
> **Note:** LAS support for Console on-prem is from release 14.1-51.83 onwards. However, file-based licensing is deprecated from Console on-prem releases 14.1-51.83 onwards and 13.1-60.26 onwards, and goes EOL on April 15th, 2026. That is, even if you upgrade to Console on-prem release 14.1-51.83 or release 13.1-60.26 or later, you can continue using file-based

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> licensing. However you must upgrade to Console on-prem release 14.1-51.83 or later, and switch to LAS before 15th April 2026 because file-based licensing reaches EOL.
>
> 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 configure NetScaler Pooled capacity on the NetScaler instances configured as a cluster. The following are the prerequisites for configuring Pooled capacity on NetScaler instances in cluster mode:

- Instances are individually running in a Pooled capacity license mode to form the cluster.
- All the instances must be running with the same bandwidth.
- All the instances checked out the Pooled capacity from the same NetScaler Console.
- New instances cannot be added to an existing NetScaler cluster unless their capacity and NetScaler Console configurations are the same as those of the existing instances in the cluster.

Any capacity check-out from the NetScaler cluster assigns the same capacity to all the cluster nodes and the checkout Bandwidth = Bandwidth provided * number of nodes.

For example, if you check-out 50 Mbps of bandwidth from the NetScaler cluster, and the cluster includes 12 instances, each instance automatically receives 50 Mbps. And, 600 Mbps is checked out from the pool.

> **Note**
>
> If one or more instances in the cluster become unresponsive, the cluster continues to process the traffic with the remaining instances' capacity.

Allocate NetScaler Pooled capacity to a NetScaler cluster

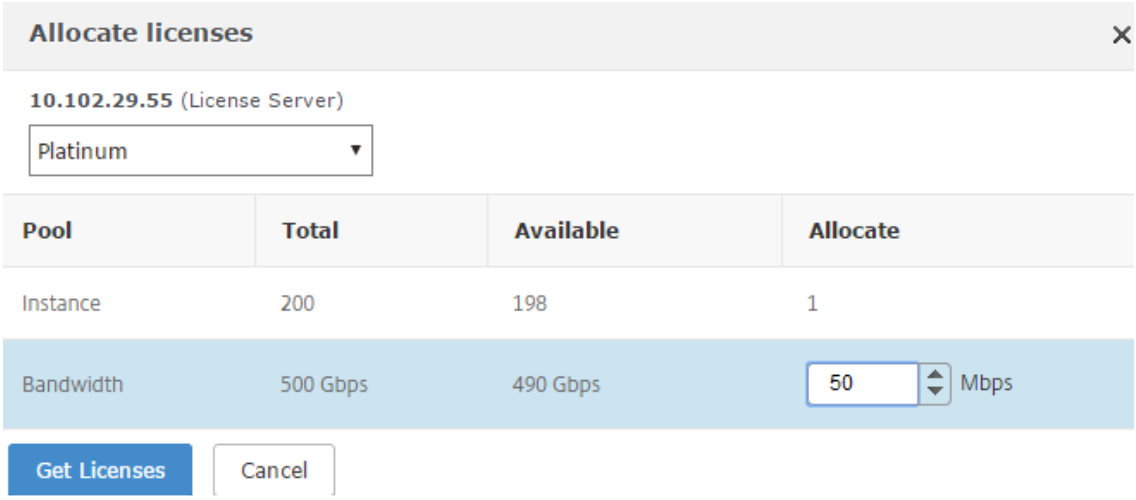
Allocate licenses to each cluster node separately. Because the commands to propagate and synchronize licenses across the cluster nodes are disabled.

Repeat the following procedure on each cluster node:

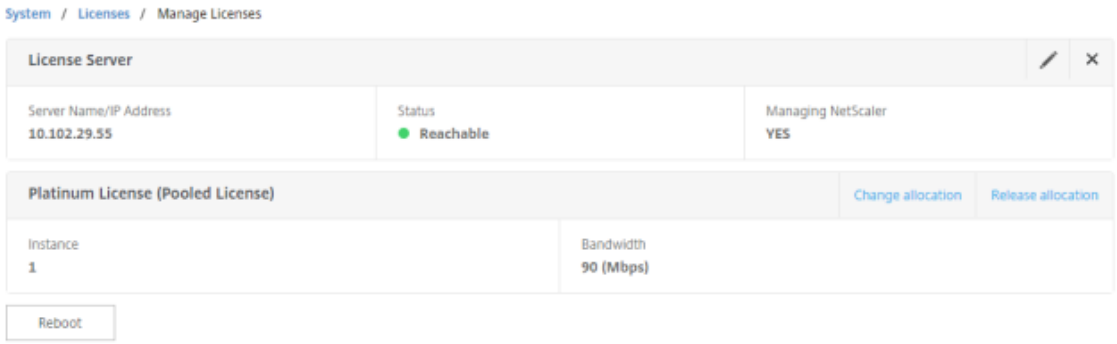
1. In a web browser, type the NetScaler IP address (NSIP). For example, `http://192.168.100.1`.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. In the **User Name** and **Password** fields, enter the administrator credentials.
3. On the **Configuration** tab, navigate to **System > Licenses > Manage Licenses**. Click **Add New License,** and select **Use Pooled Licensing**.
4. Enter the name or address of the license server in the **Server Name/IP Address** field.
5. If you want to manage your instance's pool licenses through NetScaler Console, select the **Register with NetScaler Console for manageability** checkbox and enter the NetScaler Console credentials.
6. Select the license edition and the required bandwidth, and click **Get Licenses**.



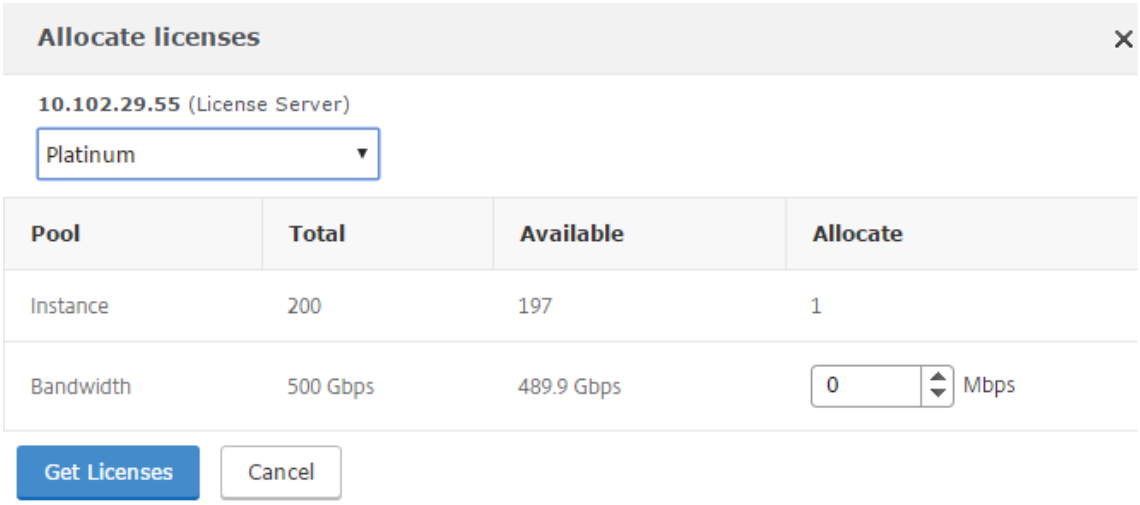
7. You can change or release the license allocation by selecting **Change allocation** or **Release allocation**.



8. If you click **Change allocation**, a pop-up window shows the licenses available on the license server.

> **Note**
>
> Bandwidth allocation must be an integral multiple of the minimum bandwidth unit of the corresponding form factor.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



9. You can allocate bandwidth or instances to the NetScaler instance from the **Allocate** drop-down list. Then click **Get Licenses**.
10. You can choose the license edition and the bandwidth required from the drop-down lists in the pop-up window.

> **Note**
>
> A restart is not required if you change the bandwidth allocation, but a warm restart is required if you change the license edition.

Allocate NetScaler Pooled capacity to a NetScaler cluster using the CLI

Allocate licenses to each cluster node separately. Because the commands to propagate and synchronize licenses across the cluster nodes are disabled.

Repeat the following procedure on each cluster node:

1. In an SSH client, enter the NetScaler IP address (NSIP), and log in by using administrator credentials.
2. To add a licensing server, enter the following command:

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
    port number >]
```

```
> add ns licenseserver 10.102.29.97 -port 27000
 Done
```

3. To show the available licenses on the licensing server, enter the following command:

```
sh licenseserverpool
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
> 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 the NetScaler VPX appliance, 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
```

Check in and check out NetScaler VPX and NetScaler BLX licenses

November 28, 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: 14.1-51.80, 13.1-60.29, 13.1-37.247 (FIPS)
> - NetScaler SVM: 14.1-51.83, 13.1-60.30
> - NetScaler Console Service: Supported from early September 2025.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> - NetScaler Console on-prem: 14.1-51.83
>
>   **Note:** LAS support for Console on-prem is from release 14.1-51.83 onwards. However, file-based licensing is deprecated from Console on-prem releases 14.1-51.83 onwards and 13.1-60.26 onwards, and goes EOL on April 15th, 2026. That is, even if you upgrade to Console on-prem release 14.1-51.83 or release 13.1-60.26 or later, you can continue using file-based licensing. However you must upgrade to Console on-prem release 14.1-51.83 or later, and switch to LAS before 15th April 2026 because file-based licensing reaches EOL.
>
> 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 and NetScaler BLX licenses to NetScaler instances on demand from NetScaler Console. The NetScaler Console software stores and manages the licenses, which have a licensing framework that provides scalable and automated license provisioning. An instance can check out the license from NetScaler Console when it is provisioned. When an instance is removed or destroyed, the instance checks back in its license to the NetScaler Console software.

Prerequisites

Make sure that the following prerequisites are met:

- You are using a NetScaler VPX image running software version 12.0.
  For example: NSVPX-ESX-12.0-xx.xx_nc.zip
- You have installed NetScaler Console running version 12.0.
  For example: MAS-ESX-12.0-xx.xx.zip

> **Note**
>
> To manage existing NetScaler VPX licenses by NetScaler Console, you need to rehost the licenses to NetScaler Console.

Installing licenses in NetScaler Console

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Note**
>
> Before installing licenses, restart the NetScaler Console virtual appliance if you have changed the software edition or bandwidth.

To install license files on NetScaler Console:

1. In a web browser, type the IP address of NetScaler Console (for example, http://192.168.100.1).
2. In User Name and Password, enter the administrator credentials.
3. Navigate to **Infrastructure > Pooled Licensing**.
4. In the **License Files** section, 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.
     To add license files, click **Browse** and select the license file (.lic) that you want to add. Then click **Finish**.
   - **Use license access code** - Citrix emails the license access code for the licenses that you purchase.
     To add license files, enter the license access code in the text box and then click **Get Licenses**.

   > **Note**
   >
   > Make sure you are connected to the internet before using the license access code for installing the licenses.

   At any time, you can add more licenses to NetScaler Console from the **License Settings** page.

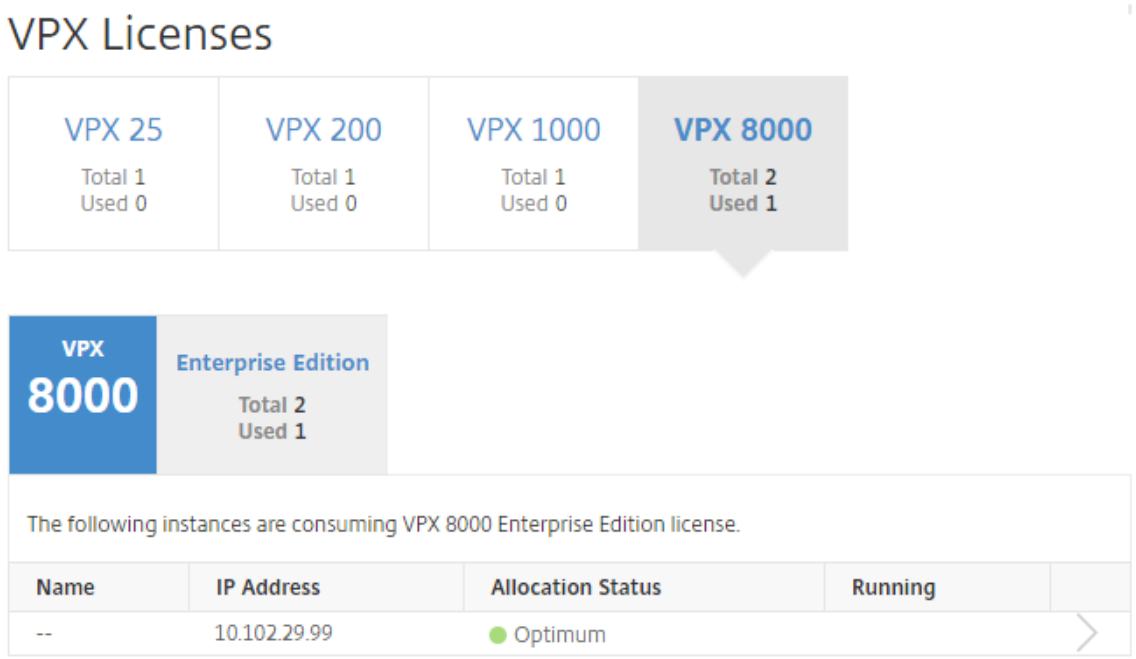
Verification

You can view the available and allocated licenses in the NetScaler Console GUI.

To display the licenses:

1. In a web browser, type the IP address of NetScaler Console (for example, http://192.168.100.1).
2. In **User Name** and **Password**, enter the administrator credentials.
3. On the Configuration tab, navigate to **Infrastructure > Pooled Licensing > VPX Licenses**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

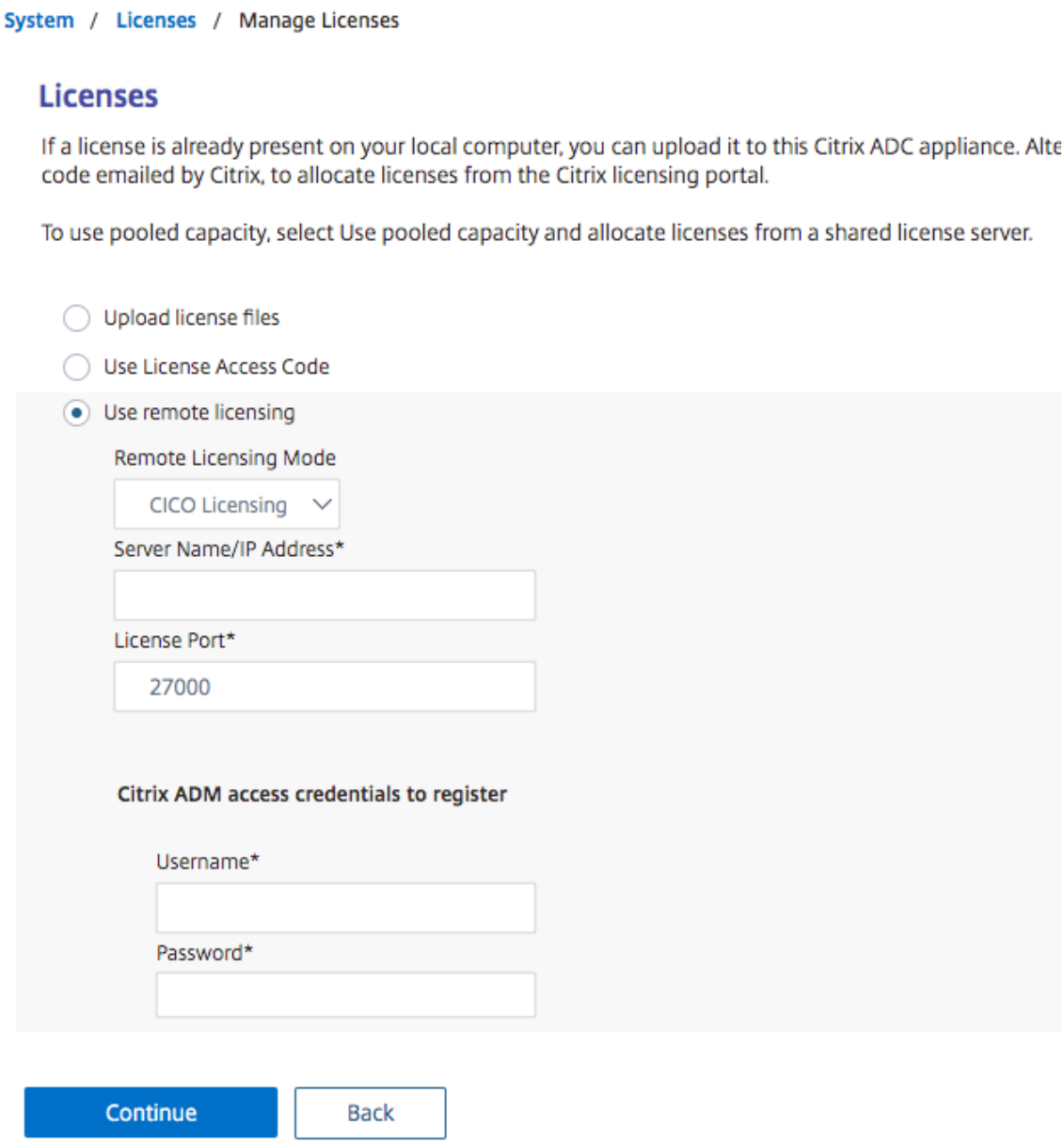


4. You can view the allocated licenses in the table under the available licenses section.

Allocate NetScaler VPX and NetScaler BLX Licenses to an NetScaler instance by using the NetScaler GUI

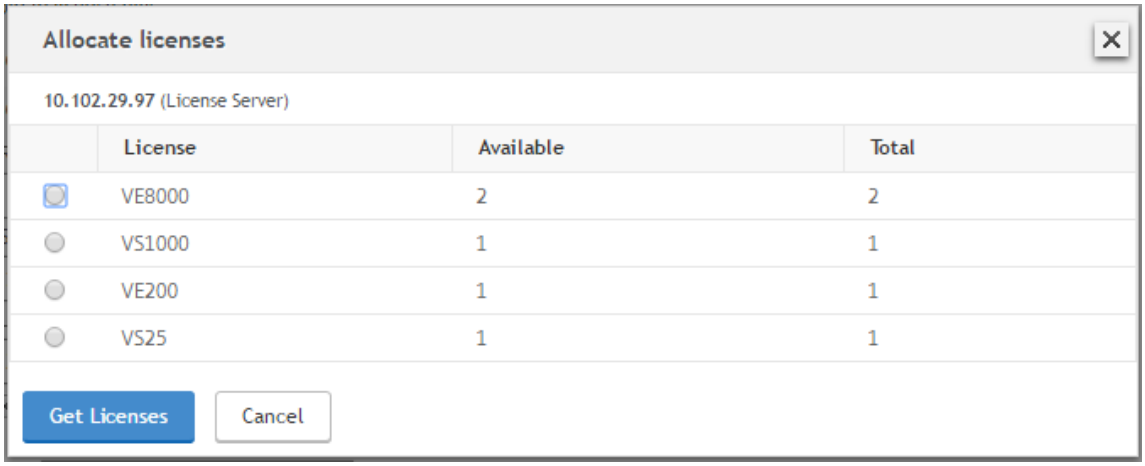
1. In a web browser, type the IP address of the NetScaler instance (for example, http://192.168.100.1).
2. In the **User Name** and **Password** fields, enter the administrator credentials.
3. On the Configuration tab, navigate to **Settings > Licenses > Manage Licenses**, click **Add New License**, and select **Use Remote Licensing > CICO Licensing**.
4. Enter the details of the license server in the **Server Name/IP Address field**.
5. In **Username** and **Password**, enter NetScaler Console credentials and click **Continue**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

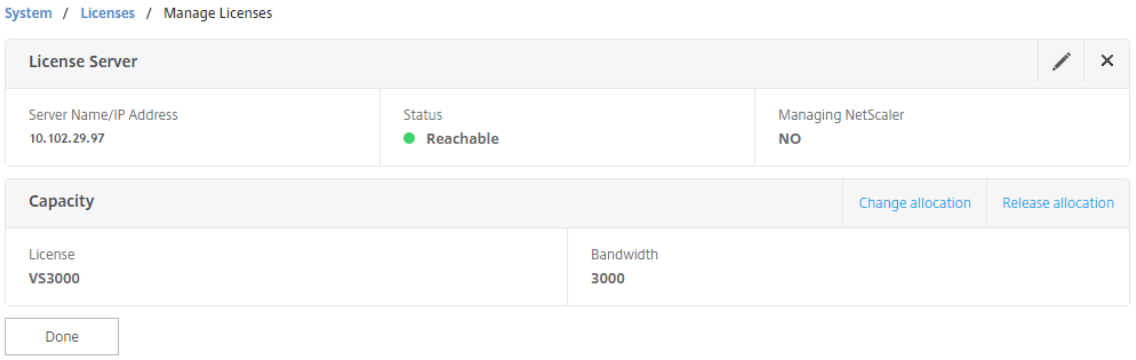


6. Select the license edition with the required bandwidth, click **Get Licenses**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



7. Click **Reboot**, your NetScaler instance reboots.
8. You can change or release the license allocation by navigating to **System > Licenses > Manage Licenses**, and selecting **Change allocation** or **Release allocation.**



9. If you click **Change allocation**, a pop-up window shows the licenses available on the license server. Select the required license, click **Get Licenses**.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Allocate NetScaler VPX and NetScaler BLX Licenses to an NetScaler instance by using the NetScaler CLI

1. In an SSH client, enter the IP address of the NetScaler instance, and log on by using administrator credentials.
2. To add a licensing server, enter the following command:

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
    port number >]
```

```
> add ns licenseserver 10.102.29.97 -port 27000
 Done
```

3. To show the available licenses on the licensing server, enter the following command:

```
sh licenseserverpool
```

```
> sh licenseserverpool
        Instance Total                  : 0
        Instance Available              : 0
        Standard Bandwidth Total        : 0 Mbps
        Standard Bandwidth Availabe     : 0 Mbps
        Enterprise Bandwidth Total      : 0 Mbps
        Enterprise Bandwidth Available  : 0 Mbps
        Platinum Bandwidth Total        : 0 Mbps
        Platinum Bandwidth Available    : 0 Mbps
        VPX25S Total                    : 1
        VPX25S Available                : 1
        VPX200E Total                   : 1
        VPX200E Available               : 1
        VPX1000S Total                  : 1
        VPX1000S Available              : 1
        VPX8000E Total                  : 2
        VPX8000E Available              : 1
 Done
```

4. To assign a license to NetScaler, 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
```

Allocate NetScaler VPX and NetScaler BLX Licenses to an NetScaler instance by using the API

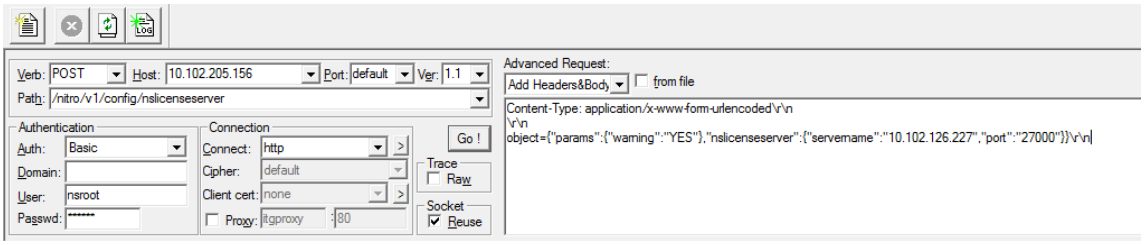
In a web browser or an API client, log on to the NetScaler instance by using the administrator credentials.

To add a licensing server:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

1. Set the request type to **Post**.
2. Set the path to /nitro/v1/config/nslicensingserver.
3. Set the payload as follows:

```
content-type: application/x-www-form-urlencoded\\r\\n
\\r\\n
object= {
  " params " ;{
 warning " : " yes "  }
 , " nslicensing server " ;{
 servername " : " \<NetScaler Console IP\> " ,  " port " : " 27000 "  }
  }
 \\r\\n
```



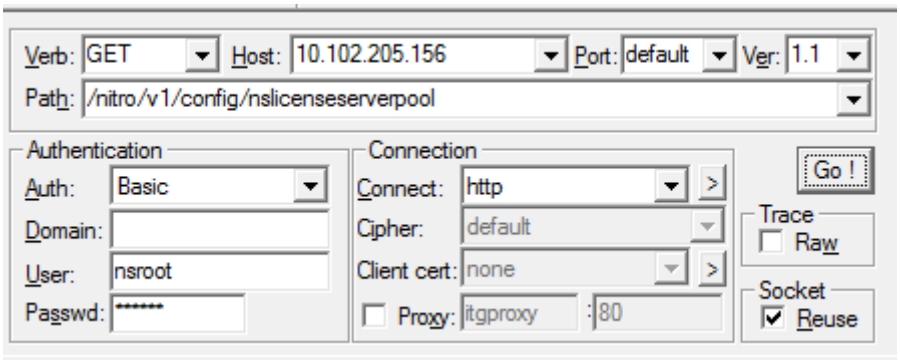
NetScaler Console responds to the request. The following sample response shows success.

```
RESPONSE: **************\n
HTTP/1.1 201 Created\r\n
Date: Fri, 06 Jan 2017 19:03:21 GMT\r\n
Server: Apache\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Content-Length: 57\r\n
Content-Type: application/json; charset=utf-8\r\n
\r\n
{ "errorcode": 0, "message": "Done", "severity": "NONE" }
finished.
```

To view the available licenses on the licensing server:

1. Set the request type to **Get**.
2. Set the path to /nitro/v1/config/nslicenseserverpool

© 1997–2025 Citrix Systems, Inc. All rights reserved.



NetScaler Console responds to the request. The following sample response shows success, and the list of available licenses on the license server.

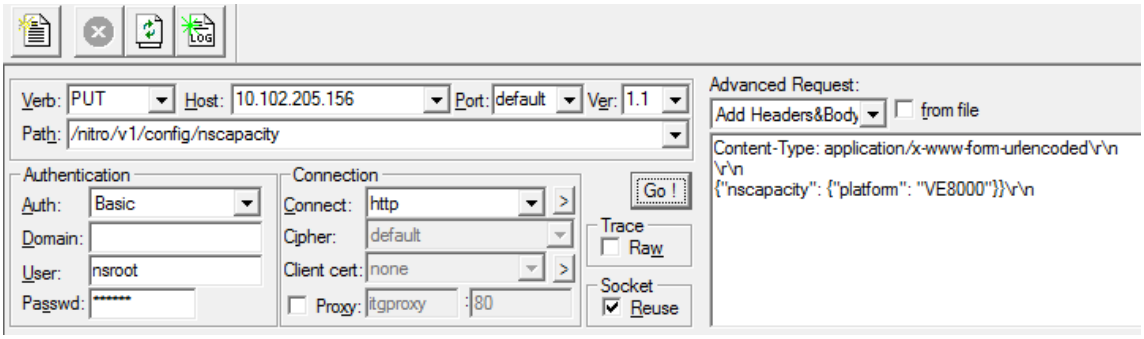
RESPONSE: **********\n
HTTP/1.1 200 OK\r\n
Date: Fri, 06 Jan 2017 19:18:54 GMT\r\n
Server: Apache\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Content-Length: 1874\r\n
Content-Type: application/json; charset=utf-8\r\n
\r\n
{ "errorcode": 0, "message": "Done", "severity": "NONE", "nslicenseserverpool": { "instancetotal": 0, "instanceavailable": 0, "standardbandwidthtotal":
0, "standardbandwidthavailable": 0, "enterprisebandwidthtotal": 0, "enterprisebandwidthavailable": 0, "platinumbandwidthtotal": 0, "platinumbandwidthav
ailable": 0, "cpxinstancetotal": 0, "cpxinstanceavailable": 0, "vpx1stotal": 0, "vpx1savailable": 0, "vpx1ptotal": 0, "vpx1pavailable": 0, "vpx5stotal"
: 0, "vpx5savailable": 0, "vpx5ptotal": 0, "vpx5pavailable": 0, "vpx10stotal": 0, "vpx10savailable": 0, "vpx10etotal": 0, "vpx10eavailable": 0, "vpx10p
total": 0, "vpx10pavailable": 0, "vpx25stotal": 0, "vpx25savailable": 0, "vpx25etotal": 0, "vpx25eavailable": 0, "vpx25ptotal": 0, "vpx25pavailable": 0
, "vpx50stotal": 0, "vpx50savailable": 0, "vpx50etotal": 0, "vpx50eavailable": 0, "vpx50ptotal": 0, "vpx50pavailable": 0, "vpx100stotal": 0, "vpx100sav
ailable": 0, "vpx100etotal": 0, "vpx100eavailable": 0, "vpx100ptotal": 0, "vpx100pavailable": 0, "vpx200stotal": 0, "vpx200savailable": 0, "vpx200etota
l": 0, "vpx200eavailable": 0, "vpx200ptotal": 0, "vpx200pavailable": 0, "vpx500stotal": 0, "vpx500savailable": 0, "vpx500eto
tal": 0, "vpx500eavailable": 0, "vpx500ptotal": 0, "vpx500pavailable": 0, "vpx1000stotal": 0, "vpx1000savailable": 0, "vpx1000etotal": 0, "vpx1000eavail
able": 0, "vpx1000ptotal": 0, "vpx1000pavailable": 0, "vpx2000ptotal": 0, "vpx2000pavailable": 0, "vpx3000stotal": 0, "vpx3000savailable": 0, "vpx3000e
total": 0, "vpx3000eavailable": 0, "vpx3000ptotal": 0, "vpx3000pavailable": 0, "vpx4000ptotal": 0, "vpx4000pavailable": 0, "vpx5000stotal": 0, "vpx5000
savailable": 0, "vpx5000etotal": 0, "vpx5000eavailable": 0, "vpx5000ptotal": 0, "vpx5000pavailable": 0, "vpx8000stotal": 1, "vpx8000savailable": 1, "vp
x8000etotal": 2, "vpx8000eavailable": 1, "vpx8000ptotal": 1, "vpx8000pavailable": 1 } }
finished.

To assign a license to NetScaler:

1. Set the request type to **Post**.
2. Set the path to /nitro/v1/config/nscapacity.
3. Set the payload as follows:

```
content-type: application/x-www-form-urlencoded\\r\\n
\\r\\n
{
  " nscapacity:{
  " platform " : " VE8000 "  }
   }
 \\r\\n
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.



NetScaler Console responds to the request. The following sample response shows success.

```
RESPONSE: **************\n
HTTP/1.1 200 OK\r\n
Date: Fri, 06 Jan 2017 19:16:21 GMT\r\n
Server: Apache\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Content-Length: 57\r\n
Content-Type: application/json; charset=utf-8\r\n
\r\n
{ "errorcode": 0, "message": "Done", "severity": "NONE" }
finished.
```

Update a licensing server IP address

You can update the licensing server IP address in NetScaler VPX and NetScaler BLX instances, without any impact on the allocated license bandwidth on the instance and data loss.

Update using the CLI: To update the licensing server IP address using the CLI, type the following command on the instance:

```
add licenseserver <licensing server IP address> -forceUpdateIP
```

This command connects to the new server and releases the resources associated with the previous licensing server.

Update using the GUI: To update the licensing server IP address using the GUI, navigate to **System > Licenses > Manage Licenses**, click **Add New License** For more information, see Allocate NetScaler VPX and NetScaler BLX Licenses to an NetScaler instance by using the NetScaler GUI.

Configure Expiry Checks for NetScaler VPX and NetScaler BLX Check-In and Check-Out Licenses

You can now configure the license expiry threshold for NetScaler VPX and NetScaler BLX licenses. By setting thresholds, NetScaler Console sends notifications via email or SMS when a license is due to

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

To configure license expiry checks:

1. Navigate to **Infrastructure > Pooled Licensing**.
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.
3. In the **Notification Settings** section, click the **Edit** icon and specify the alert threshold. You can set a percentage of Pooled license capacity to be used to notify administrators.
4. Choose the type of notification that you want to send by selecting the appropriate checkbox. The notification types are as follows:
   a) **Email Profile**: Specify a mail server and profile details. An email is triggered when your licenses are about to expire.
   b) **SMS Profile**: Specify a Short Message Service (SMS) server and profile details. An SMS message is triggered when your licenses are about to expire.
5. Then, specify when you want to send the notification in terms of the number of days before license expiry.
6. Click **Save**.

NetScaler virtual CPU licensing

October 3, 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> after April 15, 2026, supporting NetScaler Flexed licenses (CPL/UHMC), legacy NetScaler Pooled licenses, and NetScaler Fixed term Bandwidth licenses. To remain supported, your NetScaler and NetScaler Console deployments must be on a LAS compatible version.
>
> The minimum required NetScaler® versions that are LAS compatible are:
>
> - NetScaler ADCs: 14.1-51.80, 13.1-60.29, 13.1-37.247 (FIPS)
> - NetScaler SVM: 14.1-51.83, 13.1-60.30
> - NetScaler Console Service: Supported from early September 2025.
> - NetScaler Console on-prem: 14.1-51.83
>
> **Note:** LAS support for Console on-prem is from release 14.1-51.83 onwards. However, file-based licensing is deprecated from Console on-prem releases 14.1-51.83 onwards and 13.1-60.26 onwards, and goes EOL on April 15th, 2026. That is, even if you upgrade to Console on-prem release 14.1-51.83 or release 13.1-60.26 or later, you can continue using file-based licensing. However you must upgrade to Console on-prem release 14.1-51.83 or later, and switch to LAS before 15th April 2026 because file-based licensing reaches EOL.
>
> All the other forms of legacy NetScaler licenses such as Pooled vCPU, CICO, perpetual will not be supported with LAS. NetScaler instances leveraging perpetual licenses without an active maintenance will become unlicensed upon upgrade to the above mentioned software versions.
>
> LAS-based licenses may not be available to customers where prohibited by law or regulations.
>
> If you have questions or concerns, contact Customer Care. Citrix may limit or suspend your Citrix Maintenance for non-compliance with these requirements without liability in addition to any other remedies Citrix may have at law or equity. These requirements don't apply where prohibited by law or regulation.

Read the following note before proceeding further.

> **Note:**
>
> vCPU license is no longer available for purchase. For more information, see Licensing.

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 function virtualization (NFV)
- Network virtualization (NV)
- Micro-services

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Such a movement also needs the software requirements to be dynamic, flexible, and agile to meet the ever-changing business needs. Licenses are also expected to be managed by a central management tool with full visibility into the usage.

Virtual CPU licensing for NetScaler VPX

Earlier, NetScaler VPX licenses were allocated based on the bandwidth consumption by the instances. A NetScaler VPX is restricted to use a specific bandwidth and other performance metrics based on the license edition that it is bound to. To increase the available bandwidth, you must upgrade to a license edition that provides more bandwidth. In certain scenarios, the bandwidth requirement might be less, but the requirement is more for other L7 performance such as SSL TPS and compression throughput. 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 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, 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.

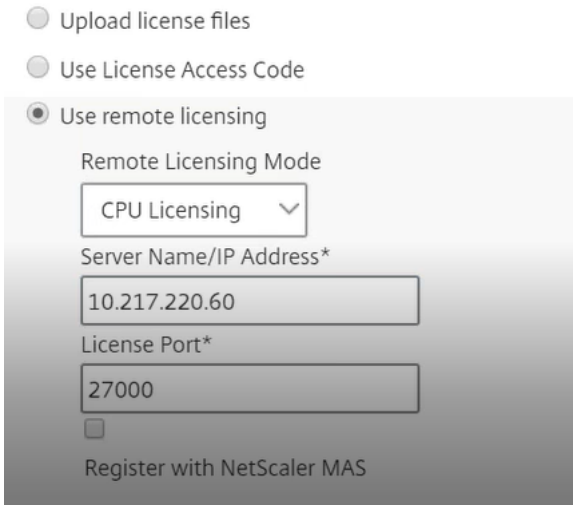
Similar to Pooled license capacity and CICO licensing functionalities, the NetScaler Console license server manages a separate set of virtual CPU licenses. Here also, the three editions managed for virtual CPU licenses are Standard, Advanced, and Premium. These editions unlock the same set of features 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 NetScaler VPX after checking out the licenses.

To configure licensing server in NetScaler VPX using GUI:

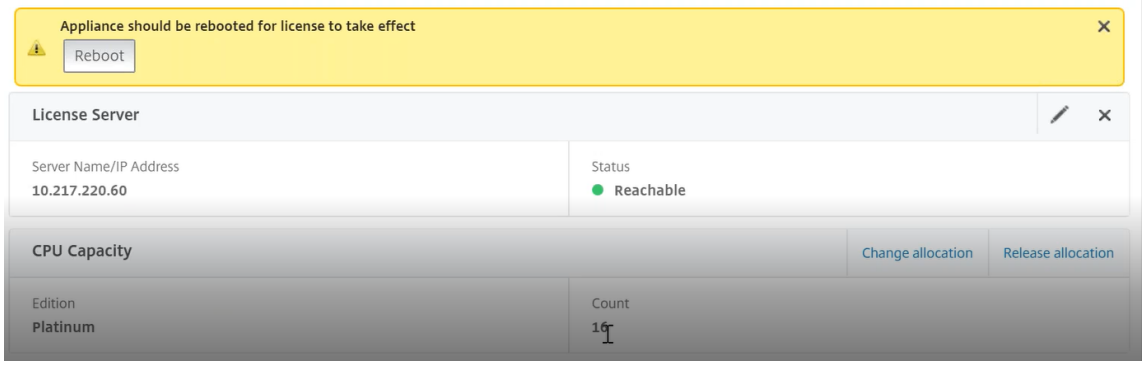
1. In NetScaler VPX, navigate to **System > Licenses** and click **Manage Licenses**.
2. On the **License** page, click **Add New License**.
3. On the **Licenses** page, select the **Use remote licensing** option.
4. Select **CPU licensing** from the **Remote Licensing Mode** list.
5. Type the IP address of the license server and the port number.
6. Click **Continue**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



> **Note**
>
> You must always register the 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**.
8. 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.

Configuring a licensing server in NetScaler VPX license using CLI

In the NetScaler VPX console, type the following commands for the following two tasks:

1. To add the licensing server to NetScaler VPX:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
add licenseserver <IP address of the license server>
```

2. To apply for the licenses:

```
set capacity -vcpu - edition premium
```

When prompted, reboot the instance by typing the following command:

```
reboot -w
```

Update a licensing server IP address

You can update the licensing server IP address in the NetScaler VPX instance, without any impact on the allocated license bandwidth on the instance and data loss. To update the licensing server IP address, type the following command on the NetScaler VPX instance:

```
add licenseserver <licensing server IP address> -forceUpdateIP
```

This command connects to the new server and releases the resources associated with the previous licensing server.

Managing virtual CPU licenses on NetScaler Console

1. In NetScaler Console, navigate to **Infrastructure > Pooled Licensing > Pooled VCPU**.
2. The page displays the licenses allocated for each type of license edition.
3. Click the number within each donut to view the NetScaler instances that are using this license.



Virtual CPU licensing for NetScaler CPX

While provisioning the NetScaler CPX instance, you can configure the NetScaler CPX instance to check out licenses from the license server depending on the CPU usage on the instance.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

NetScaler CPX relies on the license server, running on NetScaler Console, to manage the licenses. NetScaler CPX checks out the licenses from the license server when it is starting up. The licenses are checked in back to the license server when NetScaler CPX shuts down.

You can download the NetScaler CPX image from the Quay container registry using the 'docker pull' command and deploy it on your environment.

There are three license types available for NetScaler CPX licensing:

1. Virtual CPU subscription licenses supported for NetScaler CPX and VPX
2. Pooled Capacity licenses
3. CP1000 licenses that support single to multiple vCPUs for NetScaler CPX only

To configure vCPU subscription licenses while provisioning the NetScaler CPX instance:

Specify the number of vCPU licenses that the NetScaler CPX instance uses.

- This value is entered as an environment variable through Docker, Kubernetes, or Mesos/-Marathon.
- The target variable is "CPX_CORES."NetScaler CPX can support from 1 to 16 cores.

To specify 2 cores, you can perform the docker run command as follows:

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
    -e EULA=yes -e CPX_CORES=2
```

While provisioning a NetScaler CPX instance, define the NetScaler licensing server as an environmental variable in the **docker run** command as shown below:

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
    -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
    LS_PORT> cpx:11.1
```

Where,

- *<LS_IP_ADDRESS>* is the IP address of the NetScaler licensing server.
- *<LS_PORT>* is the port of the NetScaler licensing server. By default, the port is 27000.

> **Note**
>
> By default, the NetScaler CPX instance checks out the license from the vCPU subscription pool. The NetScaler CPX instance checks out an "n"number of licenses if the instance is running with "n"CPUs.

To configure NetScaler Pooled capacity or CP1000 licenses while provisioning the NetScaler CPX instance:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

If you want to check out the license for the NetScaler CPX instance using the Pooled licensing (bandwidth-based) or the NetScaler CPX private pool (CP1000 or private-pool-based), you must provide the environment variables accordingly.

For example,

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
    -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
    LS_PORT> -e PLATFORM=CP1000 cpx:11.1
```

CP1000. This command triggers the checkout from CP1000 pool (NetScaler CPX private pool). The NetScaler CPX instance then retrieves “n”number of instances for “n”number of cores specified for CPX_CORES. The most common use case is to specify n = 1 for a checkout of a single instance. Multi-core NetScaler CPX use cases check out “n”vCPUs (where “n”is from 1 to 7).

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
    -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
    LS_PORT> -e BANDWIDTH=2000 cpx:11.1
```

Pooled capacity. This command checks out one license from the instance pool and consumes 1000 Mbps of bandwidth from the Premium bandwidth pool yet enables NetScaler CPX to run up to 2000 Mbps. In Pooled licensing, the first 1000 Mbps is not charged.

> **Note**
>
> Specify the corresponding number of vCPUs for the desired target bandwidth when checking out from the bandwidth pool as detailed in the following table:

Number of cores (vCPU)	Maximum bandwidth
1	1000 Mbps
2	2000 Mbps
3	3500 Mbps
4	5000 Mbps
5	6500 Mbps
6	8000 Mbps
7	9300 Mbps

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Expected behaviors when issues arise

October 3, 2025

Following are the expected behaviors of the license servers and NetScaler instances when they experience the issues described:

License server stops responding

> **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: 14.1-51.80, 13.1-60.29, 13.1-37.247 (FIPS)
> - NetScaler SVM: 14.1-51.83, 13.1-60.30
> - NetScaler Console Service: Supported from early September 2025.
> - NetScaler Console on-prem: 14.1-51.83
>
> **Note:** LAS support for Console on-prem is from release 14.1-51.83 onwards. However, file-based licensing is deprecated from Console on-prem releases 14.1-51.83 onwards and 13.1-60.26 onwards, and goes EOL on April 15th, 2026. That is, even if you upgrade to Console on-prem release 14.1-51.83 or release 13.1-60.26 or later, you can continue using file-based licensing. However you must upgrade to Console on-prem release 14.1-51.83 or later, and switch to LAS before 15th April 2026 because file-based licensing reaches EOL.
>
> 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.

Read the following note before proceeding further.

> **Warning**
>
> The license server is not responding. NetScaler continues to operate with the current capacity for 30 days. After 30 days, if the connectivity to the license server is not restored, NetScaler loses its current capacity and stops processing traffic. If connectivity is restored within 30 days, NetScaler continues to operate at current capacity and continues to process traffic.

NetScaler Pooled instance stops responding

If the NetScaler Pooled instance stops responding and the license server is in a healthy state, the license server checks in all the NetScaler instance's licenses after 10 minutes. When the instance reboots, it sends a request to check out all the licenses from the licensing server.

Both license server and NetScaler Pooled instance stop responding

If both the license server and the NetScaler Pooled instance restart and reestablish the connection, the license server checks-in all its licenses after 10 minutes, and the NetScaler Pooled instances automatically checkout the licenses after the reboot is completed.

The NetScaler Pooled instance shuts down gracefully

During a graceful shutdown, you can choose to check-in the licenses or keep the licenses that were allocated before the graceful shutdown. If you choose to check-in the licenses, the NetScaler Pooled instance is unlicensed after it restarts. If you choose to keep the licenses, they are checked in to the licensing server when the instance shuts down. After the instance restarts, it reestablishes the connection with the licensing server and checks out the licenses as specified in the saved configuration.

If the system reboots and the checkout fails due to no capacity available in the pool, NetScaler checks the inventory of NetScaler Console pool licenses and checks out any available capacity. An SNMP alarm is raised to notify this condition to the user if NetScaler is not running at full capacity as per the configuration. If no capacity is available in the bandwidth pool, the pool instance becomes unlicensed.

Network connectivity issues

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Error message (syslog)**
>
> License server is not responding.

If the license server and NetScaler Pooled instances are in a healthy state but the network connectivity is lost, the instances continue to operate at their current capacity for 30 days. After 30 days, if the connectivity to the license server is not restored, the instances lose their capacity and stop processing traffic, and the license server checks-in all its licenses. After the license server reestablishes connectivity with the NetScaler instances, the instances checkout the licenses again.

Grace period

When a NetScaler Pooled instance is in a healthy state and the license server stops responding, the instance continues to operate with the current capacity for 30 days. If the connectivity to the license server is not restored after 30 days, the instance loses its capacity and stops processing traffic.

Manage system settings

September 27, 2025

The following table describes the list of options available under **Settings** > **Administration**:

Network Configurations

Network Configurations	Options	Description
IP Address, Second NIC, Host Name and Proxy Server	IP address	Displays the NetScaler Console network configuration IP address details that are used to deploy NetScaler Console
	Second NIC	Enables you to configure a second NIC to isolate NetScaler Console management access. For more information, see Configure a dual NIC to access NetScaler Console

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Network Configurations	Options	Description
	Host name	Enables you to assign a host name to NetScaler Console. For more information, see Assign a host name to a NetScaler Console server
	Proxy Server	Enables you to configure NetScaler Console as a proxy server. For more information, see NetScaler Console as an API proxy server
Static Routes		Enables you to configure static routes to establish connection between NetScaler Console and NetScaler VPX instances
NTP Servers		Ensures NetScaler Console clock has the same date and time settings as the other servers on the network. For more information, see Configure NTP server
NetScaler Console Ports Information		Enables you to understand which port must be open for communication between NetScaler Console and NetScaler instances. For more information, see Supported Ports

System Configurations

System Configurations	Options	Description
System, Time zone, Allowed URLs and Message of the day	Basic Settings	Enables you to modify system settings such as enable `nsrecover` login, enable session timeout, and so on

© 1997–2025 Citrix Systems, Inc. All rights reserved.

System Configurations	Options	Description
	Time Zone	Enables you to modify the timezone to be used in NetScaler Console. The default timezone is UTC
	Allowed URL List	Enables you to configure URLs to send uninterrupted requests to NetScaler Console. You can configure it with the value "none"if no URL to be added
	Message of the day	Enables you to create a welcome message in NetScaler Console. You can use this feature to set reminder messages for yourself or the user who logs on to NetScaler Console. Click **Enable Message**, type the message in the message box, and click **Save**
View NetScaler Console Fingerprint		Enables you to copy the unique NetScaler Console fingerprint ID to get started with service graph
Configure Customer Identity		Enables you to protect the network resources by permitting only authenticated customers or users to access its network. For more information, see Data Governance
CUXIP Settings		If you select this check box, usage statistics are collected for the sole purpose of improving the GUI. The received data is used only by Citrix engineers and is not shared with anyone

© 1997–2025 Citrix Systems, Inc. All rights reserved.

System Maintenance

System Maintenance	Description
Upgrade NetScaler Console	Enables you to upgrade the NetScaler Console through GUI. For more information, see Upgrade
Reboot NetScaler Console	Enables you to reboot NetScaler Console
Shut Down NetScaler Console	Enables you to shut down NetScaler Console
Disaster Recovery	Enables you to view disaster recovery node information. For more information, see Configure Disaster Recovery

Data Pruning

Data Pruning	Options	Description
System and Instance Data Pruning	System	Enables you to limit the amount of reporting data being stored in NetScaler Console server database. For more information, see Configure system prune settings
	Instance Events	Enables you to limit the event messages reporting data stored in NetScaler Console
	Instance Syslog	Enables you to limit the amount of syslog data stored in the database. For more information, see Configure instance syslog prune settings
	Network Reporting	Enables you to limit the network reporting data stored in NetScaler Console

Backup

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Backup	Options	Description
Configure System and Instance backup	System	Enables you to configure the initial backup settings before doing a system backup. For more information, see System Backup Settings
	Instance	Enables you to configure settings on NetScaler Console to back up a selected NetScaler instance or multiple instances. For more information, see Configure instance backup settings

Event Notifications

Event Notifications	Options	Description
Configure Event Notification and Digest	Event Notification	You can send notifications to select groups of users for several system-related functions. These system functions are organized into event categories such as SystemReboot, StatusPoll, SystemState, and so on. You can configure NetScaler Console to send you notifications either through Email, SMS, or Slack. This ensures that you are notified of any system-level activities such as exceeding of data storage or backup failure.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

	Event Digest	Enables you to get a consolidated report of important system and feature events

SSL Settings

SSL Settings	Description
Install SSL Certificate	Enables you to install SSL certificate and SSL Key file
View SSL Certificate	Enables you to view the SSL certificate details
Configure SSL Settings	For more information, see Configure SSL settings
SSL Certificates	Enables you to upload, download, or delete an SSL certificate or SSL Key file
Cipher Groups	For more information, see Configure a Cipher Groups

Configure Features

Configure Features	Description
Disable or enable features	You can enable or disable features in NetScaler Console. For more information, see Enable or disable NetScaler Console features

Configure system backup settings

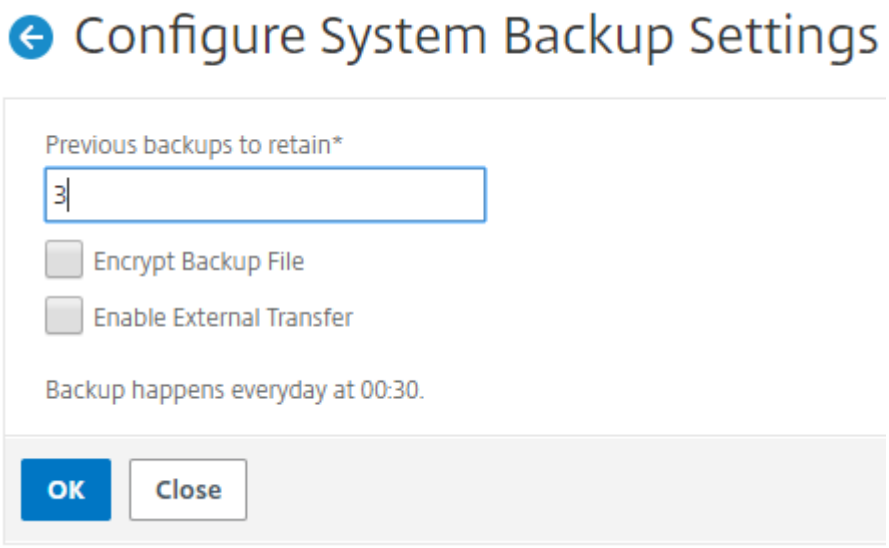
September 27, 2025

Set your initial System Backup Settings before you need to back up and restore the NetScaler Console.

1. Navigate to **Settings > Administration**. Under **Backup**, click **Configure System and Instance backup**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. On the **Backup > System** page, specify the following:
    - Previous backups to retain. You can only retain up to 10 backups.
    - Select **Encrypt Backup File** to encrypt the backup files.
    - Select **Enable External Transfer** to transfer a copy of your backup file to another system. When you want to restore the configuration, you have to first upload the file to the NetScaler Console server and then perform the restore operation. Specify the server, user name and password, port, the transfer protocol to be used, and the directory path. To learn more about external transfer, see Transfer a NetScaler Console Backup File to an External System.
3. Click **OK**.



Configure proxy server settings

October 16, 2025

NetScaler Console® allows you to configure a proxy server for outbound connectivity. You can also upload its CA certificates for NetScaler Console deployments where the SSL-inspecting proxy intercepts outbound traffic. NetScaler Console trusts the proxy's certificate only when its CA certificate is uploaded. This feature ensures that all external communication from NetScaler Console passes through a secured and controlled proxy server.

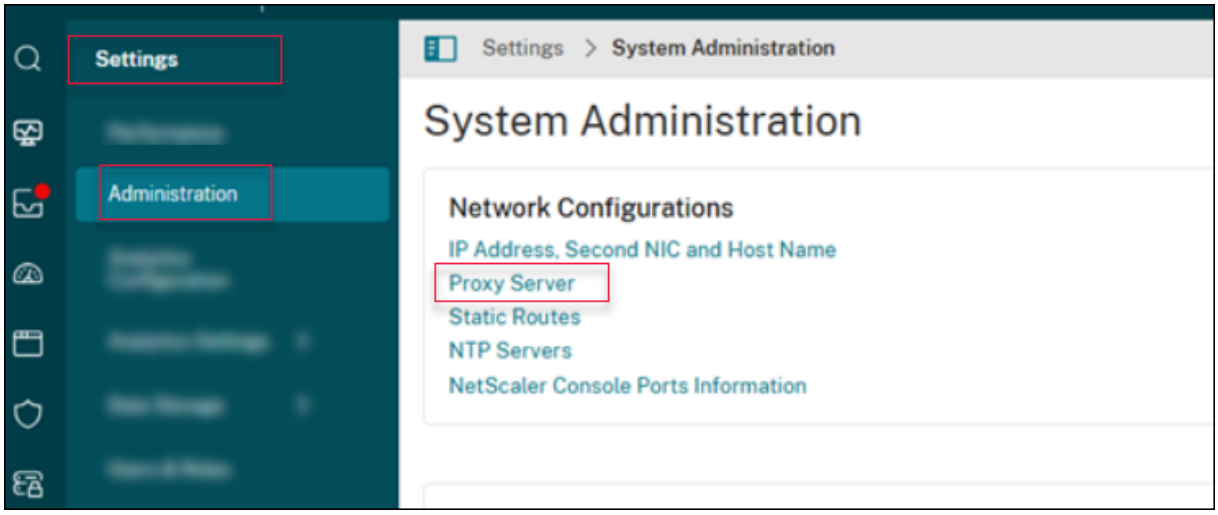
This feature provides the following benefits:

- Ensures that the communication is secure when proxies perform SSL interception.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Prevents connectivity issues for telemetry uploads and Cloud Connect communication.

To configure a proxy server, navigate to **Settings > Administration** and click **Proxy Server**.



Points to note

- Ensure that the proxy server is reachable from NetScaler Console over the specified IP/port.
- If SSL interception is enabled, import in NetScaler Console, the proxy's CA certificate to avoid connectivity failures.
- Changes to proxy configuration might impact automated telemetry upload or Cloud Connect until the new details are added.

Proxy server configuration

You can use the **Proxy Server Configuration** tab to add proxy details and credentials.

Prerequisite

- Add `adm.cloud.com` to Allow list.

To add a proxy server to route all outbound traffic, perform the following steps:

1. Navigate to **Settings > Administration** and click **Proxy Server**.
2. On the **Proxy Server Configuration** tab, select **Enable Proxy Server**.
3. Specify the **IP Address/Hostname** of the proxy server and its listening **Port**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

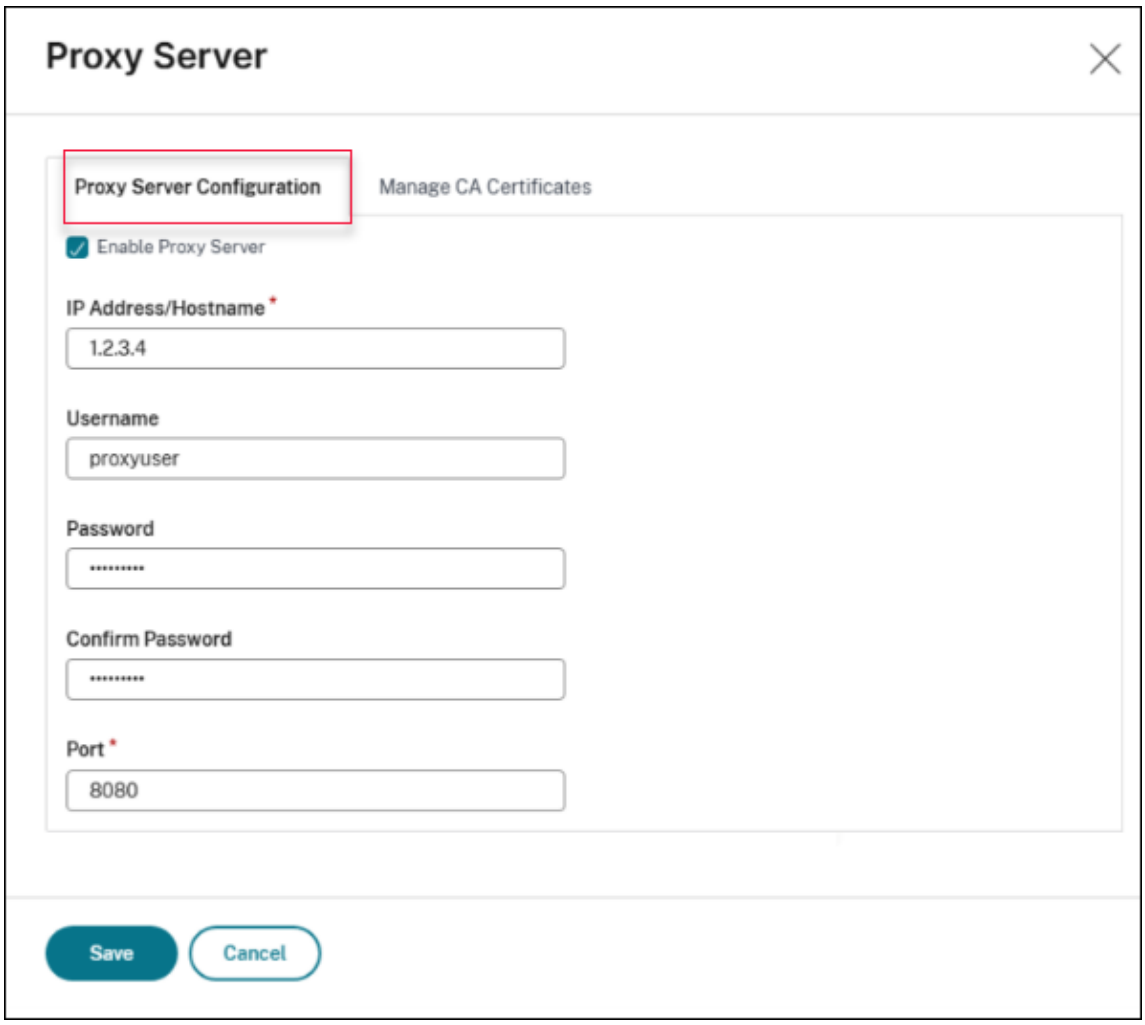
> **Note:**
>
> - Starting from 14.1 release build 56.x, NetScaler Console supports using DNS host names (FQDNs) in addition to IP addresses for proxy configuration.
> - Using host names is beneficial in environments that:
>   - Use DNS-based redundancy (for example, GSLB) to route traffic across multiple proxy servers.
>   - Have no load balancer, but rely on DNS to manage high availability and failover.
>   - Require scalable and resilient proxy configurations across data centers.
>
> The support to use DNS host names allows NetScaler Console to dynamically resolve the most appropriate proxy endpoint, improving reliability and simplifying management.

4. Provide a **Username** and the corresponding **Password** if the proxy requires credentials.

> **Note:**
>
> NetScaler Console currently supports basic authentication for proxy.

5. Click **Save**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Manage CA certificate

If the proxy server performs SSL inspection, use the **Manage CA Certificates** tab to upload the CA certificate of proxy server. You can either add or delete the certificate as per your needs.

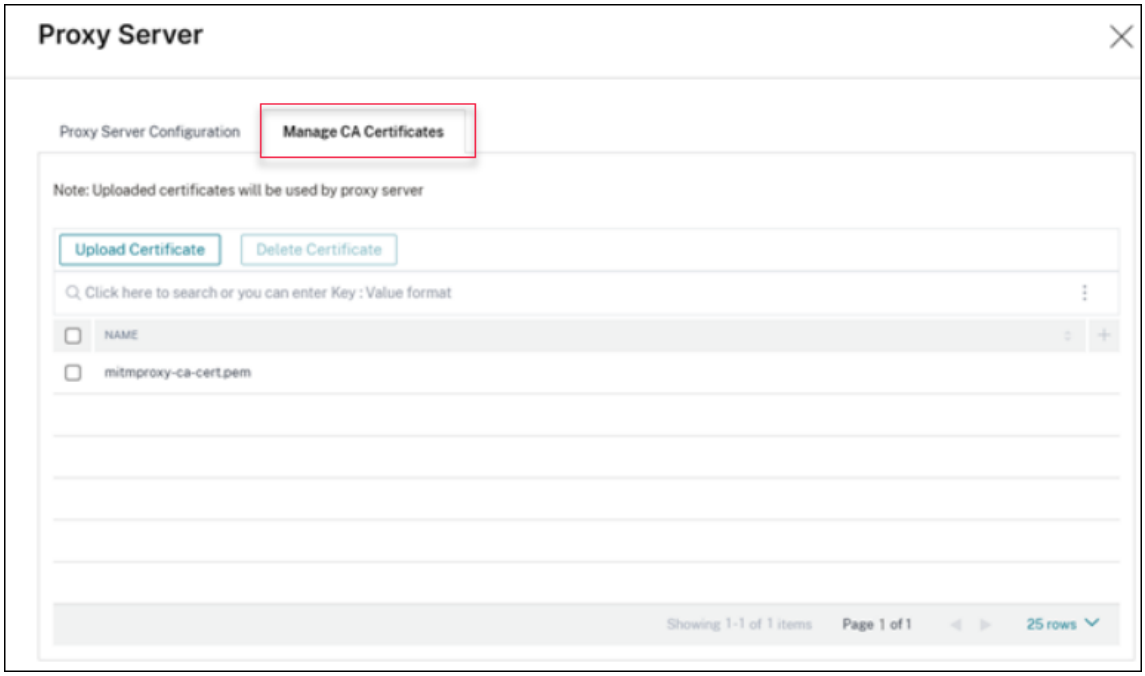
To upload the CA certificate of the proxy server, perform the following steps:

1. Navigate to **Settings > Administration** and click **Proxy Server**.
2. Click **Upload Certificate**.

To delete the CA certificate of the proxy server, perform the following steps:

1. Navigate to **Settings > Administration** and click **Proxy Server**.
2. Select the certificate to be deleted.
3. Click **Delete Certificate**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Configure an NTP server

September 27, 2025

You can configure a Network Time Protocol (NTP) server in NetScaler Console to synchronize its clock with the NTP server. Configuring an NTP server ensures that the NetScaler Console clock has the same date and time settings as the other servers on the network.

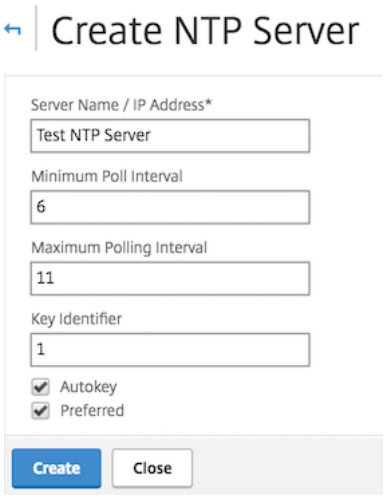
To configure an NTP server on NetScaler Console:

1. Navigate to **Settings > NTP Servers**, and then click **Add**.
2. On the **Create NTP Server** page, enter the following details:
    - **Server Name/IP Address** –Enter the domain name or IP address of the NTP server. The name or IP address cannot be changed after you have added the NTP server.
    - **Minimum Poll Interval** –Specify the minimum value for the interval between transmitted NTP messages, in seconds as a power of 2. For example, if you want the minimum poll interval to be 64 seconds, which can be expressed as 2^6, enter 6.
    - **Maximum Poll Interval** –Specify the maximum value for the interval between transmitted NTP messages, in seconds as a power of 2. For example, if you want the maximum poll interval to be 256 seconds, which can be expressed as 2^8, enter 8.
    - **Key Identifier** - Enter the key identifier that can be used for symmetric key authentication with the NTP server. Do not add a key identifier if you choose to select Autokey.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

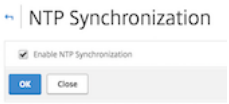
- **Autokey** - Select **Autokey** if you want to use public key authentication with the NTP server. Do not select if you want to add a key identifier.
- **Preferred** –Select this option if you want to specify this NTP server as the preferred server for clock synchronization. This applies only if more than one server is configured.

3. Click **Create**.



To enable NTP synchronization on NetScaler Console:

1. Navigate to **Settings > NTP Servers**.
2. Click **NTP Synchronization** and select the **Enable NTP Synchronization** check box.
3. Click **OK**.



> Note
>
> You can find the NTP logs messages in the /var/log directory in the file `/var/log/ntpd.log` file.

Upgrade NetScaler Console

October 16, 2025

Each NetScaler Console release offers new and updated features with increased functionality. A comprehensive list of enhancements is listed in the release notes accompanying the release announcement. Take a moment to read the release notes before you upgrade the software. It is important to understand the licensing framework and types of licenses before you start to upgrade.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Pre-upgrade checks

Before triggering an upgrade from the NetScaler Console, the system automatically performs a pre-upgrade check to validate system readiness and upgrade image integrity. This check ensures that the upgrade proceeds smoothly and reduces the likelihood of encountering failures during the upgrade process.

> **Note:**
>
> The pre-upgrade check feature is available from NetScaler Console 14.1 release build 56.x. The check runs automatically before every upgrade initiated through the NetScaler Console on-premises.

If the check detects any issues, the NetScaler Console displays detailed information about the discrepancies and prompts you to address them before continuing with the upgrade.

The pre-upgrade check includes the following validations:

- Memory availability check –Verifies that the NetScaler Console has sufficient available RAM to perform the upgrade safely.
- Disk space check –Ensures that the required free disk space is available for extracting and installing the upgrade image.
- Image file requirements check –Confirms that all mandatory image files required for the upgrade are available.
- Image file integrity check –Validates the checksum of the upgrade image to ensure that the file is complete and not corrupted.

In addition to resource and file validations, NetScaler Console verifies the health and connectivity of the system to ensure a safe upgrade. The verification includes the following checks:

- Database integrity check –Detects missing or corrupted database files to prevent upgrade failures.
- Database streaming channel status –Confirms that the streaming channel is active and operational.
- Secondary node connectivity –Ensures proper communication with the secondary node for redundancy.
- Password-less SSH verification –Confirms that password-less SSH login to the secondary node is working.

The pre-upgrade check feature provides the following benefits:

- Performing these validations before the upgrade helps prevent failures caused by insufficient resources or corrupted image files.
- By identifying potential issues in advance, the pre-upgrade check improves upgrade reliability and minimizes downtime due to recovery or reinstallation efforts.

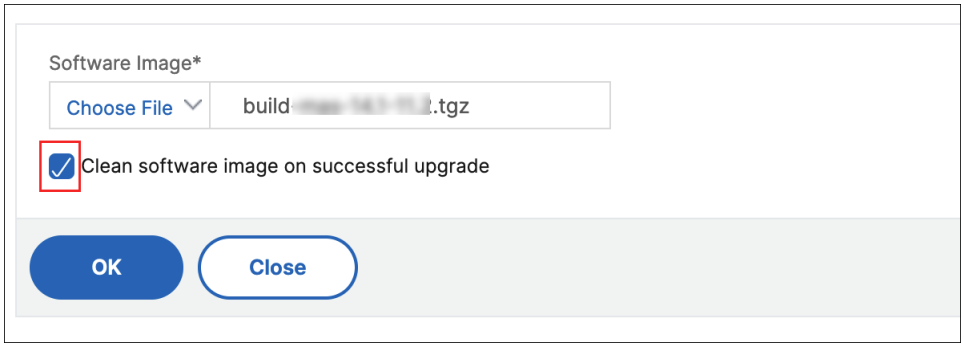
© 1997–2025 Citrix Systems, Inc. All rights reserved.

To upgrade NetScaler Console:

1. Navigate to **Settings > Administration**. Under **System Maintenance**, click **Upgrade NetScaler Console**.
2. On the Upgrade NetScaler Console page, upload a new image file by selecting either **Local** (your local computer) or **Appliance**.

   > **Note**
   >
   > When you select **Appliance**, ensure that the upgrade image is available at `/var/mps/mps_images` in NetScaler Console.

   By default, the software image is cleaned up after a successful upgrade.
3. Click **OK**.



How to reset the password for NetScaler Console

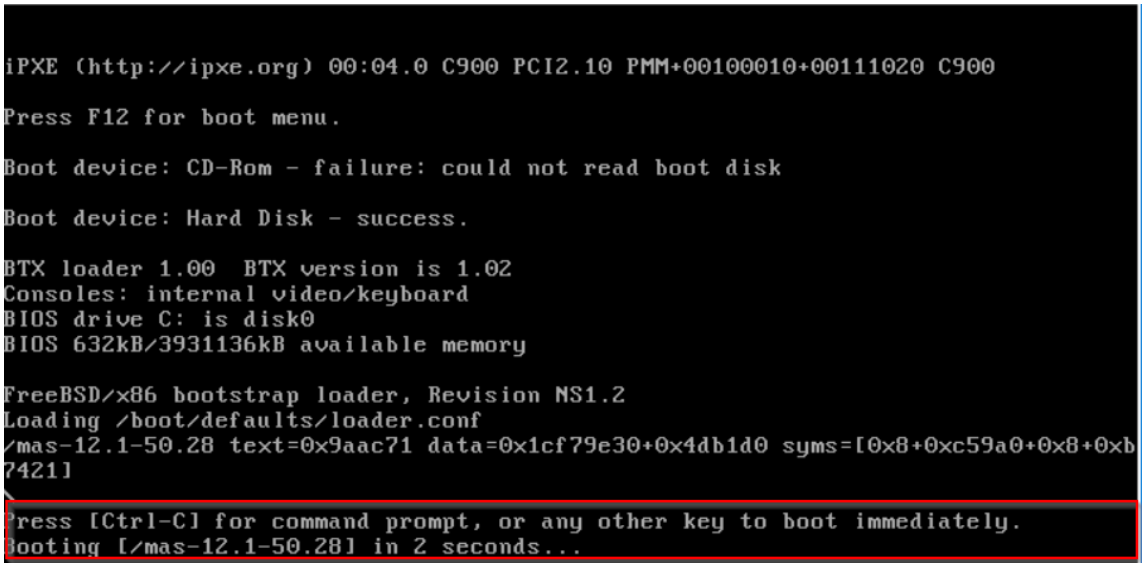
September 27, 2025

The procedure to reset the password for NetScaler Console might differ on hypervisors where it is hosted. If you have changed your default password and want to reset to default password, you can reset the password by rebooting the NetScaler Console node.

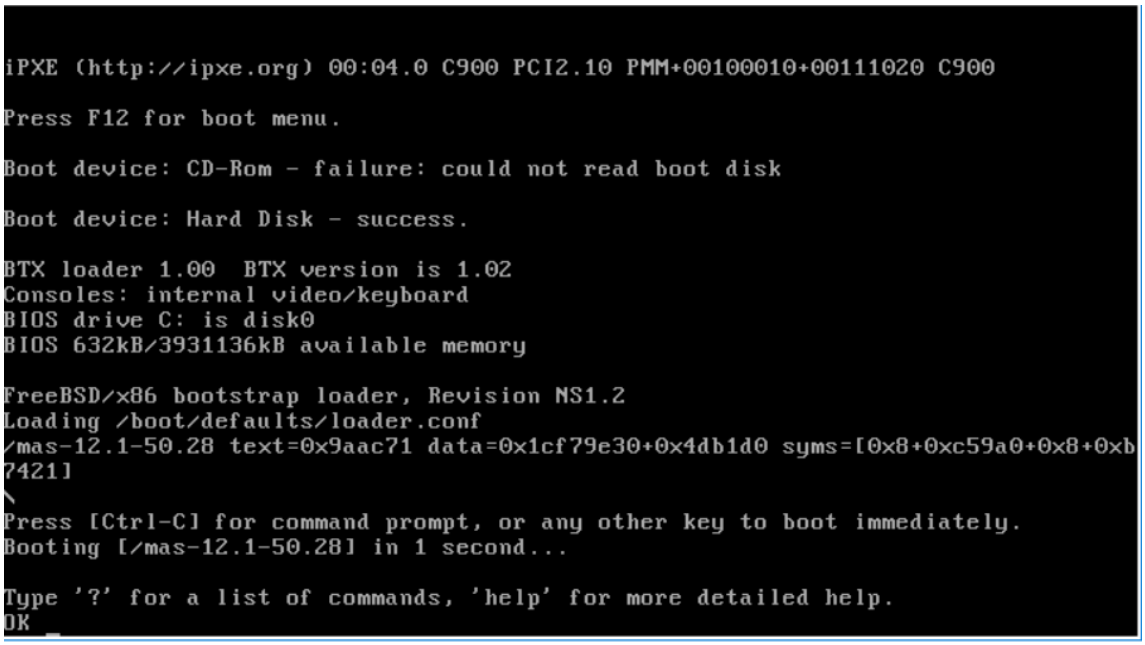
Citrix Hypervisor™ using XenCenter:

1. Log on to Citrix Hypervisor using XenCenter.
2. Select the NetScaler Console node, right-click, and select **Reboot**.
3. On the **Console** tab, press **CTL + C** to interrupt the boot sequence.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

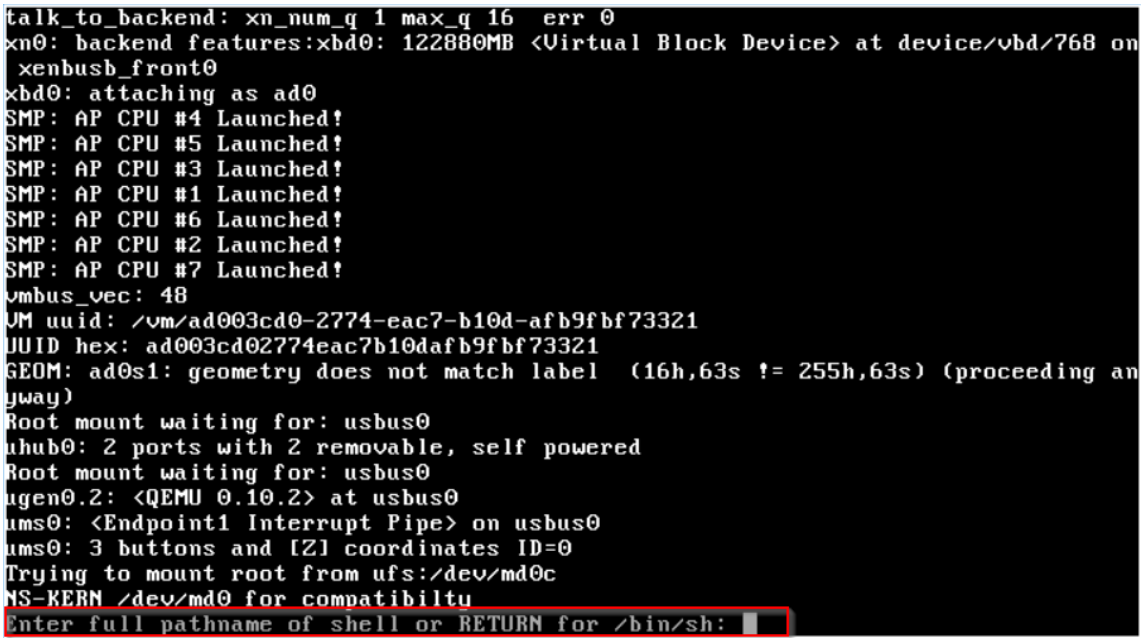


4. Run **boot -s** command at the OK prompt.

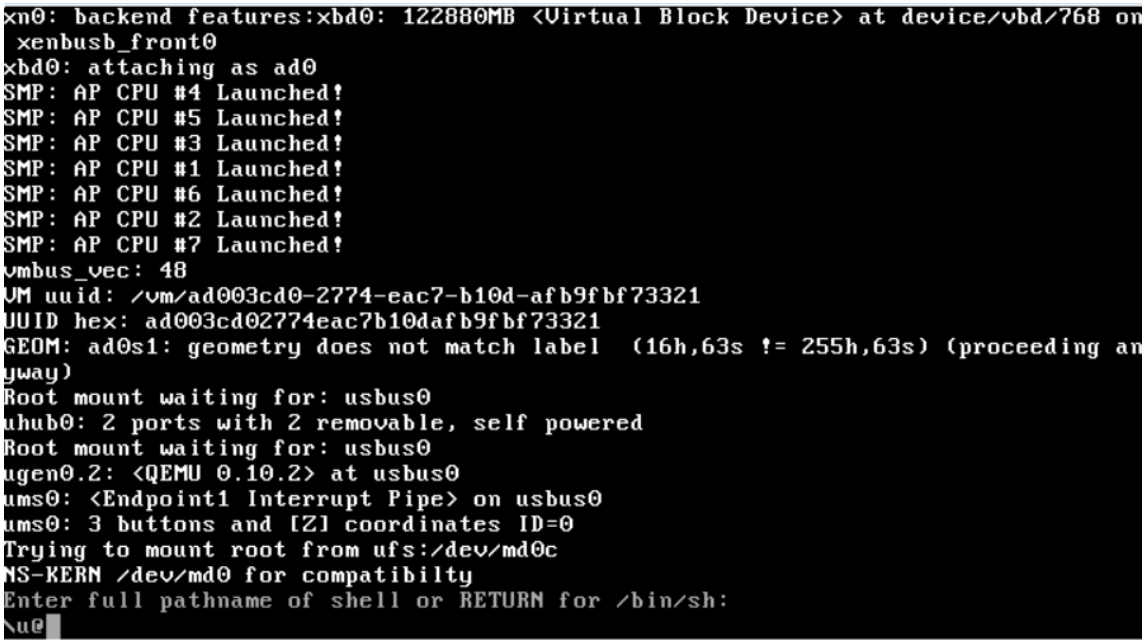


NetScaler Console reboots and displays the following message:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



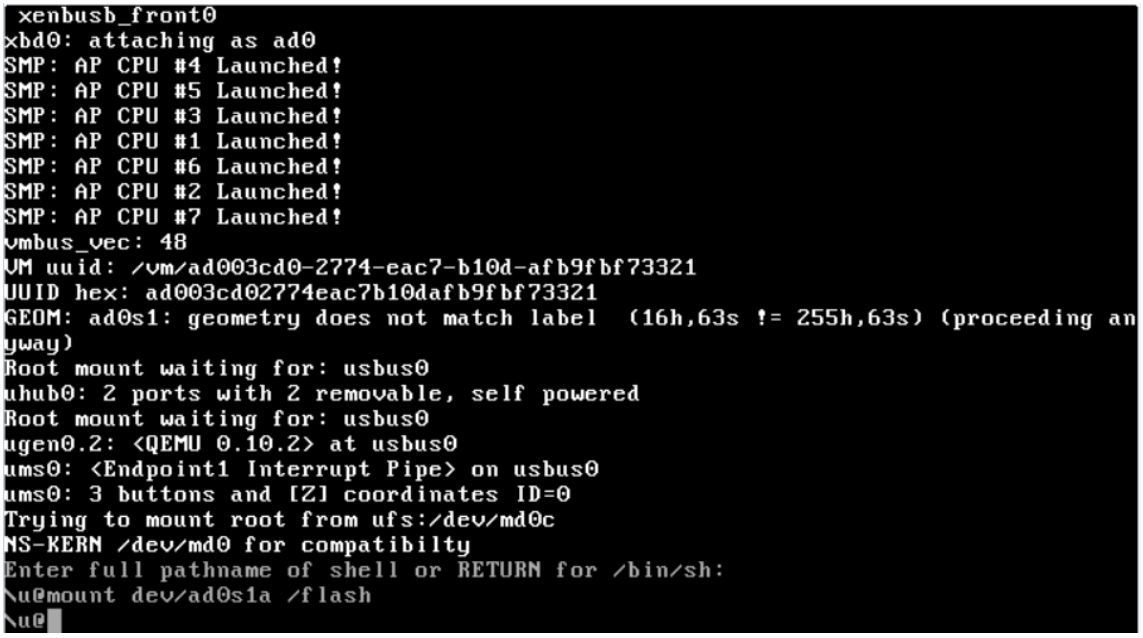
5. Press **Enter** to get the /u@ prompt.



6. Mount the flash partition using the following command:

```
mount /dev/ada0s1a /flash
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

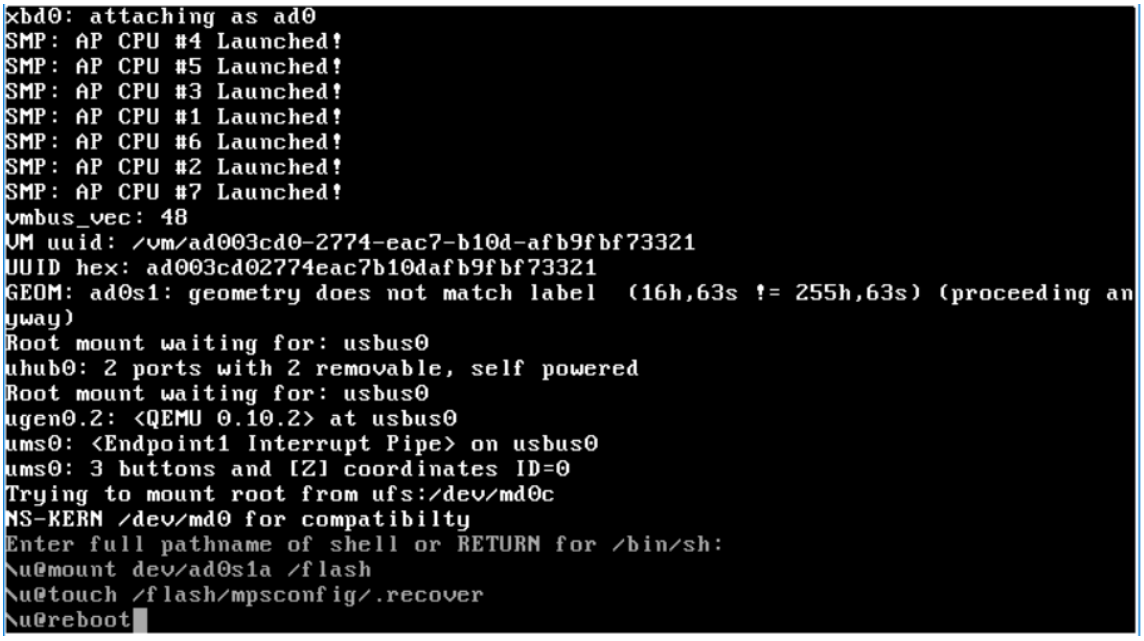


7. Create a file using the following command:

   ```
   touch /flash/mpsconfig/.recover
   ```

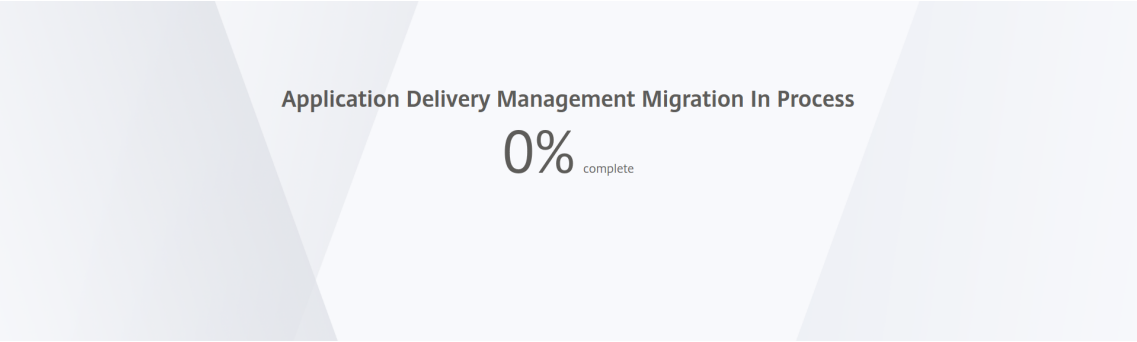
   The password is now reset to default password.

8. Run the **Reboot** command to reboot NetScaler Console.



9. Access the NetScaler Console GUI and wait until the reboot is complete.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

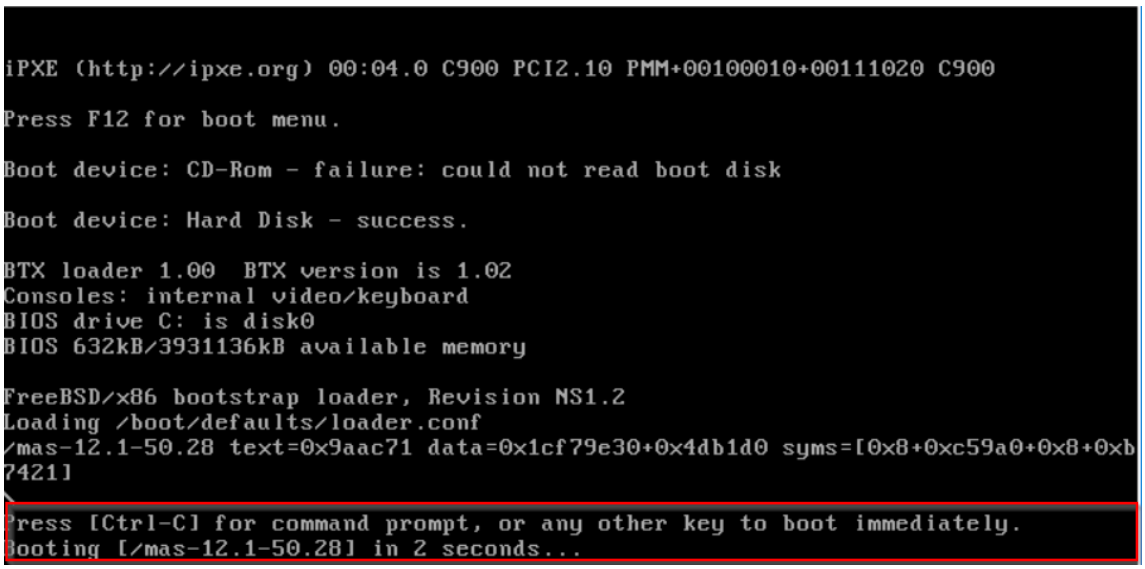


You can now use *nsroot/nsroot* credentials to log on from GUI and *nsrecover/nsroot* to log on from hypervisor.

> Note
>
> After you reboot, if the password has not reset to default password, repeat the same procedure (step 1 to step 7). Then, run the following commands and reboot NetScaler Console:
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm –rf /etc/passwd`

Esx using vSphere:

1. Log on to ESX using vSphere.
2. Select the NetScaler Console node, right-click, and then select **Reboot**.
3. On the **Console** tab, press **CTL + C** to interrupt the boot sequence.



4. Run **boot -s** command in the OK prompt.

   The NetScaler Console reboots.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

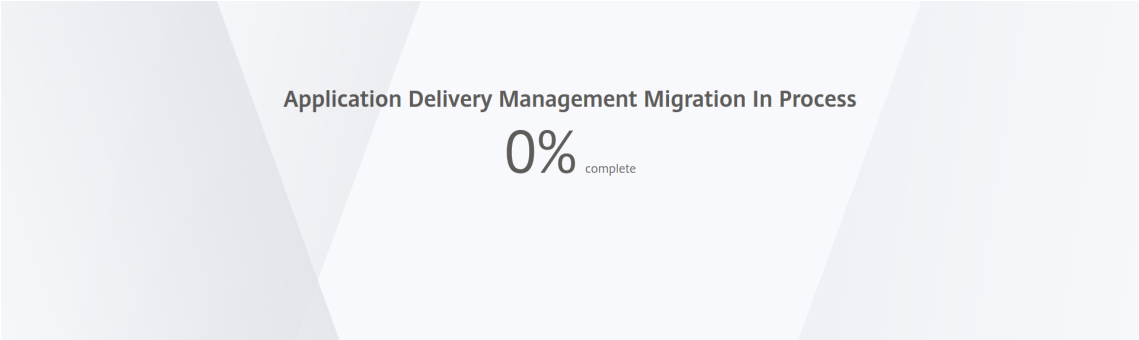
5. Press **Enter** to get the /u@ prompt.
6. Mount the flash partition using the following command:

   ```
   mount dev/da0s1a /flash
   ```

7. Create a file using the following command:

   ```
   touch /flash/mpsconfig/.recover
   ```

   The password is now reset to default password.
8. Run the **Reboot** command to reboot NetScaler Console.
9. Access the NetScaler Console GUI and wait until the reboot is complete.



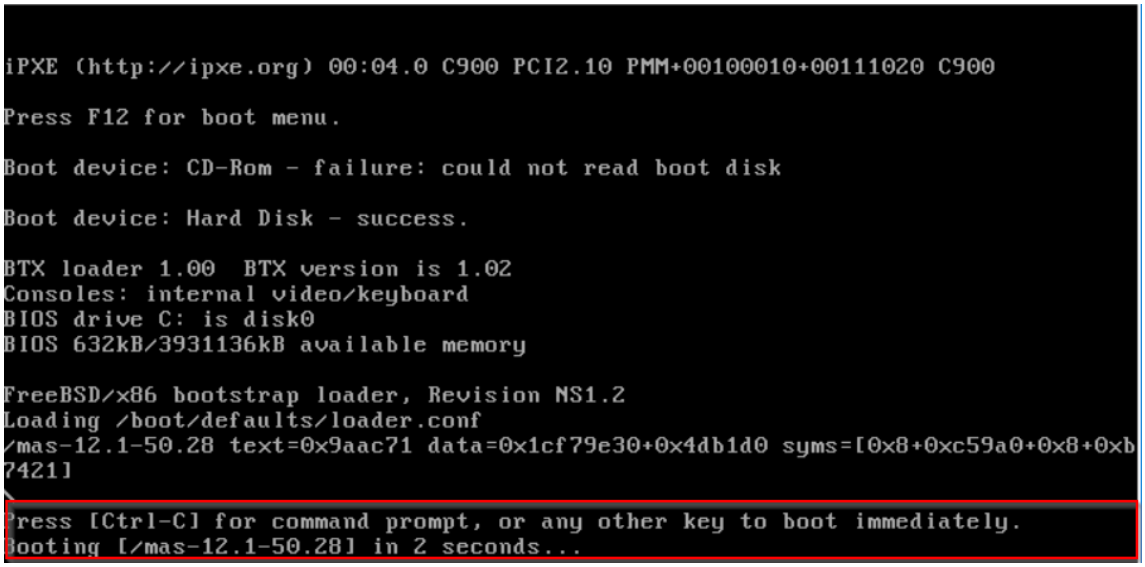
You can now use *nsroot/nsroot* credentials to log on from GUI and *nsrecover/nsroot* to log on from ESX server.

> Note
>
> After you reboot, if the password has not reset to default password, repeat the same procedure (step 1 to step 7). Then, run the following commands and reboot NetScaler Console:
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm –rf /etc/passwd`

Hyper-v using Hyper-v manager:

1. Log on to hyper-v using hyper-v manager.
2. Select the NetScaler Console node, right-click, and then select **Reboot**.
3. On the **Console** tab, press **CTL + C** to interrupt the boot sequence.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



4. Run the **boot -s** command at the OK prompt.

   The NetScaler Console reboots.

5. Press **Enter** to get the /u@ prompt.
6. Mount the flash partition using the following command:

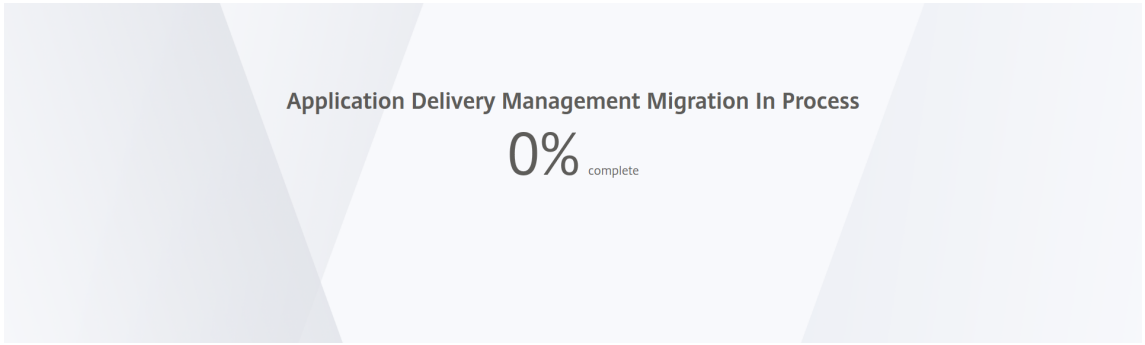
   ```
   mount dev/ad0s1a /flash
   ```

7. Create a file using the following command:

   ```
   touch /flash/mpsconfig/.recover
   ```

   The password is now reset to default password.

8. Run the **Reboot** command to reboot NetScaler Console.
9. Access the NetScaler Console GUI and wait until the reboot is complete.



You can now use *nsroot/nsroot* credentials to log on from GUI and *nsrecover/nsroot* to log on from hyper-v manager.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> Note
>
> After you reboot, if the password has not reset to default password, repeat the same procedure (step 1 to step 7). Then, run the following commands and reboot NetScaler Console:
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm –rf /etc/passwd`

Linux KVM server (SSH to KVM Server by using any SSH client):

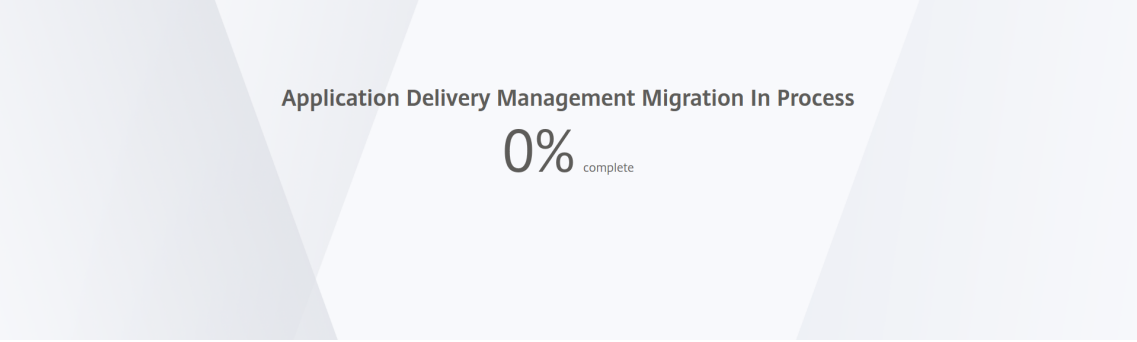
1. Log on to NetScaler Console using an SSH client to the KVM server.
2. Reboot NetScaler Console.
3. Press **CTL + C** to interrupt the boot sequence shortly after the **Loading /boot/defaults/loader.conf** message is displayed.
4. At the OK prompt, run the following command:

   ```
   set console='comconsole,vidconsole'
   ```
5. Run the **boot -s** command to reboot NetScaler Console.
6. After the **Enter full path of shell or RETURN for /bin/sh:** message is displayed, press **Enter** to get the /u@ prompt.
7. Mount the flash partition using the following command:

   ```
   mount dev/vtbd0s1a /flash
   ```
8. Create a file using the following command:

   ```
   touch /flash/mpsconfig/.recover
   ```

   The password is now reset to default password.
9. Run the **Reboot** command to reboot NetScaler Console.
10. Access the NetScaler Console GUI and wait until the reboot is complete.



You can now use *nsroot/nsroot* credentials to log on from GUI and *nsrecover/nsroot* to log on from the SSH console.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> Note
>
> After you reboot, if the password has not reset to default password, repeat the same procedure (step 1 to step 7). Then, run the following commands and reboot NetScaler Console:
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm –rf /etc/passwd`

Configure a secondary NIC to access NetScaler Console

September 27, 2025

You can configure a second NIC for isolating management access to NetScaler Console. Using this second NIC feature, depending upon your requirement, you can choose how you want to isolate the traffic that is received and sent through the NetScaler Console.

Consider a scenario in which you want to isolate the traffic to:

- Have all communications between NetScaler Console and its managed NetScaler instances in one network.
- Have management access to NetScaler Console in another network.

In this scenario, as an administrator, you can:

- Configure one IP address for the traffic between NetScaler Console and its managed NetScaler instances.
- Configure another IP address for managing the NetScaler Console software to perform all administrative tasks in the software.

> **Note**
>
> If NetScaler Console is configured as an HA pair, the management IP address configured on the second NIC is associated with the primary node.

Prerequisites

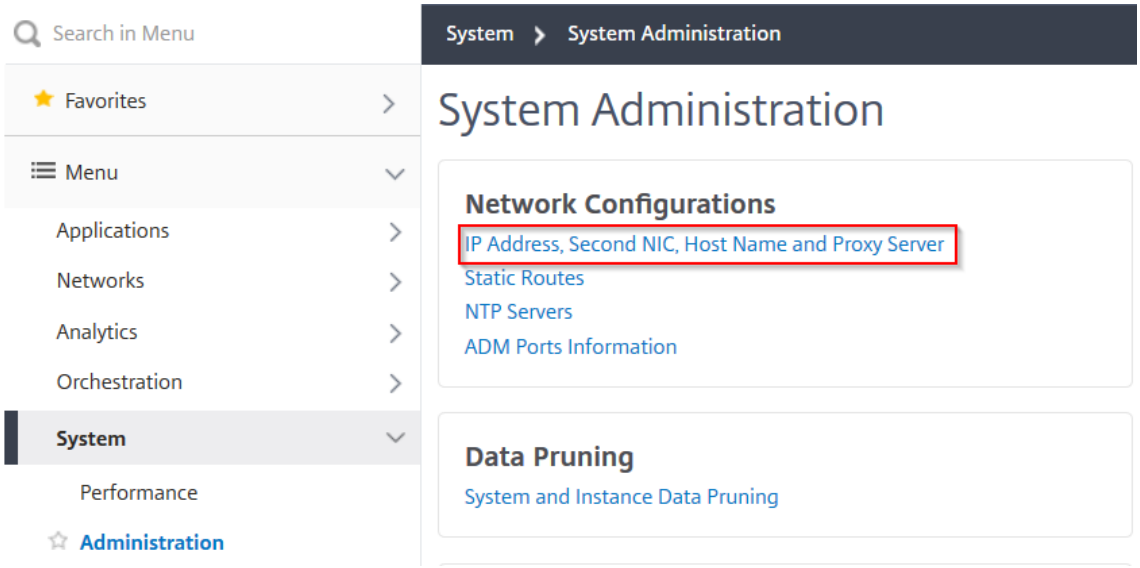
- Ensure you have deployed and configured **NetScaler Console 13.0 Build 47.x or later** on the hypervisor (Citrix Hypervisor, Microsoft Hyper-V, Linux KVM, or VMware ESXi).
- Ensure you have added the second NIC on the hypervisor (Citrix Hypervisor™, Microsoft Hyper-V, Linux KVM, or VMware ESXi).

© 1997–2025 Citrix Systems, Inc. All rights reserved.

To assign an IP address to a NIC on a Citrix Hypervisor and create a secondary interface, see Assign an IP Address to a NIC.

Configure a second NIC in NetScaler Console

1. Log on to NetScaler Console GUI.
2. Navigate to **Settings > Administration**.
3. Under **Network Configuration**, click **IP Address, Second NIC, Host Name and Proxy Server**.



   The **Network Configuration** page is displayed.

4. Click the Second NIC tab and configure the following parameters:

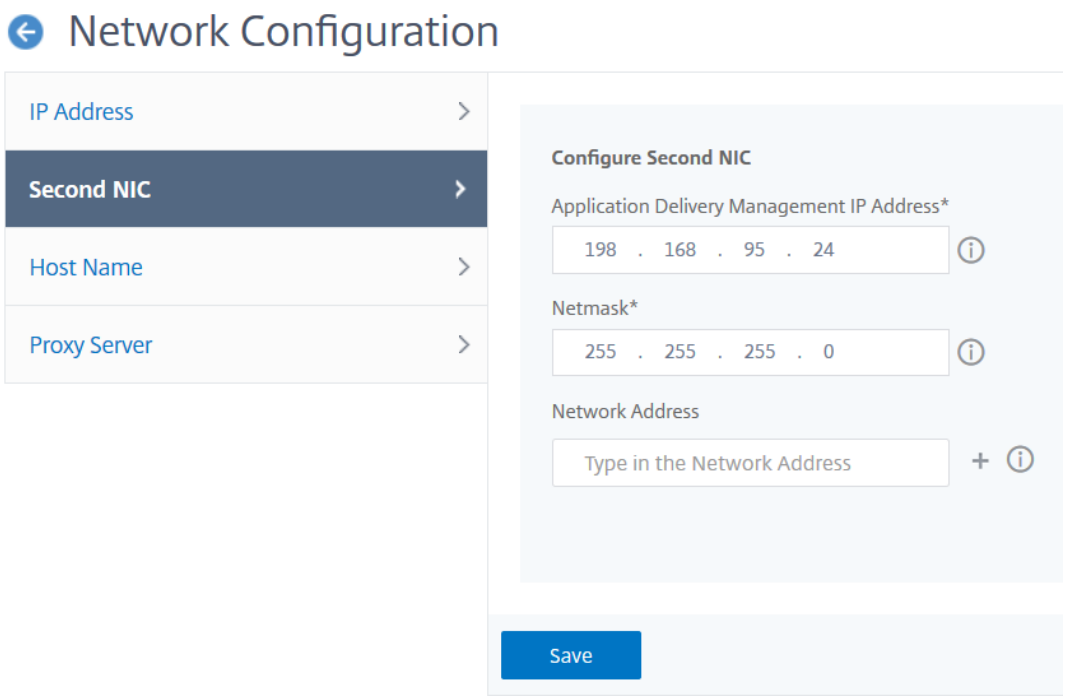
   a) **Application Delivery Management IP Address** –Enter a valid IP address to access NetScaler Console. You can use this IP address to access NetScaler Console, apart from the existing management IP address.

   b) **Netmask** –Enter the netmask address to specify the network host. The default address is 255.255.255.0.

   c) **Network Address** –Enter an IP address to add a route entry for NetScaler Console. Click **+** to add more IP addresses. This field is optional.

   d) Click **Save**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Configure a secondary NIC to access NetScaler® agent

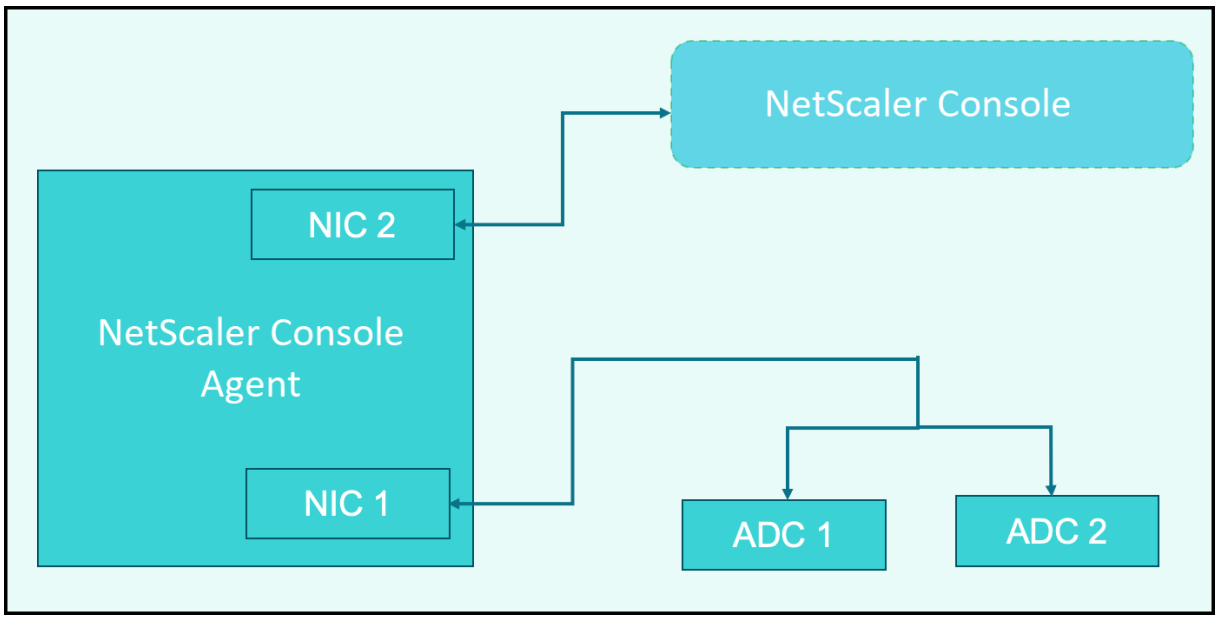
September 27, 2025

You can configure two NICs on an agent. Using the Dual NIC architecture, agent will be able to:

- Establish communication between 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 agent and 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 and NetScaler instances needs to be separated.

Modify the IPV4 NIC network addresses using CLI

1. Open an SSHconnection to the NetScaler agent console by using an SSH client, such as PuTTY.
2. Log in using the **nsrecover/nsroot** credentials and switch to the shell prompt.
3. Run the command **ifconfig**. You can see the details of the two NICs that you have configured -
    - NIC 1 –For communication between Agent to NetScaler Communication
    - NIC 2 –For communication between Agent to NetScaler Console

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
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.

5. Select a menu item to modify. Save and quit the settings.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Configure syslog purging interval

September 27, 2025

Syslog is a standard protocol for logging. It has two components: the Syslog auditing module, which runs on the Citrix NetScaler instance, and the Syslog server, which can run either on the underlying FreeBSD operating system (OS) of the NetScaler instance or on a remote system. SYSLOG uses User Datagram Protocol (UDP) for data transfer.

Syslog enables isolation of the system that generates information and the system that stores the information. You can consolidate logging information and derive insights from the collected data. You can also configure syslog to log different types of events.

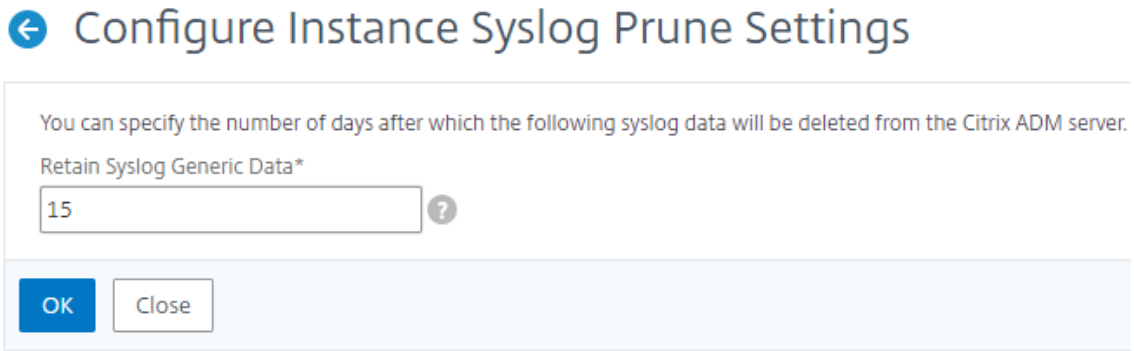
To limit the amount of syslog data stored in the database, you can specify the interval at which you want to prune syslog data. You can specify the number of days after which the following syslog data will be deleted from NetScaler Console:

- Generic Syslog Data
- AppFirewall Data
- NetScaler Gateway Data

You can also configure the NetScaler Gateway prune interval by syslog type. This prune interval takes precedence over the rune interval configured to retain NetScaler Gateway data.

To configure syslog prune interval settings for NetScaler Console:

1. Navigate to **Settings > Data Storage > Data Retention Policy**. The page for **Data Pruning** is displayed. Click **Instance Syslog**.
2. In **Configure Instance Syslog Prune Settings** page, specify **Retain Syslog Generic Data(days)**. Type the number of days for which NetScaler Console retains generic syslog messages.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Configure system prune and event prune settings

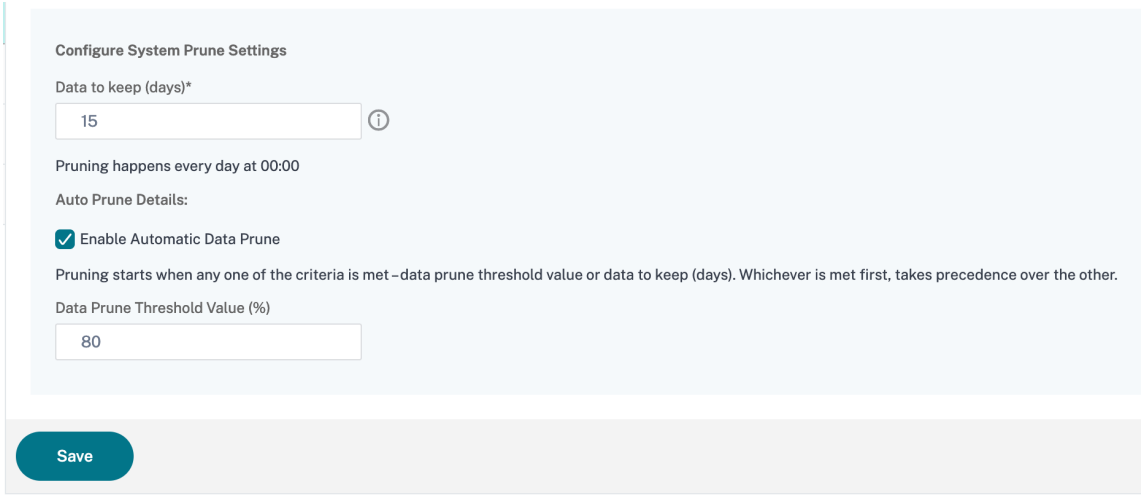
September 27, 2025

To limit the amount of reporting data being stored in your NetScaler Console software database, you can prune it. You can specify the interval for which you want NetScaler Console to retain network reporting data, events, audit logs, and task logs. By default, this data is pruned every 24 hours (at 00.00 hours).

> **Note**
>
> The value you specify can't be more than 30 days or be less than 15 days.

To configure system prune settings for performance reports:

1. Navigate to **Settings** > **Administration**. Under **Data Pruning**, click **System and Instance Data Pruning**.
2. In the **Configure System Prune Settings** page, specify the following:
   - Number of days to keep the data
   - Percentage of disk space (pruning threshold)
3. Click **OK**.



You can enable automatic pruning by selecting the **Enable Automatic Data Prune** check box. An alarm is triggered and an email is sent when disk usage breaches the configured **Data Prune Threshold Value**.

> **Note**
>
> Pruning starts when any one of the criteria is met –data prune threshold value or data to keep

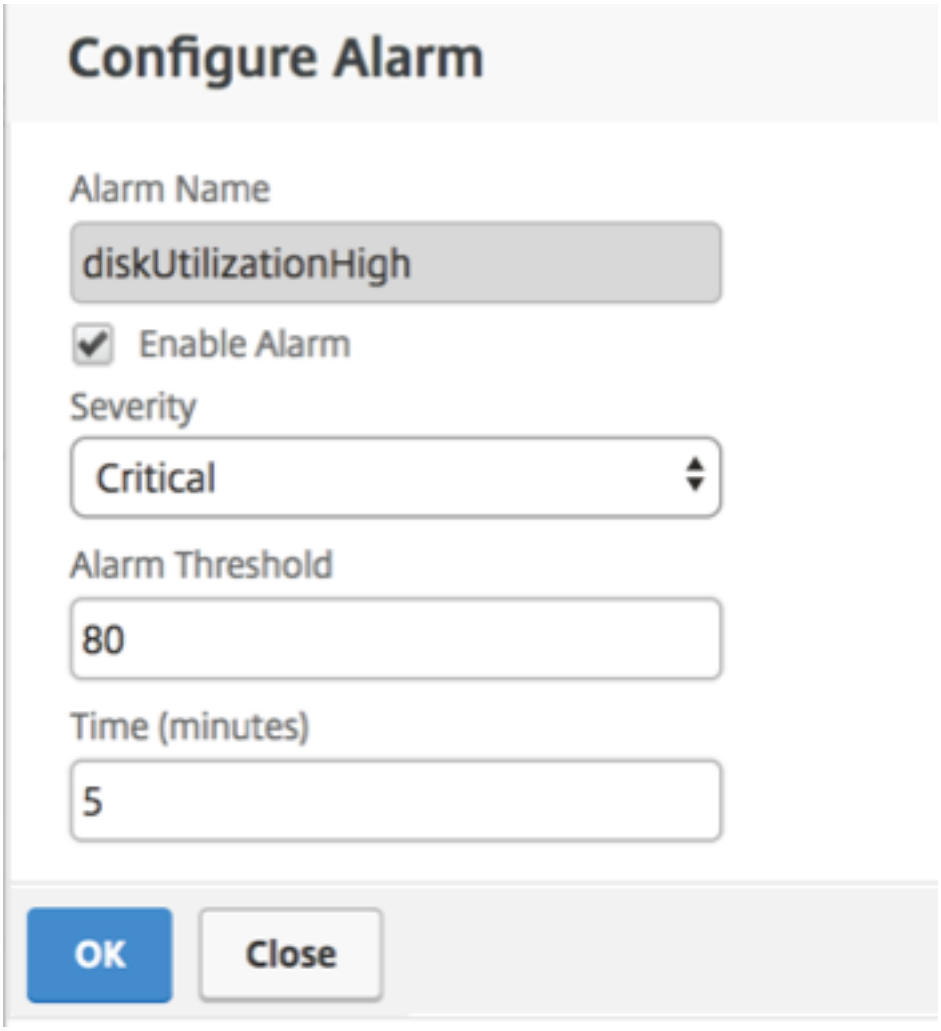
© 1997–2025 Citrix Systems, Inc. All rights reserved.

> (days). Whichever is met first, takes precedence over the other.

To configure and enable alarm settings:

1. Navigate to **Settings** > **SNMP**. Click **Alarms** on the upper-right corner.
2. Select the alarm that you want to configure (for example, diskUtilizationHigh) and click **Edit**.
3. In the **Configure Alarm** page, specify the following:

- **Severity**—Select the severity level.
- **Alarm Threshold**—Type the value for which the event severity is calculated.
- **Time**—Type the time (in minutes) after which you want to trigger the alarm.



Configure Events Prune Settings by Using NetScaler Console

To limit the amount of event messages data being stored in your NetScaler Console database, you can specify the interval for which you want NetScaler Console to retain network reporting data, events,

© 1997–2025 Citrix Systems, Inc. All rights reserved.

audit logs, and task logs. By default, this data is pruned every 24 hours (at 00.00 hours).

1. Navigate to **Settings > Administration > Data Pruning** and click **System and Instance Data Pruning**. Click **Instance Events**.
2. Enter the time interval, in days, for which you want to keep the data on the NetScaler Console server and click **Save**.

Enable shell access for non-default users

September 27, 2025

You can enable shell access for non-default users in NetScaler Console. You can use this feature to enable and set up communication mode with instances.

> **Note**
>
> By default, shell access is disabled for non-default users.

To enable shell access for non-default users in NetScaler Console:

1. In NetScaler Console, navigate to **Settings > Administration**.
2. In **System Configurations**, click **System, Time Zone, Allowed URLs and Agent Settings**.
3. On the **System Configurations** page, configure the following parameters:
    - **Communication with instances** - Select the communication protocol.
    - **Secure Access** - Enable secure access for NetScaler Console.
    - **Enable Session Timeout** - Specify the time period for which to retain an inactive session.
    - **Allow Basic Authentication** - Allow Management Service to accept credentials given using Basic Authentication Protocol.
    - **Enable nsrecover Login** - Enable `nsrecover` login on Management Service.
    - **Enable Certificate Download** - Enables you to download certificates from the added NetScaler.
    - **Enable Shell access for non-nsroot User** - Enable shell access for non-default users in NetScaler Console.
    - **Prompt user credentials for instance login** - Allow users to enter their user credentials while logging on to instances from NetScaler Console.
        - **Prompt Credentials for Stylebooks Operations** - Allow users to enter their user credentials while using StyleBook and config pack operations on NetScaler instances.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Note:**
> If **Prompt Credentials for Instance Login** is selected and **Prompt Credentials for Stylebook Operations** is cleared, users are not prompted to provide credentials for StyleBook and config pack operations on NetScaler instances.

4. Click **OK**.

Recover inaccessible NetScaler Console servers

September 27, 2025

NetScaler Console now provides a database maintenance tool to perform cleanup of the system database. You can now launch the NetScaler Console utility tool to connect to the file system, delete a few components, and make the database accessible. NetScaler Console recovery script is a tool that helps to recover space in the file system by clearing old or unused database tables and files. The tool assists you to navigate through the database tables and files in successive steps and shows the current space occupied on the filesystem by respective items. Once you have selected the database tables and files to be deleted, the tool deletes those from the filesystem after confirmation.

How to Use NetScaler Console Database Recovery Script for a NetScaler Console Standalone Deployment

Use the following procedure in a single server NetScaler Console deployment to connect to the file system, delete a few components, and make the database accessible, and then perform the recovery operations.

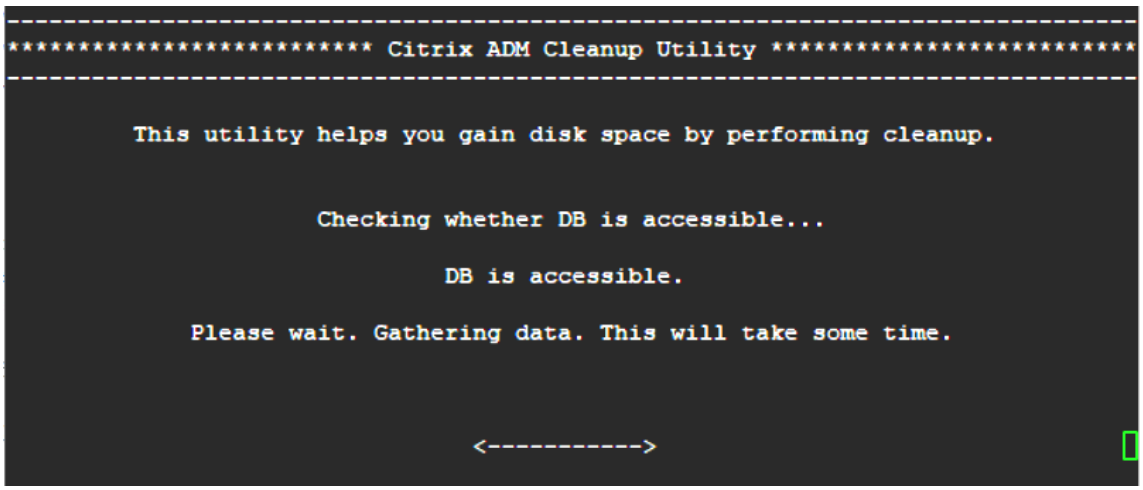
1. Using an SSH client or your hypervisor's console, logon to NetScaler Console and type the following command:

```
Last login: Fri Nov 30 09:51:19 2018 from 10.252.241.100
Have a nice daybash-3.2# /mps/mas_recovery/mas_recovery.py
```

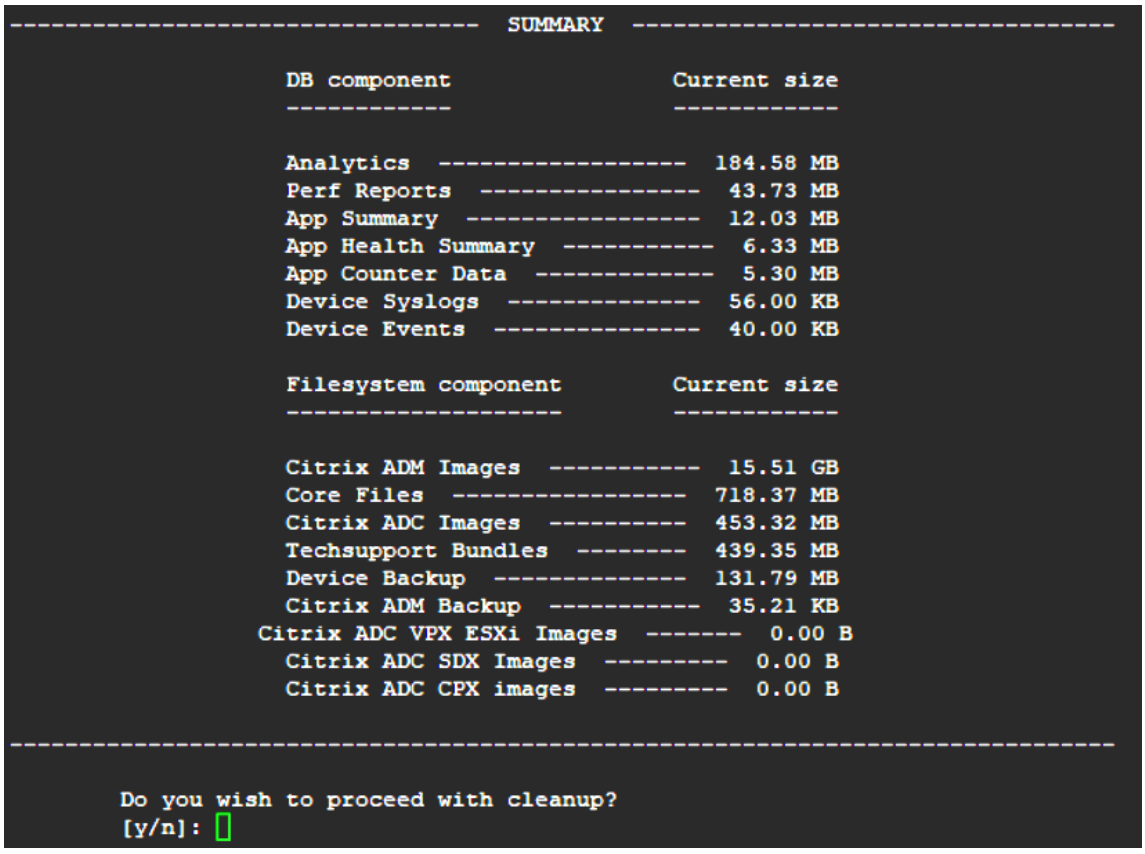
2. When the screen displays a caution message for stopping a few NetScaler Console processes, type "y"and press the **Enter** key.

   The following screen appears while the system determines which components of the database you can delete without affecting the system's core files.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. The screen displays the list of files in the database. Type “y”and press the Enter key to begin the cleanup process.

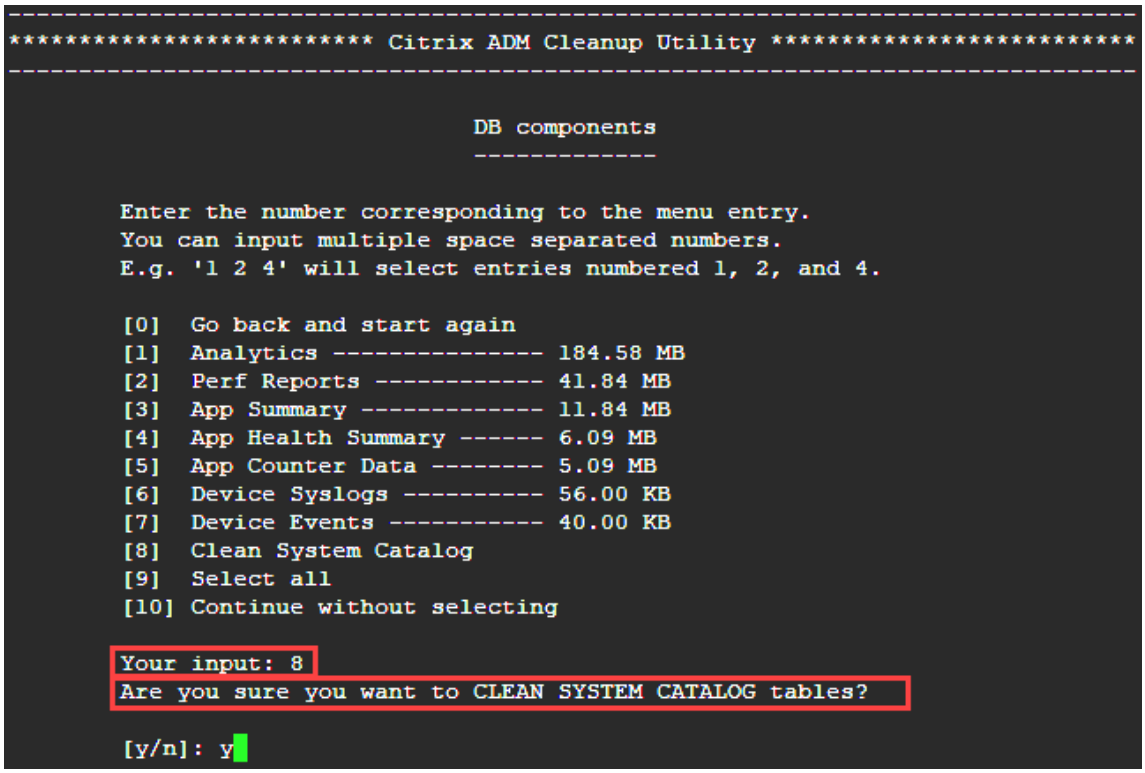


4. You can select the specific database component that needs to be cleaned and type the corresponding number. Press the **Enter** key.

   For example, to perform System Catalog cleanup, select option 8 in the **DB component** selection menu and type “y”and press the **Enter** key to continue with the system catalog clean up.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> **Note**
>
> NetScaler Console includes user tables known as system catalog. The system catalog is a location in the NetScaler Console database where a relational database management system stores schema metadata, such as information about tables and columns and internal records. The tables in the system catalog are like regular tables that can accumulate inflated and dead rows over time and therefore, need periodic cleanup for optimal performance. It is a good practice to regularly maintain these tables. The activity not only frees up disk space but also improves the overall performance of the database and therefore of the NetScaler Console.



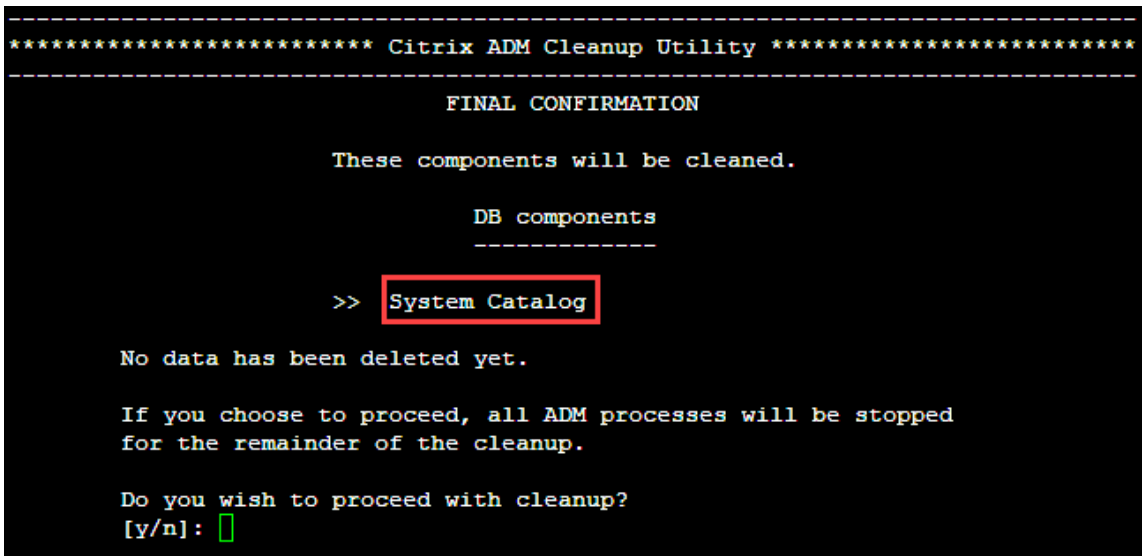
The cleanup utility gives you an option to clean database components and file components. You can select any file component by typing a number between “1”and “9,”or type “11”and press the Enter key to clean the database component.

> **Note**
>
> The number “11”indicates that you have not selected any file component to be cleaned and you are going ahead with cleaning up the earlier database component that you had earlier selected. In this example, it is “system catalog.”

© 1997–2025 Citrix Systems, Inc. All rights reserved.

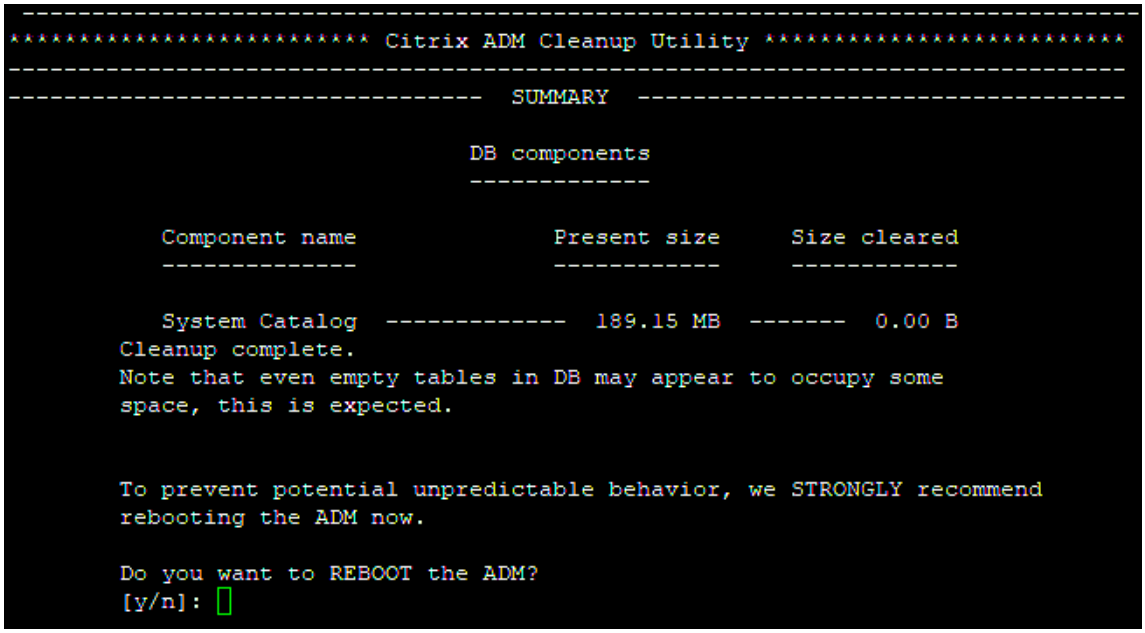


5. Type “y”and press the **Enter** key again in the final confirmation screen.



The System Catalog is cleaned up, which may take time depending on the size of the table in the System Catalog. After the process is complete, a summary screen is shown.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



6. Type “y”and press the **Enter** key to restart NetScaler Console.

   Ensure you restart NetScaler Console after system clean up. Wait for about 30 minutes for internal database operations to complete after NetScaler Console has restarted. You should then be able to connect to NetScaler Console database. If not, run the recovery script again to free up more space. When NetScaler Console is up and running, it should work as expected.

   > **Note**
   >
   > The current size of the system catalog table is never equal to Zero after clean up. This is because only empty rows are removed from the table and the table might have some valid entries even after they are cleaned up.

How to use NetScaler Console database recovery script for a NetScaler Console high availability deployment

The database system for NetScaler Console servers in a high availability deployment is in continuous synchronization mode. While using the new database recovery tool, you do not need to replicate the procedure on both the NetScaler Console servers.

1. Using an SSH client or hypervisor’s console, log on to the primary node.
2. Run the following command:

   ```
   /mps/mas_recovery/mas_recovery.py
   ```

3. Follow the procedure from step 2 available for NetScaler Console Standalone Deployment Recovery Script

© 1997–2025 Citrix Systems, Inc. All rights reserved.

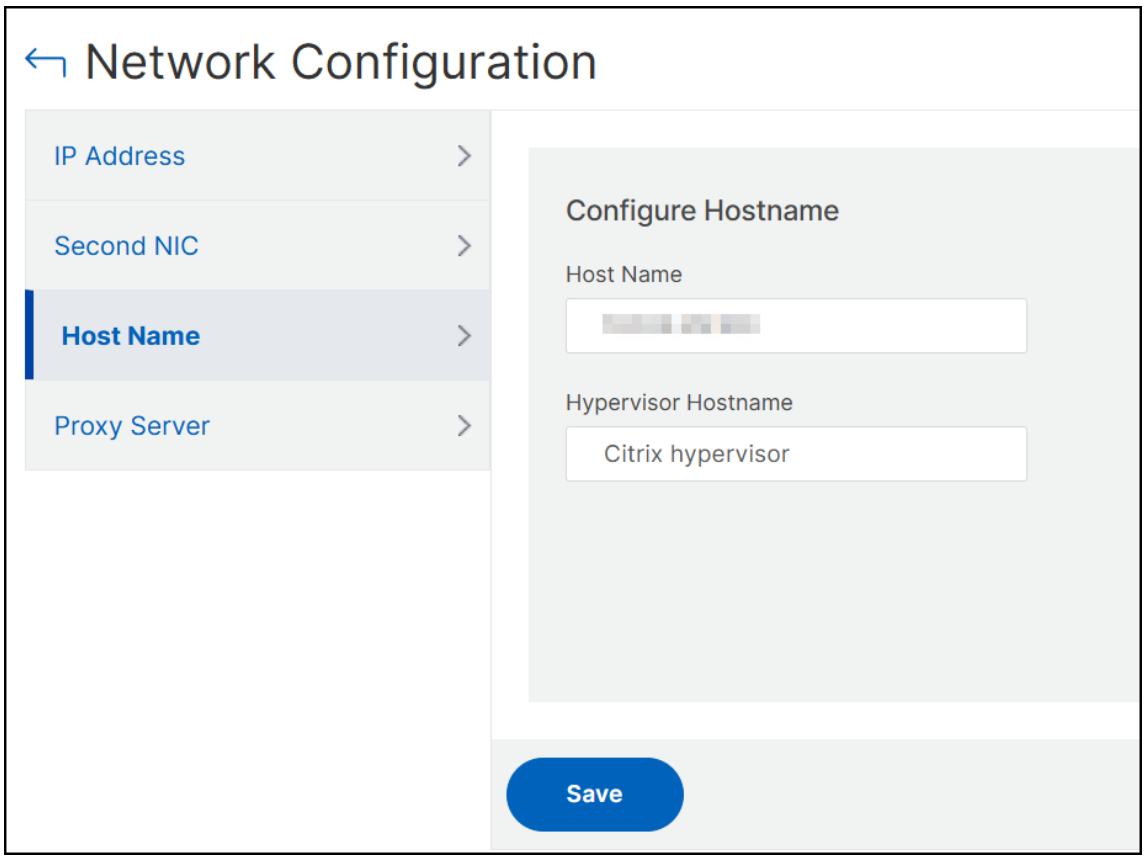
Assign a host name to a NetScaler Console server

December 23, 2024

To identify a NetScaler Console server, you can assign the server a host name.

To assign a host name to a NetScaler Console server:

1. In NetScaler Console, navigate to **Settings > Administration**.
2. Under **Network Configurations**, click **IP Address, Second NIC, Host Name and Proxy Server**.
3. Select **Host Name**, enter a host name and hypervisor host name, and click **Save**.



> **Note:**
>
> You can also use the `networkconfig` command in your hypervisor and change the host name.

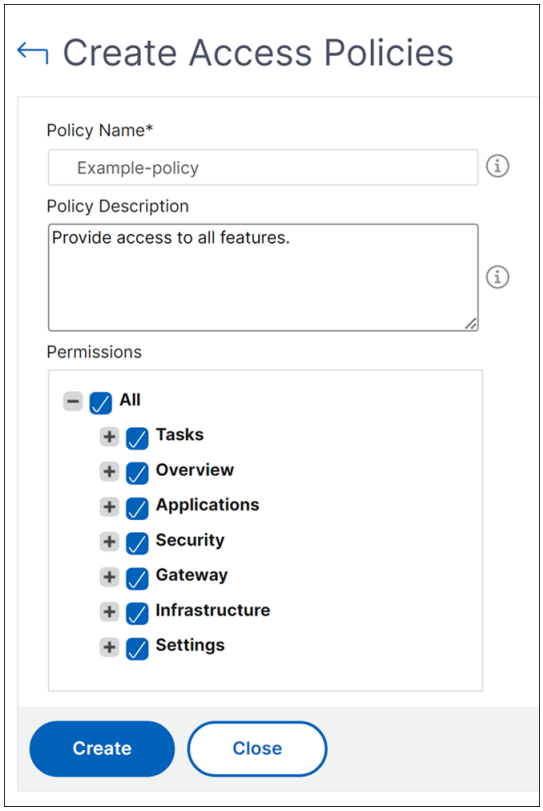
© 1997–2025 Citrix Systems, Inc. All rights reserved.

Back up and restore your NetScaler Console server

September 27, 2025

You can take periodic backups of your NetScaler Console server. You can back up and restore the configuration files, instance details, system data, and so on.

> **Important**
>
> Citrix recommends you to restore the NetScaler Console server using a backup of the same version. For example, if the NetScaler Console version is 13.0, use the 13.0 NetScaler Console backup to restore the server.
>
> User access to backup and restore the NetScaler Console server is limited. The **Settings > Backup Files** page appears only to the users who have access to all NetScaler Console features. A user can access this page only if their access policy has all permissions. Typically, superusers have the access to all NetScaler Console features.



> For more information, see Configure access policies.

Before you upgrade, back up the NetScaler Console server configuration files for precautionary reasons.

The backup includes the following components:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- NetScaler Console Configuration Files:
  - SNMP
  - Syslog server configuration files
  - NTP files
  - SSL certificates
  - Control Center files
- Backups of NetScaler instances that the NetScaler Console server manages.
- Configuration audit templates.
- System data stored on the database:
  - List of tenants and users created.
  - External authentication server configuration (LDAP, RADIUS, and others).
  - Configuration jobs and job templates created.
- Infrastructure and application data stored on the database:
  - Data from added and managed NetScaler instances.
  - Instance profile details, version details, instance group details, and so on.
  - A static application (group of virtual servers) created by the administrator.
- SNMP settings.

> **Note**
>
> Analytics data, events, NetScaler Console licenses, and syslog messages are excluded from the backup.

Back up the NetScaler Console configuration

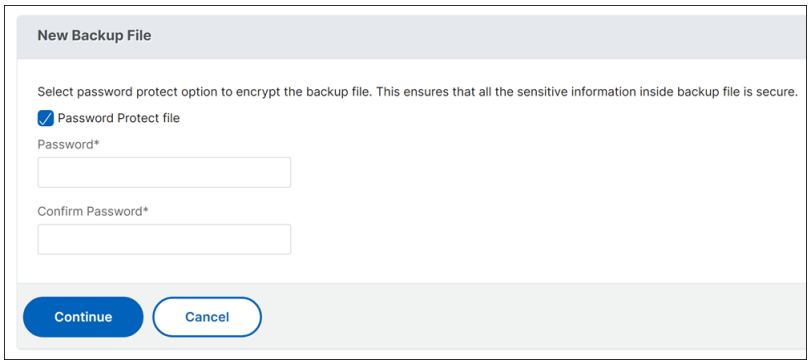
By default, the NetScaler Console server backs up the configuration every 24 hours (at 00.30 hours). You can also schedule and select the time for the backup. Further, you can move a copy of the backed-up file to another system.

The backup is stored as a compressed TAR file that can also be encrypted. By default, three backup files are retained in the server. To avoid any low disk space issues, you can store a maximum of 10 backup files on your NetScaler Console server. However, We recommend you to store some copies of your backup files on the server or transfer the files to another system as a precautionary measure.

To backup a NetScaler Console configuration:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

1. Navigate to **Settings > Backup Files**, and then click **Back Up**.
2. To encrypt the backup file, select the **Password Protect file** check box, and then provide a password to encrypt the file.



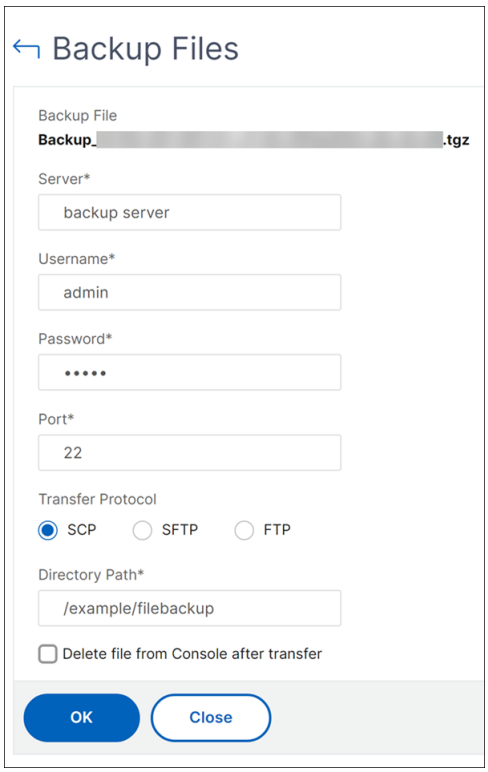
Transfer a NetScaler Console backup file to an external system

You can transfer a copy of the backup file to another system as a precautionary measure. When you want to restore the configuration, first upload the file to the NetScaler Console server and then perform the restore operation.

To transfer a NetScaler Console backup file:

1. Navigate to **Settings > Backup Files**.
2. Select the backup file that you want to move to another system, and then click **Transfer**.
3. On the **Backup Files** page, specify the following parameters:
   - **Server** - IP address of the system where you want to transfer the backed-up file.
   - **User Name and Password** - User credentials of the new system where the backed-up files are being copied.
   - **Port** - Port number of the system the files are being transferred to.
   - **Transfer Protocol** - Protocol being used to make the backup file transfer. You can select SCP, SFTP, or FTP protocols to transfer the backed-up file.
   - **Directory Path** - The location where the backed-up file is being transferred to on the new system.
4. You can delete the backup file from NetScaler Console after transfer by selecting the **Delete file from Application Delivery Management after transfer** check box.
5. Click **OK** to make the transfer.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



> **Note**
>
> To save a copy of the backup file in your local system, navigate to **Settings > Backup Files**, select the file you want to copy, and then click **Download**.

Restore the NetScaler Console configuration from a backup file

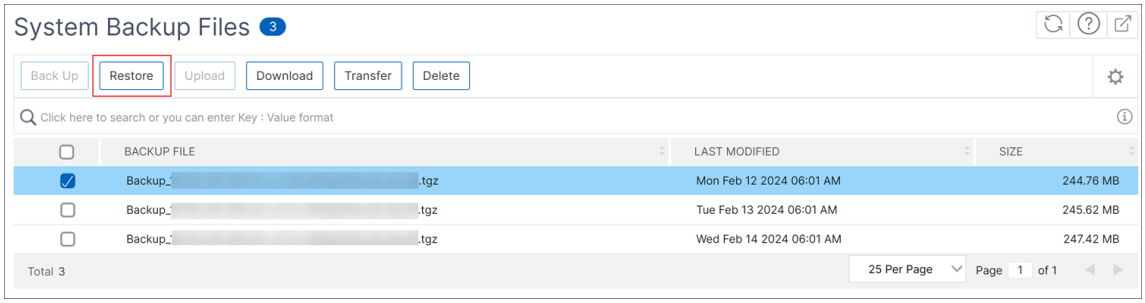
When you restore the NetScaler Console configuration from a previously backed up file, the restore operation untars the backup file and then restores the configuration. The restore operation deletes the existing configuration and replaces it with the configuration in the backup file.

> **Note**
>
> The restore operation fails if the backup file is renamed or if the backup file contents are modified.

To restore a NetScaler Console configuration from a backup file:

1. Navigate to **Settings > Backup Files**.
2. Select the backup file that you want to restore, and then click **Restore**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



3. On the confirmation dialog box, click **Yes**.

> **Note**
>
> To restore the configuration from a backup file stored in an external system, upload the backup file to the NetScaler Console server before performing the restore operation. To upload the file, navigate to **Settings > Backup Files**, and then click **Upload**.

VM snapshots of NetScaler Console in high availability deployment

September 27, 2025

You can take snapshots of NetScaler Console servers in the HA deployment before starting your upgrade. Snapshots capture the entire state of the virtual machine at the time that you take them.

Take a snapshot of NetScaler Console servers

Use the following sequence to take snapshots of the NetScaler Console servers:

1. NetScaler Console secondary server
2. NetScaler Console primary server

To take a snapshot of NetScaler Console servers:

1. On your hypervisor, select the NetScaler Console secondary server from the list of virtual machines.
2. Take a VM snapshot.

> **Note:**
>
> We recommend you select **Take VM memory** while taking the snapshot.

3. Give the snapshot a meaningful name and enter a description, if needed.

   The snapshot is stored in the default VM directory.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

4. Repeat the same steps for the primary server.

> **Note:**
>
> You don't have to power off the VM while taking a snapshot.

Restore a snapshot of NetScaler Console servers

When you restore a snapshot, you return the virtual machine's memory, settings, and the state of the virtual machine disks to the state they were in at the time you took the snapshot.

Use the following sequence to restore snapshots of the NetScaler Console servers:

1. NetScaler Console primary server
2. NetScaler Console secondary server

To restore the snapshot of NetScaler Console servers:

1. On your hypervisor, select the NetScaler Console primary server from the list of virtual machines.
2. Right-click the VM and revert the snapshot.

   The virtual machine is reverted to the most recent snapshot.
3. Repeat the same steps for the NetScaler Console secondary server.

View auditing information

September 27, 2025

Audit logs have records with certain information for a specific duration such as user details, operations, and actions performed. You can view syslog messages for the following example scenarios:

- If your NetScaler® Console is a HA pair and if there is any latency issue in the database replication between the primary and secondary nodes, you can view details as an event.
- If there are any invalid login attempts (user name or password error) or successful logins, you can view details as an event.

As an administrator, you can use these logs for maintaining security and for recovering lost transactions.

To configure a syslog server on NetScaler Console:

1. Navigate to **Settings > Audit log messages > Syslog Servers**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. In the **Syslog Server** page, click **Add**.
3. On the **Create Syslog Server** page, enter the following values:
    - **Name** - Name for the syslog server.
    - **IP Address** - IP address of the syslog server.
    - **Port** - Syslog server port.
4. Choose the log levels (All, None, or Custom).
5. Click **Create**.

To configure the syslog date and time format on NetScaler Console:

1. Navigate to **Settings > Audit log messages > Syslog Servers**.
2. In the **Syslog Server** page, select a syslog server, and then, click **Syslog Parameters**.
3. On the **Configure Syslog Parameters** page, specify the date and time format.
4. Click **OK**.

To view syslog messages on NetScaler Console:

Navigate to **Settings > Audit log messages**.

You can also apply filters from the following filters and view the system log messages:

- Event
- Message
- Module
- Severity
- Source

For more information, see Syslog message references.

Configure SSL settings

September 27, 2025

SSL (Secure Socket layer) and TLS (Transport Layer Security) are commonly used security networking protocols that provide encrypted communication between users and servers. You can configure SSL settings on NetScaler Console and specify the type of clients that connect to the system.

To configure SSL settings for NetScaler Console:

1. Navigate to **Settings > Administration**. Under **SSL Settings**, click **Configure SSL Settings**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. On the **SSL Settings** page, review the current protocol settings and the cipher suites applied to the system.
3. To modify the protocol settings, click the **+** icon in **Protocol Settings** under **Edit Settings**, and make the changes that you want.
4. To modify the applied cipher suites, click the **+** icon in **Cipher Suites** under **Edit Settings**, and make the changes that you want.
5. Click **OK**, and then click **Close**.

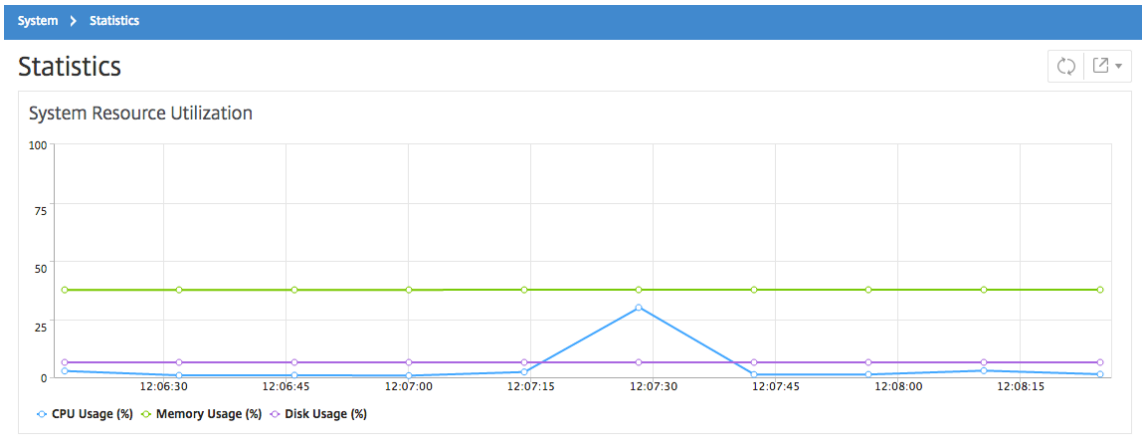
Monitor CPU, memory, and disk usage

February 9, 2024

You can use the information maintained in logs and statistics. This information is also displayed in reports that helps you to configure and maintain NetScaler Console.

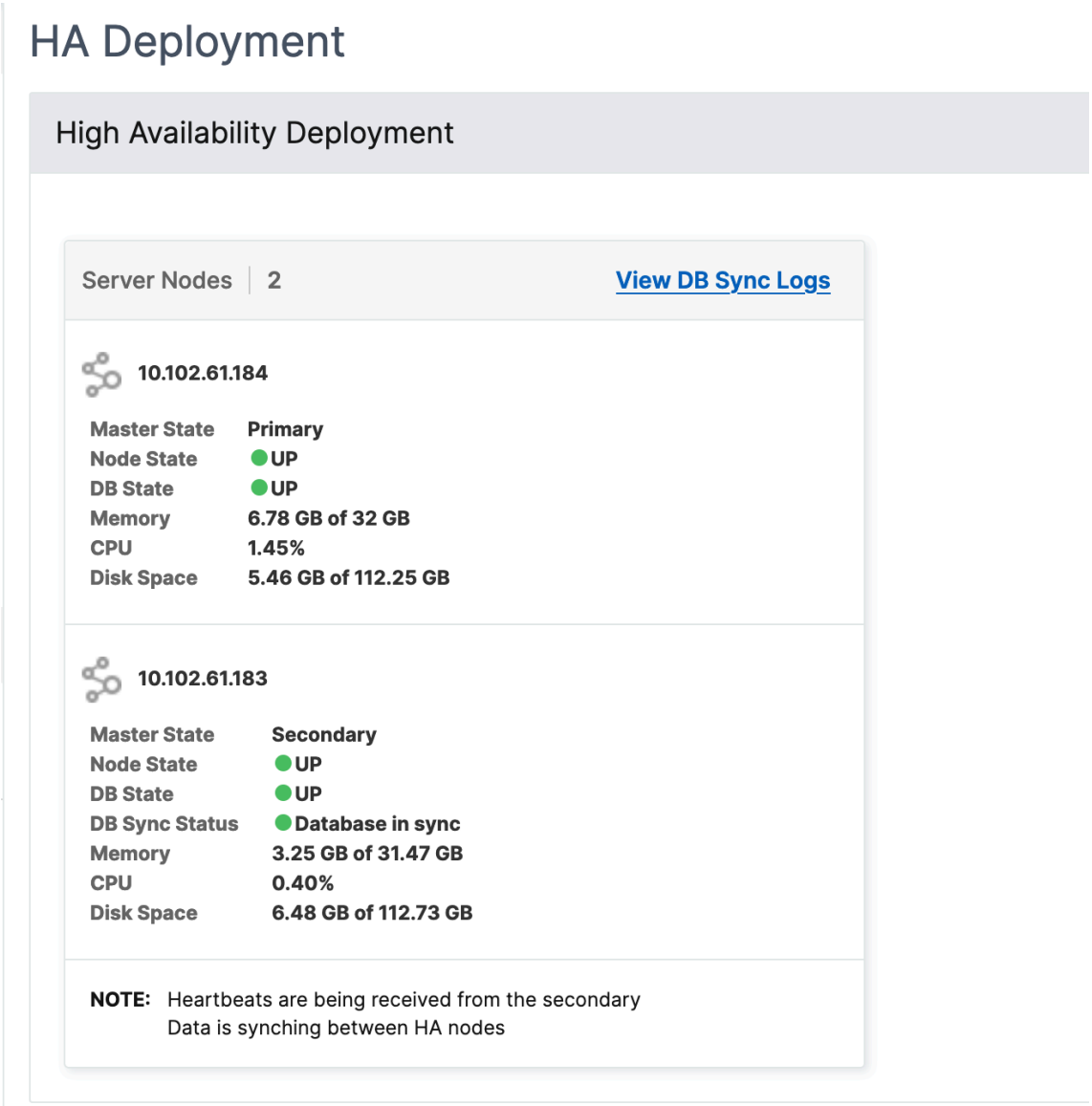
To monitor CPU, memory, and disk usage,

- **Standalone deployment.** Navigate to **System** > **Statistics**. You can view real-time CPU, memory, and disk utilization charts.



- **High availability deployment.** Navigate to **Settings > Deployment**. The statistics for memory, CPU, disk space, and managed instances are displayed numerically as shown in the following figure:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Configure notification settings

September 27, 2025

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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.

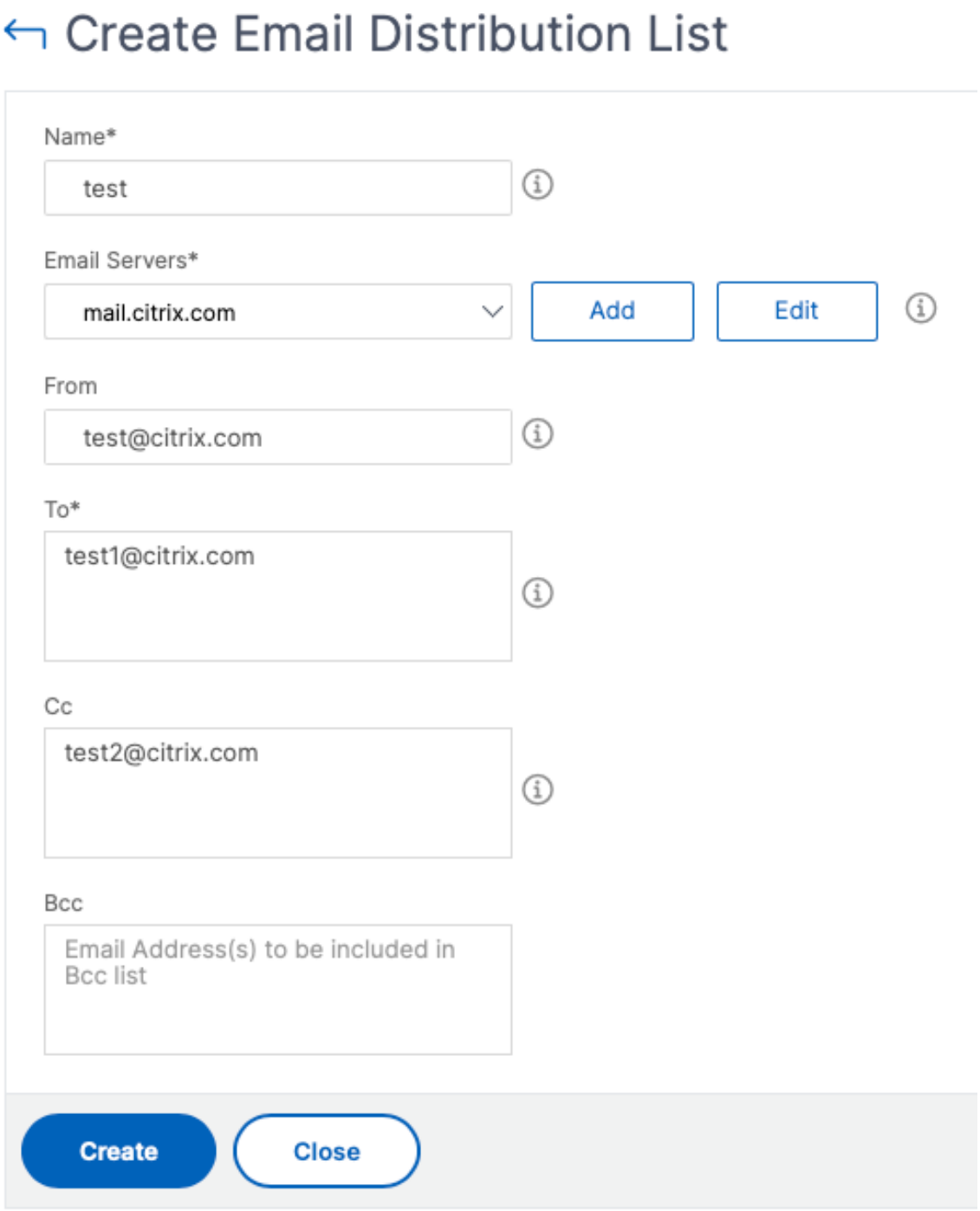
Create an email distribution list

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.
    - **Email Server** - Select the email server that sends email notification. If you want to add an email server, click **Add**.
    - **From** - Specify the email address from which NetScaler Console has to send messages.
    - **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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Create an SMS distribution list

To receive SMS notifications for NetScaler Console functions, you must add an SMS server and phone numbers.

Perform the following steps to configure SMS notification settings:

1. Navigate to **Settings > Notifications**.
2. In **SMS**, click **Add**.
3. In **Create SMS Distribution List**, specify the following details:
    - **Name** - Specify the distribution list name.
    - **SMS Server** - Select the SMS server that sends SMS notification.
    - **To** - Specify the phone number to which NetScaler Console has to send messages.
4. Click **Create**.

Repeat this procedure to create multiple SMS distribution lists. The **SMS** tab displays all the SMS distribution lists present in NetScaler Console.

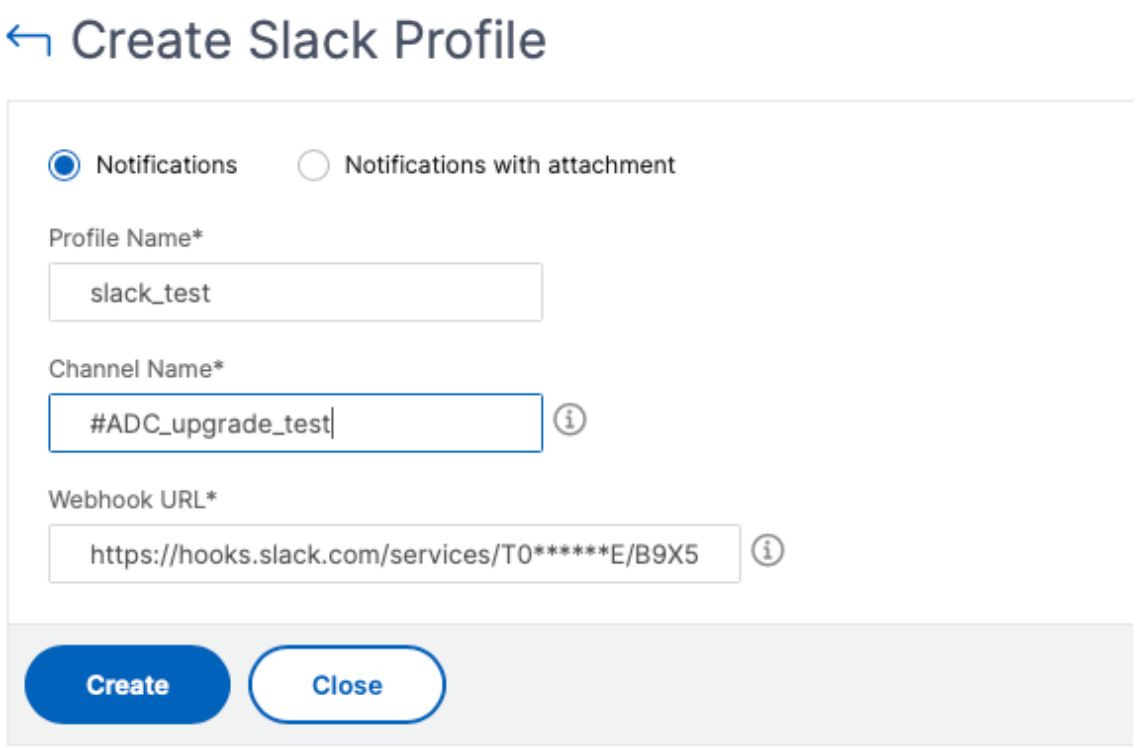
Create a Slack profile

To receive Slack notifications for NetScaler Console functions, you must create a slack profile.

Perform the following steps to create a Slack profile:

1. Navigate to **Settings > Notifications**.
2. In **Slack**, click **Add**.
3. In **Create Slack Profile**, specify the following details:
    - **Profile Name** - Specify the profile name. This name appears in the Slack profile list.
    - **Channel Name** - Specify the Slack channel name to which NetScaler Console has to send notifications.
    - **Webhook URL** - Specify the Webhook URL of the channel. Incoming Webhooks are a simple way to post messages from external sources into Slack. The URL is internally linked to the channel name. And, all event notifications are sent to this URL are posted on the designated Slack channel. An example of webhook is as follows: https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK

© 1997–2025 Citrix Systems, Inc. All rights reserved.



4. Click **Create**.

Repeat this procedure to create multiple Slack profiles. The **Slack** tab displays all the Slack profiles present in NetScaler Console.

Create a PagerDuty profile

You can add a PagerDuty profile to monitor the incident notifications based on the PagerDuty configurations. PagerDuty enables you to configure notifications through email, SMS, push notification, and phone call on a registered number.

Before you add a PagerDuty profile in NetScaler Console, ensure you have completed the required configurations in PagerDuty. To get started with PagerDuty, see PagerDuty documentation.

Perform the following steps to create a PagerDuty profile:

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Integration Key** - Specify the integration key. You can obtain this key from your PagerDuty portal. When creating a service in PagerDuty for integration, use the **Generic Events API Integration** option.

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**.

Generate a tech support file

November 11, 2024

We recommend you generate an archive of NetScaler Console data and statistics before contacting technical support for debugging an issue. The archive is a TAR file that you can send to the technical support team.

> **Note**
>
> For NetScaler Console servers in a high availability mode, you can generate a technical support file from either of the servers. Citrix advises you to not use the load balancing virtual server IP address to generate the technical support file.

To configure and send a technical support file from NetScaler Console:

1. Navigate to **Settings** > **Diagnostics** > **Technical Support**, and then click **Generate Technical Support File**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. On the **Generate Support File** page, select the following options:

- **Collect Debug Logs** –Select this option to collect `afdecoder` logs.
- **Duration** –Enter the duration for which debug logs must be collected. You will only see this option, if you enable the **Collect Debug Logs** option.
- **Collect Data Distribution** –Select this option to collect distinct and diverse logs from the database.

```
The archive file is created as a TAR file.

For example, the archive file that is created might be named as
   follows:   Citrix_ADM_<ADM_IP_address>_<DDMMYY>_<time_stamp>.
   tar.gz
```

1. You can send the technical support files to the support team in two ways:

   a) You can download the file from the NetScaler Console GUI to your local storage and then use a web browser to upload to Citrix Insight Services(CIS).

   b) You can also upload the technical support files to the CIS website by running a script on the Console.

      i. Using SSH, log on to the Console.

      ii. Switch to the Shell prompt and type:

      /mps/collector_upload.pl

The full command is given below with the attributes you need to provide:

```
/mps/collector_upload.pl [-proxy [<proxy_user>:<proxy_password>@]<
   proxy_host>:<proxy_port>] [-user <user>] [-password <password>] [-sr
    <sr>] [-description <description>] [-debug] <file>
```

The advantage of running the Perl script is that you don't have to download the technical support file from NetScaler Console to your local system and then upload it to CIS. As an option, you can upload the file to CIS directly by using a proxy from the Console.

Ensure that you have an account on CIS. You can use your Citrix account credentials to upload files to CIS.

What if you don't have a proxy server? Or what if you are facing some issues with SSL forward proxies? (This can happen if the Perl script does not trust the proxy server's root certificate.)
You can still upload the file directly from the NetScaler Console shell to CIS.

> **Note**
>
> You can still download the file and email them to the Citrix technical support team in a situation where NetScaler Console fails to upload the file to CIS from the console. Or, you can download

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> the file from NetScaler Console to your local storage and then use a web browser to upload to CIS.

Configure a cipher group

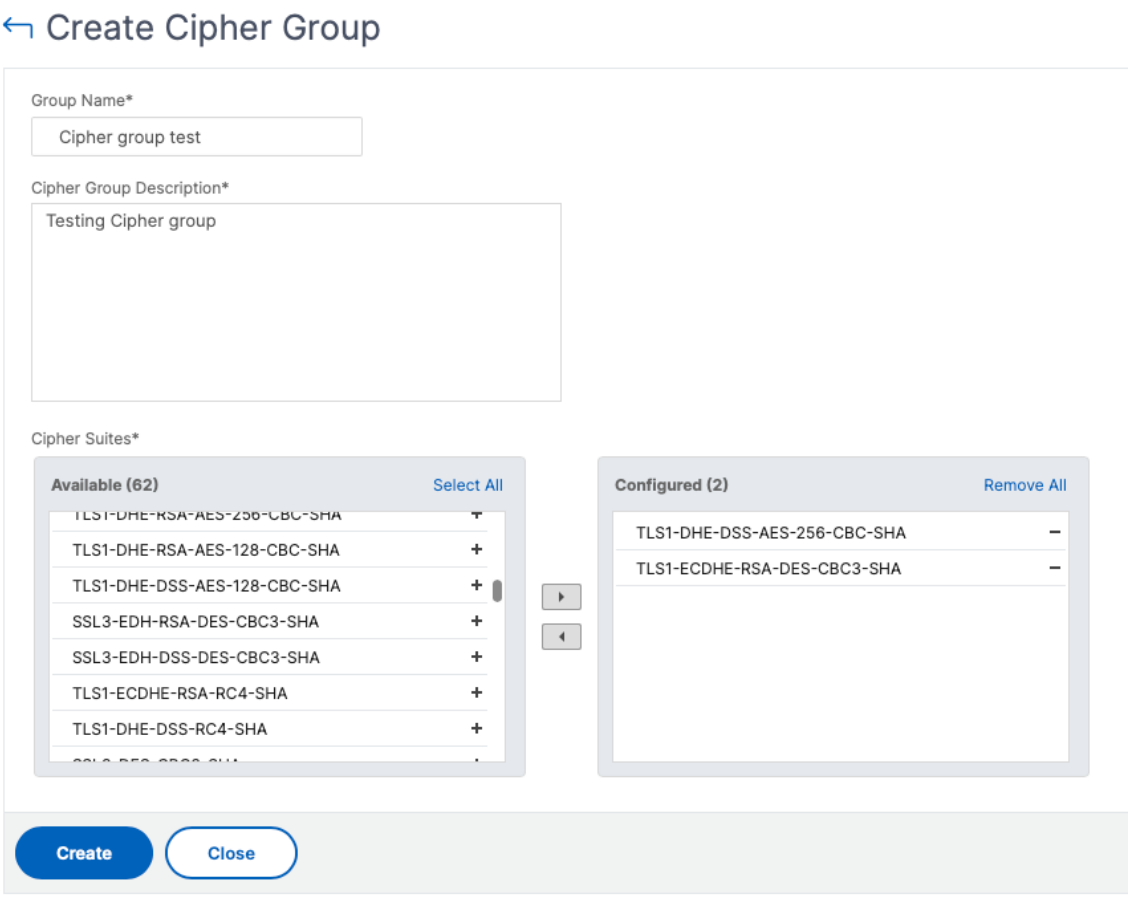
September 27, 2025

A cipher group is a set of cipher suites that you bind to an SSL virtual server, service, or service group on the Citrix NetScaler instance. A cipher suite comprises a protocol, a key exchange (Kx) algorithm, an authentication (Au) algorithm, an encryption (Enc) algorithm, and a message authentication code (Mac) algorithm.

To add a cipher group on NetScaler Console:

1. Navigate to **Settings > Administration**
2. Under **SSL Settings**, click **Cipher Groups**
3. Click **Add**
4. On the **Create Cipher Group** page, enter the following details:
   - **Group Name** - Name for the cipher group.
   - **Cipher Group Description** –Provide a description for your cipher group.
   - **Cipher Suites** –Click Add to select cipher suites from the Available list, and then move the selected (or all) cipher suites to the Configured list.
5. Click **Create**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Create SNMP trap destination, manager community, and users

September 27, 2025

Whenever an abnormal condition occurs on the NetScaler Console, an SNMP trap is generated. The traps are then sent to a remote device called a trap destination server or the *SNMP trap destination*. Here, NetScaler Console is configured as the trap destination. You can query the SNMP agent for system-specific information from a remote device called an *SNMP manager*. The agent then searches the management information base (MIB) for requested data and sends the data to the SNMP manager.

To create an SNMP trap destination on NetScaler Console:

1. Navigate to **System** > **SNMP** > **Trap Destinations**.
2. Under **SNMP Traps**, click **Add** to create an SNMP trap, and then specify the following details:
    - **Version.** Select the SNMP version to use.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Destination Server.** Name or IP address of the trap destination.
- **Port.** Enter the trap destination's port. The port is set to 162 by default.
- **Community.** Specify the community string to use when sending a trap to the trap listener.

3. Click **Create**.

> **Note**
>
> If you are creating an SNMP v3 trap destination, specify the SNMP user credentials to which you want to bind the trap. To add an SNMP user credential, click **Insert** and then add the user from the list of SNMP users available.

To create an SNMP manager community:

1. Navigate to **System** > **SNMP** > **Managers**.
2. Under **SNMP Manager**, click **Add** to create an SNMP manager community, and then specify the following details:
   - **SNMP Manager.** Enter the name or IP address of the SNMP manager.
   - **Community.** Specify the community string to use when sending traps to the trap listener.
3. Optionally, you can select the **Enable Management Network** check box to specify the **Netmask** which is the subnet mask of the SNMP manager network.
4. Click **Create**.

To create an SNMP user:

1. Navigate to **System** > **SNMP** > **Users**.
2. Under **SNMP User**, click **Add**.
3. Enter the user name and assign a security level to the user from the menu.
4. 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.

Configure and view system alarms

September 27, 2025

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

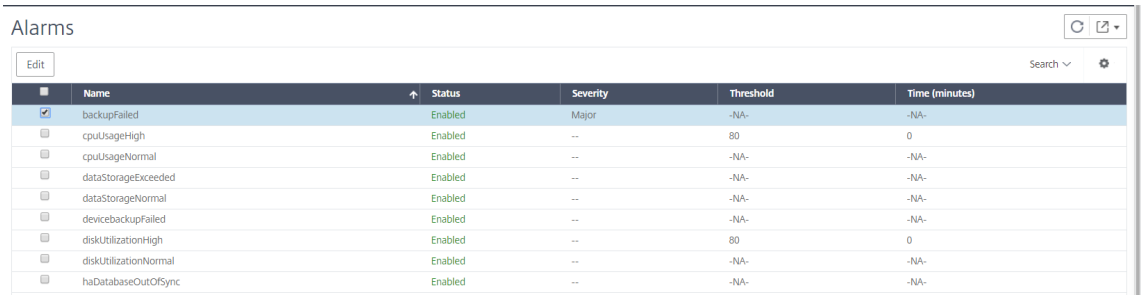
You can assign or modify the severity of an alarm. The severity levels that you can assign are Critical, Major, Minor, Warning, and Informational.

Consider a scenario where you want to monitor whenever there is a failed back up 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 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** on the upper-right corner.



2. Select the alarm you want to configure (for example, backupFailed) and click **Edit** to modify its settings.
3. The alarm is enabled by default. Assign a severity level (example: Major), and then click **OK**.

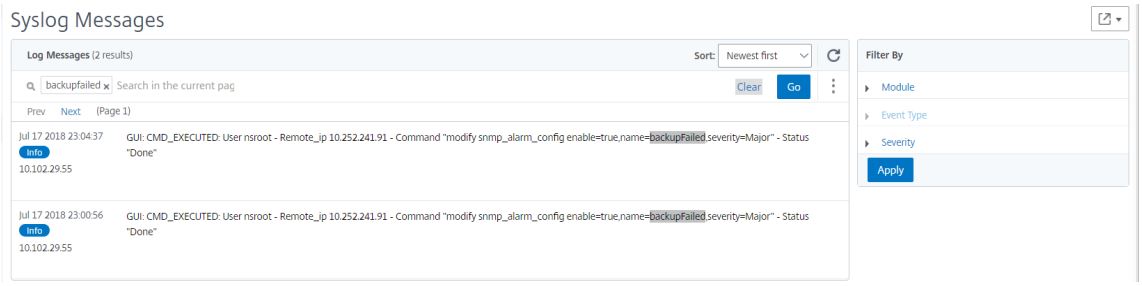
> **Note**
>
> For a few alarms, you cannot set a threshold.
> When the alarm is triggered, you can view the generated event as a syslog message.

To view the event generated by the backupFailed alarm by using NetScaler Console:

1. Navigate to **System** > **Auditing**.
2. In the **Auditing** page, under **Audit Messages**, select **Syslog Messages**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

3. In the search field, type in the name of the alarm.
   In this example, you can see that an event was generated for a failed back up attempt.



   You can also set notifications to send you either an email or an SMS (Short Message Service) text when an alarm is triggered. For information about how to configure system notifications, see How to Configure System Notification Settings of NetScaler Console.

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.

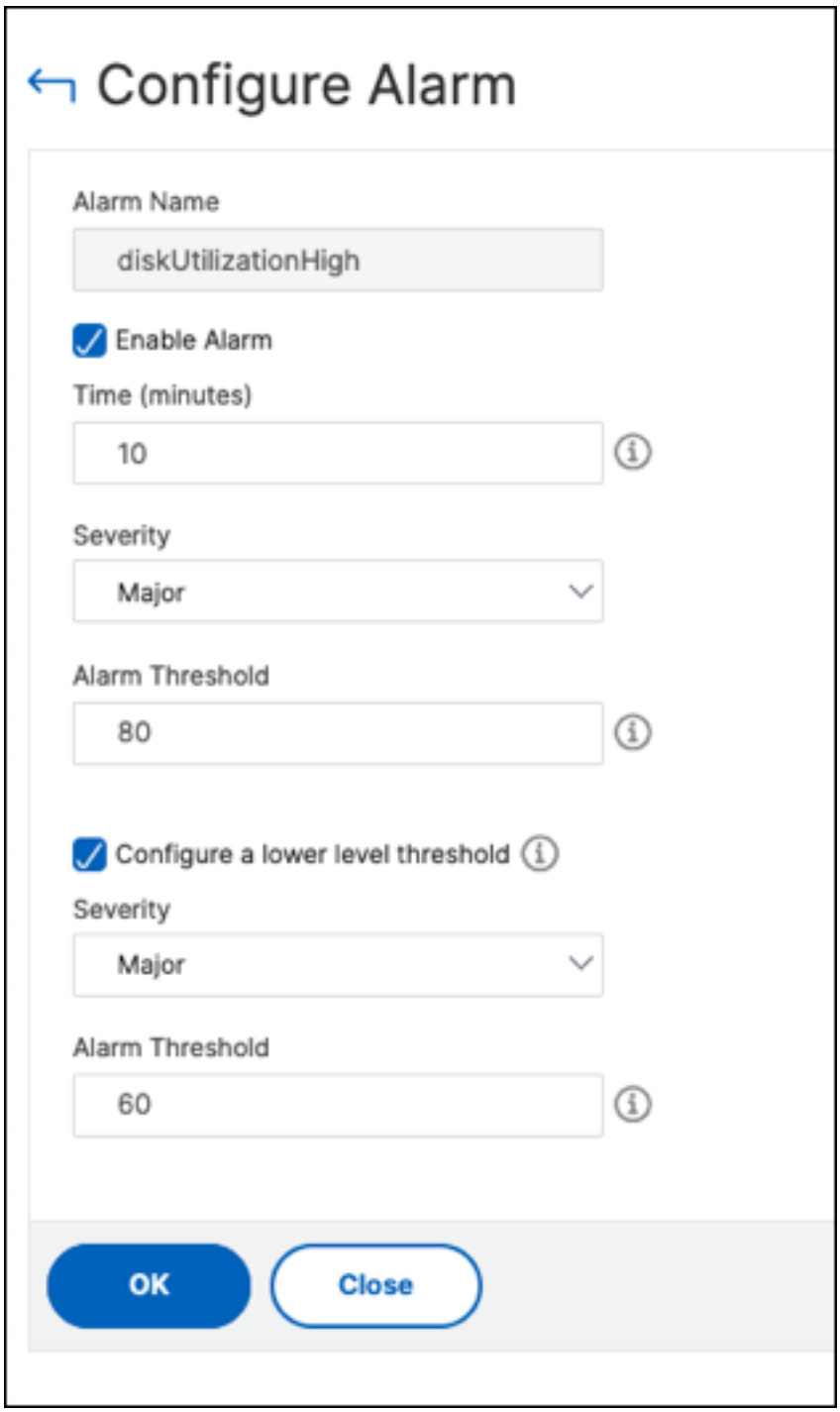
As an admin, when you receive alerts, you can choose to delete unnecessary data or allocate additional storage resources to prevent service disruptions or performance degradation.

Starting from release 14.1-25.x, 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.

Create SNMP managers and users for NetScaler agent

September 27, 2025

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.

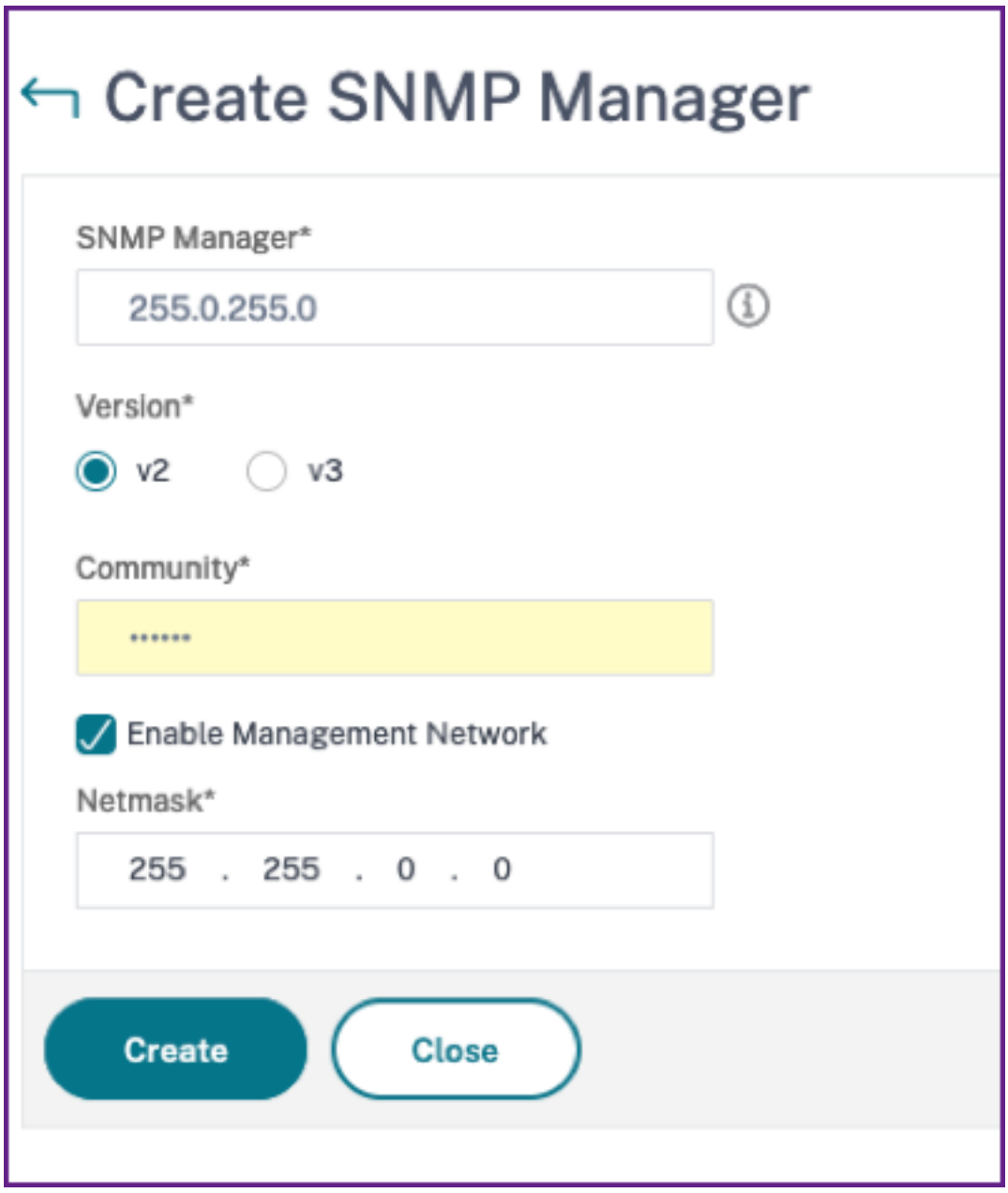
You can add an SNMP manager to query a NetScaler agent. The manager complies with SNMP V2 and V3. If you specify one or more SNMP managers, the NetScaler agent does not accept SNMP queries from any hosts except the specified SNMP managers.

Add an SNMP v2 manager

To add an SNMP v2 manager for the NetScaler agent:

1. Navigate to **Infrastructure > Agents**, select a NetScaler agent, and click **Select Action> Manage SNMP**.
2. In the **SNMP> SNMP Manager** tab, click **Add**.
3. In the **Create SNMP Manager** page, specify the following details:
    - **SNMP Manager**. Enter the name or IP address of the SNMP Manager.
    - **Version**. Select v2.
    - **Community**. Enter a community name. An SNMP community configuration authenticates SNMP queries from SNMP managers.
    - **Enable Management Network**: Select this check box to specify the netmask of the SNMP manager network.
    - **Netmask**: Enter the subnet mask associated with an IP address.
4. Click **Create**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Add an SNMP v3 manager

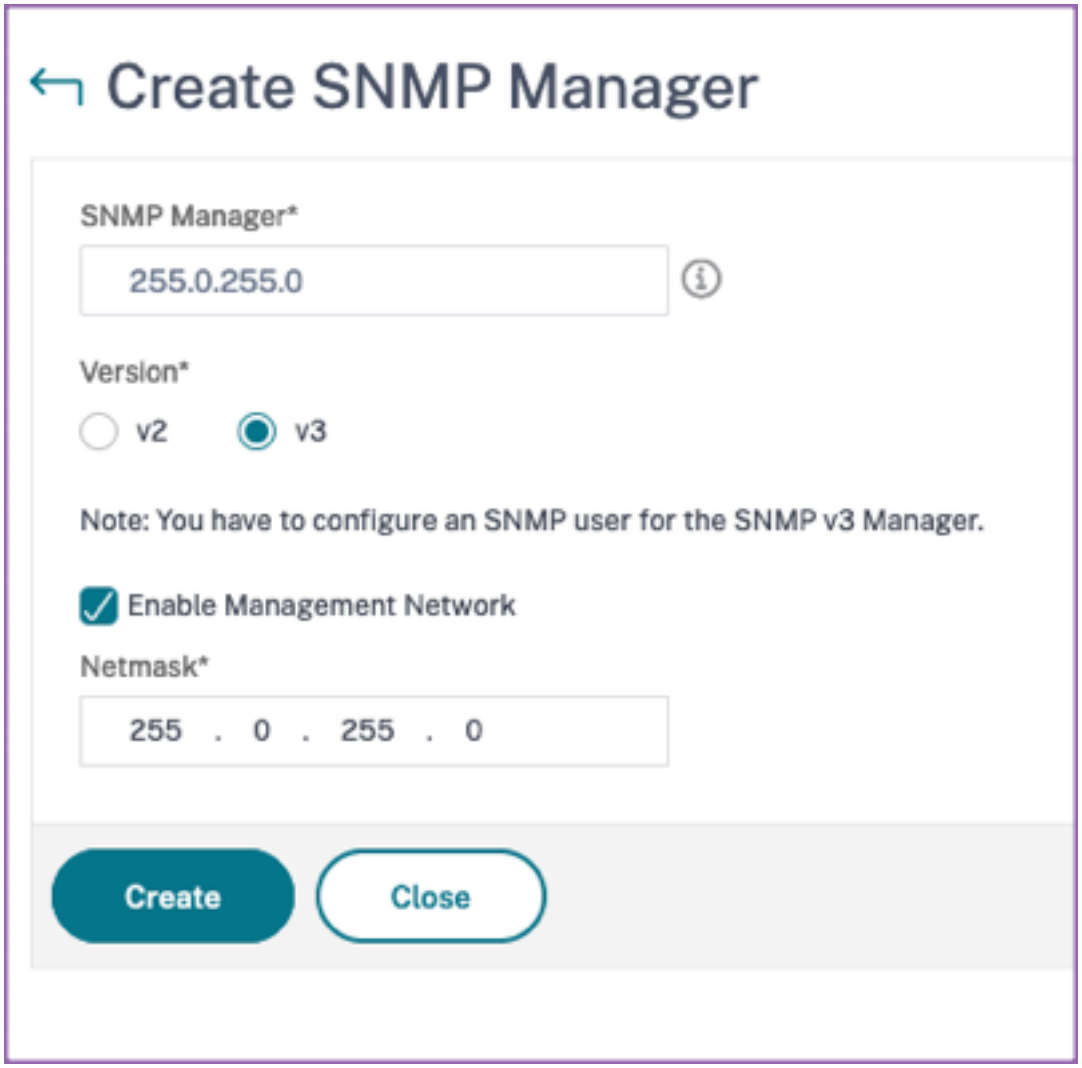
To add an SNMP v3 Manager for the NetScaler agent:

1. Navigate to **Infrastructure > 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:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

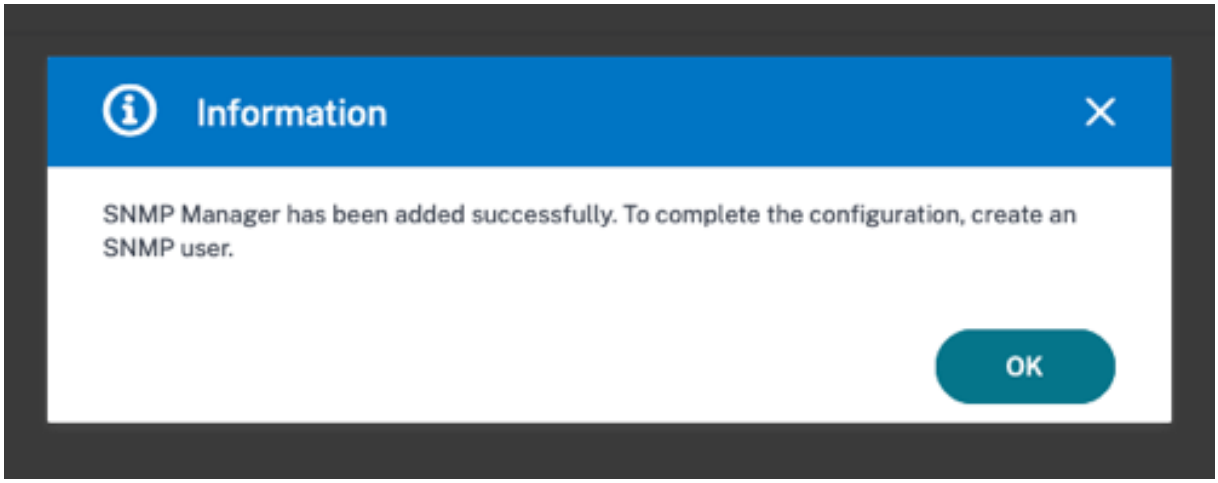
- **SNMP Manager**. Enter the name or IP address of the SNMP Manager.
- **Version**. Select v3.
- **Enable Management Network**: Select this check box to specify the netmask of the SNMP manager network.
- **Netmask**: Enter the subnet mask associated with an IP address.

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**.

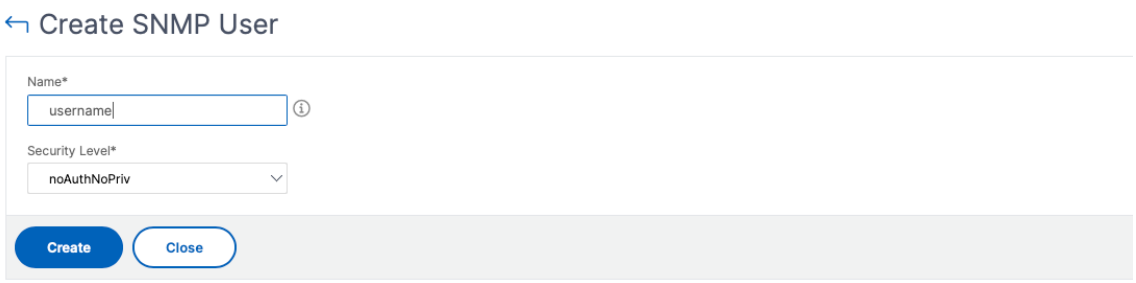
Add an SNMP user

Add an SNMP user to respond to the SNMP v3 queries from an SNMP manager.

To add an SNMP user for the NetScaler agent:

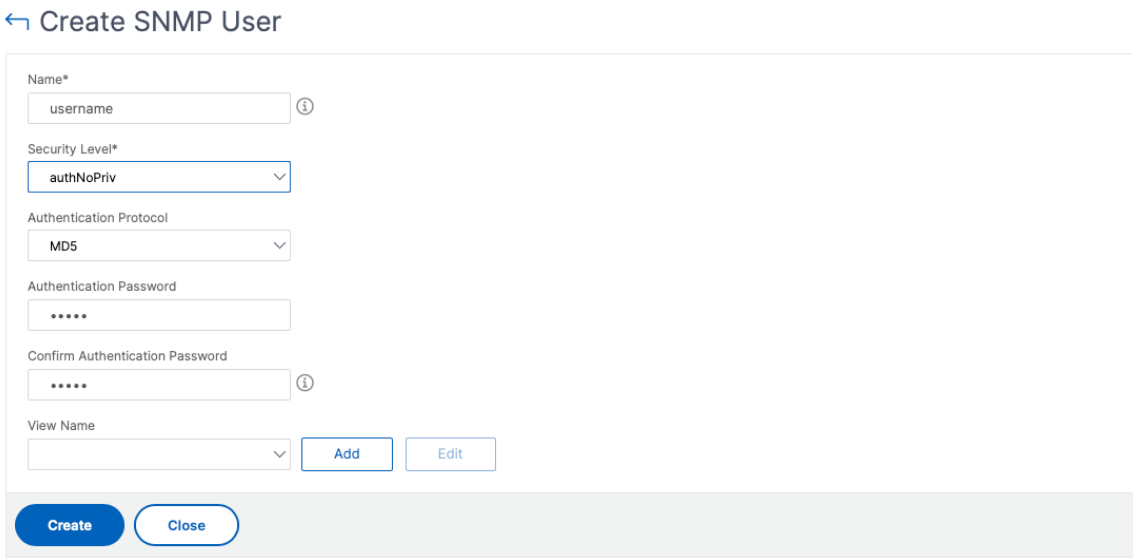
1. Navigate to **Infrastructure > Agents**, select a NetScaler agent, and click **Select Action> Manage SNMP**.
2. In the **SNMP> SNMP User** tab, click **Add**.
3. In the **Create SNMP User** page, add the following details:
    - **Name**. Enter the user name.
    - **Security Level**. Security level required for communication between the NetScaler agent and the SNMP manager.

      Select one of the following security levels:
    - **noAuthNoPriv**. Require neither authentication nor encryption.

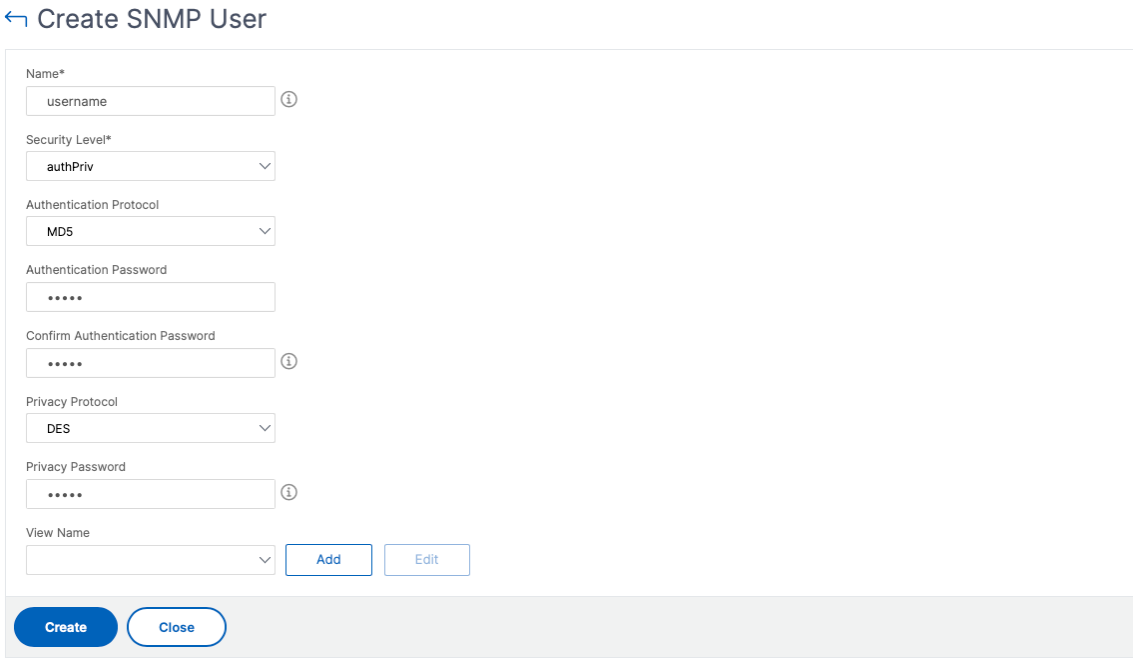


© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **authNoPriv**. Require authentication but no encryption.



- **authPriv**. Require authentication and encryption.



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.

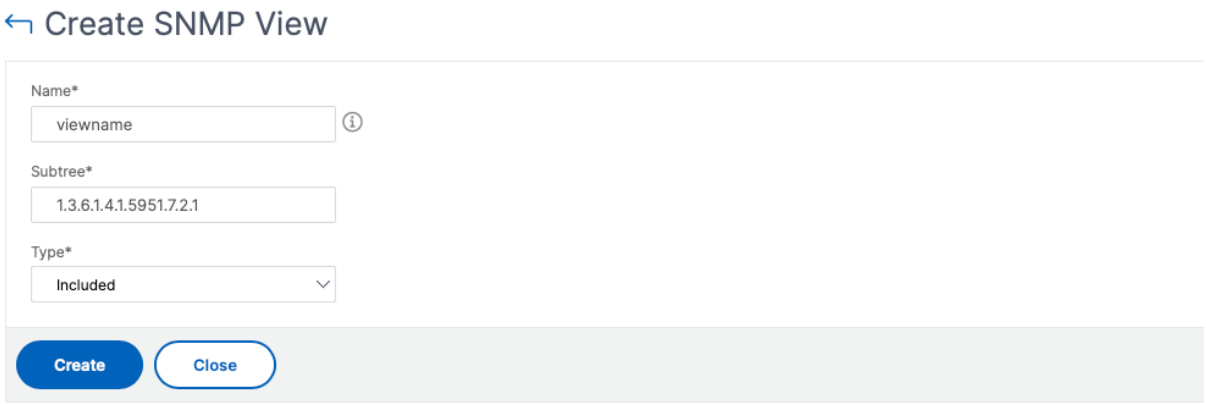
Managing SNMP views

SNMP views are used to implement access control for an SNMP user. The SNMP views restrict the user access to specific portions of MIB.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

To allow or restrict an SNMP OID for the NetScaler agent:

1. Navigate to **Infrastructure > Agents > Manage SNMP** and in the **SNMP View** tab, click **Add**.
2. 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.
3. Click **Create**.



Configure agent settings

September 27, 2025

You can modify the NetScaler Console agent's keep-alive interval and password change requirements.

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 > Administration**.
2. Select **System, Time zone, Allowed URLs and Agent Settings** under **System Configurations**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

3. In **Basic Settings > Agent Settings**, specify the keep-alive interval between 30–120 seconds.
4. Click **Save**.

Change agent's password without the current password

You can allow agent passwords to be changed without their current password.

1. Navigate to **Settings > Administration**.
2. Select **System, Time zone, Allowed URLs and Agent Settings** under **System Configurations**.
3. In **Basic Settings > Agent Settings > Remove current password prerequisite for agent password change** check box, you can do the following:
   - Select the check box to remove the **Current password** field in the **Change Agent Password** page.
   - Clear the check box to keep the **Current password** field in the **Change Agent Password** page.
4. Click **Save**.

> **Note**
>
> To view the **Change Agent Password** page, navigate to **Infrastructure > Instances > Agents**, select an agent, and click **Select Action > Change Password**.

Use Data Storage Management dashboard

September 27, 2025

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- View data ingestion status - The data ingestion activity occurs as long as the consumed storage is within the limits of the entitled storage. When the consumed storage is more than the entitled storage, the data activity is paused.
- Send notifications - You can set notifications to be sent when consumed storage reaches 75% or 100% of the entitled storage, allowing users to manage their storage.
- Flexibility to manage data storage space - You can create more space within the stored data by pruning data that you consider suitable for removal or reduction.

Navigate to **Settings > Data Storage** to view your data storage dashboard.

The following sections outline how to use the **Data Storage Management** dashboard for effective data storage management:

- Understand your data storage - This section helps you understand how you can use the dashboard to view information about your data storage.
- Manage your data storage - This section provides information on what actions you can take in the dashboard to manage your data storage.

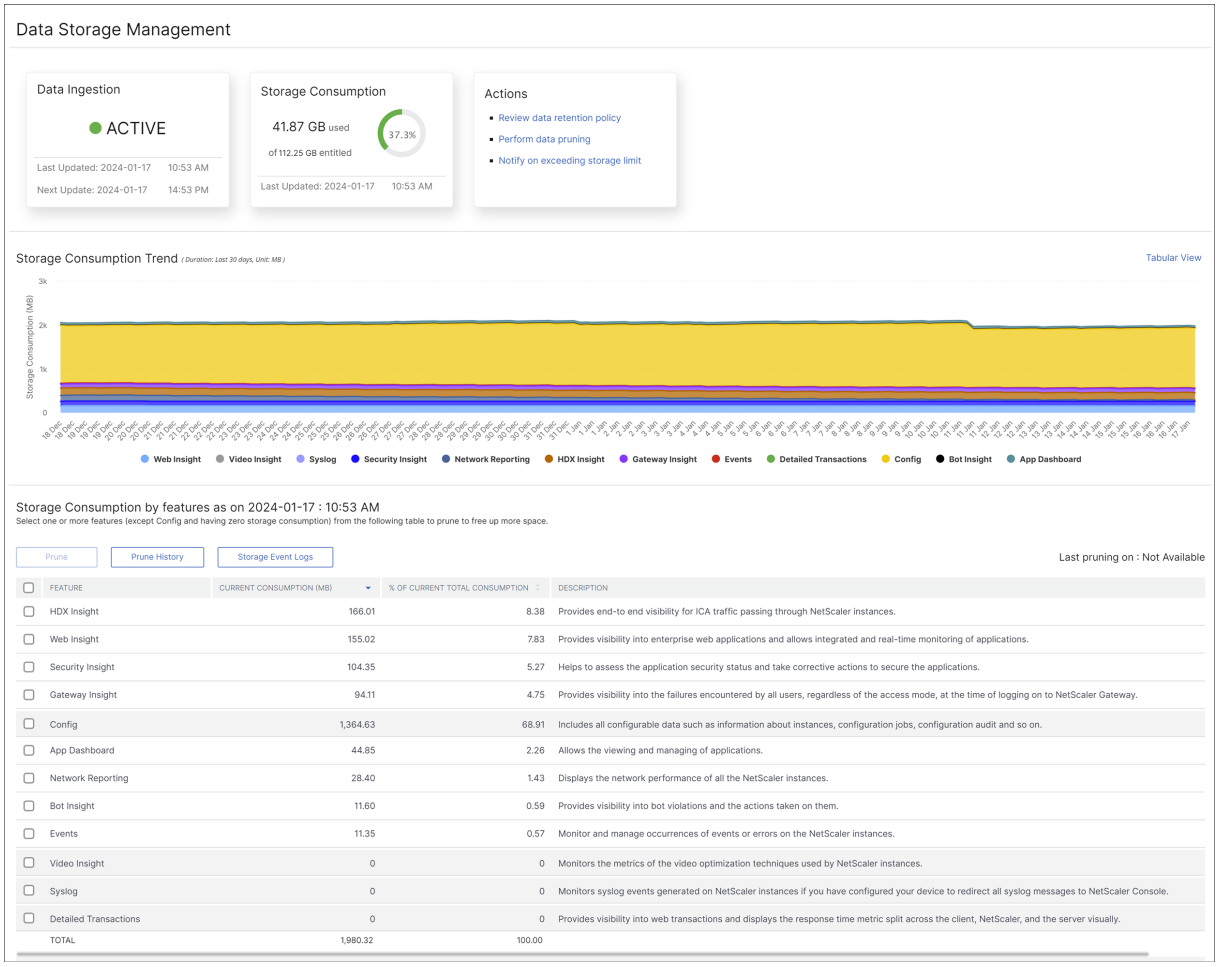
Understand your data storage

September 27, 2025

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**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



The Data Storage Management dashboard indicates the following information:

- State of your data ingestion activity
- Total storage consumption
- Storage consumption trends
- Storage consumption by features

State of your data ingestion activity

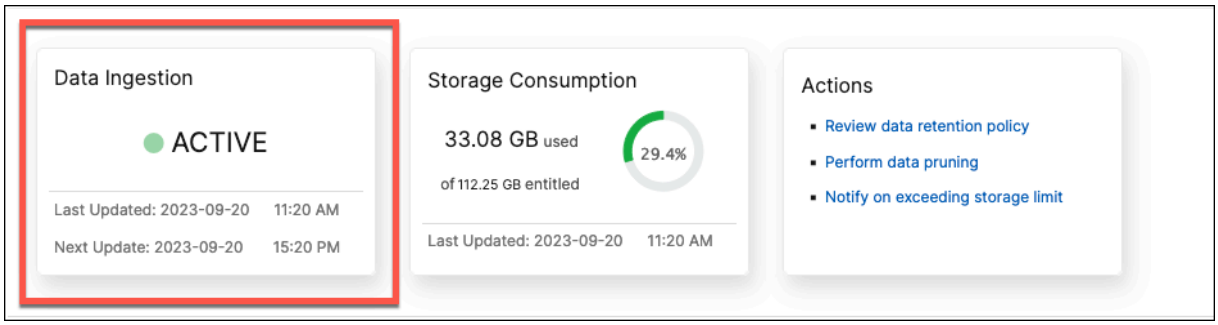
Data ingestion refers to the process of importing large and assorted data from all the managed NetScaler instances across various features like Events, Syslogs, Network Reporting, and so on into the NetScaler Console storage.

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.

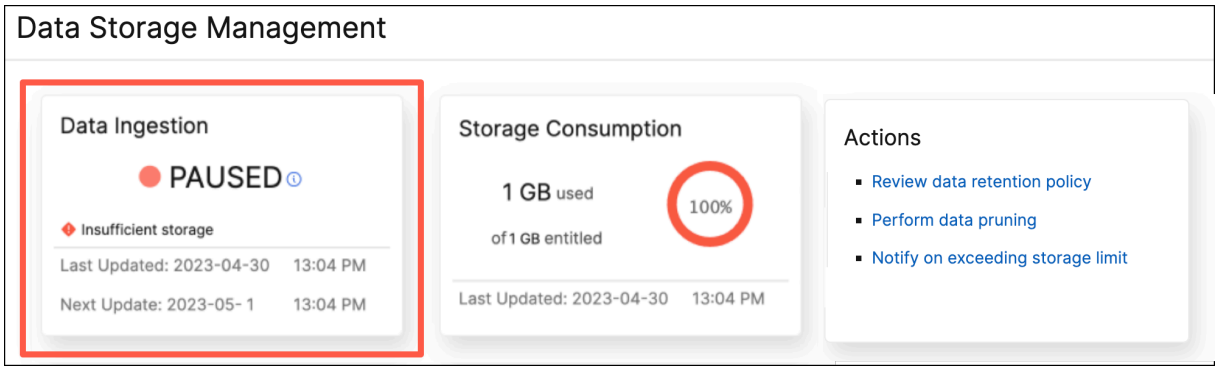
View the **Data Ingestion** tile to understand the current state of data ingestion. This tile displays either of the following two states:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **Active** - The data ingestion activity is in progress.



- **Paused** - The data ingestion activity is paused since the consumed storage exceeds the entitled storage.

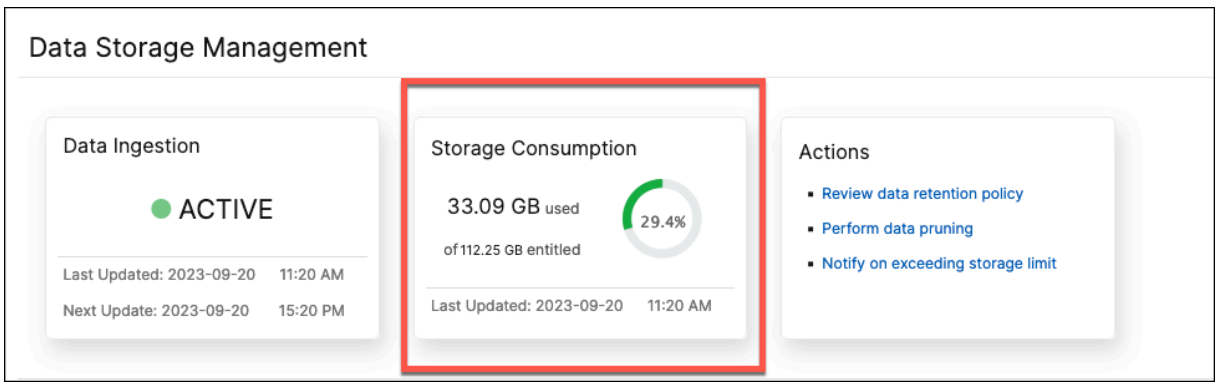


How to resume your paused data ingestion

To resume your data ingestion activity, you can perform data pruning. For more information, see Perform data pruning.

Total storage consumption

For a quick overview of your data storage, view the **Storage Consumption** tile.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

The **Storage Consumption** tile displays the total storage used by all the features in the deployment.

Hover over the donut chart to view the following:

Entitled Storage

The entitled storage is the total storage available for you to use as per your license. If you have an Express license, you get 500 MB of entitled storage. If you have an Advanced license, you get the sum of 500 MB of storage per purchased VIP and any additional storage that was bought directly without buying VIPs.

Consider the following scenarios:

- You bought 20 VIPs. You get 500 MB of free storage for each VIP. Your entitled storage is 20*500 = 10 GB.
- You bought 20 VIPs and an add-on storage of 5 GB. You get 500 MB of free storage for each VIP. Your entitled storage is 20*500 + 5 = 15 GB.

Consumed Storage

The consumed storage is the total storage used by all the features in the deployment. The following color coding criteria specify the amount of storage used by the features:

- **Green** - The consumed storage is less than 75% of entitled storage.
- **Amber** - The consumed storage is between 75% to 99% of entitled storage.
- **Red** - The consumed storage limit has reached or is above the current entitled storage.

Storage consumption trends

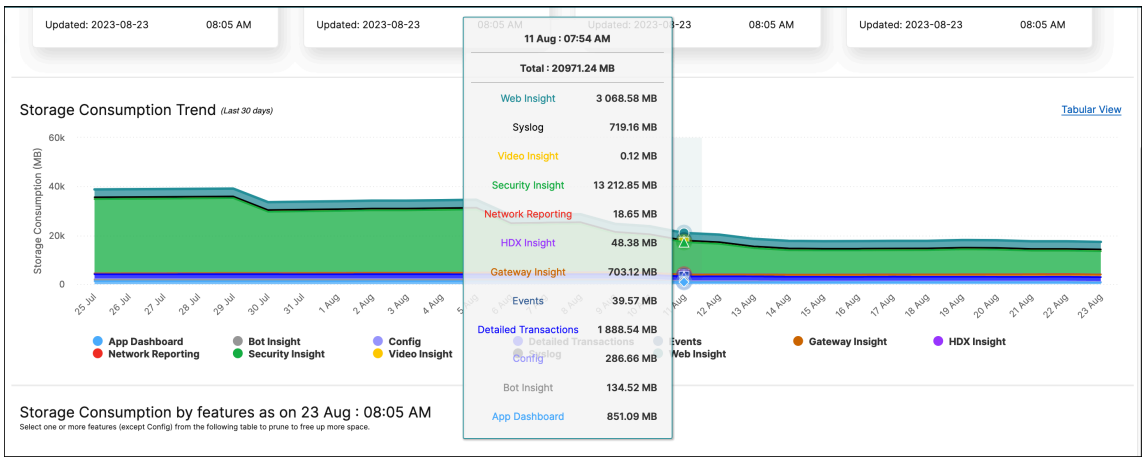
To know how data is being consumed over the last 30 days, view the **Storage Consumption Trend** section.

Storage Consumption Trend provides insights into which features use the most or least storage over a time period and help you effectively manage your data storage consumption.

You can view the storage data trends in either of the following forms:

- **Graphical View** –Displays how the data storage is distributed across the different NetScaler Console features. Hover your mouse over the timeline to view the data storage information for any day of the month.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



> **Note:**
>
> The **Graphical View** is the default view.

- **Tabular View** –Click **Tabular View** to display the data storage information in a table form.



> **Note:**
>
> The tabular view allows you to filter the data by using the search field.

The following table describes the fields displayed in the **Storage Consumption Trend** section:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.
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.

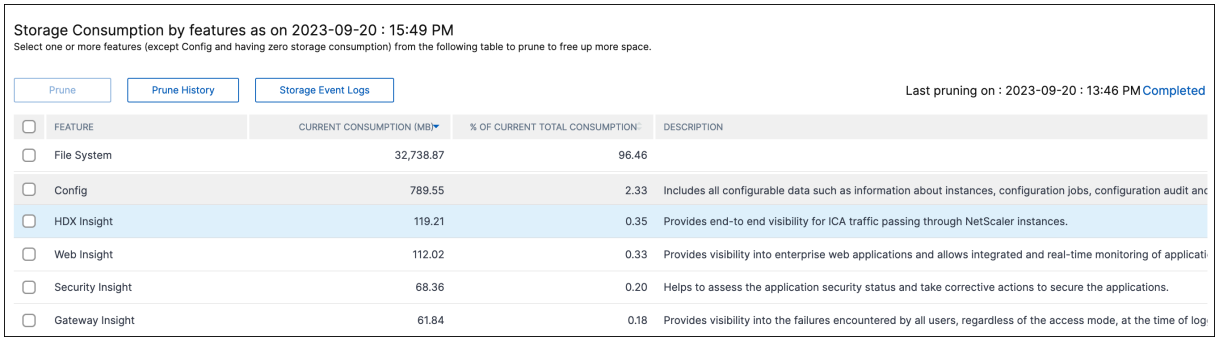
Storage consumption by features

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.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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



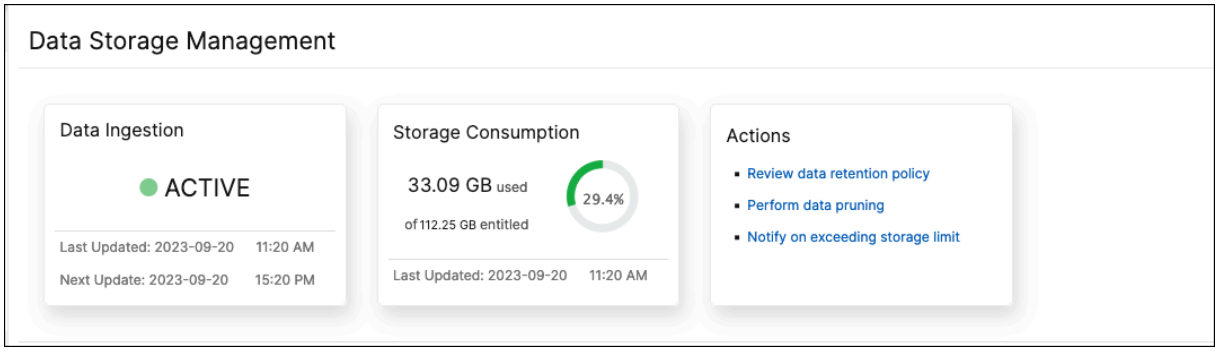
If you want to sort the table entries, the headers of the table. NetScaler Console alpha-numerically sorts the table from top to bottom based on the data in the chosen column. To sort the table in reverse order, click the column heading again.

For information on pruning your data, prune history, and Storage Event logs, see Manage your data storage

Manage your storage space

December 31, 2023

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- Perform data pruning
- Notify on exceeding the storage limit

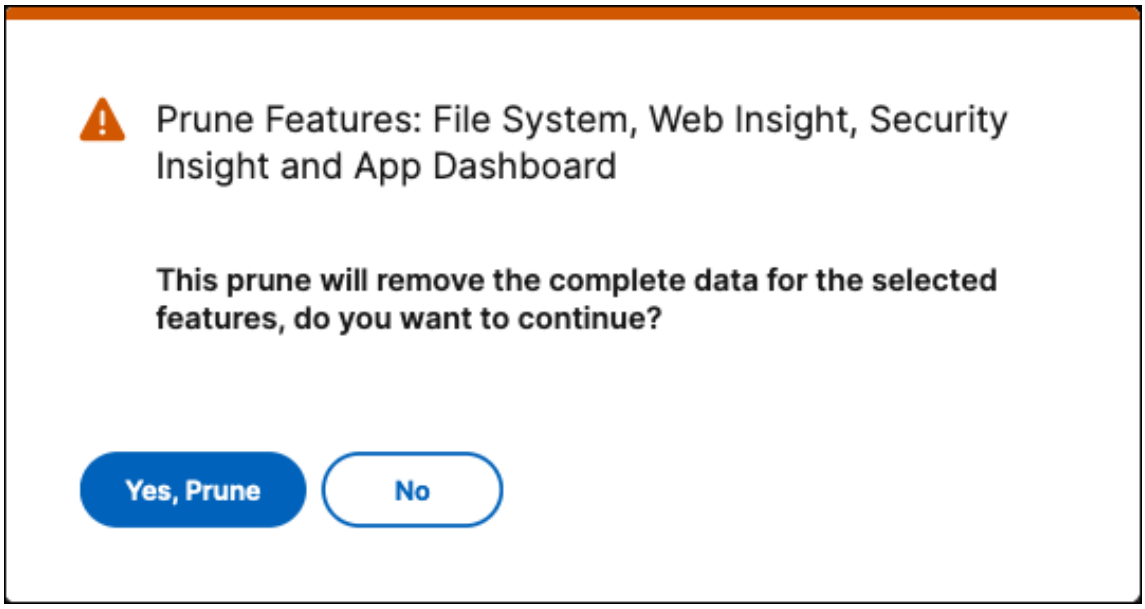
Perform data pruning

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.

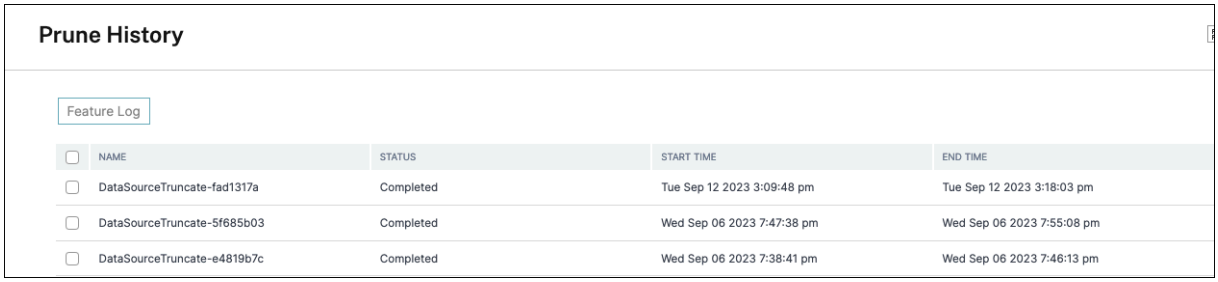
   A pop-up window prompts you to confirm if you want to delete all the data for the selected features. Click **Yes, Prune**.



View prune history

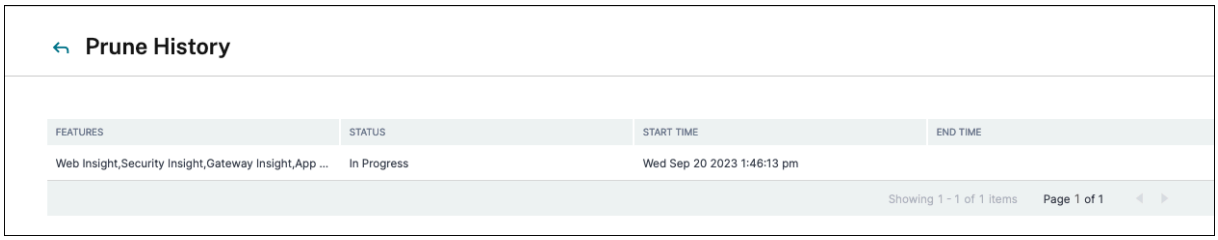
Click **View Prune History** to get details on the all the prune activities that you did in NetScaler Console.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



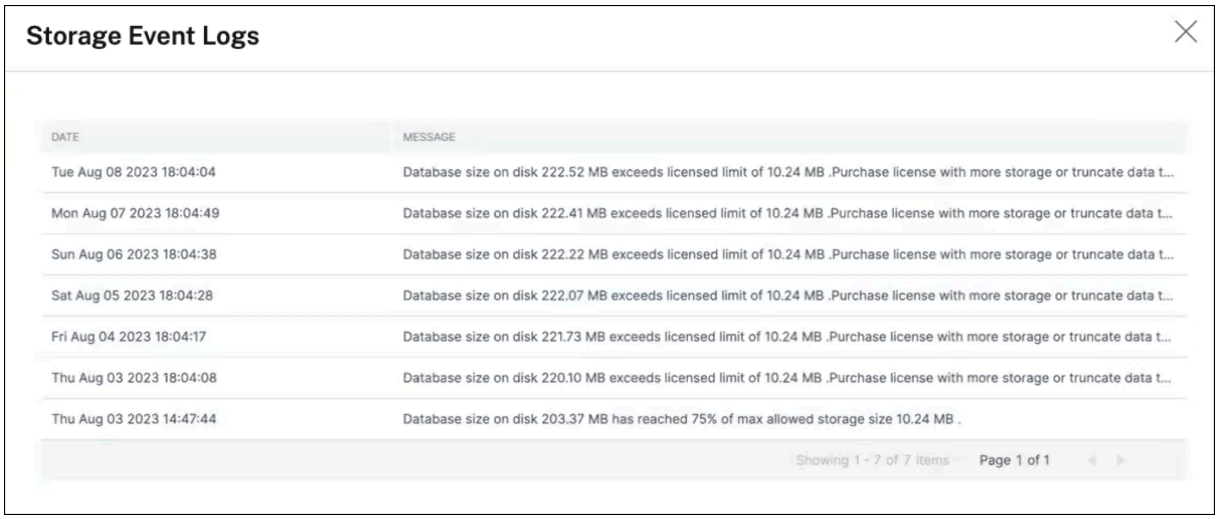
The **Prune Logs: Task Logs** page displays the list of all the prune tasks, including their respective statuses, start time, and end time.

To understand which features were removed in each of the prune operations, select a task and click **Feature Log**.



View storage event logs

Click **Storage Event Logs** to get insights into all the times that your data went over or reached 75% of your licensed limit.



Review data retention policy

The data retention policy refers to a set of rules and configurations that determine how NetScaler Console manages and maintains historical data over time. This policy outlines how long data is stored

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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.

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

September 27, 2025

To limit the amount of reporting data being stored in your NetScaler Console server's database, you can specify the interval for which you want NetScaler Console to keep network reporting data, events, audit logs, and task logs. By default, this data is pruned every 24 hours (at 00.00 hours).

Configure system prune settings

To configure system prune setting:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

1. Navigate to **Settings > Data Storage > Data Retention Policy**.
2. In the **Data Pruning** page, click **System**.
3. In the **System** page, enter the following details:
    - **Data to keep(days)** - Enter the number of days for which the data must be retained. You must specify a value between 1 and 30.
    - **Data Prune Threshold Value (%)** - Enter a threshold limit (in percentage) to set as a condition for data pruning or data cleanup processes. When the data in the database reaches this specified percentage of storage capacity, data pruning procedures are triggered to remove to data and free up space.
    - **Auto Prune Details** - Select **Enable Automatic Data Prune** if you want data pruning to start when either of the following criteria is met:
        - The data threshold value specified in **Data Prune Threshold Value (%)** is reached.
        - The number of days specified in **Data to keep (days)** value is reached.
    - **Data Ingestion Setting** - Enter a threshold limit (in percentage) to set as a condition for data ingestion. When the data in the database reaches this specified percentage, the data ingestion activity is paused. You must specify a limit within the range of 50% to 80%.
4. Click **Save** to save the settings.

Configure instance event prune settings

To limit the amount of event messages data being stored in your NetScaler Console server's database, you can specify the interval for which you want NetScaler Console to retain network reporting data, events, audit logs, and task logs. By default, this data is pruned every 24 hours (at 00:00 hours).

To configure instance event prune settings:

1. Navigate to **Settings > Data Storage > Data Retention Policy**.
2. In the **Data Pruning** page, click **Instance Events**.
3. In the **Data to keep (days)** field, enter the time interval, in days, for which you want to retain data on the NetScaler Console server and click **Save**.

Configure instance syslog prune settings

To limit the amount of syslog data stored in the database, you can specify the interval at which you want to purge syslog data. You can specify the number of days after which the generic syslog data is deleted from NetScaler Console.

To configure instance syslog purge settings:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

1. Navigate to **Settings > Data Storage > Data Retention Policy**.
2. In the **Data Pruning** page, click **Instance Events**.
3. In the **Retain Syslog Generic Data** field, specify the number of days between 1 and 180.
4. Click **Save**.

Configure network reporting prune settings

To limit the network reporting data stored in NetScaler Console, you can specify the interval for which you want to retain the network reporting historical data.

To configure instance event prune settings:

1. Navigate to **Settings > Data Storage > Data Retention Policy**.
2. In the **Data Pruning** page, click **Network Reporting**.
3. In the **Data to keep (days)** field, specify the number of days between 1 and 30.
4. Click **Save**.

NetScaler Console as an API proxy server

September 27, 2025

In addition to being able to receive NITRO REST API requests for its own management and analytics functionality, NetScaler Application Delivery Management (NetScaler Console) can function as a REST API proxy server for its managed instances. Instead of sending API requests directly to the managed instances, REST API clients can send the API requests to NetScaler Console. NetScaler Console can differentiate between the API requests to which it must respond and the API requests that it must forward unchanged to a managed instance.

As an API proxy server, NetScaler Console provides you with the following benefits:

- **Validation of API requests**. NetScaler Console validates all API requests against configured security and role-based access control (RBAC) policies. NetScaler Console is also tenant-aware and ensures that API activity does not cross tenant boundaries.
- **Centralized auditing**. NetScaler Console maintains an audit log of all API activity related to its managed instances.
- **Session management**. NetScaler Console frees API clients from the task of having to maintain sessions with managed instances.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

How NetScaler Console Works as an API Proxy Server

When you want NetScaler Console to forward a request to a managed instance, you configure the API client to include any one of the following HTTP headers in the API request:

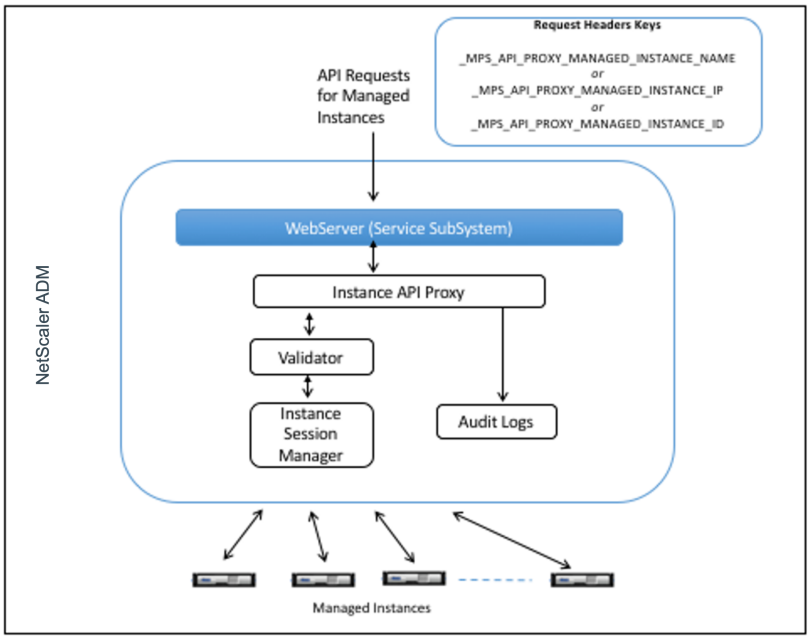
Header values	Description
_MPS_API_PROXY_MANAGED_INSTANCE_NAME	Name of the managed instance.
_MPS_API_PROXY_MANAGED_INSTANCE_IP	IP address of the managed instance.
_MPS_API_PROXY_MANAGED_INSTANCE_ID	ID of the managed instance.
_MPS_API_PROXY_TIMEOUT	Timeout value for a NITRO API request. Set the timeout value in seconds. When you set a proxy timeout, NetScaler Console waits for the specified duration before it times out the request.
_MPS_API_PROXY_MANAGED_INSTANCE_USERNAME	User name to access the managed NetScaler instance.
_MPS_API_PROXY_MANAGED_INSTANCE_PASSWORD	Password to access the managed NetScaler instance.
_MPS_API_PROXY_MANAGED_INSTANCE_SESSID	Session ID to access the managed instance.

> **Note**
>
> In **Settings > Administration > System Configurations > Basic Settings**, if you select **Prompt Credentials for Instance Login**, ensure to configure user name and password of a managed instance. Alternatively, you can also specify the instance session ID.

The presence of any of these HTTP headers helps NetScaler Console identify an API request as one that it must forward to a managed instance. The value of the header helps NetScaler Console identify the managed instance to which it must forward the request.

This flow is depicted in the following figure:

© 1997–2025 Citrix Systems, Inc. All rights reserved.



As shown in the above figure, when one of these HTTP headers appears in a request, NetScaler Console processes the request as follows:

1. Without modifying the request, NetScaler Console forwards the request to the instance API proxy engine.
2. The instance API proxy engine forwards the API request to a validator and logs the details of the API request in the audit log.
3. The validator ensures that the request does not violate configured security policies, RBAC policies, tenancy boundaries, and so on. It performs extra checks, such as a check to determine whether the managed instance is available.

If the API request is valid and can be forwarded to the managed instance, NetScaler Console identifies a session that is maintained by the instance Session Manager and then sends the request to the managed instance.

> **Note**
>
> Ensure the **Prompt Credentials for Instance Login** option is disabled. To do so:
>
> 1. Navigate to **Settings > Administration**.
> 2. In **System Configurations**, select **System, Time zone, Allowed URLs and Message of the day**.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

How to use NetScaler Console as an API proxy server

The following examples show REST API requests that an API client sends to a NetScaler Console server that has an IP address of 192.0.2.5. NetScaler Console is required to forward the requests, unchanged, to a managed instance with IP address 192.0.2.10. All examples use the _MPS_API_PROXY_MANAGED_INSTANCE_IP header.

Before sending NetScaler Console the API requests, the API client must:

- Log in to NetScaler Console
- Obtain a session ID
- Include the session ID in subsequent API requests.

The logon API request is of the following form:

```
POST /nitro/v1/config/login
Content-Type: application/json

{

    "login": {

        "username":"nsroot",
        "password":"nsroot"
      }

 }
```

NetScaler Console responds to the logon request with a response that includes the session ID. The following sample response body shows a session ID:

```
{


  "errorcode": 0,

  "message": "Done",

  "operation": "add",

  "resourceType": "login",

  "username": "***********",

  "tenant_name": "Owner",

  "resourceName": "nsroot",

  "login": [

    {
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
21
22
23        "tenant_name": "Owner",
24
25        "permission": "superuser",
26
27        "session_timeout": "36000",
28
29        "challenge_token": "",
30
31        "username": "",
32
33        "login_type": "",
34
35        "challenge": "",
36
37        "client_ip": "",
38
39        "client_port": "-1",
40
41        "cert_verified": "false",
42
43        "sessionid": "##
      D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D",
44
45        "token": "b2f3f935e93db6a"
46       }
47
48
49    ]
50
51  }
```

Example 1: Retrieve load balancing virtual server statistics

The client must send NetScaler Console an API request of the following form:

```
1     GET /nitro/v1/stat/lbvserver
2     Content-type: application/json
3     _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4     SESSID: ##
         D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
```

Where the value of the Cookie Header is the Session ID returned from the login API call. And the value of the _MPS_API_PROXY_MANAGED_INSTANCE_IP is the IP address of the NetScaler.

Example 2: Create a load balancing virtual server

The client must send NetScaler Console an API request of the following form:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
POST /nitro/v1/config/lbvserver/sample_lbvserver
Content-type: application/json
Accept-type: application/json
_MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
SESSID: ##
   D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D

{

     "lbvserver":{

         "name":"sample_lbvserver",
         "servicetype":"HTTP",
         "ipv46":"10.102.1.11",
         "port":"80"
      }

 }
```

Example 3: Modify a load balancing virtual server

The client must send NetScaler Console an API request of the following form:

```
PUT /nitro/v1/config/lbvserver
Content-type: application/json
Accept-type: application/json
_MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
SESSID: ##
   D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D

{

   "lbvserver":{

        "name":"sample_lbvserver",
        "appflowlog":"DISABLED"
    }

 }
```

Example 4: Delete a load balancing virtual server

The client must send NetScaler Console an API request of the following form:

```
DELETE /nitro/v1/config/lbvserver/sample_lbvserver
Accept-type: application/json
_MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
SESSID: ##
   D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Example 5: Download the CLI running config on the NetScaler

The client must send NetScaler Console an API request of the following form:

```
GET /nitro/v1/config/nsrunningconfig
Accept-type: application/json
_MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
SESSID: ##
   D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
```

FAQs

September 27, 2025

This section provides the FAQ on the following NetScaler Application Delivery Management (NetScaler Console) features. Click a feature name in the following table to view the list of FAQs for that feature.

Analytics	Authentication	Configuration Management
Certificate Management	Deployment	Deployment (Disaster recovery)
Event Management	Instance Management	StyleBooks
System Management		

Analytics

Is it required to enable EUEM virtual channel on NetScaler Gateway instances deployed in single-hop mode?

EUEM virtual channel data is part of HDX Insight data that the NetScaler Console receives from Gateway instances. EUEM virtual channel provides the data about ICA RTT. If the EUEM virtual channel is not enabled, the remaining HDX Insight data are still displayed on NetScaler Console.

The EUEM virtual channel is a default service running on Citrix Virtual Desktop applications (VDA). If it is not running, start the “Citrix End User Experience Monitoring”process in VDA services.

How do I enable NetScaler Console to monitor web-application and virtual-desktop traffic?

1. Navigate to **Infrastructure** > **Instances** > **NetScaler**, and select the NetScaler instance on which you want to enable analytics.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. From the **Select Action** list, select **Configure Analytics**.
3. In the **Configure Analytics** page, select all the virtual servers on which you want to enable analytics, and click **Enable AppFlow**. For more details, see How to Enable Analytics on Instances.

> **Note:**
>
> For NetScaler instances of 11.0 release, 65.30 build and later, there is no option on NetScaler Console to enable Security Insight explicitly. Ensure that you configure the AppFlow parameters on the NetScaler instances, so that NetScaler Console starts receiving the Security Insight traffic along with the Web Insight traffic. For more information on how to set the AppFlow parameters on NetScaler instances, see To set the AppFlow parameters by using the configuration utility.

After I add the NetScaler instances, does NetScaler Console automatically start collecting analytical information?

No. Enable analytics on the virtual servers hosted in NetScaler instances that are managed by NetScaler Console. For more details, see How to Enable Analytics on Instances.

Is it required to access the individual NetScaler appliance for enabling analytics?

No. All configurations are done from the NetScaler Console user interface, which lists the virtual servers hosted on the specific NetScaler instance. For more details, see How to Enable Analytics on Instances.

What are the types of virtual servers that can be listed on a NetScaler instance to enable analytics?

Currently, the NetScaler Console user interface lists the following virtual servers for enabling analytics:

- Load balancing virtual server
- Content switching virtual server
- VPN virtual server
- Cache redirection virtual server

How do I attach an extra disk to the NetScaler Console?

To attach an extra disk to NetScaler Console:

1. Shut down the NetScaler Console virtual machine.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. In the hypervisor, attach an extra disk of the required disk size to the NetScaler Console virtual machine.

   For example, Let us consider that you want to increase the disk space to 200 GB, in a NetScaler Console virtual machine of 120 GB. In this scenario, you must attach a disk space of 200 GB instead of 80 GB. Newly attached 200 GB of disk space will be used to store Database data, NetScaler Console log files. The existing 120 GB disk space is used to store core files, Operating System Log files, and so on.

3. Start the NetScaler Console virtual machine.

What do you mean by collectors are not configured on NetScaler instances?

A collector receives AppFlow records generated by the NetScaler appliance.

NetScaler Console receives Security Insight and Web Insight traffic from the NetScaler instances when the AppFlow feature is enabled. When you enable the AppFlow feature on a NetScaler instance, you must specify at least one collector to which the AppFlow records are sent. If the collectors are not configured on the NetScaler instances, NetScaler Console does not receive the traffic from the instances.

For example, five NetScaler instances are added to NetScaler Console. If collectors are not specified for two instances, no traffic flows to NetScaler Console. Self-service diagnostics detects the issue and displays the issue as "Collectors are not configured on 2 instances."

For more information about how to configure the AppFlow Feature, see Configuring the AppFlow Feature.

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.

Authentication

What is load balancing of authentication requests?

The authentication-server load balancing feature enables NetScaler Console to load balance the authentication requests that are directed to the external authentication servers. Load balancing the authentication servers ensures that the authentication load is split across multiple authentication

© 1997–2025 Citrix Systems, Inc. All rights reserved.

servers and thus avoid an authentication server from being overloaded. You can create an authentication service to connect with and get user information from your existing external authentication server using the authentication protocols like LDAP, RADIUS, or TACACS.

Why do we need to cascade external authentication servers?

Cascaded external authentication servers provide uninterrupted authentication processing, allowing access to legitimate users if an authentication server fails. There is no limitation on which types of authentication servers you can cascade. You can have all RADIUS servers, or all LDAP servers, or a combination of RADIUS and LDAP servers.

How many external authentication servers can I cascade?

You can cascade up to 32 external authentication servers in NetScaler Console.

Do I have an alternative when external authentication fails?

There can be a situation when external authentication completely fails, even when you have cascaded several servers. For example, the external servers can become unreachable, or a new user's credentials might not have been entered in any of the external authentication servers. To prevent locking users out in such a situation, you can enable fallback local authentication. For more details, see Fallback Local Authentication.

What is fallback local authentication?

Fallback local authentication is an option to authenticate your users locally when external authentication fails. If external authentication fails, NetScaler Console accesses the local user database to authenticate your users.

In NetScaler Console, navigate to **Settings > Authentication > Authentication Configuration**. On this page, you can add multiple external authentication servers in a cascade, and you can select the **Enable fallback local authentication** option.

What is an extraction of external user groups?

If you have added external servers for authenticating the users, you can import (extract) existing user groups into NetScaler Console. You have to import user groups once and provide a group permission to a user group rather than importing individual users and giving them individual permissions. You do not have to recreate the users on NetScaler Console.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Why do we need to assign group permissions?

When you are using the load balancing feature of NetScaler, you can integrate NetScaler Console with external authentication servers, and import user group information from the authentication servers. Log in to NetScaler Console and manually create the same group information in NetScaler Console and assign permission to those groups. The user and user group permission is managed in NetScaler Console and not in the external server. The users have different role-based access permissions on the external servers. Configure the same permissions for the users in NetScaler Console also. Instead of configuring permissions individually for each user, you can configure a group-level permission so that the user-group members can access specific services on the load balanced virtual servers. The typical permissions that you can assign are permissions to manage NetScaler instances, NetScaler SDX instances, virtual servers, and so on, so that the users of that group can manage only those instances or virtual servers. You can later edit the permissions given to the users at the group level. You can even remove one or more user groups; other group users still function on NetScaler Console.

Configuration Management

Can I perform configuration across multiple NetScaler instances simultaneously using NetScaler Console?

Yes, you can use configuration jobs to perform configuration across multiple NetScaler instances.

What are configuration jobs on NetScaler Console?

A job is a set of configuration commands that you can create and run on one or more managed instances. You can create jobs to make configuration changes across instances, replicate configurations on multiple instances on your network, and record-and-play configuration tasks using the NetScaler Console GUI. You can also convert the recorded tasks 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.

Can I schedule jobs using built-in templates in NetScaler Console?

Yes! 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 choose to run the job immediately, or schedule the job to be run later.

You can save the configuration of a job that was previously created, and run the job again after modifying the commands, the parameters, the configuration source, and targeted instances. This is useful

© 1997–2025 Citrix Systems, Inc. All rights reserved.

when the same set of commands has to be run on a different instance, or when the job encounters an error and stops further execution.

Certificate Management

Does the deletion of SSL certificates from NetScaler Console lead to the deletion of certificates from NetScaler instances?

No

Deployment

What is the default user name and password?

- After you complete the initial network configuration, you can log on to NetScaler Console from the hypervisor or SSH console, using the default user name and password (nsrecover/nsroot).
- The default user name and password to log on from the GUI is *nsroot/nsroot*.

How to change the default password?

> **Note:**
>
> Starting from Release 14.1-8x, after you log on to NetScaler Console GUI or API with the default credentials for the first time, you are prompted to change the default password.

To change the password:

1. In NetScaler Console, navigate to **Settings > User Administration > Users**.

   The **Users page** is displayed.

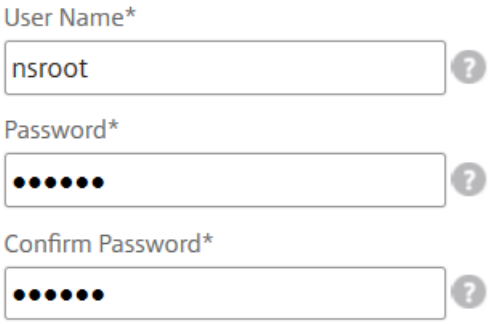
2. Select the user name **nsroot** and click **Edit**.

   The **Configure System User** page is displayed.

3. Select **Change Password** and create a password of your choice.

© 1997–2025 Citrix Systems, Inc. All rights reserved.



4. Click **OK**.

   You can now use the new password to log on from the GUI, hypervisor, or SSH console.

   > **Note:**
   >
   > You cannot modify the user name.

How to reset the password?

You can see this documentation to reset the password.

In a HA pair, if the password is changed in the primary node and if the Break HA pair option is selected later, what is the behavior?

You can log on to both standalone nodes using your new password.

If two standalone servers have different passwords, what is the impact in deploying these two servers in HA pair?

It is recommended to have default password for both servers when you deploy two standalone servers to HA pair.

The HA configuration is complete, but the primary node GUI is not accessible. What can be the reason?

It takes a few minutes for the configuration to take effect. You can try accessing again after a few minutes.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

The HA configuration is complete, but the floating IP address GUI is not accessible. What can be the reason?

After the HA configuration, you need to first access the primary node GUI and complete the deployment. For more information, see Deploy the primary and secondary node as a high availability pair. After the deployment is complete, the server reboots and gets ready for high availability deployment. You can then access the floating IP address GUI.

What DB is supported in NetScaler Console standalone and NetScaler Console HA?

Both NetScaler Console standalone and NetScaler Console HA support PostgreSQL.

What is the potential data loss to the secondary node?

The secondary node listens to the heartbeat messages that the primary node sends through the NetScaler Console database. If the secondary node does not receive the heartbeats for more than 180 seconds, then the secondary node performs an SSH-based check on the primary node. If the heartbeat and SSH-based check fail, the primary node is considered to be down.

In this scenario, the secondary node takes over as the primary node and the 180 seconds timeframe can be considered as the possible data loss to the secondary node.

What happens if the primary node is down?

The secondary node takes over and becomes the primary node.

How to reinstall the failed node?

It is recommended to install a fresh VM build. To reinstall:

1. Break the HA pair. Navigate to **Settings > Deployment**

   The deployment page is displayed. Click **Break HA**
2. Delete the failed node from the hypervisor.
3. Import the .XVA image file to the hypervisor.
4. From the Console tab, configure NetScaler Console with the initial network configurations. For more information, see Register and deploy the first server (primary node) and Register and deploy the second server (secondary node).
5. Redeploy the HA pair.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Does NetScaler Console support SAN Storage?

We recommend you to host the NetScaler Console VHD on a local storage. When hosted on storage devices in a SAN, NetScaler Console might not work as expected. So, NetScaler Console deployment on SAN is not supported.

Does NetScaler Console support an extra disk?

Yes. A new installation of NetScaler Console HA pair allocates 120 GB of storage by default. For more than 120 GB storage, you can add one extra disk for a maximum of 3 TB storage. Adding more than one extra disk is not supported.

After disabling the HA pair, what happens to the floating IP address configured?

The floating IP address is no longer accessible and you need to redeploy the high availability pair.

Can I give a different floating IP address while redeploy?

Yes. You can configure a new floating IP address.

Why is secondary node GUI not accessible?

Secondary node is only a read-replica server and acts as a primary node only if the primary node is down for any reason. We recommend accessing either the primary node GUI or the floating IP address GUI.

If the primary node is down for a long duration, can the configurations still be done using the floating IP address GUI?

Yes. You can still continue to do configurations and the configurations get saved in the secondary node. After the primary node is back, all the configurations are synchronized.

If there is a necessity to change the primary node IP address or secondary node IP address or floating IP address in the future (for example, changing it to IPv6), what are the recommended solutions to follow?

Changing the IP addresses in HA pair is not supported without breaking the HA pair.

To update the primary node or the secondary node IP address:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

1. Break the HA pair. Navigate to **Settings > Deployment**.

   The Deployment page is displayed. Click **Break HA**

   a) Log on to the primary node using an SSH client or from the hypervisor.

   b) Use `nsrecover` as the user name and enter the password that you have set.

   c) Enter **networkconfig**. Perform the procedure from **step 3** available at Register and deploy the first server (primary node).

      During the initial network configuration, you can provide a different IP address.

   d) Perform the same procedure for secondary node and continue with the procedure from **step 3** available at Register and deploy the second server (secondary node).

To update the floating IP address:

1. Navigate to **Settings > Deployment**.

   The Deployment page is displayed.

   a) Click **HA Settings**.

   b) Click **Configure Floating IP Address for High Availability Mode**.

   c) Enter the floating IP address and click **OK**.

Does NetScaler Console support AMD processors?

AMD processor is supported in:

- **NetScaler Console 13.1 build 4.43 or later**.
- **NetScaler agent 13.1 build 17.42 or later**.

Deployment (Disaster Recovery)

How frequent does the replication happens between the primary site and disaster recovery site?

The replication between the primary site and the disaster recovery site is real time.

After initiating the backup script at the DR site, does the DR site becomes the temporary primary site, until the primary site is recovered and fully operational?

No. The DR site will now become the primary site. To revert the HA pair as the primary site, see Revert configurations to the original primary site

© 1997–2025 Citrix Systems, Inc. All rights reserved.

If the Break HA pair option is selected, both nodes operate as a standalone server. Since DR support is not applicable for standalone server, what happens to the DR site if Break HA pair is selected?

If you select Break HA pair option, the replication between the primary site and the DR site is terminated. You need to reconfigure the DR site as part of redeploying HA pair.

Event Management

How can I keep track of all the events that have been generated on my managed NetScaler instances using NetScaler Console?

As a network administrator, you can view details such as configuration changes, log on conditions, hardware failures, threshold violations, and entity state changes on your NetScaler instances, along with events and their severity on specific instances. You can use the NetScaler Console events dashboard to view reports generated for critical event severity details on all your NetScaler instances.

What are event rules?

Using NetScaler Console, you can configure rules to monitor specific events. Event Rules make it easier to monitor many events generated across your NetScaler Console 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, and failure objects. The actions you can assign to the events are sending an email notification, forwarding SNMP traps from managed NetScaler instances to the NetScaler Console, and sending an SMS notification.

Instance Management

What happens if a NetScaler instance cannot connect to NetScaler Console after bandwidth allocation when you use NetScaler pooled capacity licensing?

If the heartbeat between the NetScaler instance and NetScaler Console fails, the instance enters a grace period of 30 days. And after communication is re-established, pooled capacity licensing starts working. When in grace period, NetScaler functions are not affected. After 30 days of grace period, the NetScaler instance initiates warm restart and is unlicensed.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

What are data centers in NetScaler Console?

A NetScaler Console data center is a logical grouping of the NetScaler instances in a specific geographical location. Each server can monitor and manage several NetScaler instances within a data center. You can use the NetScaler Console server to manage data such as syslog, application traffic flow, and SNMP traps from the managed instances. For more details on configuring data centers, see How to Configure Data Centers for Geomaps in NetScaler Console.

What are the different NetScaler appliances that are supported by NetScaler Console?

Instances are the NetScaler appliances or virtual appliances that you want to discover, manage, and monitor from NetScaler Console. You must add these instances to the NetScaler Console server. You can add the following NetScaler appliances and virtual appliances to NetScaler Console:

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler Gateway

You can add instances either while setting up the NetScaler Console server for the first time or later.

What is an instance profile?

An instance profile is used by NetScaler Console to access an instance.

An instance profile contains the user name and password for access to one or more instances. A default profile is available for each instance type. For example, the ns-root-profile is the default profile for NetScaler instances. It contains the default NetScaler administrator credentials. When you change the credentials required for access to instances, you can define custom instance profiles for those instances.

Can I rediscover multiple NetScaler VPX instances in NetScaler Console?

Yes, you can rediscover multiple Citrix **VPX** instances in NetScaler Console to learn the latest states and configurations of the instances.

Navigate to **Infrastructure > Instances > NetScaler > VPX**, select the instances that you want to rediscover, and in the **Action** list click **Rediscover**. For more information, see How to Rediscover Multiple VPX Instances.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Can NetScaler Console be installed on NetScaler SDX?

No

Can I add a NetScaler instance on the NetScaler Console software by using a public IP address?

Yes, you can by using network address translation (NAT).

- For adding a single instance: use NAT IP of the public IP address of the NetScaler instance.
- For adding a NetScaler HA pair: add the NAT IP addresses of the HA pair in this format:

  <NAT **public** IP of the primary instance>#<NAT **public** IP of the secondary instance>
- For adding a NetScaler cluster: add all the NAT public IP addresses of all the instances in the cluster, each separated by a comma, and add the NAT IP of the CLUSTER IP inside parentheses or round brackets. An example format: NAT1, NAT2, NAT3,(NATIP of CLUSTERIP).

For more information, see the following topics:

- Add instances to NetScaler Console
- Configuring Network Address Translation

How to register a disaster recovery node if the DR node credentials are changed?

Reset the disaster recovery (DR) node credentials to `nsrecover`/`nsroot` using the following command:

```
./mps/change_freebsd_password.sh <username> <password>
```

To register a DR node, follow the steps in Deploy and register the NetScaler Console DR node using DR console.

StyleBooks

Can StyleBooks be used to configure different NetScaler instances running on different versions of the NetScaler software?

Yes, you can use StyleBooks to configure different NetScaler instances running on different versions if there is no discrepancy between the commands across different versions.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

When a StyleBook is used to configure multiple NetScaler instances at the same time, and configuration of one NetScaler instance fails, what happens?

If applying the configuration to a NetScaler instance fails, the configuration is not applied to any more instances, and already-applied configurations are rolled back.

Do NetScaler backups made through NetScaler include configurations applied through StyleBooks?

Yes

System Management

Can I assign a host name to my NetScaler Console server?

Yes, you can assign a host name to identify your NetScaler Console server. To assign a host name, navigate to **System**> **System Administration** > **System Settings**, and click **Change Hostname**.

The host name is displayed on the Universal license for NetScaler Console. For more information, see How to Assign a Host Name to a NetScaler Console Server.

Can I back up and restore my NetScaler Console configuration?

Yes, you can back up configuration files (NTP files and SSL certificates), system data, infrastructure and application data, and all your **SNMP** settings. If your NetScaler Console ever becomes unstable, you can use the backed-up files to restore your NetScaler Console to a stable state.

To back up and restore your NetScaler Console configuration, navigate to **System** > **Advanced Settings** > **Backup Files**, and click **Back Up** or **Restore** as the case might be. For more information, see How to back up and Restore Configuration on NetScaler Console.

We recommend that you use this feature before performing an upgrade or for precautionary reasons.

What are Thresholds and Alerts on NetScaler Console?

You can set thresholds and alerts to monitor the state of a NetScaler instance and monitor entities on managed instances.

When the value of a counter exceeds the threshold, NetScaler Console generates an alert to signify a performance-related issue. When the counter value returns to the clear value specified in the threshold, the event is cleared.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Can I generate a technical support file for NetScaler Console?

Yes. We recommend that you generate an archive of NetScaler Console data and statistics before contacting technical support for debugging an issue. The archive is a TAR file that you can send to the technical support team.

You can generate a technical support file that contains debug logs, the duration for which debug logs were collected, and distinct and diverse logs from the NetScaler Console database.

To configure and send a technical support file, navigate to **System** > **Diagnostics** > **Technical Support**, and then, click **Generate Technical Support File**. For more information, see How to Generate a Tech Support File for NetScaler Console.

What is syslog purging?

Syslog is a standard protocol for logging. Syslog enables isolation of the system that generates information and the system that stores the information. You can consolidate logging information and derive insights from the collected data. You can also configure syslog to log different types of events.

To limit the amount of syslog data stored in the database, you can specify the interval at which you want to purge syslog data. You can specify the number of days after which all Generic Syslog data, AppFirewall data, and NetScaler Gateway data will be deleted from NetScaler Console.

Can I configure NTP server on NetScaler Console?

You can configure a Network Time Protocol (NTP) server in NetScaler Console to synchronize the NetScaler Console clock with the NTP server. Configuring an NTP server ensures that the NetScaler Console clock has the same date and time settings as the other servers on the network.

To configure an NTP server, navigate to **System** > **NTP Servers**, and then click **Add**. For more information, see How to Configure NTP Server on NetScaler Console.

From which version is the NetScaler Console active-passive HA deployment supported?

The NetScaler Console active-passive HA deployment mode is supported from NetScaler Console version 12.0 build 51.24.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

I had a NetScaler Console active-active HA setup and had configured a NetScaler appliance with load balancing virtual server on it for unified GUI access. How do I update this configuration?

After you upgrade the NetScaler Console HA pair to active-passive mode, you have to run the following command on the NetScaler appliance to update the load balancing configuration:

add lb monitor MAS_Monitor **TCP-ECV -send "GET /mas_health HTTP/1.1\r\nAccept-Encoding: identity\r\nUser-Agent: NetScaler-Monitor\r\nConnection: close\r\n\r\n"" -recv "{\"status-code\":0, \"is_passive\":0}"-LRTM DISABLED**

Can I configure load balancing of the NetScaler Console HA pair on a NetScaler Instance using port 443?

No, you cannot configure load balancing of the NetScaler Console HA pair on a NetScaler Instance using port 443.

When you configure the `http-ecv` and `https-ecv` monitors on NetScaler, it does not monitor the NetScaler Console HA nodes correctly.

Can a NetScaler Console server backup file be used to restore the configuration of another NetScaler Console server?

Yes

After NetScaler Console backs up a NetScaler instance, can that backup file be used to restore the configuration of another NetScaler instance through NetScaler Console?

Yes. Download the NetScaler Console backup file, upload it into another NetScaler instance's backup repository, and restore that instance. Make sure that the network information and authentication information do not conflict. For example, check for IP-address or port conflicts, mismatched password profiles. Also make sure that the restored VPX instance has the same NSIP address and NetScaler license as the one that was backed up.

Before restoring an instance in a high availability pair, make sure the IP addresses and state (primary or secondary) stored in the backup file match those of the original HA configuration. Also verify that the new primary and secondary have the same type of NetScaler license.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Can we force NetScaler Console to use a SNIP address to communicate with the NetScaler instances, instead of using the NSIP address of the NetScaler Console server?

Yes, you can add a SNIP address (with management enabled) in NetScaler Console for communication with NetScaler instances.

When I back up NetScaler Instances in NetScaler Console, is the result a full back-up or a basic back-up?

Backups of NetScaler instances by NetScaler Console are full backups.

Is there a troubleshooting guide for NetScaler Console?

Yes. See https://support.citrix.com/article/CTX224502.

How are NetScaler instances managed when a NetScaler Console HA failover occurs?

If the heartbeat and SSH based check fails, the primary node is considered to be down and the secondary node takes over as the primary node. All the NetScaler instances are updated with the latest primary node details as their SNMP trap destination by default.

The new primary (active) NetScaler Console node checks to determine whether the previously active node was configured as the AppFlow collector or syslog server, if it was, the new primary adds the AppFlow collector or syslog server details to the information sent to the instances.

For syslog it replaces the old server details.

What happens when the NetScaler Console HA node that went down comes back up?

After returning to service, the NetScaler Console node remains passive unless the active node fails over

How are NetScaler instances distributed across NetScaler Console HA nodes?

All the NetScaler instances are managed by the primary NetScaler Console node.

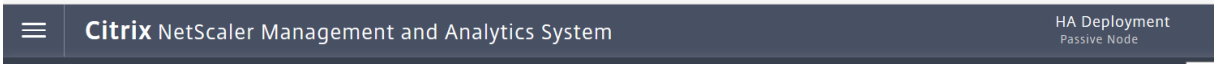
© 1997–2025 Citrix Systems, Inc. All rights reserved.

How are virtual server licenses managed if there is NetScaler Console HA failover?

If the NetScaler Console primary node on which virtual server licenses are applied goes down, the new primary node manages the virtual server licenses for a grace period of 30 days. Reapply the licenses on the new primary before the end of the grace period. For alternatives, contact NetScaler support.

Is a load balancer mandatory for a NetScaler Console HA setup?

No, but if there is no load balancer, NetScaler Console nodes must be accessed through their own IP addresses. The passive node is marked with the tag "Passive", and we recommend not to create any configurations on the passive node.



Does NetScaler Console support an external database?

No

Can a NetScaler instance that is being managed by NetScaler Console be used as a Load balancer for NetScaler Console HA?

Yes

What data is synchronized between NetScaler Console HA nodes?

Complete NetScaler Console database is synchronized, and the following folders are synchronized:

- /var/mps/tenants/root/
- /var/mps/ns_images/
- /var/mps/sdx_images/
- /var/mps/xen_nsvpx_images/
- /var/mps/cbwanopt_images/
- /var/mps/sdwanvw_images/
- /var/mps/mps_images/
- /var/mps/ssl_certs/
- /var/mps/ssl_keys/
- /mpsconfig/ssl/
- /var/mps/backup/
- /var/mps/esx_nsvpx_images/
- /var/mps/locdb/

© 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.