NetScaler Gateway 14.1

Contents

NetScaler Gateway Release Notes

January 8, 2024

Release notes describe how the software has changed in a particular build, and the issues known to exist in that build.

The release notes document includes all or some of the following sections:

- **What's New**: The enhancements and other changes released in the build.
- **Fixed Issues**: The issues that are fixed in the build.
- **Known Issues**: The issues that exist in the build.
- **Points to Note**: The important aspects to keep in mind while using the build.
- **Limitations**: The limitations that exist in the build.

> **Important:** The NetScaler Gateway release notes are covered as a part of ADC release notes. For detailed information about NetScaler Gateway 13.1 enhancements, known issues, and bug fixes, see release notes page.

Note:

- The [# XXXXXX] labels under the issue descriptions are internal tracking IDs used by the NetScaler team.
- These release notes do not document security related fixes. For a list of security related fixes and advisories, see the security bulletin.

About NetScaler Gateway

January 8, 2024

NetScaler Gateway is easy to deploy and simple to administer. The most typical deployment configuration is to locate the NetScaler Gateway appliance in the DMZ. You can install multiple NetScaler Gateway appliances in the network for more complex deployments.

The first time you start NetScaler Gateway, you can perform the initial configuration by using a serial console, the Setup Wizard in the configuration utility, or the Dynamic Host Configuration Protocol (DHCP). On the MPX appliance, you can use the LCD keypad on the front panel of the appliance to perform the initial configuration. You can configure basic settings that are specific to your internal network, such as the IP address, subnet mask, default gateway IP address, and Domain Name System (DNS) address. After you configure the basic network settings, you then configure the settings specific

to the NetScaler Gateway operation, such as the options for authentication, authorization, network resources, virtual servers, session policies, and endpoint policies.

Before you install and configure NetScaler Gateway, review the topics in this section for information about planning your deployment. Deployment planning can include determining where to install the appliance, understanding how to install multiple appliances in the DMZ, and licensing requirements. You can install NetScaler Gateway in any network infrastructure without requiring changes to the existing hardware or software running in the secure network. NetScaler Gateway supports other networking products, such as server load balancers, cache engines, firewalls, routers, and IEEE 802.11 wireless devices.

You can write your settings in the Pre-Installation Checklist to have on hand before you configure NetScaler Gateway.

NetScaler Gateway Appliances	Provides information about NetScaler Gateway appliances and the appliance installation instructions.
Pre-Installation Checklist	Provides planning information to review and a list of tasks to complete before you install NetScaler Gateway in your network.
Common Deployments	Provides information about deploying the NetScaler Gateway in the network DMZ, in a secure network without a DMZ, and with other appliances to support load balancing and failover. Also provides information about deploying NetScaler Gateway with Citrix Virtual Apps and Desktops.
Licensing	Provides information about installing licenses on the appliance. Also provides information about installing licenses on multiple NetScaler Gateway appliances.

NetScaler Gateway architecture

The core components of NetScaler Gateway are:

- **Virtual servers**. The NetScaler Gateway virtual server is an internal entity that is a representative of all the configured services available to users. The virtual server is also the access point

through which users access these services. You can configure multiple virtual servers on a single appliance, allowing one NetScaler Gateway appliance to serve multiple user communities with differing authentication and resource access requirements.

- **Authentication, authorization, and auditing**. You can configure authentication, authorization, and accounting to allow users to log on to NetScaler Gateway with credentials that either NetScaler Gateway or authentication servers located in the secure network, such as LDAP or RADIUS, recognize. Authorization policies define user permissions, determining which resources a given user is authorized to access. For more information about authentication and authorization, see Configuring Authentication and Authorization. Auditing servers maintain data about NetScaler Gateway activity, including user logon events, resource access instances, and operational errors. This information is stored on NetScaler Gateway or on an external server. For more information about auditing, see Configuring Auditing on NetScaler Gateway
- **User connections**. Users can log on to NetScaler Gateway by using the following access methods:
  - The Citrix Secure Access client for Windows is software that is installed on a Windows-based computer. Users log on by right-clicking an icon in the notification area on a Windows-based computer. If users are using a computer in which the Citrix Secure Access client is not installed, they can log on by using a web browser to download and install the plug-in. If users have Citrix Workspace app installed, users log on with the Citrix Secure Access client from Citrix Workspace app. When Citrix Workspace app and the Citrix Secure Access client are installed on the user device, Citrix Workspace app adds the Citrix Secure Access client automatically.
  - The Citrix Secure Access client for macOS X that allows users running macOS X to log on. It has the same features and functions as the Citrix Secure Access client for Windows. You can provide endpoint analysis support for this plug-in version by installing NetScaler Gateway 10.1, Build 120.1316.e.
  - Citrix Workspace app that allows user connections to published applications and virtual desktops in a server farm by using the Web Interface or Citrix StoreFront.
  - Citrix Workspace app, Secure Hub, WorxMail, and WorxWeb that allows users access to web and SaaS applications, iOS and Android mobile apps, and ShareFile data hosted in Citrix Endpoint Management.
  - Users can connect from an Android device that uses the NetScaler Gateway web address. When users start an app, the connection uses Micro VPN to route network traffic to the internal network. If users connect from an Android device, you must configure DNS settings on NetScaler Gateway. For more information, see Supporting DNS Queries by Using DNS Suffixes for Android Devices.

  - Users can connect from an iOS device that uses the NetScaler Gateway web address. You configure Secure Browse either globally or in a session profile. When users start an app on their iOS device, a VPN connection starts and the connection routes through NetScaler Gateway.
  - Clientless access that provides users with the access they need without installing software on the user device.

    When configuring NetScaler Gateway, you can create policies to configure how users log on. You can also restrict user logon by creating session and endpoint analysis policies.

- **Network resources**. These include all network services that users access through NetScaler Gateway, such as file servers, applications, and websites.
- **Virtual adapter**. The NetScaler Gateway virtual adapter supports applications that require IP spoofing. The virtual adapter is installed on the user device when the Citrix Secure Access client is installed. When users connect to the internal network, the outbound connection between NetScaler Gateway and internal servers uses the intranet IP address as the source IP address. The Citrix Secure Access client receives this IP address from the server as part of the configuration.

  If you enable split tunneling on NetScaler Gateway, all intranet traffic is routed through the virtual adapter. When intercepting intranet bound traffic, the virtual adapter will intercept A and AAAA record type DNS queries while leaving all other DNS queries intact. Network traffic that is not bound for the internal network is routed through the network adapter installed on the user device. Internet and private LAN (LAN) connections remain open and connected. If you disable split tunneling, all connections are routed through the virtual adapter. Any existing connections are disconnected and the user must reestablish the session.

  If you configure an intranet IP address, traffic to the internal network is spoofed with the intranet IP address through the virtual adapter.

How user connections work

Users can connect to their emails, file shares, and other network resources from a remote location. Users can connect to internal network resources with the following software:

- Citrix Secure Access client
- Citrix Workspace app
- WorxMail and WorxWeb
- Android and iOS mobile devices

Connect with the Citrix Secure Access client

The Citrix Secure Access client allows user access to resources in the internal network through the following steps:

1. A user connects to NetScaler Gateway for the first time by typing the web address in a web browser. The logon page appears and the user is prompted to enter a user name and password. If external authentication servers are configured, NetScaler Gateway contacts the server and the authentication servers verify the user's credentials. If local authentication is configured, NetScaler Gateway performs the user authentication.
2. If you configure a preauthentication policy, when the user types the NetScaler Gateway web address in a web browser on a Windows-based computer or a macOS X computer, NetScaler Gateway checks to see if any client-based security policies are in place before the logon page appears. The security checks verify that the user device meets the security-related conditions, such as operating system updates, antivirus protection, and a properly configured firewall. If the user device fails the security check, NetScaler Gateway blocks the user from logging on. A user who cannot log on must download the necessary updates or packages and install them on the user device. When the user device passes the preauthentication policy, the logon page appears and the user can enter the logon credentials. You can use Advanced Endpoint Analysis on a macOS X computer if you install NetScaler Gateway 10.1, Build 120.1316.e.
3. When NetScaler Gateway successfully authenticates the user, NetScaler Gateway initiates the VPN tunnel. NetScaler Gateway prompts the user to download and install the Citrix Secure Access client for Windows or the Citrix Secure Access client for macOS X.
4. If you configure a post-authentication scan, after a user successfully logs on, NetScaler Gateway scans the user device for the required client security policies. You can require the same security-related conditions as for a preauthentication policy. If the user device fails the scan, either the policy is not applied or the user is placed in a quarantine group and the user's access to network resources is limited.
5. When the session is established, the user is directed to a NetScaler Gateway home page where the user can select resources to access. The home page that is included with NetScaler Gateway is called the Access Interface. If the user logs on by using the Citrix Secure Access client for Windows, an icon in the notification area on the Windows desktop shows that the user device is connected and the user receives a message that the connection is established. The user can also access resources in the network without using the Access Interface, such as opening Microsoft Outlook and retrieving email.
6. If the user request passes both preauthentication and post-authentication security checks, NetScaler Gateway then contacts the requested resource and initiates a secure connection between the user device and that resource.
7. The user can close an active session by right-clicking the NetScaler Gateway icon in the notification area on a Windows-based computer and then clicking Logoff. The session can also time

out due to inactivity. When the session is closed, the tunnel is shut down and the user no longer has access to internal resources. The user can also type the NetScaler Gateway web address in a browser. When the user presses Enter, the Access Interface appears from which users can log off.

Note: If you deploy Citrix Endpoint Management in your internal network, a user who connects from outside the internal network must connect to NetScaler Gateway first. When the user establishes the connection, the user can access web and SaaS applications, Android and iOS mobile apps, and ShareFile data hosted on Citrix Endpoint Management. A user can connect with the Citrix Secure Access client through clientless access, or by using Citrix Workspace app or Secure Hub.

Connect with Citrix Workspace app

Users can connect with Citrix Workspace app to access their Windows-based applications and virtual desktops. Users can also access applications from Endpoint Management. To connect from a remote location, users also install the Citrix Secure Access client on their device. Citrix Workspace app automatically adds the Citrix Secure Access client to its list of plug-ins. When users log on to Citrix Workspace app, they can also log on to the Citrix Secure Access client. You can also configure NetScaler Gateway to perform single sign-on to the Citrix Secure Access client when users log on to Citrix Workspace app.

Connect with iOS and Android devices

Users can connect from an iOS or Android device by using Secure Hub. Users can access their email by using Secure Mail and connect to websites with WorxWeb.

When users connect from the mobile device, the connections route through NetScaler Gateway to access internal resources. If users connect with iOS, you enable Secure Browse as part of the session profile. If users connect with Android, the connection uses the Micro VPN automatically. In addition, Secure Mail and WorxWeb use Micro VPN to establish connections through NetScaler Gateway. You do not have to configure Micro VPN on NetScaler Gateway.

Common NetScaler Gateway deployments

January 8, 2024

You can deploy NetScaler Gateway at the perimeter of your organization's internal network (or intranet) to provide a secure single point of access to the servers, applications, and other network re-

sources that reside in the internal network. All remote users must connect to NetScaler Gateway before they can access any resources in the internal network.

NetScaler Gateway is most commonly installed in the following locations in a network:

- In the network DMZ
- In a secure network that does not have a DMZ

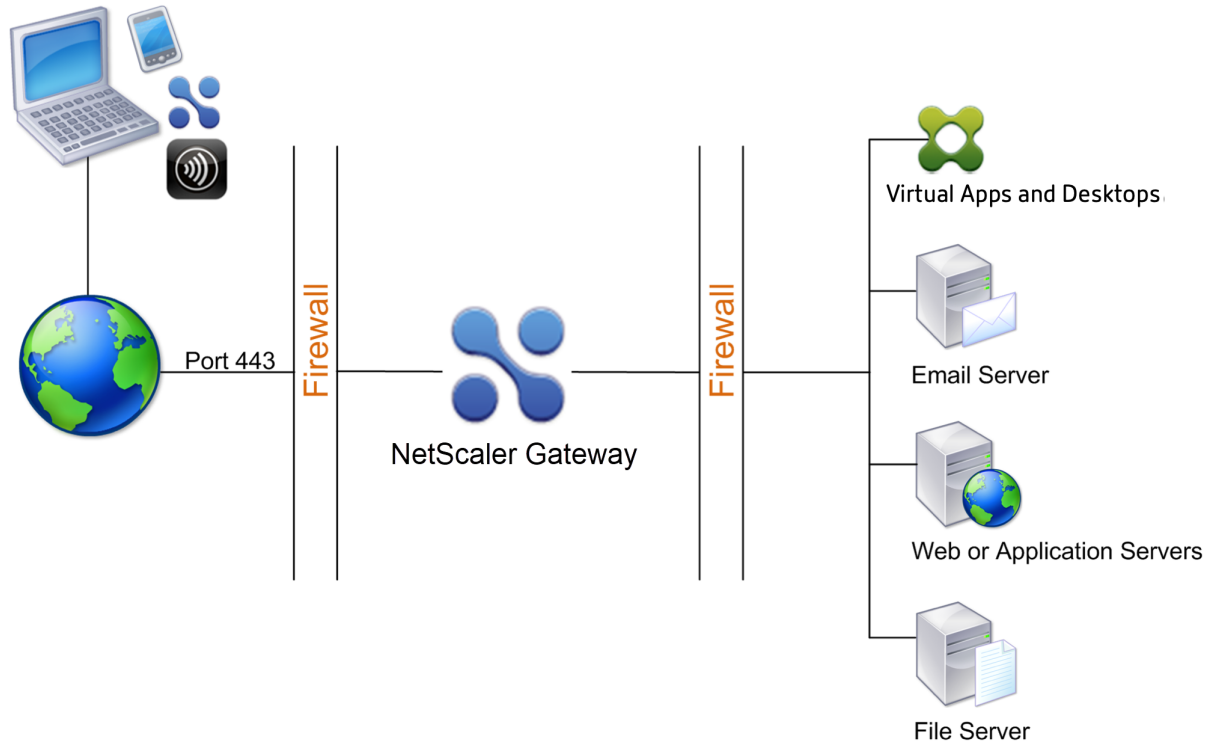
You can also deploy NetScaler Gateway with Citrix Virtual Apps, Citrix Virtual Desktops, StoreFront, and Citrix Endpoint Management to allow users to access their Windows, web, mobile, and SaaS applications. If your deployment includes Citrix Virtual Apps, StoreFront, and Desktops 7, you can deploy NetScaler Gateway in a single-hop or double-hop DMZ configuration. A double-hop deployment is not supported with earlier versions of Citrix Virtual Desktops or Citrix Endpoint Management.

For more information about expanding your NetScaler Gateway installation with these and other supported NetScaler solutions, see Integrating with NetScaler products topic.

Deploy NetScaler Gateway in a DMZ

Many organizations protect their internal network with a DMZ. A DMZ is a subnet that lies between an organization's secure internal network and the Internet (or any external network). When you deploy NetScaler Gateway in the DMZ, users connect with the Citrix Secure Access for Windows or Citrix Workspace app.

Figure 1. NetScaler Gateway deployed in the DMZ



In the configuration shown in the preceding figure, you install NetScaler Gateway in the DMZ and configure it to connect to both the Internet and the internal network.

NetScaler Gateway connectivity in a DMZ

When you deploy NetScaler Gateway in the DMZ, user connections must traverse the first firewall to connect to NetScaler Gateway. By default, user connections use SSL on port 443 to establish this connection. To allow user connections to reach the internal network, you must allow SSL on port 443 through the first firewall.

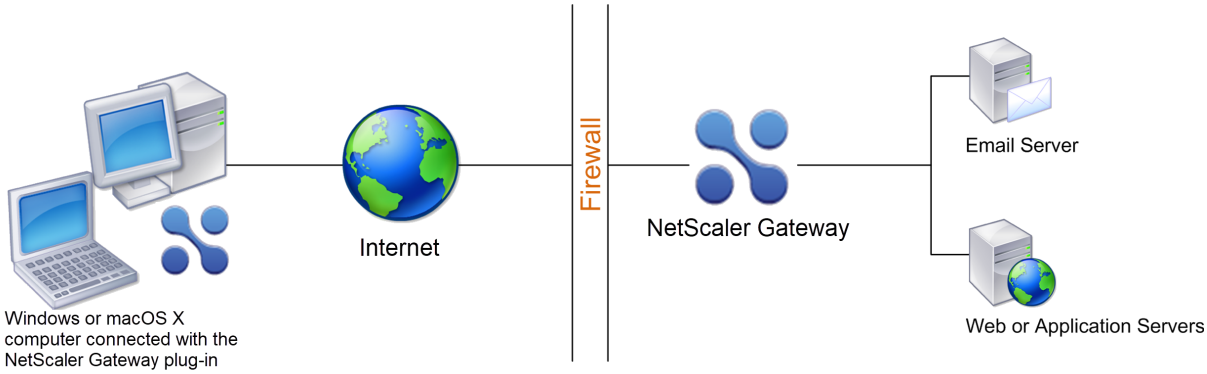
NetScaler Gateway decrypts the SSL connections from the user device and establishes a connection on behalf of the user to the network resources behind the second firewall. The ports that must be open through the second firewall are dependent on the network resources that you authorize external users to access.

For example, if you authorize external users to access a web server in the internal network, and this server listens for HTTP connections on port 80, you must allow HTTP on port 80 through the second firewall. NetScaler Gateway establishes the connection through the second firewall to the HTTP server on the internal network on behalf of the external user devices.

Deploy NetScaler Gateway in a secure network

You can install NetScaler Gateway in the secure network. In this scenario, one firewall stands between the Internet and the secure network. NetScaler Gateway resides inside the firewall to control access to the network resources.

Figure 1. NetScaler Gateway deployed in the secure network



When you deploy NetScaler Gateway in the secure network, connect one interface on NetScaler Gateway to the Internet and the other interface to servers running in the secure network. Putting NetScaler Gateway in the secure network provides access for local and remote users. Because this configuration only has one firewall, it makes the deployment less secure for users connecting from a remote location. Although NetScaler Gateway intercepts traffic from the Internet, the traffic enters the secure

network before users are authenticated. When NetScaler Gateway is deployed in a DMZ, users are authenticated before network traffic reaches the secure network.

When NetScaler Gateway is deployed in the secure network, Citrix Secure Access for Windows connections must traverse the firewall to connect to NetScaler Gateway. By default, user connections use the SSL protocol on port 443 to establish this connection. To support this connectivity, you must open port 443 on the firewall.

Client Software Requirements

January 8, 2024

NetScaler Gateway supports user connections by using the Citrix Secure Access client. When users log on with the plug-in, it establishes a full VPN tunnel. With the Citrix Secure Access client, users can connect to the network resources to which you allow access.

If endpoint policies are configured on NetScaler Gateway, then NetScaler Gateway downloads and installs the Citrix EPA client on the user device automatically when users log on.

Citrix Secure Access client system requirements

Citrix Secure Access client establishes a secure connection from the client machine to the NetScaler Gateway appliance.

The plug-in is distributed as a desktop app for Microsoft Windows, macOS X, and Linux operating systems. After you authenticate to the secure URL of the NetScaler Gateway appliance with your Web browser, the plug-in is downloaded and installed automatically on your machine.

The plug-in is provisioned as a mobile app for Android and iOS devices.

> **Note:**
>
> - To install the plug-in, admin/root privileges are required on the operating system.
> - The browsers that support the Citrix Secure Access client also support clientless VPN.

Citrix Secure Access client as a desktop app is supported for the following operating systems and Web browsers.

Operating System	Supported Browsers
macOS X (10.9 and later)	Safari 7.1 or later; Google Chrome Release 30 or later; Mozilla Firefox Release 30 or later
Windows 11	Google Chrome Release 30 or later; Mozilla Firefox Release 24 or later; Edge Chromium
Windows 10 (x86 and x64)	Google Chrome Release 30 or later; Mozilla Firefox Release 24 or later; Edge Chromium
Linux; Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS.	Mozilla Firefox Release 44 and above; Google Chrome 50 and above

> **Note:**
>
> Currently, Citrix Secure Access client and Citrix EPA client for Ubuntu support only the default GNOME display manager.

If the required dependency packages are missing, the command lists them and the plug-in installation fails. These dependency packages must be manually installed. Administrators can install a missing package by typing the following command using the command line interface.

```
apt-get install <dependency package>
```

Citrix Secure Access client as a mobile app is supported for the following operating systems.

VPN App	Supported Operating Systems
Android	Android 7.0 and later
iOS	iOS 12.0 and later

> **Note:**
>
> If you are using the latest Apple OS versions such as macOS 14/iOS 17 and later, then we recommend that you upgrade to Citrix Secure Access client or Citrix SSO version 23.09.1 or later.

Endpoint Analysis requirements

NetScaler Gateway installs the Citrix EPA client on the user device. The Citrix EPA client scans the user device for the endpoint security requirements that you have configured on NetScaler Gateway. The requirements include information, such as the operating system, antivirus, or web browser versions.

When users connect to NetScaler Gateway using the browser for the first time, the portal requests the installation of the Citrix EPA client. On subsequent logon attempts, the Citrix EPA client verifies the

upgrade control configuration to confirm whether the Citrix EPA client upgrade is necessary. If it is necessary, the user receives a prompt to download and install the latest Citrix EPA client. The Citrix EPA client for Windows is installed as a Windows 32-bit application. The Citrix EPA client for macOS is installed as a 64-bit application. No special privileges are required to install or use the Citrix EPA client, except when using EPA to access device certificates. For details on how to use EPA for device certificate authentication, see Use device certificates for authentication.

The tooltips on the Admin UI console explain the scans in detail. For details on the EPA libraries, see https://www.citrix.com/en-in/downloads/citrix-gateway/epa-libraries/.

> **Important:**
>
> - The browsers that support EPA also support clientless VPN.
> - In pre-authentication endpoint analysis, the user cannot log on with the Citrix Secure Access client if the user does not install the Endpoint Analysis plug-in or skips the scan.
> - In post-authentication endpoint analysis, the user can access resources for which a scan is not required by using either clientless access or by using the Citrix Workspace app.
> - For OPSWAT related scans, you must install the binary package `epaPackage.exe` on the client machine.

The following software is required on the user devices to use the Endpoint Analysis plug-in:

Operating System	Supported Browsers
macOS (10.9 and later)	Safari 7.1 or later; Google Chrome Release 30 or later; Mozilla Firefox Release 30 or later
Windows 11	Google Chrome Release 30 or later; Mozilla Firefox Release 24 or later; Edge Chromium
Windows 10	Google Chrome Release 30 or later; Mozilla Firefox Release 24 or later; Edge Chromium
Linux; Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS.	Mozilla Firefox Release 44 and later; Google Chrome 50 and later

Note:

- All editions of the operating system variants mentioned previously are supported.
- Windows 10 and Windows 11 in S modes are not supported.
- For Windows editions, all service packs and critical updates must be installed.
- For Mozilla Firefox versions, endpoint analysis must be plug-in enabled. The minimum required version is 3.0.

NetScaler Gateway compatibility with NetScaler products

July 16, 2024

The following table provides the products and versions with which NetScaler Gateway is compatible.

> **Note:**
>
> NetScaler Gateway features are available on NetScaler VPX.

NetScaler products and supported versions

NetScaler product	Release version
Citrix SD-WAN	10.2, 11.0, 11.1, 11.2, 11.3, 11.4
NetScaler Platforms	All current MPX, BLX, and VPX models including FIPS compliant appliances.
StoreFront	All currently supported StoreFront versions.
Citrix Virtual Apps and Desktops	All currently supported Citrix Virtual Apps and Desktops versions.
Citrix Endpoint Management	All currently supported Citrix Endpoint Management versions.

Citrix Workspace apps, Citrix Mobile Productivity Apps, and plug-ins

*The first supported build for each software release is listed in the following table. All subsequent builds are supported unless specified otherwise. For more information about the release lifecycle, refer to Product matrix.

Citrix Workspace app or plug-in	Minimum supported version*
Citrix Secure Access client for macOS X	3.1.8
Citrix Secure Access client for Windows	12.0
Citrix Secure Access client for iOS	3.1.4
Citrix Secure Access client for Android	2.0.14
Citrix Workspace app for Android	3.11

Citrix Workspace app or plug-in	Minimum supported version*
Citrix Workspace app for iOS	7.1.3
Citrix Workspace app for Mac	12.4
Citrix Workspace app for Windows	4.4
Citrix Workspace app for Linux	13.4
Citrix Workspace app for HTML5	2.3
Citrix Workspace app for Chrome	2.3
Secure Hub for iOS	10.5
Secure Hub for Android	10.5
Secure Mail for iOS	10.5
SecureWeb for iOS	10.5
Secure Mail for Android	10.5
SecureWeb for Android	10.5

> **Note:**
>
> - For details on some of the commonly used features supported for each VPN client, see NetScaler Gateway VPN clients and supported features.

NetScaler Gateway licensing

January 8, 2024

After you install NetScaler Gateway, you can obtain your Platform or Universal license files from Citrix. You log on to the Citrix website to access your available licenses and generate a license file. After the license file is generated, you download it to a computer. When the license file is on the computer, you then upload it to NetScaler Gateway. For more information about Citrix licensing, see Citrix Licensing System.

Before obtaining your license files, make sure you configure the host name of the appliance by using the Setup Wizard and then restart the appliance.

To obtain your licenses, go to the Activate, upgrade, and manage NetScaler licenses webpage. On this page, you can get your new license and activate, upgrade, and manage NetScaler licenses.

Important:

> - You must install licenses on NetScaler Gateway. The appliance does not obtain licenses from NetScaler license Server.
> - Citrix recommends that you retain a local copy of all license files you receive. When you save a backup copy of the configuration file, all uploaded licenses files are included in the backup. If you must reinstall the NetScaler Gateway appliance software and do not have a backup of the configuration, you need the original license files.

Before installing licenses on NetScaler Gateway, set the host name of the appliance and then restart NetScaler Gateway. You use the Setup Wizard to configure the host name. When you generate the Universal license for NetScaler Gateway, the host name is used in the license.

NetScaler Gateway license types

NetScaler Gateway requires a Platform license. The Platform license allows an unlimited number of connections to Citrix Virtual Apps, Citrix Virtual Desktops, or StoreFront by using ICA Proxy. To allow VPN connections to the network from the Citrix Secure Access client, a SmartAccess log on point, or Secure Hub, WorxWeb, or Secure Mail, you must also add a Universal license. NetScaler Gateway VPX comes with the Platform license.

The Platform license is supported on the following NetScaler Gateway versions:

- NetScaler Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.1
- NetScaler Gateway 11.0
- NetScaler Gateway 10.5
- NetScaler Gateway 10.1
- Access Gateway 10
- NetScaler VPX

> **Important:** Citrix recommends that you retain a local copy of all license files that you receive. When you save a backup copy of the configuration file, all uploaded license files are included in the backup. If you need to reinstall the NetScaler Gateway appliance software and do not have a backup of the configuration, you need the original license files.

The Platform License

The Platform license allows unlimited user connections to published applications on Citrix Virtual Apps or virtual desktops from Citrix Virtual Desktops. Connections by using Citrix Receiver do not use

a NetScaler Gateway Universal license. These connections only need the Platform license. The Platform license is delivered electronically with all new NetScaler Gateway orders, whether physical or virtual. If you already own an appliance covered by a warranty or maintenance agreement, you can obtain the Platform license from the Citrix website.

The Universal License

The NetScaler Gateway universal license limits the number of concurrent user sessions to the number of licenses purchased. If you purchase 100 licenses, you can have 100 concurrent sessions at any time. If you purchase a Standard edition license, you can have 500 concurrent sessions at any time. When a user ends a session, that license is released for the next user. A user who logs on to NetScaler Gateway from more than one computer occupies a license for each session.

If all licenses are occupied, no additional connections can be opened until a user ends a session or the administrator terminates the session using the configuration utility. When a connection is closed, the license is released and can be used for a new user.

When you receive your NetScaler Gateway appliance, licensing occurs in the following order:

- You receive the license access code (license key) in an email.
- You use the Setup Wizard to configure NetScaler Gateway with the host name.
- You allocate the NetScaler Gateway licenses from the Citrix website. Use the host name to bind the licenses to the appliance during the allocation process.
- You install the license file on NetScaler Gateway.

The Universal license supports the following features:

- Full VPN tunnel
- Micro VPN
- Endpoint analysis
- Policy-based SmartAccess
- Clientless access to websites and file shares

Obtaining the Universal License You need the following information before going to the Citrix website for the universal license.

- Your Citrix account user ID and password.

  Register at the Citrix website (https://www.citrix.com/welcome/create-account/) to receive your user ID and password.
  Note: If you cannot locate either the license code or your user ID and password, contact Citrix Customer Service.

- The host name of the NetScaler Gateway

  The entry field for this name on the Citrix website is case-sensitive, so make sure that you copy the host name exactly as it is configured on the NetScaler appliance.

- The number of licenses you want to include in the license file

  You do not have to download all the licenses you are entitled to at once. For example, if your company purchased 100 licenses, you can choose to download 50. You can allocate the rest in another license file later. Multiple license files can be installed on the NetScaler Gateway.

  Note: Before obtaining your licenses, make sure you configure the host name of the NetScaler appliance using the Setup Wizard and then restart the appliance.

To obtain your universal license

1. Log in to the Citrix website (https://www.citrix.com/en-in/account/) using your Citrix credentials.
2. Under **Citrix Manage Licenses is here**, follow the directions to obtain your license file.

Installing the Universal License To install the license, see "Installing the License". After installation, verify that the license was installed correctly.

Verifying Installation of the Universal License Before proceeding, verify that your universal license is installed correctly.

To verify installation of the universal license by using the CLI

1. Open an SSH connection to the NetScaler appliance by using an SSH client, such as PuTTY.
2. Log on to the NetScaler appliance by using the administrator credentials.
3. Use the show license command to verify that "SSL VPN = YES"and that Maximum Users have increased from 5 to the expected number of concurrent users.

To verify installation of the universal license by using the GUI

1. In a Web browser, type the IP address of the NetScaler appliance, such as `http://192.168.100.1`.
2. In User Name and Password, type the administrator credentials.
3. In the navigation pane, expand System, and then click Licenses.

4. In the Licenses pane, you see a green check mark next to **Citrix Gateway**. The field Maximum NetScaler Gateway Users Allowed displays the number of concurrent user sessions licensed on the NetScaler appliance.

Related resources

- Citrix Licensing System
- NetScaler data sheet
- Types of NetScaler and NetScaler Gateway licenses

Install a license on NetScaler Gateway

January 8, 2024

After you successfully download the license file to your computer, you can then install the license on NetScaler Gateway. The license is installed in the /nsconfig/license directory.

If you used the Setup Wizard to configure the initial settings on NetScaler Gateway, the license file is installed when you run the wizard. If you allocate part of your licenses and then later, you allocate an extra number, you can install the licenses without using the Setup Wizard.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **System** and then click **Licenses**.
2. In the details pane, click **Manage Licenses**.
3. Click **Add New License**, then click **Browse**, navigate to the license file, and then click **OK**.

   A message appears in the configuration utility that you must restart NetScaler Gateway. Click Reboot.

Set the maximum number of users

After you install the license on the appliance, you need to set the maximum number of users that are allowed to connect to the appliance. You set the maximum user count in the global authentication policy.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway** and then click **Global Settings**.
2. In the details pane, under Settings, click **Change authentication AAA settings**.

3. In Maximum Number of Users, type the total number of users, and then click **OK**.

   The number in this field corresponds to the number of licenses contained within the license file. This number must be less than or equal to the total number of licenses installed on the appliance. For example, you install one license that contains 100 user licenses and a second license that contains 400 user licenses. The total number of licenses equals 500. The maximum number of users who can log on is equal to or less than 500. If 500 users are logged on, any users who attempt to log on beyond that number are denied access until a user logs off or you terminate a session.

Verify Universal license installation

Before proceeding, verify that your Universal license is installed correctly.

To verify installation of the Universal license by using the GUI

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand System and then click Licenses.

   In the Licenses pane, you see a green check mark next to NetScaler Gateway. The Maximum NetScaler Gateway Users Allowed field displays the number of concurrent user sessions licensed on the appliance.

To verify installation of the Universal license by using the CLI

1. Open a Secure Shell (SSH) connection to the appliance by using an SSH client, such as PuTTY.
2. Log on to the appliance using the administrator credentials.
3. At a command prompt, type;

```
show license
```

The license is installed correctly if the parameter SSL VPN equals Yes and the maximum users parameter equals the number of licenses.

NetScaler Gateway licensing FAQs

January 8, 2024

How do I get assistance with trial or demo licenses?

Many of the NetScaler products are now offered as comprehensive, private, 1:1, expert-led demo experiences. Our Citrix experts customize the demo to fit your needs, use cases, and active projects. No downloads, no license, or installation required. You need a minimal setup to see an instant demo. After the demo, to proceed with a proof of concept or trial of a Citrix solution that applies to your services, contact Citrix experts. For demos, click https://demo.citrix.com/.

How to install licenses?

For details on installing licenses, see To install a license on NetScaler Gateway.

What are the different types of Gateway licenses?

The Platform license allows an unlimited number of connections to Citrix Virtual Apps, Citrix Virtual Desktops, or StoreFront by using ICA Proxy.
The Universal License is an add-on license on top of NetScaler platform licenses. This allows VPN connections to the network from the Citrix Secure Access client, a SmartAccess log on point, or Secure Hub, Secure Web, or Secure Mail. For more details, see NetScaler Gateway License Types.

How many concurrent user sessions are supported?

The supported sessions depend on the gateway license type. For details, see NetScaler Gateway License Types.

Another factor to consider is the capacity of the underlying hardware itself. Refer to NetScaler MPX/SDX data sheet or NetScaler VPX data sheet for performance considerations.

How to check the current concurrent user sessions licensed?

In the configuration utility on the Configuration tab, expand **System** and then click **Licenses**.
In the **Licenses** pane, you see a green check mark next to NetScaler Gateway. The **Maximum NetScaler Gateway Users Allowed** field displays the number of concurrent user sessions licensed on the appliance.

How to check whether the licensed throughput limit is reached?

You can extract the real-time throughput using `newnslog`. For example, if license throughput is 500 Mbps, then you can extract the real-time throughput over 500 by using the following command.


```
nsconmsg -K newnslog -g mbits -d past -s disptime=1 -s ratecount=500 |
    more
```

```
reltime:mili second between two records Mon Feb  5 13:47:13 2018
 Index   rtime totalcount-val      delta rate/sec symbol-name&device-no&time
    12    7000      801130681       3701      528 allnic_tot_rx_mbits  Mon Feb  5 13:47:55 2018
    13       0      460776045       3682      526 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:47:55 2018
    14    7000      801134437       3756      536 allnic_tot_rx_mbits  Mon Feb  5 13:48:02 2018
    15       0      460779784       3739      534 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:02 2018
    16    7000      801138166       3729      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:09 2018
    17       0      460783497       3713      530 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:09 2018
    18    7000      801141896       3730      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:16 2018
    19       0      460787213       3716      530 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:16 2018
    20    7000      801145623       3727      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:23 2018
    21       0      460790929       3716      530 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:23 2018
    22    7000      801149353       3730      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:30 2018
    23       0      460794646       3717      531 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:30 2018
    24    7000      801153067       3714      530 allnic_tot_rx_mbits  Mon Feb  5 13:48:37 2018
    25       0      460798342       3696      528 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:37 2018
```

How to check whether packets are dropped on licensing throughput being reached?

You can use the following command to check whether packets are dropped.

```
nsconmsg -K newnslog -d current -g nic_err_rl_pkt_drops -s disptime=1 |
    more
```

```
reltime:mili second between two records Fri Feb  2 00:12:38 2018
 Index   rtime    totalcount-val      delta rate/sec symbol-name&device-no&time
     0 1966993       23723602        478       68 nic_err_rl_pkt_drops interface(1/2) Fri Feb  2 00:12:38 2018
     1       0       48048402        465       66 nic_err_rl_pkt_drops interface(1/1) Fri Feb  2 00:12:38 2018
     2       0     8307679782     145475    20782 nic_err_rl_pkt_drops interface(0/2) Fri Feb  2 00:12:38 2018
     3    7000       23723933        331       47 nic_err_rl_pkt_drops interface(1/2) Fri Feb  2 00:12:45 2018
     4       0       48048712        310       44 nic_err_rl_pkt_drops interface(1/1) Fri Feb  2 00:12:45 2018
     5       0     8307787105     107323    15331 nic_err_rl_pkt_drops interface(0/2) Fri Feb  2 00:12:45 2018
     6    7000       23723941          8        1 nic_err_rl_pkt_drops interface(1/2) Fri Feb  2 00:12:52 2018
     7       0       48048735         23        3 nic_err_rl_pkt_drops interface(1/1) Fri Feb  2 00:12:52 2018
     8       0     8307811163      24058     3436 nic_err_rl_pkt_drops interface(0/2) Fri Feb  2 00:12:52 2018
```

How can I find out what the licensed throughput is for a NetScaler appliance?

Run the `show license` command from the CLI, and then use the model number to get the throughput from the ADC or gateway MPX, SDX, and VPX data sheet.


```
> sh license
        License status:
                          Web Logging: YES
                       Surge Protection: YES
                         Load Balancing: YES
                      Content Switching: YES
                      Cache Redirection: YES
                            Sure Connect: YES
                   Compression Control: YES
                     Delta Compression: NO
                      Priority Queuing: YES
                         SSL Offloading: YES
          Global Server Load Balancing: YES
                         GSLB Proximity: YES
                   Http DoS Protection: YES
                       Dynamic Routing: YES
                     Content Filtering: YES
                    Integrated Caching: YES
                               SSL VPN: YES   (Maximum users = 5)   (Maximum ICA u
sers = 0)
                                   AAA: YES
                           OSPF Routing: YES
                            RIP Routing: YES
                            BGP Routing: YES
                                Rewrite: YES
             IPv6 protocol translation: YES
                  Application Firewall: YES
                              Responder: YES
                          HTML Injection: YES
                          NetScaler Push: YES
                   Web Interface on NS: YES
                                AppFlow: YES
                             CloudBridge: YES
                       Model Number ID: 5500
 Done
>
```

CITRIX

Citrix NetScaler | Datasheet

NetScaler platform	MPX 9500	MPX 7500	MPX 5500	VPX 10/200/1000/3000
Platform attributes				
Processor	Intel Xeon L5410 (4 cores total)	Intel Xeon L5410 (4 cores total)	Intel Xeon E5205 (2 cores total)	Minimum Server Req.:[1] Dual core server with Intel® VTx or AMD-V™
Memory	8 GB	8 GB	4 GB	
Ethernet ports	8x 10/100/1000 BASE-T OR 4x 10/100/1000 BASE-T AND 4x 1000BASE-X SFP (fiber or copper)	8x 10/100/1000 BASE-T OR 4x 10/100/1000 BASE-T AND 4x 1000BASE-X SFP (fiber or copper)	4x 10/100/1000 BASE-T	• Citrix® XenServer® 5 (update 3 or better) • Windows Server 2008 R2 with Hyper-V role • VMWare ESX/ESXi 3.5 or higher • 4G RAM/20 GB hard drive • Hypervisor supported NIC
Transceivers support	SX, LX	SX, LX		
Software upgradable performance		Upgrade option to MPX 9500		Upgrade options to VPX 200, VPX 1000 and VPX 3000
Platform performance				
System throughput, Gbps	3	1	0.5	Up to 3.0[2]
HTTP requests/sec	200,000	100,000	50,000	Up to 100,000
SSL transactions/sec	20,000	10,000	5,000	Up to 500
SSL throughput, Gbps	3	1	0.5	Up to 1.0
Compression throughput, Gbps	2	1	0.5	Up to 0.75
SSL VPN: concurrent users	10,000	10,000	5,000	Up to 300[3]

How to add more users to existing Gateway licenses?

You can install an extra universal license. For example, assume that you have installed one universal license that contains 100 user licenses. If you install the second universal license that contains 400 user licenses, then the total number of user licenses is equal to 500.

Before Getting Started

January 8, 2024

Before you install NetScaler Gateway, you must evaluate your infrastructure and collect information to plan an access strategy that meets the specific needs of your organization. When you define your access strategy, you need to consider the security implications and complete a risk analysis. You also need to determine the networks to which users are allowed to connect and decide on policies that enable user connections.

In addition to planning for the resources available for users, you also need to plan your deployment scenario. NetScaler Gateway is compatible the following NetScaler products:

- Citrix Endpoint Management
- Citrix Virtual Apps
- Citrix Virtual Desktops
- StoreFront
- Web Interface
- Citrix SD-WAN

For more information about deploying NetScaler Gateway, see Common Deployments and Integrating With NetScaler products

As you prepare your access strategy, take the following preliminary steps:

- Identify resources. List the network resources for which you want to provide access, such as Web, SaaS, mobile or published applications, virtual desktops, services, and data that you defined in your risk analysis.
- Develop access scenarios. Create access scenarios that describe how users access network resources. An access scenario is defined by the virtual server used to access the network, endpoint analysis scan results, authentication type, or a combination thereof. You can also define how users log on to the network.
- Identify client software. You can provide full VPN access with the Citrix Secure Access client, requiring users to log on with Citrix Workspace app, Secure Hub, or by using clientless access. You can also restrict email access to Outlook Web App or WorxMail. These access scenarios also

determine the actions users can perform when they gain access. For example, you can specify whether users can modify documents by using a published application or by connecting to a file share.
- Associate policies with users, groups, or virtual servers. The policies you create on NetScaler Gateway enforce when the individual or set of users meets specified conditions. You determine the conditions based on the access scenarios that you create. You then create policies that extend the security of your network by controlling the resources users can access and the actions users can perform on those resources. You associate the policies with appropriate users, groups, virtual servers, or globally.

This section includes the following topics to help you plan your access strategy:

- Planning for Security includes information about authentication and certificates.
- Prerequisites that define network hardware and software you might need.
- The Pre-Installation Checklist that you can use to write down your settings before you configure NetScaler Gateway.

Prerequisites for installing NetScaler Gateway

Before you configure settings on NetScaler Gateway, review the following prerequisites:

- NetScaler Gateway is physically installed in your network and has access to the network. NetScaler Gateway is deployed in the DMZ or internal network behind a firewall. You can also configure NetScaler Gateway in a double-hop DMZ and configure connections to a server farm. Citrix recommends deploying the appliance in the DMZ.
- You configure NetScaler Gateway with a default gateway or with static routes to the internal network so users can access resources in the network. NetScaler Gateway is configured to use static routes by default.
- The external servers used for authentication and authorization are configured and running. For more information, see Authentication and Authorization.
- The network has a domain name server (DNS) or Windows Internet Naming Service (WINS) server for name resolution to provide correct NetScaler Gateway user functionality.
- You downloaded the Universal licenses for user connections with the Citrix Secure Access client from the Citrix website and the licenses are ready to be installed on NetScaler Gateway.
- NetScaler Gateway has a certificate that is signed by a trusted Certificate Authority (CA). For more information, see Installing and Managing Certificates.

Before you install NetScaler Gateway, use the Pre-Installation Checklist to write down your settings.

Planning for security

When planning your NetScaler Gateway deployment, you must understand the basic security issues associated with certificates, and with authentication and authorization.

Configure secure certificate management

By default, NetScaler Gateway includes a self-signed Secure Sockets Layer (SSL) server certificate that enables the appliance to complete SSL handshakes. Self-signed certificates are adequate for testing or for sample deployments, but NetScaler does not recommend using them for production environments. Before you deploy NetScaler Gateway in a production environment, Citrix recommends that you request and receive a signed SSL server certificate from a known Certificate Authority (CA) and upload it to NetScaler Gateway.

If you deploy NetScaler Gateway in any environment where NetScaler Gateway must operate as the client in an SSL handshake (initiate encrypted connections with another server), you must also install a trusted root certificate on NetScaler Gateway. For example, if you deploy NetScaler Gateway with Citrix Virtual Apps and the Web Interface, you can encrypt connections from NetScaler Gateway to the Web Interface with SSL. In this configuration, you must install a trusted root certificate on NetScaler Gateway.

Authentication support

You can configure NetScaler Gateway to authenticate users and to control the level of access (or authorization) that users have to the network resources on the internal network.

Before deploying NetScaler Gateway, your network environment must have the directories and authentication servers in place to support one of the following authentication types:

- LDAP
- RADIUS
- TACACS+
- Client certificate with auditing and smart card support
- RSA with RADIUS configuration
- SAML authentication

If your environment does not support any of these authentication types, or you have a small population of remote users, you can create a list of local users on NetScaler Gateway. You can then configure NetScaler Gateway to authenticate users against this local list. With this configuration, you do not need to maintain user accounts in a separate, external directory.

Secure your NetScaler Gateway deployment

Different deployments might require different security considerations. The NetScaler secure deployment guidelines provide general security guidance to help you decide on an appropriate secure deployment based on your specific security requirements.

For details, see NetScaler secure deployment guidelines.

Gateway pre-installation checklist

January 8, 2024

The checklist consists of a list of tasks and planning information you must complete before you install NetScaler Gateway.

Space is provided so that you can check off each task as you complete it and make notes. Citrix recommends that you make note of the configuration values that you need to enter during the installation process and while configuring NetScaler Gateway.

For steps to install and configure NetScaler Gateway, see Installing NetScaler Gateway.

User devices

- Ensure that user devices meet the installation prerequisites described in Citrix Secure Access System Requirements
- Identify the mobile devices with which users connect. **Note**: If users connect with an iOS device, you must enable Secure Browse in a session profile.

NetScaler Gateway basic network connectivity

Citrix recommends that you obtain licenses and signed server certificates before you start to configure the appliance.

- Identify and write down the NetScaler Gateway host name. **Note**: This is not the fully qualified domain name (FQDN). The FQDN is contained in the signed server certificate that is bound to the virtual server.
- Obtain Universal licenses from the Citrix Website
- Generate a Certificate Signing Request (CSR) and send to a Certificate Authority (CA). Enter the date you send the CSR to the Certificate Authority.
- Write down the system IP address and subnet mask.

- Write down the subnet IP address and subnet mask.
- Write down the administrator password. The default password that comes with NetScaler Gateway is `nsroot`.
- Write down the port number on which NetScaler Gateway listens for secure user connections. The default is TCP port 443. This port must be open on the firewall between the unsecured network (Internet) and the DMZ.
- Write down the default gateway IP address.
- Write down the DNS server IP address and port number. The default port number is 53. In addition, if you are adding the DNS server directly, you must also configure ICMP (ping) on the appliance.
- Write down the first virtual server IP address and host name.
- Write down the second virtual server IP address and host name (if applicable).
- Write down the WINS server IP address (if applicable).

Internal networks accessible through NetScaler Gateway

- Write down the internal networks that users can access through NetScaler Gateway. Example: 10.10.0.0/24
- Enter all internal networks and network segments that users need access to when they connect through NetScaler Gateway by using the Citrix Secure Access client.

High availability

If you have two NetScaler Gateway appliances, you can deploy them in a high availability configuration in which one NetScaler Gateway accepts and manages connections, while a second NetScaler Gateway monitors the first appliance. If the first NetScaler Gateway stops accepting connections for any reason, the second NetScaler Gateway takes over and begins actively accepting connections.

- Write down the NetScaler Gateway software version number.
- The version number must be the same on both NetScaler Gateway appliances.
- Write down the administrator password (`nsroot`). The password must be the same on both appliances.
- Write down the primary NetScaler Gateway IP address and ID. The maximum ID number is 64.
- Write down the secondary NetScaler Gateway IP address and ID.
- Obtain and install the Universal license on both appliances.
- Install the same Universal license on both appliances.
- Write down the RPC node password.

Authentication and Authorization

NetScaler Gateway supports several different authentication and authorization types that can be used in various combinations. For detailed information about authentication and authorization, see Authentication and Authorization.

LDAP authentication

If your environment includes an LDAP server, you can use LDAP for authentication.

- Write down the LDAP server IP address and port.

  If you allow unsecure connections to the LDAP server, the default port is 389. If you encrypt connections to the LDAP server with SSL, the default port is 636.

- Write down the security type.

  You can configure security with or without encryption.

- Write down the administrator bind DN.

  If your LDAP server requires authentication, enter the administrator DN that NetScaler Gateway must use to authenticate when making queries to the LDAP directory. An example is cn=administrator,cn=Users,dc=ace, dc=com.

- Write down the administrator password.

  The password is associated with the administrator bind DN.

- Write down the Base DN.

  DN (or directory level) under which users are located; for example, ou=users,dc=ace,dc=com.

- Write down the server logon name attribute.

  Enter the LDAP directory person object attribute that specifies a user's logon name. The default is sAMAccountName. If you are not using Active Directory, the common values for this setting are cn or uid.
  For more information about LDAP directory settings, see Configuring LDAP Authentication

- Write down the group attribute.
  Enter the LDAP directory person object attribute that specifies the groups to which a user belongs. The default is memberOf. This attribute enables NetScaler Gateway to identify the directory groups to which a user belongs.

- Write down the subattribute name.

RADIUS authentication and authorization

If your environment includes a RADIUS server, you can use RADIUS for authentication. RADIUS authentication includes RSA SecurID, SafeWord, and Gemalto Protiva products.

- Write down the primary RADIUS server IP address and port. The default port is 1812.
- Write down the primary RADIUS server secret (shared secret).
- Write down the secondary RADIUS server IP address and port. The default port is 1812.
- Write down the secondary RADIUS server secret (shared secret).
- Write down the type of password encoding (PAP, CHAP, MS-CHAP v1, MSCHAP v2).

SAML Authentication

The Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization between Identity Providers (IdP) and Service Providers.

- Obtain and install on NetScaler Gateway a secure IdP certificate.
- Write down the redirect URL.
- Write down the user field.
- Write down the signing certificate name.
- Write down the SAML issuer name.
- Write down the default authentication group.

Opening ports through the firewalls (single-hop DMZ)

If your organization protects the internal network with a single DMZ and you deploy the NetScaler Gateway in the DMZ, open the following ports through the firewalls. If you are installing two NetScaler Gateway appliances in a double-hop DMZ deployment, see Opening the Appropriate Ports on the Firewalls.

On the firewall between the unsecured network and the DMZ

- Open a TCP/SSL port (default 443) on the firewall between the Internet and NetScaler Gateway. User devices connect to NetScaler Gateway on this port.

On the firewall between the secured network

- Open one or more appropriate ports on the firewall between the DMZ and the secured network. NetScaler Gateway connects to one or more authentication servers or to computers running Citrix Virtual Apps and Desktops in the secured network on these ports.

- Write down the authentication ports.

  Open only the port appropriate for your NetScaler Gateway configuration.

  - For LDAP connections, the default is TCP port 389.
  - For a RADIUS connection, the default is UDP port 1812. Write down the Citrix Virtual Apps and Desktops ports.

- If you are using NetScaler Gateway with Citrix Virtual Apps and Desktops, open TCP port 1494. If you enable session reliability, open TCP port 2598 instead of 1494. Citrix recommends keeping both of these ports open.

Citrix Virtual Desktops, Citrix Virtual Apps, the Web Interface, or StoreFront

Complete the following tasks if you are deploying NetScaler Gateway to provide access to Citrix Virtual Apps and Desktops through the Web Interface or StoreFront. The Citrix Secure Access client is not required for this deployment. Users access published applications and desktops through NetScaler Gateway by using only web browsers and Citrix Receiver.

- Write down the FQDN or IP address of the server running the Web Interface or StoreFront.
- Write down the FQDN or IP address of the server running the Secure Ticket Authority (STA) (for Web Interface only).

Citrix Endpoint Management

Complete the following tasks if you deploy Citrix Endpoint Management in your internal network. If users connect to Endpoint Management from an external network, such as the Internet, users must connect to NetScaler Gateway before accessing mobile, web, and SaaS apps.

- Write down the FQDN or IP address of Endpoint Management.
- Identify web, SaaS, and mobile iOS or Android applications users can access.

Double-Hop DMZ deployment with Citrix Virtual Apps

Complete the following tasks if you are deploying two NetScaler Gateway appliances in a double-hop DMZ configuration to support access to servers running Citrix Virtual Apps.

NetScaler Gateway in the first DMZ

The first DMZ is the DMZ at the outermost edge of your internal network (closest to the Internet or unsecure network). Clients connect to NetScaler Gateway in the first DMZ through the firewall sepa-

rating the Internet from the DMZ. Collect this information before installing NetScaler Gateway in the first DMZ.

- Complete the items in the NetScaler Gateway Basic Network Connectivity section of this checklist for this NetScaler Gateway.

  When completing those items, Interface 0 connects this NetScaler Gateway to the Internet and Interface 1 connects this NetScaler Gateway to NetScaler Gateway in the second DMZ.

- Configure the second DMZ appliance information on the primary appliance.

  To configure NetScaler Gateway as the first hop in the double-hop DMZ, you must specify the host name or IP address of NetScaler Gateway in the second DMZ on the appliance in the first DMZ. After specifying when the NetScaler Gateway proxy is configured on the appliance in the first hop, bind it to NetScaler Gateway globally or to a virtual server.

- Write down the connection protocol and port between appliances.

  To configure NetScaler Gateway as the first hop in the double DMZ, you must specify the connection protocol and the port on which NetScaler Gateway in the second DMZ listens for connections. The connection protocol and port is SOCKS with SSL (default port 443). The protocol and port must be open through the firewall that separates the first DMZ and the second DMZ.

NetScaler Gateway in the second DMZ

The second DMZ is the DMZ closest to your internal, secure network. NetScaler Gateway deployed in the second DMZ serves as a proxy for ICA traffic, traversing the second DMZ between the external user devices and the servers on the internal network.

- Complete the tasks in the NetScaler Gateway Basic Network Connectivity section of this checklist for this NetScaler Gateway.

  When completing those items, Interface 0 connects this NetScaler Gateway to NetScaler Gateway in the first DMZ. Interface 1 connects this NetScaler Gateway to the secured network.

Install and configure the NetScaler Gateway appliance

January 8, 2024

When you receive your NetScaler Gateway appliance, you unpack the appliance and prepare the site and rack. After you determine that the location where you install your appliance meets the environmental standards and the server rack is in place according to the instructions, you install the hardware. After you mount the appliance, you connect it to the network, to a power source, and to the console

terminal that you use for initial configuration. After you turn on the appliance, you perform the initial configuration, and assign management and network IP addresses. Be sure to observe the cautions and warnings listed with the installation instructions.

When installing a NetScaler VPX virtual appliance, you must first acquire the virtual appliance image and install it on a hypervisor or other virtual machine monitor.

Citrix recommends using the NetScaler Gateway Pre-Installation Checklist topic so you can make a note of your settings before attempting to configure a NetScaler Gateway appliance. The checklist includes information about installing NetScaler Gateway and an appliance.

Configure the NetScaler Gateway appliance by using wizards

January 8, 2024

NetScaler Gateway has the following six wizards that you can use to configure settings on the appliance:

- The first-time setup wizard appears when you log on to the NetScaler Gateway appliance for the first time.
- The quick configuration wizard helps you configure the correct policies, expressions, and settings for connections to Citrix Endpoint Management, StoreFront, and the Web Interface.
- The NetScaler Gateway wizard helps you configure NetScaler Gateway-specific settings.
- The setup wizard helps you configure basic NetScaler Gateway settings for the first time.
- Citrix Endpoint Management Integrated Configuration helps you configure your NetScaler Gateway and Citrix Endpoint Management environment.
- The Published Applications wizard helps you configure settings for user connections by using Citrix Workspace app.

First-time setup wizard

When you finish installing and configuring the initial settings on the NetScaler Gateway appliance, when you log on to the configuration utility for the first time, the First-time Setup wizard appears if the following conditions are not met:

- You did not install a license on the appliance.
- You did not configure a subnet or mapped IP address.
- If the default IP address of the appliances is 192.168.100.1.

Configure NetScaler Gateway with the first-time setup wizard

To configure the NetScaler Gateway (the physical appliance or the VPX virtual appliance) for the first time, you need an administrative computer configured on the same network as the appliance.

Assign a NetScaler Gateway IP (NSIP) address as the management IP address of your appliance and a subnet IP (SNIP) address to which your servers can connect. You assign a subnet mask that applies to both NetScaler Gateway and SNIP addresses. Also configure a time zone. If you assign a host name, you can access the appliance by specifying its name instead of the NSIP address.

There are two sections in the First-time Setup Wizard. In the first section, you configure the basic system settings for the NetScaler Gateway appliance including:

NSIP address, SNIP address, and subnet mask
Appliance host name
DNS servers
Time zone
Administrator password
In the second section, you install licenses. If you specify the address of a DNS server, you can use the hardware serial number (HSN) or license key to allocate your licenses, instead of uploading your licenses from a local computer to the appliance.

Note: Citrix recommends saving your licenses to your local computer.

When you finish configuring these settings, NetScaler Gateway prompts you to restart the appliance. When you log on to the appliance again, you can use other wizards and the configuration utility to configure other settings.

Quick Configuration wizard

The Quick Configuration wizard allows you to configure multiple virtual servers on NetScaler Gateway. You can add, edit, and remove virtual servers.

The Quick Configuration wizard allows for seamless configuration for the following deployments:

- Web Interface connections to Citrix Virtual Apps and Desktops, with the ability to configure multiple instances of the Secure Ticket Authority (STA)
- Citrix Endpoint Management only
- StoreFront only
- Citrix Endpoint Management and StoreFront together

The Quick Configuration wizard allows you to configure the following settings on the appliance:

- Virtual server name, IP address, and port

- Redirection from an unsecure to a secure port
- LDAP server
- RADIUS server
- Certificates
- DNS server
- Citrix Endpoint Management and Citrix Virtual Apps and Desktops

  Note: To enable SSO, you have to manually enable the **Single Sign-on to web applications** option in the **Create NetScaler Gateway Session Profile > Client Experience** tab for the session action.

NetScaler Gateway supports user connections directly to Citrix Endpoint Management, which gives users access to their web, SaaS, and mobile apps, along with access to ShareFile. You can also configure settings to StoreFront which gives users access to their Windows-based applications and virtual desktops.

When you run the Quick Configuration wizard, the following policies are created based on your Citrix Endpoint Management, StoreFront, and Web Interface settings:

- Session policies, including policies and profiles for Receiver, Receiver for Web, Citrix Secure Access client, and Program Neighborhood Agent
- Clientless access
- LDAP and RADIUS authentication

Configure settings with the quick configuration wizard

You can configure settings in NetScaler Gateway to enable communication with Citrix Endpoint Management, StoreFront, or Web Interface by using the Quick Configuration wizard. When you complete the configuration, the wizard creates the correct policies for communication between NetScaler Gateway, Endpoint Management, StoreFront, or the Web Interface. These policies include authentication, session, and clientless access policies. When the wizard completes, the policies are bound to the virtual server.

When you complete the Quick Configuration wizard, NetScaler Gateway can communicate with Endpoint Management or StoreFront, and users can access their Windows-based applications and virtual desktops and web, SaaS, and mobile apps. Users can then connect directly to Endpoint Management.

During the wizard, you configure the following settings:

- Virtual server name, IP address, and port
- Redirection from an unsecure to a secure port

- Certificates
- LDAP server
- RADIUS server
- Client certificate for authentication (only for two-factor authentication)
- Endpoint Management, StoreFront, or Web Interface

The Quick Configuration wizard supports LDAP, RADIUS, and client certificate authentication. You can configure two-factor authentication in the wizard by following these guidelines:

- If you select LDAP as your primary authentication type, you can configure RADIUS as the secondary authentication type.
- If you select RADIUS as your primary authentication type, you can configure LDAP as the secondary authentication type.
- If you select client certificates as your primary authentication type, you can configure LDAP or RADIUS as the secondary authentication type.

You cannot create multiple LDAP authentication policies by using the Quick Configuration wizard. For example, you want to configure one policy that uses sAMAccountName in the **Server Logon Name Attribute** field and a second LDAP policy that uses the User Principal Name (UPN) in the **Server Logon Name Attribute** field. To configure these separate policies, use the NetScaler Gateway configuration utility to create the authentication policies. For more information, see Configuring LDAP Authentication.

You can configure certificates for NetScaler Gateway in the Quick Configuration wizard by using the following methods:

- Select a certificate that is installed on the appliance.
- Install a certificate and private key.
- Select a test certificate.
  Note: If you use a test certificate, you must add the fully qualified domain name (FQDN) that is in the certificate.

You can open the **Quick Configuration wizard** in one of the following two ways:

- When you are on the NetScaler Gateway logon page and select **NetScaler Gateway** in **Deployment Type**, the **Home** tab appears. If you select any other option in **Deployment Type**, the **Home** tab does not appear.
- From the link **Create/Monitor NetScaler Gateway** in the NetScaler Gateway details pane. The link appears if you install a license that enables NetScaler features. If you license the appliance for NetScaler Gateway only, the link does not appear.

After you initially run the wizard, you can run the wizard again to create more virtual servers and settings.

Important: If you use the Quick Configuration wizard to configure an extra NetScaler Gateway virtual server, you must use a unique IP address. You cannot use the same IP address that is used on an existing virtual server. For example, you have a virtual server with the IP address 192.168.10.5 with a port number of 80. You run the Quick Configuration wizard to create a second virtual server with the IP address 192.168.10.5 with port number 443. When you try to save the configuration, an error occurs.

To configure settings with the Quick Configuration wizard

1. In the configuration utility, do one of the following:
   a) If the appliance is licensed for NetScaler Gateway only, click the **Home** tab.
   b) If the appliance is licensed to include NetScaler features, on the Configuration tab, in the navigation pane, click **NetScaler Gateway** and then in the details pane, under **Getting Started**, click **Configure NetScaler Gateway for Enterprise Store**.
2. In the dashboard, click **Create New NetScaler Gateway**.
3. In **NetScaler Gateway Settings**, configure the following:
   a) In **Name**, type a name for the virtual server.
   b) In **IP address**, type the IP address for the virtual server.
   c) In **Port**, type the port number. The default port number is 443.
   d) Select Redirect requests from port 80 to secure port to allow user connections from port 80 to go to port 443.
4. Click **Continue**.
5. On the Certificate page, do one of the following:
   a) Click **Choose Certificate** and then in Certificate, select the certificate.
   b) Click **Install Certificate,** and then in **Choose Certificate** and in **Choose Key**, click **Browse** to navigate to the certificate and private key.
   c) Click **Use Test Certificate** and then in Certificate FQDN enter the fully qualified domain name (FQDN) contained in the test certificate.
6. Click **Continue**.
7. In Authentication Settings, do the following:
   a) In **Primary Authentication**, select LDAP, RADIUS, or Cert.
   b) Select an authentication server or configure the settings for the authentication type you selected in the previous step. If you select Cert, either select the client certificate or install a new client certificate.
   c) In **Secondary Authentication**, select the authentication type and then configure the authentication server settings.
8. Click **Continue**.

When you finish configuring the network and authentication settings, you can then configure Citrix Endpoint Management or Citrix Virtual Apps and Desktops (StoreFront or Web Interface) settings.

Configure enterprise store settings NetScaler Gateway supports user access to web, SaaS, and mobile apps and ShareFile only through Endpoint Management. If you also deploy StoreFront or the Web Interface, users have access to Windows-based apps and virtual desktops. You can configure settings for the following options:

- Endpoint Management only
- StoreFront only
- Endpoint Management and StoreFront together
- Web Interface only

When you click **Continue** from the preceding procedure, you can then configure the settings for your deployment scenario. The following procedures start on the Citrix Integration Settings page.

After you create the virtual server, editing the virtual server in the Quick Configuration wizard does not allow you to change Citrix Endpoint Management or Citrix Virtual Apps and Desktops settings.

For example, if you cancel the configuration of a virtual server at any stage before configuring the **Citrix Enterprise Store** settings, the wizard automatically selects the Web interface without configuring any settings. When this situation occurs, you can edit the virtual server details for configuring the Web Interface, but you cannot switch to Citrix Endpoint Management. To switch, you must create a new virtual server and must not cancel the wizard at any time during the configuration. If you do not need the Web Interface virtual server, you can delete it by using the Quick Configuration wizard.

To configure settings for StoreFront only

1. Click **Citrix Virtual Apps and Desktops**.
2. In **Deployment Type**, select **StoreFront**.
3. In **StoreFront FQDN**, enter the fully qualified domain name (FQDN) of the StoreFront server.
4. In **Receiver for Web Path**, leave the default path or enter your own path.
5. Select **HTTPS** for secure user connections.
6. In **Single Sign-on Domain**, enter the domain for StoreFront.
7. In **STA URL**, enter the complete IP address or FQDN of the server running the Secure Ticket Authority (STA) if you deploy StoreFront and provide access to published applications from Citrix Virtual Apps or virtual desktops from Citrix Virtual Desktops.
8. Click **Done**.

When users connect through NetScaler Gateway to StoreFront, users can start their apps and desktops from either Receiver for Web or Receiver.

To configure settings for Endpoint Management only

1. Click **Citrix Endpoint Management**.
2. In **App Controller FQDN**, enter the FQDN for Endpoint Management.
3. Click **Done**.

To configure Web Interface settings

1. In the Quick Configuration wizard, click **Citrix Virtual Apps and Desktops**.
2. In **Deployment Type**, select **Web Interface**, and then configure the following:
   a) In **Citrix Virtual Apps Site URL**, type the complete IP address or FQDN of the Web Interface.
   b) In **Citrix Virtual Apps Services Site URL**, type the complete IP address or FQDN of the Web Interface with the Citrix Workspace app Path. You can enter the default path or enter your own path.
   c) In **Single Sign-on Domain**, enter the domain to use.
   d) In **STA URL**, type the complete IP address or FQDN of the server running the STA.
3. Click **Done**.

NetScaler Gateway wizard

You use the NetScaler Gateway wizard to configure the following settings on the appliance:

- Virtual servers
- Certificates
- Name service providers
- Authentication
- Authorization
- Port redirection
- Clientless access
- Clientless access for SharePoint

Configure Settings by using the NetScaler Gateway wizard

After you run the Setup Wizard, you can run the NetScaler Gateway wizard to configure other settings on NetScaler Gateway. You run the NetScaler Gateway wizard from the configuration utility.

NetScaler Gateway comes with a test certificate. If you do not have a signed certificate from a Certificate Authority (CA), you can use the test certificate when using the NetScaler Gateway wizard. When you receive the signed certificate, you can remove the test certificate and install the signed certificate.

Citrix recommends obtaining the signed certificate before making NetScaler Gateway publicly available for users.

Note: You can create a Certificate Signing Request (CSR) from within the NetScaler Gateway wizard. If you use the NetScaler Gateway wizard to create the CSR, you must exit from the wizard and then start the wizard again when you receive the signed certificate from the Certificate Authority. For more information about certificates, see
Installing and Managing Certificates.

You can configure user connections for Internet Protocol version 6 (IPv6) in the NetScaler Gateway wizard when you configure a virtual server. For more information about using IPv6 for user connections, see Configuring IPv6 for User Connections.

To start the NetScaler Gateway wizard

1. In the configuration utility, click the Configuration tab and then in the navigation pane, click NetScaler Gateway.
2. In the details pane, under Getting Started, click NetScaler Gateway wizard.
3. Click Next and then follow the directions in the wizard.

Setup Wizard

You use the Setup Wizard to configure the following initial settings on the appliance:

- System IP address and subnet mask
- Mapped IP address and subnet mask
- Host name
- Default gateway
- Licenses

Note: Before running the Setup Wizard, download your licenses from the Citrix website. For more information, see
Licensing NetScaler Gateway

Published Applications wizard

You use the Published Applications wizard to configure NetScaler Gateway to connect to servers running Citrix Virtual Apps and Desktops in the internal network. With the Published Applications wizard, you can:

- Select a virtual server for connections to the server farm.

- Configure the settings for user connections for the Web Interface or StoreFront, single sign-on, and the Secure Ticket Authority.
- Create or select session policies for SmartAccess.

Within the wizard, you can also create session policy expressions for user connections. For more information about configuring NetScaler Gateway to connect to a server farm, see Providing Access to Published Applications and Virtual Desktops Through the Web Interface.

Integrated Citrix Endpoint Management configuration

You can deploy NetScaler Gateway with Citrix Endpoint Management MDM that provides the ability to scale, ensure high availability for apps, and maintain security. To use the Citrix Endpoint Management configuration, you need to install Version 10.1, Build 120.1316.e.

The Integrated Citrix Endpoint Management Configuration creates the following:

- Load balancing servers for Device Manager.
- Load balancing servers for Microsoft Exchange with email filtering.
- Load balancing servers for ShareFile.

For more information about creating settings with the Integrated Citrix Endpoint Management Configuration, see Configuring Settings for Your Citrix Endpoint Management Environment

Configure NetScaler Gateway

January 8, 2024

After you configure the base network settings on NetScaler Gateway, you then configure the detailed settings so users can connect to network resources in the secure network. These settings include:

- Virtual servers. You can configure multiple virtual servers on NetScaler Gateway, which allows you to create different policies depending on the user scenario you must implement. Each virtual server has its own IP address, certificate, and policy set. For example, you can configure a virtual server and restrict users to network resources in the internal network depending on their membership in groups and the policies you bind to the virtual servers. You can create virtual servers by using the following methods:
  - Quick Configuration wizard
  - NetScaler Gateway wizard
  - Configuration utility

- High availability. You can configure high availability when you deploy two NetScaler Gateway appliances in your network. If the primary appliances fail, the secondary appliance can take over without affecting user sessions.
- Certificates. You can use certificates to secure user connections to NetScaler Gateway. When you create a Certificate Signing Request (CSR), you add the fully qualified domain name to the certificate. You can bind certificates to virtual servers.
- Authentication. NetScaler Gateway supports several authentication types, including Local LDAP, RADIUS, SAML, client certificates, and TACACS+. In addition, you can configure cascading and two-factor authentication.
  Note: If you use RSA, Safeword, or Gemalto Protiva for authentication, you configure these types by using RADIUS.
- User connections. You can configure user connections by using session profiles. Within the profile, you can determine the plug-ins users can log on with, along with any restrictions users might require. Then, you can create a policy with one profile. You can bind session policies to users, groups, and virtual servers.
- Home page. You can use the default Access Interface as your home page, or you can create a custom home page. The home page appears after users successfully log on to NetScaler Gateway.
- Endpoint analysis. You can configure policies on NetScaler Gateway that check the user device for software, files, registry entries, processes, and operating systems when users log on. Endpoint analysis allows you to increase the security of your network by requiring the user device to have the required software.

Using the configuration utility

The configuration utility allows you to configure most of the NetScaler Gateway settings. You use a web browser to access the configuration utility.

Log on to the configuration utility

1. In a web browser, type the system IP address of NetScaler Gateway, such as `http://192.168.100.1`.
   Note: NetScaler Gateway is preconfigured with a default IP address of
   192.168.100.1 and subnet mask of
   255.255.0.0.
2. In User Name and Password, type `nsroot`.
3. In Deployment Type, select NetScaler Gateway and then click Login.

When you log on to the configuration utility for the first time, the Dashboard opens by default on the **Home** tab. On the **Home** tab, you can use the Quick Configuration wizard to configure the settings for

a virtual server, authentication, certificates, and Citrix Endpoint Management. You can also configure either StoreFront or Web Interface settings in the Quick Configuration wizard.

For more information about configuring NetScaler Gateway, see:

- Configuring Initial Settings Using the Setup Wizard.
- Configuring Settings with the Quick Configuration Wizard
- Configuring Settings by Using the NetScaler Gateway Wizard.

Create virtual servers

March 22, 2024

A virtual server is an access point to which users log on. Each virtual server has its own IP address, certificate, and policy set. A virtual server consists of a combination of an IP address, port, and protocol that accepts incoming traffic. Virtual servers contain the connection settings for when users log on to the appliance. You can configure the following settings on virtual servers:

- Certificates
- Authentication
- Policies
- Bookmarks
- Address pools (also known as IP pools or intranet IPs)
- Double-hop DMZ deployment with NetScaler Gateway
- Secure Ticket Authority
- SmartAccess ICA Proxy Session Transfer

If you run the NetScaler Gateway wizard, you can create a virtual server during the wizard. You can configure more virtual servers in the following ways:

- **From the virtual servers node**. This node is on the navigation pane in the configuration utility. You can add, edit, and remove virtual servers by using the configuration utility.
- **With the Quick Configuration wizard**. If you deploy Citrix Endpoint Management, StoreFront or the Web Interface in your environment, you can use the Quick Configuration wizard to create the virtual server and all the policies needed for your deployment.

If you want users to log on and use a specific authentication type, such as RADIUS, you can configure a virtual server and assign the server a unique IP address. When users log on, they are directed to the virtual server and then prompted for their RADIUS credentials.

You can also configure the ways users log on to NetScaler Gateway. You can use a session policy to configure the type of user software, the access method, and the home page users see after logging

on.

To create virtual servers

You can add, modify, enable or disable, and remove virtual servers by using the NetScaler Gateway GUI or the Quick Configuration wizard. For more information about configuring a virtual server with the Quick Configuration wizard, see
Configuring Settings with the Quick Configuration Wizard.

> **Note:**
>
> The VPN virtual server supports DTLS version 1.0, by default. To enable DTLS version 1.2, see Configure DTLS VPN virtual server using SSL VPN virtual server.

HTTP QUIC VPN virtual server

From release 14.1 build 8.x, NetScaler Gateway supports using HTML5 on your browser to send ICA traffic using QUIC and to launch Citrix DaaS sessions. You can create a VPN virtual server of service type HTTP QUIC to launch Citrix DaaS applications over QUIC on HTML5 clients, without a client plug-in software. Previously, Citrix DaaS applications had to be launched through browsers using the Citrix Workspace app client plug-in software or HTML5 client apps using WebSockets (clientless access).

HTML5 clients support the WebTransport protocol. The WebTransport protocol uses HTTP3 over QUIC to establish communication between a client and a web server. For more information about HTTP over QUIC, see HTTP over QUIC protocol.

Configure the HTTP QUIC VPN virtual server by using the GUI

1. Configure HTTP QUIC VPN virtual server.
   a) Navigate to **Configuration > NetScaler Gateway > Virtual Servers**.
   b) On the **NetScaler Gateway Virtual Servers** page, click **Add**.
   c) In **Protocol**, select **HTTP_QUIC**.
   d) Update the remaining fields as required and click **OK**.
2. Enable HTTP/3 WebTransport on the HTTP profile.
   - Navigate to **System > Profiles > HTTP Profiles**. In the **HTTP/3** section, enable the **HTTP/3 WebTransport** checkbox. For details about HTTP profiles, see HTTP configurations.

Configure the HTTP QUIC VPN virtual server by using the CLI

1. Configure a VPN virtual server of service type `HTTP QUIC`.

```
add vpn vserver <VPN server name> -service type <HTTP_QUIC> -dtls
    <off> -Listenpolicy <NONE> -httpProfileName <name of the HTTP
    QUIC profile> -deploymentType <ICA_STOREFRONT> -vserverFqdn <
    URL>
```

2. Enable HTTP/3 WebTransport on the HTTP profile.

```
set httpprofile nshttp_default_http_quic_profile -http3webTransport
 ENABLED
```

The output of the following show command displays the parameter `HTTP/3 WebTransport: ENABLED`. This parameter indicates that the service type `HTTP QUIC` is being used to send WebTransport traffic between the client and the VPN virtual server.

```
sh httpprofile <name>

HTTP/2 Strict Cipher: ENABLED
        HTTP/3: ENABLED
        HTTP/3 maximum header field section size: 24576
        HTTP/3 maximum header table size: 4096
        HTTP/3 maximum header blocked streams: 100
        HTTP/3 WebTransport: ENABLED
        gRPC Buffer Limit: 131072
        gRPC Buffer Timeout: 1000
        gRPC Length Delimited Message: ENABLED
        Apdex Client Response Threshold: 500
        HTTP pipeline req buffer size: 131072
        Reference count: 2
```

> **Notes:**
>
> - The IP address and port number must be the same for the SSL and HTTP QUIC VPN virtual servers. However, DTLS must be disabled on the SSL VPN virtual server because you cannot run both DTLS and HTTP_QUIC on a common IP address and port number. For details about the DTLS VPN virtual server, see Configure DTLS VPN virtual server using SSL VPN virtual server.
> - The HTTP profile configured with the alternative service value set to `Altsvc=h3=":port number"` must be bound to the SSL VPN virtual server. For details about the Alternative Service parameter, see HTTP/2 for HTTP load balancing configuration.

To create a virtual server by using the GUI

1. Navigate to **NetScaler Gateway > Virtual Servers**.

2. In the details pane, click **Add**.
3. Configure the settings as per your requirement.
4. Click **Create** and then click **Close**.

To create a virtual server by using the CLI

At the command prompt, type;

```
add vpn vserver <name> <serviceType> [<IPAddress> <port>]
```

Example:

```
add vpn vserver gatewayserver SSL 1.1.1.1 443
```

Points to note when binding a net profile to the VPN virtual server

You can create net profiles (network profiles) to configure the appliance to use a specified source IP address and bind the net profile to the VPN virtual server. However, note the following when binding a net profile to the VPN virtual server.

- When you bind a net profile to a NetScaler Gateway virtual server, the net profile does not select a specific SNIP to be used by the virtual server or service for the traffic to back-end servers. Instead, the gateway appliance ignores the net profile binding and uses the round robin method for selecting the SNIPs.
- Net profile does not work for dynamically generated services (STA, SF monitor). For STA and other dynamically generated services, you can bind the net profile to those monitors directly and those monitors are used at that point. However, if you have multiple gateways on the same appliance, all gateways use the same net profile for the configured monitors.

  For more details about net profile, see Use a specified source IP for back-end communication.

Net profile source IP address in a DTLS VPN virtual server configuration for UDP launch

Starting from release 14.1 build 17.38, NetScaler Gateway configured with DTLS Listener chooses the source IP address from the net profile to establish a UDP connection with the Virtual Delivery Agent (VDA). Ensure that the net profile is bound to the SSL VPN virtual server.

Run the following CLI commands to configure a net profile in the VPN virtual server:

```
add ip <IPAddress><netmask> -type SNIP
add netprofile net1 -srcIP <IPAddress>
set vpn vserver <name> -netProfile net1
```

To verify if the chosen source IP address is used, run the `show connectiontable` CLI command.

Current users and total connected users on the virtual server

Current users: Number of users logged on to a specific virtual server. It is recommended that you monitor the current users for tracking CCUs.

Total connected users: Number of users who have one or more active connections through the specific virtual server. The total number of connected users is mostly used in ICA Proxy.

You can use the number of total connected users counter in the following scenarios:

- Consider that an ICA connection is established but no corresponding authentication, authorization, and auditing session are established. In this scenario, a user launches an application or a desktop and closes the browser, continues to work on the launched app or desktop. The authentication, authorization, and auditing session times out but the connection is still active. Total number of connected users can be used to identify the users that are still connected.
- In HDX optimal routing, authentication gateway and ICA gateway can be on different appliances. The total connected users in this case can be used to identify the number of connected users on the ICA gateway.

Points to note:

- Current users exceed total connected users when there are active sessions (not yet timed out) but there are no active connections on these sessions. For example, a user launched an application or a desktop and closed it immediately but did not log out from the authentication, authorization, and auditing session.
- Total connected users exceed current users if authentication, authorization, and auditing sessions timeout but ICA connections are still active.
- In a pure VPN setup (no ICA is involved), the number of current users and total connected users are equal.

Configure connection types on the virtual server

When you create and configure a virtual server, you can configure the following connection options:

- Connections with Citrix Workspace app only to Citrix Virtual Apps and Desktops without SmartAccess, endpoint analysis, or network layer tunneling features.
- Connections with the Citrix Secure Access client and SmartAccess, which allow the use of SmartAccess, endpoint analysis, and network layer tunneling functions.
- Connections with Secure Hub that establishes a Micro VPN connection from mobile devices to NetScaler Gateway.
- Parallel connections made over the ICA session protocol by a user from multiple devices. The connections are migrated to a single session to prevent the use of multiple Universal licenses.

If you want users to log on without user software, you can configure a clientless access policy and bind it to the virtual server.

To configure Basic or SmartAccess connections on a virtual server

1. Navigate to **NetScaler Gateway** and then click **Virtual Servers**.
2. In the details pane, click **Add**.
3. In **Name**, type a name for the virtual server.
4. In **IP Address** and **Port**, type the IP address and port number for the virtual server.
5. Do one of the following:
   - To allow ICA connections only, click **Basic Mode**.
   - To allow user logon with Secure Hub, the Citrix Secure Access client and SmartAccess, click **SmartAccess Mode**.
   - To allow SmartAccess to manage ICA Proxy sessions for multiple user connections, click **ICA Proxy Session Migration**.
6. Configure the other settings for the virtual server, click **Create**, and then click **Close**.

Configure a listen policy for wildcard virtual servers

You can configure NetScaler Gateway virtual servers to restrict the ability for a virtual server to listen on a specific VLAN. You can create a wildcard virtual server with a listen policy that restricts it to processing traffic on the specified VLAN.

The configuration parameters are:

Parameter	Description
Name	The name of the virtual server. The name is required and you cannot change it after you create the virtual server. The name cannot exceed 127 characters and the first character must be a number or letter. You can also use the following characters: at symbol (@), underscore (_), dash (-), period (.), colon (:), pound sign (#), and a space.
IP	The IP address of the virtual server. For a wildcard virtual server bound to the VLAN, the value is always *.

Parameter	Description
Type	The behavior of the service. Your choices are HTTP, SSL, FTP, TCP, SSL_TCP, UDP, SSL_BRIDGE, NNTP, DNS, ANY, SIP-UDP, DNS-TCP, and RTSP.
Port	The port on which the virtual server listens for user connections. The port number must be between 0 and 65535. For the wildcard virtual server bound to a VLAN, the value is usually *.
Listen Priority	The priority that is assigned to the listening policy. Priority is evaluated in reverse order; the lower the number, the higher the priority assigned to the listen policy.
Listen Policy Rule	The policy rule to use to identify the VLAN to which the virtual server must listen. The rule is `CLIENT.VLAN.ID.EQ (<ipaddressat>)`. Replace `<ipaddressat>` with the ID assigned to the VLAN.

To create a wildcard virtual server with a listen policy

1. In the navigation pane, expand **NetScaler Gateway** and then click **Virtual Servers**.
2. In the details pane, click **Add**.
3. In **Name**, type a name for the virtual server.
4. In **Protocol**, select the protocol.
5. In **IP Address**, type the IP address for the virtual server.
6. In **Port**, type the port for the virtual server.
7. On the **Advanced** tab, under Listen Policy, in **Listen Priority**, type the priority for the listen policy.
8. Next to Listen Policy Rule, click **Configure**.
9. In the **Create Expression** dialog box, click **Add**, configure the expression, and then click **OK**.
10. Click **Create** and then click **Close**.

Configure IP addresses on NetScaler Gateway

January 8, 2024

You can configure IP addresses to log on to the configuration utility and for user connections. NetScaler Gateway is configured with a default IP address of 192.168.100.1 and subnet mask of 255.255.0.0 for management access. The default IP address is used whenever a user-configured value for the system IP (NSIP) address is absent.

- NSIP address. The management IP address for NetScaler Gateway that is used for all management-related access to the appliance. NetScaler Gateway also uses the NSIP address for authentication.
- **Default gateway**. The router that forwards traffic from outside the secure network to NetScaler Gateway.
- **Subnet IP (SNIP) address**. The IP address that represents the user device by communicating with a server on a secondary network.

The SNIP address uses ports 1024 through 64000.

How NetScaler Gateway uses IP addresses

NetScaler Gateway sources traffic from IP addresses based on the function that is occurring. The following list describes several functions and the way NetScaler Gateway uses IP addresses for each, as a general guideline:

- **Authentication.** The IP address that NetScaler Gateway uses depends on the authentication server type.
  - LDAP/RADIUS/TACACS servers. If AAAD directly communicates with the authentication virtual server, then the NSIP address is used.
  - If a load balancer is used as proxy, then the load balancer uses the SNIP address for authentication. AAAD uses the NSIP address to communicate with the load balancer. The IP address that the NetScaler uses depends on the entity that is communicating with the authentication virtual server.
  - SAML/OAUTH/WEBAUTH servers: These servers communicate using the SNIP address.
- **File transfers from the home page.** NetScaler Gateway uses the SNIP address.
- **DNS and WINS queries.** NetScaler Gateway uses the SNIP address.
- **Network traffic to resources in the secure network.** NetScaler Gateway uses the SNIP address or IP pooling, depending on the configuration on NetScaler Gateway.
- **ICA proxy setting.** NetScaler Gateway uses the SNIP address.

Subnet IP addresses

The subnet IP address allows the user to connect to NetScaler Gateway from an external host that resides on another subnet. When you add a subnet IP address, a corresponding route entry is made

in the route table. Only one entry is made per subnet. The route entry corresponds to the first IP address added in the subnet.

Unlike the system IP address and the mapped IP address, it is not mandatory to specify the subnet IP address during the initial configuration of NetScaler Gateway.

The mapped IP address and subnet IP addresses use ports 1024 through 64000.

To add a subnet IP address

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **System \ > Network**, and then click **IPs**.
2. In the details pane, click **Add**.
3. In the Create IP dialog box, in IP Address, type the IP address.
4. In Netmask, type the subnet mask.
5. Under IP Type, select Subnet IP, click **Close,** and then click **Create**.

Configure IPv6 for user connections

You can configure NetScaler Gateway to listen for user connections by using Internet Protocol version 6 (IPv6). When you configure one of the following settings, you can select the IPv6 check box and then enter the IPv6 address in the dialog box:

- Global Settings - Published Applications - ICA Proxy
- Global Authentication - RADIUS
- Global Authentication - LDAP
- Global Authentication - TACACS
- Session Profile - Published Applications - ICA Proxy
- NetScaler Gateway Virtual Servers
- Create Authentication Server - RADIUS
- Create Authentication Server - LDAP
- Create Authentication Server - TACACS
- Create Auditing Server
- High Availability Setup
- Bind / Unbind Route Monitors for High Availability
- Virtual server (Load Balancing)

When you configure the NetScaler Gateway virtual server to listen on an IPv6 address, users can connect only with Citrix Workspace app. User connections with the Citrix Secure Access client are not supported with IPv6.

You can use the following guidelines for configuring IPv6 on NetScaler Gateway:

- Citrix Virtual Apps and Web Interface. When you configure IPv6 for user connections and if there is a mapped IP address that uses IPv6, Citrix Virtual Apps and Web Interface servers can also use IPv6. The Web Interface must be installed behind NetScaler Gateway. When users connect through NetScaler Gateway, the IPv6 address is translated to IPv4. When the connection returns, the IPv4 address is translated to IPv6.
- Virtual servers. You can configure IPv6 for a virtual server when you run the NetScaler Gateway wizard. In the NetScaler Gateway wizard on the Virtual Servers page, click IPv6 and enter the IP address. You can only use configure an IPv6 address for a virtual server by using the NetScaler Gateway wizard.
- Other. To configure IPv6 for ICA Proxy, authentication, auditing, and high availability, select the IPv6 check box in the dialog box and then type the IP address.

Resolve DNS servers located in the secure network

January 8, 2024

If your DNS server is located in the secure network behind a firewall and the firewall is blocking ICMP traffic, you cannot test connections to the server because the firewall is blocking the request. You can resolve this issue by doing the following steps:

- Creating a DNS service with a custom DNS Monitor that resolves to a known fully qualified domain name (FQDN).
- Creating a non-directly addressable DNS virtual server on NetScaler Gateway.
- Binding the service to the virtual server.

Note:

- Configure a DNS virtual server and DNS service only if your DNS server is located behind a firewall.
- If you install a NetScaler load balancing license on the appliance, the Virtual Servers and Services node does not appear in the navigation pane. You can perform this procedure by expanding Load Balancing and then clicking Virtual Servers.

To configure a DNS service and DNS Monitor

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand Virtual Servers and Services and then click Virtual Servers.
2. In the details pane, click Add.
3. In Name, type a name for the service.

4. In Protocol, select DNS.
5. In IP Address, type the IP address of the DNS server.
6. In Port, type the port number.
7. On the Services tab, click Add.
8. On the Monitors tab, under Available, select DNS, click Add, click Create, and then click Close.
9. In the Create Virtual Server (Load Balancing) dialog box, click Create and then click Close.

Next, create the DNS virtual server by using the procedure To configure a DNS virtual server and then bind the DNS service to the virtual server.

To bind a DNS service to a DNS virtual server

1. In the Configure Virtual Service (Load Balancing) dialog box, on the Services tab, click Add, select the DNS service, click Create, and then click Close.

Configure DNS virtual servers

January 8, 2024

To configure a DNS virtual server, you specify a name and IP address. Like the NetScaler Gateway virtual server, you must assign an IP address to the DNS virtual server. However, this IP address must be on the internal side of the targeted network so that user devices resolve all internal addresses. Also, specify the DNS port.

Note: If you install a NetScaler load balancing license on the appliance, the
Virtual Servers and Services node does not appear in the navigation pane. You can configure this feature by using the load balancing virtual server. For more information, see the NetScaler documentation in the NetScaler product Documentation.

To configure a DNS virtual server

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand Virtual Servers and Services and then click Virtual Servers.
2. In the details pane, click Add.
3. In Name, type a name for the virtual server.
4. In IP Address, type the IP address of the DNS server.
5. In Port, type the port on which the DNS server listens.
6. In Protocol, select DNS and then click Create.

Finally, associate the DNS virtual server with NetScaler Gateway through one of the following two methods, depending on the needs of your deployment:

- Bind the server globally to NetScaler Gateway.
- Bind the DNS virtual server on a per-virtual server basis.

If you deploy the DNS virtual server globally, all users have access to it. Then, you can restrict users by binding the DNS virtual server to the virtual server.

Configure name service providers

January 8, 2024

NetScaler Gateway uses name service providers to convert web addresses to IP addresses.

When you run the NetScaler Gateway wizard, you can configure either a DNS server or a WINS server. You can use the configuration utility to also configure other DNS or WINS servers.

To add a DNS server to NetScaler Gateway

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Network Configuration tab, click Add.
4. In the Insert Name Server dialog box, in IP Address, type the IP address of the DNS server, click Create, and then click Close.
5. Click OK in the configuration utility.

To add a WINS server to NetScaler Gateway

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Network Configuration tab, in WINS Server IP, type the IP address of the WINS server and then click OK.

Next, specify the DNS virtual server name and IP address. Like the NetScaler Gateway virtual server, an IP address must be assigned to the virtual server. However, this IP address must be on the internal side of the targeted network so that user devices resolve all internal addresses properly. You must also specify the DNS port.

If you configure a DNS server and WINS server for name resolution, you can then use the NetScaler Gateway wizard to select which server performs name lookup first.

To specify name lookup priority

1. In the configuration utility, click the Configuration tab and then in the navigation pane, click NetScaler Gateway.
2. In the details pane, under Getting Started, click NetScaler Gateway wizard.
3. Click Next to accept the current settings until you come to the Name Service Providers page.
4. In Name Lookup Priority, select WINS or DNS and then continue to the end of the wizard.

Configure server-initiated connections

January 8, 2024

For each user logged on to NetScaler Gateway with IP addresses enabled, the DNS suffix is appended to the user name and a DNS address record is added to the appliance's DNS cache. This technique helps in providing users with a DNS name rather than the IP addresses of the users.

When an IP address is assigned to a user's session, it is possible to connect to the user's device from the internal network. For example, users connecting with the Remote Desktop or a virtual network computing (VNC) client can access the user device for diagnosing a problem application. It is also possible for two NetScaler Gateway users with internal network IP addresses who are remotely logged on to communicate with each other through NetScaler Gateway. Allowing discovery of the internal network IP addresses of the logged-on users on the appliance aids in this communication.

A remote user can use the following ping command to discover the internal network IP address of a user who can be logged on to NetScaler Gateway then:

```
ping \<username.domainname\>
```

A server can initiate a connection to a user device in the following different ways:

- TCP or UDP connections. The connections can originate from an external system in the internal network or from another computer logged on to NetScaler Gateway. The internal network IP address that is assigned to each user device logged on to NetScaler Gateway is used for these connections. The different types of server-initiated connections that NetScaler Gateway supports are described.
  For TCP or UDP server-initiated connections, the server has prior knowledge about the user device's IP address and port and makes a connection to it. NetScaler Gateway intercepts this connection.

Then, the user device makes an initial connection to the server and the server connects to the user device on a port that is known or derived from the first configured port.

In this scenario, the user device makes an initial connection to the server and then exchanges ports and IP addresses with the server by using an application-specific protocol where this information is embedded. This enables the NetScaler Gateway to support applications, such as active FTP connections.

- Port command. This is used in an active FTP and in certain Voice over IP protocols.
- Connections between plug-ins. NetScaler Gateway supports connections between plug-ins by using the internal network IP addresses.

  With this type of connection, two NetScaler Gateway user devices that use the same NetScaler Gateway can initiate connections with each other. An example of this type is using instant messaging applications, such as Office Communicator or Yahoo! Messenger.

If a user logs off NetScaler Gateway and the logoff request did not reach the appliance, the user can log on again by using any device and replace the previous session with a new session. This feature might be beneficial in deployments where one IP address is assigned per user.

When a user logs on to NetScaler Gateway for the first time, a session is created and an IP address is assigned to the user. If the user logs off but the logoff request is lost or the user device fails to perform a clean logoff, the session is maintained on the system. If the user tries to log on again from the same device or another device, after successful authentication, a transfer logon dialog box appears. If the user chooses to transfer the logon, the previous session on NetScaler Gateway is closed and a new session is created. The transfer of logon is active for only two minutes after logoff, and if logon is attempted from multiple devices simultaneously, the last logon attempt replaces the original session.

Configure private port range for server-initiated connections

Starting from Citrix Secure Access client release 23.10.1.7, you can configure a private port ranging from 49152 to 64535 for server-initiated connections (SIC). Configuring private ports avoids conflicts that might arise when you use ports to create sockets between Citrix Secure Access client and third party apps on the client machines. This is applicable only if the WFP driver is in use.

You can configure the private ports by using the `SicBeginPort` Windows VPN registry. Alternatively, you can configure the private port range by using a VPN plug-in customization JSON file on NetScaler.

If a server initiates a connection, Citrix Secure Access client uses the first 1000 ports starting from the `SicBeginPort` Windows VPN registry, to create the sockets. If the registry is configured on a client machine, the registry setting takes precedence over the NetScaler JSON setting.

The following is an example of the VPN plug-in JSON configuration on NetScaler:


```
root@ADC# cat /var/netscaler/gui/vpn/pluginCustomization.json

{
 "SicBeginPort" : 51000 }
```

For details about the registry settings, see NetScaler Gateway Windows VPN client registry keys.

> **Note:**
>
> The default port range that is used to create sockets is 62500–63500.

Configure routing on NetScaler Gateway

January 8, 2024

To provide access to internal network resources, NetScaler Gateway routes data to your internal, secure networks. By default, NetScaler Gateway uses a static route.

The networks to which NetScaler Gateway can route data are determined by the way you configure the NetScaler Gateway routing table and the default gateway that you specify for NetScaler Gateway.

The NetScaler Gateway routing table must contain the routes necessary to route data to any internal network resource that a user might need to access.

NetScaler Gateway supports the following routing protocols:

- Routing Information Protocol (RIP v1 and v2)
- Open Shortest Path First (OSPF)
- Border Gateway Protocol (BGF)

Configure a static route

When setting up communication with another host or network, you need to configure a static route from NetScaler Gateway to the new destination if you do not use dynamic routing.

To configure a static route

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **System > Network > Advanced** and then click **Routes**.
2. In the details pane, on the Basic tab, click **Add**.
3. Configure the settings for the route, and then click **Create**.

To test a static route

1. In the configuration utility, in the navigation pane, expand **System,** and then click **Diagnostics**.
2. In the details pane, under Utilities, click **Ping**.
3. Under Parameters, in Host name, type the name of the device.
4. Under Advanced, in Source IP Address, type the IP address of the device, and then click **Run**.

   If you are successfully communicating with the other device, messages indicate that the same number of packets were transmitted and received, and zero packets were lost.

   If you are not communicating with the other device, the status messages indicate that zero packets were received and all the packets were lost. To correct this lack of communication, repeat the procedure to add a static route.

To stop the test, in the **Ping** dialog box, click **Stop,** and then click **Close**.

Configure auto negotiation

January 8, 2024

By default, the appliance is configured to use auto negotiation, in which NetScaler Gateway transmits network traffic both directions simultaneously and determines the appropriate adapter speed. If you leave the default setting to
Auto Negotiation, NetScaler Gateway uses full-duplex operation, in which the network adapter is capable of sending data in both directions simultaneously.

If you disable auto negotiation, NetScaler Gateway uses half-duplex operation, in which the adapter can send data in both directions between two nodes, but the adapter can only use one direction or the other at a time.

For first time installation, Citrix recommends that you configure NetScaler Gateway to use auto negotiation for ports that are connected to the appliance. After you log on initially and configure NetScaler Gateway, you can disable auto negotiation. You cannot configure auto negotiation globally. You must enable or disable the setting for each interface.

To enable or disable auto negotiation

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **System \ > Network,** and then click **Interfaces**.
2. In the details pane, select the interface, and then click **Open**.

3. Do one of the following in the **Configure Interface** dialog box:
    - To enable auto negotiation, click **Yes** next to Auto Negotiation, and then click **OK**.
    - To disable auto negotiation, click **No** next to Auto Negotiation, and then click **OK**.

Configure the host name and FQDN on NetScaler Gateway

January 8, 2024

The host name is the name of the NetScaler Gateway appliance that is associated with the license file. The host name is unique to the appliance and is used when you download the Universal license. You define the host name when you run the Setup Wizard to configure NetScaler Gateway for the first time.

The fully qualified domain name (FQDN) is included in the signed certificate that is bound to a virtual server. You do not configure the FQDN on NetScaler Gateway. One appliance can have a unique FQDN assigned to each virtual server that is configured on NetScaler Gateway by using certificates.

You can find the FQDN of a certificate by viewing the details of the certificate. The FQDN is located in the subject field of the certificate.

To view the FQDN of a certificate

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **SSL,** and then click **Certificates**.
2. In the details pane, select a certificate, click **Action,** and then click **Details**.
3. In the Certificate Details dialog box, click **Subject**. The FQDN of the certificate appears in the list.

Policies and profiles on NetScaler Gateway

January 8, 2024

Policies and profiles on NetScaler Gateway allow you to manage and implement configuration settings under specified scenarios or conditions. An individual policy states or defines the configuration settings that go into effect when a specified set of conditions is met. Each policy has a unique name and can have a profile bound to the policy.

How policies work

A policy consists of a Boolean condition and collection of settings called a profile. The condition is evaluated at runtime to determine if the policy must be applied.

A profile is a collection of settings, using specific parameters. The profile can have any name and you can reuse it in more than one policy. You can configure multiple settings within the profile, but you can only include one profile per policy.

You can bind policies, with the configured conditions and profiles, to virtual servers, groups, users, or globally. Policies are referred to by the type of configuration settings they control. For example, in a session policy, you can control how users log on and the number of time users can stay logged on.

If you are using NetScaler Gateway with Citrix Virtual Apps, NetScaler Gateway policy names are sent to Citrix Virtual Apps as filters. When configuring NetScaler Gateway to be compatible with Citrix Virtual Apps and SmartAccess, you configure the following settings in Citrix Virtual Apps:

- The name of the virtual server that is configured on the appliance. The name is sent to Citrix Virtual Apps as the NetScaler Gateway farm name.
- The names of the pre-authentication or session policies are sent as filter names.

For more information about configuring NetScaler Gateway to be compatible with Citrix Endpoint Management, see Configuring Settings for Your Citrix Endpoint Management Environment.

For more information about configuring NetScaler Gateway to be compatible with Citrix Virtual Apps and Desktops, see Accessing Citrix Virtual Apps and Citrix Virtual Desktops Resources with the Web Interface and Integrating with Citrix Endpoint Management or StoreFront.

For more information about preauthentication policies, see Configuring Endpoint Polices.

Conditional policies

When configuring policies, you can use any Boolean expression to express the condition for when the policy applies. When you configure conditional policies, you can use any of the available system expressions, such as the following:

- Client security strings
- Network information
- HTTP headers and cookies
- Time of day
- Client certificate values

You can also create policies to apply only when the user device meets specific criteria, such as a session policy for SmartAccess.

Another example of configuring a conditional policy is varying the authentication policy for users. For example, you can require users who are connecting with the Citrix Secure Access client from outside the internal network, such as from their home computer or by using Micro VPN from a mobile device, to be authenticated by using LDAP and users who are connecting through the WAN to be authenticated using RADIUS.

Note: You cannot use policy conditions based on endpoint analysis results if the policy rule is configured as part of security settings in a session profile.

Priorities of policies

Policies are prioritized and evaluated in the order in which the policy is bound.

The following two methods determine policy priority:

- The level to which the policy is bound: globally, virtual server, group, or user. Policy levels are ranked from highest to lowest as follows:
  - User (highest priority)
  - Group
  - Virtual server
  - Global (lowest priority)
- Numerical priority takes precedence regardless of the level at which the policy is bound. If a policy that is bound globally has a priority number of one and another policy bound to a user has a priority number of two, the global policy takes precedence. A lower priority number gives the policy a higher precedence.

Create policies on NetScaler Gateway

You can use the configuration utility to create policies. After you create a policy, you bind the policy to the appropriate level: user, group, virtual server, or global. When you bind a policy to one of these levels, users receive the settings within the profile if the policy conditions are met. Each policy and profile has a unique name.

If you have Citrix Endpoint Management or StoreFront as part of your deployment, you can use the Quick Configuration wizard to configure the settings for this deployment. For more information about the wizard, see Configuring Settings with the Quick Configuration Wizard.

Configuring System Expressions

January 8, 2024

A system expression specifies the conditions under which the policy is enforced. For example, expressions in a preauthentication policy are enforced while a user is logging on. Expressions in a session policy are evaluated and enforced after the user is authenticated and logged on to NetScaler Gateway.

Expressions on NetScaler Gateway include:

- General expressions that limit the objects users can use when establishing a connection to NetScaler Gateway. For example, see:
  - Session policies
- Client security expressions that define the software, files, processes, or registry values that must be installed and running on the user device. For example, see:
  - Endpoint policies
- Network-based expressions that restrict access based on network settings. For example, see:
  - Traffic policies
  - Authorization policies

NetScaler Gateway can also be used as a NetScaler appliance. Some expressions on the appliance are more applicable to NetScaler. General and network-based expressions are used commonly with NetScaler and are not generally used with NetScaler Gateway. Client security expressions are used on NetScaler Gateway to determine that the correct items are installed on the user device.

Configuring Client Security Expressions

Expressions are a component of a policy. An expression represents a single condition that is evaluated against a request or a response. You can create a simple expression security string to check for conditions, such as:

- User device operating system including service packs
- Antivirus software version and virus definitions
- Files
- Processes
- Registry values
- User certificates

Certificates management on NetScaler Gateway

January 8, 2024

On NetScaler Gateway, you use certificates to create secure connections and to authenticate users.

To establish a secure connection, a server certificate is required at one end of the connection. A root certificate of the Certificate Authority (CA) that issued the server certificate is required at the other end of the connection.

- Server certificate. A server certificate certifies the identity of the server. NetScaler Gateway requires this type of digital certificate.
- Root certificate. A root certificate identifies the CA that signed the server certificate. The root certificate belongs to the Certificate Authority. A user device requires this type of digital certificate to verify the server certificate.

When establishing a secure connection with a web browser on the user device, the server sends its certificate to the device.

When the user device receives a server certificate, the web browser, such as Internet Explorer checks to see which CA issued the certificate and if the CA is trusted by the user device. If the CA is not trusted, or if it is a test certificate, the web browser prompts the user to accept or decline the certificate (effectively accepting or declining the ability to access the site).

NetScaler Gateway supports the following three types of certificates:

- A test certificate that is bound to a virtual server and can also be used for connections to a server farm. NetScaler Gateway comes with a pre-installed test certificate.
- A certificate in PEM or DER format that is signed by a CA and is paired with a private key.
- A certificate in PKCS#12 format that is used for storing or transporting the certificate and private key. The PKCS#12 certificate is typically exported from an existing Windows certificate as a PFX file and then installed on NetScaler Gateway.

Citrix recommends using a certificate signed by a trusted CA, such as Thawte or Verisign.

Create a certificate signing request

January 8, 2024

To provide secure communications using SSL or TLS, a server certificate is required on NetScaler Gateway. Before you can upload a certificate to NetScaler Gateway, you need to generate a Certificate Signing Request (CSR) and private key. You use the Create Certificate Request included in the NetScaler

Gateway wizard or the configuration utility to create the CSR. The Create Certificate Request creates a .csr file that is emailed to the Certificate Authority (CA) for signing and a private key that remains on the appliance. The CA signs the certificate and returns it to you at the email address you provided. When you receive the signed certificate, you can install it on NetScaler Gateway. When you receive the certificate back from the CA, you pair the certificate with the private key.

Important: When you use the NetScaler Gateway wizard to create the CSR, you must exit the wizard and wait for the CA to send you the signed certificate. When you receive the certificate, you can run the NetScaler Gateway wizard again to create the settings and install the certificate. For more information about the NetScaler Gateway wizard, see
Configuring Settings by Using the NetScaler Gateway Wizard.

Create a CSR by using the NetScaler Gateway wizard

1. In the configuration utility, click the Configuration tab and then in the navigation pane, click **NetScaler Gateway**.
2. In the details pane, under Getting Started, click **NetScaler Gateway** wizard.
3. Follow the directions in the wizard until you come to the Specify a server certificate page.
4. Click **Create a Certificate Signing Request** and complete the fields.
   Note: The fully qualified domain name (FQDN) does not need to be the same as the NetScaler Gateway host name. The FQDN is used for user logon.
5. Click **Create** to save the certificate on your computer, and then click **Close**.
6. Exit the NetScaler Gateway wizard without saving your settings.

Create a CSR by using the NetScaler GUI

You can also use the NetScaler GUI to create a CSR, without running the NetScaler Gateway wizard.

1. Navigate to **Traffic Management** > **SSL > SSL Files** and select **Create Certificate Signing Request (CSR)**.
2. Complete the settings for the certificate and then click **Create**.

After you create the certificate and private key, email the certificate to the CA, such as Thawte or Verisign.

For detailed procedure, see Create a certificate signing request.

Install the signed certificate on NetScaler Gateway

When you receive the signed certificate from the Certificate Authority (CA), pair it with the private key on the appliance and then install the certificate on NetScaler Gateway.

Pair the signed certificate with a private key by using the GUI

1. Copy the certificate to NetScaler Gateway to the folder nsconfig/ssl by using a Secure Shell (SSH) program such as WinSCP.
2. In the configuration utility, on the Configuration tab, in the navigation pane, expand **SSL > Certificates**.
3. In the **SSL Certificate** page, click **Get Started**.
4. In the details pane, click **Install**.
5. In **Certificate-Key Pair Name**, type the name of the certificate.
6. In **Certificate File Name**, click **Appliance**.
7. Navigate to the certificate, click **Select**, and then click **Open**.
8. In **Key File Name**, click **Appliance**. The name of the private key is the same name as the Certificate Signing Request (CSR). The private key is located on NetScaler Gateway in the directory \nsconfig\ssl.
9. Choose the private key, and then click **Open**.
10. If the certificate is PEM-format, in **Password**, type the password for the private key.
11. If you want to configure notification for when the certificate expires, select **Notify When Expires**.
12. In **Notification Period**, type the number of days, click **Create**, and then click **Close**.

Bind the certificate and private key to a virtual server by using the GUI

After you create and link a certificate and private key pair, bind it to a virtual server.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway > Virtual Servers**.
2. In the details pane, click a virtual server, and then click **Open**.
3. On the Certificates tab, under **Available**, select a certificate, click **Add**, and then click **OK**.

Bind the certificate and private key to a virtual server by using the CLI

At the command prompt, type;

```
bind ssl vserver <vServerName> -certkeyName <string> -ocspCheck (
    Mandatory | Optional )
```

Example:

```
bind ssl vserver TestClient -CertkeyName ag51.xm.nsi.test.com -CA -
    ocspCheck Mandatory
```

Note: oscpCheck is optional if OCSP check is not required for device certificate.

Unbind test certificates from the virtual server by using the GUI

After you install the signed certificate, unbind any test certificates that are bound to the virtual server. You can unbind test certificates using the configuration utility.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway > Virtual Servers**.
2. In the details pane, click a virtual server, and then click **Open**.
3. On the Certificates tab, under **Configured**, select the test certificate, and then click **Remove**.

Configure intermediate certificates

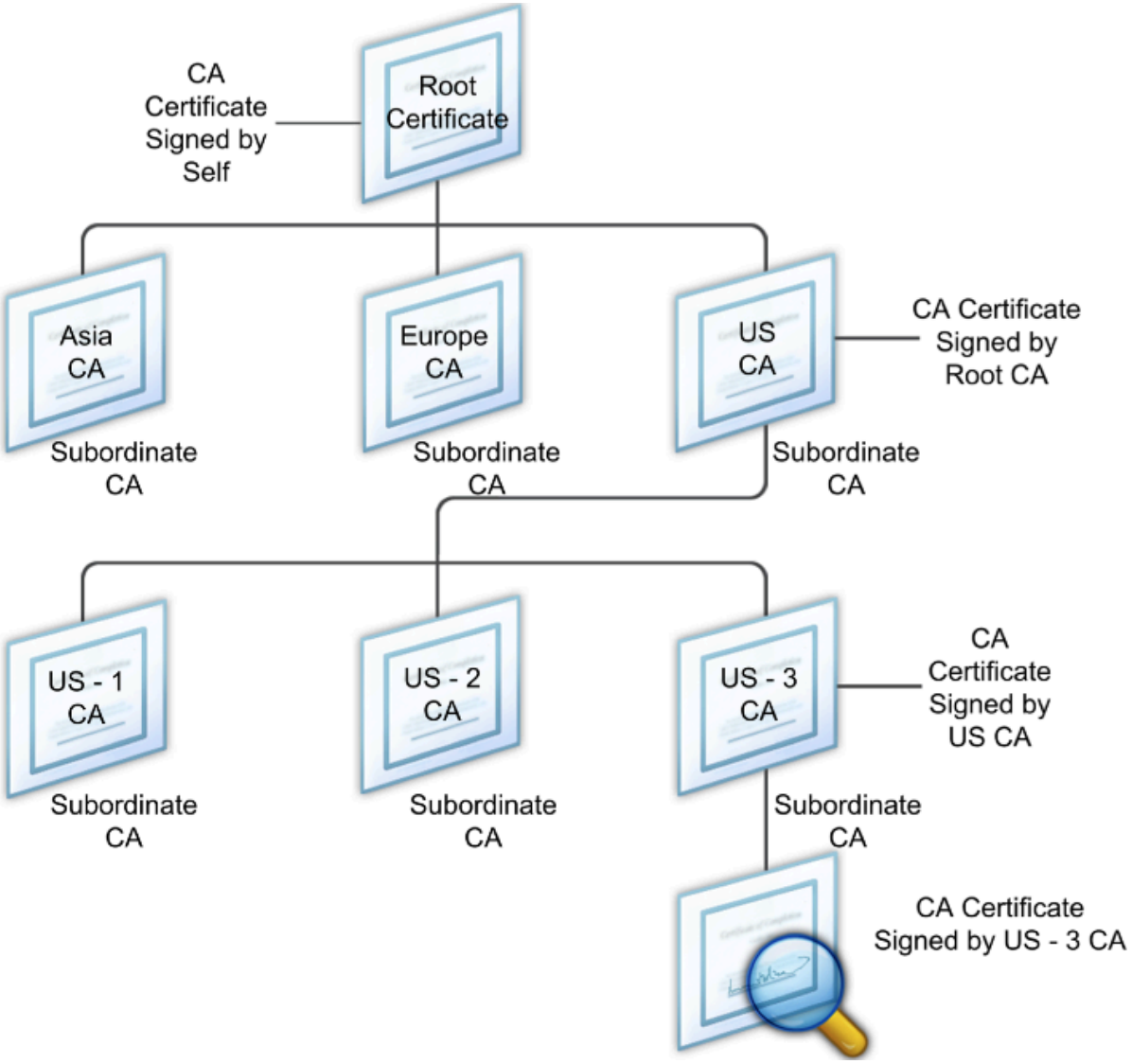
January 8, 2024

An intermediate certificate is a certificate that goes between NetScaler Gateway (the server certificate) and a root certificate (installed on the user device). An intermediate certificate is part of a chain.

Some organizations delegate the responsibility for issuing certificates to resolve the issue of geographical separation between organization units, or to apply different issuing policies to different sections of the organization.

Responsibility for issuing certificates can be delegated by setting up subordinate Certificate Authorities (CAs). CAs can sign their own certificates (that is, they are self-signed) or they can be signed by another certificate authority. The X.509 standard includes a model for setting up a hierarchy of CAs. In this model, as shown in the following figure, the root CA is at the top of the hierarchy and is a self-signed certificate by the certificate authority. The CAs that are directly subordinate to the root CA have CA certificates signed by the root certificate authority. CAs under the subordinate CAs in the hierarchy have their CA certificates signed by the subordinate CAs.

Figure 1. The X.509 model showing the hierarchical structure of a typical digital certificate chain



If a server certificate is signed by a CA with a self-signed certificate, the certificate chain is composed of exactly two certificates: the end entity certificate and the root certificate authority. If a user or server certificate is signed by an intermediate certificate authority, the certificate chain is longer.

The following figure shows that the first two elements are the end entity certificate (in this case, gwy01.company.com) and the certificate of the intermediate certificate authority, in that order. The intermediate certificate authority's certificate is followed by the certificate of its certificate authority. This listing continues until the last certificate in the list is for a root certificate authority. Each certificate in the chain attests to the identity of the previous certificate.

Figure 2. A typical digital certificate chain

Install an intermediate certificate

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand SSL and then click Certificates.
2. In the details pane, click Install.
3. In Certificate-Key Pair Name, type the name of the certificate.
4. Under Details, in Certificate File Name, click Browse (Appliance) and in the list, select Local or Appliance.
5. Navigate to the certificate on your computer (Local) or on NetScaler Gateway (Appliance).
6. In Certificate Format, select PEM.
7. Click Install and then click Close.

When you install an intermediate certificate on NetScaler Gateway, you do not need to specify the private key or a password.

After the certificate is installed on the appliance, the certificate needs to be linked to the server certificate.

Link an intermediate certificate to a server certificate

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand SSL and then click Certificates.
2. In the details pane, select the server certificate and then in Action, click Link.
3. Next to CA Certificate Name, select the intermediate certificate from the list and then click OK.

Use device certificates for authentication

January 8, 2024

NetScaler Gateway supports the device certificate check that enables you to bind the device identity to a certificate's private key. The device certificate check can be configured as part of classic or advanced

Endpoint Analysis (EPA) policies. In classic EPA policies, the device certificate can be configured only for preauthentication EPA.

NetScaler Gateway verifies the device certificate before the endpoint analysis scan runs or before the logon page appears. If you configure endpoint analysis, the endpoint scan runs to verify the user device. When the device passes the scan and after NetScaler Gateway verifies the device certificate, users can then log on to the NetScaler Gateway.

> **Important:**
>
> - By default, Windows mandates admin privileges for accessing device certificates.
> - To add a device certificate check for non-admin users, you must install the VPN plug-in. The VPN plug-in version must be the same version as the EPA plug-in on the device.
> - You can add multiple CA certificates to the gateway and validate the device certificate.
> - If you install two or more device certificates on NetScaler Gateway, users must select the correct certificate when they start to log on to NetScaler Gateway or before the endpoint analysis scan runs.
> - When you create the device certificate, it must be an X.509 certificate.
> - If you have a device certificate issued by an intermediate CA, then both intermediate and root CA certificates must be bound.
> - The EPA client needs the user to have local administrator rights to be able to access the machine certificate store. This is rarely the case, so a workaround is to install the full NetScaler Gateway plug-in which can access the local store.

For more information about creating device certificates, see the following:

- Network Device Enrollment Service (NDES) in Active Directory Certificate Services (AD CS) on the Microsoft website.
- How to request a certificate from a Microsoft Certificate Authority using DCE/RPC and the Active Directory Certificate profile payload on the Apple support website.
- iPad / iPhone Certificate Issuance on the Ask the Directory Services Team Microsoft support blog.
- Setting Up Network Device Enrollment Service on the Windows IT Pro website.
- Step-by-Step Example Deployment of the PKI Certificates for Configuration Manager: Windows Server 2008 Certification Authority on the Microsoft System Center website.

Steps to configure device certificates

To configure a device certificate, you must complete the following steps:

- Install the device certificate issuer's certificate authority certificate on NetScaler Gateway. For details, see Installing the Signed Certificate on NetScaler Gateway.

- Bind the device certificate issuer's certificate authority certificate to the NetScaler Gateway virtual server and enable OCSP check. For details, see Installing the Signed Certificate on NetScaler Gateway.
- Create and bind OCSP (responder) on device certificate issuer's certificate authority certificate. For details, see Monitor certificate status with OCSP.

Enable device certificate check on the virtual server and add device certificate issuer's certificate authority certificate to the device certificate checklist. For details, see Enable device certificate check on a virtual server for classic EPA policy.

Complete the client-side configuration and verification of device certificate on the Windows machine. For details, see Verification of device certificate on a Windows machine.

> **Note:**
>
> All the clients intended to avail the device certificate EPA check must have the device certificate installed in the system certificate store of the machine.

Enable device certificate check on a virtual server for classic EPA policy

After you create the device certificate, you install the certificate on NetScaler Gateway by using the procedure for Importing and Installing an Existing Certificate to NetScaler Gateway.

1. On the Configuration tab, navigate to **NetScaler Gateway > Virtual Servers**.
2. On the **NetScaler Gateway Virtual Servers** page, select an existing virtual server and click **Edit**.
3. On the **VPN Virtual Servers** page, under **Basic Settings** section, click **Edit**.
4. Clear the **Enable Authentication** box to disable authentication.
5. Select the **Enable Device Certificate** box to enable device certificate
6. Click **Add** to add an available device certificate issuer's CA certificate name to the list.
7. For binding a CA certificate to the virtual server, click **CA certificate** under the **CA for Device Certificate** section, click **Add**, select the certificate, and then click **+**.

> **Note:**
>
> For information on enabling and binding device certificates on a virtual server for advanced EPA policy, see Device Certificate in nFactor as an EPA component.

Verification of device certificate on a Windows machine

1. Open a browser and access the NetScaler Gateway FQDN.
2. Allow the Citrix End Point Analysis (EPA) client to run. If not already installed then install EPA.

Citrix EPA runs and validates the Device Certificate and redirects to the authentication page if the Device Certificate EPA check passes, else it redirects you to the EPA error page. In case you have other EPA checks, then the EPA scan results depend on the configured EPA checks.

For further debugging on the client, examine the following EPA logs on the client:
C:\Users<User name>\AppData\Local\Citrix\AGEE\nsepa.txt

Note:

> Device certificate verification with CRL is not supported.

Import and install an existing certificate

January 8, 2024

You can import an existing certificate from a Windows-based computer running Internet Information Services (IIS) or from a computer running the Secure Gateway.

When you export the certificate, make sure you also export the private key. Sometimes, you cannot export the private key, which means you cannot install the certificate on NetScaler Gateway. If this occurs, use the Certificate Signing Request (CSR) to create a certificate. For details, see Creating a Certificate Signing Request.

When you export a certificate and private key from Windows, the computer creates a Personal Information Exchange (.pfx) file. This file is then installed on NetScaler Gateway as a PKCS#12 certificate.

If you are replacing the Secure Gateway with NetScaler Gateway, you can export the certificate and private key from the Secure Gateway. If you are doing an in-place migration from the Secure Gateway to NetScaler Gateway, the fully qualified domain name (FQDN) on the application and the appliance must be the same. When you export the certificate from the Secure Gateway, you immediately retire the Secure Gateway, install the certificate on NetScaler Gateway, and then test the configuration. The Secure Gateway and NetScaler Gateway cannot be running on your network at the same time if they have the same FQDN.

If you are using Windows Server 2003 or Windows Server 2008, you can use the Microsoft Management Console to export the certificate. For more information, see the Windows online Help.

Leave the default values for all the other options, define a password, and save the .pfx file to your computer. When the certificate is exported, you then install it on NetScaler Gateway.

To install the certificate and private key on NetScaler Gateway

1. In the configuration utility, click the Configuration tab and then in the navigation pane, click **NetScaler Gateway**.
2. In the details pane, under Getting Started, click **NetScaler Gateway wizard**.
3. Click **Next**, select an existing virtual server, and then click **Next**.
4. In **Certificate Options**, select **Install a PKCS#12 (.pfx) fil**e.
5. In **PKCS#12 File Name**, click **Browse**, navigate to the certificate, and then click **Select**.
6. In ((Password)), type the password for the private key.

   This is the password you used when converting the certificate to PEM format.
7. Click **Next** to finish the NetScaler Gateway wizard without changing any other settings.

When the certificate is installed on NetScaler Gateway, the certificate appears in the configuration utility in the **SSL \ > Certificates** node.

To create a private Key

1. In the configuration utility, on the Configuration tab, in the navigation pane, click **SSL**.
2. In the details pane, under **SSL Keys**, click **Create RSA Key**.
3. In **Key Filename**, type the name of the private key or click Browse to navigate to an existing file.
4. In **Key Size (Bits)**, type the size of the private key.
5. In **Public Exponent Value**, select F4 or 3.

   The public exponent value for the RSA key. This is part of the cipher algorithm and is required for creating the RSA key. The values are F4 (Hex: 0x10001) or 3 (Hex: 0x3). The default is F4.
6. In **Key Format**, select PEM or DER. Citrix recommends PEM format for the certificate.
7. In **PEM Encoding Algorithm**, select DES or DES3.
8. In **PEM Passphrase** and **Verify Passphrase**, type the password, click **Create**, and then click **Close**.

   Note: To assign a passphrase, the Key Format must be PEM and you must select the encoding algorithm.

To create a DSA private key in the configuration utility, click **Create DSA Key** and follow the steps performed for creating the RSA private key.

Certificate revocation lists

January 8, 2024

From time to time, Certificate Authorities (CAs) issue certificate revocation lists (CRLs). CRLs contain information about certificates that can no longer be trusted. For example, suppose Ann leaves XYZ Corporation. The company can place Ann's certificate on a CRL to prevent her from signing messages with that key.

Similarly, you can revoke a certificate if a private key is compromised or if that certificate expired and a new one is in use. Before you trust a public key, make sure that the certificate does not appear on a CRL.

NetScaler Gateway supports the following two CRL types:

- CRLs that list the certificates that are revoked or are no longer valid
- Online Certificate Status Protocol (OSCP), an Internet protocol used for obtaining the revocation status of X.509 certificates

To add a CRL:

Before you configure the CRL on the NetScaler Gateway appliance, make sure that the CRL file is stored locally on the appliance. In the case of a high availability setup, the CRL file must be present on both NetScaler Gateway appliances, and the directory path to the file must be the same on both appliances.

If you need to refresh the CRL, you can use the following parameters:

- CRL Name: The name of the CRL being added on the NetScaler. Maximum 31 characters.
- CRL File: The name of the CRL file being added on the NetScaler. The NetScaler looks for the CRL file in the /var/netscaler/ssl directory by default. Maximum 63 characters.
- URL: Maximum 127 characters
- Base DN: Maximum 127 characters
- Bind DN: Maximum 127 characters
- Password: Maximum 31 characters
- Days: Maximum 31

1. In the configuration utility, on the Configuration tab, expand SSL and then click CRL.
2. In the details pane, click Add.
3. In the Add CRL dialog box, specify the values for the following:
    - CRL Name
    - CRL File
    - Format (optional)

- CA Certificate (optional)

4. Click **Create** and then click **Close**. In the CRL details pane, select the CRL that you configured and verify that the settings that appear at the bottom of the screen are correct.

To configure CRL autorefresh by using LDAP or HTTP in the GUI:

A CRL is generated and published by a CA periodically or, sometimes, immediately after a particular certificate is revoked. Citrix recommends that you update CRLs on the NetScaler Gateway appliance regularly for protection against clients trying to connect with certificates that are not valid.

The NetScaler Gateway appliance can refresh CRLs from a web location or an LDAP directory. When you specify refresh parameters and a web location or an LDAP server, the CRL does not have to be present on the local hard disk drive at the time you run the command. The first refresh stores a copy on the local hard disk drive, in the path specified by the CRL File parameter. The default path for storing the CRL is /var/netscaler/ssl.

CRL refresh parameters

- **CRL Name**

  The name of the CRL being refreshed on the NetScaler Gateway.

- **Enable CRL Auto Refresh**

  Enable or disable CRL auto refresh.

- **CA Certificate**

  The certificate of the CA that has issued the CRL. This CA certificate must be installed on the appliance. The NetScaler can update CRLs only from CAs whose certificates are installed on it.

- **Method**

  Protocol in which to obtain the CRL refresh from a web server (HTTP) or an LDAP server. Possible Values: HTTP, LDAP. Default: HTTP.

- **Scope**

  The extent of the search operation on the LDAP server. If the scope specified is Base, the search is at the same level as the base DN. If the scope specified is One, the search extends to one level below the base DN.

- **Server IP**

  The IP address of the LDAP server from which the CRL is retrieved. Select IPv6 to use an IPv6 IP address.

- **Port**

  The port number on which the LDAP or the HTTP server communicates.

- **URL**

  The URL for the web location from which the CRL is retrieved.

- **Base DN**

  The base DN used by the LDAP server to search for the CRL attribute.
  Note: Citrix recommends using the base DN attribute instead of the Issuer-Name from the CA certificate to search for the CRL in the LDAP server. The Issuer-Name field may not exactly match the LDAP directory structure's DN.

- **Bind DN**

  The bind DN attribute is used to access the CRL object in the LDAP repository. The bind DN attributes are the administrator credentials for the LDAP server. Configure this parameter to restrict unauthorized access to the LDAP servers.

- **Password**

  The administrator password used to access the CRL object in the LDAP repository. Password is required if the access to the LDAP repository is restricted, that is, anonymous access is not allowed.

- **Interval**

  The interval at which the CRL refresh must be carried out. For an instantaneous CRL refresh, specify the interval as NOW. Possible values: MONTHLY, DAILY, WEEKLY, NOW, NONE.

- **Days**

  The day on which the CRL refresh must be performed. The option is not available if the interval is set to DAILY.

- **Time**

  The exact time in 24-hour format when the CRL refresh must be performed.

- **Binary**

  Set the LDAP-based CRL retrieval mode to binary. Possible values: YES, NO. Default: NO.

1. In the navigation pane, expand SSL and then click CRL.
2. Select the configured CRL for which you want to update refresh parameters and then click Open.
3. Select the Enable CRL Auto Refresh option.
4. In the CRL Auto Refresh Parameters group, specify values for the following parameters:
   Note: An asterisk (*) indicates a required parameter.

   - Method
   - Binary
   - Scope

- Server IP
- Port*
- URL
- Base DN*
- Bind DN
- Password
- Interval
- Days
- Time

5. Click Create. In the CRL pane, select the CRL that you configured and verify that the settings that appear at the bottom of the screen are correct.

Monitor certificate status with OCSP

Online Certificate Status Protocol (OCSP) is an Internet protocol that is used to determine the status of a client SSL certificate. NetScaler Gateway supports OCSP as defined in RFC 2560. OCSP offers significant advantages over certificate revocation lists (CRLs) in terms of timely information. Up-to-date revocation status of a client certificate is especially useful in transactions involving large sums of money and high-value stock trades. It also uses fewer system and network resources. NetScaler Gateway implementation of OCSP includes request batching and response caching.

NetScaler Gateway implementation of OCSP

OCSP validation on a NetScaler Gateway appliance begins when NetScaler Gateway receives a client certificate during an SSL handshake. To validate the certificate, NetScaler Gateway creates an OCSP request and forwards it to the OCSP responder. To do so, NetScaler Gateway either extracts the URL for the OCSP responder from the client certificate or uses a locally configured URL. The transaction is in a suspended state until NetScaler Gateway evaluates the response from the server and determines whether to allow the transaction or to reject it. If the response from the server is delayed beyond the configured time and no other responders are configured, NetScaler Gateway allows the transaction or displays an error, depending on whether you set the OCSP check to optional or mandatory. NetScaler Gateway supports batching of OCSP requests and caching of OCSP responses to reduce the load on the OCSP responder and provide faster responses.

OCSP request batching

Each time NetScaler Gateway receives a client certificate, it sends a request to the OCSP responder. To help avoid overloading the OCSP responder, NetScaler Gateway can query the status of more than

one client certificate in the same request. For request batching to work efficiently, you need to define a time-out so that processing of a single certificate is not delayed while waiting to form a batch.

OCSP response caching

Caching of responses received from the OCSP responder enables faster responses to the user and reduces the load on the OCSP responder. Upon receiving the revocation status of a client certificate from the OCSP responder, NetScaler Gateway caches the response locally for a predefined length of time. When a client certificate is received during an SSL handshake, NetScaler Gateway first checks its local cache for an entry for this certificate. If an entry is found that is still valid (within the cache time-out limit), the entry is evaluated and the client certificate is accepted or rejected. If a certificate is not found, NetScaler Gateway sends a request to the OCSP responder and stores the response in its local cache for a configured length of time.

Configure OCSP certificate status

Configuring an Online Certificate Status Protocol (OCSP) involves adding an OCSP responder, binding the OCSP responder to a signed certificate from a Certificate Authority (CA), and binding the certificate and private key to a Secure Sockets Layer (SSL) virtual server. If you need to bind a different certificate and private key to an OCSP responder that you already configured, you need to first unbind the responder and then bind the responder to a different certificate.

To configure OCSP

1. On the Configuration tab, in the navigation pane, expand SSL and then click OCSP Responder.
2. In the details pane, click Add.
3. In Name, type a name for the profile.
4. In URL, type the web address of the OCSP responder.

   This field is mandatory. The Web address cannot exceed 32 characters.
5. To cache the OCSP responses, click Cache and in Time-out, type the number of minutes that NetScaler Gateway holds the response.
6. Under Request Batching, click Enable.
7. In Batching Delay, specify the time, in milliseconds, allowed for batching a group of OCSP requests.

   The values can be from 0 through 10000. The default is 1.

8. In Produced At Time Skew, type the amount of time NetScaler Gateway can use when the appliance must check or accept the response.
9. Under Response Verification, select Trust Responses if you want to disable signature checks by the OCSP responder.

   If you enable Trust Responses, skip Step 8 and Step 9.
10. In Certificate, select the certificate that is used to sign the OCSP responses.

    If a certificate is not selected, the CA that the OCSP responder is bound to is used to verify responses.
11. In Request Time-out, type the number of milliseconds to wait for an OCSP response.

    This time includes the Batching Delay time. The values can be from 0 through 120000. The default is 2000.
12. In Signing Certificate, select the certificate and private key used to sign OCSP requests. If you do not specify a certificate and private key, the requests are not signed.
13. To enable the number used once `(nonce)extension`, select Nonce.
14. To use a client certificate, click Client Certificate Insertion.
15. Click Create and then click Close.

Manage NetScaler Gateway configuration settings

January 8, 2024

When you make configuration changes to NetScaler Gateway, the changes are saved in log files. You can view several types of configuration settings:

- Saved configuration. You can view the settings you have saved on NetScaler Gateway.
- Running configuration. You can view active settings, such as a virtual server or authentication policy, that you have configured but have not saved as a saved configuration to NetScaler Gateway.
- Running versus saved configuration. You can compare side by side the running and saved configuration on NetScaler Gateway.

You can also clear configuration settings on NetScaler Gateway.

Important: If you choose to clear settings on NetScaler Gateway, certificates, virtual servers, and policies are removed. Citrix recommends that you do not clear the configuration.

Save the NetScaler Gateway Configuration

You can save your current configuration on NetScaler Gateway to a computer in your network, view the current running configuration, and compare the saved and running configurations.

To save the configuration on NetScaler Gateway

1. In the configuration utility, above the details pane, click the Save icon and then click Yes.

To view and save the configuration file on NetScaler Gateway

The saved configuration are the settings that are saved in a log file on NetScaler Gateway, such as settings for virtual servers, policies, IP addresses, users, groups, and certificates.

When you configure settings on NetScaler Gateway, you can save the settings to a file on your computer. If you need to reinstall the NetScaler Gateway software or you accidentally remove some settings, you can use this file to restore your configuration. If you need to restore the settings, you can copy the file to NetScaler Gateway and restart the appliance by using the command-line interface or a program, such as WinSCP, to copy the file to NetScaler Gateway.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand System and then click Diagnostics.
2. In the details pane, under View Configuration, click Saved configuration.
3. In the Saved Configuration dialog box, click Save output text to a file, name the file, and then click Save.
   Note: Citrix recommends saving the file using the file name ns.conf.

To view the current running configuration

Any changes to NetScaler Gateway that occur without an effort to save them is called the running configuration. These settings are active on NetScaler Gateway, but are not saved on the appliance. If you configured additional settings, such as a policy, virtual server, users, or groups, you can view these settings in the running configuration.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand System and then click Diagnostics.
2. In the details pane, under View Configuration, click Running configuration.

To compare the saved and running configuration

You can see which settings are saved on the appliance and compare those settings against the running configuration. You can choose to save the running configuration or make changes to the configuration.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand System and then click Diagnostics.
2. In the details pane, under View Configuration, click Saved v/s running.

Clear the NetScaler Gateway configuration

You can clear the configuration settings on NetScaler Gateway. You can choose from among the following three levels of settings to clear:

Important: Citrix recommends saving your configuration before you clear the NetScaler Gateway configuration settings.

- Basic. Clears all settings on the appliance except for the system IP address, default gateway, mapped IP addresses, subnet IP addresses, DNS settings, network settings, high availability settings, administrative password, and feature and mode settings.
- Extended. Clears all settings except for the system IP address, mapped IP addresses, subnet IP addresses, DNS settings, and high availability definitions.
- Full. Restores the configuration to the original factory settings, excluding the system IP (NSIP) address and default route, which are required to maintain network connectivity to the appliance.

When you clear all or part of the configuration, the feature settings are set to the factory default settings.

When you clear the configuration, files that are stored on NetScaler Gateway, such as certificates and licenses, are not removed. The file ns.conf is not altered. If you want to save the configuration before clearing the configuration, save the configuration to your computer first. If you save the configuration, you can restore the ns.conf file on NetScaler Gateway. After you restore the file to the appliance and restart NetScaler Gateway, any configuration settings in ns.conf are restored.

Modifications to configuration files, such as rc.conf, are not reverted.

If you have a high availability pair, both NetScaler Gateway appliances are modified identically. For example, if you clear the basic configuration on one appliance, the changes are propagated to the second appliance.

To clear NetScaler Gateway configuration settings

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand System and then click Diagnostics.
2. In the details pane, under Maintenance, click Clear configuration.
3. In Configuration Level, select the level you want to clear and then click Run.

Certificates management on NetScaler Gateway

January 8, 2024

On NetScaler Gateway, you use certificates to create secure connections and to authenticate users.

To establish a secure connection, a server certificate is required at one end of the connection. A root certificate of the Certificate Authority (CA) that issued the server certificate is required at the other end of the connection.

- Server certificate. A server certificate certifies the identity of the server. NetScaler Gateway requires this type of digital certificate.
- Root certificate. A root certificate identifies the CA that signed the server certificate. The root certificate belongs to the Certificate Authority. A user device requires this type of digital certificate to verify the server certificate.

When establishing a secure connection with a web browser on the user device, the server sends its certificate to the device.

When the user device receives a server certificate, the web browser, such as Internet Explorer checks to see which CA issued the certificate and if the CA is trusted by the user device. If the CA is not trusted, or if it is a test certificate, the web browser prompts the user to accept or decline the certificate (effectively accepting or declining the ability to access the site).

NetScaler Gateway supports the following three types of certificates:

- A test certificate that is bound to a virtual server and can also be used for connections to a server farm. NetScaler Gateway comes with a pre-installed test certificate.
- A certificate in PEM or DER format that is signed by a CA and is paired with a private key.
- A certificate in PKCS#12 format that is used for storing or transporting the certificate and private key. The PKCS#12 certificate is typically exported from an existing Windows certificate as a PFX file and then installed on NetScaler Gateway.

Citrix recommends using a certificate signed by a trusted CA, such as Thawte or Verisign.

Create a certificate signing request

January 8, 2024

To provide secure communications using SSL or TLS, a server certificate is required on NetScaler Gateway. Before you can upload a certificate to NetScaler Gateway, you need to generate a Certificate Signing Request (CSR) and private key. You use the Create Certificate Request included in the NetScaler Gateway wizard or the configuration utility to create the CSR. The Create Certificate Request creates a .csr file that is emailed to the Certificate Authority (CA) for signing and a private key that remains on the appliance. The CA signs the certificate and returns it to you at the email address you provided. When you receive the signed certificate, you can install it on NetScaler Gateway. When you receive the certificate back from the CA, you pair the certificate with the private key.

Important: When you use the NetScaler Gateway wizard to create the CSR, you must exit the wizard and wait for the CA to send you the signed certificate. When you receive the certificate, you can run the NetScaler Gateway wizard again to create the settings and install the certificate. For more information about the NetScaler Gateway wizard, see
Configuring Settings by Using the NetScaler Gateway Wizard.

Create a CSR by using the NetScaler Gateway wizard

1. In the configuration utility, click the Configuration tab and then in the navigation pane, click **NetScaler Gateway**.
2. In the details pane, under Getting Started, click **NetScaler Gateway** wizard.
3. Follow the directions in the wizard until you come to the Specify a server certificate page.
4. Click **Create a Certificate Signing Request** and complete the fields.
   Note: The fully qualified domain name (FQDN) does not need to be the same as the NetScaler Gateway host name. The FQDN is used for user logon.
5. Click **Create** to save the certificate on your computer, and then click **Close**.
6. Exit the NetScaler Gateway wizard without saving your settings.

Create a CSR by using the NetScaler GUI

You can also use the NetScaler GUI to create a CSR, without running the NetScaler Gateway wizard.

1. Navigate to **Traffic Management** > **SSL > SSL Files** and select **Create Certificate Signing Request (CSR)**.
2. Complete the settings for the certificate and then click **Create**.

After you create the certificate and private key, email the certificate to the CA, such as Thawte or Verisign.

For detailed procedure, see Create a certificate signing request.

Install the signed certificate on NetScaler Gateway

When you receive the signed certificate from the Certificate Authority (CA), pair it with the private key on the appliance and then install the certificate on NetScaler Gateway.

Pair the signed certificate with a private key by using the GUI

1. Copy the certificate to NetScaler Gateway to the folder nsconfig/ssl by using a Secure Shell (SSH) program such as WinSCP.
2. In the configuration utility, on the Configuration tab, in the navigation pane, expand **SSL > Certificates**.
3. In the **SSL Certificate** page, click **Get Started**.
4. In the details pane, click **Install**.
5. In **Certificate-Key Pair Name**, type the name of the certificate.
6. In **Certificate File Name**, click **Appliance**.
7. Navigate to the certificate, click **Select**, and then click **Open**.
8. In **Key File Name**, click **Appliance**. The name of the private key is the same name as the Certificate Signing Request (CSR). The private key is located on NetScaler Gateway in the directory \nsconfig\ssl.
9. Choose the private key, and then click **Open**.
10. If the certificate is PEM-format, in **Password**, type the password for the private key.
11. If you want to configure notification for when the certificate expires, select **Notify When Expires**.
12. In **Notification Period**, type the number of days, click **Create**, and then click **Close**.

Bind the certificate and private key to a virtual server by using the GUI

After you create and link a certificate and private key pair, bind it to a virtual server.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway > Virtual Servers**.
2. In the details pane, click a virtual server, and then click **Open**.
3. On the Certificates tab, under **Available**, select a certificate, click **Add**, and then click **OK**.

Bind the certificate and private key to a virtual server by using the CLI

At the command prompt, type;

```
bind ssl vserver <vServerName> -certkeyName <string> -ocspCheck (
    Mandatory | Optional )
```

Example:

```
bind ssl vserver TestClient -CertkeyName ag51.xm.nsi.test.com -CA -
    ocspCheck Mandatory
```

Note: oscpCheck is optional if OCSP check is not required for device certificate.

Unbind test certificates from the virtual server by using the GUI

After you install the signed certificate, unbind any test certificates that are bound to the virtual server. You can unbind test certificates using the configuration utility.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway > Virtual Servers**.
2. In the details pane, click a virtual server, and then click **Open**.
3. On the Certificates tab, under **Configured**, select the test certificate, and then click **Remove**.

Configure intermediate certificates

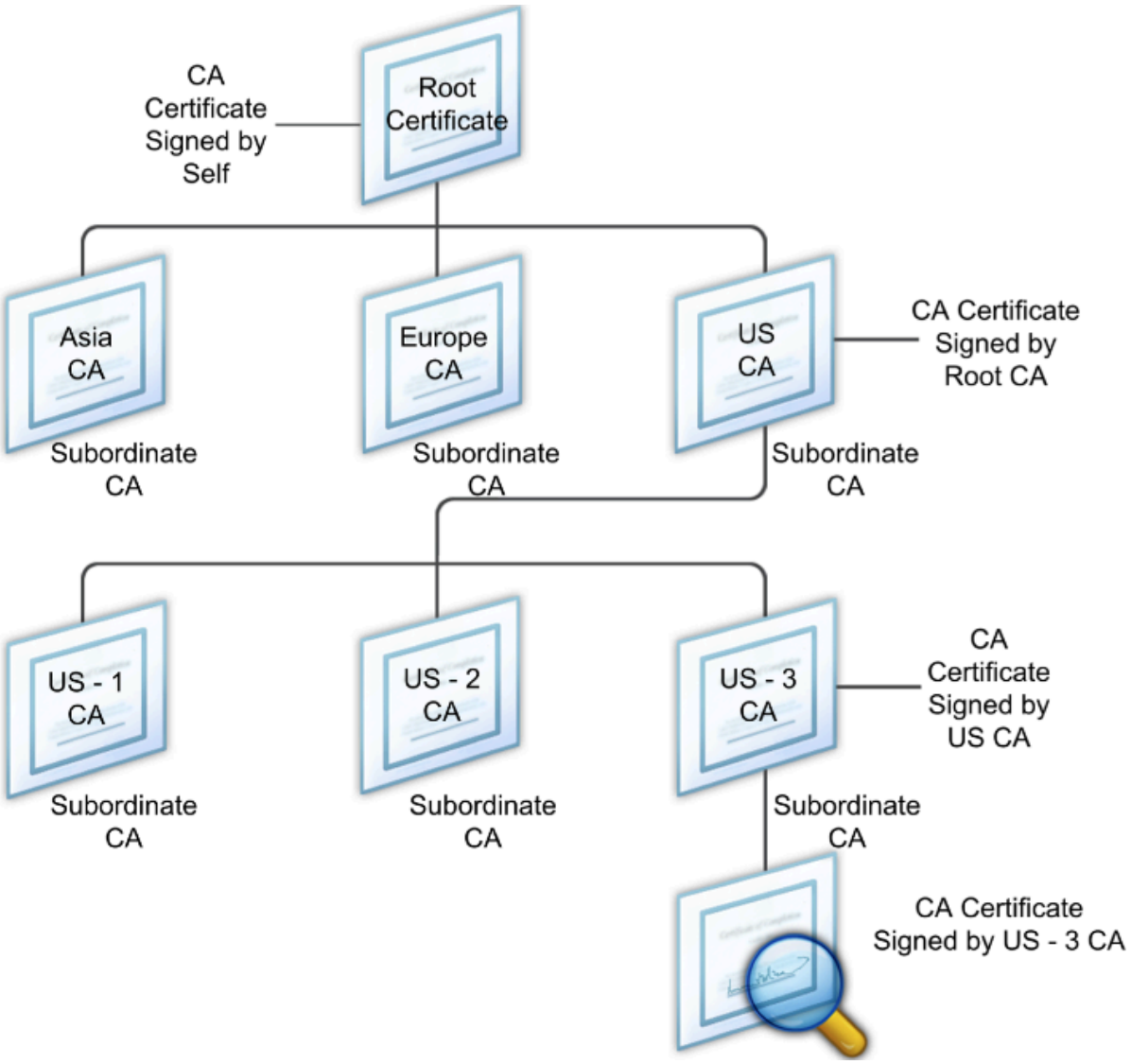
January 8, 2024

An intermediate certificate is a certificate that goes between NetScaler Gateway (the server certificate) and a root certificate (installed on the user device). An intermediate certificate is part of a chain.

Some organizations delegate the responsibility for issuing certificates to resolve the issue of geographical separation between organization units, or to apply different issuing policies to different sections of the organization.

Responsibility for issuing certificates can be delegated by setting up subordinate Certificate Authorities (CAs). CAs can sign their own certificates (that is, they are self-signed) or they can be signed by another certificate authority. The X.509 standard includes a model for setting up a hierarchy of CAs. In this model, as shown in the following figure, the root CA is at the top of the hierarchy and is a self-signed certificate by the certificate authority. The CAs that are directly subordinate to the root CA have CA certificates signed by the root certificate authority. CAs under the subordinate CAs in the hierarchy have their CA certificates signed by the subordinate CAs.

Figure 1. The X.509 model showing the hierarchical structure of a typical digital certificate chain



If a server certificate is signed by a CA with a self-signed certificate, the certificate chain is composed of exactly two certificates: the end entity certificate and the root certificate authority. If a user or server certificate is signed by an intermediate certificate authority, the certificate chain is longer.

The following figure shows that the first two elements are the end entity certificate (in this case, gwy01.company.com) and the certificate of the intermediate certificate authority, in that order. The intermediate certificate authority's certificate is followed by the certificate of its certificate authority. This listing continues until the last certificate in the list is for a root certificate authority. Each certificate in the chain attests to the identity of the previous certificate.

Figure 2. A typical digital certificate chain

Install an intermediate certificate

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand SSL and then click Certificates.
2. In the details pane, click Install.
3. In Certificate-Key Pair Name, type the name of the certificate.
4. Under Details, in Certificate File Name, click Browse (Appliance) and in the list, select Local or Appliance.
5. Navigate to the certificate on your computer (Local) or on NetScaler Gateway (Appliance).
6. In Certificate Format, select PEM.
7. Click Install and then click Close.

When you install an intermediate certificate on NetScaler Gateway, you do not need to specify the private key or a password.

After the certificate is installed on the appliance, the certificate needs to be linked to the server certificate.

Link an intermediate certificate to a server certificate

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand SSL and then click Certificates.
2. In the details pane, select the server certificate and then in Action, click Link.
3. Next to CA Certificate Name, select the intermediate certificate from the list and then click OK.

Use device certificates for authentication

January 8, 2024

NetScaler Gateway supports the device certificate check that enables you to bind the device identity to a certificate's private key. The device certificate check can be configured as part of classic or advanced

Endpoint Analysis (EPA) policies. In classic EPA policies, the device certificate can be configured only for preauthentication EPA.

NetScaler Gateway verifies the device certificate before the endpoint analysis scan runs or before the logon page appears. If you configure endpoint analysis, the endpoint scan runs to verify the user device. When the device passes the scan and after NetScaler Gateway verifies the device certificate, users can then log on to the NetScaler Gateway.

> **Important:**
>
> - By default, Windows mandates admin privileges for accessing device certificates.
> - To add a device certificate check for non-admin users, you must install the VPN plug-in. The VPN plug-in version must be the same version as the EPA plug-in on the device.
> - You can add multiple CA certificates to the gateway and validate the device certificate.
> - If you install two or more device certificates on NetScaler Gateway, users must select the correct certificate when they start to log on to NetScaler Gateway or before the endpoint analysis scan runs.
> - When you create the device certificate, it must be an X.509 certificate.
> - If you have a device certificate issued by an intermediate CA, then both intermediate and root CA certificates must be bound.
> - The EPA client needs the user to have local administrator rights to be able to access the machine certificate store. This is rarely the case, so a workaround is to install the full NetScaler Gateway plug-in which can access the local store.

For more information about creating device certificates, see the following:

- Network Device Enrollment Service (NDES) in Active Directory Certificate Services (AD CS) on the Microsoft website.
- How to request a certificate from a Microsoft Certificate Authority using DCE/RPC and the Active Directory Certificate profile payload on the Apple support website.
- iPad / iPhone Certificate Issuance on the Ask the Directory Services Team Microsoft support blog.
- Setting Up Network Device Enrollment Service on the Windows IT Pro website.
- Step-by-Step Example Deployment of the PKI Certificates for Configuration Manager: Windows Server 2008 Certification Authority on the Microsoft System Center website.

Steps to configure device certificates

To configure a device certificate, you must complete the following steps:

- Install the device certificate issuer's certificate authority certificate on NetScaler Gateway. For details, see Installing the Signed Certificate on NetScaler Gateway.

- Bind the device certificate issuer's certificate authority certificate to the NetScaler Gateway virtual server and enable OCSP check. For details, see Installing the Signed Certificate on NetScaler Gateway.
- Create and bind OCSP (responder) on device certificate issuer's certificate authority certificate. For details, see Monitor certificate status with OCSP.

Enable device certificate check on the virtual server and add device certificate issuer's certificate authority certificate to the device certificate checklist. For details, see Enable device certificate check on a virtual server for classic EPA policy.

Complete the client-side configuration and verification of device certificate on the Windows machine. For details, see Verification of device certificate on a Windows machine.

> **Note:**
>
> All the clients intended to avail the device certificate EPA check must have the device certificate installed in the system certificate store of the machine.

Enable device certificate check on a virtual server for classic EPA policy

After you create the device certificate, you install the certificate on NetScaler Gateway by using the procedure for Importing and Installing an Existing Certificate to NetScaler Gateway.

1. On the Configuration tab, navigate to **NetScaler Gateway > Virtual Servers**.
2. On the **NetScaler Gateway Virtual Servers** page, select an existing virtual server and click **Edit**.
3. On the **VPN Virtual Servers** page, under **Basic Settings** section, click **Edit**.
4. Clear the **Enable Authentication** box to disable authentication.
5. Select the **Enable Device Certificate** box to enable device certificate
6. Click **Add** to add an available device certificate issuer's CA certificate name to the list.
7. For binding a CA certificate to the virtual server, click **CA certificate** under the **CA for Device Certificate** section, click **Add**, select the certificate, and then click **+**.

> **Note:**
>
> For information on enabling and binding device certificates on a virtual server for advanced EPA policy, see Device Certificate in nFactor as an EPA component.

Verification of device certificate on a Windows machine

1. Open a browser and access the NetScaler Gateway FQDN.
2. Allow the Citrix End Point Analysis (EPA) client to run. If not already installed then install EPA.

Citrix EPA runs and validates the Device Certificate and redirects to the authentication page if the Device Certificate EPA check passes, else it redirects you to the EPA error page. In case you have other EPA checks, then the EPA scan results depend on the configured EPA checks.

For further debugging on the client, examine the following EPA logs on the client:
C:\Users<User name>\AppData\Local\Citrix\AGEE\nsepa.txt

Note:

> Device certificate verification with CRL is not supported.

Import and install an existing certificate

January 8, 2024

You can import an existing certificate from a Windows-based computer running Internet Information Services (IIS) or from a computer running the Secure Gateway.

When you export the certificate, make sure you also export the private key. Sometimes, you cannot export the private key, which means you cannot install the certificate on NetScaler Gateway. If this occurs, use the Certificate Signing Request (CSR) to create a certificate. For details, see Creating a Certificate Signing Request.

When you export a certificate and private key from Windows, the computer creates a Personal Information Exchange (.pfx) file. This file is then installed on NetScaler Gateway as a PKCS#12 certificate.

If you are replacing the Secure Gateway with NetScaler Gateway, you can export the certificate and private key from the Secure Gateway. If you are doing an in-place migration from the Secure Gateway to NetScaler Gateway, the fully qualified domain name (FQDN) on the application and the appliance must be the same. When you export the certificate from the Secure Gateway, you immediately retire the Secure Gateway, install the certificate on NetScaler Gateway, and then test the configuration. The Secure Gateway and NetScaler Gateway cannot be running on your network at the same time if they have the same FQDN.

If you are using Windows Server 2003 or Windows Server 2008, you can use the Microsoft Management Console to export the certificate. For more information, see the Windows online Help.

Leave the default values for all the other options, define a password, and save the .pfx file to your computer. When the certificate is exported, you then install it on NetScaler Gateway.

To install the certificate and private key on NetScaler Gateway

1. In the configuration utility, click the Configuration tab and then in the navigation pane, click **NetScaler Gateway**.
2. In the details pane, under Getting Started, click **NetScaler Gateway wizard**.
3. Click **Next**, select an existing virtual server, and then click **Next**.
4. In **Certificate Options**, select **Install a PKCS#12 (.pfx) fil**e.
5. In **PKCS#12 File Name**, click **Browse**, navigate to the certificate, and then click **Select**.
6. In ((Password)), type the password for the private key.

   This is the password you used when converting the certificate to PEM format.
7. Click **Next** to finish the NetScaler Gateway wizard without changing any other settings.

When the certificate is installed on NetScaler Gateway, the certificate appears in the configuration utility in the **SSL \ > Certificates** node.

To create a private Key

1. In the configuration utility, on the Configuration tab, in the navigation pane, click **SSL**.
2. In the details pane, under **SSL Keys**, click **Create RSA Key**.
3. In **Key Filename**, type the name of the private key or click Browse to navigate to an existing file.
4. In **Key Size (Bits)**, type the size of the private key.
5. In **Public Exponent Value**, select F4 or 3.

   The public exponent value for the RSA key. This is part of the cipher algorithm and is required for creating the RSA key. The values are F4 (Hex: 0x10001) or 3 (Hex: 0x3). The default is F4.
6. In **Key Format**, select PEM or DER. Citrix recommends PEM format for the certificate.
7. In **PEM Encoding Algorithm**, select DES or DES3.
8. In **PEM Passphrase** and **Verify Passphrase**, type the password, click **Create**, and then click **Close**.

   Note: To assign a passphrase, the Key Format must be PEM and you must select the encoding algorithm.

To create a DSA private key in the configuration utility, click **Create DSA Key** and follow the steps performed for creating the RSA private key.

Certificate revocation lists

January 8, 2024

From time to time, Certificate Authorities (CAs) issue certificate revocation lists (CRLs). CRLs contain information about certificates that can no longer be trusted. For example, suppose Ann leaves XYZ Corporation. The company can place Ann's certificate on a CRL to prevent her from signing messages with that key.

Similarly, you can revoke a certificate if a private key is compromised or if that certificate expired and a new one is in use. Before you trust a public key, make sure that the certificate does not appear on a CRL.

NetScaler Gateway supports the following two CRL types:

- CRLs that list the certificates that are revoked or are no longer valid
- Online Certificate Status Protocol (OSCP), an Internet protocol used for obtaining the revocation status of X.509 certificates

To add a CRL:

Before you configure the CRL on the NetScaler Gateway appliance, make sure that the CRL file is stored locally on the appliance. In the case of a high availability setup, the CRL file must be present on both NetScaler Gateway appliances, and the directory path to the file must be the same on both appliances.

If you need to refresh the CRL, you can use the following parameters:

- CRL Name: The name of the CRL being added on the NetScaler. Maximum 31 characters.
- CRL File: The name of the CRL file being added on the NetScaler. The NetScaler looks for the CRL file in the /var/netscaler/ssl directory by default. Maximum 63 characters.
- URL: Maximum 127 characters
- Base DN: Maximum 127 characters
- Bind DN: Maximum 127 characters
- Password: Maximum 31 characters
- Days: Maximum 31

1. In the configuration utility, on the Configuration tab, expand SSL and then click CRL.
2. In the details pane, click Add.
3. In the Add CRL dialog box, specify the values for the following:
    - CRL Name
    - CRL File
    - Format (optional)

- CA Certificate (optional)

4. Click **Create** and then click **Close**. In the CRL details pane, select the CRL that you configured and verify that the settings that appear at the bottom of the screen are correct.

To configure CRL autorefresh by using LDAP or HTTP in the GUI:

A CRL is generated and published by a CA periodically or, sometimes, immediately after a particular certificate is revoked. Citrix recommends that you update CRLs on the NetScaler Gateway appliance regularly for protection against clients trying to connect with certificates that are not valid.

The NetScaler Gateway appliance can refresh CRLs from a web location or an LDAP directory. When you specify refresh parameters and a web location or an LDAP server, the CRL does not have to be present on the local hard disk drive at the time you run the command. The first refresh stores a copy on the local hard disk drive, in the path specified by the CRL File parameter. The default path for storing the CRL is /var/netscaler/ssl.

CRL refresh parameters

- **CRL Name**

  The name of the CRL being refreshed on the NetScaler Gateway.

- **Enable CRL Auto Refresh**

  Enable or disable CRL auto refresh.

- **CA Certificate**

  The certificate of the CA that has issued the CRL. This CA certificate must be installed on the appliance. The NetScaler can update CRLs only from CAs whose certificates are installed on it.

- **Method**

  Protocol in which to obtain the CRL refresh from a web server (HTTP) or an LDAP server. Possible Values: HTTP, LDAP. Default: HTTP.

- **Scope**

  The extent of the search operation on the LDAP server. If the scope specified is Base, the search is at the same level as the base DN. If the scope specified is One, the search extends to one level below the base DN.

- **Server IP**

  The IP address of the LDAP server from which the CRL is retrieved. Select IPv6 to use an IPv6 IP address.

- **Port**

  The port number on which the LDAP or the HTTP server communicates.

- **URL**

  The URL for the web location from which the CRL is retrieved.

- **Base DN**

  The base DN used by the LDAP server to search for the CRL attribute.
  Note: Citrix recommends using the base DN attribute instead of the Issuer-Name from the CA certificate to search for the CRL in the LDAP server. The Issuer-Name field may not exactly match the LDAP directory structure's DN.

- **Bind DN**

  The bind DN attribute is used to access the CRL object in the LDAP repository. The bind DN attributes are the administrator credentials for the LDAP server. Configure this parameter to restrict unauthorized access to the LDAP servers.

- **Password**

  The administrator password used to access the CRL object in the LDAP repository. Password is required if the access to the LDAP repository is restricted, that is, anonymous access is not allowed.

- **Interval**

  The interval at which the CRL refresh must be carried out. For an instantaneous CRL refresh, specify the interval as NOW. Possible values: MONTHLY, DAILY, WEEKLY, NOW, NONE.

- **Days**

  The day on which the CRL refresh must be performed. The option is not available if the interval is set to DAILY.

- **Time**

  The exact time in 24-hour format when the CRL refresh must be performed.

- **Binary**

  Set the LDAP-based CRL retrieval mode to binary. Possible values: YES, NO. Default: NO.

1. In the navigation pane, expand SSL and then click CRL.
2. Select the configured CRL for which you want to update refresh parameters and then click Open.
3. Select the Enable CRL Auto Refresh option.
4. In the CRL Auto Refresh Parameters group, specify values for the following parameters:
   Note: An asterisk (*) indicates a required parameter.

   - Method
   - Binary
   - Scope

- Server IP
- Port*
- URL
- Base DN*
- Bind DN
- Password
- Interval
- Days
- Time

5. Click Create. In the CRL pane, select the CRL that you configured and verify that the settings that appear at the bottom of the screen are correct.

Monitor certificate status with OCSP

Online Certificate Status Protocol (OCSP) is an Internet protocol that is used to determine the status of a client SSL certificate. NetScaler Gateway supports OCSP as defined in RFC 2560. OCSP offers significant advantages over certificate revocation lists (CRLs) in terms of timely information. Up-to-date revocation status of a client certificate is especially useful in transactions involving large sums of money and high-value stock trades. It also uses fewer system and network resources. NetScaler Gateway implementation of OCSP includes request batching and response caching.

NetScaler Gateway implementation of OCSP

OCSP validation on a NetScaler Gateway appliance begins when NetScaler Gateway receives a client certificate during an SSL handshake. To validate the certificate, NetScaler Gateway creates an OCSP request and forwards it to the OCSP responder. To do so, NetScaler Gateway either extracts the URL for the OCSP responder from the client certificate or uses a locally configured URL. The transaction is in a suspended state until NetScaler Gateway evaluates the response from the server and determines whether to allow the transaction or to reject it. If the response from the server is delayed beyond the configured time and no other responders are configured, NetScaler Gateway allows the transaction or displays an error, depending on whether you set the OCSP check to optional or mandatory. NetScaler Gateway supports batching of OCSP requests and caching of OCSP responses to reduce the load on the OCSP responder and provide faster responses.

OCSP request batching

Each time NetScaler Gateway receives a client certificate, it sends a request to the OCSP responder. To help avoid overloading the OCSP responder, NetScaler Gateway can query the status of more than

one client certificate in the same request. For request batching to work efficiently, you need to define a time-out so that processing of a single certificate is not delayed while waiting to form a batch.

OCSP response caching

Caching of responses received from the OCSP responder enables faster responses to the user and reduces the load on the OCSP responder. Upon receiving the revocation status of a client certificate from the OCSP responder, NetScaler Gateway caches the response locally for a predefined length of time. When a client certificate is received during an SSL handshake, NetScaler Gateway first checks its local cache for an entry for this certificate. If an entry is found that is still valid (within the cache time-out limit), the entry is evaluated and the client certificate is accepted or rejected. If a certificate is not found, NetScaler Gateway sends a request to the OCSP responder and stores the response in its local cache for a configured length of time.

Configure OCSP certificate status

Configuring an Online Certificate Status Protocol (OCSP) involves adding an OCSP responder, binding the OCSP responder to a signed certificate from a Certificate Authority (CA), and binding the certificate and private key to a Secure Sockets Layer (SSL) virtual server. If you need to bind a different certificate and private key to an OCSP responder that you already configured, you need to first unbind the responder and then bind the responder to a different certificate.

To configure OCSP

1. On the Configuration tab, in the navigation pane, expand SSL and then click OCSP Responder.
2. In the details pane, click Add.
3. In Name, type a name for the profile.
4. In URL, type the web address of the OCSP responder.

   This field is mandatory. The Web address cannot exceed 32 characters.
5. To cache the OCSP responses, click Cache and in Time-out, type the number of minutes that NetScaler Gateway holds the response.
6. Under Request Batching, click Enable.
7. In Batching Delay, specify the time, in milliseconds, allowed for batching a group of OCSP requests.

   The values can be from 0 through 10000. The default is 1.

8. In Produced At Time Skew, type the amount of time NetScaler Gateway can use when the appliance must check or accept the response.
9. Under Response Verification, select Trust Responses if you want to disable signature checks by the OCSP responder.

   If you enable Trust Responses, skip Step 8 and Step 9.
10. In Certificate, select the certificate that is used to sign the OCSP responses.

    If a certificate is not selected, the CA that the OCSP responder is bound to is used to verify responses.
11. In Request Time-out, type the number of milliseconds to wait for an OCSP response.

    This time includes the Batching Delay time. The values can be from 0 through 120000. The default is 2000.
12. In Signing Certificate, select the certificate and private key used to sign OCSP requests. If you do not specify a certificate and private key, the requests are not signed.
13. To enable the number used once (`nonce`)`extension`, select Nonce.
14. To use a client certificate, click Client Certificate Insertion.
15. Click Create and then click Close.

Test your NetScaler Gateway configuration

January 8, 2024

After you configure the initial settings on NetScaler Gateway, you can test your settings by connecting to the appliance.

To test the NetScaler Gateway settings, create a local user account. Then, using either the virtual server IP address or the fully qualified domain name (FQDN) of the appliance, open a web browser and type the web address. For example, in the address bar, type `https://my.company.com` or `https://192.168.96.183`.

At the logon screen, enter the user name and password of the user account you created earlier. After you log on, you are prompted to download and install the Citrix Secure Access client.

After you install and then successfully connect with the Citrix Secure Access client, the Access Interface appears. The Access Interface is the default home page for NetScaler Gateway.

Create a user account by using the GUI

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway \ > User Administration**, and then click **AAA Users**.
2. In the details pane, click Add.
3. In User Name, type the user name.
4. If using local authentication, clear the External Authentication check box. Authenticating users with external authentication types, such as LDAP or RADIUS, is the default. If you clear this check box, NetScaler Gateway authenticates users.
5. In Password and Confirm Password, type the password for the user, click Create, and then click Close.

When you add users by using the configuration utility, you can bind the following policies to the user:

- Authorization
- Traffic, session, and auditing
- Bookmarks
- Intranet applications
- Intranet IP addresses

If you have problems logging on with the test user account, check the following:

- If you receive a certificate warning, either a test certificate or an invalid certificate is installed on NetScaler Gateway. If a certificate signed by a Certificate Authority (CA) is installed on the appliance, make sure that there is a corresponding root certificate on the user device.
- If you used a CA-signed certificate, verify that you generated the site certificate correctly by using the signed Certificate Signing Request (CSR), and that the Distinguished Name (DN) data entered in the CSR is accurate. The problem might also be that the host name does not match the IP address that is on the signed certificate. Check that the configured certificate's common name corresponds to the configured virtual server IP address information.
- If the logon screen does not appear or if any other error message appears, review the setup process and confirm that you performed all steps correctly and entered all parameters accurately.

Upgrade the NetScaler Gateway software

January 8, 2024

You can upgrade the software that resides on NetScaler Gateway when new releases are made available. You can check for updates on the Citrix website. You can upgrade to a new release only if your

NetScaler Gateway licenses are under the Subscription Advantage program when the update is released. You can renew Subscription Advantage at any time. For more information, see the NetScaler support website.

The upgrade path and compatible products information are also available in the Citrix Upgrade Guide.

For information about the latest NetScaler Gateway maintenance release, see the Citrix Knowledge Center.

Check for software updates

1. Go to the Citrix website.
2. Click **My Account** and log on.
3. Click **Downloads**.
4. Under Find Downloads, select **NetScaler Gateway**.
5. In **Select Download Type**, select **Product Software** and then click **Find**.
   You can also select **Virtual Appliances** to download NetScaler VPX. When you select this option, you receive a list of software for the virtual machine for each hypervisor.
6. On the NetScaler Gateway page, expand **NetScaler Gateway or Access Gateway**.
7. Click the appliance software version you want to download.
8. On the appliance software page for the version you want to download, select the virtual appliance, and then click **Download**.
9. Follow the instructions on your screen to download the software.

When the software is downloaded to your computer, you can use the Upgrade Wizard or the command prompt to install the software.

Upgrade the NetScaler Gateway by using the Upgrade Wizard

1. In the configuration utility, on the **Configuration tab**, in the navigation pane, click System.
2. In the details pane, click **Upgrade Wizard**.
3. Click **Next** and then follow the directions in the wizard.

Upgrade the NetScaler Gateway by using a command prompt

1. To upload the software to NetScaler Gateway, use a secure FTP client, such as WinSCP, to connect to the appliance.
2. Copy the software from your computer to the /var/`nsinstall` directory on the appliance.
3. Use a Secure Shell (SSH) client, such as PuTTY, to open an SSH connection to the appliance.

4. Log on to NetScaler Gateway.
5. At a command prompt, type: `shell`
6. To change to the `nsinstall` directory, at a command prompt, type: `cd /var/nsinstall`
7. To view the contents of the directory, type: `ls`
8. To unpack the software, type: tar –xvzf build_X_XX.tgz, where build_X_XX.tgz is the name of the build to which you want to upgrade.
9. To start the installation, at a command prompt, type: `./installns`
10. When the installation is complete, restart NetScaler Gateway.

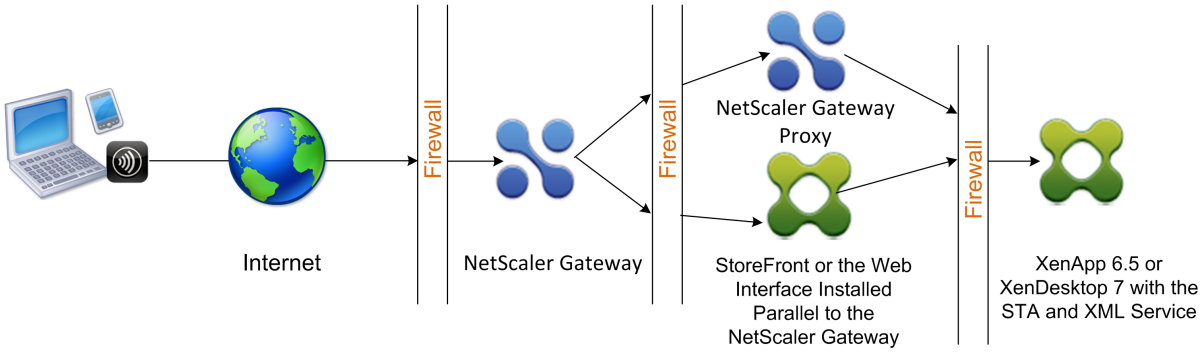
After NetScaler Gateway restarts, to verify successful installation, start the configuration utility. The NetScaler Gateway version that is on the appliance appears in the upper-right corner.

Deploy NetScaler Gateway in a double-hop DMZ

January 8, 2024

Some organizations use three firewalls to protect their internal networks. The three firewalls divide the DMZ into two stages to provide an extra layer of security for the internal network. This network configuration is called a double-hop DMZ.

Figure 1. NetScaler Gateway appliances deployed in a double-hop DMZ



> **Note:**
>
> For illustration purposes, the preceding example describes a double-hop configuration using three firewalls with StoreFront, the Web Interface, and Citrix Virtual Apps. However, you can also have a double-hop DMZ with one appliance in the DMZ and one appliance in the secure network. If you configure a double-hop configuration with one appliance in the DMZ and one in the secure network, you can ignore the instructions for opening ports on the third firewall.

You can configure a double-hop DMZ to support Citrix StoreFront or the Web Interface installed parallel to the NetScaler Gateway proxy. Users connect by using Citrix Workspace app.

> **Note:**
>
> If you deploy NetScaler Gateway in a double-hop DMZ with StoreFront, email-based AutoDiscovery for Citrix Workspace app does not work.

How a double-Hop deployment works

You can deploy NetScaler Gateway appliances in a double-hop DMZ to control access to servers running Citrix Virtual Apps. The connections in a double-hop deployment occur as follows:

- Users connect to NetScaler Gateway in the first DMZ by using a web browser and by using the Citrix Workspace app to select a published application.
- Citrix Workspace app starts on the user device. The user connects to NetScaler Gateway to access the published application running in the server farm in the secure network.

  Note: Secure Hub and the Citrix Secure Access client for Windows are not supported in a double-hop DMZ deployment. Only the Citrix Workspace app is used for user connections.
- 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.
- 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. Communications between NetScaler Gateway in the first DMZ and the Secure Ticket Authority (STA) in the internal network are also proxied through NetScaler Gateway in the second DMZ.

NetScaler Gateway supports IPv4 and IPv6 connections. You can use the configuration utility to configure the IPv6 address.

The following table suggests the double-hop deployment support for the various ICA features:

ICA feature	Double-hop support
SmartAccess	Yes
SmartControl	Yes
Enlightened Data Transport (EDT)	Yes
HDX Insight	Yes
ICA Session Reliability (Port 2598)	Yes
ICA Session Migration	Yes

ICA feature	Double-hop support
ICA Session Timeout	Yes
Multi-Stream ICA	Yes (TCP only)
Framehawk	No
UDP audio	No

Prepare for a double-hop DMZ deployment

When configuring a double-hop DMZ deployment, you must answer the following questions:

- Do I want to support load balancing?
- What ports do I open on the firewalls?
- How many SSL certificates do I need?
- What components do I need before I begin the deployment?

The topics in this section contain information to help you answer these questions as appropriate for your environment.

Components required to begin the deployment

Before you begin a double-hop DMZ deployment, ensure that you have the following components:

- At minimum, two NetScaler Gateway appliances must be available (one for each DMZ).
- Servers running Citrix Virtual Apps must be installed and operational in the internal network.
- The Web Interface or StoreFront must be installed in the second DMZ and configured to operate with the server farm in the internal network.
- At minimum, one SSL server certificate must be installed on NetScaler Gateway in the first DMZ. This certificate ensures that the Web browser and user connections to NetScaler Gateway are encrypted.

  You need extra certificates if you want to encrypt connections that occur among the other components in a double-hop DMZ deployment.

Communication flow in a double-hop DMZ deployment

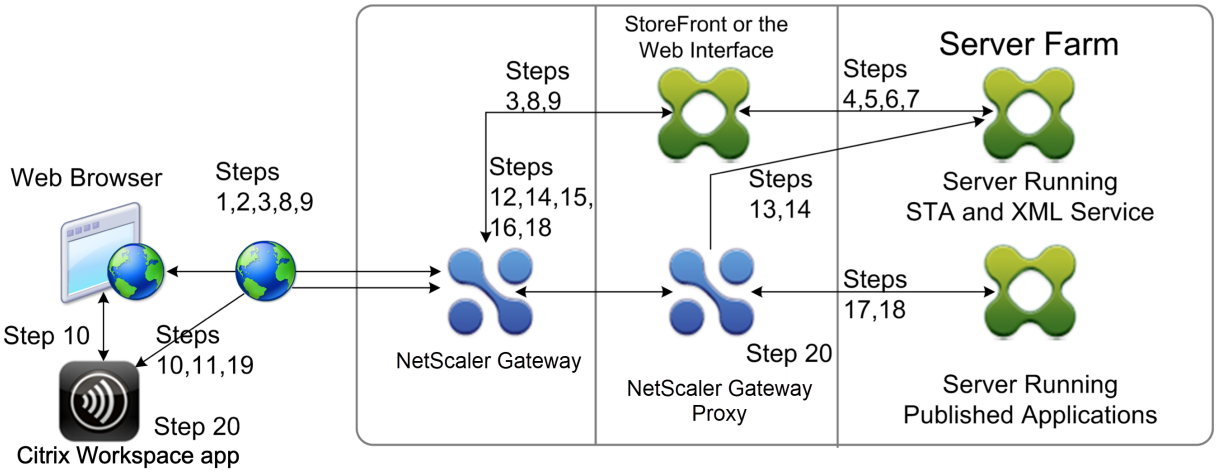
January 8, 2024

To understand the configuration issues involved in a double-hop DMZ deployment, you must have a basic understanding of how the various NetScaler Gateway and Citrix Virtual Apps components in a double-hop DMZ deployment communicate to support a user connection. The connection process for StoreFront and the Web Interface is the same.

Although the user connection process occurs in one continuous flow, the following high-level steps are involved in the process.

- Authenticate users
- Create a session ticket
- Start the Citrix Workspace app
- Complete the connection

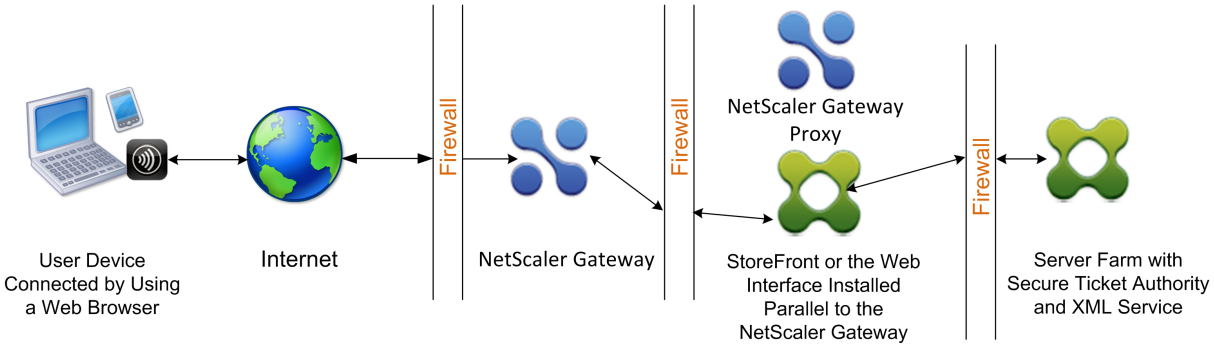
The following figure shows the steps that occur in the user connection process to either StoreFront or the Web Interface. In the secure network, computers running Citrix Virtual Apps are also running the Secure Ticket Authority (STA), XML Service, and published applications.



Connection process

Authenticating users is the first step of the user connection process in a double-hop DMZ deployment.

The following figure shows the user connection process in this deployment.



During the user authentication stage, the following basic process occurs:

1. A user types the address of NetScaler Gateway, such as https://www.ng.wxyco.com in a web browser to connect to NetScaler Gateway in the first DMZ. If you enabled logon page authentication on NetScaler Gateway, NetScaler Gateway authenticates the user.
2. NetScaler Gateway in the first DMZ receives the request.
3. NetScaler Gateway redirects the web browser connection to the Web Interface.
4. The Web Interface sends the user credentials to the Citrix XML service running in the server farm in the internal network.
5. The Citrix XML Service authenticates the user.
6. The XML Service creates a list of the published applications that the user is authorized to access and sends this list to the Web Interface.

   Note:

   - If you enable authentication on NetScaler Gateway, the appliance sends the NetScaler Gateway logon page to the user. The user enters authentication credentials on the logon page and the appliance authenticates the user. NetScaler Gateway then returns the user credentials to the Web Interface.
   - If you do not enable authentication, NetScaler Gateway does not perform authentication. The appliance connects to the Web Interface, retrieves the Web Interface logon page, and sends the Web Interface logon page to the user. The user enters authentication credentials on the Web Interface logon page and NetScaler Gateway passes the user credentials back to the Web Interface.

   Creating the session ticket is the second stage of the user connection process in a double-hop DMZ deployment.

   During the session ticket creation stage, the following basic process occurs:

7. The Web Interface communicates with both the XML Service and the Secure Ticket Authority (STA) in the internal network to produce session tickets for each of the published applications

the user is authorized to access. The session ticket contains an alias address for the computer running Citrix Virtual Apps that hosts a published application.

8. The STA saves the IP addresses of the servers that host the published applications. The STA then sends the requested session tickets to the Web Interface. Each session ticket includes an alias that represents the IP address of the server that hosts the published application, but not the actual IP address.

9. The Web Interface generates an ICA file for each of the published applications. The ICA file contains the ticket issued by the STA. The Web Interface then creates and populates a webpage with a list of links to the published applications and sends this webpage to the web browser on the user device.

   Starting Citrix Workspace app is the third stage of the user connection process in a double-hop DMZ deployment. The basic process is as follows:

10. The user clicks a link to a published application in the Web Interface. The Web Interface sends the ICA file for that published application to the browser for the user device.

    The ICA file contains data instructing the web browser to start Receiver.

    The ICA file also contains the fully qualified domain name (FQDN) or the Domain Name System (DNS) name of the NetScaler Gateway in the first DMZ.

11. The web browser starts Receiver and the user connects to NetScaler Gateway in the first DMZ by using the NetScaler Gateway name in the ICA file. Initial SSL/TLS handshaking occurs to establish the identity of the server running NetScaler Gateway.

    Completing the connection is the fourth and last stage of the user connection process in a double-hop DMZ deployment.

    During the connection completion stage, the following basic process occurs:

    - The user clicks a link to a published application in the Web Interface.
    - The web browser receives the ICA file generated by the Web Interface and starts Citrix Workspace app.
      Note: The ICA file contains code that instructs the web browser to start Citrix Workspace app.
    - Citrix Workspace app initiates an ICA connection to NetScaler Gateway in the first DMZ.
    - NetScaler Gateway in the first DMZ communicates with the Secure Ticket Authority (STA) in the internal network to resolve the alias address in the session ticket to the real IP address of a computer running Citrix Virtual Apps or StoreFront. This communication is proxied through the second DMZ by the NetScaler Gateway proxy.
    - NetScaler Gateway in the first DMZ completes the ICA connection to Citrix Workspace app.
    - Citrix Workspace app can now communicate through both NetScaler Gateway appliances to the computer running Citrix Virtual Apps on the internal network.

The detailed steps for completing the user connection process are as follows:

12. Citrix Workspace app sends the STA ticket for the published application to NetScaler Gateway in the first DMZ.
13. NetScaler Gateway in the first DMZ contacts the STA in the internal network for ticket validation. To contact the STA, NetScaler Gateway establishes a SOCKS or SOCKS with SSL connection to the NetScaler Gateway proxy in the second DMZ.
14. The NetScaler Gateway proxy in the second DMZ passes the ticket validation request to the STA in the internal network. The STA validates the ticket and maps it to the computer running Citrix Virtual Apps that hosts the published application.
15. The STA sends a response to the NetScaler Gateway proxy in the second DMZ, which is passed to NetScaler Gateway in the first DMZ. This response completes the ticket validation and includes the IP address of the computer that hosts the published application.
16. NetScaler Gateway in the first DMZ incorporates the address of the Citrix Virtual Apps server into the user connection packet and sends this packet to the NetScaler Gateway proxy in the second DMZ.
17. The NetScaler Gateway proxy in the second DMZ makes a connection request to the server specified in the connection packet.
18. The server responds to the NetScaler Gateway proxy in the second DMZ. The NetScaler Gateway proxy in the second DMZ passes this response to NetScaler Gateway in the first DMZ to complete the connection between the server and NetScaler Gateway in the first DMZ.
19. NetScaler Gateway in the first DMZ completes the SSL/TLS handshake with the user device by passing the final connection packet to the user device. The connection from the user device to the server is established.
20. The ICA traffic flows between the user device and the server through NetScaler Gateway in the first DMZ and the NetScaler Gateway proxy in the second DMZ.

Install and configuring NetScaler Gateway in a double-hop DMZ

January 8, 2024

You need to complete several steps to deploy NetScaler Gateway in a double-hop DMZ. The steps include installation of appliances in both DMZs and configuring the appliances for user device connections.

Install NetScaler Gateway in the first DMZ

To install NetScaler Gateway in the first DMZ, follow the instructions in Install the hardware.

If you are installing multiple NetScaler Gateway appliances in the first DMZ, you can deploy the appliances behind a load balancer.

Configure NetScaler Gateway in the first DMZ

In a double-hop DMZ deployment, it is mandatory that you configure each NetScaler Gateway in the first DMZ to redirect connections to either StoreFront or the Web Interface in the second DMZ.

Redirection to StoreFront or the Web Interface is performed at the NetScaler Gateway Global or virtual server level. To connect to the Web Interface through NetScaler Gateway, a user must be associated with a NetScaler Gateway user group for which redirection to the Web Interface is enabled.

Install NetScaler Gateway in the second DMZ

The NetScaler Gateway appliance in the second DMZ is called the NetScaler Gateway proxy because it proxies ICA and Secure Ticket Authority (STA) traffic across the second DMZ.
Install the hardware to install each NetScaler Gateway appliance in the second DMZ.

You can use this installation procedure to install other appliances in the second DMZ.

After you install NetScaler Gateway appliances in the second DMZ, you configure the following settings:

- Configure a virtual server on the NetScaler Gateway proxy.
- Configure NetScaler Gateway appliances in the first and second DMZ to communicate with each other.
- Bind the NetScaler Gateway in the second DMZ globally or to a virtual server.
- Configure the STA on the appliance in the first DMZ.
- Open ports in the firewalls separating the DMZ.
- Install certificates on the appliances.

Configure settings on the virtual servers on the NetScaler Gateway Proxy

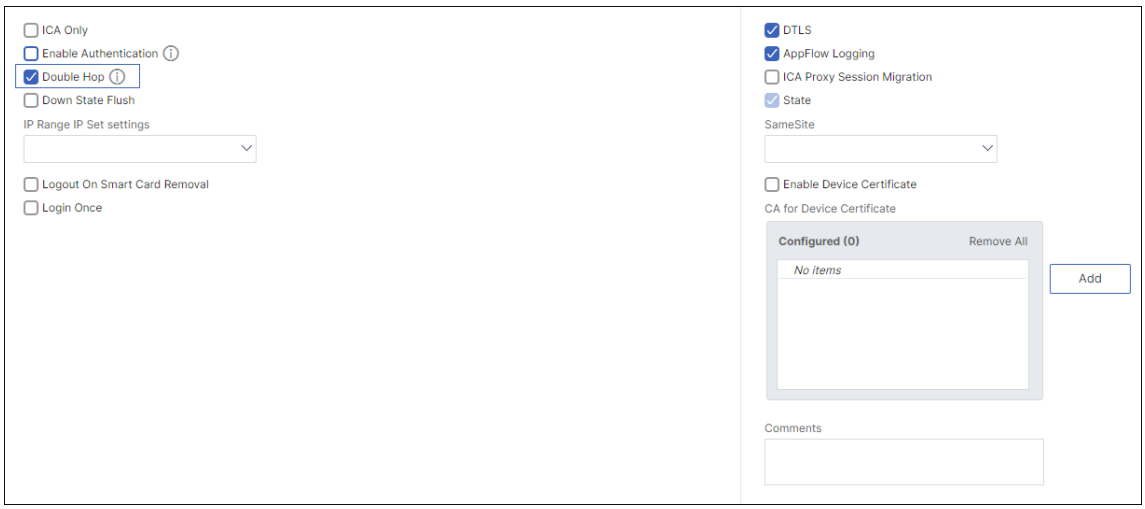
January 8, 2024

To allow connections to pass between the NetScaler Gateway appliances, you enable double-hop in the virtual server on the NetScaler Gateway proxy.

When users connect, the NetScaler Gateway appliance authenticates users and then proxies the connection to the proxy appliance. On the NetScaler Gateway in the first DMZ, configure the virtual server to communicate with NetScaler Gateway in the second DMZ. Do not configure authentication or policies on the NetScaler Gateway proxy. Citrix recommends disabling authentication on the virtual server.

To enable double hop on the virtual server on the NetScaler Gateway proxy by using the GUI

1. Navigate to **Configuration > NetScaler Gateway > Virtual Servers**.
2. Select a virtual server and click **Edit**.
3. In the **Basic Settings** section, click the edit icon and then click **More**.
4. Select **Double Hop**.

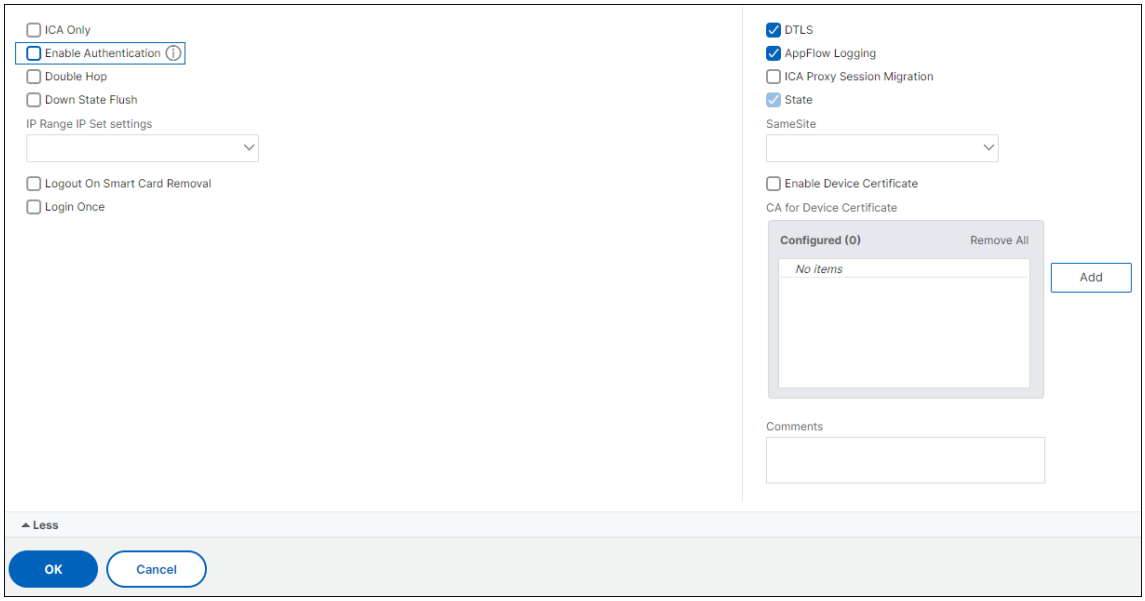


5. Click **OK**.

To disable authentication on the virtual server on the NetScaler Gateway proxy by using the GUI

1. Navigate to **Configuration > NetScaler Gateway > Virtual Servers**.
2. Select a virtual server and click **Edit**.
3. In the **Basic Settings** section, click the edit icon and then click **More**.

4. Clear the **Enable Authentication** check box.



5. Click **OK**.

Configure the appliance to communicate with the appliance proxy

January 8, 2024

When you deploy NetScaler Gateway in a double-hop DMZ, you must configure NetScaler Gateway in the first DMZ to communicate with the NetScaler Gateway proxy in the second DMZ.

If you deploy multiple appliances in the second DMZ, you configure each appliance in the first DMZ to communicate with every proxy appliance in the second DMZ.

Note: If you want to use IPv6, you configure the next hop server by using the configuration utility. To do so, expand

NetScaler Gateway > Resources and then click
Next Hop Servers. Follow the steps in the following procedure and then select the
IPv6 check box.

To configure NetScaler Gateway to communicate with the NetScaler Gateway Proxy

1. In the configuration utility, on the Configuration tab, expand NetScaler Gateway > Resources and then click Next Hop Servers.
2. In the details pane, click Add.
3. In Name, type a name for the first NetScaler Gateway.
4. In IP address, type the virtual server IP address of the NetScaler Gateway proxy in the second DMZ.
5. In Port, type the port number, click Create and then click Close. If you are using a secure port, such as 443, select Secure.

You must configure each NetScaler Gateway installed in the first DMZ to communicate with all NetScaler Gateway proxy appliances installed in the second DMZ.

After you configure the settings for the NetScaler Gateway proxy, bind the policy to Next Hop Servers in NetScaler Gateway Global or to a virtual server.

To bind the NetScaler Gateway next hop server globally

1. In the configuration utility, on the Configuration tab, expand NetScaler Gateway > Resources and then click Next Hop Servers.
2. In the details pane, select a next hop server and then in Action, select Global Bindings.
3. In the Configure Next Hop Server Global Binding dialog box, in Next Hop Server Name, select the proxy appliance and then click OK.

To bind the NetScaler Gateway next hop server to a virtual server

1. In the configuration utility, on the Configuration tab, expand NetScaler Gateway and then click Virtual Servers.
2. In the details pane, select a virtual server and then click Open.
3. On the Published Applications tab, under Next Hop Servers, click an item and then click OK.

You can also add a next hop server from the Published Applications tab.

Configure NetScaler Gateway to handle the STA and ICA traffic

January 8, 2024

When you deploy NetScaler Gateway in a double-hop DMZ, you must configure NetScaler Gateway in the first DMZ to handle communications with the Secure Ticket Authority (STA) and ICA traffic appropriately. The server running the STA can be bound either globally or to a virtual server.

After you configure the STA, you can bind the STA either globally or to a virtual server.

To configure and bind the STA globally:

1. In the GUI, on the Configuration tab, expand **NetScaler Gateway** and then click **Global Settings**.
2. In the details pane, under **Servers**, click **Bind/Unbind STA Servers to be used by the Secure Ticket Authority**.
3. In the **Bind/Unbind STA Servers** dialog box, click **Add**.
4. In the **Configure STA Server** dialog box, in **URL**, type the path to the server running the STA, such as http://mycompany.com or http://ipAddress and then click **Create**.

To configure and bind the STA to a virtual server:

1. In the GUI, on the Configuration tab, expand **NetScaler Gateway** and then click **Virtual Servers**.
2. In the details pane, select a virtual server and then click **Open**.
3. On the **Published Applications** tab, under **Secure Ticket Authority**, click **Add**.
4. In the **Configure STA Server** dialog box, in URL, type the path to the server running the STA, such as http://mycompany.com or http://ipAddress and then click **Create**.

Note:

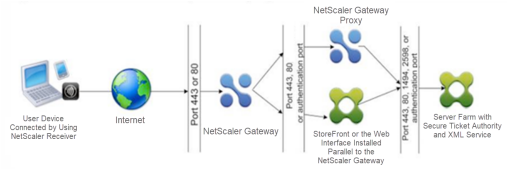
If the VPN virtual servers share the same next hop virtual server and STA servers, the connection is reset when the common STA server is unbound from a virtual server that shares the same next hop virtual server.

Open the appropriate ports on the firewalls

January 8, 2024

You must ensure that the appropriate ports are open on the firewalls to support the different connections that occur among the various components involved in a double-hop DMZ deployment. For more information about the connection process, see Communication Flow in a Double-Hop DMZ Deployment.

The following figure shows common ports that can be used in a double-hop DMZ deployment.



The following table shows the connections that occur through the first firewall and the ports that must be open to support the connections.

Connections through the first firewall	Ports used
The web browser from the Internet connects to NetScaler Gateway in the first DMZ. **Note:** NetScaler Gateway includes an option to redirect connections that are made on port 80 to a secure port. If you enable this option on NetScaler Gateway, you can open port 80 through the first firewall. When a user makes an unencrypted connection to NetScaler Gateway on port 80, NetScaler Gateway automatically redirects the connection to a secure port.	Open TCP port 443 through the first firewall.
Citrix Workspace app from the Internet connects to NetScaler Gateway in the first DMZ.	Open TCP port 443 through the first firewall.

The following table shows the connections that occur through the second firewall and the ports that must be open to support the connections.

Connections through the second firewall	Ports used
NetScaler Gateway in the first DMZ connects to the Web Interface in the second DMZ.	Open either TCP port 80 for an unsecure connection or TCP port 443 for a secure connection through the second firewall.
NetScaler Gateway in the first DMZ connects to NetScaler Gateway in the second DMZ.	Open TCP port 443 for a secure SOCKS connection through the second firewall.
If you enabled authentication on NetScaler Gateway in the first DMZ, this appliance might need to connect to an authentication server in the internal network.	Open the TCP port on which the authentication server listens for connections. Examples include port 1812 for RADIUS and port 389 for LDAP.

The following table shows the connections that occur through the third firewall and the ports that

must be open to support the connections.

Connections through the third firewall	Ports used
StoreFront or the Web Interface in the second DMZ connects to the XML Service hosted on a server in the internal network.	Open either port 80 for an unsecure connection or port 443 for a secure connection through the third firewall.
StoreFront or the Web Interface in the second DMZ connects to the Secure Ticket Authority (STA) hosted on a server in the internal network.	Open either port 80 for an unsecure connection or port 443 for a secure connection through the third firewall.
NetScaler Gateway in the second DMZ connects to the STA residing in the secure network.	Open either port 80 for an unsecure connection or port 443 for a secure connection through the third firewall.
NetScaler Gateway in the second DMZ makes an ICA connection to a published application or virtual desktop on a server in the internal network.	Open TCP port 1494 to support ICA connections through the third firewall. If you enabled session reliability on Citrix Virtual Apps, open TCP port 2598 instead of 1494.
If you enabled authentication on NetScaler Gateway in the first DMZ, this appliance might need to connect to an authentication server in the internal network.	Open the TCP port on which the authentication server listens for connections. Examples include port 1812 for RADIUS and port 389 for LDAP.

Maintaining and Monitoring the System

January 8, 2024

Once you complete the configuration of your NetScaler Gateway, you need to maintain and monitor the appliance. You can do so in the following ways:

- You can upgrade NetScaler Gateway to the latest version of the software. When you log on to the Citrix website, you can navigate to the NetScaler Gateway download site and the download the software. You can find the readme for maintenance builds in the Citrix Knowledge Center.
- You can assign NetScaler Gateway configuration and management tasks to different members of your group. With delegated administration, you can assign access levels to individuals which restrict them to performing specific tasks on NetScaler Gateway.
- You can save the NetScaler Gateway configuration either to the appliance or a file on your computer. You can compare the current running and saved configuration. You can also clear the configuration from NetScaler Gateway.

- You can view, refresh, and end user sessions within the NetScaler Gateway configuration utility.
- You can configure logging on NetScaler Gateway. The logs provide important information about the appliance and are useful in case you experience problems.

Configuring Delegated Administrators

January 8, 2024

NetScaler Gateway has a default administrator user name and password. The default user name and password is `nsroot`. When you run the Setup Wizard for the first time, you can change the administrator password.

You can create more administrator accounts and assign each account with different levels of access to NetScaler Gateway. These additional accounts are called delegated administrators. For example, you have one person assigned to monitor NetScaler Gateway connections and logs and another person responsible for configuring specific settings on NetScaler Gateway. The first administrator has read-only access and the second administrator has limited access to the appliance.

To configure a delegated administrator, you use command policies and system users and groups.

When you are configuring a delegated administrator, the configuration process is:

- Add a system user. A system user is an administrator with specified privileges. All administrators inherit the policies of the groups to which they belong.
- Add a system group. A system group contains systems users with specific privileges. Members of the system group inherit the policies of the group or groups to which they belong.
- Create a command policy. Command policies allow you to define what parts of the NetScaler Gateway configuration a user or group is allowed to access and modify. You can also regulate which commands, such as command groups, virtual servers, and other elements administrators and groups are permitted to configure.
- Bind the command policy to the user or group by setting the priority. When configuring delegated administration, assign priorities to the administrator or group so NetScaler Gateway can determine which policy takes precedence.

NetScaler Gateway has a default deny system command policy. Command policies cannot be bound globally. Bind the policies directly to system administrators (users) or groups. If users and groups do not have an associated command policy, the default deny policy is applied and users cannot run any commands or configure NetScaler Gateway.

You can configure custom command policies to define a greater level of detail for user rights assignments. For example, you can give one person the ability to add session policies to NetScaler Gateway, but not allow the user to perform any other configuration.

Configuring Command Policies for Delegated Administrators

January 8, 2024

NetScaler Gateway has four built-in command policies that you can use for delegated administration:

- **Read-only** allows read-only access to show all commands except for the system command group and `ns.conf show` commands.
- **Operator** allows read-only access and also allows access to enable and disable commands on services. This policy also allows access to set services and servers as "access down."
- **Network** permits almost complete system access, excluding system commands and the shell command.
- **Superuser** grants full system privileges, such as the privileges granted to the default administrator, `nsroot`.

Command policies contain built-in expressions. Use the configuration utility to create system users, system groups, command policies, and to define permissions.

To create an administrative user on NetScaler Gateway

1. In the configuration utility, in the navigation pane, on the **Configuration** tab, expand **System** > **User Administration** and then click **System Users**.
2. In the details pane, click **Add**.
3. In **User Name**, type a user name.
4. In the **Password** and **Confirm Password** fields, type the password.
5. To add users to a group, in **Member of**, click **Add**.
6. In **Available**, select a group and then click the right arrow.
7. Click **Command Policies > Action > Insert**.
8. In the Insert Command Policies dialog box, select the command, click **OK > Create > Close**.

Creating Administrative Groups

Administrative groups contain users who have administrative privileges on NetScaler Gateway. You can create administrative groups in the configuration utility.

To configure an administrative group by using the configuration utility

1. In the configuration utility, in the navigation pane, on the **Configuration** tab, expand **System** > **User Administration** and then click **System Groups**.

2. In the details pane, click **Add**.
3. In **Group Name**, type a name for the group.
4. To add an existing user to the group, in **Members**, click **Add**.
5. Under **Available**, select a user and then click the right arrow.
6. Under **Command Policies**, in **Action**, click **Insert**, select a policy or policies, click **OK**, click **Create** and then click **Close**.

Configuring Custom Command Policies for Delegated Administrators

January 8, 2024

When configuring a custom command policy, you provide a policy name and then configure the policy components to create the command specification. With the command specification, you can limit the commands administrators are allowed to use. For example, you want to deny administrators the ability to use the remove command. When configuring the policy, set the action to deny and then configure the parameters.

You can configure a simple or advanced command policy. When you configure a simple policy, you configure a component on the appliance, such as NetScaler Gateway and authentication. When you configure an advanced policy, you select the component, called an entity group and then select the commands administrators are allowed to perform in the group.

To create a simple custom command policy

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, expand **System** > **User Administration** and then click **Command Policies.**
2. In the details pane, click **Add.**
3. In **Policy Name**, type a name for the policy.
4. In **Action**, select **Allow** or **Deny**.
5. Under **Command Spec**, click **Add**.
6. In the **Add Command** dialog box, on the **Simple** tab, in Operation, select the action that delegated administrators can perform.
7. Under **Entity Group**, select one or more groups.

   You can press the CTRL key to select multiple groups.
8. Click **Create** and then click **Close**.

To create an advanced custom command policy

1. In the configuration utility, in the navigation pane, on the **Configuration** tab, expand **System** > **User Administration** and then click **Command Policies**.
2. In the details pane, click **Add**.
3. In **Policy Name**, type a name for the policy.
4. In **Action**, select **Allow** or **Deny**.
5. Under **Command Spec**, click **Add**.
6. In the **Add Command** dialog box, click the **Advanced** tab.
7. In **Entity Group** select the group to which the command belongs, such an authentication or high availability.
8. Under **Entity**, select the policy.

   You can press the CTRL key to select multiple items in the list.
9. In **Operation**, select the command, click **Create,** and then click **Close**.

   You can press the CTRL key to select multiple items in the list.
10. Click **Create,** and then click **Close**.
11. In the **Create Command Policy** dialog box, click **Create,** and then click **Close**.

When you click **Create**, the expression appears under Command Spec in the **Create Command Policy** dialog box.

After creating the custom command policy, you can bind it to a user or a group.

> **Note:** You can only bind custom command policies to the users or groups you create. You cannot bind a custom command policy to the user `nsroot`.

To bind a custom command policy to a user or group

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, expand **System** > **User Administration** and then click **System Users** or click **Systems Groups**.
2. In the details pane, select a user or group from the list and then click **Open**.
3. Under **Command Policies**, select the policy and then click **OK**.

Configuring Auditing on NetScaler Gateway

January 8, 2024

NetScaler Gateway allows you to log the states and status information that the appliance collects. You can use the audit logs to view the event history in chronological order. The messages within the logs contain information about the event that generated the message, a time stamp, the message type, and predefined log levels and message information. You can configure settings that determine the information that is logged and the location where the messages are stored.

NetScaler Gateway currently supports 2 log formats: a proprietary log format for local logs, and the syslog format for use with syslog servers. You can configure the audit logs to provide the following information:

Level	Description
EMERGENCY	Logs major errors only. Entries in the log indicate that NetScaler Gateway is experiencing a critical problem that is causing it to be unusable.
ALERT	Logs problems that might cause NetScaler Gateway to function incorrectly, but are not critical to its operation. Corrective action can be taken as soon as possible to prevent NetScaler Gateway from experiencing a critical problem.
CRITICAL	Logs critical conditions that do not restrict the operation of NetScaler Gateway, but might escalate to a larger problem.
ERROR	Logs entries that result from a failed operation on NetScaler Gateway.
WARNING	Logs potential issues that can result in an error or a critical error.
NOTICE	Logs more in-depth issues than the information level log, but serves the same purpose as notification.
INFORMATION	Log actions taken by NetScaler Gateway. This level is useful for troubleshooting problems.

The NetScaler Gateway audit log also stores compression statistics for NetScaler Gateway if you configure TCP compression. The compression ratio achieved for different data is stored in the log file for each user session.

NetScaler Gateway uses the log signature SessionID. This allows you to track logs per session rather than per user. Logs that are generated as part of a session have the same SessionID. If a user establishes two sessions from the same user device with the same IP address, each session has a unique SessionID.

> **Important:** If you have written custom log parsing scripts, you need to make this signature change within the custom parsing scripts.

Configuring Logs on NetScaler Gateway

January 8, 2024

When you configure logging on NetScaler Gateway, you can choose to store the audit logs on NetScaler Gateway or send them to a syslog server. You use the configuration utility to create auditing policies and configure settings to store the audit logs.

To create an auditing policy

1. In the configuration utility, on the Configuration tab, expand **NetScaler Gateway** > **Policies** > **Auditing**.
2. In **Name**, type a name for the policy.
3. Select one of the following:
   - Syslog if you want to send the logs to a Syslog server.
   - `Nslog` to store the logs on NetScaler Gateway.

     > **Note:** If you select this option, logs are stored in the /var/log folder on the appliance.
4. In the details pane, click **Add**.
5. Type the following information for the server information where the logs are stored:
   - In Name, type the name of the server.
   - Under Server, type the name or the IP address of the log server.
6. Click Create and then click Close.

After you create the auditing policy, you can bind the policy to any combination of the following:

- Globally
- Virtual servers
- Groups
- Users

To bind an auditing policy globally

1. In the configuration utility, on the Configuration tab, expand **NetScaler Gateway** > **Policies** > **Auditing**.
2. Select either `Syslog` or `Nslog`.
3. In the details pane, click **Action** and then click **Global Bindings**.
4. In the **Bind/Unbind Auditing Policies** to **Global** dialog box, under **Details**, click **Insert Policy**.
5. Under **Policy Name**, select a policy and then click **OK**.

To modify an auditing policy

You can modify an existing auditing policy to change the server to which the logs are sent.

1. In the configuration utility, on the **Configuration** tab, expand **NetScaler Gateway** > **Policies** > **Auditing**
2. Select either `Syslog` or `Nslog`.
3. In the details pane, click a policy and then click **Open**.
4. In Server, select the new server, and then click **OK**.

To remove an auditing policy

You can remove an auditing policy from NetScaler Gateway. When you remove an auditing policy, the policy is unbound automatically.

1. In the configuration utility, on the Configuration tab, expand **NetScaler Gateway** > **Policies** > **Auditing**.
2. Select either **Syslog** or `Nslog`.
3. In the details pane, click a policy and then click **Remove**.

Configuring ACL Logging

January 8, 2024

You can configure NetScaler Gateway to log details for packets that match an extended access control list (ACL). In addition to the ACL name, the logged details include packet-specific information, such as the source and destination IP addresses. The information is stored either in a syslog or `nslog` file, depending on the type of logging (syslog or `nslog`) that you enable.

You can enable logging at both the global level and the ACL level. However, to enable logging at the ACL level, you must also enable it at the global level. The global setting takes precedence.

To optimize logging, when multiple packets from the same flow match an ACL, only the first packet's details are logged. The counter is incremented for every other packet that belongs to the same flow. A flow is defined as a set of packets that have the same values for the following parameters:

- Source IP
- Destination IP
- Source port
- Destination port
- Protocol (TCP or UDP)

If the packet is not from the same flow, or if the time duration is beyond the mean time, a new flow is created. Mean time is the time during which packets of the same flow do not generate additional messages (although the counter is incremented).

> **Note:** The total number of different flows that can be logged at any given time is limited to 10,000.

The following table describes the parameters with which you can configure ACL logging at the rule level for extended ACLs.

Parameter Name	Description
`Logstate`	State of the logging feature for the ACL. Possible values: ENABLED and DISABLED. Default: DISABLED.
`Ratelimit`	Number of log messages that a specific ACL can generate. Default: 100.

To configure ACL logging by using the configuration utility

You can configure logging for an ACL and specify the number of log messages that the rule can generate.

1. In the configuration utility, in the navigation pane, expand **System** > **Network** and then click ACLs.
2. In the details pane, click the **Extended ACLs** tab and then click Add.
3. In the **Create Extended ACL** dialog box, in Name, type a name for the policy.
4. Select the **Log State** check box.
5. In the **Log Rate Limit** text box, type the rate limit that you want to specify for the rule and then click **Create**.

After you configure ACL logging, you can enable it on NetScaler Gateway. Create an auditing policy and then bind it to a user, group, virtual server, or globally.

To enable ACL or TCP logging on NetScaler Gateway

1. In the configuration utility, in the navigation pane, expand **NetScaler Gateway** > **Policies** > **Auditing**.
2. Select either syslog or `nslog`.
3. On the **Servers** tab, click **Add**.
4. In the **Create Auditing Server** dialog box, in **Name**, type a name for the server and then configure the server settings.
5. Click **ACL Logging** or **TCP Logging** and then click **Create**.

Enabling Citrix Secure Access Logging

January 8, 2024

You can configure the Citrix Secure Access client to log all errors to text files that are stored on the user device. Users can configure the Citrix Secure Access client to set the level of logging on the user device to record specific user activities. When users configure logging, the plug-in creates the following two files on the user device:

- hooklog<num>.txt, which logs interception messages that the Citrix Secure Access client generates.
- nssslvpn.txt, which lists errors with the plug-in.

> **Note:** The hooklog.txt files are not deleted automatically. Citrix recommends deleting the files periodically.

User logs are located in the following directories in Windows on the user device:

- Windows XP (all users): %SystemDrive%:\Documents and Settings\All Users\Application Data\Citrix\AGEE
- Windows XP (user-specific): %SystemDrive%:\Documents and Settings\%username%\Local Settings\Application Data\Citrix\AGEE
- Windows Vista (all users): %SystemDrive%:\ProgramData\Citrix\AGEE
- Windows Vista (user-specific): %SystemDrive%:\Users\%username%\AppData\Local\Citrix\AGEE
- Windows 7 (all users): %SystemDrive%:\ProgramData\Citrix\AGEE
- Windows 7 (user-specific): %SystemDrive%:\Users\%username%\AppData\Local\Citrix\AGEE
- Windows 8 (all users): %SystemDrive%:\ProgramData\Citrix\AGEE
- Windows 8 (user-specific): %SystemDrive%:\Users\%username%\AppData\Local\Citrix\AGEE

You can use these log files to troubleshoot the Citrix Secure Access client. Users can email the log files to Technical Support.

In the Configuration dialog box, users can set the level of logging for the Citrix Secure Access client. The logging levels are:

- Record error messages
- Record event messages
- Record Citrix Secure Access client statistics
- Record all errors, event messages, and statistics

For more details about the logging feature of Citrix Secure Access client for Windows, refer to Improved log collection for Windows client.

To monitor ICA connections

January 8, 2024

You can monitor active user sessions on your server farm by using the ICA Connections dialog box. This dialog box provides the following information:

- User name of the person connecting to the server farm
- Domain name of the server farm
- IP address of the user device
- Port number of the user device
- IP address of the server running Citrix Virtual Apps and Desktops
- Port number of the server running Citrix Virtual Apps and Desktops

1. Navigate to **Configuration > NetScaler Gateway**.
2. In the **Monitor Connections** section, click **ICA Connections**.

ICA session logs

The `ns.log` file prints the ICA session logs in the following format:

```
May  2 09:29:02 <local0.info> 10.106.40.223  05/02/2023:09:29:02 GMT
    0-PPE-1 : default ICA Message 141327 0 :  "[Remote ip =
    10.10.99.86:514] [EDT] [CGP][ICAUUID=0006ab3454-d7de-1450-9678-
    c6333447a76] Received response from STA server {
 sta-server=10.11.40.222:80,type=ResponseData }
 "
```

Starting from release version 13.1 build 50.x, the following enhancements are made to the ICA logs:

- Displays connection types such as TCP, EDT, CGP, and SOCKS.
- Displays the ICA Universally Unique Identifier (UUID).
- All the STA logs are displayed as info-level logs.

Authentication and Authorization

January 8, 2024

NetScaler Gateway employs a flexible authentication design that permits extensive customization of user authentication for NetScaler Gateway. You can use industry-standard authentication servers and configure NetScaler Gateway to authenticate users with the servers. NetScaler Gateway also supports authentication based on attributes present in a client certificate. NetScaler Gateway authentication is designed to accommodate simple authentication procedures that use a single source for user authentication, and more complex, cascaded authentication procedures that rely upon multiple authentication types.

NetScaler Gateway authentication incorporates local authentication for the creation of local users and groups. This design centers around the use of policies to control the authentication procedures that you configure. The policies you create can be applied at NetScaler Gateway global or virtual server levels and can be used to set authentication server parameters conditionally based on the user's source network.

Because policies are bound either globally or to a virtual server, you can also assign priorities to your policies to create a cascade of multiple authentication servers as part of authentication.

NetScaler Gateway includes support for the following authentication types.

- Local
- Lightweight Directory Access Protocol (LDAP)
- RADIUS
- SAML
- TACACS+
- Client certificate authentication (including smart card authentication)

NetScaler Gateway also supports RSA SecurID, Gemalto Protiva, and SafeWord. You use a RADIUS server to configure these types of authentication.

While authentication allows users to log on to NetScaler Gateway and connect to the internal network, authorization defines the resources within the secure network to which users have access. You configure authorization with LDAP and RADIUS policies.

Configuring Default Global Authentication Types

January 8, 2024

When you installed NetScaler Gateway and ran the NetScaler Gateway wizard, you configured authentication within the wizard. This authentication policy is bound automatically to the NetScaler Gateway global level. The authentication type you configure within the NetScaler Gateway wizard is the default authentication type. You can change the default authorization type by running the NetScaler Gateway wizard again or you can modify the global authentication settings in the configuration utility.

If you need to add additional authentication types, you can configure authentication policies on NetScaler Gateway and bind the policies to NetScaler Gateway by using the configuration utility. When you configure authentication globally, you define the type of authentication, configure the settings, and set the maximum number of users that can be authenticated.

After configuring and binding the policy, you can set the priority to define which authentication type takes precedence. For example, you configure LDAP and RADIUS authentication policies. If the LDAP policy has a priority number of 10 and the RADIUS policy has a priority number of 15, the LDAP policy takes precedence, regardless of where you bind each policy. This is called cascading authentication.

You can select to deliver logon pages from the NetScaler Gateway in-memory cache or from the HTTP server running on NetScaler Gateway. If you choose to deliver the logon page from the in-memory cache, the delivery of the logon page from NetScaler Gateway is significantly faster than from the HTTP server. Choosing to deliver the logon page from the in-memory cache reduces the wait time when a large number of users log on at the same time. You can only configure the delivery of logon pages from the cache as part of a global authentication policy.

You can also configure the network address translation (NAT) IP address that is a specific IP address for authentication. This IP address is unique for authentication and is not the NetScaler Gateway subnet, mapped, or virtual IP addresses. This is an optional setting.

Note: You cannot use the NetScaler Gateway wizard to configure SAML authentication.

You can use the Quick Configuration wizard to configure LDAP, RADIUS, and client certificate authentication. When you run the wizard, you can select from an existing LDAP or RADIUS server configured on NetScaler Gateway. You can also configure the settings for LDAP or RADIUS. If you use two-factor authentication, Citrix recommends using LDAP as the primary authentication type.

To configure authentication globally

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click Global Settings.
2. In the details pane, under Settings, click Change authentication settings.
3. In Maximum Number of Users, type the number of users who can be authenticated by using this authentication type.
4. In NAT IP address, type the unique IP address for authentication.
5. Select Enable static caching to deliver logon pages faster.
6. Select Enable Enhanced Authentication Feedback to provide a message to users if authentication fails. The message users receive include password errors, account disabled or locked, or the user is not found, to name a few.
7. In Default Authentication Type, select the authentication type.
8. Configure the settings for your authentication type and then click OK.

Configuring Authentication Without Authorization

January 8, 2024

Authorization defines the resources to which users are allowed to connect through NetScaler Gateway. You configure authorization policies by using an expression and then setting the policy to be allowed or denied. You can configure NetScaler Gateway to use authentication only, without authorization.

When you configure authentication without authorization, NetScaler Gateway does not perform a group authorization check. The policies that you configure for the user or group are assigned to the user.

For more information about configuring authorization, see Configuring Authorization.

Configuring Authorization

January 8, 2024

Authorization specifies the network resources to which users have access when they log on to NetScaler Gateway. The default setting for authorization is to deny access to all network resources. Citrix recommends using the default global setting and then creating authorization policies to define the network resources users can access.

You configure authorization on NetScaler Gateway by using an authorization policy and expressions. After you create an authorization policy, you can bind it to the users or groups that you configured on the appliance.

Configuring Authorization Policies

January 8, 2024

When you configure an authorization policy, you can set it to allow or deny access to network resources in the internal network. For example, to allow users access to the 10.3.3.0 network, use the following expression:

CLIENT.IP.DST.IN_SUBNET(10.3.0.0/16)

Authorization policies are applied to users and groups. After a user is authenticated, NetScaler Gateway performs a group authorization check by obtaining the user's group information from either an RADIUS, LDAP, or TACACS+ server. If group information is available for the user, NetScaler Gateway checks the network resources allowed for the group.

To control which resources users can access, you must create authorization policies. If you do not need to create authorization policies, you can configure default global authorization.

If you create an expression within the authorization policy that denies access to a file path, you can only use the subdirectory path and not the root directory. For example, use fs.path contains "\\dir1\\dir2"instead of fs.path contains "\\rootdir\\dir1\\dir2". If you use the second version in this example, the policy fails.

After you configure the authorization policy, you then bind it to a user or group as shown in the tasks below.

By default, authorization policies are validated first against policies that you bind to the virtual server and then against policies bound globally. If you bind a policy globally and want the global policy to take precedence over a policy that you bind to a user, group, or virtual server, you can change the priority number of the policy. Priority numbers start at zero. A lower priority number gives the policy higher precedence.

For example, if the global policy has a priority number of one and the user has a priority of two, the global authentication policy is applied first.

> **Important:**
>
> - Classic authorization policies are applied only on TCP traffic.
> - Advanced authorization policy can be applied on all types of traffic (TCP/UDP/ICMP/DNS).

> – To apply policy on UDP/ICMP/DNS traffic, policies must be bound at type UDP_REQUEST, ICMP_REQUEST, and DNS_REQUEST respectively.
> – While binding, if “type”is not explicitly mentioned or “type”is set to REQUEST, the behavior does not change from earlier builds, that is these policies are applied only to TCP traffic.
> – The policies bound at UDP_REQUEST do not apply for DNS traffic. For DNS, policies must be explicitly bound to DNS_REQUEST TCP_DNS is similar to other TCP requests.

For more details on advanced authorization policies, see article https://support.citrix.com/article/CTX232237.

Sample authorization policy expressions

Following are the expression examples of authorization policies:

- `add authorization policy athzPol1 "HTTP.REQ.USER.IS_MEMBER_OF(\"allowedGroup\")"ALLOW`
- `add authorization policy athzPol2 "CLIENT.IP.DST.BETWEEN(10.102.75.10,10.1 "DENY`
- `add authorization policy athzPol3 "HTTP.REQ.HOSTNAME.CONTAINS(\"portal-srv")|| CLIENT.IP.DST.IN_SUBNET(10.102.75.0/25)"ALLOW`

To configure an authorization policy by using the GUI

1. Navigate to **NetScaler Gateway > Policies > Authorization.**
2. In the details pane, click **Add**.
3. In **Name**, type a name for the policy.
4. In **Action**, select **Allow** or **Deny**.
5. In **Expression**, click **Expression Editor**.
6. To start to configure the expression, click **Select** and choose the necessary elements.
7. Click **Done** when your expression is complete.
8. Click **Create**.

To bind an authorization policy to a user by using the GUI

1. Navigate to **NetScaler Gateway > User Administration.**
2. Click **AAA Users**.
3. In the details pane, select a user and then click **Edit**.

4. In **Advanced Settings**, click **Authorization Policies**.
5. In **Policy Binding** page, select a policy or create a policy.
6. In **Priority**, set the priority number.
7. In **Type**, select the request type and then click **OK**.

To bind an authorization policy to a group by using the GUI

1. Navigate to **NetScaler Gateway > User Administration**.
2. Click **AAA Groups**.
3. In the details pane, select a group and then click **Edit**.
4. In **Advanced Settings**, click **Authorization Policies**.
5. In **Policy Binding** page, select a policy or create a policy.
6. In **Priority**, set the priority number.
7. In **Type**, select the request type and then click **OK**.

Setting Default Global Authorization

January 8, 2024

To define the resources to which users have access on the internal network, you can configure default global authorization. You configure global authorization by allowing or denying access to network resources globally on the internal network.

Any global authorization action you create is applied to all users who do not already have an authorization policy associated with them, either directly or through a group. A user or group authorization policy always overrides the global authorization action. If the default authorization action is set to Deny, you must apply authorization policies for all users or groups in order to make network resources accessible to those users or groups. This requirement helps to improve security.

To set default global authorization:

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Security tab, next to Default Authorization Action, select Allow or Deny then and click OK.

Disabling Authentication

January 8, 2024

If your deployment does not require authentication, you can disable it. You can disable authentication for each virtual server that does not require authentication.

Important: Citrix recommends disabling authentication with caution. If you are not using an external authentication server, create local users and groups to allow NetScaler Gateway to authenticate users. Disabling authentication stops the use of authentication, authorization, and accounting features that control and monitor connections to NetScaler Gateway. When users type a web address to connect to NetScaler Gateway, the logon page does not appear.

To disable authentication

1. In the configuration utility, in the navigation pane, expand NetScaler Gateway and then click Virtual Servers.
2. In the details pane, click a virtual server and then click Open.
3. On the Authentication tab, under User Authentication, click to clear Enable Authentication.

Configuring Authentication for Specific Times

January 8, 2024

You can configure an authentication policy so users are allowed access to the internal network at specific times, such as during normal working hours. When users try to log on at a different time, logon is denied.

To restrict when users log on to NetScaler Gateway, create an expression within the authentication policy and then bind it to a virtual server or globally.

To configure authentication for time, date, or day of week

1. In the configuration utility, on the Configuration tab, expand NetScaler Gateway > Policies > Authentication.
2. Under Authentication, select the authentication type.
3. In the details pane, click the Policies tab, select an authentication policy and then click Open.

4. In the Configure Authentication Policy dialog box, under Expression, next to Match Any Expression, click Add.
5. In the Add Expression dialog box, in Expression Type, select Date/Time.
6. In Qualifier, select one of the following:

   - TIME to configure the time users cannot log on.
   - DATE to configure the date users cannot log on.
   - DAYOFWEEK to configure the day users cannot log on.

   Example: TIME: 2020-10-12-02:30:00GMT DATE: 2020-10-12 DAYOFWEEK: Monday
7. In Operator, select the value.
8. In Value, click the calendar next to the text box and then select the day, date, or time.
9. Click OK twice, click Close, and click OK.

How Authentication Policies Work

January 8, 2024

When users log on to NetScaler Gateway, they are authenticated according to a policy that you create. The policy defines the authentication type. A single authentication policy can be used for simple authentication needs and is typically bound at the global level. You can also use the default authentication type, which is local. If you configure local authentication, you must also configure users and groups on NetScaler Gateway.

You can configure multiple authentication policies and bind them to create a detailed authentication procedure and virtual servers. For example, you can configure cascading and two-factor authentication by configuring multiple policies. You can also set the priority of the authentication policies to determine which servers and the order in which NetScaler Gateway checks user credentials. An authentication policy includes an expression and an action. For example, if you set the expression to True value, when users log on, the action evaluates user logon to true and then users have access to network resources.

After you create an authentication policy, you bind the policy at either the global level or to virtual servers. When you bind at least one authentication policy to a virtual server, any authentication polices that you bound to the global level are not used when users log on to the virtual server, unless the global authentication type has a higher precedence than the policy bound to the virtual server.

When a user logs on to NetScaler Gateway, authentication is evaluated in the following order:

- The virtual server is checked for any bound authentication policies.

- If authentication policies are not bound to the virtual server, NetScaler Gateway checks for global authentication policies.
- If an authentication policy is not bound to a virtual server or globally, the user is authenticated through the default authentication type.

If you configure LDAP and RADIUS authentication policies and want to bind the policies globally for two-factor authentication, you can select the policy in the configuration utility and then select if the policy is the primary or secondary authentication type. You can also configure a group extraction policy.

Configuring Authentication Profiles

January 8, 2024

You can create an authentication profile by using the NetScaler Gateway wizard or the configuration utility. The profile contains all of the settings for the authentication policy. You configure the profile when you create the authentication policy.

With the NetScaler Gateway wizard, you can use the chosen authentication type to configure authentication. If you want to configure additional authentication policies after running the wizard, you can use the configuration utility. For more information about the NetScaler Gateway wizard, see Configuring Settings by Using the NetScaler Gateway Wizard.

To create an authentication policy by using the configuration utility

1. In the configuration utility, on the Configuration tab, expand NetScaler Gateway > Policies > Authentication.
2. In the navigation pane, under Authentication, select an authentication type.
3. In the details pane, on the Policies tab, click Add.
4. If you are using an external authentication type, next to Server, click New.
5. In the Create Authentication Server dialog box, configure the settings for your authentication type, click Create and then click Close.
6. In the Create Authentication Policy dialog box, next to Named Expressions, select True value, click Add Expression, click Create and then click Close.
   Note: When you select an authentication type and save the authentication profile, you cannot change the authentication type. To use a different authentication type, you must create a new policy.

To modify an authentication policy by using the configuration utility

You can modify configured authentication policies and profiles, such as the IP address of the authentication server or the expression.

1. In the configuration utility, on the Configuration tab, expand NetScaler Gateway > Policies > Authentication.
2. In the navigation pane, under Authentication, select an authentication type.
3. In the details pane, on the Servers tab, select a server and then click Open.

To remove an authentication policy

If you changed or removed an authentication server from your network, remove the corresponding authentication policy from NetScaler Gateway.

1. In the configuration utility, on the Configuration tab, expand NetScaler Gateway > Policies > Authentication.
2. In the navigation pane, under Authentication, select an authentication type.
3. In the details pane, on the Policies tab, select a policy and then click Remove.

Binding Authentication Policies

January 8, 2024

After you configure the authentication policies, you bind the policy either globally or to a virtual server. You can use either the configuration utility to bind an authentication policy.

To bind an authentication policy globally by using the GUI

1. In the configuration utility, on the Configuration tab, expand **NetScaler Gateway > Policies > Authentication**.
2. Click an authentication type.
3. In the details pane, on the **Policies** tab, click a server, and then in **Action**, click **Global Bindings**.
4. On the **Primary or Secondary** tab, under **Details**, click **Insert Policy**.
5. Under **Policy Name**, select the policy, and then click **OK**.

   Note: When you select the policy, NetScaler Gateway sets the expression to True value automatically.

To unbind a global authentication policy by using the GUI

1. In the configuration utility, on the Configuration tab, expand **NetScaler Gateway > Policies > Authentication**.
2. On the **Policies** tab, in **Action**, click **Global Bindings**.
3. In the **Bind/Unbind Authentication Policies to Global** dialog box, on the **Primary or Secondary** tab, in **Policy Name**, select the policy, click **Unbind Policy**, and then click **OK**.

Setting Priorities for Authentication Policies

January 8, 2024

By default, authentication polices are validated first against policies that you bind to the virtual server and then against policies bound globally. If you bind an authentication policy globally and want the global policy to take precedence over a policy that you bind to a virtual server, you can change the priority number of the policy. Priority numbers start at zero. A lower priority number gives the authentication policy higher precedence.

For example, if the global policy has a priority number of one and the virtual server has a priority of two, the global authentication policy is applied first.

To set or change the priority for global authentication policies

1. In the configuration utility, on the Configuration tab, expand NetScaler Gateway > Policies > Authentication.
2. On the Policies tab, in Action, click Global Bindings.
3. In the Bind/Unbind Authentication Global Policies dialog box, on either the Primary or Secondary tab, under Priority, type the number and then click OK.

To change the priority for an authentication policy bound to a virtual server

You can also modify an authentication policy that is bound to a virtual server.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click Virtual Servers.
2. Select a virtual server and then click Open.
3. Click the Authentication tab and then select either Primary or Secondary.
4. Select the policy and in Priority, type the number of the priority and then click OK.

Configuring Local Users

January 8, 2024

You can create user accounts locally on NetScaler Gateway 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.

If you are using local authentication, create users and then add them to groups that you create on NetScaler Gateway. After configuring users and groups, you can apply authorization and session policies, create bookmarks, specify applications, and specify the IP address of file shares and servers to which users have access.

To create local users

1. In the configuration utility, click the **Configuration** tab and in the navigation pane, expand **NetScaler Gateway > User Administration**, and then click **AAA Users**.
2. In the details pane, click **Add**.
3. In **User Name**, type the user name.
4. If you are using local authentication, clear **External Authentication**.
   Note: Select **External Authentication** to have users authenticate against an external authentication server, such as LDAP or RADIUS. Clear the check box to have NetScaler Gateway authenticate against the local user database.
5. In **Password** and **Confirm Password**, type the password for the user, click **Create**, and then click **Close**.

To change a user password

After creating a local user, you can change the user's password or configure the user account to be authenticated against an external authentication server.

1. In the configuration utility, click the **Configuration** tab and in the navigation pane, expand **NetScaler Gateway > User Administration**, and then click **AAA Users**.
2. In the details pane, select a user and then click **Open**.
3. In **Password** and **Confirm Password**, type the new password for the user, and then click **OK**.

To change a user's authentication method

If you have users who are configured for local authentication, you can change the authentication to an external authentication server. To do this, enable external authentication.

1. In the configuration utility, click the **Configuration** tab and in the navigation pane, expand **NetScaler Gateway > User Administration**, and then click **AAA Users**.
2. In the details pane, select a user and then click **Open**.
3. Select **External Authentication**, and then click **OK**.

To remove a user

You can also remove a user from NetScaler Gateway.

1. In the configuration utility, click the **Configuration** tab and in the navigation pane, expand **NetScaler Gateway > User Administration**, and then click **AAA Users**.
2. In the details pane, select a user, and then click **Remove**.

When you remove a user from NetScaler Gateway, all associated policies are also removed from the user profile.

Configuring Groups

January 8, 2024

You can have groups on NetScaler Gateway that are local groups and can authenticate users with local authentication. If you are using external servers for authentication, groups on NetScaler Gateway are configured to match 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 Gateway.

After you configure groups, you can apply authorization and session policies, create bookmarks, specify applications, and specify the IP address of file shares and servers to which the user has access.

If you are using local authentication, create users and add them to groups that are configured on NetScaler Gateway. The users then inherit the settings for that group.

Important: If users are a member of an Active Directory group, the name of the group on NetScaler Gateway must be the same as the Active Directory group.

To create a group

1. In the configuration utility, click the **Configuration** tab and in the navigation pane, expand **NetScaler Gateway > User Administration** and then click **AAA Groups**.
2. In the details pane, click **Add**.
3. In **Group Name**, type a name for the group, click **Create**, and then click **Close**.

To delete a group

You can also delete user groups from NetScaler Gateway.

1. In the configuration utility, click the **Configuration** tab and in the navigation pane, expand **NetScaler Gateway > User Administration** and then click **AAA Groups**.
2. In the details pane, select the group, and then click **Remove**.

Adding Users to Groups

January 8, 2024

You can add users to a group either during creation of the group or later. You can add users to multiple groups so users can inherit the policies and settings that are bound to those groups.

To add users to groups:

1. In the configuration utility, click the Configuration tab and in the navigation pane, expand **NetScaler Gateway > User Administration**, and then click **AAA Users**.
2. In the details pane, select a group, and then click **Open**.
3. On the **Users** tab, under **Available Users**, select the users, click **Add**, and click **OK**.

Configuring Policies with Groups

January 8, 2024

After you configure groups, you can use the Group dialog box to apply policies and settings that specify user access. If you are using local authentication, you create users and add them to groups that are configured on NetScaler Gateway. The users then inherit the settings for that group.

You can configure the following policies or settings for a group of users in the Group dialog box:

- Users
- Authorization policies
- Auditing policies
- Session policies
- Traffic policies
- Bookmarks
- Intranet applications
- Intranet IP addresses

In your configuration, you might have users that belong to more than one group. In addition, each group might have one or more bound session policies, with different parameters configured. Users that belong to more than one group inherit the session policies assigned to all the groups to which the user belongs. To ensure which session policy evaluation takes precedence over the other, you must set the priority of the session policy.

For example, you have group1 that is bound with a session policy configured with the home page www.homepage1.com. Group2 is bound with a session policy configured with home page www.homepage2.com. When these policies are bound to respective groups without a priority number or with a same priority number, the home page that appears to users who belong to both the groups depends on which policy is processed first. By setting a lower priority number, which gives higher precedence, for the session policy with home page www.homepage1.com, you can ensure that users who belong to both the groups receive the home page www.homepage1.com.

If session policies do not have a priority number assigned or have the same priority number, precedence is evaluated in the following order:

- User
- Group
- Virtual server
- Global

If policies are bound to the same level, without a priority number or if the policies have the same priority number, the order of evaluation is per the policy bind order. Policies that are bound first to a level receive precedence over policies bound later.

If we have a user bound to multiple groups with each group having IIP bound, the user can get free IP from any of the bound groups.

Configuring LDAP Authentication

January 8, 2024

You can configure the NetScaler Gateway to authenticate user access with one or more LDAP servers.

LDAP authorization requires identical group names in the Active Directory, on the LDAP server, and on the NetScaler Gateway. The characters and case must also match.

By default, LDAP authentication is secure by using Secure Sockets Layer (SSL) or Transport Layer Security (TLS). There are two types of secure LDAP connections. With one type, the LDAP server accepts the SSL or TLS connections on a port separate from the port that the LDAP server uses to accept clear

LDAP connections. After users establish the SSL or TLS connections, LDAP traffic can be sent over the connection.

The port numbers for LDAP connections are:

- 389 for unsecured LDAP connections
- 636 for secure LDAP connections
- 3268 for Microsoft unsecure LDAP connections
- 3269 for Microsoft secure LDAP connections

The second type of secure LDAP connections uses the StartTLS command and uses port number 389. If you configure port numbers 389 or 3268 on NetScaler Gateway, the server tries to use StartTLS to make the connection. If you use any other port number, the server attempts to make connections by using SSL or TLS. If the server cannot use StartTLS, SSL, or TLS, the connection fails.

If you specify the root directory of the LDAP server, NetScaler Gateway searches all the subdirectories to find the user attribute. In large directories, this approach can affect performance. For this reason, Citrix recommends that you use a specific organizational unit (OU).

The following table contains examples of user attribute fields for LDAP servers:

LDAP server	User attribute	Case sensitive
Microsoft Active Directory Server	sAMAccountName	No
Novell eDirectory	ou	Yes
IBM Directory Server	uid	Yes
Lotus Domino	CN	Yes
Sun ONE directory (formerly iPlanet)	uid or cn	Yes

This table contains examples of the base DN:

LDAP server	Base DN
Microsoft Active Directory Server	DC=citrix,DC=local
Novell eDirectory	ou=users,ou=dev
IBM Directory Server	cn=users
Lotus Domino	OU=City,O=Citrix, C=US
Sun ONE directory (formerly iPlanet)	ou=People,dc=citrix,dc=com

The following table contains examples of bind DN:

LDAP server	Bind DN
Microsoft Active Directory Server	CN=Administrator, CN=Users, DC=citrix, DC=local
Novell eDirectory	cn=admin, o=citrix
IBM Directory Server	LDAP_dn
Lotus Domino	CN=Notes Administrator, O=Citrix, C=US
Sun ONE directory (formerly iPlanet)	uid=admin,ou=Administrators, ou=TopologyManagement,o=NetscapeRoot

Note: For more information regarding LDAP server settings, see Determining Attributes in Your LDAP Directory.

To configure LDAP authentication by using the configuration utility

January 8, 2024

1. Navigate to **NetScaler Gateway** >**Policies** > **Authentication**.
2. Click **LDAP**.
3. In the details pane, on the **Policies** tab, click **Add**.
4. In **Name**, type a name for the policy.
5. Next to **Server**, click **New**.
6. In **Name**, type the name of the server.
7. Under **Server**, in **IP Address and Port**, type the IP address and port number of the LDAP server.
8. In **Type**, select either **AD** for Active Directory or **NDS** for Novell Directory Services.
9. Under **Connection Settings**, complete the following:

   a) In **Base DN (location of users)**, type the base DN under which users are located. Base DN search the users located under the selected directory (AD or NDS).

   The base DN is derived from the Bind DN by removing the user name and specifying the group where users are located. Examples of the syntax for base DN are:

```
ou=users,dc=ace,dc=com
cn=Users,dc=ace,dc=com
```


b) In **Administrator Bind DN**, type the administrator bind DN for queries to the LDAP directory. Examples for the syntax of bind DN are:

```
domain/user name
ou=administrator,dc=ace,dc=com
user@domain.name (for Active Directory)
cn=Administrator,cn=Users,dc=ace,dc=com
```

For Active Directory, the group name specified as cn=groupname is required. The group name that you define in NetScaler Gateway and the group name on the LDAP server must be identical.

For other LDAP directories, the group name either is not required or, if necessary, is specified as ou=groupname.

NetScaler Gateway binds to the LDAP server using the administrator credentials and then searches for the user. After locating the user, NetScaler Gateway unbinds the administrator credentials and rebinds with the user credentials.

c) In **Administrator Password and Confirm Administrator Password**, type the administrator password for the LDAP server.

10. To retrieve more LDAP settings automatically, click **Retrieve Attributes**.

    When you click **Retrieve Attributes**, the fields under Other Settings populate automatically. If you want to ignore this step, continue with Steps 12 and 13. Otherwise, skip to Step 14.

11. Under **Other Settings**, in Server Logon Name Attribute, type the attribute under which NetScaler Gateway must look for user logon names for the LDAP server that you are configuring. The default is `samAccountName`.

12. In **Search Filter**, type the value to search for the users associated with single or multiple active directory groups.

    For example, “memberOf=CN=GatewayAccess,OU=Groups,DC=Users,DC=lab”.

    > **Note**
    >
    > You can use the preceding example to restrict NetScaler Gateway access only to the members of a specific AD group.

13. In **Group Attribute**, leave the default memberOf for Active Directory or change the attribute to the attribute of the LDAP server type you are using. This attribute enables NetScaler Gateway to obtain the groups associated with a user during authorization.

14. In **Security** Type, select the security type and then click **Create**.

15. To allow users to change their LDAP password, select **Allow Password Change**.

    Note:

- If you select **PLAINTEXT** as the security type, allowing users to change their passwords is not supported.
- If you select **PLAINTEXT** or **TLS** for security, use port number 389. If you select **SSL**, use port number 636.

Determine attributes in your LDAP directory

January 8, 2024

If you need help with determining your LDAP directory attributes so you can configure authentication settings on NetScaler Gateway, you can easily look them up with the free LDAP browser from Softerra.

You can download the LDAP browser from the Softerra LDAP Administrator website. After you install the browser, set the following attributes:

- The host name or IP address of your LDAP server.
- The port of your LDAP server. The default is 389.
- The base DN field, which you can leave blank. The information provided by the LDAP browser can help you determine the base DN that you must configure this setting on NetScaler Gateway.
- The Anonymous Bind check determines if the LDAP server requires user credentials to connect to it. If the LDAP server requires credentials, leave the check box cleared.

After completing the settings, the LDAP browser displays the profile name in the left pane and connects to the LDAP server.

Configuring LDAP Group Extraction

January 8, 2024

If you are using two-factor authentication, groups extracted from both the primary and secondary authentication sources are concatenated. Authorization policies can be applied to the group that is extracted from the primary or secondary authentication server.

The group names obtained from the LDAP server are compared with the group names created locally on NetScaler Gateway. If the two group names match, the properties of the local group apply to the group obtained from the LDAP servers.

If users belong to more than one LDAP group, NetScaler Gateway extracts user information from all the groups to which users belong. If a user is a member of two groups on NetScaler Gateway and each

group has a bound session policy, the user inherits the session policies from both groups. To make sure that users receive the correct session policy, set the priority for the session policy.

For more information about LDAP group membership attributes, see the following:

- How LDAP Group Extraction Works from the User Object Directly
- How LDAP Group Extraction Works from the Group Object Indirectly

How LDAP Group Extraction Works from the User Object Directly

January 8, 2024

LDAP servers that evaluate group memberships from group objects support NetScaler Gateway authorization.

Some LDAP servers enable user objects to contain information about groups to which the objects belong, such as Active Directory (by using the memberOf attribute) or IBM eDirectory (by using the groupMembership attribute). A user's group membership can be attributes from the user object, such as IBM Directory Server (by using ibm-allGroups) or Sun ONE directory server (by using nsRole). Both of these types of LDAP servers support NetScaler Gateway group extraction.

For example, in IBM Directory Server, all group memberships, including the static, dynamic, and nested groups, can be returned by using the ibm-allGroups attribute. In Sun ONE, all roles, including managed, filtered, and nested, are calculated by using the nsRole attribute.

How LDAP Group Extraction Works from the Group Object Indirectly

January 8, 2024

LDAP servers that evaluate group memberships from group objects indirectly are not compatible with NetScaler Gateway authorization.

Some LDAP servers, such as Lotus Domino, enable group objects only to contain information about users. These LDAP servers do not enable the user object to contain information about groups and thus is not compatible with NetScaler Gateway group extraction. For this LDAP server type, group membership searches are performed by locating the user in the member list of groups.

LDAP Authorization Group Attribute Fields

January 8, 2024

The following table contains examples of LDAP group attribute fields:

LDAP servers	LDAP attribute
Microsoft Active Directory Server	memberOf
Novell eDirectory	groupMembership
IBM Directory Server	ibm-allGroups
Sun ONE directory (formerly iPlanet)	nsRole

To configure LDAP authorization

January 8, 2024

You configure LDAP authorization in the authentication policy by setting the group attribute name and the subattribute.

1. In the configuration utility, on the Configuration tab, expand NetScaler Gateway > Policies > Authentication.
2. Under Authentication, click an authentication type.
3. In the details pane, click Add.
4. In Name, type a name for the policy.
5. Next to Server, click New.
6. In Name, type the name of the server.
7. Under Server, type the IP address and port of the LDAP server.
8. In Group Attribute, type memberOf.
9. In Sub attribute Name, type CN and then click Create.
10. In the Create Authentication Policy dialog box, next to Named Expressions, select the expression, click Add Expression, click Create and then click Close.

Configuring LDAP Nested Group Extraction

January 8, 2024

NetScaler Gateway can query LDAP groups and extract group and user information from ancestor groups that you configure on the authentication server. For example, you created group1 and within that group, you created group2 and group3. If the user belongs to group3, NetScaler Gateway extracts information from all the nested ancestor groups (group2, group1) up to the specified level.

You can use an authentication policy to configure LDAP nested group extraction. When the query is run, NetScaler Gateway searches the groups until it reaches the maximum nesting level or until it searches all available groups.

To configure LDAP nested group extraction

1. In the configuration utility, in the navigation pane, expand **NetScaler Gateway > Policies > Authentication/Authorization > Authentication > Authentication** and then click **LDAP**.
2. In the details pane, on the Policies tab, click **Add**.
3. In Name, type a name for the policy.
4. Next to Server, click **New**.
5. In Name, type the name of the server.
6. Configure the settings for the LDAP server.
7. Expand **Nested Group Extraction**, and then click **Enable**.
8. In **Maximum Nesting Level**, type the number of levels that NetScaler Gateway checks.
9. In **Group Name Identifier**, type the LDAP attribute name that uniquely identifies a group name on the LDAP server, such as `sAMAccountName`.
10. In **Group Search Attribute**, type the LDAP attribute name that is to be obtained in the search response to determine the parent groups of any group. For example, `memberOf`.
11. In **Group Search Sub-Attribute**, type the LDAP subattribute name that is to be searched for as part of the Group Search Attribute to determine the parent groups of any group. For example, type CN.
12. In **Group Search Filter**, type the query string. For example, the filter can be `&(samaccountname=test)(objectClass=\*)`.
13. Click **Create**, and then click **Close**.
14. In the Create Authentication Policy dialog box, next to Named Expressions, select the expression, click **Add Expression**, click **Create**, and then click **Close**.

Configuring LDAP Group Extraction for Multiple Domains

January 8, 2024

If you have multiple domains for authentication and are using StoreFront or the Web Interface, you can configure NetScaler Gateway to use group extraction to send the correct domain name to the Web Interface.

In Active Directory, you need to create a group for each domain in your network. After you create the group, you add users that belong to the group and specified domain. After the groups are configured in Active Directory, you configure LDAP group extraction for multiple domains on NetScaler Gateway.

To configure NetScaler Gateway for group extraction for multiple domains, you need to create the same number of session and authentication policies as the number of domains in your network. For example, you have two domains, named `Sampa` and Child. Each domain receives one session policy and one authentication policy.

After creating the policies, you create groups on NetScaler Gateway, and you bind the session policies to the group. Then, you bind the authentication policies to a virtual server.

If you deploy StoreFront in multiple domains, there must be a trust relationship between domains.

If you deploy Citrix Endpoint Management or the Web Interface in multiple domains, the domains do not need to trust each other.

Creating Session Policies for Group Extraction

January 8, 2024

The first step when you create session policies for group extraction is to create two session profiles and set the following parameters:

- Enable ICA Proxy.
- Add the Web Interface Web address.
- Add the Windows domain.
- Add the profile to a session policy and set the expression to true.

To create the session profiles for group extraction

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway > Policies** and then click **Session**.

2. In the details pane, click the **Profiles** tab and then click **Add**.
3. In **Name**, type a name for the profile. For example, type `Sampa`.
4. On the **Published Applications** tab, do the following:

   a) Next to **ICA Proxy**, click **Override Global** and then select **ON**.
   b) Next to **Web Interface Address**, click **Override Global** and then type the Web address of the Web Interface.
   c) Next to **Single Sign-On Domain**, click **Override Global**, type the name of the Windows domain and then click **Create**.

5. In **Name**, clear the name of the first domain and type the name of the second domain, such as Child.
6. Next to **Single Sign-On Domain**, clear the name of the first Windows domain and type the name of the second domain, click **Create,** and then click **Close**.

After you create the session profiles, you create two session policies. Each session policy uses one of the profiles.

To create a session policy

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway > Policies** and then click **Session**.
2. In the details pane, on the **Policies** tab, click **Add**.
3. In **Name**, type a name for the policy.
4. In **Request Profile**, select the profile for the first domain.
5. Next to **Named Expressions**, click **General**, select **True value**, click **Add Expression,** and then click **Create**.
6. In **Name**, change the name to the second domain.
7. In **Request Profile**, select the profile for the second domain, click **Create,** and then click **Close**.

Creating LDAP Authentication Policies for Multiple Domains

January 8, 2024

After you create session policies on NetScaler Gateway, you create LDAP authentication policies that are almost identical. When configuring the authentication policy, the important field is Search Filter. In this field, you must type the name of the group you created in the Active Directory.

Create the authentication profiles first and then create the authentication policy.

To create authentication profiles for multiple domain group extractions

1. In the configuration utility, on the Configuration tab, expand Citrix **Gateway > Policies > Authentication**.
2. In the navigation pane, click **LDAP**.
3. In the details pane, click the **Servers** tab and then click **Add**.
4. In **Name**, type the name of the first domain, such as `Sampa`.
5. Configure the settings for the LDAP server, and then click **Create**.
6. Repeat Steps 3, 4, and 5 to configure the authentication profile of the second domain, and then click **Close**.

After you create and save the profiles, create the authentication policies.

To create authentication policies for multiple domain group extractions

1. In the configuration utility, on the Configuration tab, expand **NetScaler Gateway > Policies > Authentication**.
2. In the details pane, click the **Policies** tab and then click **Add**.
3. In **Name**, type the name of the first domain.
4. In **Authentication Type**, select **LDAP**.
5. In **Server**, select the authentication profile for the first domain.
6. Next to **Named Expressions**, click **General**, select **True value**, click **Add Expression,** and then click **Create**.
7. In Name, type the name of the second domain.
8. In **Server**, select the authentication profile for the second domain, click **Create,** and then click **Close**.

Creating Groups and Binding Policies for LDAP Group Extraction for Multiple Domains

January 8, 2024

After you create authentication policies, you create groups on NetScaler Gateway. After you create the groups, you bind the authentication policy to a virtual server.

To create groups on NetScaler Gateway

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, expand **NetScaler Gateway > User Administration** and then click **AAA Groups**.
2. In the details pane, click **Add**.
3. In **Group Name**, type the name of the first Active Directory group.
   Important: When creating groups on NetScaler Gateway for group extraction from multiple domains, group names must be the same as the groups you defined in the Active Directory. Group names are also case-sensitive and the case must match the case you entered in the Active Directory.
4. On the **Policies** tab, click **Session**, and then click **Insert Policy**.
5. Under **Policy Name**, double-click the policy, and then click **Create**.

To bind the authentication policies to a virtual server

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, expand **NetScaler Gateway** and then click **Virtual Servers**.
2. In the details pane, click a virtual server, and then click **Open**.
3. On the Authentication tab, click **Primary**, under **Policy Name**, double-click **Insert Policy**, and then select the first authentication policy.
4. Under **Policy Name**, click **Insert Policy**, double-click the second authentication policy, and then click **OK**.

14-day password expiry notification for LDAP authentication

January 8, 2024

The NetScaler Gateway appliance supports 14-day password expiry notification for LDAP based authentication. By using this feature, administrators can notify the end users about the password expiry threshold time in days. For more details, see 14-day password expiry notification for LDAP authentication.

Configuring Client Certificate Authentication

January 8, 2024

Users logging on to a NetScaler Gateway virtual server can also be authenticated based on the client certificate attributes presented to the virtual server. Client certificate authentication can also be used with other authentication types, such as LDAP or RADIUS, to provide two-factor authentication.

To authenticate users based on the client-side certificate attributes, client authentication must be enabled on the virtual server and the client certificate must be requested. You must bind a root certificate to the virtual server on NetScaler Gateway.

When users log on to the NetScaler Gateway virtual server, after authentication, the user name information is extracted from the specified field of the certificate. Typically, this field is Subject:CN. If the user name is extracted successfully, the user is then authenticated. The authentication fails in the following cases.

- If the user does not provide a valid certificate during the Secure Sockets Layer (SSL) handshake.
- The user name extraction fails, authentication fails.

You can authenticate users based on the client certificate by setting the default authentication type to use the client certificate. You can also create a certificate action that defines what is to be done during the authentication based on a client SSL certificate.

To configure the client certificate as the default authentication type by using the GUI

1. Go to **Configuration > NetScaler Gateway,** and then click **Global Settings**.
2. In the details pane, under **Authentication Settings**, click **Change authentication CERT settings**.
3. Select **ON** to enable two factor authentication using the certificate as per your requirement.
4. In **User Name Field**, select the type of certificate field that holds the user names.
5. In **Group Name Field**, select the type of the certificate field that holds the group name.
6. In **Default Authorization Group**, type the name of the default group, and then click **OK**.

Extracting the User Name from the Client Certificate

If client certificate authentication is enabled on NetScaler Gateway, users are authenticated based on certain attributes of the client certificate. After authentication is successful, the user name or the user and group name of the user are extracted from the certificate. Also, the policies specified for that user are applied.

Configuring and Binding a Client Certificate Authentication Policy

January 8, 2024

You can create a client certificate authentication policy and bind it to a virtual server. You can use the policy to restrict access to specific groups or users. This policy takes precedence over the global policy.

To configure a client certificate authentication policy:

1. In the configuration utility, on the Configuration tab, expand **NetScaler Gateway > Policies > Authentication**.
2. In the navigation pane, under **Authentication**, click **CERT**.
3. In the details pane, click **Add**.
4. In **Name** field, type a name for the policy.
5. Next to **Server**, click **New**.
6. In **Name**, type a name for the profile.
7. Next to **Two Factor**, select **OFF**.
8. In **User Name** field and **Group Name** field, select the values and then click &**Create**.
   Note: If you previously configured client certificates as the default authentication type, use the same names that you used for the policy. If you completed the
   User Name field and
   Group Name field for the default authentication type, use the same values for the profile.
9. In the **Create Authentication Policy** dialog box, next to **Named Expressions**, select the expression, click **Add Expression**, click **Create** and then click **Close**.

To bind a client certificate policy to a virtual server:

After you configure the client certificate authentication policy, you can bind it to a virtual server.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway** and then click **Virtual Servers**.
2. In the details pane, click a virtual server and then click **Open**.
3. In the configure **NetScaler Gateway Virtual Server** dialog box, click the **Authentication** tab.
4. Click **Primary** or **Secondary**.
5. Under **Details**, click **Insert Policy**.
6. In **Policy Name**, select the policy and then click **OK**.

To configure a virtual server to request the client certificate:

When you want to use a client certificate for authentication, you must configure the virtual server so that client certificates are requested during the SSL handshake.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway** and then click **Virtual Servers**.
2. In the details pane, click a **Virtual Server** and then click **Open**.
3. On the **Certificates** tab, click **SSL Parameter**.
4. Under **Others**, click **Client Authentication**.

5. In **Client Certificate**, select **Optional** or **Mandatory** and then click OK twice. Select **Optional** if you want to allow other authentication types on the same virtual server and do not require the use of client certificates.

> **Note**
>
> - For more information about Callback URL, see Import a NetScaler Gateway.
> - For more information about certificates, see Install, link, and update certificates.

Configuring Two-Factor Client Certificate Authentication

January 8, 2024

You can configure a client certificate to authenticate users first and then require users to log on with a secondary authentication type, such as LDAP or RADIUS. In this scenario, the client certificate authenticates users first. Then, a logon page appears where they can enter their user name and password. When the Secure Sockets Layer (SSL) handshake is complete, the logon sequence can take one of the following two paths:

- Neither the user name nor the group is extracted from the certificate. The logon page appears to the user with a prompt to enter valid logon credentials. NetScaler Gateway authenticates the user credentials as in the case of normal password authentication.
- The user name and group name are extracted from the client certificate. If only the user name is extracted, a logon page appears to the user in which the logon name is present and the user cannot modify the name. Only the password field is blank.

Group information that NetScaler Gateway extracts during the second round of authentication is appended to the group information, if any, that NetScaler Gateway extracted from the certificate.

Configuring Smart Card Authentication

January 8, 2024

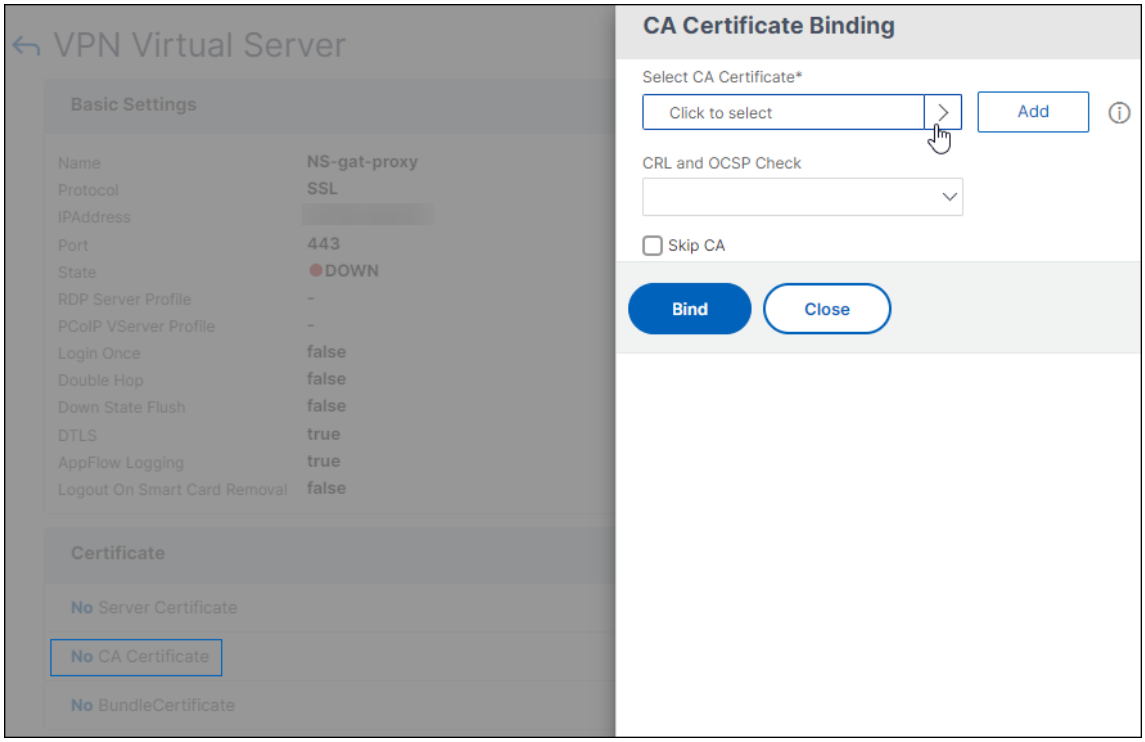
You can configure NetScaler Gateway to use a cryptographic smart card to authenticate users.

To configure a smart card with NetScaler Gateway, you need to do the following:

- Create a certificate authentication policy. For more information, see Configuring Client Certificate Authentication.

- Bind the authentication policy to a virtual server.
- Add the root certificate of the Certificate Authority (CA) issuing the client certificates to NetScaler Gateway. For more information, see To install a root certificate on NetScaler Gateway.

  Important: When you add the root certificate to the virtual server for smart card authentication, you must select the certificate from the **Select CA Certificate** list.



After you create the client certificate, you can write the certificate, known as flash, onto the smart card. When you complete that step, you can test the smart card.

If you configure the Web Interface for smart card passthrough authentication, if either of the following conditions exist, single sign-on to the Web Interface fails:

- If you set the domain on the **Published Applications** tab as `mydomain`.com instead `mydomain`.
- If you do not set the domain name on the **Published Applications** tab and if you run the command `wi-sso-split-upn` setting the value to 1. In this instance, the UserPrincipalName contains the domain name "`mydomain`.com."

You can use smart card authentication to streamline the logon process for your users while also enhancing the security of user access to your infrastructure. Access to the internal corporate network is protected by certificate-based two-factor authentication using the public key infrastructure. Private keys are protected by hardware controls and never leave the smart card. Your users get the con-

venience of accessing their desktops and applications from a range of corporate devices using their smart cards and PINs.

You can use smart cards for user authentication through StoreFront to desktops and applications provided by Citrix Virtual Apps and Desktops. Smart card users logging on to StoreFront can also access applications provided by NetScaler Endpoint Management. However, users must authenticate again to access Endpoint Management web applications that use client certificate authentication.

For more information, see Configure smart card authentication in the StoreFront documentation.

Configuring Smart Card Authentication with Secure ICA Connections

Users who log on and establish a secure ICA connection by using a smart card with single sign-on configured on NetScaler Gateway might receive prompts for their personal identification number (PIN) twice.

- When logging on and when trying to start a published resource. This situation occurs if the web browser and the Citrix Workspace app are using the same virtual server that is configured to use client certificates.
- Citrix Workspace app does not share a process or a Secure Sockets Layer (SSL) connection with the web browser. Therefore, when the ICA connection completes the SSL handshake with NetScaler Gateway, the client certificate is required a second time.

To prevent users from receiving the second PIN prompt, you have to change two settings:

- Client authentication on the VPN Virtual Server must be disabled.
- SSL renegotiation must be enabled.

After you configure the virtual server, bind one or more STA servers to the virtual server, as described in Configuring NetScaler Gateway Settings in Web Interface 5.3.

You might also want to test smart-card authentication.

To disable client authentication:

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click Virtual Servers.
2. Select the relevant virtual server in the main details pane, and then click Edit.
3. In the Advanced options pane, click SSL Parameters.
4. Clear the Client Authentication check box.
5. Click Done.

To enable SSL renegotiation:

1. Using the configuration utility, from the Configuration tab, navigate to Traffic Management, and then clickSSL.

2. In the main panel, click Change advanced SSL settings.
3. From the Deny SSL Renegotiation menu, select NO.

To test smart card authentication:

1. Connect the smart card to the user device.
2. Open your web browser and log on to NetScaler Gateway.

Configuring RADIUS Authentication

January 8, 2024

You can configure NetScaler Gateway to authenticate user access with one or more RADIUS servers. If you are using RSA SecurID, SafeWord, or Gemalto Protiva products, each of these products is configured by using a RADIUS server.

Your configuration might require using a network access server IP address (NAS IP) or a network access server identifier (NAS ID). When configuring NetScaler Gateway to use a RADIUS authentication server, use the following guidelines:

- If you enable use of the NAS IP, the appliance sends its configured IP address to the RADIUS server, rather than the source IP address used in establishing the RADIUS connection.
- If you configure the NAS ID, the appliance sends the identifier to the RADIUS server. If you do not configure the NAS ID, the appliance sends its host name to the RADIUS server.
- When you enable the NAS IP, the appliance ignores any NAS ID that is configured using the NAS IP to communicate with the RADIUS server.

Configuring Gemalto Protiva

Protiva is a strong authentication platform that Gemalto developed to use the strengths of Gemalto's smart card authentication. With Protiva, users log on with a user name, password, and a one-time password that the Protiva device generates. Similar to RSA SecurID, the authentication request is sent to the Protiva authentication server and the server either validates or rejects the password. To configure Gemalto Protiva to be compatible with NetScaler Gateway, use the following guidelines:

- Install the Protiva server.
- Install the Protiva SAS Agent Software, that extends the Internet Authentication Server (IAS), on a Microsoft IAS RADIUS server. Make sure you note the IP address and port number of the IAS server.
- Configure a RADIUS authentication profile on NetScaler Gateway and enter the settings of the Protiva server.

Configuring SafeWord

The SafeWord product line provides secure authentication using a token-based passcode. After the user enters the passcode, SafeWord immediately invalidates the passcode and it cannot be used again. When you configure the SafeWord server, you need the following information:

- The IP address of NetScaler Gateway. The IP address must be the same IP address that you configured in the RADIUS server client configuration. NetScaler Gateway uses the internal IP address to communicate with the RADIUS server. When you configure the shared secret, use the internal IP address. If you configure two appliances for high availability, use the virtual internal IP address.
- A shared secret.
- The IP address and port of the SafeWord server. The default port number is 1812.

To configure RADIUS authentication

January 8, 2024

1. In the configuration utility, on the Configuration tab, expand NetScaler Gateway > Policies > Authentication.
2. Click RADIUS, and then in the details pane, on the Policies tab, click Add .
3. In the Create Authentication Policy dialog box, in Name, type a name for the policy.
4. In Name, type a name for the policy.
5. Next to Server, click New.
6. In the Create Authentication Policy dialog box, in Name, type a name for the server.
7. Under Server, in IP Address, type the IP address of the RADIUS server.
8. In Port, type the port. The default is 1812.
9. Under Details, in Secret Key and Confirm Secret Key, type the RADIUS server secret.
10. In NAS ID, type the identifier number and then click Create.
11. In the Create Authentication Policy dialog box, next to Named Expressions, select the expression, click Add Expression, click Create and then click Close.

Choosing RADIUS Authentication Protocols

January 8, 2024

NetScaler Gateway supports implementations of RADIUS that are configured to use several protocols for user authentication, including:

- Password Authentication Protocol (PAP)
- Challenge-Handshake Authentication Protocol (CHAP)
- Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP Version 1 and Version 2)

If your deployment of the NetScaler Gateway is configured to use RADIUS authentication and your RADIUS server is configured to use PAP, you can strengthen user authentication by assigning a strong shared secret to the RADIUS server. Strong RADIUS shared secrets consist of random sequences of uppercase and lowercase letters, numbers, and punctuation and are at least 22 characters long. If possible, use a random character generation program to determine RADIUS shared secrets.

To further protect RADIUS traffic, assign a different shared secret to each NetScaler Gateway appliance or virtual server. When you define clients on the RADIUS server, you can also assign a separate shared secret to each client. If you do this, you must configure separately each NetScaler Gateway policy that uses RADIUS authentication.

When you create a RADIUS policy, you configure shared secrets on NetScaler Gateway as part of the policy.

Configuring IP Address Extraction

January 8, 2024

You can configure NetScaler Gateway to extract the IP address from a RADIUS server. When a user authenticates with the RADIUS server, the server returns a framed IP address that is assigned to the user. The framed IP address is also called RADIUS Attribute 8 Framed-IP-Address in Access Requests.

The following are components for IP address extraction:

- Allows a remote RADIUS server to supply an IP address from the internal network for a user logged on to NetScaler Gateway.
- Allows configuration for any RADIUS attribute using the type **ipaddress**, including attributes that are vendor encoded.

When configuring the RADIUS server for IP address extraction, you configure the vendor identifier and the attribute type. The vendor ID and attributes are used to make the association between the RADIUS client and the RADIUS server.

- The vendor identifier (ID) enables the RADIUS server to assign an IP address to the client from a pool of IP addresses that are configured on the RADIUS server. The vendor ID is the attribute in the RADIUS response that provides the IP address of the internal network. A value of zero indicates that the attribute is not vendor encoded

- The attribute type is the remote IP address attribute in a RADIUS response. The minimum value is 1 and the maximum value is 255.

A common configuration is to extract the RADIUS attribute **framed IP address**. The vendor ID is set to 0 or is not specified. The attribute type is set to 8.

To configure IP address extraction from a RADIUS server by using the GUI:

1. Navigate to **NetScaler Gateway > Policies > Authentication** and the click **RADIUS**.
2. In the **Details** pane, on the **Policies** tab, select a RADIUS policy, and then click **Open**.
3. In the **Configure Authentication Policy** dialog box, next to Server, click **Modify**.
4. Under **Details**, in **Group Vendor Identifier**, type the value.
5. In **Group Attribute Type**, type the value, and then click **OK** twice.

Configuring RADIUS Group Extraction

January 8, 2024

You can configure RADIUS authorization by using a method called group extraction. Configuring group extraction allows you to administer users on your RADIUS server instead of adding them to NetScaler Gateway.

You configure RADIUS authorization by using an authentication policy and configuring the group vendor identifier (ID), the group attribute type, the group prefix, and a group separator. When you configure the policy, you add an expression, and then bind the policy either globally or to a virtual server.

Configuring RADIUS on Windows Server 2003

If you are using Microsoft Internet Authentication Service (IAS) for RADIUS authorization on Windows Server 2003, during configuration of NetScaler Gateway, you need to provide the following information:

- Vendor ID is the vendor-specific code that you entered in IAS.
- Type is the vendor-assigned attribute number.
- Attribute name is the type of attribute name that you defined in IAS. The default name is CTX-SUserGroups=

If IAS is not installed on the RADIUS server, you can install it from Add or Remove Programs in Control Panel. For more information, see the Windows online Help.

To configure IAS, use the Microsoft Management Console (MMC) and install the snap-in for IAS. Follow the wizard, making sure you select the following settings:

- Select local computer.
- Select Remote Access Policies and create a custom policy.
- Select Windows-Groups for the policy.
- Select one of the following protocols:
  - Microsoft Challenge-Handshake Authentication Protocol version 2 (MS-CHAP v2)
  - Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP)
  - Challenge-Handshake Authentication Protocol (CHAP)
  - Unencrypted authentication (PAP, SPAP)
- Select the Vendor-Specific Attribute.

  The Vendor-Specific Attribute needs to match the users whom you defined in the group on the server with the users on NetScaler Gateway. To meet this requirement, you send the Vendor-Specific Attributes to NetScaler Gateway. Make sure you select RADIUS=Standard.
- The RADIUS default is 0. Use this number for the vendor code.
- The vendor-assigned attribute number is 0.

  This is the assigned number for the User Group attribute. The attribute is in string format.
- Select String for the Attribute format.

  The Attribute value requires the attribute name and the groups.

  For the Access Gateway, the attribute value is CTXSUserGroups=groupname. If two groups are defined, such as sales and finance, the attribute value is CTXSUserGroups=sales;finance. Separate each group with a semicolon.
- Remove all other entries in the Edit Dial-in Profile dialog box, leaving the one that says Vendor-Specific.

After you configure the Remote Access Policy in IAS, you configure RADIUS authentication and authorization on NetScaler Gateway.

When configuring RADIUS authentication, use the settings that you configured on the IAS server.

Configuring RADIUS for Authentication on Windows Server 2008

On Windows Server 2008, you configure RADIUS authentication and authorization by using the Network Policy Server (NPS), which replaces Internet Authentication Service (IAS). You can use Server Manager and add NPS as a role to install NPS.

When you install NPS, select the Network Policy Service. After installation, you can configure RADIUS settings for your network by starting the NPS from Administrative Services on the Start menu. When you open the NPS, you add NetScaler Gateway as a RADIUS client and then configure server groups.

When you configure the RADIUS client, make sure you select the following settings:

- For the vendor name, select RADIUS Standard.
- Make note of the shared secret because you will need to configure the same shared secret on NetScaler Gateway.

For the RADIUS groups, you need the IP address or host name of the RADIUS server. Do not change the default settings.

After you configure the RADIUS client and groups, you then configure settings in the following two policies:

- Connection Request Policies where you configure the settings for the NetScaler Gateway connection including the type of network server, the conditions for the network policy, and the settings for the policy.
- Network Policies where you configure the Extensible Authentication Protocol (EAP) authentication and the vendor-specific attributes.

When you configure the connection request policy, select Unspecified for the type of network server. You then configure your condition by selecting NAS Port Type as the condition and Virtual (VPN) as the value.

When you configure a network policy, you need to configure the following settings:

- Select Remote Access Server (VPN Dial-up) as the type of network access server.
- Select Encrypted Authentication (CHAP) and Unencrypted Authentication (PAP and SPAP) for the EAP.
- Select RADIUS Standard for the Vendor-Specific Attribute.

  The default attribute number is 26. This attribute is used for RADIUS authorization.

  NetScaler Gateway needs the vendor-specific attribute to match the users defined in the group on the server with those on NetScaler Gateway. This is done by sending the vendor-specific attributes to the NetScaler Gateway.
- Select String for the attribute format.

  The Attribute value requires the attribute name and the groups.

  For NetScaler Gateway, the attribute value is CTXSUserGroups= groupname. If two groups are defined, such as sales and finance, the attribute value is CTXSUserGroups=sales;finance. Separate each group with a semicolon.
- The separator is that which you used on the NPS to separate groups, such as a semicolon, a colon, a space, or a period.

When you are finished configuring the remote access policy in IAS, you can configure RADIUS authentication and authorization on NetScaler Gateway.

To configure RADIUS authorization

January 8, 2024

1. In the configuration utility, on the Configuration tab, expand NetScaler Gateway > Policies > Authentication.
2. Click RADIUS.
3. In the Policies tab, click Add.
4. In Name, type a name for the policy.
5. Below the Server* click +
6. In Name, type the name of the RADIUS server.
7. Under Server, type the IP address and port of the RADIUS server.
8. Under Details, enter the values for Group Vendor Identifier and Group Attribute Type.
9. In Password Encoding, select the authentication protocol and then click Create.
10. In the Create Authentication Policy dialog box, next to Named Expressions, select the expression, click Add Expression, click Create and then click Close.

Configuring RADIUS user accounting

January 8, 2024

NetScaler Gateway can send user-session start and stop messages to your RADIUS accounting server. The messages, which are sent for each user session, include a subset of the attributes defined in RFC2866. Table 1 lists the supported attributes and the types of RADIUS accounting messages (RAD_START and RAD_STOP) in which they are sent. Table 2 lists the predefined values that can be assigned to the `Acct-Terminate-Cause` attribute, and the corresponding NetScaler Gateway events.

Table 1. Supported RADIUS Attributes

Attribute	Meaning	RAD_START	RAD_STOP
User-Name	Name of user associated with the session.	X	X
Session-Id	The NetScaler session ID.	X	X
Acct-Session-Time	Session duration seconds.		X

Attribute	Meaning	RAD_START	RAD_STOP
Acct-Terminate-Cause	Reason for account termination.		X

Table 2. RADIUS Termination Causes

NetScaler Logout Method	RADIUS Termination Cause
LOGOUT_SESSN_TIMEDOUT	RAD_TERM_SESSION_TIMEOUT
LOGOUT_SESSN_INITIATEDBYUSER	RAD_TERM_USER_REQUEST
LOGOUT_SESSN_KILLEDBYADMIN	RAD_TERM_ADMIN_RESET
LOGOUT_SESSN_TLOGIN	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_MAXLICRCHD	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_CLISECCHK_FAILED	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_PREAUTH_CHANGED	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_COOKIE_MISMATCH	RAD_TERM_NAS_REQUEST
LOGOUT_SESSS_DHT	RAD_TERM_NAS_REQUEST
LOGOUT_SESSS_2FACTOR_FAIL	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_ICALIC	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_INTERNALERR	RAD_TERM_NAS_ERROR
Other	RAD_TERM_NAS_ERROR

Configuration of RADIUS user accounting requires the creation of a pair of policies. The first policy is a RADIUS authentication policy that designates a RADIUS server to which to send accounting messages. The second is a session policy that uses the RADIUS accounting policy as its action.

To configure RADIUS user accounting, you must:

1. Create a RADIUS policy to define the RADIUS accounting server. The accounting server can be the same server that you use for RADIUS authentication.
2. Create a session policy, using the RADIUS policy as an action that specifies the RADIUS user accounting server.
3. Bind the session policy either globally, so that it applies to all traffic, or to a NetScaler Gateway virtual server, so that it applies only to traffic flowing through that virtual server.

To create a RADIUS policy

1. In the configuration utility, in the navigation pane, expand the NetScaler Gateway node, and then Policies.
2. Expand Authentication and select RADIUS.
3. In the details pane, on the Policies tab, click Add.
4. Enter a name for the policy.
5. Select a server from the Server menu, or click the + icon and follow the prompts to add a new RADIUS server.
6. In the Expression pane, from the Saved Policy Expressions menu, select ns_true.
7. Click Create.

To create a session policy

After configuring a RADIUS policy that specifies the RADIUS accounting server, create a session policy that applies this accounting server in an action, as follows:

1. In the configuration utility, in the navigation pane, expand the NetScaler Gateway node, and then Policies.
2. Select Session.
3. In the main details pane, select Add.
4. Enter a name for the policy.
5. In the Action menu, click the + icon to add a new session action.
6. Enter a name for the session action.
7. Click the Client Experience tab.
8. In the Accounting Policy menu, select the RADIUS policy that you created earlier.
9. Click Create.
10. In the Expression pane, from the Saved Policy Expressions menu, select ns_true.
11. Click Create.

To bind the session policy globally

1. In the configuration utility, in the navigation pane, expand the NetScaler Gateway node, and then Policies.
2. Select Session.
3. From the Action menu in the main details pane, select Global Bindings.
4. Click Bind.
5. In the Policies pane, select the session policy that you created earlier, and then click Insert.
6. In the Policies listings, click the Priority entry for the session policy and enter a value from 0 to 64000.

7. Click OK.

To bind the session policy to a NetScaler Gateway virtual server

1. In the configuration utility, in the navigation pane, expand the NetScaler Gateway node, and then select Virtual Servers.
2. In the main details pane, select a virtual server, and then click Edit.
3. In the Policies pane, click the + icon to select a policy.
4. From the Choose Policy menu, select Session, and make sure that Request is selected in the Choose Type menu.
5. Click Continue.
6. Click Bind.
7. In the Policies pane, select the session policy that you created earlier, and then click Insert.
8. Click OK.

Configuring SAML Authentication

January 8, 2024

The Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization between Identity Providers (IdP) and Service Providers. NetScaler Gateway supports SAML authentication.

When you configure SAML authentication, you create the following settings:

- IdP Certificate Name. This is the public key that corresponds to the private key at the IdP.
- Redirect URL. This is the URL of the authentication IdP. Users who are not authenticated are redirected to this URL.
- User Field. You can use this field to extract the user name if the IdP sends the user name in a different format than the NameIdentifier tag of the Subject tag. This is an optional setting.
- Signing Certificate Name. This is the private key of the NetScaler Gateway server that is used to sign the authentication request to the IdP. If you do not configure a certificate name, the assertion is sent unsigned or the authentication request is rejected.
- SAML Issuer name. This value is used when the authentication request is sent. There must be a unique name in the issuer field to signify the authority from which the assertion is sent. This is an optional field.
- Default authentication group. This is the group on the authentication server from which users are authenticated.
- Two Factor. This setting enables or disables two-factor authentication.

- Reject unsigned assertion. If enabled, NetScaler Gateway rejects user authentication if the signing certificate name is not configured.

NetScaler Gateway supports HTTP POST-binding. In this binding, the sending party replies to the user with a 200 OK that contains a form-auto post with required information. Specifically, the default form must contain two hidden fields called `SAMLRequest` and `SAMLResponse`, depending on whether the form is a request or response. The form also includes RelayState, which is a state or information used by the sending party to send arbitrary information that is not processed by a relying party. The relying party sends the information back so that when the sending party gets the assertion along with RelayState, the sending party knows what to do next. It is recommended that you encrypt or obfuscate the RelayState.

> **Note**
>
> - When NetScaler Gateway is used as an IdP to Citrix Cloud, you need not configure the **RelayState** rule on NetScaler Gateway.
> - In case of IdP chaining, it is sufficient to configure the **RelayState** rule only on the first SAML policy. In this context, IdP chaining is a scenario where a configured SAML action refers to an authentication virtual server IdP containing another SAML action.

Configuring Active Directory Federation Services 2.0

You can configure Active Directory Federation Services (AD FS) 2.0 on any Windows Server 2008 or Windows Server 2012 computer that you use in a federated server role. When you configure the ADFS server to be compatible with NetScaler Gateway, you need configure the following parameters by using the Relying Party Trust Wizard in Windows Server 2008 or Windows Server 2012.

Windows Server 2008 Parameters:

- Relying Party Trust. You provide the NetScaler Gateway metadata file location, such as `https://vserver.fqdn.com/ns.metadata.xml`, where vserver.fqdn.com is the fully qualified domain name (FQDN) of the NetScaler Gateway virtual server. You can find the FQDN on the server certificate bound to the virtual server.
- Authorization Rules. You can allow or deny users access to the relying party.

Windows Server 2012 Parameters:

- Relying Party Trust. You provide the NetScaler Gateway metadata file location, such as `https://vserver.fqdn.com/ns.metadata.xml`, where vserver.fqdn.com is the fully qualified domain name (FQDN) of the NetScaler Gateway virtual server. You can find the FQDN on the server certificate bound to the virtual server.
- AD FS Profile. Select the AD FS profile.

- Certificate. NetScaler Gateway does not support encryption. You do not need to select a certificate.
- Enable support for the SAML 2.0 WebSSO protocol. This enables support for SAML 2.0 SSO. You provide the NetScaler Gateway virtual server URL, such as `https:netScaler.virtualServerName.com/cgi/samlauth`.

  This URL is the Assertion Consumer Service URL on the NetScaler Gateway appliance. This is a constant parameter and NetScaler Gateway expects a SAML response on this URL.
- Relying party trust identifier. Enter the name NetScaler Gateway. This is a URL that identifies relying parties, such as `https://netscalerGateway.virtualServerName.com/adfs/services/trust`.
- Authorization Rules. You can allow or deny users access to the relying party.
- Configure claim rules. You can configure the values for LDAP attributes by using the Issuance Transform Rules and use the template Send LDAP Attributes as Claims. You then configure LDAP settings that include:
  - Email addresses
  - sAMAccountName
  - User Principal Name (UPN)
  - MemberOf
- Certificate Signature. You can specify the signature verification certificates by selecting the Properties of a Relaying Party and then adding the certificate.

  If the signing certificate is less than 2048 bits, a warning message appears. You can ignore the warning to proceed. If you are configuring a test deployment, disable the Certificate Revocation List (CRL) on the Relaying Party. If you do not disable the check, AD FS tries the CRL to validate the certificate.

  You can disable the CRL by running the following command: Set-ADFWRelayingPartyTrust - SigningCertficateRevocatonCheck None-TargetName NetScaler

After you configure the settings, verify the relying party data before you complete the Relaying Party Trust Wizard. You check the NetScaler Gateway virtual server certificate with the endpoint URL, such as `https://vserver.fqdn.com/cgi/samlauth`.

After you finish configuring settings in the Relaying Party Trust Wizard, select the configured trust and then edit the properties. Perform the following:

- Set the secure hash algorithm to SHA-1.

  Note: NetScaler supports SHA-1 only.
- Delete the encryption certificate. Encrypted assertions are not supported.

- Edit the claim rules, including the following:
  - Select Transform Rule
  - Add Claim Rule
  - Select Claim Rule Template: Send LDAP attributes as claims
  - Give a Name
  - Select Attribute Store: Active Directory
  - Select LDAP attribute: <Active Directory parameters>
  - Select Out Going Claim Rule as “Name ID”

  Note: Attribute Name XML tags are not supported.

- Configure the Logout URL for Single Sign-off. The claim rule is Send logout URL. The custom rule must be the following:

  ```
  pre codeblock => issue(Type = "logoutURL", Value = "https://<adfs
  .fqdn.com>/adfs/ls/", Properties["http://schemas.xmlsoap.org/ws
  /2005/05/identity/claimproperties/attributename"] = "urn:oasis:
  names:tc:SAML:2.0:attrname-format:unspecified");
  ```

After you configure AD FS settings, download the AD FS signing certificate and then create a certificate key on NetScaler Gateway. You can then configure SAML authentication on NetScaler Gateway by using the certificate and key.

Configuring SAML Two-Factor Authentication

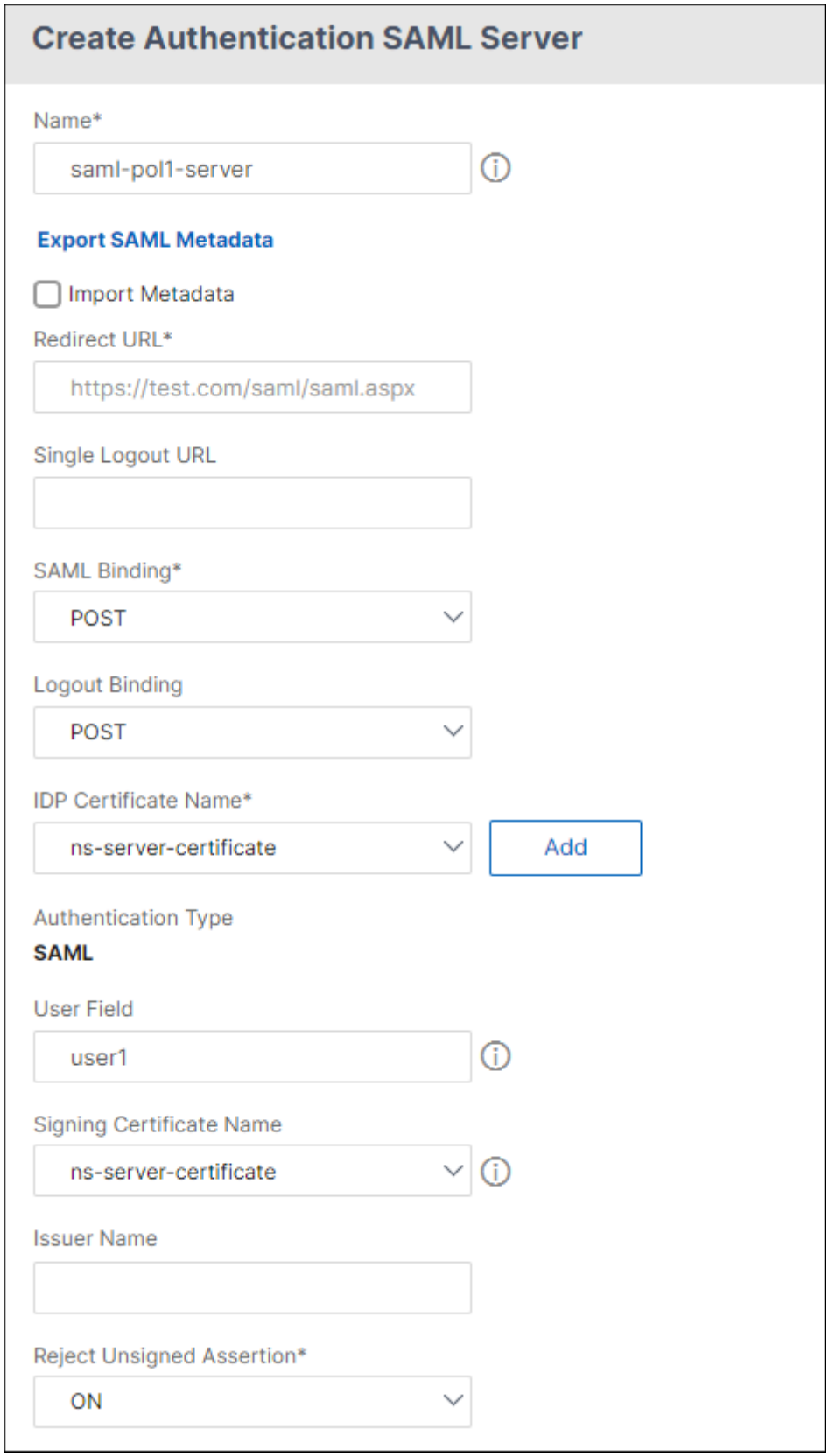
You can configure SAML two-factor authentication. When you configure SAML authentication with LDAP authentication, use the following guidelines:

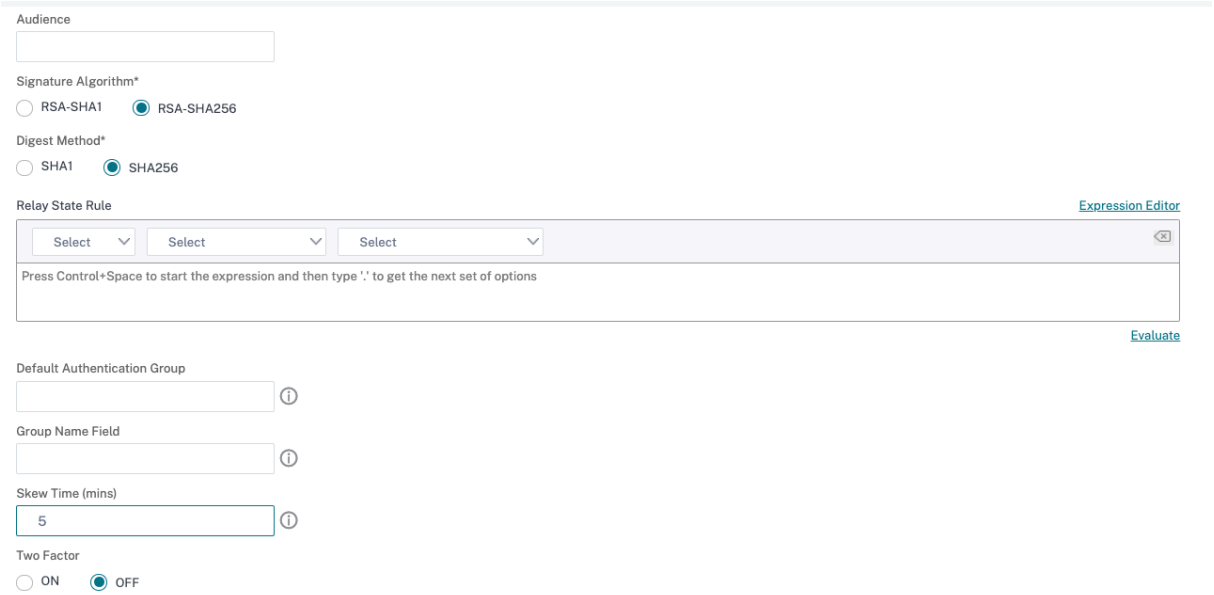
- If SAML is the primary authentication type, disable authentication in the LDAP policy and configure group extraction. Then, bind the LDAP policy as the secondary authentication type.
- SAML authentication does not use a password and only uses the user name. Also, SAML authentication only informs users when authentication succeeds. If SAML authentication fails, users are not notified. Since a failure response is not sent, SAML has to be either the last policy in the cascade or the only policy.
- It is recommended that you configure actual user names instead of opaque strings.
- SAML cannot be bound as the secondary authentication type.

To configure SAML authentication

January 8, 2024

1. In the configuration utility, on the Configuration tab, expand **NetScaler Gateway > Policies > Authentication**.
2. In the navigation pane, click **SAML**.
3. In the details pane, click **Add**.
4. In the Create Authentication Policy dialog box, in **Name**, type a name for the policy.





1. Next to Server, click **Add**.
2. In **Name**, type a name for the server profile.
3. In IdP Certificate Name, select a certificate or click **Install**. This is the certificate installed on the SAML or IdP server.

   If you click Install, add the certificate and private key. For more information, see Installing and Managing Certificates.
4. In **Redirect URL**, enter the URL of the authentication Identity Provider (IdP).

   This is the URL for the user logon to the SAML server. This is the server to which NetScaler Gateway redirects the initial request.
5. In **Single Logout URL**, specify the URL so that the appliance can recognize when to send the client back to the IdP to complete the sign-out process.
6. In **SAML Binding**, select the method that is to be used to move the client from the SP to the IdP. This needs to be the same on the IdP so that it understands how the client connects to it. When the appliance acts as an SP, it supports POST, REDIRECT, and ARTIFACT bindings.
7. In **Logout Binding**, select **REDIRECT.**
8. In **IDP Certificate Name**, select the IdPCert Certificate (Base64) present under the SAML Signing Certificate.

   > **Note:**
   >
   > You can also click **Import Metadata** and select the URL where the metadata configuration is stored.
9. In **User Field**, enter the user name to extract.

10. In **Signing Certificate Name**, Select the SAML SP certificate (with private key) that the appliance uses to sign authentication requests to the IdP. The same certificate (without private key) must be imported to the IdP, so that the IdP can verify the authentication request signature. This field is not needed by most IdPs

    This is the certificate that is bound to the NetScaler Gateway virtual IP address. The SAML Issuer Name is the fully qualified domain name (FQDN) to which users log on, such as lb.example.com or ng.example.com.

11. In **Issuer Name**, enter the FQDN of the load balancing or NetScaler Gateway virtual IP address to which the appliance sends the initial authentication (GET) request.
12. In **Reject unsigned assertion**, specify if you require the Assertions from the IdP to be signed. You can ensure that only the Assertion must be signed (ON) or both the assertion and the response from the IdP must be signed (STRICT).
13. In **Audience**, enter the audience for which the assertion sent by IdP is applicable. This is typically an entity name or URL that represents the service provider.
14. In **Signature Algorithm**, select RSA-SHA256
15. In **Digest Method**, select SHA256
16. In **Default Authentication Group**, enter the default group that is chosen when the authentication succeeds in addition to the extracted groups.
17. In **Group Name**, enter the name of the tag in the assertion that contains user groups.
18. In **Skew Time (mins)**, specify the allowed clock skew in minutes that the service provider allows on an incoming assertion.
19. Click **Create,** and then click **Close**.
20. In the Create authentication policy dialog box, next to Named Expressions, select General, select True value, click **Add Expression**, click **Create**, and then click **Close**.

References

- NetScaler as a SAML SP
- NetScaler as a SAML IdP
- Additional features supported for SAML

Using SAML authentication to log in to NetScaler Gateway

January 8, 2024

You can use SAML authentication to log in to NetScaler Gateway using the VPN clients and the Workspace app. The plug-in supports SAML authentication only through advanced SAML policies bound to the authentication virtual server, that is nFactor authentication.

Important: The plug-in does not support SAML authentication when SAML policies are bound directly to the VPN virtual server, that is non-nFactor authentication.

Supported platforms and apps

The following table lists the platforms and applications that support SAML authentication for logging in to NetScaler Gateway.

Product	Version
NetScaler Gateway	Version 12.0 build 41.16 and later
VPN client	Version 12.1 build 49.37 and later. **Supported platforms**: Windows 7, Windows 8, Windows 8.1, Windows 10
Workspace app versions	Windows: 1808; Mac: 1808

Configure for SAML authentication using advanced SAML policies

For details on configuring SAML authentication using advanced SAML policies see, NetScaler as a SAML IdP.

Improvements in SAML Authentication

January 8, 2024

This feature requires SAML knowledge, fundamental authentication proficiency, and FIPS understanding to use this information.

You can use the following NetScaler features with third party applications and servers that are compatible with the SAML 2.0 specification:

- SAML Service Provider (SP)
- SAML Identity Provider (IdP)

SP and IdP allow a SingleSignOn (SSO) between cloud services. The SAML SP feature provides a way of addressing user claims from an IdP. The IdP can be a third party service or another NetScaler appliance. The SAML IdP feature is used to assert user logons and provide claims consumed by SPs.

As part of the SAML support, both IdP and SP modules digitally sign the data that is sent to peers. The digital signature includes an authentication request from SP, Assertion from IdP, and logout messages between these two entities. The digital signature validates the message authenticity.

The current implementations of SAML SP and IdP perform the signature computation in a packet engine. These modules use SSL certificates to sign the data. In a FIPS compliant NetScaler, the private key of the SSL certificate is not available in the packet engine or user space, so the SAML module today is not ready for FIPS hardware.

This document describes the mechanism to offload signature calculations to the FIPS card. Signature verification is done in the software, as the public key is available.

Solution

The SAML feature set is enhanced to use an SSL API for signature offload. See NetScaler product Documentation for details about these affected SAML subfeatures:

1. SAML SP Post Binding –Signing of AuthnRequest
2. SAML IdP Post Binding –Signing of Assertion/Response/Both
3. SAML SP Single Logout scenarios –Signing of LogoutRequest in SP initiated model and Signing of LogoutResponse in IdP initiated model
4. SAML SP Artifact binding –Signing of ArtifactResolve request
5. SAML SP Redirect Binding –Signing of AuthnRequest
6. SAML IdP Redirect Binding –Signing of Response/Assertion/Both
7. SAML SP Encryption support –Decryption of Assertion

Platform

The API can be offloaded only to a FIPS platform.

Configuration

Offload configuration is performed automatically on the FIPS platform.

However, since SSL private keys are not available to user space in FIPS hardware, there is a slight configuration change in creating the SSL certificate on FIPS hardware.

Here's the configuration information:

- `add ssl fipsKey fips-key`

  Create a CSR and use it at the CA server to generate a certificate. You can then copy that certificate in `/nsconfig/ssl`. Let's assume that the file is fips3cert.cer.

- `add ssl certKey fips-cert -cert fips3cert.cer -fipsKey fips-key`

  Then specify this certificate in the SAML action for the SAML SP module.

- `set samlAction <name> -samlSigningCertName fips-cert`

  Likewise, you use this in the `samlIdpProfile` for the SAML IdP module.

- `set samlidpprofile fipstest –samlIdpCertName fips-cert`

The FIPS key is not available the first time. If there's no FIPS key, create one as described Create a FIPS key.

```
create ssl fipskey <fipsKeyName> -modulus <positive_integer> [-exponent
    (3 | F4)]

create certreq <reqFileName> -fipskeyName <string>
```

Configuring TACACS+ Authentication

January 8, 2024

You can configure a TACACS+ server for authentication. Similar to RADIUS authentication, TACACS+ uses a secret key, an IP address, and the port number. The default port number is 49.

To configure NetScaler Gateway to use a TACACS+ server, provide the server IP address and the TACACS+ secret. You need to specify the port only when the server port number in use is something other than the default port number of 49.

To configure TACACS+ authentication using user interface, perform the following steps.

1. In the configuration utility, on the Configuration tab, expand **NetScaler Gateway > Policies > Authentication**.
2. Click **TACACS**.
3. In the details pane, click **Add**.
4. In **Name** field, type a name for the policy.
5. Next to **Server** field, click **Add** to create a new TACACS server or click **Edit** to make changes to an existing TACACS server.
6. In **Name** field, type a name for the server.

7. Under **IP Address**, type the IP address.
8. Under **Port**, use the default port number 49.
9. In **TACACS Key** field, type the key. In **Confirm TACACS key** field, type the same key to confirm.
10. Click **More**.
11. In **Authorization**, select **ON** and then click **Create**.
12. In the **Create Authentication TACACS Policy** dialog box, select the Expression, click Create and then click Close.

To configure TACACS+ authentication using command line interface, type the following command.

```
add authentication tacacsAction <name> [-serverIP <ip_addr|ipv6_addr|*>][-serverPort <port>] [-authTimeout <positive_integer>] {
 -tacacsSecret  }

[-authorization ( ON | OFF )] [-accounting ( ON | OFF )][-auditFailedCmds ( ON | OFF )] [-groupAttrName <string>][-defaultAuthenticationGroup <string>] [-Attribute1 <string>] [-Attribute2 <string>] [-Attribute3 <string>] [-Attribute4 <string>]
[-Attribute5 <string>] [-Attribute6 <string>] [-Attribute7 <string>] [-Attribute8 <string>] [-Attribute9 <string>] [-Attribute10 <string>]
[-Attribute11 <string>] [-Attribute12 <string>] [-Attribute13 <string>] [-Attribute14 <string>] [-Attribute15 <string>] [-Attribute16 <string>]
```

After you configure the TACACS+ server settings in NetScaler Gateway, bind the policy to make it active. You can bind the policy on either the global or virtual server level. For more information about binding authentication policies, see Binding Authentication Policies.

Clear Config Basic Must Not Clear TACACS Config

January 8, 2024

This topic focuses on not clearing all RBA (Role Based Access) related configurations when the clear config command is run.

The current clear config command is performed in one of three levels:

- Basic
- Extended
- Full

Based on the level, NetScaler configurations are cleared and reset to the factory default.

The command used is;

```
clear ns config [-force] <level>
```


The new command adds a knob to allow/deny the deletion of all RBA related configurations.

New Command

Described are the Clear RBA config features:

1. YES/NO knob with Default: YES.

   The admin decides whether to retain the RBA config or not.

2. ONLY the BASIC LEVEL of clear config is supported.
3. The following configurations not cleared:

   - Add/bind system user/group.
   - Add cmd policy.
   - TACACS commands (add TACACS action/policy).
   - Bind system global

   Note: TACACS related config (action/policy) is preserved if the policy is bound to the system global or else it is cleared

CLI Configuration

The command used is;

```
clear config [ – force] <level> [-RBAconfig]
```

By default it is set to YES, and clears the configurations based on the level.

If –`RBAconfig` is set to NO, the RBA related config is retained. The following is included:

- Add /bind system user /group
- Bind system global
- TACACS related commands (add TACACS action/policy)
- Add cmd policy

Configuring Multifactor Authentication

January 8, 2024

You can configure two types of multifactor authentication in NetScaler Gateway:

- Cascading authentication that sets the authentication priority level
- Two-factor authentication that requires users to log on by using two types of authentication

If you have multiple authentication servers, you can set the priority of your authentication polices. The priority levels you set determine the order in which the authentication server validates users' credentials. A policy with a lower priority number takes precedence over a policy with a higher number.

You can have users authenticate against two different authentication servers. For example, you can configure an LDAP authentication policy and an RSA authentication policy. When users log on, they authenticate first with their user name and password. Then, they authenticate with a personal identification number (PIN) and the code from the RSA token.

Configuring Cascading Authentication

January 8, 2024

Authentication allows you to create a cascade of multiple authentication servers using policy prioritization. When you configure a cascade, the system traverses each authentication server, as defined by the cascaded policies, to validate a user's credentials. Prioritized authentication policies are cascaded in ascending order and can have priority values in the range of 1–9999. You define these priorities when binding your policies at either the global or the virtual server level.

During authentication, when a user logs on, the virtual server is checked first and then global authentication policies are checked. If a user belongs to an authentication policy on both the virtual server and globally, the policy from the virtual server is applied first and then the global authentication policy. If you want users to receive the authentication policy that is bound globally, change the priority of the policy. When a global authentication policy has a priority number of one and an authentication policy bound to a virtual server has a priority number two, the global authentication policy takes precedence. For example, you can have three authentication policies bound to the virtual server and you can set the priority of each policy.

If a user fails to authenticate against a policy in the primary cascade, or if that user succeeds in authenticating against a policy in the primary cascade but fails to authenticate against a policy in the secondary cascade, the authentication process stops and the user is redirected to an error page.

Note: Citrix recommends that when you bind multiple policies to a virtual server or globally, you define unique priorities for all authentication policies.

To set the priority for global authentication policies

1. In the configuration utility, on the Configuration tab, expand **NetScaler Gateway > Policies > Authentication**.
2. Select the policy that is bound globally and then in **Action**, click **Global Bindings**.
3. In the **Bind/Unbind Authentication Global Polices** dialog box, under Priority, type the number, and then click **OK**.

To change the priority for an authentication policy bound to a virtual server

You can also modify an authentication policy that is bound to a virtual server.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway**, and then click **Virtual Servers**.
2. In the details pane, select a virtual server, and then click **Open**.
3. Click the **Authentication** tab, and then click either **Primary** or **Secondary**.
4. Next to the authentication policy, under **Priority**, type the number, and then click **OK**.

Configuring Two-Factor Authentication

January 8, 2024

NetScaler Gateway supports two-factor authentication. Normally, when authenticating users, NetScaler Gateway stops the authentication process as soon as it successfully authenticates a user through any one of the configured authentication methods. In certain instances, you may need to authenticate a user to one server, but extract groups from a different server. For example, if your network authenticates users against a RADIUS server, but you also use RSA SecurID token authentication and user groups are stored on that server, you may need to authenticate users to that server so you can extract the groups.

If users are authenticated by using two authentication types, and if one of those types is client certificate authentication, you can configure the certificate authentication policy as the second method of authentication. For example, you use LDAP as your primary authentication type and the client certificate as the secondary authentication. When users log on with their user name and password, they then have access to network resources.

When you configure two-factor authentication, you select if the authentication type is the primary or secondary type.

To configure two-factor authentication

1. In the configuration utility, on the Configuration tab, expand NetScaler Gateway > Policies > Authentication.
2. On the Policies tab, click Global Bindings.
3. In the Bind/Unbind Authentication Policies to Global dialog box, click Primary.
4. Click Insert Policy.
5. Under Policy Name, select the authentication policy.
6. Click Secondary, repeat Steps 4 and 5 and then click OK.

Selecting the Authentication Type for Single Sign-On

January 8, 2024

If you have single sign-on and two-factor authentication configured on NetScaler Gateway, you can select which password to use for single sign-on. For example, you have LDAP configured as the primary authentication type and RADIUS configured as the secondary authentication type. When users access resources that require single sign-on, the user name and primary password are sent by default. You set which password must be used for single sign-on to web applications within a session profile.

To configure authentication for single sign-on

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway > Policies > Session**.
2. In the details pane, click the **Profiles** tab, and then do one of the following:
   - To create a new profile, click **Add**.
   - To modify an existing profile, click **Open**.
3. On the Client Experience tab, next to Credential Index, click **Override Global**, select either **Primary** or **Secondary**.
4. If this is a new profile, click **Create**, and then click **Close**.
5. If you are modifying an existing profile, click **OK**.

Configuring Client Certificates and LDAP Two-Factor Authentication

January 8, 2024

You can use a secure client certificate with LDAP authentication and authorization, such as using smart card authentication with LDAP. The user logs on and then the user name is extracted from the client certificate. The client certificate is the primary form of authentication and LDAP is the secondary form. The client certificate authentication must take priority over the LDAP authentication policy. When you set the priority of the policies, assign a lower number to the client certificate authentication policy than the number you assign to the LDAP authentication policy.

To use a client certificate, you must have an enterprise Certificate Authority (CA), such as Certificate Services in Windows Server 2008, running on the same computer that is running Active Directory. You can use the CA to create a client certificate.

To use a client certificate with LDAP authentication and authorization, it must be a secure certificate that uses the Secure Sockets Layer (SSL). To use secure client certificates for LDAP, install the client certificate on the user device and install a corresponding root certificate on NetScaler Gateway.

Before configuring a client certificate, do the following:

- Create a virtual server.
- Create an LDAP authentication policy for the LDAP server.
- Set the expression for the LDAP policy to True value.

To configure client certificate authentication with LDAP

1. In the configuration utility, on the Configuration tab, expand **NetScaler Gateway > Policies \ > Authentication**.
2. In the navigation pane, under Authentication, click Cert.
3. In the details pane, click Add.
4. In Name, type a name for the policy.
5. In Authentication Type, select Cert.
6. Next to Server, click New.
7. In Name, type a name for the server, and then click Create.
8. In the Create Authentication Server dialog box, in Name, type the name of the server.
9. Next to Two Factor, select ON.
10. In the User Name Field, select Subject:CN and then click Create.
11. In the Create Authentication Policy dialog box, next to Named Expressions, select True value, click Add Expression, click Create, and then click Close.

After you create the certificate authentication policy, bind the policy to the virtual server. After binding the certificate authentication policy, bind the LDAP authentication policy to the virtual server.

Important: You must bind the certificate authentication policy to the virtual server before you bind the LDAP authentication policy to the virtual server.

To install a root certificate on NetScaler Gateway

After you create the certificate authentication policy, you download and install a root certificate from your CA in Base64 format and save it on your computer. You can then upload the root certificate to NetScaler Gateway.

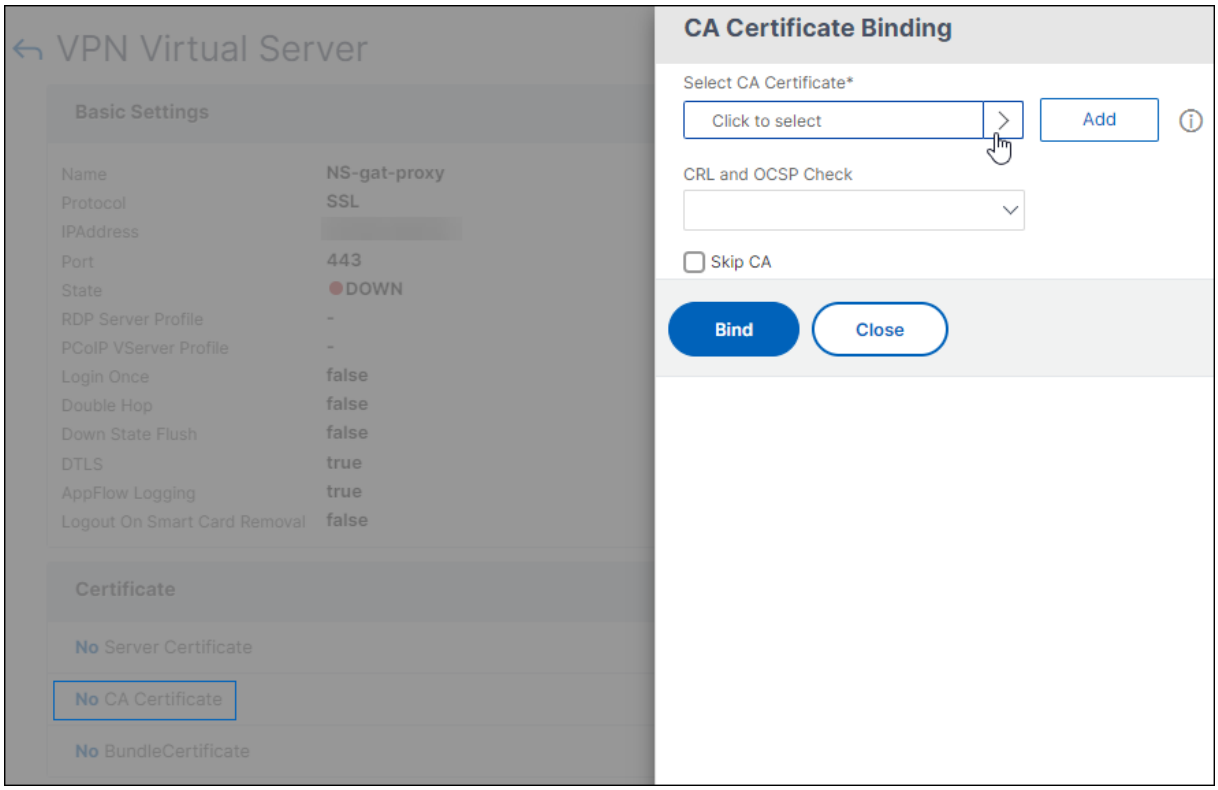
1. In the configuration utility, on the Configuration tab, in the navigation pane, expand SSL and then click Certificates.
2. In the details pane, click Install.
3. In Certificate - Key Pair Name, type a name for the certificate.
4. In Certificate File Name, click Browse and in the list, select either Appliance or Local.
5. Navigate to the root certificate, click Open, and then click Install.

To add a root certificate to a virtual server

After installing the root certificate on NetScaler Gateway, add the certificate to the certificate store of the virtual server.

Important: When you add the root certificate to the virtual server for smart card authentication, you must select the certificate from the
Select CA Certificate list box, as shown in the following figure.

Figure 1. Adding a root certificate as a CA



1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click Virtual Servers.
2. In the details pane, select a virtual server and then click Open.
3. On the Certificates tab, under Available, select the certificate, next to Add, in the list, click CA, and then click OK.
4. Repeat Step 2.
5. On the Certificates tab, click SSL Parameters.
6. Under Others, select Client Authentication.
7. Under Others, next to Client Certificate, select Optional and then click OK twice.
8. After configuring the client certificate, test the authentication by logging on to NetScaler Gateway with the Citrix Secure Access client. If you have more than one certificate installed, you receive a prompt asking you to select the correct certificate. After you select the certificate, the logon screen appears with the user name populated with the information obtained from the certificate. Type the password and then click Login.

If you do not see the correct user name in the User Name field on the logon screen, check the user accounts and groups in your LDAP directory. The groups that are defined on NetScaler Gateway must be the same as those in the LDAP directory. In Active Directory, configure groups at the domain root level. If you create Active Directory groups that are not in the domain root level, incorrect reading of the client certificate can result.

If users and groups are not at the domain root level, the NetScaler Gateway logon page displays the user name that is configured in Active Directory. For example, in Active Directory, you have a folder called Users and the certificate says CN=Users. In the logon page, in User Name, the word Users appears.

If you do not want to move your group and user accounts to the root domain level, when configuring the certificate authentication server on NetScaler Gateway, leave User Name Field and Group Name Field blank.

Configuring Single Sign-On

January 8, 2024

You can configure NetScaler Gateway to support single sign-on with Windows, to Web applications (such as SharePoint), to file shares, and to the Web Interface. Single sign-on also applies to file shares that users can access through the file transfer utility in the Access Interface or from the NetScaler Gateway icon menu in the notification area.

If you configure single sign-on when users log on, they are automatically logged on again without having to enter their credentials a second time.

Configuring Single Sign-On with Windows

January 8, 2024

Users open a connection by starting the Citrix Secure Access client from the desktop. You can specify that the Citrix Secure Access client start automatically when the user logs on to Windows by enabling single sign-on. When you configure single sign-on, users' Windows Logon credentials are passed to NetScaler Gateway for authentication. Enabling single sign-on for the Citrix Secure Access client facilitates operations on the user device, such as installation scripts and automatic drive mapping.

Enable single sign-on only if user devices are logging on to your organization's domain. If single sign-on is enabled and a user connects from a device that is not on your domain, the user is prompted to log on.

You configure single sign-on with Windows either globally or by using a session profile that is attached to a session policy.

To configure single sign-on with Windows globally

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, expand **NetScaler Gateway** and then click **Global Settings**.
2. In the details pane, under **Settings**, click **Change global settings**.
3. On the **Client Experience** tab, click **Single Sign-on with Windows**, and then click **OK**.

To configure single sign-on with Windows by using a session policy

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, expand **NetScaler Gateway > Policies**, and then click **Session**.
2. In the details pane, click **Add**.
3. In **Name**, type a name for the policy.
4. **Next to Request Profile**, click **New**.
5. In **Name**, type a name for the profile.
6. On the **Client Experience** tab, next to **Single Sign-On with Windows**, click **Override Global**, click **Single Sign-on with Windows**, and then click **OK**.
7. In the **Create Session Policy** dialog box, next to **Named Expressions**, select **General**, select True value, click **Add Expression**, click **Create**, and then click **Close**.

Configuring Single Sign-On to Web Applications

January 8, 2024

You can configure NetScaler Gateway to provide single sign-on to servers in the internal network that use web-based authentication. With single sign-on, you can redirect the user to a custom home page, such as a SharePoint site or to the Web Interface. You can also configure single sign-on to resources through the Citrix Secure Access client from a bookmark configured on the home page or a web address that users type in the web browser.

If you are redirecting the home page to a SharePoint site or Web Interface, provide the web address for the site. When users are authenticated, either by NetScaler Gateway or an external authentication server, users are redirected to the specified home page. User credentials are passed transparently to the web server. If the web server accepts the credentials, users are logged on automatically. If the web server denies the credentials, users receive an authentication prompt asking for their user name and password.

You can configure single sign-on to web applications globally or by using a session policy.

To configure single sign-on to web applications globally

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Client Experience tab, click Single sign-on to Web Applications and then click OK.

To configure single sign-on to web applications by using a session policy

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway > Policies and then click Session.
2. In the details pane, on the Policies tab, select a session policy and then click Open.
3. In the Configure Session Policy dialog box, next to Request Profile, click Modify.
4. On the Client Experience tab, next to Single Sign-On to Web Applications, click Global Override, click Single Sign-On to Web Applications and then click OK.

To define the HTTP port for single sign-on to web applications

Single sign-on is attempted only for network traffic where the destination port is considered an HTTP port. To allow single sign-on to applications that use a port other than port 80 for HTTP traffic, add one

or more port numbers on NetScaler Gateway. You can enable multiple ports. The ports are configured globally.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Network Configuration tab, click Advanced Settings.
4. Under HTTP Ports, type the port number, click Add and then click OK twice.

   You can repeat Step 4 for each port you want to add.

Note: If web applications in the internal network use public IP addresses, single sign-on does not function. To enable single sign-on, split tunneling must be enabled as part of the global policy setting, regardless if clientless access or the Citrix Secure Access client is used for user device connections. If it is not possible to enable split tunneling on a global level, create a virtual server that use a private address range.

Configuring single sign-on to Web Applications by Using LDAP

January 8, 2024

When you configure single sign-on and users log on by using the user principal name (UPN) with a format of
username@domain.com, by default single sign-on fails and users must authenticate two times. If you need to use this format for user logon, modify the LDAP authentication policy to accept this form of user name.

To configure single sign-on to web applications

1. In the configuration utility, on the **Configuration** tab, expand **NetScaler Gateway > Policies > Authentication**.
2. In the details pane, on the **Policies** tab, select an LDAP policy and then click **Open**.
3. In the **Configure Authentication Policy** dialog box, next to **Server**, click **Modify**.
4. Under **Connection Settings**, in Base DN (location of users), type DC=domainname,DC=com.
5. In **Administrator Bind DN**, type LDAPaccount@domainname.com, where domainname.com is the name of your domain.
6. In **Administrator Password** and **Confirm Administrator Password**, type the password.
7. Under **Other Settings**, in **Server Logon Name Attribute**, type UserPrincipalName.
8. In **Group Attribute**, type memberOf.

9. In **Sub Attribute Name**, type CN.
10. In **SSO Name Attribute**, type the format by which users log on, and then click **OK** twice. This value is either `SamAccountName` or `UserPrincipalName`.

Configuring Single Sign-On to a Domain

January 8, 2024

If users connect to servers running Citrix Virtual Apps and use SmartAccess, you can configure single sign-on for users connecting to the server farm. When you configure access to published applications using a session policy and profile, use the domain name for the server farm.

You can also configure single sign-on to file shares in your network.

To configure single sign-on to a domain

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway > Policies and then click Session.
2. In the details pane, on the Policies tab, select a session policy and then click Open.
3. In the Configure Session Policy dialog box, next to Request Profile, click Modify.
4. In the Configure Session Profile dialog box, on the Published Applications tab, in Single-sign-on Domain, click Override Global, type the domain name and then click OK twice.

For more information about configuring the NetScaler Gateway with Citrix Virtual Apps, see Integrate NetScaler Gateway with Citrix Virtual Apps and Desktops.

Configuring Single Sign-On for Microsoft Exchange 2010

January 8, 2024

The following section describes the configuration of Single Sign-On (SSO) for Microsoft Exchange 2010 on NetScaler Gateway. The SSO for Outlook Web Access (OWA) 2010 does not work in the following conditions:

- Using the forms based authentication on Microsoft Exchange 2010.
- Load balancing virtual server with authentication, authorization, and auditing traffic management policy.

> **Note:** This configuration works only for load balancing virtual server with authentication, authorization, and auditing traffic management policy. It does not work for SSO in OWA 2010 with clientless VPN.

The following steps are prerequisites that you must consider before configuring SSO for Microsoft Exchange 2010 on NetScaler Gateway.

- The Action URL for SSO form is different in OWA 2010. Modify the traffic management policy accordingly.
- You require a rewrite policy to set the `PBack` cookie in the logon.aspx request. In normal scenarios, you set the `PBack` cookie at the client and click Submit.
- When you are using SSO, the response to logon.aspx is consumed and the NetScaler Gateway generates the form request. The cookie is not attached in the form submission request.
- The OWA server expects the `PBack` cookie in the form submission request. The rewrite policy is required to attach the `PBack` cookie in the form submission request.

Perform the following by using the CLI

1. Configure the authentication, authorization, and auditing traffic management

   ```
   add tm formSSOAction OWA_Form_SSO_SSOPro -actionURL "/owa/auth.
   owa"-userField username -passwdField password -ssoSuccessRule "
   http.RES.SET_COOKIE.COOKIE(\"cadata\").VALUE(\"cadata\").LENGTH.
   GT(70"-responsesize 15000 -submitMethod POST
   ```

2. Configure the traffic management policy and bind the policy

   - `add tm trafficAction OWA_2010_Prof -appTimeout 1 -SSO ON -formSSO Action OWA_Form_SSO_SSOPro`
   - `add tm trafficPolicy owa2k10_pol "HTTP.REQ.URL.CONTAINS(\"owa/auth/logon.aspx\")"OWA_2010_Prof`
   - `bind tm global -policyName owa2k10_pol -priority 100`

Rewrite configuration using CLI

At the command prompt, type:

- `add rewrite action set_pback_cookie insert_after "http.REQ.COOKIE.VALUE(\"OutlookSession\")""\";PBack=0\""-bypassSafetyCheck YES`
- `add rewrite policy set_pback_cookie "http.REQ.URL.CONTAINS(\"logon.aspx\")"set_pback_cookie`

- `bind rewrite global set_pback_cookie 100 END -type REQ_DEFAULT`

Alternate rewrite configuration

In rare cases, the Microsoft Outlook might not issue OWA session cookies and the `Pback` cookies might also not get inserted. The issue might occur after you have run the preceding commands to implement the rewrite configuration.

To overcome such scenarios and as a workaround, you can configure the following commands instead of the rewrite configuration.

At the command prompt, type:

- `add rewrite action set_pback_cookie insert_http_header "Cookie"'" PBack=0"'`
- `add rewrite policy set_pback_cookie "http.REQ.URL.CONTAINS(\" logon.aspx\")"set_pback_cookie`
- `set rewrite policy set_pback_cookie -action set_pback_cookie`
- `bind rewrite global set_pback_cookie 100 END -type REQ_DEFAULT`

Configuring One-Time Password Use

January 8, 2024

You can configure NetScaler Gateway to use one-time passwords, such as a token personal identification number (PIN) or passcode. After a user enters the passcode or PIN, the authentication server immediately invalidates the one-time password and the user cannot enter the same PIN or password again.

Products that include using a one-time password include:

- RSA SecurID
- Imprivata OneSign
- SafeWord
- Gemalto Protiva
- Nordic SMS PASSCODE

To use each of these products, configure the authentication server in the internal network to use RADIUS. For more information, see Configuring RADIUS Authentication.

If you configure authentication on NetScaler Gateway to use a one-time password with RADIUS, as provided by an RSA SecurID token, for example, NetScaler Gateway attempts to reauthenticate users by using the cached password. This reauthentication occurs when you make changes to NetScaler Gateway or if the connection between the Citrix Secure Access client and NetScaler Gateway is interrupted and then restored.

An attempt to reauthenticate can also occur when connections are configured to use Citrix Workspace app and users connect to the Web Interface by using RADIUS or LDAP. When a user starts an application and uses the application, and then returns to Receiver to start another application, NetScaler Gateway uses cached information to authenticate the user.

Configuring RSA SecurID Authentication

January 8, 2024

When configuring the RSA/ACE server for RSA SecureID authentication, you need to complete the following steps:

Configure the RADIUS client with the following information:

- Provide the name of the NetScaler Gateway appliance.
- Provide a description (not mandatory).
- Provide the system IP address.
- Provide the shared secret between NetScaler Gateway and the RADIUS server.
- Configure the make/model as Standard RADIUS.

In the agent host configuration, you need the following information:

- Provide the fully qualified domain name (FQDN) of NetScaler Gateway (as it appears on the certificate bound to the virtual server). After providing the FQDN, click the Tab key and the Network Address window populates itself.

  After you enter the FQDN, the network address automatically appears. If it does not, enter the system IP address.

- Provide the Agent Type by using Communication Server.
- Configure to import all users or a set of users who are allowed to authenticate through NetScaler Gateway.

If it is not already configured, create an Agent Host entry for the RADIUS server, including the following information:

- Provide the FQDN of the RSA server.

  After you enter the FQDN, the network address automatically appears. If it does not, provide the IP address of the RSA server.

- Provide the Agent Type, which is the RADIUS server.

For more information about configuring an RSA RADIUS server, see the manufacturer's documentation.

To configure RSA SecurID, create an authentication profile and policy and then bind the policy globally or to a virtual server. To create a RADIUS policy to use RSA SecurID, see Configuring RADIUS Authentication.

After creating the authentication policy, bind it to a virtual server or globally. For more information, see Binding Authentication Policies.

Configuring Password Return with RADIUS

January 8, 2024

You can replace domain passwords with a one-time password that a token generates from a RADIUS server. When users log on to NetScaler Gateway, they enter a personal identification number (PIN) and the passcode from the token. After NetScaler Gateway validates their credentials, the RADIUS server returns the user's Windows password to NetScaler Gateway. NetScaler Gateway accepts the response from the server and then uses the returned password for single sign-on instead of using the passcode that users typed during the logon. This password return with the RADIUS feature allows you to configure single sign-on without requiring users to recall their Windows password.

When users log on by using password return, they can access all allowed network resources in the internal network, including Citrix Endpoint Management, StoreFront, and the Web Interface.

To enable single sign-on by using returned passwords, you configure a RADIUS authentication policy on NetScaler Gateway by using the Password Vendor Identifier and Password Attribute Type parameters. These two parameters return the user's Windows password to NetScaler Gateway.

NetScaler Gateway supports Imprivata OneSign. The minimum required version of Imprivata OneSign is 4.0 with service pack 3. The default password vendor identifier for Imprivata OneSign is 398. The default password attribute type code for Imprivata OneSign is 5.

You can use other RADIUS servers for password return, such as RSA, Cisco, or Microsoft. Configure the RADIUS server to return the user single sign-on password in a vendor-specific attribute value pair. In a NetScaler Gateway authentication policy, you must add the **Password Vendor Identifier and Password** Attribute Type parameters for these servers.

You can find a complete list of vendor identifiers on the Internet Assigned Numbers Authority (IANA) website. For example, the vendor identifier for RSA security is 2197, for Microsoft, it is 311, and for Cisco Systems, it is 9. The vendor-specific attribute that a vendor supports must be confirmed with the vendor. For example, Microsoft has published a list of vendor-specific attributes at Microsoft Vendor-specific RADIUS Attributes.

You can select any of the vendor-specific attributes to store the single sign-on password for users on the RADIUS server of the vendor. If you configure NetScaler Gateway with the vendor identifier and attribute where the user password is stored on the RADIUS server, NetScaler Gateway requests the value of the attribute in the access request packet that is sent to the RADIUS server. If the RADIUS server responds with the corresponding attribute-value pair in the access-accept packet, password return works regardless of the RADIUS server you use.

To configure single sign-on by using returned passwords:

1. In the configuration utility, on the Configuration tab, expand **NetScaler Gateway > Policies \ > Authentication**.
2. In the navigation pane, click **RADIUS**.
3. In the details pane, click **Add**.
4. In the **Create Authentication Policy** dialog box, in Name, type a name for the policy.
5. Next to **Server**, click **New**.
6. In **Name**, type the name of the server.
7. Configure the settings for the RADIUS server.
8. In **Password Vendor Identifier**, type the vendor identifier that is returned by the RADIUS server. This identifier must have a minimum value of 1.
9. In **Password Attribute Type**, type the attribute type that is returned by the RADIUS server in the vendor-specific AVP code. The value can range from 1 through 255.
10. In the **Create Authentication Policy** dialog box, next to **Named Expressions**, select the expression, click **Add Expression**, click **Create**, and then click **Close**.

Configuring SafeWord Authentication

January 8, 2024

The SafeWord product line helps to provide secure authentication by using a token-based passcode. After users enter a passcode, it is invalidated by SafeWord and cannot be used again.

If Access Gateway is replacing the Secure Gateway in a Secure Gateway and Web Interface deployment, you can choose to not configure authentication on Access Gateway and continue to allow the Web Interface to provide SafeWord authentication for incoming HTTP traffic.

Access Gateway supports SafeWord authentication for the following products:

- SafeWord 2008
- SafeWord PremierAccess
- SafeWord for Citrix
- SafeWord RemoteAccess

You can configure Access Gateway to authenticate using SafeWord products in the following ways:

- Configure authentication to use a PremierAccess RADIUS server that is installed as part of SafeWord PremierAccess and allow it to handle authentication.
- Configure authentication to use the SafeWord IAS agent, which is a component of SafeWord RemoteAccess, SafeWord for Citrix, and SafeWord PremierAccess 4.0.
- Install the SafeWord Web Interface Agent to support the Citrix Web Interface. You do not have to configure authentication on Access Gateway and the Citrix Web Interface can handle this. This configuration does not use the PremierAccess RADIUS server or the SafeWord IAS Agent.

When configuring the SafeWord RADIUS server, you need the following information:

- The IP address of Access Gateway. When you configure client settings on the RADIUS server, use the Access Gateway IP address.
- A shared secret.
- The IP address and port of the SafeWord server.

Configuring Gemalto Protiva Authentication

January 8, 2024

Protiva is a strong authentication platform that was developed to use the strengths of Gemalto's smart card authentication. With Protiva, users log on with a user name, password, and one-time password generated by the Protiva device. Similar to RSA SecurID, the authentication request is sent to the Protiva Authentication Server and the password is either validated or rejected.

To configure Gemalto Protiva to support NetScaler Gateway, use the following guidelines:

- Install the Protiva server.
- Install the Protiva Internet Authentication Server (IAS) agent plug-in on a Microsoft IAS RADIUS server. Make sure you note the IP address and port number of the IAS server.

nFactor for gateway authentication

January 8, 2024

nFactor authentication enables a whole new set of possibilities regarding authentication. Administrators using nFactor enjoy authentication, authorization, and auditing flexibility when configuring authentication factors for virtual servers.

Two policy banks or two factors no longer restrict an administrator. The number of policy banks can be extended to suit different needs. Based on previous factors, nFactor determines a method of authentication. Dynamic login forms and on-failure actions are possible by using nFactor.

> **Important**
>
> - Starting from release 13.0 build 67.x, nFactor authentication is supported with Standard license only for Gateway/VPN virtual server, and not for the authentication virtual server. In Standard license, the nFactor visualizer GUI cannot be used to create the EPA in the nFactor flow. Also, you cannot edit the login schema, but must use the out-of-the-box login schema as-is.
> - For NetScaler to support nFactor authentication, an Advanced license or a Premium license is required. For more information about nFactor authentication with NetScaler, see nFactor authentication.

Authentication, authorization, and auditing feature licensing requirements

The following table lists the licensing requirements for the available authentication, authorization, and auditing features.

	Standard License	Advanced License	Premium License
LOCAL authentication	Yes	Yes	Yes
LDAP authentication	Yes	Yes	Yes
RADIUS authentication	Yes	Yes	Yes
TACACS authentication	Yes	Yes	Yes

	Standard License	Advanced License	Premium License
Web authentication	Yes	Yes	Yes
Client cert authentication	Yes	Yes	Yes
Negotiate authentication	Yes	Yes	Yes
SAML authentication	Yes	Yes	Yes
OAuth authentication	No	Yes	Yes
Native OTP	No	Yes	Yes
Email OTP	No	Yes	Yes
Push notification for OTP	No	No	Yes
Knowledge based question and answer (KBA authentication)	No	Yes	Yes
Self service password reset (SSPR)	No	Yes	Yes
nFactor Visualizer	Yes	Yes	Yes

Note

- For steps to configure nFactor for the NetScaler Standard License, see the section Create a Gateway virtual server for nFactor authentication in NetScaler Standard license.
- Only a non-addressable authentication, authorization, and auditing virtual server can be bound to a Gateway/VPN virtual server in NetScaler Standard license.
- Customization of LoginSchema is not allowed in the NetScaler Standard license. The nFactor support is basic with only default and already added login schemas that come with the appliance. The administrator can use them in their configurations, but they cannot add a

> login schema. Hence the GUI option is disabled.

Use cases

nFactor authentication enables dynamic authentication flows based on the user profile. Sometimes, the flows can be simple and intuitive to the user. In other cases, they can be coupled with securing active directory or other authentication servers. The following are some requirements specific to Gateway:

1. **Dynamic user name and password selection.** Traditionally, the Clients (including Browsers and Receivers) use the active directory (AD) password as the first password field. The second password is reserved for the One-Time-Password (OTP). However, to secure AD servers, OTP is required to be validated first. nFactor can do this without requiring client modifications.
2. **Multi-Tenant Authentication End-point.** Some organizations use different Gateway servers for Certificate and non-certificate users. With users using their own devices to log in, user's access levels vary on the NetScaler appliance based on the device being used. Gateway can cater to different authentication needs.
3. **Authentication based on group membership.** Some organizations obtain user properties from AD servers to determine authentication requirements. Authentication requirements can be varied for individual users.
4. **Authentication co-factors.** Sometimes, different pairs of authentication policies are used to authenticate different sets of users. Providing pair policies increases effective authentication. Dependent policies can be made from one flow. In this manner, independent sets of policies become flows of their own that increase efficiency and reduce complexity.

Authentication response handling

The NetScaler Gateway callback registers handle authentication responses. AAAD (authentication daemon) responses and success/failure/error/dialogue codes are feed to the callback handle. The success/failure/error/dialogue codes direct Gateway to take the appropriate action.

Client support

The following table details configuration details.

Client	nFactor Support	Authentication Policy Bind Point	EPA
Browsers	Yes	Authentication	Yes
Citrix Workspace app	Yes	VPN	Yes
Gateway Plug-in	Yes	VPN	Yes

Note:

- Citrix Workspace app supports nFactor authentication for the supported operating systems from the following listed versions.
  - Windows 4.12
  - Linux 13.10
  - Mac 1808
  - iOS 2007
  - Android 1808
  - HTML5: Supported through Store Web
  - Chrome: Supported through Store Web

Command line configuration

The Gateway virtual server needs an authentication virtual server named as an attribute. Virtual server name as an attribute is the only configuration required for this model.

```
add authnProfile <name-of-profile> -authnVsName <name-of-auth-vserver>
```

The authnVsName is the name of the authentication virtual server. The authnVsName virtual server must be configured with advanced authentication policies and is used for nFactor authentication.

```
add vpn vserver <name> <serviceType> <IP> <PORT> -authnProfile <name-of
    -profile>
set vpn vserver <name> -authnProfile <name-of-profile>
```

Where authnProfile is the previously created authentication profile.

Interop challenges

Most of the Legacy Gateway clients, in addition to rfWeb clients, are modeled on responses sent by Gateway. For example, a 302 response to /vpn/index.html is expected for many clients. These clients also depend on various gateway cookies such as “`pwcount`,”“NSC_CERT.”

Endpoint analysis (EPA)

EPA in nFactor is not supported for the NetScaler authentication, authorization, and auditing module. Hence, the NetScaler Gateway virtual server performs EPA. After EPA, the login credentials are sent to the authentication virtual server using the previously mentioned API. Once authentication is complete, Gateway continues to the postauthentication process and it establishes the user session.

Misconfiguration considerations

The Gateway client sends the user credentials only once. Gateway gets either one or two credentials from the client with the login request. In the legacy mode, there are a maximum of two factors. The passwords obtained are used for these factors. However, with nFactor the number of factors that can be configured is practically unlimited. The passwords obtained from the Gateway client are reused (as per configuration) for configured factors. Care must be taken such that the one-time-password (OTP) must not be reused multiple times. Likewise, an administrator must ensure that the password reused at a factor is indeed applicable to that factor.

Defining Clients

The configuration option is provided to help NetScaler determine browser clients versus thick clients such as Receiver.

A pattern set, ns_vpn_client_useragents, is provided for the administrator to configure patterns for all Clients.

Likewise, binding the "Citrix Receiver"string to the above `patset` to ignore all Clients that have "Citrix Receiver"in the User-Agent.

Restricting nFactor for Gateway

nFactor for gateway authentication does not happen if the following conditions are present.

1. The authnProfile is not set to NetScaler Gateway.
2. Advanced authentication policies are not bound to the authentication virtual server and the same authentication virtual server is mentioned in `authnProfile`.
3. The User-Agent string in the HTTP request matches the User-Agents configured in `patset` ns_vpn_client_useragents.

If these conditions are not met, the classic authentication policy bound to Gateway is used.

If a User-Agent, or portion of it is bound to the previously mentioned patset, requests coming from those user-agents do not participate in the nFactor flow. For example, the following command restricts configuration for all browsers (assuming all browsers contain "Mozilla"in the user-agent string):

```
bind patset ns_vpn_client_useragents Mozilla
```

LoginSchema

LoginSchema is a logical representation of the logon form. The XML language defines it. The Syntax of the loginSchema conforms to Citrix's Common Forms Protocol specification.

LoginSchema defines the "view"of the product. An Administrator can provide a customized description, assistive text, and so forth of the form. The login schema includes the labels of the form itself. A customer can provide the success or failure message that describes the form presented at a given point.

Use the following command to configure a login schema.

```
add authentication loginSchema <name> -authenticationSchema <string> [-
    userExpression <string>] [-passwdExpression <string>] [-
    userCredentialIndex <positive_integer>]
[-passwordCredentialIndex <positive_integer>] [-authenticationStrength
    <positive_integer>] [-SSOCredentials ( YES | NO )]
```

Parameter description

- name - Name for the new login schema. This is a mandatory argument. Maximum Length: 127
- authenticationSchema - Name of the file for reading authentication schema to be sent for Login Page UI. This file contains the xml definition of the elements as per the Citrix Forms Authentication Protocol to be able to render the login form. If the administrator does not want to prompt users for other credentials but continue with previously obtained credentials, then noschema can be given as an argument. This applies only to loginSchemas that are used with the user-defined factors, and not the virtual server factor.

This is a mandatory argument. Maximum Length: 255

- userExpression - Expression for user name extraction during login. This can be any relevant advanced policy expression. Maximum Length: 127
- passwdExpression - Expression for password extraction during login. This can be any relevant advanced policy expression. Maximum Length: 127

- userCredentialIndex - The index at which the user entered user name must be stored in session. Minimum value: 1, Maximum value: 16
- passwordCredentialIndex - The index at which the user entered the password must be stored in session. Minimum value: 1, Maximum value: 16
- authenticationStrength - Weight of the current authentication Minimum value: 0, Maximum value: 65535
- `SSOCredentials` - This option indicates whether current factor credentials are the default SSO (SingleSignOn) credentials. Possible values: YES, NO. Default value: NO

LoginSchema and nFactor knowledge required

Pre-built loginSchema files are found in the following NetScaler location **/nsconfig/loginschema/LoginSchema/**. These pre-built loginSchema files cater to common use cases, and can be modified for slight variations if necessary.

Also, most single factor use cases with few customizations do not need the login schema configuration.

The administrator is advised to check the documentation for other configuration options that enable NetScaler to discover the factors. Once the user submits the credentials, the administrator can configure more than one factor to flexibly choose and process the authentication factors.

Configuring dual factor authentication without using LoginSchema

NetScaler automatically determines dual factor requirements based on configuration. Once the user presents these credentials, the administrator can configure the first set of policies at the virtual server. Against each policy there can be a "nextFactor"configured as a "passthrough."A "passthrough"implies that the NetScaler must process the logon using the existing credential set without going to the user. By using "passthrough"factors, an administrator can programmatically drive the authentication flow. Administrators are advised to read the nFactor specification or the deployment guides for further details. See
Multi-Factor (nFactor) authentication.

User name and password expressions

To process the login credentials, the administrator must configure the loginSchema. Single factor or dual factor use cases with few loginSchema customizations does not need a specified XML definition. The LoginSchema has other properties such as userExpression and passwdExpression that can be used to alter the user name or password that the user presents.

Login schemas are advanced policy expressions and can be used to override the user input as well. This can be achieved by appending a string for parameters in **-authenticationSchema** as shown in the following example.

Following are the examples to modify user inputs for user name and for password respectively.

- Change the user input for user name from `username@citrix.com` to `username@xyz.com`

```
add authentication loginSchema user_schema -authenticationSchema
    LoginSchema/DualAuth.xml -userExpression "AAA.LOGIN.USERNAME.
    BEFORE_STR(\"@\").APPEND(\"@xyz.com\")"
```

- Consider a scenario where the user provides a password and a passcode in the first factor as part of the login schema configured. To use the **passcode** provided by the user in the first factor and the **password** in the second factor, you can modify the existing login schema by using the following commands.

```
add authentication loginSchema user_schema -authenticationSchema
    LoginSchema/DualAuth.xml -passwdExpression "AAA.LOGIN.
    PASSWORD2"
```

```
add authentication loginSchema user_schema_second -
    authenticationSchema noschema  -passwdExpression "AAA.LOGIN.
    PASSWORD"
```

High-level steps in nFactor configuration

The following diagram illustrates the high-level steps involved in nFactor configuration.

GUI Configuration

The following topics are described in this section:

- Create a Virtual Server
- Create Authentication Virtual Server
- Create Authentication CERT Profile
- Create an Authentication Policy
- Add an LDAP authentication server
- Add an LDAP authentication policy
- Add a RADIUS authentication server
- Add a RADIUS Authentication Policy
- Create an Authentication Login Schema
- Create a Policy Label

Create a virtual server

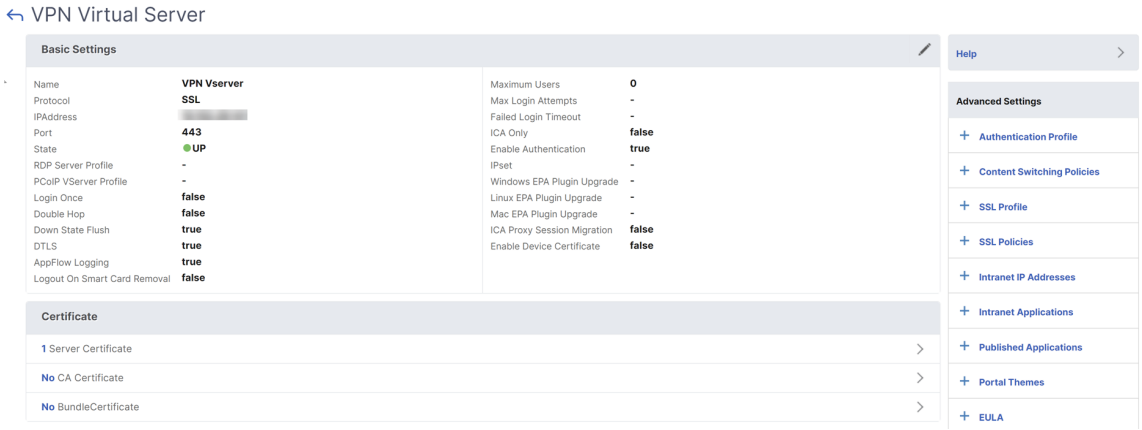
1. Navigate to **NetScaler Gateway > Virtual Servers.**

2. Click the **Add** button to create a gateway virtual server.
3. Enter the following information and click **OK**.

Parameter name	Parameter Description
Enter the Name of the virtual server.	Name for the NetScaler Gateway virtual server. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the virtual server is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, “my server”or ‘my server’).
Enter the IP Address Type for the virtual server	Select an IP Address or Non-addressable option from the drop-down menu.
Enter the IP Address of the virtual server.	An Internet Protocol address (IP address) is a numerical label assigned to each device participating in the computer network that uses the Internet Protocol for communication.
Enter the Port number for the virtual server.	Enter the port number.
Enter the Authentication Profile.	Authentication Profile entity on virtual server. This entity can be used to offload authentication to authentication, authorization, and auditing virtual server for multi-factor (nFactor) authentication
Enter the RDP Server Profile.	Name of the RDP server profile associated with the virtual server.
Enter the Maximum Users.	Maximum number of concurrent user sessions allowed on this virtual server. The actual number of users allowed to log on to this virtual server depends on the total number of user licenses.
Enter the Max Login Attempts.	Maximum number of logon attempts.
Enter the Failed Login Timeout.	Number of minutes an account is locked if the user exceeds the maximum permissible attempts.
Enter the Windows EPA plug-in Upgrade.	Option to set plug-in upgrade behavior for Win.

Parameter name	Parameter Description
Enter the Linux EPA plug-in upgrade.	Option to set plug-in upgrade behavior for Linux.
Enter the MAC EPA plug-in upgrade	Option to set plug-in upgrade behavior for Mac.
Login Once	This option enables/disables seamless SSO for this virtual server.
ICA Only	When set to ON, it implies Basic mode where the user can log on using either the Citrix Workspace app or a browser and get access to the published apps configured at the Citrix Virtual Apps and Desktops environment pointed out by the `Wihome` parameter. Users are not allowed to connect using the Citrix Secure Access client and end point scans cannot be configured. The numbers of users that can log in and access the apps are not limited by the license in this mode. - When set to OFF, it implies SmartAccess mode where the user can log on using either the Citrix Workspace app or a browser or a Citrix Secure Access client. The admin can configure end point scans to be run on the client systems and then use the results to control access to the published apps. In this mode, the client can connect to the gateway in other client modes namely VPN and clientless VPN. The numbers of users that can log in and access the resources are limited by the CCU licenses in this mode.
Enable Authentication	Require authentication for users connecting to NetScaler Gateway.
Double Hop	Use the NetScaler Gateway appliance in a double-hop configuration. A double-hop deployment provides an extra layer of security for the internal network by using three firewalls to divide the DMZ into two stages. Such a deployment can have one appliance in the DMZ and one appliance in the secure network.

Parameter name	Parameter Description
Down State Flush	Close existing connections when the virtual server is marked DOWN, which means the server might have timed out. Disconnecting existing connections frees resources and in certain cases speeds recovery of overloaded load balancing setups. Enable this setting on servers in which the connections can safely be closed when they are marked DOWN. Do not enable DOWN state flush on servers that must complete their transactions.
DTLS	This option starts/stops the turn service on the virtual server
AppFlow Logging	Log AppFlow records that contain standard NetFlow or IPFIX information, such as time stamps for the beginning and end of a flow, packet count, and byte count. Also log records that contain application-level information, such as HTTP web addresses, HTTP request methods and response status codes, server response time, and latency.
ICA Proxy Session Migration	This option determines if an existing ICA Proxy session is transferred when the user logs on from another device.
State	The current state of the virtual server, as UP, DOWN, BUSY, and so on.
Enable Device Certificate	Indicates whether the device certificate check as a part of EPA is on or off.



4. Select the **No Server Certificate** section of the page.
5. Click **>** under **Select Server Certificate** to select the server certificate.
6. Select the SSL Certificate and click the **Select** button.
7. Click **Bind**.
8. If you see a warning about **No usable ciphers**, click **OK**
9. Click the **Continue** button.
10. In the Authentication section, click the **+** icon in the top right.

Create an authentication virtual server

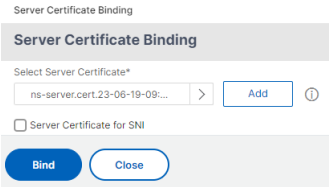
1. Navigate to **Security > AAA –Application Traffic > Virtual Servers.**
2. Click the **Add** button.
3. Complete the following Basic Settings to create the Authentication Virtual Server.

   Note: The * sign to the right of the setting name indicates mandatory fields.

   - Enter the **Name** for the new authentication virtual server.
   - Enter the **IP Address Type**. The IP Address Type can be configured as Non-addressable.
   - Enter the **IP Address**. The IP Address can be zero.
   - Enter the **Protocol** type of the authentication virtual server.
   - Enter the **TCP Port** on which the virtual server accepts connections.
   - Enter the **domain** of the authentication cookie set by the authentication virtual server.
4. Click **OK**.
5. Click the **No Server Certificate** section.

6. Click **>** under **Select Server Certificate**.
7. Choose the desired SSL Certificate and click the **Select** button.

   Note: The Authentication virtual server does not need a certificate bound to it.
8. Configure the **Server Certificate Binding**.
   - Check the **Server Certificate for SNI** box to bind one or more Cert keys used for SNI processing.
   - Click the **Bind** button.



Create an authentication CERT profile

1. Navigate to **Security > AAA –Application Traffic > Policies > Authentication > Basic Policies > CERT.**
2. Select the Profiles tab and then select **Add**.
3. Complete the following fields to create the Authentication CERT Profile. The * sign to the right of the setting name indicates mandatory fields.
   - **Name** - Name for the client cert authentication server profile (action).
   - **Two factor** –In this instance the two-factor authentication option is NOOP.
   - **User Name Field** –enter the client-cert field from which the user name is extracted. Must be set to either ‘“‘Subject’”’or ‘“‘Issuer’”’(include both sets of double quotation marks).
   - **Group Name Field** - enter the client-cert field from which the group is extracted. Must be set to either ‘“‘Subject’”’or ‘“‘Issuer’”’(include both sets of double quotation marks).
   - **Default Authentication Group** - This is the default group that is chosen when the authentication succeeds in addition to the extracted groups.
4. Click **Create**.

Create an authentication policy

> **Note**
>
> If you configure a first factor policy with a policy rule using AAA.login, then the following expression must be configured with OR condition for Citrix Workspace app to support the nFactor deployment.
>
> `|| HTTP.REQ.URL.CONTAINS("/cgi/authenticate")`

1. Navigate to **Security > AAA –Application Traffic > Policies > Authentication > Advanced Policies > Policy.**
2. Select the **Add** button
3. Complete the following information to create an authentication policy. The * sign to the right of the setting name indicates mandatory fields.

   a) **Name** –enter the Name for the advance AUTHENTICATION policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the authentication policy is created.

   The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy"or 'my authentication policy').

   b) **Action Type** - enter the type of the Authentication Action.

   c) **Action** - enter the name of the authentication action to be performed if the policy matches.

   d) **Log Action** - enter the name of the message log action to use when a request matches this policy.

   e) **Expression** - enter the name of the NetScaler named rule, or a default syntax expression, that the policy uses to determine whether to attempt to authenticate the user with the AUTHENTICATION server.

   f) **Comments** –enter any comments to preserve information about this policy.
4. Click **Create**

Add an LDAP authentication server

1. Navigate to **Security > AAA –Application Traffic > Policies > Authentication > Basic Policies > LDAP.**
2. Add an LDAP server by selecting the **Server** tab and selecting the **Add** button.

Add an LDAP authentication policy

1. Go to **Security > AAA –Application Traffic > Policies > Authentication > Advanced Policies > Policy**.
2. Click **Add** to add an Authentication Policy.
3. Complete the following information to Create an Authentication Policy. The * sign to the right of the setting name indicates mandatory fields.

   a) **Name** - Name for the advance AUTHENTICATION policy.
   Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the authentication policy is created.

   The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy"or 'my authentication policy').

   b) **Action Type** - Type of the Authentication Action.

   c) **Action** - Name of the authentication action to be performed if the policy matches.

   d) **Log Action** - Name of message log action to use when a request matches this policy.

   e) **Expression** - Name of the NetScaler named rule, or a default syntax expression, that the policy uses to determine whether to attempt to authenticate the user with the AUTHENTICATION server.

   f) **Comments** - Any comments to preserve information about this policy.
4. Click **Create.**

Add a RADIUS authentication server

1. Navigate to **Security > AAA –Application Traffic > Policies Authentication > Basic Policies > RADIUS**.
2. To add a Server select the **Servers** tab and select the **Add** button.
3. Enter the following to create an Authentication RADIUS Server. The * sign to the right of the setting name indicates mandatory fields.

   a) Enter a **Name** for the RADIUS Action.

   b) Enter the **Server Name** or **Server IP** Address assigned to the RADIUS server.

   c) Enter the **Port** number on which the RADIUS server listens for connections.

d) Enter the **Time-out** value in few seconds. The NetScaler appliance waits for a response from the RADIUS server until the configured timeout value expires.

e) Enter the **Secret Key** that is shared between the RADIUS server and the NetScaler appliance. The Secret Key is required to allow the NetScaler appliance to communicate with the RADIUS server.

f) **Confirm the Secret Key**.

4. Click **Create.**

Add a RADIUS authentication policy

1. Navigate to **Security > AAA –Application Traffic > Policies > Authentication > Advanced Policies > Policy.**
2. Click **Add** to create an Authentication Policy.
3. Complete the following information to create an authentication policy. The * sign to the right of the setting name indicates mandatory fields.

   a) **Name** - Name for the advance AUTHENTICATION policy.
   Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space (), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the AUTHENTICATION policy is created.

   The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, “my authentication policy”or ‘my authentication policy’).

   a) **Action Type** - Type of the Authentication Action.

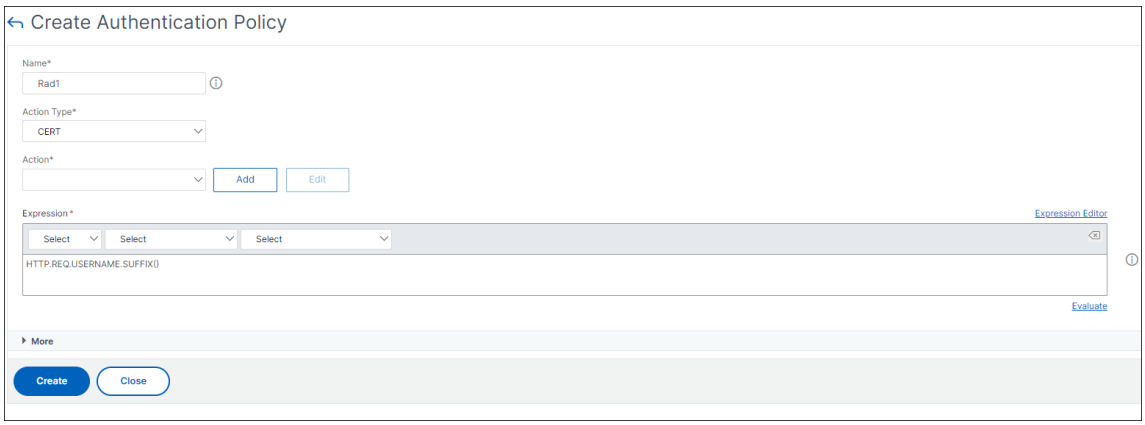
   b) **Action** - Name of the authentication action to be performed if the policy matches.

   c) **Log Action** - Name of message log action to use when a request matches this policy.

   d) **Expression** - Name of the NetScaler named rule, or a default syntax expression, that the policy uses to determine whether to attempt to authenticate the user with the AUTHENTICATION server.

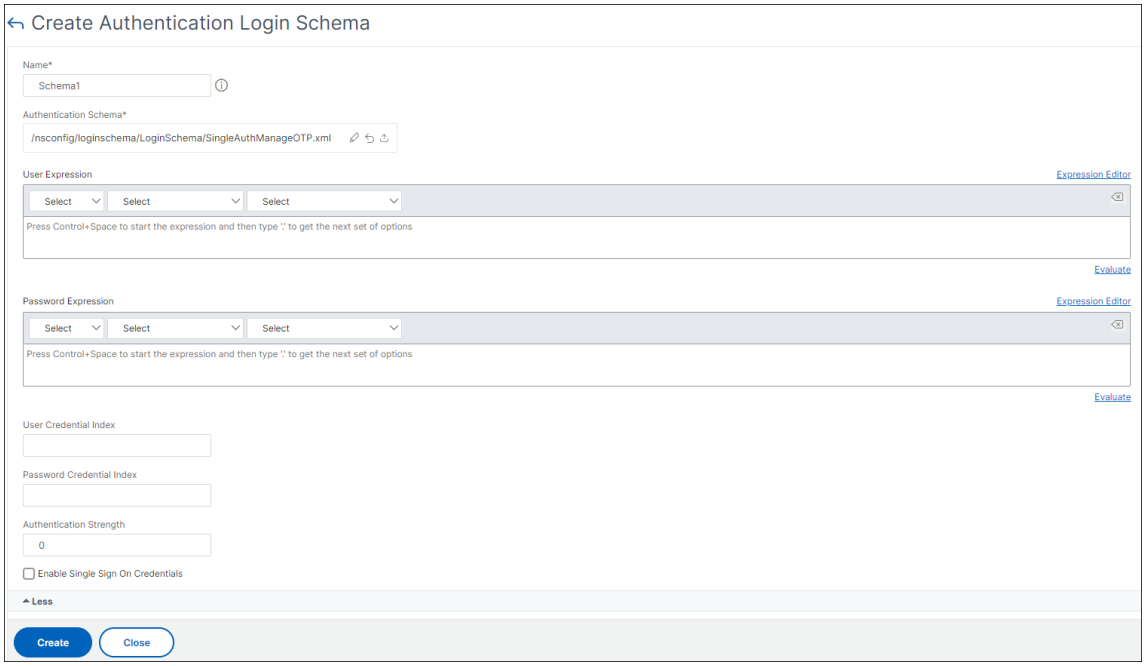
   e) **Comments** - Any comments to preserve information about this policy.

4. Click **OK.** The authentication policy that you created is listed in the list of policies.



Create an Authentication Login Schema

1. Navigate to **Security > AAA –Application Traffic > Login Schema.**
2. Select the Profiles tab and Click the **Add** button.
3. Complete the following fields to create an authentication login schema:
   a) Enter **Name** –Name for the new login schema.
   b) Enter **Authentication Schema** - Name of the file for reading the authentication schema to be sent for Login Page UI. This file must contain the xml definition of the elements as per the Citrix Forms Authentication Protocol to be able to render a login form. If an administrator does not want to prompt users for more credentials but continue with previously obtained credentials, then "noschema"can be given as an argument. This applies only to loginSchemas that are used with user-defined factors, and not the virtual server factor
   c) Enter **User Expression** - Expression for user name extraction during login
   d) Enter **Password Expression** - Expression for password extraction during login
   e) Enter **User Credential Index** - An index at which the user entered user name is stored in session.
   f) Enter **Password Credential Index** - An index at which the user entered password must be stored in session.
   g) Enter **Authentication Strength** - Weight of the current authentication.
4. Click **Create.** The login schema profile that you created must appear in the login schema profile list.

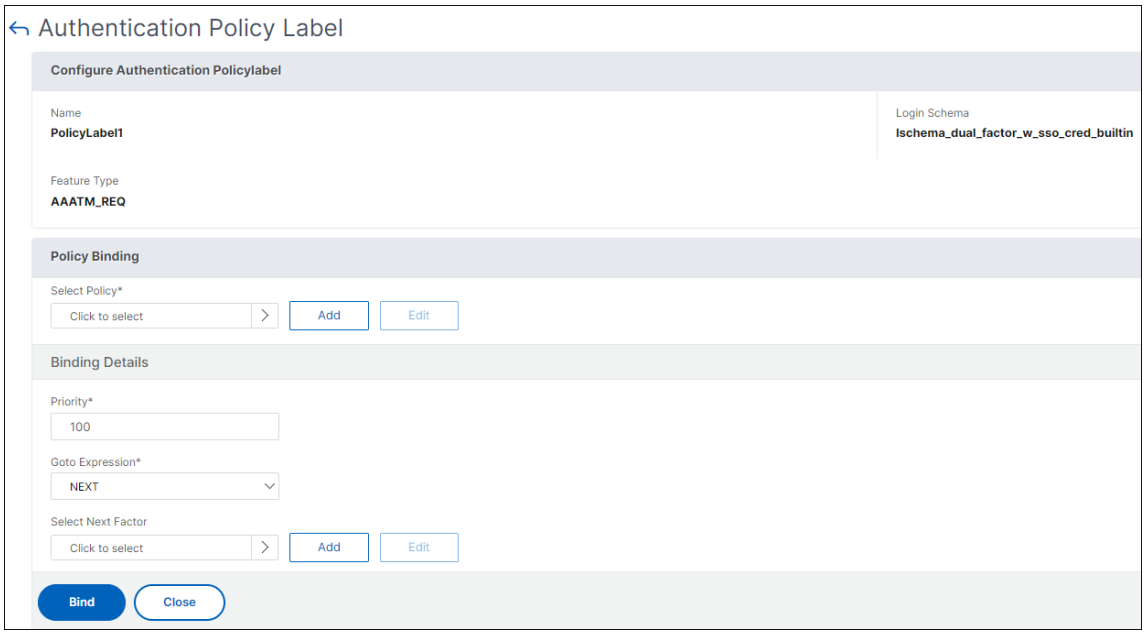


Create a policy label

A policy label specifies the authentication policies for a particular factor. Each policy label corresponds to a single factor. The policy label specifies the login form that must be presented to the user. The policy label must be bound as the next factor of an authentication policy or of another authentication policy label. Typically, a policy label includes authentication policies for a specific authentication mechanism. However, you can also have a policy label that has authentication policies for different authentication mechanisms.

1. Navigate to **Security > AAA –Application Traffic > Policies > Authentication > Advanced Policies > Policy Label.**
2. Click the **Add** button.
3. Complete the following fields to create an authentication policy label:
   a) Enter the **Name** for the new authentication policy label.
   b) Enter the **Login Schema** associated with the authentication policy label.
   c) Click **Continue**.
4. **Select a Policy** from the drop-down menu.
5. Choose the desired **Authentication Policy** and click the **Select** button.
6. Complete the following fields:
   a) Enter the **Priority** of the policy binding.

b) Enter the **Goto Expression** –the expression specifies the priority of the next policy that will be evaluated if the current policy rule evaluates to TRUE.



7. Select the desired Authentication Policy and click the **Select** button.
8. Click the **Bind** button.
9. Click **Done**.
10. Review the Authentication Policy Label.

re-Captcha configuration for nFactor authentication

Starting from NetScaler release 12.1 build 50.x, NetScaler Gateway supports a new first class action 'captchaAction'that simplifies Captcha configuration. As Captcha is a first class action, it can be a factor of its own. You can inject Captcha anywhere in the nFactor flow.

Previously, you had to write custom WebAuth policies with changes to the RfWebUI as well. With the introduction of captchaACtion, you do not have to modify the JavaScript.

> **Important**
>
> If Captcha is used along with user name or password fields in the schema, the Submit button is disabled until Captcha is met.

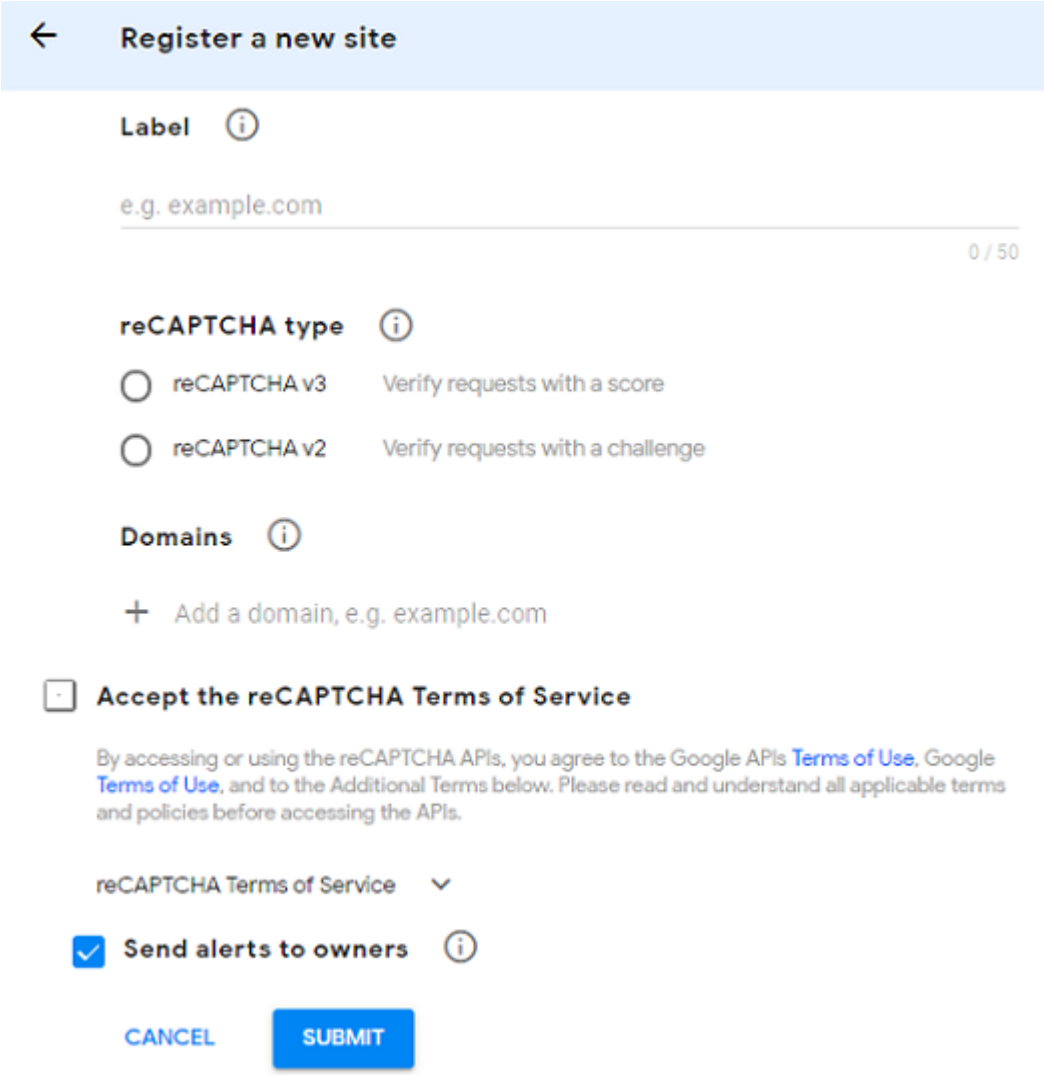
Captcha configuration

Captcha configuration involves two parts.

1. Configuration on Google for registering Captcha.
2. Configuration on NetScaler appliance to use Captcha as part of login flow.

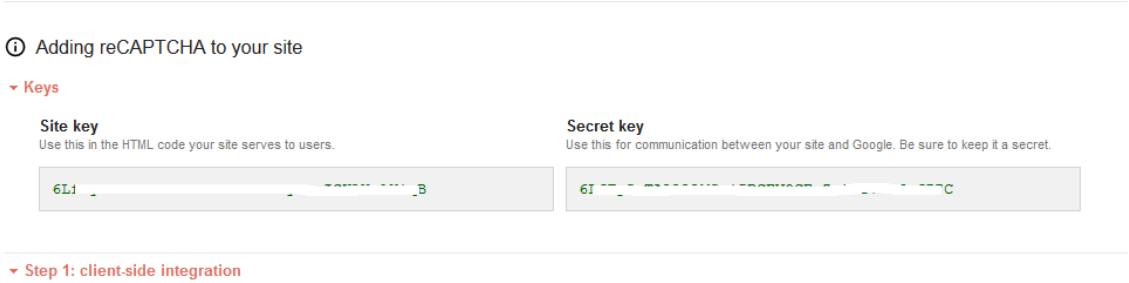
Captcha configuration on Google Register a domain for Captcha at `https://www.google.com/recaptcha/admin#list`.

1. When you navigate to this page, the following screen appears.



> **Note**
>
> Use `reCAPTCHA` v2 only. Invisible `reCAPTCHA` is still in preview.

2. After a domain is registered, the “SiteKey”and “SecretKey”are displayed.



> **Note**
>
> The "SiteKey"and "SecretKey"are grayed out for security reasons. "SecretKey"must be kept safe.

Captcha configuration on the NetScaler appliance Captcha configuration on the NetScaler appliance can be divided into three parts:

- Display Captcha screen
- Post the Captcha response to Google server
- LDAP configuration is second factor for user logon (optional)

Display Captcha screen The login form customization is done through the SingleAuthCaptcha.xml login schema. This customization is specified at the authentication virtual server and is sent to UI for rendering the login form. The built-in login schema, SingleAuthCaptcha.xml, is at `/nsconfig/loginSchema/LoginSchema` directory on the NetScaler appliance.

> **Important**
>
> - Based on your use case and different schemas, you can modify the existing schema. For instance if you need only Captcha factor (without user name or password) or dual authentication with Captcha.
> - If any custom modifications are performed or the file is renamed, Citrix recommends copying all login schemas from the /nsconfig/loginschema/LoginSchema directory to the parent directory, /nsconfig/loginschema.

To configure display of Captcha using CLI

```
- add authentication loginSchema singleauthcaptcha -
  authenticationSchema /nsconfig/loginschema/SingleAuthCaptcha.xml

- add authentication loginSchemaPolicy singleauthcaptcha -rule true -
  action singleauthcaptcha

- add authentication vserver auth SSL <IP> <Port>

```



```
- add ssl certkey vserver-cert -cert <path-to-cert-file> -key <path-to-key-file>
- bind ssl vserver auth -certkey vserver-cert
- bind authentication vserver auth -policy singleauthcaptcha -priority 5 -gotoPriorityExpression END
```

Post the Captcha response to Google server After you have configured the Captcha that must be displayed to the users, the admins post the configuration to the Google server to verify the Captcha response from the browser.

To verify the Captcha response from the browser

```
- add authentication captchaAction myrecaptcha -sitekey <sitekey-copied-from-google> -secretkey <secretkey-from-google>

- add authentication policy myrecaptcha -rule true -action myrecaptcha
- bind authentication vserver auth -policy myrecaptcha -priority 1
```

The following commands are required to configure if AD authentication is desired. Else, you can ignore this step.

```
- add authentication ldapAction ldap-new -serverIP x.x.x.x -serverPort 636 -ldapBase "cn=users,dc=aaatm,dc=com" -ldapBindDn adminuser@aaatm.com -ldapBindDnPassword <password> -encrypted -encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName memberof -subAttributeName CN -secType SSL -passwdChange ENABLED -defaultAuthenticationGroup ldapGroup

- add authenticationpolicy ldap-new -rule true -action ldap-new
```

LDAP configuration is second factor for user logon (optional) The LDAP authentication happens after Captcha, you add it to the second factor.

```
- add authentication policylabel second-factor
- bind authentication policylabel second-factor -policy ldap-new -priority 10
- bind authentication vserver auth -policy myrecaptcha -priority 1 -nextFactor second-factor
```

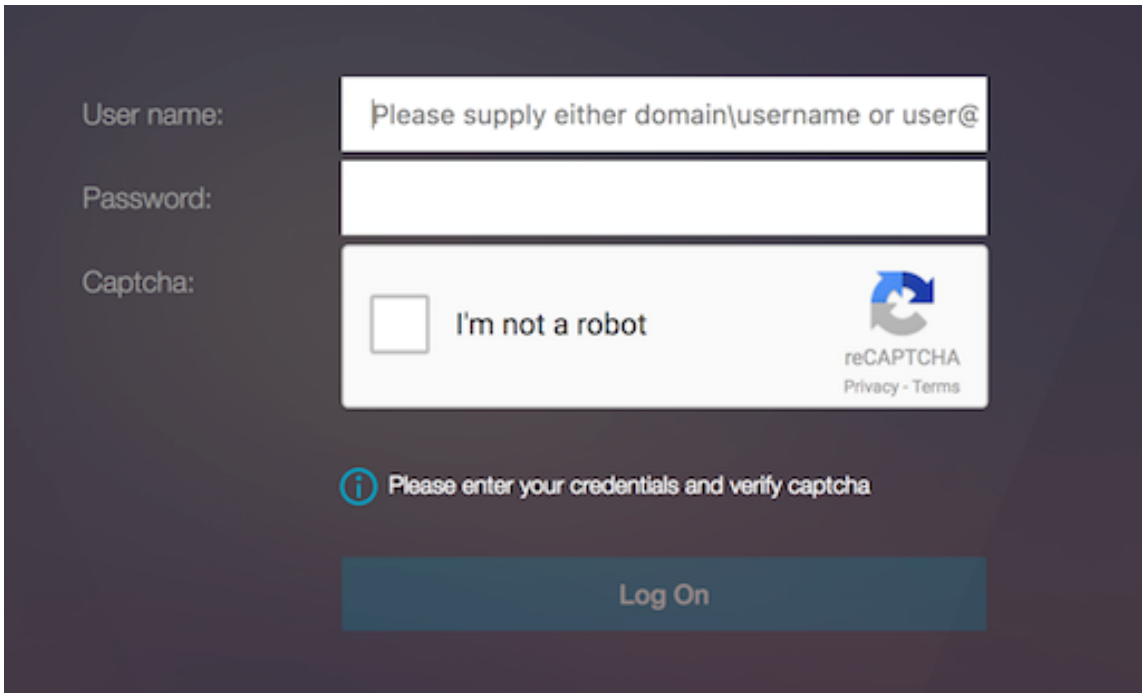
Administrator needs to add appropriate virtual servers depending on whether load balancing virtual server or NetScaler Gateway appliance is used for access. Administrator must configure the following command if a load balancing virtual server is required:

```
add lb vserver lbtest HTTP <IP> <Port> -authentication ON -authenticationHost nssp.aaatm.com`
```

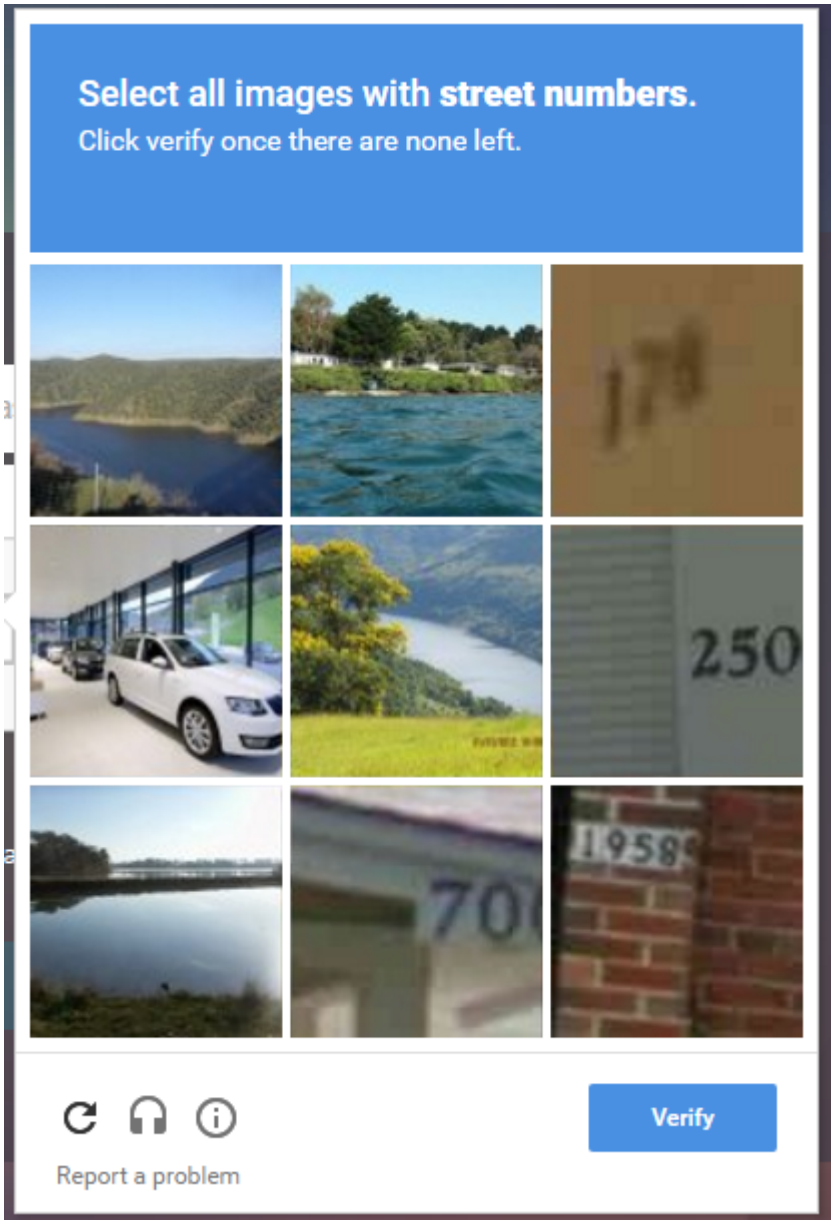
nssp.aaatm.com –Resolves to authentication virtual server.

User validation of Captcha Once you have configured all the steps mentioned in the previous sections, see the preceding user interface screen captures.

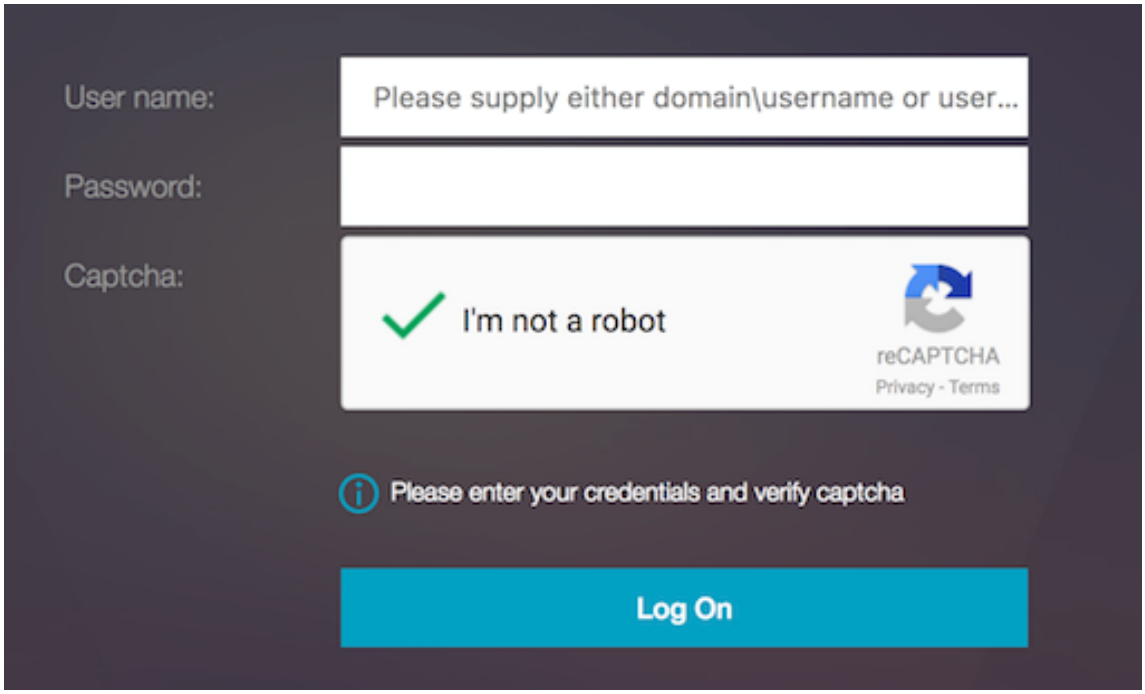
1. Once the authentication virtual server loads the login page, the logon screen is displayed. **Log On** is disabled until Captcha is complete.



2. Select I'm not a robot option. The Captcha widget is displayed.



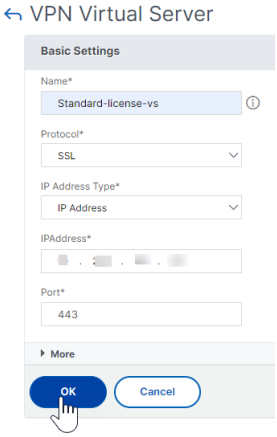
3. You are navigated through a series of Captcha images, before the completion page is displayed.
4. Enter the AD credentials, select the **I'm not a robot** check box and click **Log On**. If authentication succeeds, you are redirected to the desired resource.



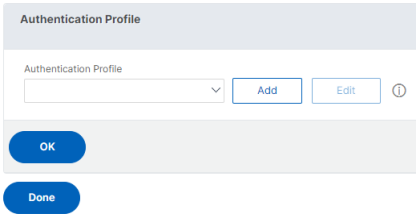
> **Note:**
>
> - If Captcha is used with AD authentication, the Submit button for credentials is disabled until Captcha is complete.
> - The Captcha happens in a factor of its own. Therefore, any subsequent validations like AD must happen in the `nextfactor` of Captcha.

Create a Gateway virtual server for nFactor authentication in NetScaler Standard license

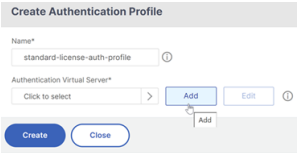
1. Navigate to **NetScaler Gateway > Virtual Servers**.
2. On the **NetScaler Gateway Virtual Servers** page, click **Add**.
3. Enter the following details on the **VPN Virtual Server** page, click **OK**, and click **Continue**.
   - Name - Name of the NetScaler Gateway virtual server
   - Protocol - Select **SSL**
   - IP Address - IP address of NetScaler Gateway virtual server
   - Port - Enter 443



1. On the **VPN Virtual Server** page, click the plus icon next to **Authentication Profile**.
2. Click **Add** to configure the authentication profile.

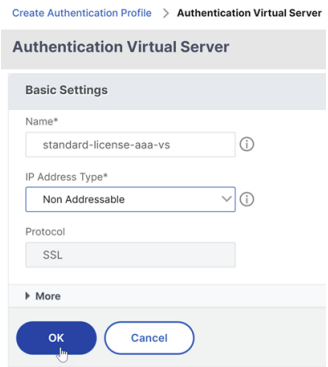


3. Enter a name for the authentication profile and click **Add**.



4. Enter the following details on the **VPN Virtual Server** page, click **OK,** and click **Continue**.

   - Name - Name of the authentication, authorization, and auditing virtual server
   - Protocol - Select **Non Addressable**. Only a non-addressable authentication, authorization, and auditing virtual server can be bound to a Gateway/VPN virtual server in NetScaler Standard license.



> **Note:**
>
> - In the NetScaler Standard license, the steps for creating policy are the same as the Premium License for supported policy types.
> - NetScaler Standard license does not support an addition of new login schemas in the nFactor configuration.

References

For an end-to-end nFactor configuration example, see Configuring nFactor authentication.

Unified Gateway Visualizer

January 8, 2024

The Unified Gateway Visualizer provides a visual representation of the configurations using the Unified Gateway Wizard. The Unified Gateway Visualizer is used to add and edit configuration, and diagnose a back-end issue.

The Unified Gateway Visualizer shows the following:

Configuration	Configuration
Pre-authentication policies	Authentication policies
CS virtual servers	VPN virtual servers
LB virtual servers	XA/XD apps
Web apps	SaaS apps

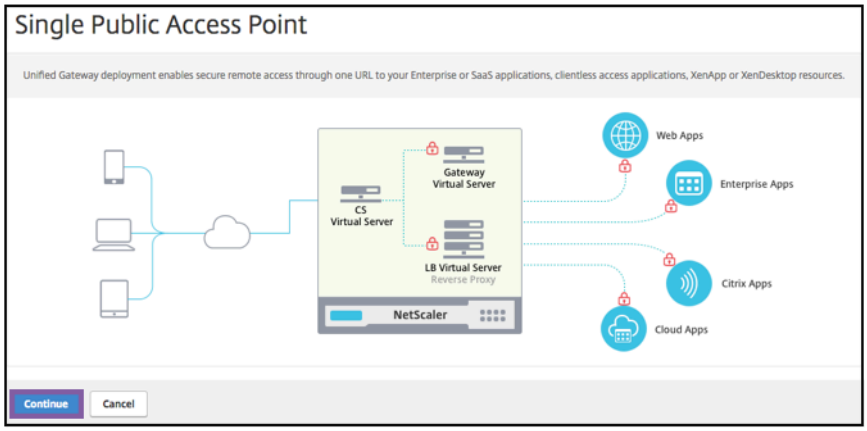
Unified Gateway deployment enables secure remote access through one URL to your Enterprise or SaaS applications, clientless access applications, Citrix Virtual Apps, and Desktops resources.

Configure Unified Gateway

1. Select Unified Gateway from the menu.
2. At the next screen, verify that you have the following information, then click **Get Started**:
    - Public IP address for the Unified Gateway.

- Server certificate chain (.PFX or.PEM) with optional Root-CA certificate.
- LDAP/RADIUS/Client Certificate based authentication details.
- Application details (URLs for SaaS applications or Citrix Virtual Apps and Desktops server details).

3. Click the **Continue** button.

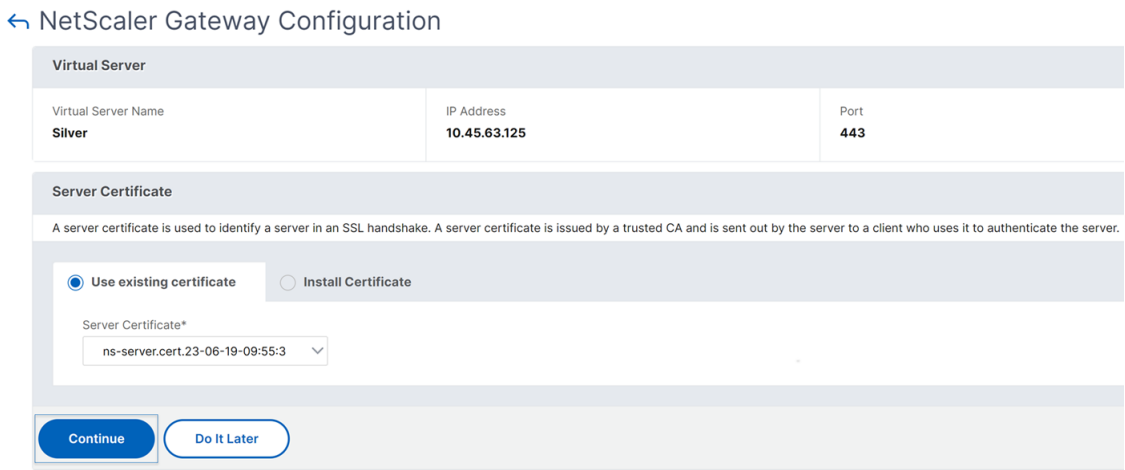


Create a Unified Gateway Configuration virtual server.

1. Enter the configuration **Name** for the virtual server.
2. Enter the public facing **Unified Gateway IP address** for the Unified Gateway deployment.
3. Enter the fully qualified domain name (**FQDN**) for the Unified Gateway deployment.
4. Enter the **Port** number. The port number range is 1–65535.
5. Click **Continue**.

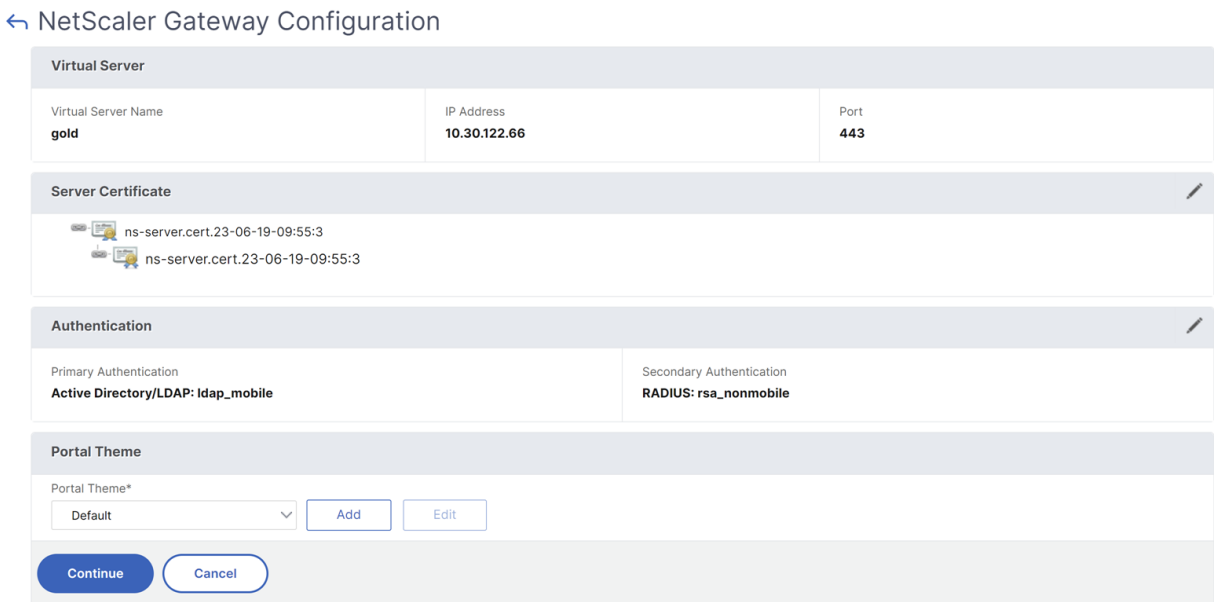
Complete the following information to specify the Server Certificate.

1. Select either the **Use existing certificate** or **Install Certificate** radio buttons.
2. Select a **Server Certificate** from the menu.
3. Click the **Continue** button.



Complete the following information to specify Authentication.

1. Select a **Primary authentication method** from the menu.
2. Select either the **Use existing server** or **Add new server** radio buttons to specify the primary authentication server details.
3. Select a **Secondary authentication method** from the menu.
4. Select either the **Use existing server** or **Add new server** radio buttons to specify the secondary authentication server details.
5. Click the **Continue** button.
6. Select the **Portal Theme** from the menu.
7. Click **Continue**.
8. Select either the **Web Application** or **Citrix Virtual Apps Desktops** radio buttons.
9. Click **Continue**.



Select application

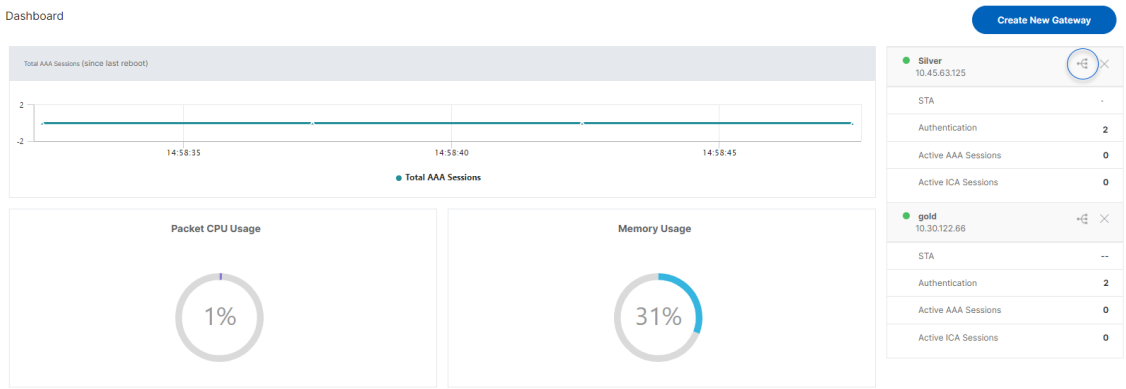
Complete the following information to specify Web Application.

1. Enter the Name of the bookmark link.
2. Select the type of application the VPN URL represents. The possible values are:
   - Intranet Application
   - Clientless Access
   - SaaS
   - PreConfigured application on this NetScaler
3. Check this box to make this application accessible through the Unified Gateway URL.
4. Enter the URL for the bookmark link.

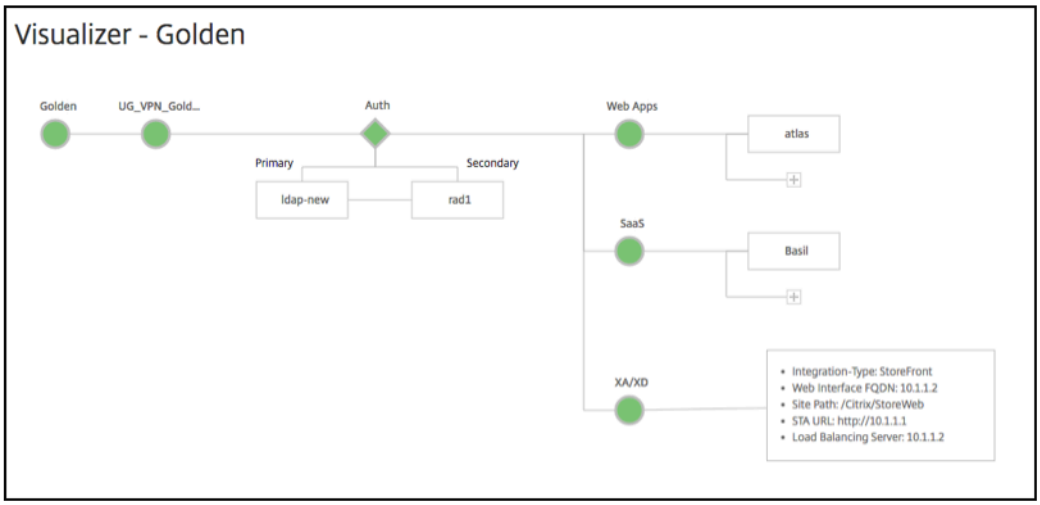
5. From the Icon URL choose a file to fetch an icon file. The MaxLength = 255
6. Click the **Continue** button.
7. Click **Done**.
8. Click **Continue**.
9. Click **Done**.

GUI Configuration

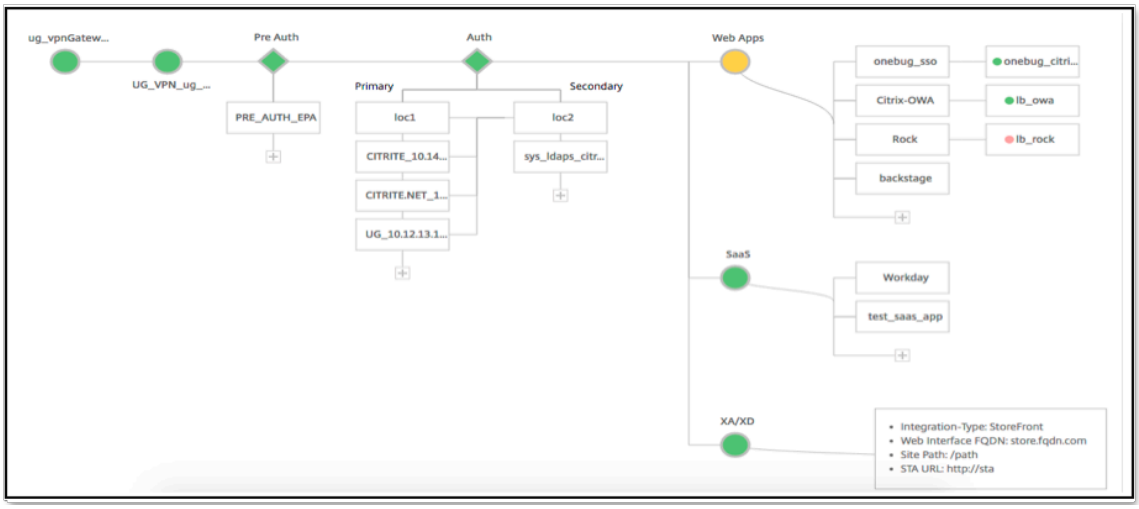
1. Select Unified Gateway from the menu.
2. Click the **Unified Gateway Visualizer** icon to access configured Gateway instances.



The Unified Gateway Visualizer looks like a flow diagram as shown in the following image:



The Unified Gateway Visualizer has PreAuth, `Auth`, and an Apps section. If the VPN virtual server has pre-authentication policy, only then the `pre-auth` is shown in the Unified Gateway Visualizer.



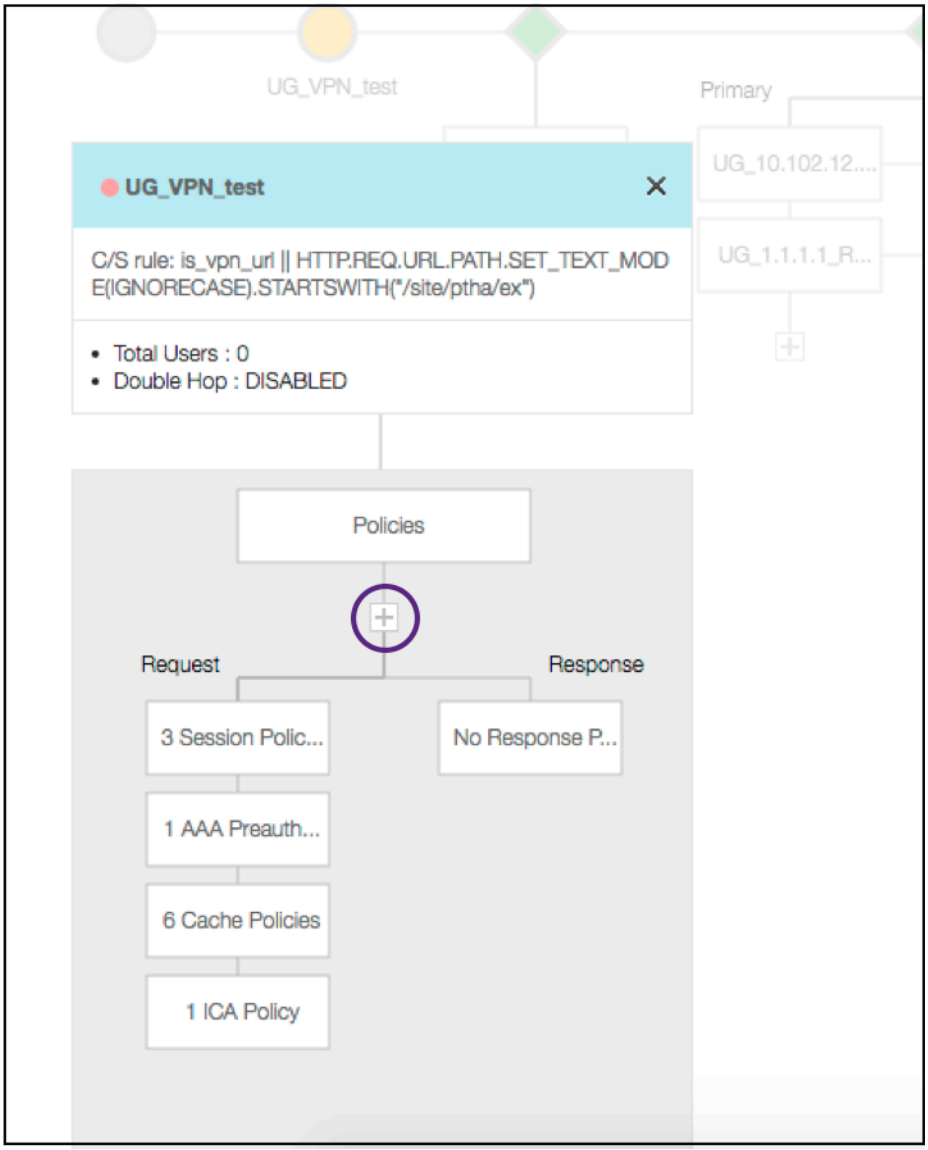
The Unified Gateway Visualizer uses a color coding scheme for the load balancing and VPN virtual servers to indicate their state.

Color	Description
Red	means the server is down.
Gray	means webapps/Citrix Virtual Apps have not been configured.
Green	means everything is fine with the virtual server.
Orange	means one of the load balancing virtual server services. is down, but still it is functioning properly.

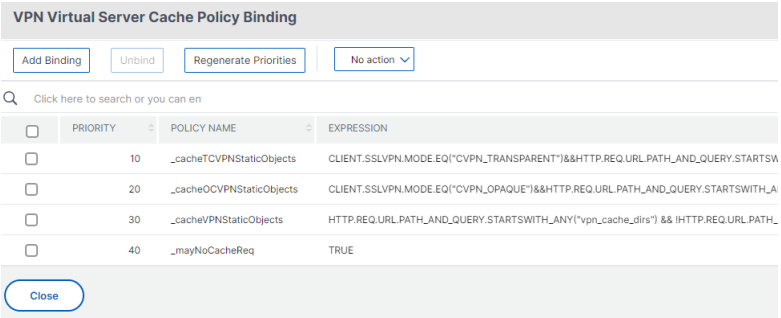
Details of VPN Virtual Servers

To get the details of the VPN virtual servers, click the **VPN virtual servers node**. The popup renders details like the C/S rule and all policies.

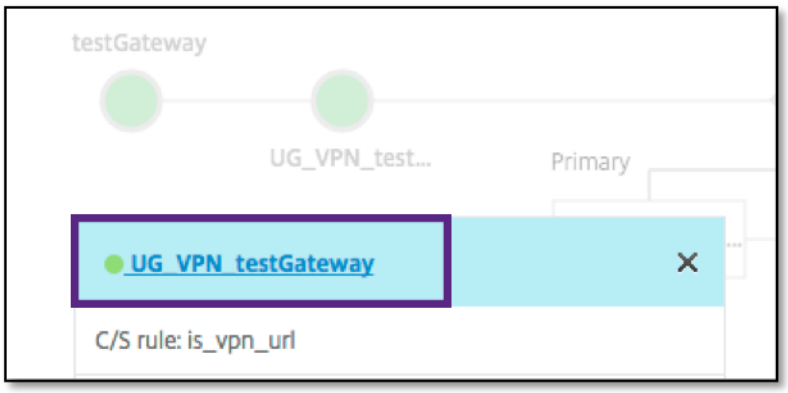
1. Add Policies to the VPN entity by clicking the (+) icon.



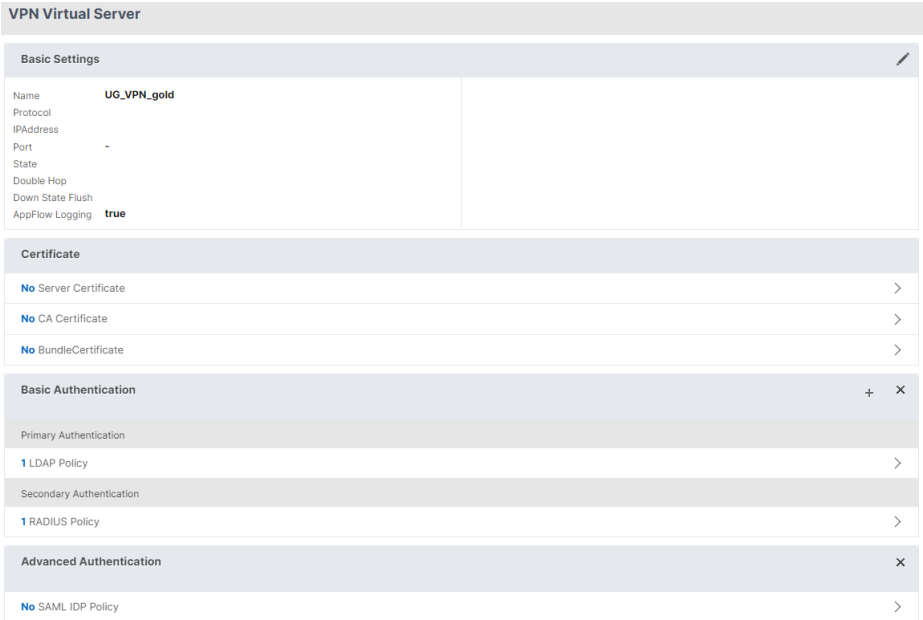
2. Click the desired node for details of policies already configured.



For VPN virtual server information, the VPN title in the popup is a clickable entity that goes to a slider that details the VPN virtual server.



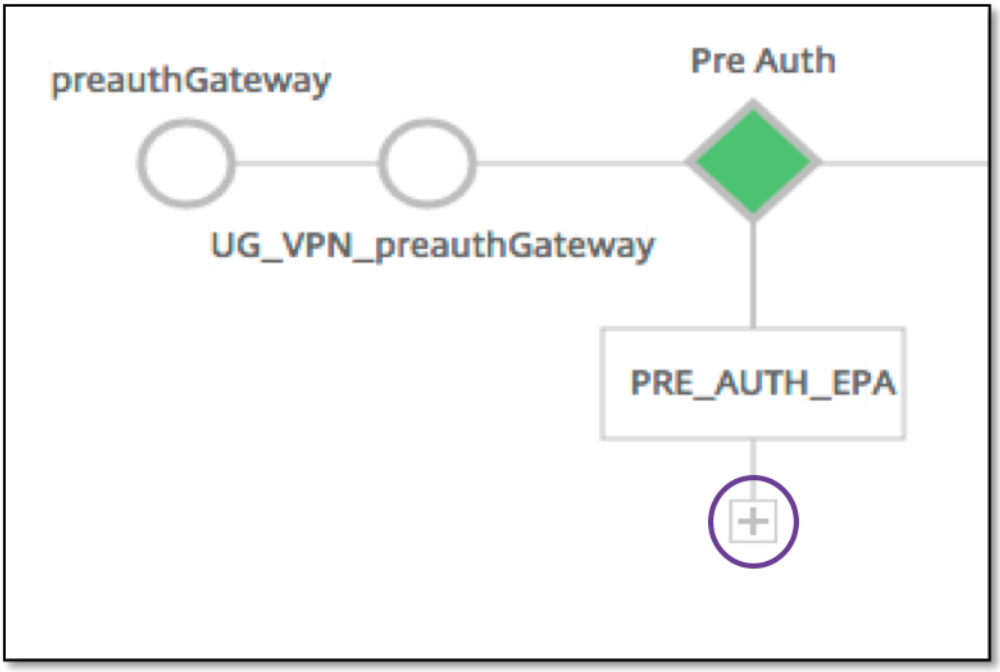
The details of the VPN server are shown here.



The `Pre Auth` Block

If a VPN virtual server has preauthentication policies associated with it, the Unified Gateway Visualizer shows a `Pre Auth` block. The `Pre Auth` block shows the policies, and provides an option to add preauthentication policies to the VPN.

1. Click the **+** to add a `preauth` policy.

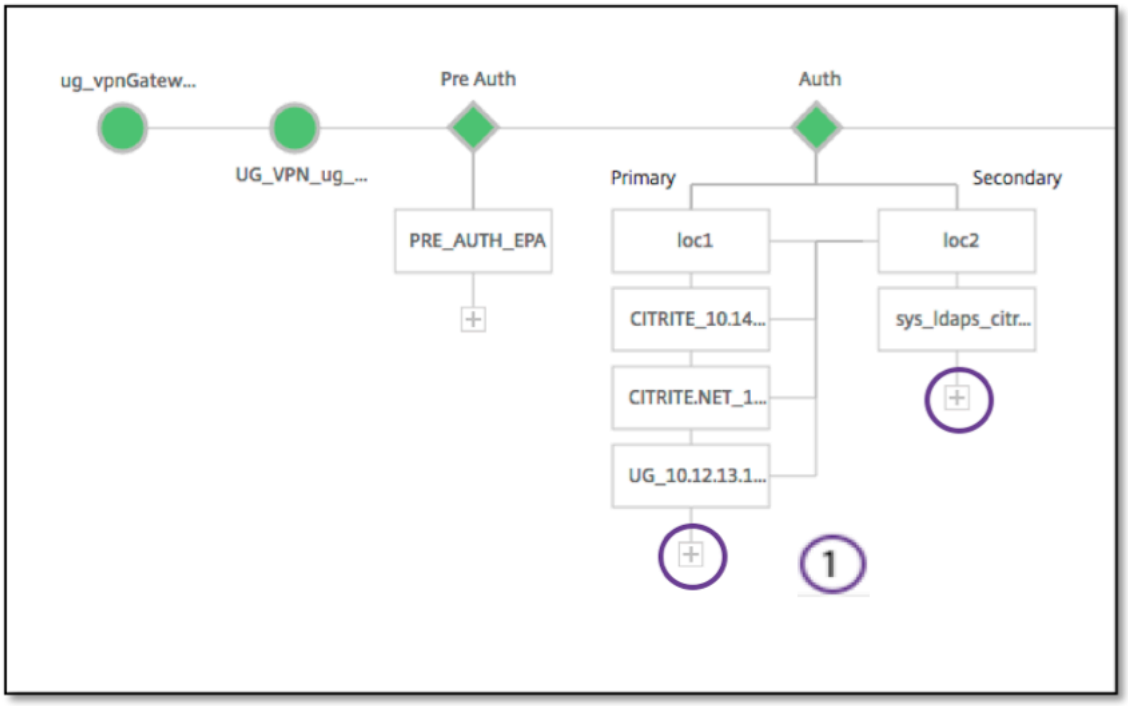


In a case where no preauthentication policies are associated, this block would be hidden from the view.

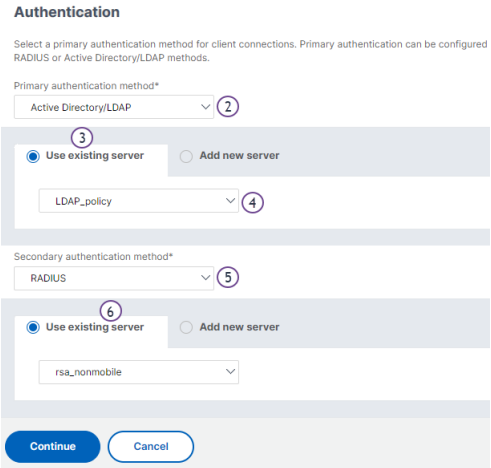
The Auth Block

The Auth block lists the primary and secondary policies. The Auth block provides an option to add policies.

1. Click **+** in the Primary list to add a Primary Authentication Binding or Click + in the Secondary list to add a Secondary Authentication Binding.



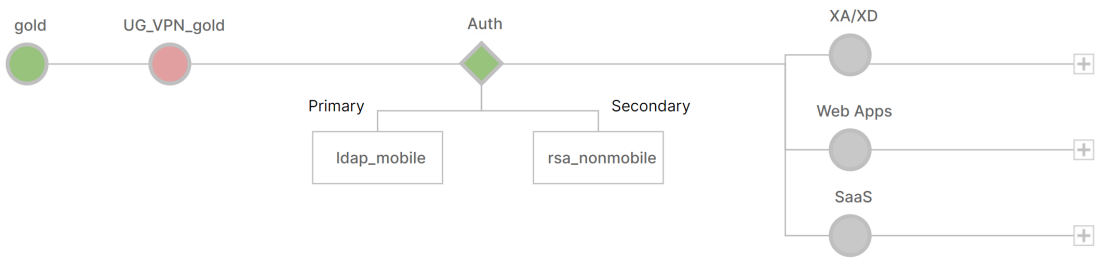
2. Select an option from the **Primary authentication method** menu.
3. Specify if it is an **existing server** or **Add new server** by selecting the radio button.
4. Select an option from the **LDAP Policy Name** menu.
5. Select **RADIUS** from the **Secondary authentication method** menu.
6. Specify if you want to **use existing server** or **Add new server** by selecting the radio button.
7. Click **Continue**.



Adding StoreFront

1. Click **+** near the XA/XD, and it takes you to adding “XA/XD”apps.

Visualizer - gold



You can choose your integration point. The options are StoreFront, WI, or WionNS. Click **Continue**.

1. Complete the following fields to configure StoreFront. The fields that require mandatory information are noted with the *.

Field	Description
StoreFront FQDN*	Enter the FQDN of the StoreFront server. Max length: 255 char.Example://storefront.xendt.net
Site Path*	Enter the path to Receiver for the website already configured on the StoreFront.
`Single Sign-on Domain`*	Enter the default domain for user authentication
Store Name*	Enter the name for the StoreFront monitors.
The STORENAME is an argument defining the StoreFront service store name to probe the health of StoreFront servers. Applicable to StoreFront monitors. Maximum Length: 31	
Secure Ticket Authority Server*	Enter the Secure Ticket Authority URL, typically present on the delivery controller.
Example: `http://sta`	
StoreFront Server*	Enter the IP Address of the StoreFront Server
Protocol*	Enter the protocol used by the server.
Port*	Enter the port used by the server.
Load Balancing	Enter the load balancing configuration for the StoreFront servers.
Virtual Server*	Enter the public facing IP address for the Unified Gateway deployment.

2. Click **Continue.**

Adding SaaS

1. Click **+** to add SaaS apps, it takes you to the Add SaaS page. Complete the following fields to configure SaaS. The fields that require mandatory information are noted with a*.

Field	Description
Name*	Enter the name of the bookmark link.
Application Type	Enter the type of application this VPN URL represents. Possible values are: Intranet Application/Clientless Access/SaaS/PreConfigured application on this NetScaler
Enter URL*	Enter URL of the Intranet application.
Choose **File**	Enter the URL to fetch the icon file for displaying this resource. MaxLength = 255

Adding WebApps

1. Click **+** to add Web apps, it takes you to the Add Web apps page. Complete the following fields to configure a Web Application. The fields that require mandatory information are noted with a *.

Field	Description
Name*	Enter the name of the bookmark link.
Application Type	Enter the type of application this VPN URL represents. Possible values are: Intranet Application/Clientless Access/SaaS/PreConfigured application on this NetScaler
Enter URL*	Enter URL of the Intranet application.
Choose **File**	Enter the URL to fetch the icon file for displaying this resource.MaxLength = 255

If an application is accessible through the Unified Gateway URL, the details of the Load Balancing server can be accessed by clicking the app:

New policies can be added by clicking (+) and all the bound policies can be viewed by clicking the node that displays policy information.

The number of services bound to the load balancer are also shown, along with the overall state information. Further click lists all the services. New services can be added to the load balancer.

For further details of the load balancer, the title of the popup is clickable that lands to the load balancing virtual server details page.

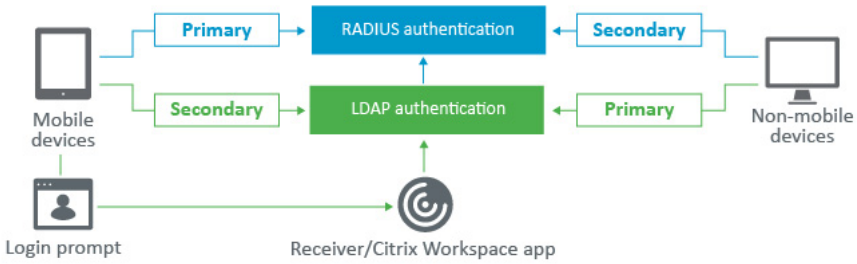
Configure NetScaler Gateway to use RADIUS and LDAP Authentication with Mobile/Tablet Devices

January 8, 2024

This section describes how to configure the NetScaler Gateway appliance to use RADIUS authentication as primary and LDAP authentication as secondary with mobile/tablet devices.

The configuration demonstrated in the section still allows all other connections to use LDAP first and RADIUS second.

When you configure two-factor authentication on the Citrix Workspace app for use with mobile/tablet devices, you must add the RSA SecureID (RADIUS authentication) as the primary authentication. But when the users get the prompt for user name and Password, Passcode on Receiver they are putting LDAP first and RADIUS as second credentials. From an administrator point of view it is a different configuration as compared to a non-mobile configuration.



Complete the following procedure to configure the NetScaler Gateway appliance to use RADIUS authentication as primary and LDAP authentication as secondary with mobile/tablet devices.

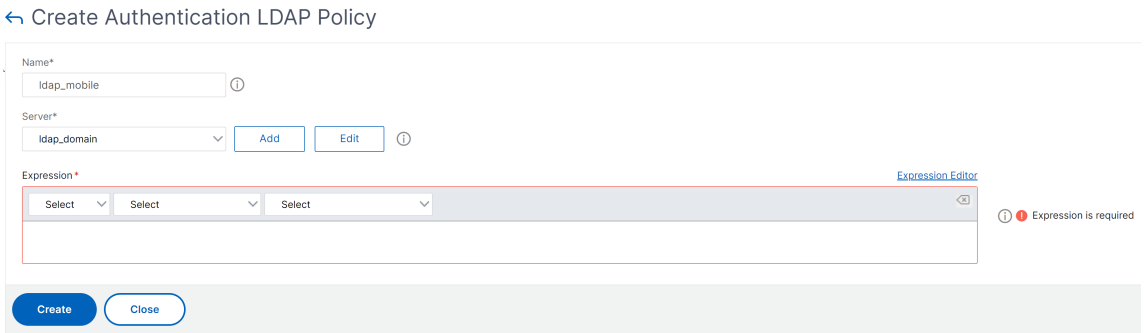
1. From the Configuration Utility, select **NetScaler Gateway > Policies > Authentication** and create an authentication policy for LDAP and RSA for mobile devices and non-mobile devices. This is necessary to avoid a logic condition that can allow users to bypass the RADIUS authentication.
2. Enter LDAP Server details after clicking the **Add** option under the **Servers** tab for LDAP.
3. Create an LDAP policy for the mobile devices by choosing the required LDAP Server.

   To bind this policy to only mobile devices, use the following expression:

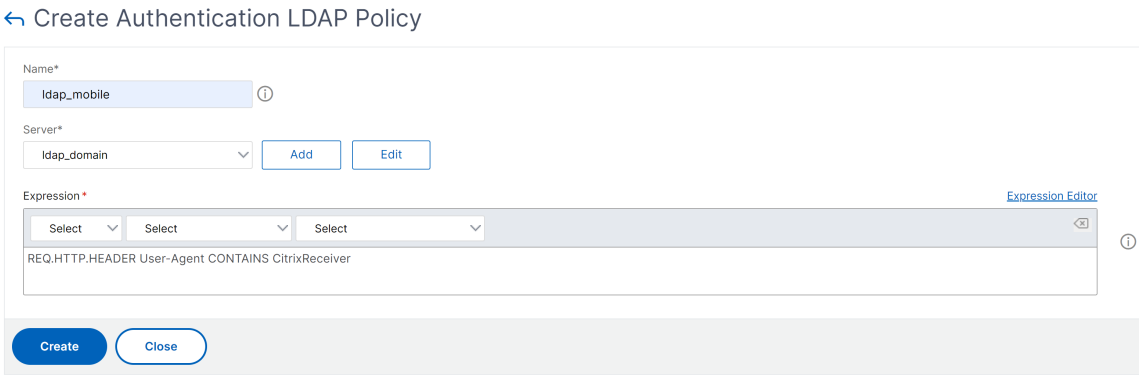
   ```
   REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver
   ```

   The corresponding advanced expression is:

   ```
   HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")
   ```

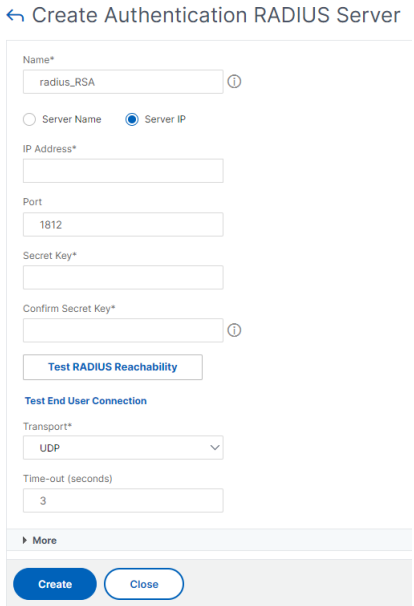


4. Click **Expression Editor** to create policy:

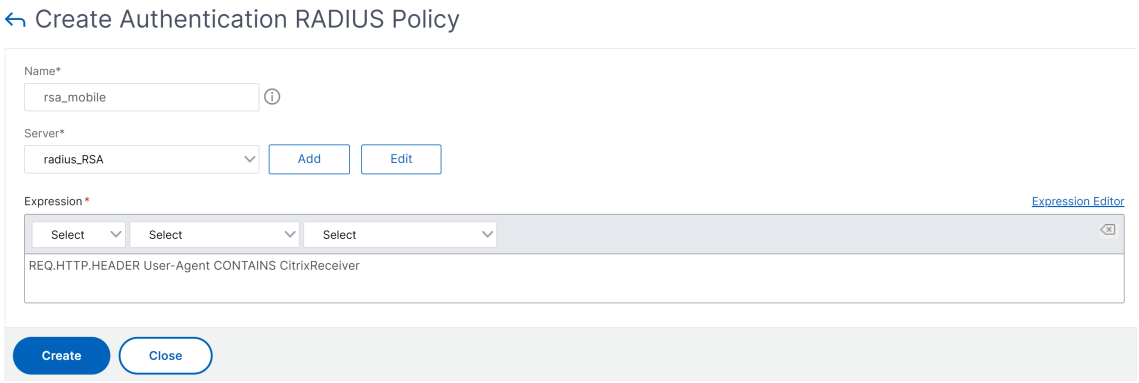


5. Create a RADIUS policy and RADIUS server for the mobile devices.

   - Navigate to the RADIUS option from **NetScaler Gateway > Policies > Authentication > RADIUS**. Click **Add** under Server tab.
   - Add the required details. The default port for RADIUS authentication is 1812.



   - To bind this policy to only mobile devices, use the following expression:

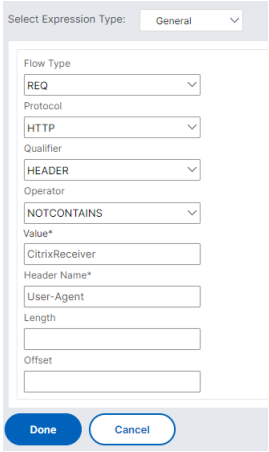


6. Follow the same step to create an LDAP policy for non-mobile devices. To bind this policy to only non-mobile devices, use the following expression:

```
REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

The corresponding advanced expression is:

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```

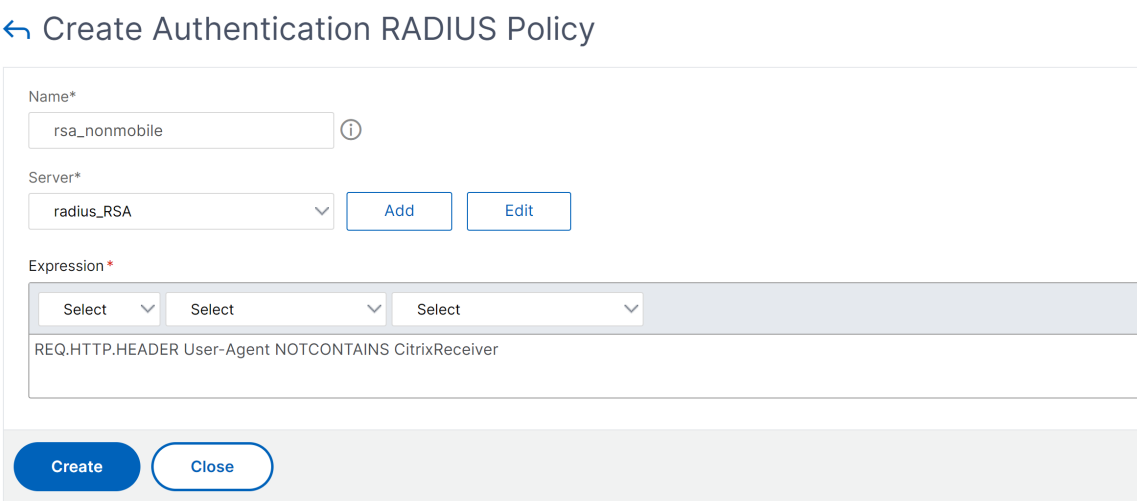


7. Create a RADIUS policy for non-mobile devices. To bind this policy to only non-mobile devices, use the following expression:

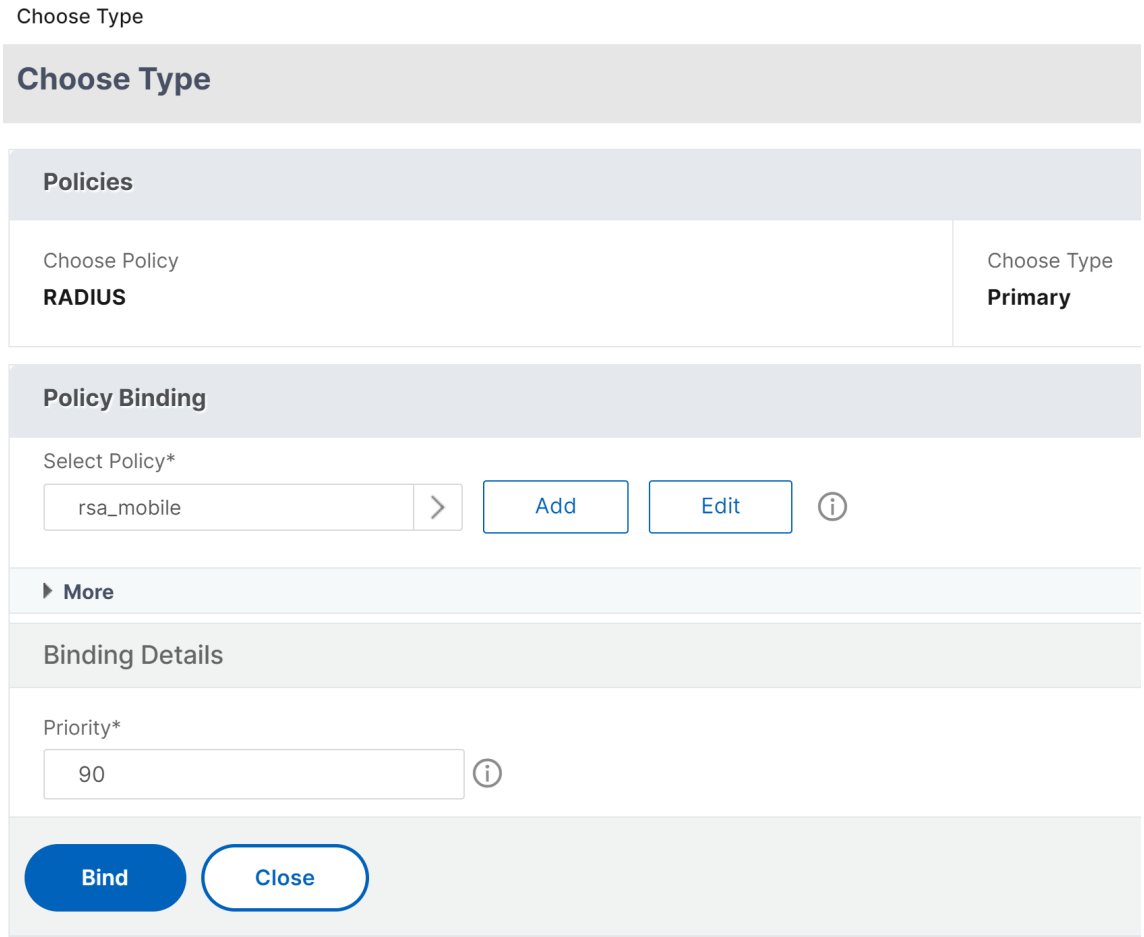
```
REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

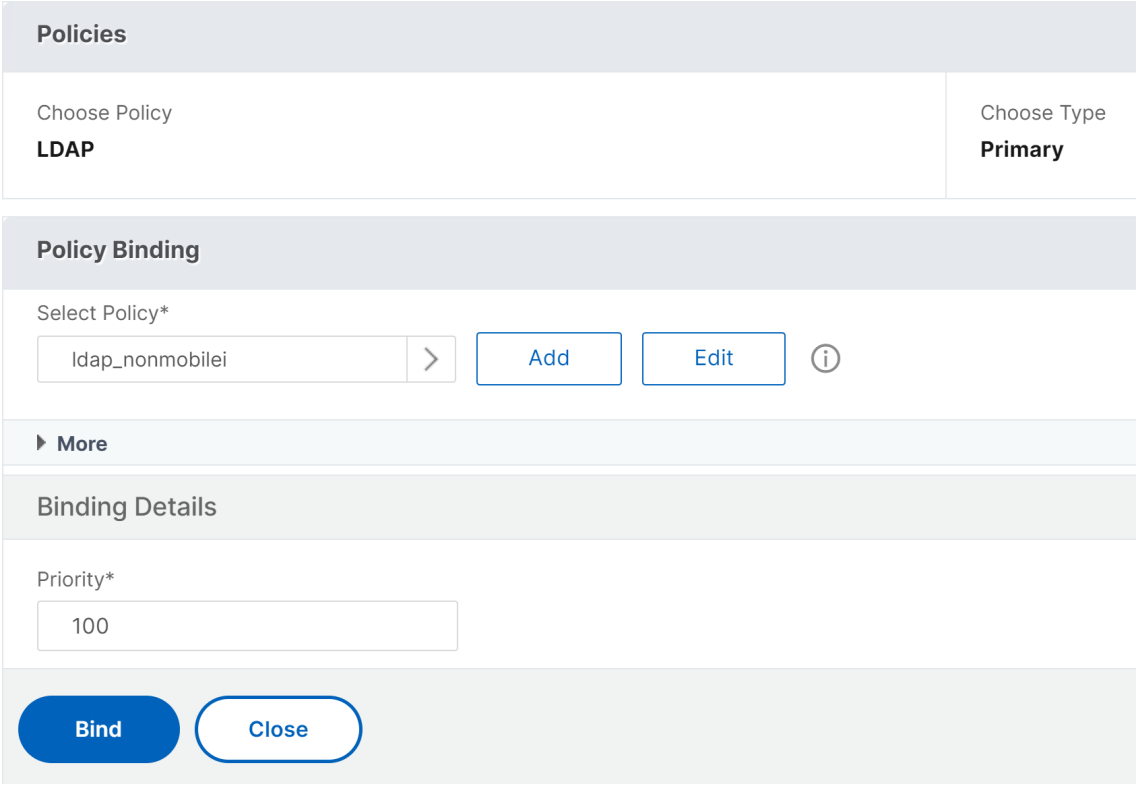
The corresponding advanced expression is:

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```

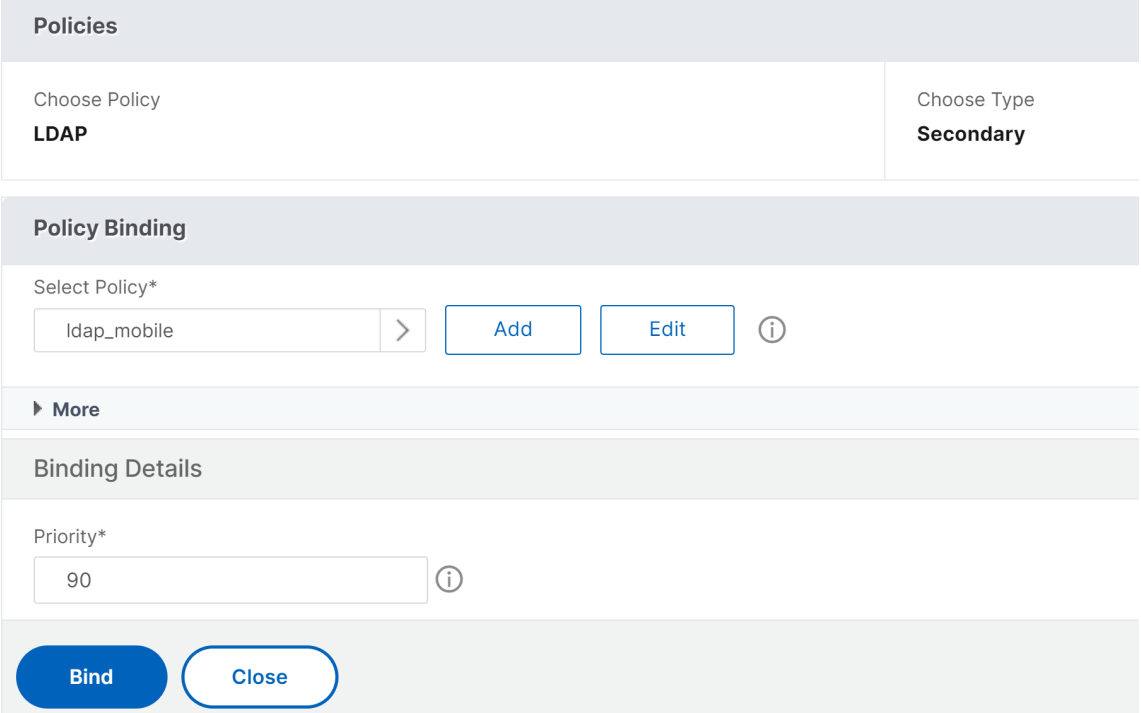



8. Go to the Properties of the NetScaler Gateway Virtual Server and click the **Authentication** tab. On the Primary Authentication Policies, add the RSA_Mobile policy as top priority and the LDAP_NonMobile policy as secondary priority:





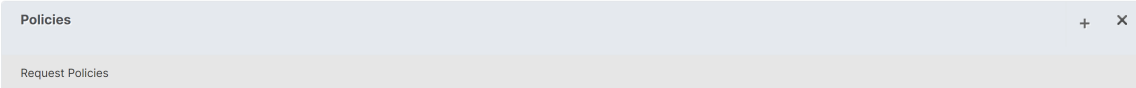
9. In the Secondary Authentication Policies, add the LDAP_Mobile policy as top priority, followed by the RSA_NonMobile policy as secondary priority:



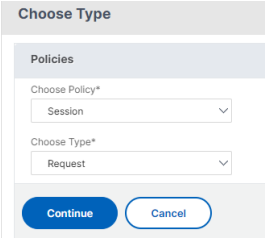
> The session policy must have the correct single sign-on Credential Index, that is, it must be the LDAP credentials. For mobile devices, the **Credential Index** under **Session Profile > Client Experience** must be set to **Secondary** which is LDAP.

Therefore you need two session policies, one for mobile devices and the other for non-mobile devices.

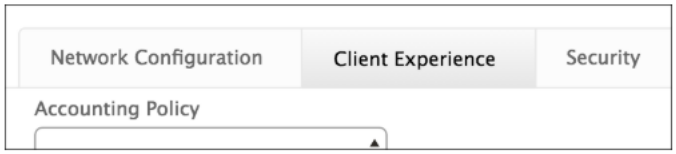
- For mobile devices, the session policy, and session profile appear as displayed in the following screenshot.
  To create session policy, navigate to the required virtual server and, click **Edit**, go to the policy section, and click + sign:

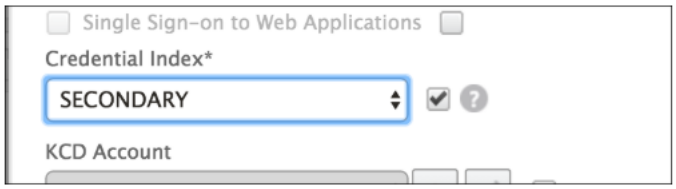


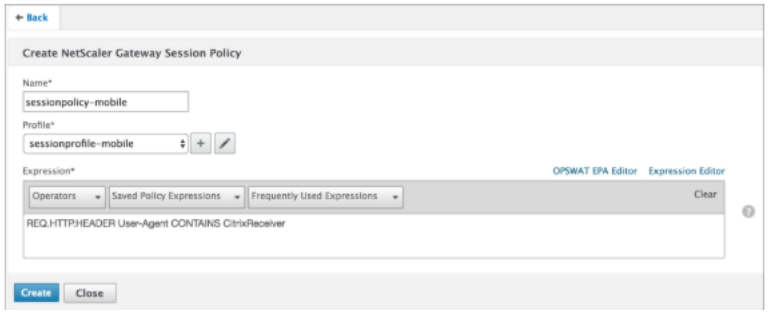
- Choose the **Session** option from the menu.



- Enter the desired Session Policy name and click + to create a profile. For mobile devices, the **Credential Index** under **Session Profile > Client Experience** must be set to **Secondary** which is LDAP.







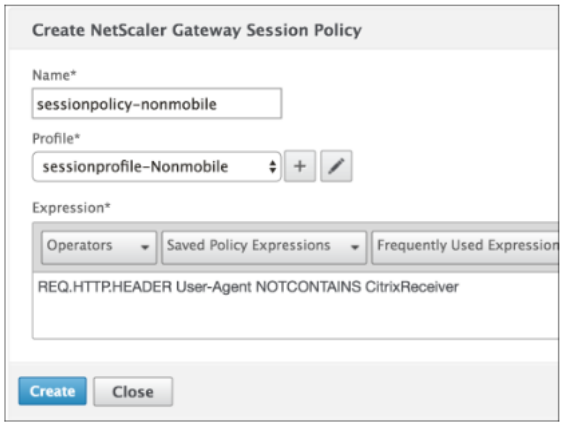
- For non-mobile devices, follow the same steps. **Credential Index** under **Session Profile > Client Experience** must be set to **Primary** which is LDAP.

The expression must be changed to:

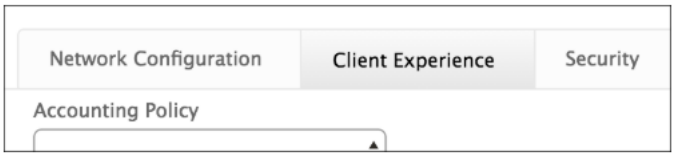
```
REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

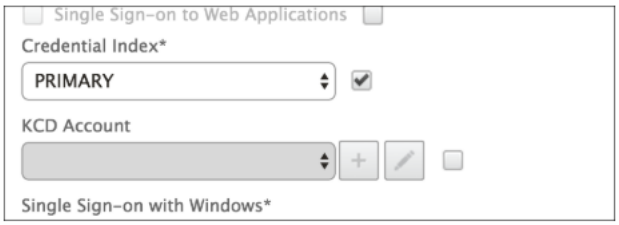
The corresponding advanced expression is:

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```

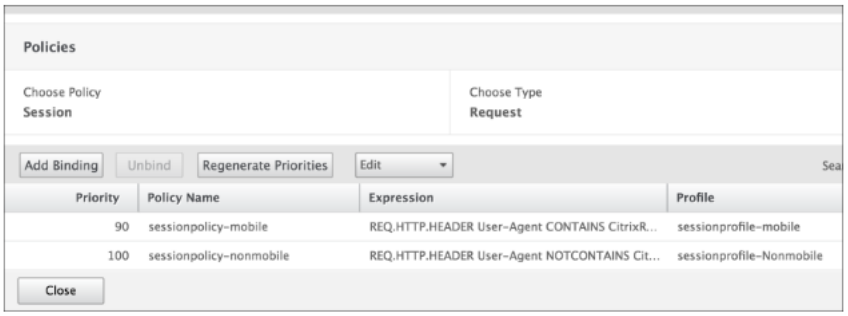


- To create profile for non-mobile user, click + sign.

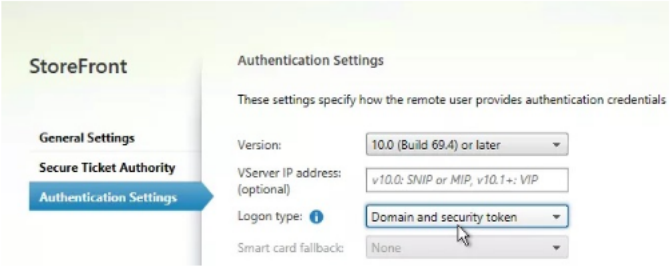


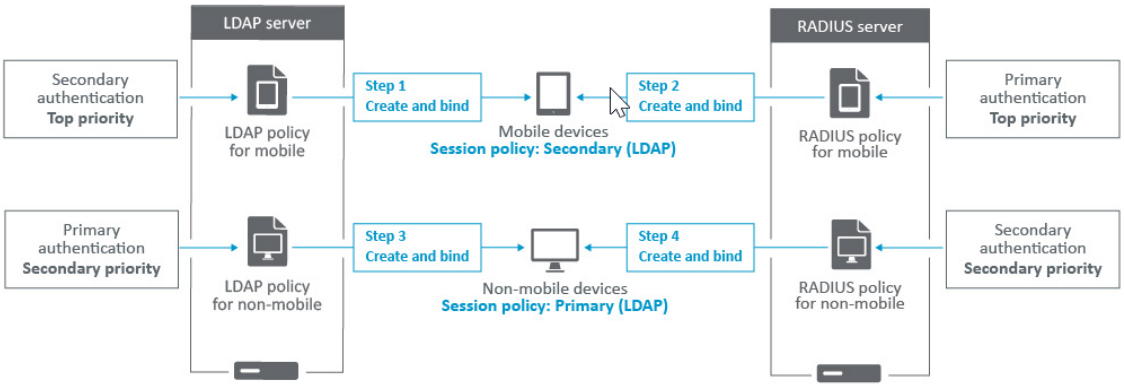


10. The following figure displays the policies and profiles under the required virtual server.



11. Also on the StoreFront, under the NetScaler Gateway configuration set to use “Logon Type”= “Domain and Security token”





Restrict access to NetScaler Gateway for members of one Active Directory group

January 8, 2024

NetScaler Gateway supports two methods of restricting logon access.

- LDAP Search Filter –Only user names that match the LDAP Search Filter (for example, Active Directory group membership) can log on to NetScaler Gateway.
- Groups allowed to log on in a NetScaler Gateway session policy or profile –This method supports multiple Active Directory groups. For details see https://support.citrix.com/article/CTX125797.

This article describes the LDAP Search Filter method.

Overview

When a user enters the credentials on the logon page of the NetScaler Gateway virtual server and presses ENTER, the appliance first searches the Active Directory (LDAP) for the user name. If an LDAP Search Filter is not defined in the LDAP policy or the server, then the appliance searches all Active Directory user names for a match. Once a match is found, the appliance then pulls the user's full Distinguished Name (DN) and uses the user's DN and password to authenticate to the Active Directory.

If an LDAP Search Filter is defined, then only user names that match the LDAP Search Filter are searched for a user name match. For example, if the LDAP Search Filter is constructed to only search members of an Active Directory group, then the user name entered by the user must match the members of the group.

Prerequisites

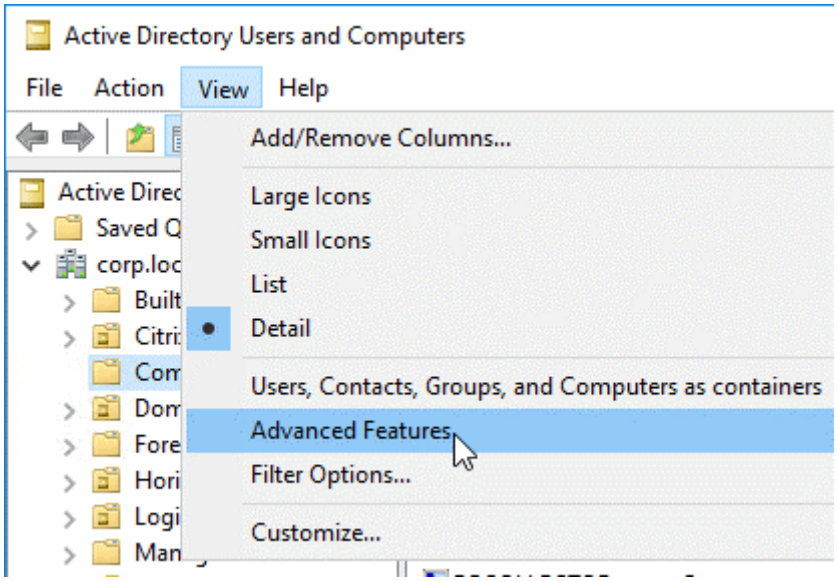
The NetScaler Gateway virtual server must be configured for LDAP authentication.

Steps to configure an LDAP Search Filter for members of one Active Directory group

1. Determine the Active Directory Group that has access permission, and get its full Distinguished Name.

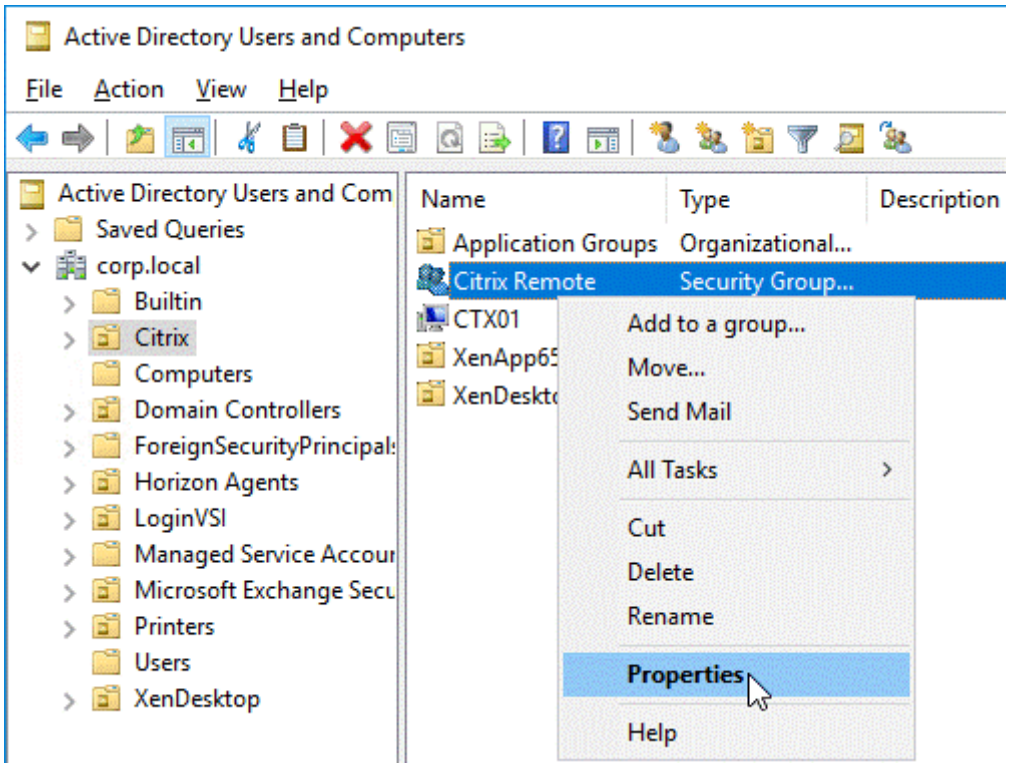
   An easy way to get the full Distinguished Name of the group is through Active Directory Users and Computers.

2. In Active Directory Users and Computers, from **View** menu, enable **Advanced Features**.

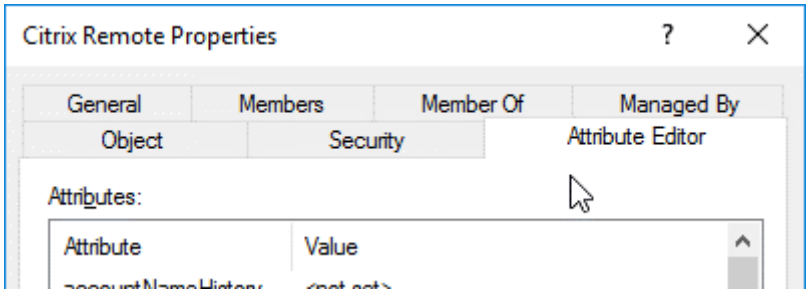


3. Browse the tree to the group object, right-click, and then and click **Properties**.

   Note: You cannot use **Find**. Instead, you must navigate through the tree to find the object.

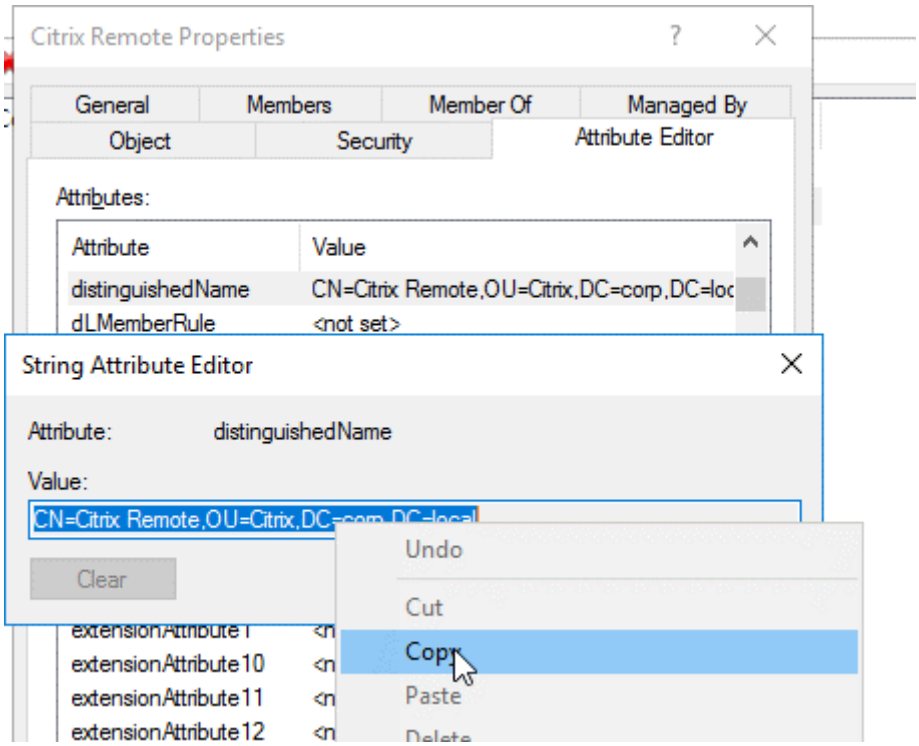


4. On the right, switch to the **Attribute Editor** tab.

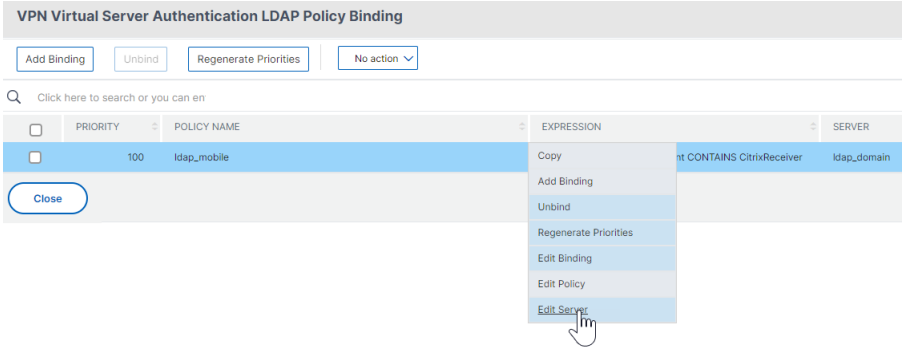


This tab is only visible if **Advanced Features** are enabled, and if you have not use the **Find** feature.

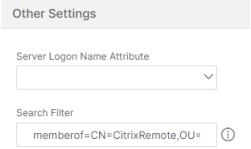
5. Scroll down to **distinguishedName**, double-click it, and then copy it to the clipbboard.



6. In the NetScaler Gateway GUI, navigate to **NetScaler Gateway > Virtual Servers**.
7. Select an existing NetScaler Gateway virtual server and click **Edit**.
8. In the Basic Authentication section, click **LDAP Policies**.
9. Right-click an existing LDAP policy, and click **Edit Server**.



10. In the **Other Settings** section, in the **Search Filter** field, type in **memberOf=** and then paste the Distinguished Name of the Active Directory group after the equals sign (=).



An example Search Filter is the following:
memberOf=CN=Citrix Remote,OU=Citrix,DC=corp,DC=local
Note: By default, NetScaler only searches for user names that are direct members of the Active Directory group. If you want to search nested groups, then add the Microsoft OID:: to the LDAP Search Filter. The OID is inserted between memberOf and =.

Example: memberOf:1.2.840.113556.1.4.1941:=CN=Citrix Remote,OU=Citrix,DC=corp,DC=local

11. Click **OK**.

Using High Availability

January 8, 2024

A high availability deployment of two NetScaler Gateway appliances can provide uninterrupted operation in any transaction. When you configure one appliance as the primary node and the other as the secondary node, the primary node accepts connections and manages servers while the secondary node monitors the primary. If, for any reason, the primary node is unable to accept connections, the secondary node takes over.

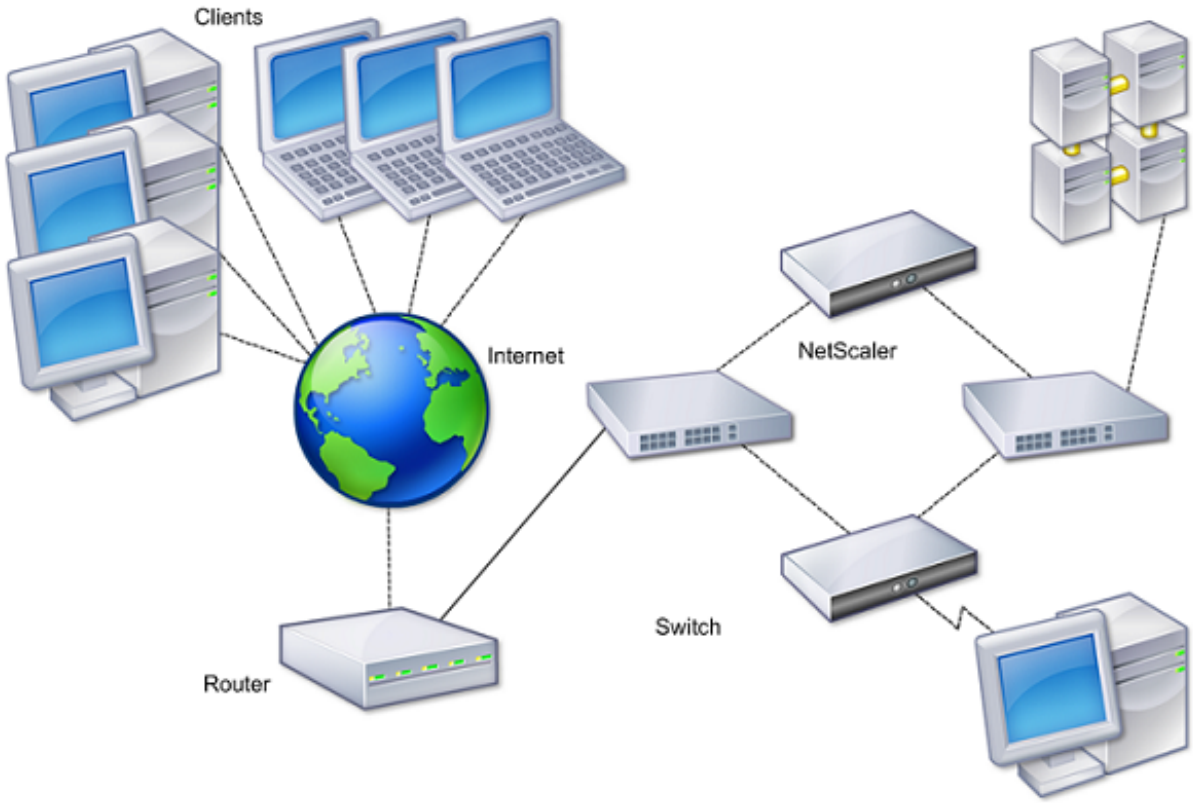
The secondary node monitors the primary by sending periodic messages (often called heartbeat messages or health checks) to determine whether the primary node is accepting connections. If a health check fails, the secondary node retries the connection for a specified period, after which it determines that the primary node is not functioning normally. The secondary node then takes over for the primary (a process called failover).

After a failover, all clients must reestablish their connections to the managed servers, but the session persistence rules are maintained as they were before the failover.

With Web server logging persistence enabled, no log data is lost due to the failover. For logging persistence to be enabled, the log server configuration must carry entries for both systems in the log.conf file.

The following figure shows a network configuration with a high availability pair.

Figure 1. NetScaler Gateway Appliances in a High Availability Configuration



The basic steps to configure high availability are as follows:

1. Create a basic setup, with both nodes in the same subnet.
2. Customize the intervals at which the nodes communicate health-check information.
3. Customize the process by which nodes maintain synchronization.
4. Customize the propagation of commands from the primary to the secondary.
5. Optionally, configure fail-safe mode to prevent a situation in which neither node is primary.
6. Configure virtual MAC addresses if your environment includes devices that do not accept NetScaler Gateway gratuitous ARP messages.

When you are ready for a more complex configuration, you can configure high availability nodes in different subnets.

To improve the reliability of your high availability setup, you can configure route monitors and create redundant links. In some situations, such as when troubleshooting or performing maintenance tasks, you might want to force a node to fail over (assign primary status to the other node), or you might want to force the secondary node to stay secondary or the primary node to stay primary.

How high availability works

January 8, 2024

When you configure NetScaler Gateway in a high availability pair, the secondary NetScaler Gateway monitors the first appliance by sending periodic messages, also called a heartbeat message or health check, to determine if the first appliance is accepting connections. If a health check fails, the secondary NetScaler Gateway tries the connection again for a specified amount of time until it determines that the primary appliance is not working. If the secondary appliance confirms the health check failure, the secondary NetScaler Gateway takes over for the primary NetScaler Gateway. This is called failover.

The following ports are used to exchange information related to high availability between NetScaler Gateway appliances:

- UDP port 3003 is used to exchange hello packets for communicating the status for intervals.
- TCP port 3010 is used for the high availability configuration synchronization.
- TCP port 3011 is used to synchronize configuration settings.

Guidelines for configuring high availability

Before configuring a high availability pair, you must review these guidelines:

- Each NetScaler Gateway appliance must be running the same version of the NetScaler Gateway software. You can find the version number at the top of the page in the configuration utility.
- NetScaler Gateway does not automatically synchronize passwords between two appliances. You can choose to configure each NetScaler Gateway with the user name and password of the other appliance in the pair.
- Entries in the configuration file, ns.conf, on both the primary and the secondary NetScaler Gateway must match, with the following exceptions:
  - The primary and secondary NetScaler Gateway appliance must each be configured with its own unique system IP address. Use the Setup Wizard to configure or modify the system IP address on either NetScaler Gateway.

  - In a high availability pair, the NetScaler Gateway ID and associated IP address must point to the other NetScaler Gateway.

    For example, if you have two appliances, named AG1 and AG2, you must configure AG1 with the unique NetScaler Gateway ID and IP address of AG2. You must configure AG2 with the unique NetScaler Gateway ID and IP address of AG1.

    Note: Each NetScaler Gateway appliance is always identified as Node 0. Configure each appliance with a unique node ID.

- Each appliance in the high availability pair must have the same license. For more information about licensing, see Licensing.
- If you create a configuration file on either node by using a method that does not go directly through the configuration utility or the command-line interface (for example, importing SSL certificates, or changing to start up scripts), you must copy the configuration file to the other node or create an identical file on that node.
- When you configure a high availability pair, make sure the mapped IP addresses and default gateway address of both the primary and the secondary appliances are identical. If necessary, you can change the mapped IP address at any time by running the Setup Wizard.

You can use the pre-installation checklist to view a list of the specific settings you need to configure in a high availability deployment. For details, see Pre-Installation Checklist.

Configuring settings for high availability

January 8, 2024

To set up a high availability configuration, you create two nodes, each of which defines the other's NetScaler Gateway IP address as a remote node. You can start by logging on to one of the two NetScaler appliances that you want to configure for high availability and add a node. Specify the other appliance's NetScaler Gateway IP address as the address of the new node. Then, log on to the other appliance and add a node that has the NetScaler Gateway IP address of the first appliance. An algorithm determines which node becomes primary and which becomes secondary.

Before you configure the appliances, add a high availability node. This node represents either the first or second NetScaler Gateway in the high availability pair. To configure high availability, you first create the node and then you configure the high availability settings.

To add a high availability node

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **System > High Availability**.

2. In the details pane, on the Nodes tab, click **Add**.
3. In the **Create HA Node** page, in the **Remote Node IP Address** text box, type the NSIP address of the NetScaler that is to be added as the remote node. If the NetScaler Gateway IP address is an IPv6 address, select the **IPv6** check box before entering the address.
4. If you want to add the local node to the remote node automatically, select Configure remote system to participate in High Availability setup. If you do not select this option, you have to log in to the appliance represented by the remote node and add the node that you are currently configuring.
5. Click to enable **Turn off HA Monitor interfaces/channels that are down**.
6. If the remote appliance has a different user name and password, in Remote System Logon Credentials, click Login credentials for the remote system are different from the self-node.
7. In **User Name**, type the user name of the remote appliance.
8. In **Password**, type the password of the remote appliance.
9. Click **OK**.

To enable or disable the secondary node

You can disable or enable the secondary node only. When you disable a secondary node, it stops sending heartbeat messages to the primary node, and therefore the primary node can no longer check the status of the secondary node. When you enable a node, the node takes part in the high availability configuration.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand System and then click High Availability.
2. In the details pane, on the Nodes tab, select the local node and then click Open.
3. In the HA Configure Node dialog box, in High Availability Status, select ENABLED (Do not participate in HA).
4. Click OK. A message appears in the status bar, stating that the node has been configured successfully.

To configure settings for high availability

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **System > High Availability**.
2. In the details pane, on the Nodes tab, select a node, and then click **Edit**.
3. In the **HA Configure Node** dialog box, in ID, type the number of the node identifier. ID specifies the unique node number for the other appliance.
4. In **IP Address**, type the system IP address and then click OK. The IP Address specifies the IP address of the other appliance.

Note: The maximum ID for nodes in a high availability pair is 64.

Changing an RPC node password

January 8, 2024

To communicate with other NetScaler Gateway appliances, each appliance requires knowledge of the other appliances, including how to authenticate on NetScaler Gateway. RPC nodes are internal system entities used for system-to-system communication of configuration and session information. One RPC node exists on each NetScaler Gateway and stores information, such as the IP addresses of the other NetScaler Gateway appliance and the passwords used for authentication. The NetScaler Gateway that makes contact with another NetScaler Gateway checks the password within the RPC node.

NetScaler Gateway requires RPC node passwords on both appliances in a high availability pair. The passwords must be the same on both the appliances. The primary appliance must be aware of the secondary RPC node password and the secondary must be aware of the primary RPC node password. Initially, each NetScaler Gateway is configured with the same RPC node password. To enhance security, you must change the default RPC node passwords. You can use the configuration utility to configure and change RPC nodes.

RPC nodes are implicitly created when adding a node or adding a Global Server Load Balancing (GSLB) site. You cannot create or delete RPC nodes manually.

> **Important:**
>
> You must also secure the network connection between the appliances. You can configure security when you configure the RPC node password by selecting the **Secure** check box.

To change an RPC node password and enable a secure connection

1. Navigate to **System > Network > RPC.**
2. In the details pane, select the node and then click **Edit**.
3. In **Password** and **Confirm Password**, type the new password.
4. In **Source IP Address**, type the system IP address of the other NetScaler Gateway appliance.
5. Click **Secure** and then click **OK**.

> **Note:**
>
> When you enable the **Secure** option, the appliance encrypts all communication sent from the

> node to other RPC nodes thus securing the RPC communication.

To change an RPC node password by using the CLI

At the command prompt, type:

```
set ns rpcNode <IPAddress> {
 -password }
  [-secure ( YES | NO )]

show ns rpcNode
```

Example:

```
> set ns rpcNode 192.0.2.4 -password mypassword -secure YES
 Done
> show rpcNode
.
.
.
 IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e
     SrcIP:  *           Secure:  ON
Done
>
```

Configuring the primary and secondary appliances for high availability

January 8, 2024

After changing the RPC node password and enabling secure communication, use the configuration utility to configure the primary and secondary NetScaler Gateway High Availability nodes.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand System and then click High Availability.
2. In the details pane, on the Nodes tab, select a node and then click Edit.
3. Under High Availability Status, click Enabled (Actively Participate in HA) and then click OK.

Configuring communication intervals

January 8, 2024

When you configure NetScaler Gateway as a high availability pair, you can configure the secondary NetScaler Gateway to listen at specific intervals, measured in milliseconds (msec). These intervals are known as hello intervals and dead intervals.

The hello interval is the interval at which the heartbeat messages are sent to the peer node. The dead interval is the time interval after which the peer node is marked DOWN if heartbeat packets are not received. The heartbeat messages are UDP packets sent to port 3003 of the other node in a high availability pair.

When you configure the hello interval, you can use the values 200 to 1000. The default value is 200. The dead interval values are 3 to 60. The default value is 3.

> **Note**
>
> Dead interval must be set as a multiple of hello interval.

To configure communication intervals for the secondary NetScaler Gateway

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand System and then click High Availability.
2. In the details pane, on the Nodes tab, select a node and then click Edit.
3. Under Intervals, do one or both of the following:
    - In Hello Interval (msec), type the value and then click OK. The default is 200 milliseconds.
    - In Dead Interval (secs), type the value and then click OK. The default setting is three seconds.

Synchronizing NetScaler Gateway appliances

January 8, 2024

Automatic synchronization of NetScaler Gateway appliances in a high availability pair is enabled by default. With automatic synchronization, you can make changes to one appliance and enable the changes to propagate automatically to the second appliance. Synchronization uses port 3010.

Synchronization starts when the following occurs:

- The secondary node restarts.
- The primary node becomes secondary after a failover.

You can disable synchronization, which prevents the secondary NetScaler Gateway from synchronizing its configuration with the primary NetScaler Gateway when a change occurs on the primary appliance. You can also force synchronization.

You enable or disable high availability synchronization on the secondary node in the pair.

To enable or disable high availability synchronization

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand System and then click High Availability.
2. In the details pane, on the Nodes tab, select a node and then click Edit.
3. In the Configure Node dialog box, under HA Synchronization, do one of the following:
   - To disable synchronization, clear the Secondary node will fetch the configuration from Primary check box.
   - To enable synchronization, select the Secondary node will fetch the configuration from Primary check box.
4. Click OK. A message appears in the status bar stating that the node configuration is successful.

To force synchronization between appliances

In addition to automatic synchronization, NetScaler Gateway supports forced synchronization between the two nodes in a high availability pair.

You can force synchronization on both the primary and secondary NetScaler Gateway appliances. However, if synchronization is already in progress, the command fails and NetScaler Gateway displays a warning. Forced synchronization also fails in the following circumstances:

- You force synchronization on a standalone system.
- The secondary node is disabled.
- You disable high availability synchronization on the secondary node.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand System and then click High Availability.
2. On the Nodes tab, click Force Synchronization.

Synchronizing configuration files in a high availability setup

January 8, 2024

In a high availability setup, you can synchronize various configuration files from the primary node to the secondary node.

Parameters for synchronizing files in a high availability setup

- Mode

  The type of synchronization to be performed. The following descriptions include, in parentheses, the command-line argument that specifies the option.

  - **Everything except licenses and rc.conf** (all). Synchronizes files related to system configuration, NetScaler Gateway bookmarks, SSL certificates, SSL CRL lists, HTML injection scripts, and Application Firewall XML objects.
  - **Bookmarks** (bookmarks). Synchronizes all NetScaler Gateway bookmarks.
  - **SSL certificates and keys** (`ssl`). Synchronizes all certificates, keys, and CRLs for the SSL feature.
  - **Licenses and rc.conf** (misc). Synchronizes all license files and the rc.conf file.
  - **Everything including licenses and rc.conf** (all_plus_misc). Synchronizes files related to system configuration, NetScaler Gateway bookmarks, SSL certificates, SSL CRL lists, HTML injection scripts, Application Firewall XML objects, licenses, and the rc.conf file.

Note: There are more options available if you install a NetScaler license on the appliance.

To synchronize files in a high availability setup by using the configuration utility

1. In the navigation pane, expand **System** and then click **Diagnostics**.
2. In the details pane, under **Utilities**, click **Start HA files synchronization**.
3. In the **Start file synchronization** dialog box, in the **Mode** menu, select the appropriate type of synchronization (for example, Everything except licenses and rc.conf), and then click **OK**.

Configuring command propagation

January 8, 2024

In a high availability setup, any command issued on the primary node propagates automatically to, and runs on, the secondary node before the command runs on the primary node. If command propagation fails, or if command execution fails on the secondary node, the primary node runs the command and logs an error. Command propagation uses port 3011.

In a high availability pair configuration, command propagation is enabled by default on both the primary and secondary nodes. You can enable or disable command propagation on either node in a high availability pair. If you disable command propagation on the primary node, commands are not propagated to the secondary node. If you disable command propagation on the secondary node, commands propagated from the primary are not run on the secondary node.

Note: After re-enabling propagation, remember to force synchronization.

Note: If synchronization occurs while you are disabling propagation, any configuration-related changes that you make before the disabling of propagation takes effect are synchronized with the secondary node. This is also true for cases in which propagation is disabled while synchronization is in progress.

To enable or disable propagation on the primary node

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **System** and then click **High Availability**.
2. In the details pane, on the **Nodes** tab, select a node, and then click **Edit**.
3. Under **HA propagation**, do one of the following:
   - To disable high availability propagation, clear the **Primary node propagates configuration to the Secondary** check box.
   - To enable high availability propagation, select the **Primary node propagates configuration to the Secondary** check box.
4. Click **OK**.

Troubleshooting command propagation

January 8, 2024

The following list describes the reasons command propagation might fail, and solutions for restoring the setting:

- Network connectivity is not active. If a command propagation fails, check the network connection between the primary and secondary NetScaler Gateway appliances.
- Missing resources on secondary NetScaler Gateway. If a command execution succeeds on the primary NetScaler Gateway but fails to propagate to the secondary NetScaler Gateway, run the command directly on the secondary NetScaler Gateway to see the error message. The error might have occurred because the resources required by the command are present on the primary NetScaler Gateway and are not available on the secondary NetScaler Gateway. Also, verify that the license files on each appliance match.

  For example, verify that all of your Secure Sockets Layer (SSL) certificates are present on each NetScaler Gateway. Verify that any initialization script customization exists on both NetScaler Gateway appliances.

- Authentication failure. If you receive an authentication failure error message, verify the RPC node settings on each appliance.

Configure fail-safe mode

January 8, 2024

In a high availability configuration, fail-safe mode ensures that one node is always primary when both nodes fail the health check. Fail-safe mode ensures that when a node is only partially available, backup methods can activate and can handle traffic.

You configure high availability fail-safe mode independently on each node.

The following table shows some of the fail-safe cases. The NOT_UP state means that the node failed the health check and yet the node is partially available. The UP state means that the node passed the health check.

Table 1. Fail-safe mode cases

Node A (primary) health state	Node B (secondary) health state	Default high availability behavior	Fail-safe enabled high availability behavior	Description
NOT_UP (failed last)	NOT_UP (failed first)	A (Secondary), B (Secondary)	A (Primary), B (Secondary)	If both nodes fail, one after the other, the node that was the last primary node remains primary.
NOT_UP (failed first)	NOT_UP (failed last)	A (Secondary), B (Secondary)	A (Secondary), B (Primary)	If both nodes fail, one after the other, the node that was the last primary node remains primary.
UP	UP	A (Primary), B (Secondary)	A (Primary), B (Secondary)	If both nodes pass the health check, no change in behavior with fail-safe enabled.

Node A (primary) health state	Node B (secondary) health state	Default high availability behavior	Fail-safe enabled high availability behavior	Description
UP	NOT_UP	A (Primary), B(Secondary)	A (Primary), B (Secondary)	If only the secondary node fails, no change in behavior with fail-safe enabled.
NOT_UP	UP	A (Secondary), B(Primary)	A (Secondary), B(Primary)	If only the primary fails, no change in behavior with fail-safe enabled.
NOT_UP	UP (STAYSEC-ONDARY)	A (Secondary), B (Secondary)	A (Primary), B (Secondary)	If the secondary is configured as STAYSECONDARY, the primary remains primary even if it fails.

To configure fail-safe mode

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand System and then click High Availability.
2. In the details pane, on the Nodes tab, select a node and then click Edit.
3. In the Configure Node dialog box, under Fail-Safe Mode, select Maintain one Primary node even when both nodes are unhealthy and then click OK.

Configuring the virtual MAC address

January 8, 2024

The virtual MAC address is shared by the primary and secondary NetScaler Gateway appliances in a high availability setup.

In a high availability setup, the primary NetScaler Gateway owns all the floating IP addresses, such as the mapped IP address or the virtual IP address. It responds to address resolution protocol (ARP) requests for these IP addresses with its own MAC address. As a result, the ARP table of an external

device (such as a router) is updated with the floating IP address and the primary NetScaler Gateway MAC address. When a failover occurs, the secondary NetScaler Gateway takes over as the new primary NetScaler Gateway. It then uses gratuitous address resolution protocol (GARP) to advertise the floating IP addresses that it acquired from the primary appliance. The MAC address, which the new primary appliance advertises, is that of its own interface.

Some devices do not accept GARP messages generated by NetScaler Gateway. As a result, some of the external devices retain the old IP-to-MAC mapping advertised by the old primary NetScaler Gateway. This situation can cause a site to become unavailable. To resolve the problem, you configure a virtual MAC address on both NetScaler Gateway appliances of a high availability pair. This configuration implies that both NetScaler Gateway appliances have identical MAC addresses. As a result, when failover occurs, the MAC address of the secondary NetScaler Gateway remains unchanged and ARP tables on the external devices do not need to be updated.

To create a virtual MAC address, create a virtual router identifier (ID) and bind it to an interface. In a high availability setup, the user needs to bind the ID to the interfaces on both the appliances.

When the virtual router ID is bound to an interface, the system generates a virtual MAC address with the virtual router ID as the last octet. An example of the generic virtual MAC address is 00:00:5e:00:01:<VRID>. For example, if you created a virtual router ID of value 60 and bind it to an interface, the resulting virtual MAC address is 00:00:5e:00:01:3c, where 3c is the hex representation of the virtual router ID. You can create 255 virtual router IDs ranging from 1 through 254.

You can configure virtual MAC addresses for IPv4 and IPv6.

Configuring IPv4 virtual MAC addresses

January 8, 2024

When you create a IPv4 virtual MAC address and bind it to a interface, any IPv4 packet sent from the interface uses the virtual MAC address that is bound to the interface. If there is no IPv4 virtual MAC address bound to an interface, the interface's physical MAC address is used.

The generic virtual MAC address is of the form 00:00:5e:00:01:<VRID>. For example, if you create a VRID with a value of 60 and bind it to an interface, the resulting virtual MAC address is 00:00:5e:00:01:3c, where 3c is the hex representation of the VRID. You can create 255 VRIDs with values from 1 to 255.

Creating or modifying an IPv4 virtual MAC address

January 8, 2024

You create an IPv4 virtual MAC address by assigning it a virtual router ID. You can then you bind the virtual MAC address to an interface. You cannot bind multiple virtual router IDs to the same interface. To verify the virtual MAC address configuration, you must display and examine the virtual MAC address and the interfaces bound to the virtual MAC address.

Parameters for configuring a virtual MAC address

- VrID

  The virtual router ID that identifies the virtual MAC address. Possible values: 1–255.

- `ifnum`

  The interface number (slot/port notation) to be bound to the virtual MAC address.

To configure a virtual MAC address

1. Navigate to **System > Network** and then click **VMAC**.
2. In the details pane, on the **VMAC** tab, click **Add**.
3. In the **Create VMAC** dialog box, in **Virtual Router ID**, type the value.
4. Under **Associated Interfaces**, in **Available Interfaces**, select a network interface, click **Add**, click **Create**, and then click **Close**.

After you create the virtual MAC address, it appears in the configuration utility. If you selected a network interface, the virtual router ID is bound to that interface.

To delete a virtual MAC address

To delete a virtual MAC address, you need to delete the corresponding virtual router ID.

1. Navigate to **System > Network,** and then click **VMAC**.
2. In the details pane, select an item and then click **Remove**.

To bind and unbind a virtual MAC address

When you created the virtual router ID, you selected a network interface on NetScaler Gateway and then bound the virtual router ID to the network interface. You can also unbind a virtual MAC address from the network interface, but leave the MAC address configured on NetScaler Gateway.

1. Navigate to **System > Network** and then click **VMAC**.
2. In the details pane, select an item, and then click **Open**.
3. Under **Configured Interfaces**, select a network interface, click **Remove**, click **OK**, and then click **Close**.

Configuring IPv6 virtual MAC addresses

January 8, 2024

The NetScaler Gateway supports virtual MAC addresses for IPv6 packets. You can bind any interface to a virtual MAC address for IPv6, even if an IPv4 virtual MAC address is bound to the interface. Any IPv6 packet sent from the interface uses the virtual MAC address bound to that interface. If there is no virtual MAC address bound to an interface, an IPv6 packet uses the physical MAC.

Creating or modifying a virtual MAC address for IPv6

January 8, 2024

Create an IPv6 virtual MAC address by assigning it an IPv6 virtual router ID. Then bind the virtual MAC address to an interface. You cannot bind multiple IPv6 virtual router IDs to an interface. To verify the virtual MAC address configuration, display and examine the virtual MAC addresses and the interfaces bound to the virtual MAC address.

Parameters for configuring a virtual MAC address for IPv6

- `Virtual Router ID`

  The virtual router ID that identifies the virtual MAC address. Possible values: 1–255.

- `ifnum`

  The interface number (slot/port notation) to be bound to the virtual MAC address.

To configure a virtual MAC address for IPv6

1. In the configuration utility, on the Configuration tab, expand **System > Network** and then click VMAC.
2. In the details pane, on the VMAC6 tab, do one of the following:
   - To create a new virtual MAC address, click Add.
   - To modify an existing virtual MAC address, click Open.
3. In the Create VMAC6 or Configure VMAC6 dialog box, in Virtual Router ID, enter the value, such as vrID6.
4. In Associate Interfaces, click **Add > Create > Close**. A message appears in the status bar, stating that the virtual MAC address is configured.

To remove a virtual MAC address for IPv6

1. In the configuration utility, on the Configuration tab, expand **System > Network** and then click VMAC.
2. In the details pane, on the VMAC6 tab, select the virtual router ID that you want to remove and then click Remove. A message appears in the status bar, stating that the virtual MAC address is removed.

Configuring high availability pairs in different subnets

January 8, 2024

A typical high availability deployment is when both appliances in a high availability pair reside on the same subnet. A high availability deployment can also consist of two NetScaler Gateway appliances in which each appliance is in a different network. This topic describes the latter configuration, and includes sample configurations and a list of differences among the high availability configurations within one network and across networks.

You can also configure link redundancy and route monitors. These NetScaler Gateway functions are helpful in a cross-network high availability configuration. The functions also cover the health check process used by each NetScaler Gateway to ensure that the partner appliance is active.

How independent network configuration works

The NetScaler Gateway appliances are connected to different routers, called R3 and R4, on two different networks. The appliances exchange heartbeat packets through these routers. A heartbeat packet is a signal that occurs at regular intervals that ensures the connection is still active. You can expand this configuration to accommodate deployments involving any number of interfaces.

Note: If you use static routing on your network, you must add static routes between all the systems to ensure that heartbeat packets are sent and received successfully. (If you use dynamic routing on your systems, static routes are unnecessary.)

When the appliances in a high availability pair reside on two different networks, the secondary NetScaler Gateway must have an independent network configuration. This means that NetScaler Gateway appliances on different networks cannot share mapped IP addresses, virtual LANs, or network routes. This type of configuration, in which the NetScaler Gateway appliances in a high availability pair have different configurable parameters, is known as independent network configuration or symmetric network configuration.

The following table summarizes the configurable parameters for an independent network configuration, and shows how you must set them on each NetScaler Gateway:

Configurable parameters	Behavior
IP addresses	NetScaler Gateway specific. Active only on that appliance.
Virtual IP address	Floating.
Virtual LAN	NetScaler Gateway specific. Active only on that appliance.
Routes	NetScaler Gateway specific. Active only on that appliance. A link load balancing (LLB) route is floating.
access control lists (ACLs)	Floating (common). Active on both appliances.
Dynamic routing	NetScaler Gateway specific. Active only on that appliance. The secondary NetScaler Gateway must also run the routing protocols and peer with upstream routers.
L2 mode	Floating (common). Active on both appliances.
L3 mode	Floating (common). Active on both appliances.
Reverse Network Address Translation (NAT)	NetScaler Gateway specific. Reverse NAT with a virtual IP address because the NAT IP address is floating.

> **Note:**
>
> IPSET in INC mode is supported with public IP addresses. For details, see NetScaler High Availability with Azure Load Balancer Front End IP Validated Reference Design.

Adding a remote node

January 8, 2024

When two nodes of a high availability pair reside on different subnets, each node must have a different network configuration. Therefore, to configure two independent systems to function as a high availability pair, you must specify independent network computing mode during the configuration process.

When you add a high availability node, you must disable the high availability monitor for each interface that is not connected or being used for traffic.

To add a remote node for independent network computing mode

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **System > High Availability**.
2. In the details pane, click the **Nodes** tab, and then click **Add**.
3. In the High Availability Setup dialog box, in the **Remote Node IP Address** text box, type the NetScaler Gateway IP address of the appliance that is the remote node.

   To use an IPv6 address, click the **IPv6** check box before entering the IP address.
4. If you want to add the local node to the remote node automatically, select Configure remote system to participate in High Availability setup. If you do not select this option, you must log on to the appliance represented by the remote node and add the node that you are currently configuring.
5. Click to enable clear HA monitor on interfaces/channels that are down.
6. Click to enable Turn on INC (Independent Network Configuration) mode on self-mode.
7. Click **OK**. The **Nodes** page displays the local and remote nodes in your high availability configuration.

To remove a remote node

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **System > High Availability**.
2. In the details pane, click the **Nodes** tab.
3. Select the node that you want to remove, click **Remove,** and then click **Yes**.

Configuring route monitors

January 8, 2024

You can use route monitors to make the high availability state dependent on the internal routing table, whether the table contains any dynamically learned or static routes. In a high availability configuration, a route monitor on each node checks the internal routing table to make sure that a route entry

for reaching a particular network is always present. If the route entry is not present, the state of the route monitor changes to DOWN.

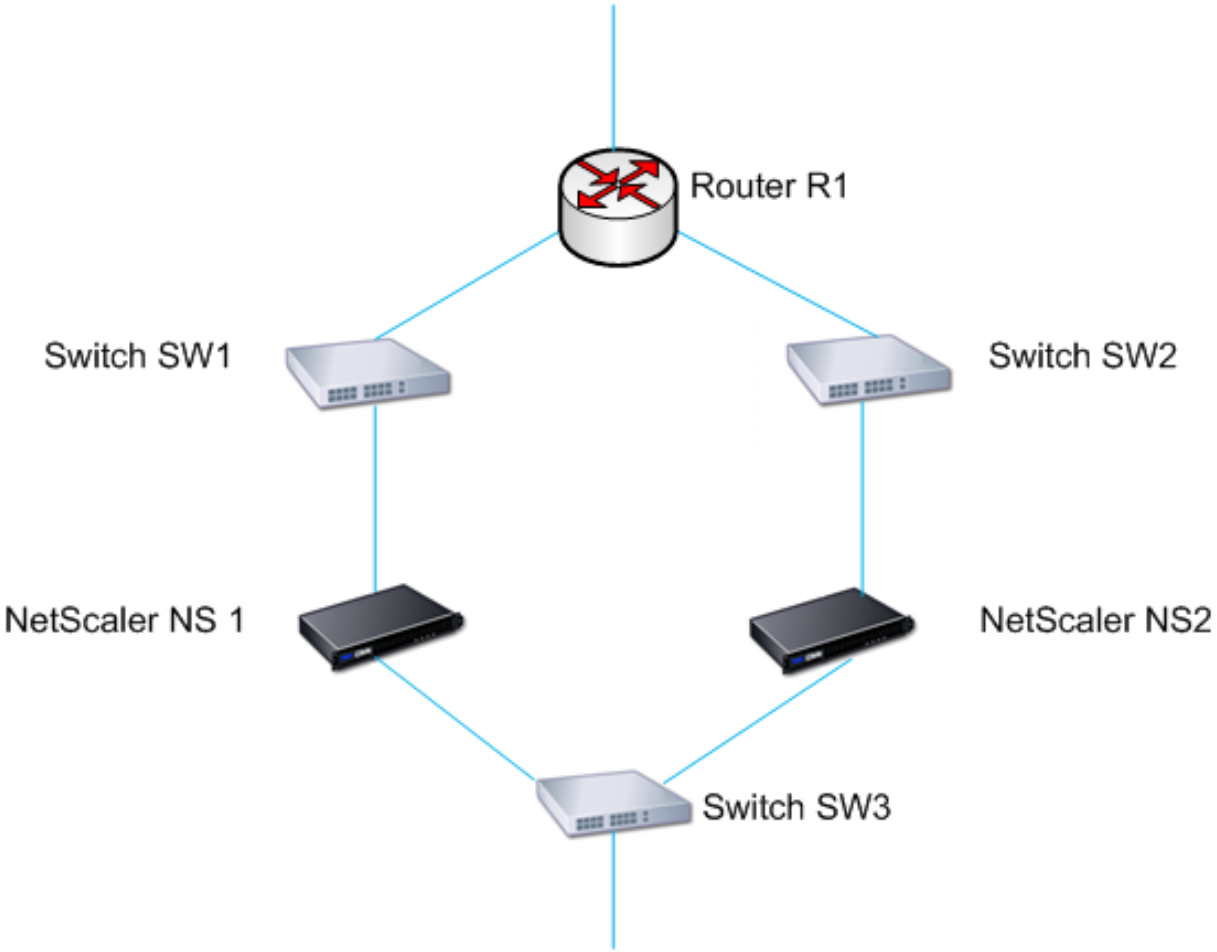
When a NetScaler Gateway appliance has only static routes for reaching a network, and you want to create a route monitor for the network, you must enable monitored static routes for the static routes. The monitored static route removes unreachable static routes from the internal routing table. If you disable monitored static routes on static routes, an unreachable static route can remain in the internal routing table, defeating the purpose of having the route monitor.

Route monitors are supported on either enabled or disabled Independent Network Configuration settings. The following table shows what occurs with route monitors in a high availability setup and with Independent Network Configuration enabled or disabled.

Route Monitors in high availability in disabled Independent Network Configuration mode	Route Monitors in high availability in enabled Independent Network Configuration mode
Route monitors are propagated by nodes and exchanged during synchronization.	Route monitors are neither propagated by nodes nor exchanged during synchronization.
Route monitors are active only in the current primary node.	Route monitors are active on both the primary and the secondary node.
The NetScaler Gateway appliance always displays the state of a route monitor as UP irrespective whether the route entry is present or not in the internal routing table.	The NetScaler Gateway appliance displays the state of the route monitor as DOWN if the corresponding route entry is not present in the internal routing table.
A route monitor starts monitoring its route in the following cases, to allow NetScaler Gateway to learn the dynamic routes, which might take up to 180 seconds: reboot, failover, set route6 command for v6 routes, set route `msr` enable/disable command for v4 routes, adding a new route monitor	Not applicable.

Route monitors are useful when you disable Independent Network Configuration mode and you want a gateway from a primary node as unreachable as one of the conditions for high availability failover.

For example, you disable Independent Network Configuration in a high availability setup in a two-arm topology that has NetScaler Gateway appliances NS1 and NS2 in the same subnet, with router R1 and switches SW1, SW2, and SW3, as shown in the following figure. Because R1 is the only router in this setup, you want the high availability setup to fail over whenever R1 is not reachable from the current primary node. You can configure a route monitor (say, RM1 and RM2, respectively) on each of the nodes to monitor the reachability of R1 from that node.



With NS1 as the current primary node, the network flow is as follows:

1. Route monitor RM1 on NS1 monitors NS1's internal routing table for the presence of a route entry for router R1. NS1 and NS2 exchange heartbeat messages through switch SW1 or SW3 at regular intervals.
2. If switch SW1 fails, the routing protocol on NS1 detects that R1 is not reachable and therefore removes the route entry for R1 from the internal routing table. NS1 and NS2 exchanges heartbeat messages through switch SW3 at regular intervals.
3. Detecting that the route entry for R1 is not present in the internal routing table, RM1 initiates a failover. If the route to R1 is down from both NS1 and NS2, failover happens every 180 seconds until one of the appliances is able to reach R1 and restore the connection.

Adding or removing route monitors

January 8, 2024

When the appliances of a high availability pair reside on different networks, the high availability state of NetScaler Gateway depends on if the appliance can be reached or not. In a cross-network high availability configuration, a route monitor on each NetScaler Gateway scans the internal routing table to make sure that an entry for the other NetScaler Gateway is always present.

To add a route monitor

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand System and then click High Availability.
2. In the Bind/Unbind Route Monitors dialog box, on the Route Monitors tab, click Action, and then click Configure.
3. Under Specify Route Monitor, in Network, type the IP address of the network of the other NetScaler Gateway appliance.

   To configure an IPv6 address, click IPv6 and then type the IP address.
4. In Netmask, type the subnet mask of the other network, click Add and then click OK.

When this procedure is complete, the route monitor is bound to NetScaler Gateway.

Note: When a route monitor is not bound to a NetScaler Gateway, the high availability state of either appliance is determined by the state of the interfaces.

To remove a route monitor

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand System and then click High Availability.
2. On the Route Monitors tab, click Action, and then click Configure.
3. Under Configured Route Monitors, select the monitor, click Remove and then click OK.

Configuring link redundancy

January 8, 2024

Link redundancy groups network interfaces together to prevent failover due to a failure on one network interface of an NetScaler Gateway that has other functioning interfaces. The failure of the first interface on the primary NetScaler Gateway triggers failover, although the first interface can still use its second link to serve user requests. When you configure link redundancy, you can group the two interfaces into a failover interface set, preventing the failure of a single link from causing failover to

the secondary NetScaler Gateway, unless all interfaces on the primary NetScaler Gateway are non-functional.

Each interface in a failover interface set maintains independent bridge entries. The monitor interfaces that are enabled and high availability on an NetScaler Gateway that are not bound to a failed interface set are known as critical interfaces, because if any of these interfaces fails, failover is triggered.

To configure link redundancy

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand System and then click High Availability.
2. On the Failover Interface Set tab, click Add.
3. In Name, type a name for the set.
4. In Interfaces, click Add.
5. Under Available Interfaces, select an interface and then click the arrow to move the interface to Configured.
6. Repeat Steps 4 and 5 for the second interface, and then click Create.

You can add as many interfaces as you need for failover between the interfaces.

To remove interfaces from the failover interface set

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand System and then click High Availability.
2. On the Failover Interface Set tab, select a set and then click Remove.

To remove a failover interface set

If you no longer need a failover interface set, you can remove it from NetScaler Gateway.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand System and then click High Availability.
2. On the Failover Interface Set tab, select a set and then click Remove.

Understanding the causes of failover

January 8, 2024

The following events can cause failover in a high availability configuration:

1. If the secondary node does not receive a heartbeat packet from the primary node for a period of time that exceeds the dead interval set on the secondary. For more information about setting the dead interval, see Configuring Communication Intervals. Possible causes for a node not receiving heartbeat packets from a peer node include:
    - A network configuration problem prevents heartbeats from traversing the network between the high availability nodes.
    - The peer node experiences a hardware or software failure that causes it to freeze (hang), reboot, or otherwise stop processing and forwarding heartbeat packets.
2. The primary node experiences a hardware failure of its SSL card.
3. The primary node does not receive any heartbeat packets on its network interfaces for three seconds.
4. On the primary node, a network interface that is not part of a Failover Interface Set (FIS) or a Link Aggregation (LA) channel and has the high availability Monitor (HAMON) enabled, fails. The interfaces are enabled, but go to a DOWN state.
5. On the primary node, all interfaces in an FIS fail. The interfaces are enabled, but go to a DOWN state.
6. On the primary node, an LA channel with HAMON enabled fails. The interfaces are enabled, but go to a DOWN state.
7. On the primary node, all interfaces fail. In this case, failover occurs regardless of the HAMON configuration.
8. On the primary node, all interfaces are manually disabled. In this case, failover occurs regardless of the HAMON configuration.
9. You force a failover by issuing the force failover command on either node.
10. A route monitor that is bound to the primary node goes DOWN.

Forcing failover from a node

January 8, 2024

You might want to force a failover if, for example, you need to replace or upgrade the primary node. You can force failover from either the primary or the secondary node. A forced failover is not propagated or synchronized. To view the synchronization status after a forced failover, you can view the status of the node.

A forced failover fails in any of the following circumstances:

- You force failover on a standalone system.
- The secondary node is disabled.

- The secondary node is configured to remain secondary.

The NetScaler Gateway appliance 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.

Forcing failover on the primary or secondary node

January 8, 2024

If you force failover on the primary node, the primary becomes the secondary and the secondary becomes the primary. Forced failover is possible only when the primary node can determine that the secondary node is UP.

If the secondary node is DOWN, the force failover command returns the following error message: "Operation not possible due to invalid peer state. Rectify and retry."

If the secondary system is in the claiming state or inactive, the command returns the following error message: `"Operation not possible now. Please wait for system to stabilize before retrying."`

If you run the force failover command from the secondary node, the secondary node becomes primary and the primary node becomes secondary. A force failover can occur only if the secondary node's health is good and the node is not configured to stay secondary.

If the secondary node cannot become the primary node, or if the secondary node was configured to stay secondary (using the STAYSECONDARY option), the node displays the following error message: "Operation not possible as my state is invalid. View the node for more information."

To force failover on the primary or a secondary node

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand System and then click High Availability.
2. In the details pane, on the Nodes tab, select the primary node, and then in Actions, click Force Failover.
3. In the Warning dialog box, click Yes.

Forcing the primary node to stay primary

January 8, 2024

In a high availability configuration, you can force the primary NetScaler Gateway to stay primary even after appliance failover. You can only configure this setting on standalone NetScaler Gateway appliances and on the NetScaler Gateway that is the primary appliance in a high availability pair.

To force the primary node to stay primary

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand System and then click High Availability.
2. In the details pane, on the Nodes tab, select a node and then click Edit.
3. Under High Availability Status, click Stay Primary and then click OK.

You can clear this configuration only by using the following command:

```
clear configuration full
```

The following commands do not change the NetScaler Gateway high availability configuration:

```
clear configuration basic
```

```
clear configuration extended
```

Forcing the secondary node to stay secondary

January 8, 2024

In a high availability setup, you can force the secondary NetScaler Gateway to stay secondary, independent of the state of the primary NetScaler Gateway. When you configure NetScaler Gateway to stay secondary, it remains secondary even if the primary NetScaler Gateway fails.

For example, in an existing high availability setup, suppose that you need to upgrade the primary NetScaler Gateway and that this process takes a specified amount of time. During the upgrade, the primary NetScaler Gateway can become unavailable, but you do not want the secondary NetScaler Gateway to take over. You want it to remain the secondary NetScaler Gateway, even if it detects a failure in the primary NetScaler Gateway.

If the status of a NetScaler Gateway in a high availability pair is configured to stay secondary, it does not participate in high availability state machine transitions. You can check the status of the NetScaler Gateway in the configuration utility on the **Nodes** tab.

This setting works on both a standalone and a secondary NetScaler Gateway.

When you set the high availability node, it is not propagated or synchronized and affects only the NetScaler Gateway on which the setting is configured.

To force the secondary node to stay secondary

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand System and then click High Availability.
2. In the details pane, on the Nodes tab, select a node, and then click Edit.
3. Under High Availability Status, click Stay Secondary (Remain in Listen Mode), and then click OK.

To return NetScaler Gateway to service as an active high availability appliance

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand System and then click High Availability.
2. In the details pane, on the Nodes tab, select the appliance that is going to stay the primary node, and then click Open.
3. Under High Availability Status, click Enabled (Actively Participate in HA), and then click OK.

Using Clustering

January 8, 2024

NetScaler Gateway can be deployed in cluster configurations to provide high throughput, high availability, and scalability for VPN client traffic. In a cluster, a group of NetScaler Gateway appliances or VMs operates as a single system image to coordinate user sessions and manage traffic to network resources. A NetScaler Gateway cluster can be built with a minimum of two and a maximum of 32 NetScaler Gateway appliances or VMs configured as cluster nodes.

Read the
NetScaler Clustering documentation before starting to configure your NetScaler Gateway cluster. Pay special attention to the following topics in that documentation.

- See Hardware and Software Requirements to verify that the systems you plan to use meet the requirements.
- See How Clustering Works for a description of clustering concepts.
- See Setting up Inter-Node Communication to plan the deployment and identify any caveats that might be relevant to your environment.

A NetScaler Gateway cluster operates as a spotted VIP configuration type NetScaler cluster.

> **Important:**
>
> The **XenApp and XenDesktop** wizard is not supported for clustering and hence you do not find the **XenApp and XenDesktop** wizard in the **GUI > Navigation pane > Integrate with NetScaler products** section.

Configuring Clustering

January 8, 2024

The primary tasks in setting up NetScaler Gateway clustering are:

1. Decide which NetScaler Gateway appliance or the virtual machine is the configuration coordinator, and create a cluster instance on that system (if one is not already present).
2. Join NetScaler Gateway systems to the cluster as nodes.
3. Create a node group on the cluster instance, with the STICKY option set.
4. Bind a single cluster node to the cluster node group.
5. Configure a NetScaler Gateway virtual server on the configuration coordinator and bind it to the cluster node group.

Multiple methods are available for configuring a NetScaler cluster. The following set of tasks uses the most direct method available in the configuration utility.

To create a NetScaler Gateway cluster instance by using the configuration utility

Once you have the deployment details in order, begin the configuration on the NetScaler Gateway that is the configuration coordinator.

Caution: Creating the cluster instance clears the configuration. If you need to save the existing system configuration for reference, archive a copy before continuing with the cluster configuration. Any existing settings to be used in the cluster can be reapplied on the configuration coordinator after the cluster is established.

1. Log on to the NetScaler configuration utility at the NSIP address.
2. Expand the System node, then the Cluster subnode.
3. In the details pane, click Manage Cluster.
4. In the Cluster Configuration dialog box, set the parameters required to create the cluster.

    a) Enter a Cluster instance ID. Cluster instance ID is the numeric identifier for the cluster instance. The default value is 1 but you can set it to any number from 1 to 16.

b) Enter the Cluster IP address. Cluster IP address is the cluster's configuration coordinator IP address, which is the management IP address for the cluster.
c) Select the preferred Backplane interface. This is this NetScaler Gateway interface to use for communication among the cluster nodes.

5. Click Create.
6. At the prompt to confirm system reboot, click Yes.
7. After the node is UP and sync is successful, from the cluster IP address, change RPC credentials for both the node and cluster IP address. For more information about changing an RPC node password, see Change an RPC node password.
8. Wait for system to restart. Once available, log on to the configuration utility at the Cluster IP address configured in step 4(2).

Note: In the **System Information detail** pane, that the local node at the NSIP address is reported as configuration coordinator. This confirms that the base cluster instance is now operating.

The local node of the configuration coordinator is automatically added to the cluster. More nodes can be added in the following task.

Adding Nodes to a NetScaler Gateway Cluster

Once the cluster instance has been established, you can begin to add other NetScaler Gateway nodes to the cluster.

To add more NetScaler Gateway systems to the cluster, you can use the configuration utility to remotely issue the cluster-node-creation and join-cluster settings.

Note: Adding nodes to the cluster must be completed before configuring your NetScaler Gateway setup. This way, you do not have to repeat the NetScaler Gateway configuration if something goes wrong with your cluster configuration and you want to remove the cluster and begin again.

1. Log on to the NetScaler configuration utility at the Cluster IP address.
2. Expand the **System** node, then the Cluster subnode.
3. In the details pane, click **Manage Cluster**.
4. In the Cluster Nodes details pane, click **Add**.
5. In the **Create Cluster Node** pane, enter a unique Node id for this node.
6. Enter the NetScaler IP address of the system to add as a cluster node.
7. In the **Cluster Node credentials** pane, enter the NetScaler Gateway user name and password for the remote NetScaler Gateway system.
8. In the Configuration Coordinator credentials pane, enter the password for the local authorized user.
9. Click **Create**.

10. When prompted, click **YES** to allow the system configuration to be saved and perform a warm reboot of the remote NetScaler Gateway.
11. After the node is UP and sync is successful, from the cluster IP address, change RPC credentials for both the node and cluster IP address. For more information about changing an RPC node password, see Change an RPC node password.

Repeat steps 4 through 11 for each additional remote NetScaler Gateway system that you want to configure as a cluster node.

Verify that the cluster nodes are included in the Active Node List in the Cluster Nodes detail pane. If any nodes are missing, repeat steps 4 through 10 until all of the necessary nodes are listed.

Creating a Cluster Node Group

Once the cluster nodes have been added, a cluster node group can be created.

1. Log on to the NetScaler configuration utility at the Cluster IP address.
2. Expand the **System** node, then the Cluster subnode.
3. Click **Node Groups**.
4. In the details pane, click **Add**.
5. Enter a name for the cluster node group.
6. Select the **Sticky** option to support the NetScaler Gateway virtual server type.
7. Click **Continue**.

The cluster node group is now established. Before leaving this area of the configuration utility, you can bind the local NetScaler Gateway node to the new cluster node group. This is the only node bound to the cluster group.

Bind the local cluster node to the cluster node group

Because a NetScaler Gateway cluster configuration is a spotted type, only one node can be bound to the node group. The following procedure binds the local node on the configuration coordinator to the node group, but any node in the cluster can be used for this binding.

1. In the Advanced pane, expand Cluster Nodes.
2. In the middle Cluster Nodes pane, select No Cluster Node.
3. On the Cluster Node configuration screen, click Bind.
4. Select the local node represented by the NSIP address for this NetScaler Gateway system.
5. Click Insert.
6. Click OK.
7. Click Done.

The cluster is now populated and ready to share a NetScaler Gateway virtual server as configured by the following task.

Binding a NetScaler Gateway Virtual Server to the Cluster Node Group

With a cluster established, you can proceed to build the NetScaler Gateway configuration the cluster deployment is intended to serve. To tie the configuration to the cluster, you need to create the NetScaler Gateway virtual server and bind it to a cluster node group that is set to type Sticky. After the virtual server is bound to the cluster node group, you can continue to configure the NetScaler Gateway.

If multiple NetScaler Gateway virtual servers are configured, those must be bound to the cluster node group as well.

Note: If NetScaler Gateway virtual servers have not yet been configured, you might have to first enable the NetScaler Gateway and Authentication, Authorization, and Auditing features first under **System > Settings > Configure Basic Features**.

1. Log on to the NetScaler configuration utility at the Cluster IP address.
2. Expand the **System** node, then the Cluster subnode.
3. Click **Node Groups**.
4. In the **Node Group** pane, select the desired node group name, and then click **Edit**.
5. In the **Advanced** pane on the right, expand the **Virtual Servers** option, and then click the + icon to add a virtual server.
6. Choose the VPN Virtual Server type, and then click **Continue**.
7. Click **Bind**.
8. If the needed virtual server is listed, select it, then click **Insert**, and then click **OK**.
9. If you have to create a new virtual server, click **Add**. Proceed through the NetScaler Virtual Server configuration. Minimally, all that is needed is to create the virtual server so that it can be bound to the cluster node group.
10. Once the virtual server is available in the NetScaler Gateway Virtual Servers list, select it, and then click **Insert**.
11. Click **OK**.
12. Click **Done**.

Note: If multiple NetScaler Gateway virtual servers are configured, those must be bound to the cluster node group as well using this same method.

Unified Gateway

January 8, 2024

NetScaler with Unified Gateway: One URL

NetScaler with Unified Gateway enables simplified secure access to any application through a single URL for desktop and mobile users. Behind this single URL, administrators have a single point for configuration, security, and control of remote access to applications. And remote users have an improved experience with seamless single sign-on to all the applications they need along with login/logout once ease of use.

To accomplish this, NetScaler with Gateway, along with NetScaler's Content Switching capacities and extensive authentication infrastructure, provides access to organizational sites and apps through this single URL. Also, remote users can use iOS or Android mobile devices and Linux, PC, or Mac systems with the Citrix Secure Access client for uniform access to the Unified Gateway URL, wherever they might be.

A Unified Gateway deployment allows single URL access to the following categories of applications:

- Intranet applications.
- Clientless applications
- Software as a Service application
- Preconfigured applications served by NetScaler
- Citrix Virtual Apps and Desktops published applications

Intranet applications might be any web-based application that resides inside the secure enterprise network. These are internal resources such as an organizational intranet site, a bug tracking application, or a wiki.

Typically also residing inside the secure enterprise network, the **clientless applications** Unified Gateway provides single URL access to are Outlook Web Access and SharePoint. These applications provide access to Exchange email and team resources without dedicated client software which need to be available to remote users.

SaaS applications, also commonly know as Cloud Apps, are external, cloud-based applications that organizations depend on such as ShareFile, Salesforce, or NetSuite. SAML based single sign-on is supported with those SaaS applications that offer it.

Some organizations might have **preconfigured NetScaler served applications** deployed in a NetScaler load balanced configuration. Often times this is also referred as a 'reverse-proxy'application. Unified Gateway supports these applications when a virtual server for the deployment resides

on the same NetScaler Unified Gateway instance or appliance. These applications might have their own authentication configuration which is independent of the Unified Gateway configuration.

Any published **Citrix Virtual Apps and Desktops published applications** can be made available through a Unified Gateway URL. SmartAccess and SmartControl policies can optionally be applied to granular policy and access control to these resources.

The Unified Gateway Configuration Wizard

The recommended method to configuring a NetScaler with Unified Gateway deployment is to use the Unified Gateway configuration wizard. The wizard walks you through configuration and creates all the necessary virtual servers, policies, and expressions, and applies settings based on the details provided. After initial setup, the wizard can be used to manage your deployment and monitor its operation.

> **Note:**
>
> The Unified Gateway configuration wizard does not perform an initial systems configuration. Your NetScaler Gateway appliance or VPX instance must have basic installation completed before configuring Unified Gateway. Refer to the installation instructions for Configuring NetScaler Gateway with the First-time Setup Wizard to complete basic configuration.

The Unified Gateway elements configured by the wizard are:

- The Unified Gateway primary virtual server
- An SSL Server Certificate for the Unified Gateway virtual server
- A primary and any optional secondary authentication configuration
- A portal theme selection and optional customization
- The user applications that are to be accessed through the Unified Gateway portal

For each of these elements, you need to provide configuration information. For a basic Unified Gateway deployment, the following information is needed.

- For the primary Unified Gateway virtual server, the public IP address and IP port number for the deployment. This is the IP address that resolves in DNS to the Unified Gateway URL's host name. For example, if your Unified Gateway deployment's URL is `https://mycompany.com/`, the IP address must resolve to mycompany.com.

- The signed SSL Server Certificate for the deployment. NetScaler Gateway supports PEM or PFX formatted certificates.

- Primary authentication server information. The authentication systems supported for this authentication configuration are LDAP/Active Directory, RADIUS, and Certificate based. A

secondary LDAP or RADIUS authentication configuration might be created as well. The authentication server IP address must be provided along with any relevant administrator credentials or directory attributes. For Certificate authentication, the device certificate attributes and a CA certificate must be provided.

- A portal theme might be selected. If a customized or branded portal design is desired, custom graphics might be uploaded to the system with the wizard.
- For web-based user applications, the URLs for the individual applications must be specified. For web applications that are to utilize SAML single sign-on authentication, the utility collects the Assertion Consumer Service URL along with other optional SAML parameters. Gather the configuration details in advance for the applications that use a SAML authentication system.
- For Citrix Virtual Apps and Desktops published resources to be made available through the Unified Gateway deployment, you must specify the integration point (StoreFront, the Web Interface, or Web Interface on NetScaler). The utility requires the integration point's fully qualified domain name, the site path, the single sign-on domain, the Secure Ticket Authority (STA) server URL, and others depending on the type of integration point.

Additional Configuration Management

For site specific settings not available in the Unified Gateway configuration utility, such as alternative SSL settings or session policies, you can manage the needed settings in the NetScaler Gateway configuration utility. You can modify these settings on the Content Switching or VPN virtual servers once they are created by the Unified Gateway configuration utility.

Content Switching Virtual Server

This is the NetScaler configuration entity behind the deployment's main IP address and URL. The SSL Server Certificates and parameters are managed on this virtual server. As this virtual server is the responding network host for the deployment, the ICMP server response and RHI state can be modified on this virtual server, if necessary. The Content Switching virtual server can be found under the **Configuration** tab at **Traffic Management** > **Content Switching** > **Virtual Servers**.

> **Important:**
>
> When you upgrade your Unified Gateway environment to release 13.0 build 58.x or later, the DTLS knob is disabled in the content switching virtual server that is configured before the gateway or VPN virtual server. Manually enable the DTLS knob in the content switching virtual server after the upgrade. Do not enable the DTLS knob if you are using the wizard for configuration.

VPN Virtual Server

All other VPN parameters, profiles, and policy bindings for the Unified Gateway configuration are managed on this virtual server, including the main authentication configuration. This entity is managed under the **Configuration** tab at **NetScaler Gateway** > **Virtual Servers**. The relevant VPN virtual server's name includes the name given to the Content Switching virtual server during initial Unified Gateway configuration.

> **Note:**
>
> The VPN virtual servers created for a Unified Gateway deployment are non-addressable and assigned the 0.0.0.0 IP address.

Unified Gateway FAQ

January 8, 2024

What is Unified Gateway?

Unified Gateway is a new feature in the NetScaler 11.0 release, providing the ability to receive traffic on a single virtual server (called a Unified Gateway virtual server) and then internally direct that traffic, as appropriate, to virtual servers that are bound to the Unified Gateway virtual server.

The Unified Gateway feature allows end users to access multiple services by using a single IP address or URL (associated with the Unified Gateway virtual server). Administrators can free up IP addresses and simplify the configuration of the NetScaler Gateway deployment.

Each Unified Gateway virtual server can front-end one NetScaler Gateway virtual server along with zero or more load balancing virtual servers as part of a formation. Unified Gateway works by using the content switching feature of the NetScaler appliance.

Some examples of Unified Gateway deployments:

- Unified Gateway Virtual server -> [one NetScaler Gateway virtual server]
- Unified Gateway Virtual server -> [one NetScaler Gateway virtual server, one load balancing virtual server]
- Unified Gateway Virtual server -> [one NetScaler Gateway virtual server, two load balancing virtual servers]
- Unified Gateway Virtual server -> [one NetScaler Gateway virtual server, three load balancing virtual servers]

Each of the load balancing virtual servers can be any standard load balancing server that a hosts a back-end service, such as Microsoft Exchange or Citrix ShareFile.

Why use Unified Gateway?

The Unified Gateway feature enables end users to access multiple services by using a single IP address or URL (associated with the Unified Gateway virtual server). For administrators, the advantage is that they can free up IP addresses and simplify the configuration of the NetScaler Gateway deployment.

Can there be more than one Unified Gateway virtual server?

Yes. There can be as many Unified Gateway virtual servers as you need.

Why is content switching needed for Unified Gateway?

The content switching feature is required because the content switching virtual server is the one that receives traffic and internally directs it to the appropriate virtual server. The content switching virtual server is the primary component of the Unified Gateway feature.

In releases previous to 11.0, content switching can be used to receive traffic for multiple virtual servers. Is that use also called Unified Gateway?

Use of a content switching virtual server for receiving traffic for multiple virtual servers is supported in releases earlier than 11.0. However, content switching cannot direct traffic to a NetScaler Gateway virtual server.

The enhancements in 11.0 enable a content switching virtual server to direct traffic to any virtual server, including a NetScaler Gateway virtual server.

What has changed with content switching policies in Unified Gateway?

1. A new command line parameter "-targetVserver"is added for the content switching action. The new parameter is used to specify the target NetScaler Gateway virtual server. Example:

   ```
   add cs action UG_CSACT_MyUG -targetVserver UG_VPN_MyUG
   ```

   In the NetScaler Gateway configuration utility, the content switching action has a new option, Target Virtual Server, which can reference a NetScaler Gateway virtual server.

2. A new advanced policy expression, is_vpn_url, can be used to match NetScaler Gateway and authentication-specific requests.

What NetScaler Gateway features are not currently supported in Unified Gateway?

All features are supported in Unified Gateway. However, a minor issue (issue ID 544325) has been reported with native logon through the VPN plug-in. In this case, seamless single sign-on (SSO) does not work.

With Unified Gateway, what is the behavior of EPA scans?

With Unified Gateway, endpoint analysis is triggered only for the NetScaler Gateway access methods, not for NetScaler AAA TM access. If a user tries to access a NetScaler AAA TM virtual server even though the authentication is done on the NetScaler Gateway virtual server, the EPA scan is not triggered. However, if the user is trying to gain clientless VPN/Full VPN access, the configured EPA scan is triggered. In that case, either authentication or seamless SSO is done.

What are the license requirements for Unified Gateway?

Unified Gateway is supported only for Advanced and Premium licenses. It is not available for NetScaler Gateway only or Standard license editions.

Does the NetScaler Gateway virtual server used with Unified Gateway need an IP/Port/SSL configuration?

For a NetScaler Gateway virtual server used with the Unified Gateway virtual server, an IP/Port/SSL configuration is not needed on the NetScaler Gateway virtual server. However, for RDP proxy functionality you can bind the same SSL/TLS server certificate to the NetScaler Gateway virtual server.

Do I need to reprovision SSL/TLS certificates that are on the NetScaler Gateway virtual server for use with a Unified Gateway virtual server?

You do not need to reprovision certificates that are currently bound to your NetScaler Gateway virtual server. You are free to reuse any existing SSL certificates and to bind those to the Unified Gateway virtual server.

What is the difference between a single URL and a multi-host deployment? Which one do I need?

Single URL refers to the ability of the Unified Gateway virtual server handle traffic for one fully qualified domain name (FQDN). This restriction exists when Unified Gateway uses an SSL/TLS server certificate that has the certificate subject populated with the FQDN. For example: ug.citrix.com

If Unified Gateway is using a wildcard server certificate, it can handle traffic for multiple subdomains. For example: *.citrix.com

Another option is SSL/TLS configuration with Server Name Indicator (SNI) functionality to allow binding of multiple SSL/TLS server certificates. Examples: auth.citrix.com, auth.citrix.de, auth.citrix.co.uk, auth.citrix.co.jp

Single host versus multiple hosts is analogous to the way websites are typically hosted on a webserver (for example the Apache HTTP server or Microsoft Internet Information Services (IIS)). If there is a single host, you can use a site path to switch traffic the same way you use alias or "virtual directory" in Apache. If there are multiple hosts, you use a host header to switch traffic similarly to the way you use Virtual Hosts in Apache.

What authentication mechanisms can be used with Unified Gateway?

All existing authentication mechanisms that are compatible with NetScaler Gateway are also compatible with Unified Gateway.

These include LDAP, RADIUS, SAML, Kerberos, Certificate based Authentication, and so on.

Whatever authentication mechanism is configured on the NetScaler Gateway virtual server before the upgrade is automatically used when the NetScaler Gateway virtual server is placed behind the Unified Gateway virtual server. There are no additional configuration steps involved, other than assigning a non-addressable IP address (0.0.0.0) to th NetScaler Gateway virtual server.

What is "SelfAuth"'Authentication?

SelfAuth is not an authentication type by itself. SelfAuth describes how a URL is created. A new command line parameter, `ssotype`, is available for VPN URL configuration. Example:

```
> add vpn url RGB RGB "http://blue.citrix.lab/"-vServerName Blue -
ssotype selfauth
```

SelfAuth is one of the values of the `ssotype` parameter. This type of URL can be used to access resources that are not in the same domain as the Unified Gateway virtual server. The setting can be seen in the configuration utility when configuring a Bookmark.

What is "StepUp"Authentication'?

When extra, more secure levels of authentication are required for accessing a NetScaler AAA TM resource, you can use StepUp authentication. On the command line, use an authnProfile command to set the authenticationLevel parameter. Example:


```
add authentication authnProfile AuthProfile -authnVsName AAATMVserver -
    AuthenticationHost auth.citrix.lab -AuthenticationDomain citrix.lab
    **-**AuthenticationLevel 100
```

This authentication profile is bound to the load balancing virtual server.

Is StepUp authentication supported for NetScaler AAA TM virtual servers?

Yes, it is supported.

What is `login once/logout once`?

`Login Once`: VPN users log in once to either a NetScaler AAA TM or a NetScaler Gateway virtual server. And from then on, VPN users have seamless access to all the Enterprise/Cloud/Web Applications. The user need not be reauthenticated. However, reauthentication is done for special cases, such as NetScaler AAA TM StepUp.

`Logout Once`: After the first NetScaler AAA TM or NetScaler Gateway session is created, it is used to create subsequent NetScaler AAA TM or NetScaler Gateway sessions for that user. If any of those sessions are logged out, the NetScaler appliance also logs out the user's other applications or sessions.

Can common authentication policies be specified at the Unified Gateway level with NetScaler AAA TM load balancing virtual server specific authenticated bound at the load balancing virtual server level? What are the configuration steps to support this use case?

If you need to specify separate authentication policies for the NetScaler AAA TM virtual server behind Unified Gateway, you need to have a separate, independently addressable authentication virtual server (similar to ordinary NetScaler AAA TM configuration). The authentication host setting on the load balancing virtual server has to point to this authentication virtual server.

How do you configure Unified Gateway so that bound NetScaler AAA TM virtual servers have their own authentication policies?

In this scenario, the load balancing server must have the authentication FQDN option set to point to the NetScaler AAA TM virtual server. The NetScaler AAA TM virtual server must have an independent IP address and be reachable from NetScaler and clients.

Is a NetScaler AAA TM Authentication Virtual server required for authenticating users coming through a Unified Gateway virtual server?

No. The NetScaler Gateway virtual server authenticates even the NetScaler AAA TM users.

Where do you specify NetScaler Gateway Authentication policies—at the Unified Gateway virtual server or at the NetScaler Gateway virtual server?

Authentication policies are to be bound to the NetScaler Gateway virtual server.

How do you enable authentication on the NetScaler AAA TM Virtual servers behind a Unified Gateway content switching virtual server?

Enable authentication on the NetScaler AAA TM and point the authentication host to the Unified Gateway content switching FQDN.

How do I add TM Virtual servers behind content switching (single URL versus multi-host)?

There is no difference between adding the NetScaler AAA TM virtual servers for a single URL and adding it for multiple hosts. In either case, the virtual server is added as a target in a content switching action. The difference between single URL vs multi-host is implemented by content-switching policy rules.

What happens to the authentication policies bound to a NetScaler AAA TM load balancing virtual server if that virtual server is moved behind a Unified Gateway virtual server?

Authentication policies are bound to the authentication virtual server, and the authentication virtual server is bound to the load balancing virtual server. For the Unified Gateway virtual server, Citrix recommends having the NetScaler Gateway virtual server as the single authentication point, which negates the need to perform authentication on an authentication virtual server (or even the need for a specific authentication virtual server). Pointing the authentication host to the Unified Gateway virtual server FQDN ensures that authentication is done by the NetScaler Gateway virtual server. If you point the authentication host to content switching for Unified Gateway and still have an authentication virtual server bound, the authentication policies bound to the authentication virtual server are ignored. However, if you point an authentication host to an independent addressable authentication virtual server, the bound authentication policies bound take effect.

How do you configure session policies for NetScaler AAA TM sessions?

If, in Unified Gateway, no authentication virtual server is specified for the NetScaler AAA TM virtual server, the NetScaler AAA TM sessions inherit the NetScaler Gateway session policies. If the authentication virtual server is specified, the NetScaler AAA TM session policies bound to that virtual server are applied.

What are the changes to the NetScaler Gateway portal in NetScaler 11.0?

In NetScaler releases earlier than 11.0, a single portal customization can be set up at the global level. Every gateway virtual server in a given NetScaler appliance uses the global portal customization.

In NetScaler 11.0, with the portal themes feature, you can set up multiple portal themes. Themes can be bound globally or to specific virtual servers.

Does NetScaler 11.0 support NetScaler Gateway portal customization?

Using the configuration utility, you can use the new portal themes feature to customize and create the portal themes completely. You can upload different images, set color schemes, change text labels and so on.

The portal pages that can be customized are:

- Login Page
- Endpoint Analysis Page
- Endpoint Analysis Error Page
- Post Endpoint Analysis Page
- VPN Connection Page
- Portal Home Page

With this release, you can customize NetScaler Gateway virtual servers with unique portal designs.

Are portal themes supported in NetScaler high availability or cluster deployments?

Yes. Portal Themes are supported in NetScaler high availability and cluster deployments.

Do my customizations be migrated as part of the NetScaler 11.0 upgrade process?

No. Existing customizations to the NetScaler Gateway portal page that are invoked through rc.conf/rc.netscaler file modification or by using custom theme functionality in 10.1/10.5 is not be automatically migrated upon upgrade to NetScaler 11.0.

Are there any pre-upgrade steps to follow to be ready for portal themes in NetScaler 11.0?

Any existing customizations must be removed from the rc.conf or rc.netscaler files.

The other option is that if custom themes are used, they have to be assigned the Default setting:

1. Navigate to **Configuration > NetScaler Gateway > Global Settings**
2. Click **Change Global Settings**.
3. Click **Client Experience** and select **Default** from the **UI Theme** list.

I have customizations that are stored on the NetScaler instance, invoked by rc.conf or rc.netscaler. How do I move to portal themes?

Citrix Knowledge Center article CTX126206 details such a configuration for NetScaler 9.3 and 10.0 releases up to 10.0 build 73.5001.e. Since NetScaler 10.0 build 10.0 73.5002.e (including 10.1 and 10.5), the UITHEME CUSTOM parameter has been available to help customers retain their customizations across reboots. If the customizations are stored on the NetScaler hard drive and you would like to continue using these customizations, back up the 11.0 GUI files and insert them into the existing custom theme file. If you want to move to portal themes, you must first unset the UITHEME parameter in the Global Settings or the Session profile, under **Client Experience**. Or, you can set it to DEFAULT or GREENBUBBLE. Then you are able to start to create and bind a Portal Theme.

How can I export my current customizations and save them before upgrading to NetScaler 11.0? Can I move the exported files to a different NetScaler appliance?

The customized files that were uploaded to the **ns_gui_custom** folder are on the disk and persist across upgrades. However, these files might not be entirely compatible with the new NetScaler 11.0 kernel and other GUI files that are part of the kernel. Therefore, Citrix recommends backing up the 11.0 GUI files and customizing the backups.

Moreover, there is no utility in the configuration utility to export the **ns_custom_gui** folder to another NetScaler appliance. Use SSH or a file transfer utility such as WinSCP to take the files off the NetScaler instance.

Are portal themes supported for NetScaler AAA TM virtual servers?

Yes. Portal Themes are supported for NetScaler AAA TM virtual servers.

What changed in the RDP Proxy feature for NetScaler Gateway 11.0?

Many enhancements have been made to RDP Proxy since the NetScaler 10.5.e enhancement release. In NetScaler 11.0 this feature is available from the first released build.

Licensing changes

The RDP Proxy feature in NetScaler 11.0 can be used only with Premium and Advanced editions. Citrix Concurrent User (CCU) licenses must be obtained for each user.

Enable Command

In NetScaler 10.5.e there was no command to enable RDP Proxy. In NetScaler 11.0, the enable command has been added:

```
enable feature rdpproxy
```

The feature must be licensed to run this command.

Other RDP Proxy Changes

A Pre-shared Key (PSK) attribute on the server profile has been made mandatory.

To migrate existing NetScaler 10.5.e configurations for RDP proxy to NetScaler 11.0, the following details must be understood and addressed.

If an administrator wants to add an existing RDP proxy configuration to a chosen Unified Gateway deployment:

- The NetScaler Gateway virtual server's IP address must be edited and set to a non-addressable IP address (0.0.0.0).
- Any SSL/TLS server certificates, authentication policies must be bound to the NetScaler Gateway virtual server that is part of the chosen Unified Gateway formation.

How do you migrate a Remote Desktop Protocol (RDP) Proxy configuration based on NetScaler 10.5.e to NetScaler 11.0?

Option 1: Keep the existing NetScaler Gateway virtual server with RDP Proxy configuration as is, with a Premium or Advanced license.

Option 2: Move the existing NetScaler Gateway virtual server with RDP Proxy configuration, placing it behind a Unified Gateway virtual server.

Option 3: Add a standalone NetScaler Gateway virtual server with RDP Proxy configuration to an existing Standard Edition appliance.

How do you set up NetScaler Gateway for RDP proxy configuration using the NetScaler 11.0 release?

There are two options for deploying RDP proxy using the NS 11.0 release:

1. Using an externally facing NetScaler Gateway virtual server. This requires one externally visible IP address/FQDN for the NetScaler Gateway virtual server. This option is what is available in NetScaler 10.5.e.
2. Using a Unified Gateway virtual server front-ending the NetScaler Gateway virtual server.

With Option 2 the NetScaler Gateway virtual server does not require its own IP address/FQDN, because it uses a non-addressable IP address (0.0.0.0).

Is HDX Insight compatible with Unified Gateway?

When NetScaler Gateway is deployed with Unified Gateway, the following conditions must be met:

- The NetScaler Gateway virtual server must have a valid SSL certificate bound to it.
- The NetScaler Gateway virtual server must be in an UP state to generate AppFlow records on NetScaler ADM, for HDX Insight reporting.

How do I migrate my existing HDX Insight configuration?

No migration is needed. AppFlow policies bound to a NetScaler Gateway virtual server carry over if that NetScaler Gateway virtual server is put behind a Unified Gateway virtual server.

For existing data on NetScaler ADM for the NetScaler Gateway virtual server, there are two possibilities:

- If the IP Address of the NetScaler Gateway virtual server is assigned to a Unified Gateway virtual server as part of migration to Unified Gateway, the data remains linked to the NetScaler Gateway virtual server
- If the Unified Gateway virtual server is assigned a separate IP address, AppFlow data from the NetScaler Gateway virtual server is linked to that new IP address. Therefore, existing data is not part of new data.

VPN configuration on a NetScaler Gateway appliance

January 8, 2024

> **Important:**
>
> The screen captures in this section are maintained in a grayscale scheme for the following reasons:
>
> - Help visually impaired readers particularly those with color-blindness or color deficiency.
> - Use of a grayscale image represents the image in a generic form that shows no impact of color coding customization that might have been done in the user's browser or the operating system.

Users can use the following methods to connect to your organization's network resources through NetScaler Gateway:

- Citrix Workspace app that contains all Citrix plug-ins installed on the user device.
- Citrix Workspace app for web that allows user connections to applications, desktops, and ShareFile by using a web browser.
- Secure Hub to allow users to access Secure Mail, WorxWeb, and mobile apps from their iOS and Android devices.
- Citrix Secure Access client for Windows, macOS X, or Linux.
- NetScaler Gateway app for iOS and Android.
- Clientless access that provides users with the access they need without installing user software.
- Interoperability with Citrix SD-WAN plug-in.

If users install the Citrix Secure Access client and then install Citrix Workspace app from Citrix Virtual Apps 6.5 for Windows Server 2008 (including Feature Pack and Feature Pack 2), Citrix Virtual Desktops 7.0 or newer, Citrix Workspace app automatically adds the Citrix Secure Access client. Users can connect with the Citrix Secure Access client from a web browser or from Citrix Workspace app.

SmartAccess determines automatically the methods of access that are allowed for a user device based on the results of an endpoint analysis scan. For more information about SmartAccess, see Configuring SmartAccess.

NetScaler Gateway supports Citrix Endpoint Management mobile productivity apps for iOS and Android mobile devices. NetScaler Gateway contains Secure Browse that allows connections to NetScaler Gateway from iOS mobile devices that establish the micro VPN tunnel. Android devices that connect with the Secure Hub also establish a micro VPN tunnel automatically that provides secure web and mobile application-level access to resources in your internal network. If users connect from an Android device with mobile productivity apps, you must configure DNS settings on NetScaler Gateway. For details, see Support DNS Queries by Using DNS Suffixes for Android Devices.

How users connect with the Citrix Secure Access client

January 8, 2024

NetScaler Gateway operates as follows:

- When users attempt to access network resources across the VPN tunnel, the Citrix Secure Access client encrypts all network traffic destined for the organization's internal network and forwards the packets to NetScaler Gateway.
- NetScaler Gateway terminates the SSL tunnel, accepts any incoming traffic destined for the private network, and forwards the traffic to the private network. NetScaler Gateway sends traffic back to the remote computer over a secure tunnel.

When users type the web address, they receive a logon page where they enter their credentials and log on. If the credentials are correct, NetScaler Gateway finishes the handshake with the user device.

If the user is behind a proxy server, the user can specify the proxy server and authentication credentials. For more information, see Enabling Proxy Support for User Connections.

The Citrix Secure Access client is installed on the user device. After the first connection, if users log on by using a Windows-based computer, they can use the icon in the notification area to establish the connection.

Establish the secure tunnel

When users connect with the Citrix Secure Access client, Secure Hub, or Citrix Workspace app, the client software establishes a secure tunnel over port 443 (or any configured port on NetScaler Gateway) and sends authentication information. When the tunnel is established, NetScaler Gateway sends configuration information to the Citrix Secure Access client, Secure Hub, or Citrix Workspace app describing the networks to be secured and containing an IP address if you enable address pools.

Tunnel private network traffic over secure connections

When the Citrix Secure Access client starts and the user is authenticated, all network traffic destined for specified private networks is captured and redirected over the secure tunnel to NetScaler Gateway. Citrix Workspace app must support the Citrix Secure Access client to establish the connection through the secure tunnel when users log on.

Secure Hub, Secure Mail, and WorxWeb use Micro VPN to establish the secure tunnel for iOS and Android mobile devices.

NetScaler Gateway intercepts all network connections that the user device makes and multiplexes them over Secure Sockets Layer (SSL) to NetScaler Gateway, where the traffic is demultiplexed and the connections are forwarded to the correct host and port combination.

The connections are subject to administrative security policies that apply to a single application, a subset of applications, or an entire intranet. You specify the resources (ranges of IP address/subnet pairs) that remote users can access through the VPN connection.

The Citrix Secure Access client intercepts and tunnels the following protocols for the defined intranet applications:

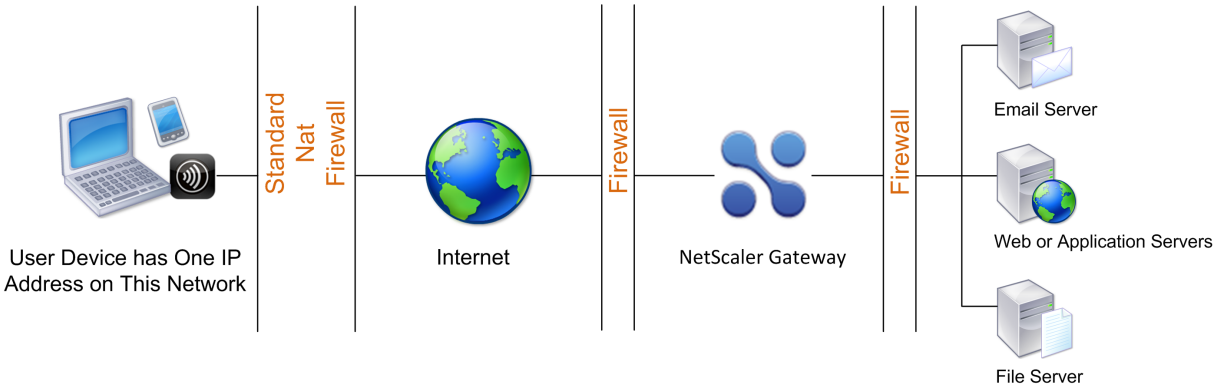
- TCP (all ports)
- UDP (all ports)
- ICMP (types 8 and 0 - echo request/reply)

Connections from local applications on the user device are securely tunneled to NetScaler Gateway, which reestablishes the connections to the target server. Target servers view connections as originating from the local NetScaler Gateway on the private network, thus hiding the user device. This is also called reverse Network Address Translation (NAT). Hiding IP addresses adds security to source locations.

Locally, on the user device, all connection-related traffic, such as SYN-ACK, PUSH, ACK, and FIN packets, is recreated by the Citrix Secure Access client to appear from the private server.

Connect through firewalls and proxies

Users of the Citrix Secure Access client are sometimes located inside another organization's firewall, as shown in the following figure:



NAT firewalls maintain a table that allows them to route secure packets from NetScaler Gateway back to the user device. For circuit-oriented connections, NetScaler Gateway maintains a port-mapped, reverse NAT translation table. The reverse NAT translation table enables NetScaler Gateway to match connections and send packets back over the tunnel to the user device with the correct port numbers so that the packets return to the correct application.

Control upgrade of Citrix Secure Access clients

System Administrators control how the NetScaler plug-in performs when its version does not match the NetScaler Gateway revision. The new options control the plug-in upgrade behavior for Mac, and Windows or operating systems.

For VPN plug-ins, the upgrade option can be set in two places in the NetScaler appliance user interface:

- At the Global Settings
- At the Session Profile level

Requirements

- Windows EPA and VPN plug-in version must be greater than 11.0.0.0
- Mac EPA plug-in version must be greater than 3.0.0.31
- Mac VPN plug-in version must be greater than 3.1.4 (357)

> **Note:**
>
> If the NetScaler appliance is upgraded to the 11.0 release, all previous VPN (and EPA) plug-ins upgrade to the latest version irrespective of upgrade control configuration. For subsequent upgrades, they respect the previous upgrade control configuration.

Plug-in behaviors

For each client type, NetScaler Gateway allows the following three options to control plug-in upgrade behavior:

- **Always**

The plug-in always gets upgraded whenever the end user's plug-in version doesn't match with the plug-in shipped with the NetScaler appliance. This is the default behavior. Choose this option if you don't want multiple plug-in versions running in your enterprise.

- **Essential** (and security)

The plug-in only upgraded when it is deemed necessary. Upgrades are deemed necessary in the following two circumstances

- Installed Plug-in is incompatible with the current NetScaler appliance version.
- Installed Plug-in must be updated for the necessary security fix.

Choose this option if you want to minimize the number of plug-in upgrades, but don't want to miss any plug-in security updates

- **Never**

The plug-in does not get upgraded.

CLI parameters for controlling VPN plug-in upgrade

NetScaler Gateway supports two types of plug-ins (EPA and VPN) for Windows and Mac operating systems. To support VPN plug-in upgrade control at the session level, NetScaler Gateway supports two session profile parameters named WindowsinPluginUpgrade and MacPluginUpgrade.

These parameters are available at global, virtual server, group, and user level. Each parameter can have a value of Always, Essential or Never. For a description of these parameters see Plug-in Behaviors.

CLI parameters for controlling EPA plug-in upgrade

NetScaler Gateway supports EPA plug-ins for Windows and Mac operating systems. To support EPA plug-in upgrade control at the virtual server level, NetScaler Gateway supports two virtual server parameters named windowsEPAPluginUpgrade and macEPAPluginUpgrade.

The parameters are available at the virtual server level. Each parameter can have a value of Always, Essential or Never. For a description of these parameters see Plug-in Behaviors

VPN configuration

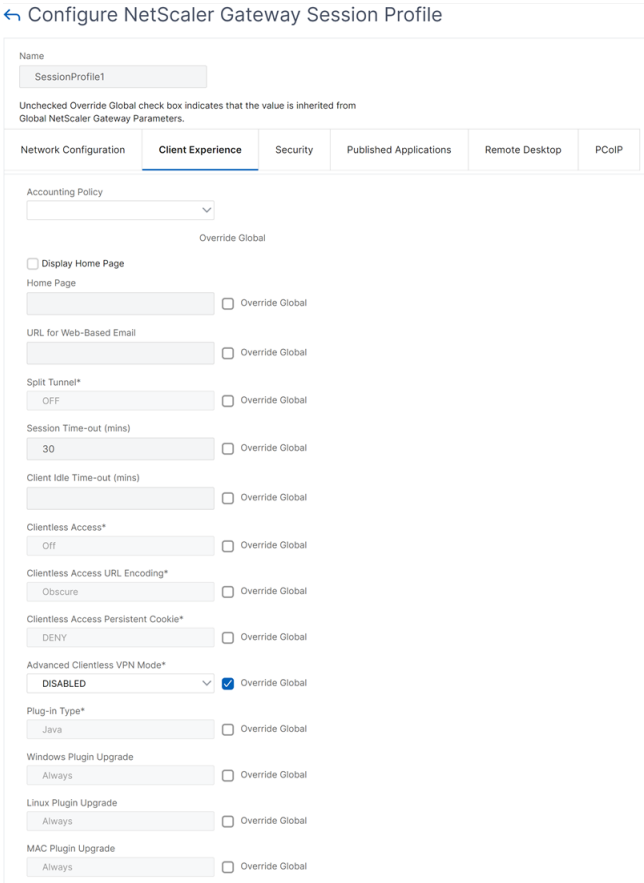
Follow these steps for the **VPN configuration of** Windows, Linux, and Mac plug-ins.

1. Go to **NetScaler > Policies > Session.**
2. Select the desired session policy, and then click **Edit**.
3. Select the **Client Experience** tab.
4. These dialog boxes options affect the upgrade behavior.

   - Always
   - Essential
   - Never

   The default is Always.

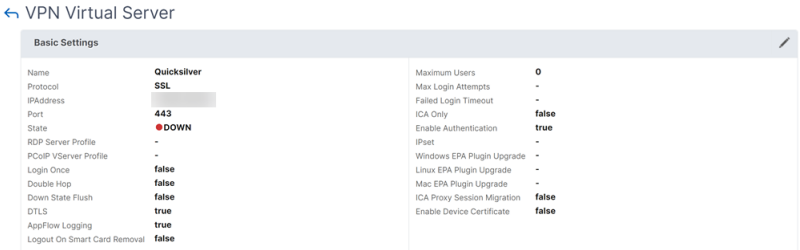
5. Select the check box to the right of each option. Select the frequency to apply the upgrade behavior.



EPA configuration

Follow these steps for the EPA configuration of Windows, Linux, and Apple plug-ins.

1. Go to **NetScaler Gateway > Virtual Servers**.
2. Select a server and click the **Edit** button.
3. Click the **pencil** icon.



4. Click **More**

5. The dialog boxes that appear affect the upgrade behavior. The available options are:
    - Always
    - Essential
    - Never

Full VPN setup on NetScaler Gateway

January 8, 2024

This section describes how to configure full VPN setup on a NetScaler Gateway appliance. It contains networking considerations and the ideal approach for resolving issues from the networking perspective.

Prerequisites

- Install an SSL certificate and bind it to the VPN virtual server.
    - CTX109260 - How to Generate and Install a Public SSL Certificate on a NetScaler Appliance
    - CTX122521 - How to Replace the Default Certificate of a NetScaler Appliance with a Trusted CA Certificate that Matches the host name of the Appliance
    - NetScaler documentation - Binding the Certificate-Key Pair to the SSL-Based Virtual Server
- Create an authentication profile for NetScaler Gateway.
    - For additional information, refer to NetScaler documentation - Configuring External User Authentication
    - For additional information, refer to Checklist: Use AD FS to implement and manage single sign-on
- Download VPN Client.
- Create a session policy allowing full VPN connections.

When users connect with the Citrix Secure Access client, Secure Hub, or Citrix Workspace app, the client software establishes a secure tunnel over port 443 (or any configured port on NetScaler Gateway) and sends authentication information. Once the tunnel has been established, NetScaler Gateway sends configuration information to the Citrix Secure Access client, Citrix Secure Hub, or Citrix Workspace app describing the networks to be secured. That information also contains an IP address if you enable intranet IPs.

You configure user device connections by defining the resources users can access in the internal network. Configuring user device connections includes the following:

- Split tunneling
- IP addresses for users, including address pools (intranet IPs)
- Connections through a proxy server
- Defining the domains to which users are allowed access
- Time-out settings
- Single sign-on
- User software that connects through NetScaler Gateway
- Access for mobile devices

You configure most user device connections by using a profile that is part of a session policy. You can also define user device connection settings by using per-authentication, traffic, and authorization policies. They can also be configured using intranet applications.

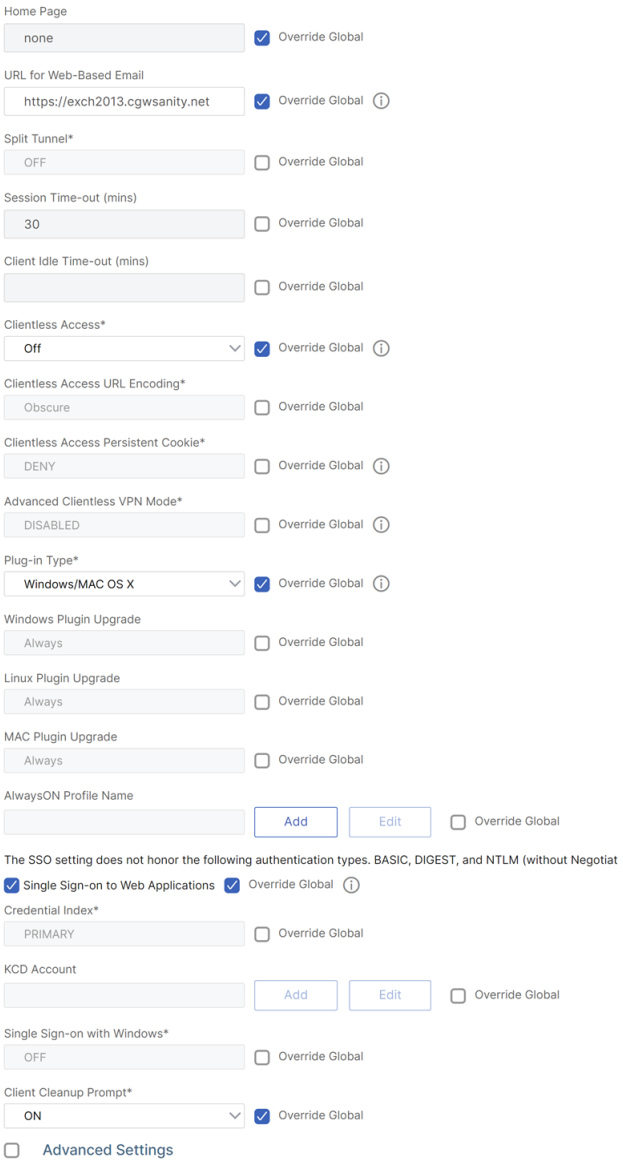
Configure a full VPN setup on a NetScaler Gateway appliance

To configure a VPN setup on the NetScaler Gateway appliance, complete the following procedure:

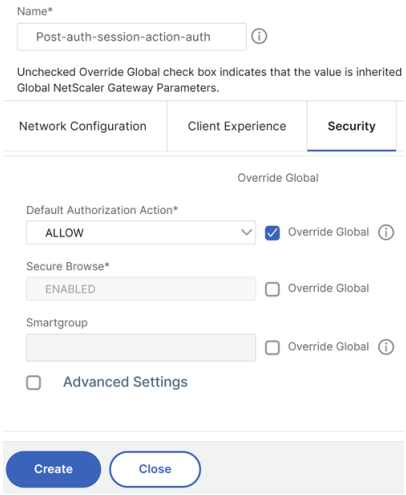
1. Navigate to **Traffic Management > DNS**.
2. Select the Name Servers node, as shown in the following screenshot. Ensure that the DNS name server is listed. If it is not available, add a DNS Name Server.

3. Expand **NetScaler Gateway > Policies**.
4. Select the **Session** node.
5. In the NetScaler Gateway Session Policies and Profiles page, click the **Profiles** tab click **Add**. For each component you configure in the Configure NetScaler Gateway Session Profile dialog box, ensure that you select the **Override Global** option for the respective component.
6. Click the **Client Experience** tab.
7. Type the intranet portal URL in the Home Page field if you would like to present any URL when the user logs into the VPN. If the home page parameter is set to “nohomepage.html,”the home page is not displayed. When the plug-in starts, a browser instance starts and gets killed automatically.
8. Ensure to select the desired setting from the Split Tunnel list.
9. Select **OFF** from the **Clientless Access** list if you want FullVPN.

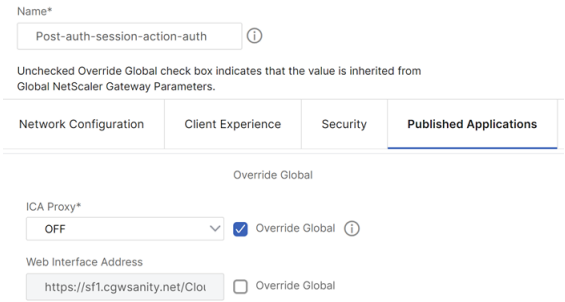
10. Ensure that **Windows/Mac OS X** is selected from the **plug-in Type** list.
11. Select the **Single Sign-on to Web Applications** option if desired.
12. Ensure that the **Client Cleanup Prompt** option is selected if necessary, as shown in the following screenshot:



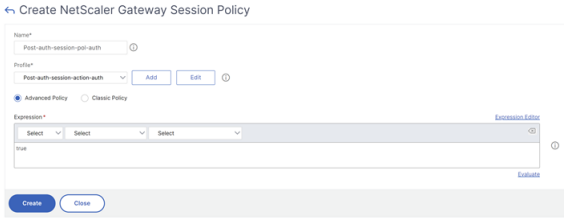
13. Click the **Security** tab.
14. Ensure that **ALLOW** is selected from the **Default Authorization Action** list.



15. Click the **Published Applications** tab.
16. Ensure that **OFF** is selected from the **ICA Proxy** list under the **Published Applications** option.



17. Click **Create**.
18. Click **Close**.
19. Click the **Policies** tab of the NetScaler Gateway Session Policies and Profiles page in the virtual server or activate the Session Policies at the GROUP/USER Level as required.
20. Create a session policy with a required expression or true, as shown in the following screenshot:

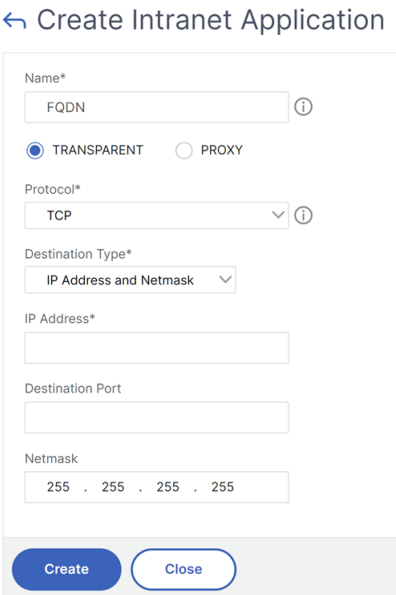


21. Bind the Session policy to the VPN virtual server. For details, see Bind session policies.

    If Split Tunnel was configured to ON, you must configure the Intranet Applications you would like the users to access when connected to the VPN. For details on Intranet Applications, see Configure intranet applications for the Citrix Secure Access client.

    a) Go to **NetScaler Gateway > Resources > Intranet Applications**.

b) Create an Intranet Application. Select Transparent for FullVPN with Windows client. Select the protocol that you would like to allow (TCP, UDP, or ANY), destination type (IP address and mask, IP address range, or host name).



c) If necessary, set a new policy for VPN on iOS and Android using the following expression: `HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixVPN")&&HTTP.REQ.HEADER("User-Agent").CONTAINS("NSGiOSplugin")&&HTTP.REQ.HEADER("User-Agent").CONTAINS("Android")`

d) Bind the Intranet Applications created at the USER/GROUP/VSERVER level as required.

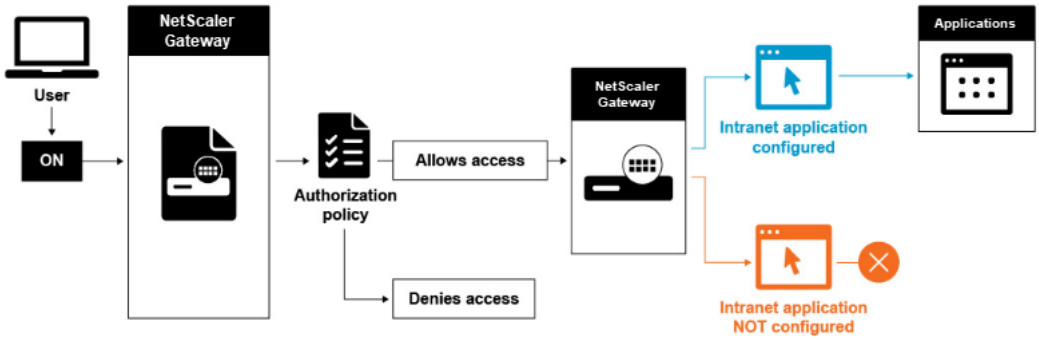
Configure split tunneling

1. Navigate to **Configuration** > **NetScaler Gateway > Policies > Session**.
2. In the details pane, on the Profiles tab, select a profile and then click **Edit**.
3. On the **Client Experience** tab, next to **Split Tunnel**, select **Global Override**, select an option, and then click **OK**.

   Configuring Split Tunneling and Authorization

   When planning your NetScaler Gateway deployment, it is important to consider split tunneling and the default authorization action and authorization policies.

   For example, you have an authorization policy that allows access to a network resource. You have split tunneling set to ON and you do not configure intranet applications to send network traffic through NetScaler Gateway. When NetScaler Gateway has this type of configuration, access to the resource is allowed, but users cannot access the resource.



If the authorization policy denies access to a network resource, the Citrix Secure Access client sends traffic to NetScaler Gateway, but access to the resource is denied in the following conditions.

- You have split tunneling set to ON.
- Intranet applications are configured to route network traffic through NetScaler Gateway

For more information about authorization policies, review the following:

- Configuring Authorization
- Configuring Authorization Policies
- Setting Default Global Authorization

To configure network access to internal network resources

1. Navigate to **Configuration** > **NetScaler Gateway > Resources > Intranet Applications**.
2. In the details pane, click **Add**.
3. Complete the parameters for allowing network access, click **Create**, and then click **Close**.

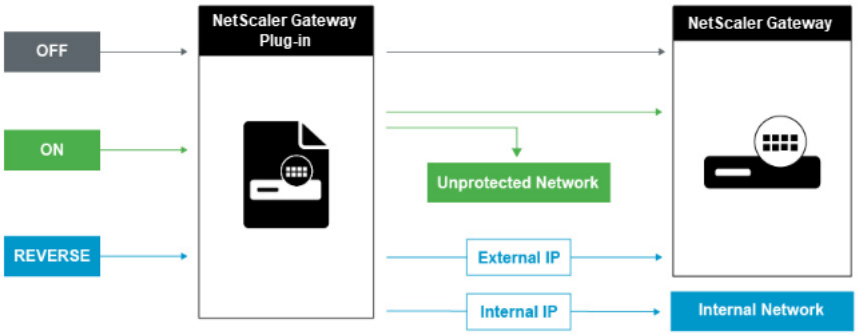
When we do not set up the intranet IPs for the VPN users, the user sends the traffic to the NetScaler Gateway VIP and then from there the NetScaler appliance builds a new packet to the intranet application resource on the internal LAN. This new packet is going to be sourced from the SNIP toward the intranet application. From here, the intranet application gets the packet, processes it and then attempts to reply to the source of that packet (the SNIP in this case). The SNIP gets the packet and sends the reply to the client who made the request.

When an Intranet IP address is used, the user sends the traffic to the NetScaler Gateway VIP and then from there the NetScaler appliance is going to map the client IP into one of the configured INTRANET IPs from the Pool. Be advised that the NetScaler appliance is going to own the Intranet IP pool and for this reason these ranges must not be used in the internal network. The NetScaler appliance assigns an Intranet IP for the incoming VPN connections like a DHCP server would do. The NetScaler appliance builds a new packet to the intranet application on the LAN that the user would access. This new packet is going to be sourced from one of the Intranet IPs toward the intranet application. From here, intranet applications get the packet, process it and then attempt to reply to the source of that packet (the

INTRANET IP). In this case the reply packet needs to be routed back to the NetScaler appliance, where the INTRANET IPs are located (Remember, the NetScaler appliance owns the Intranet IPs subnets). To accomplish this task, the network administrator must have a route to the INTRANET IP, pointing to one of the SNIPs. It is recommended to point the traffic back to the SNIP that holds the route from which the packet leaves the NetScaler appliance the first time to avoid any asymmetric traffic.

Split tunneling options

The following are the various split tunneling options.



Split tunnel OFF

When the split tunnel is set to off, the Citrix Secure Access client captures all network traffic originating from a user device and sends the traffic through the VPN tunnel to NetScaler Gateway. In other words, the VPN client establishes a default route from the client PC pointing to the NetScaler Gateway VIP, meaning that all the traffic needs to be sent through the tunnel to get to the destination. Since all the traffic is going to be sent through the tunnel, authorization policies must determine whether the traffic is allowed to pass through to internal network resources or be denied.

While set to “off,”all traffic is going through the tunnel including Standard Web traffic to websites. If the goal is to monitor and control this web traffic then you must forward these requests to an external Proxy using the NetScaler appliance. User devices can connect through a proxy server for access to internal networks as well.
NetScaler Gateway supports the HTTP, SSL, FTP, and SOCKS protocols. To enable proxy support for user connections, you must specify these settings on NetScaler Gateway. You can specify the IP address and port used by the proxy server on NetScaler Gateway. The proxy server is used as a forward proxy for all further connections to the internal network.

For more information review the following links:

- Enabling Proxy Support for User Connections

Split tunnel ON

You can enable split tunneling to prevent the Citrix Secure Access client from sending unnecessary network traffic to NetScaler Gateway. If the split tunnel is enabled, the Citrix Secure Access client sends only traffic destined for networks protected (intranet applications) by NetScaler Gateway through the VPN tunnel. The Citrix Secure Access client does not send network traffic destined for unprotected networks to NetScaler Gateway. When the Citrix Secure Access client starts, it obtains the list of intranet applications from NetScaler Gateway and establishes a route for each subnet defined on the intranet application tab in the client PC. The Citrix Secure Access client examines all packets transmitted from the user device and compares the addresses within the packets to the list of intranet applications (routing table created when the VPN connection was started). If the destination address in the packet is within one of the intranet applications, the Citrix Secure Access client sends the packet through the VPN tunnel to NetScaler Gateway. If the destination address is not in a defined intranet application, the packet is not encrypted and the user device then routes the packet appropriately using the default routing originally defined on the client PC. "When you enable split tunneling, intranet applications define the network traffic that is intercepted and send through the tunnel".

Reverse split tunnel

NetScaler Gateway also supports reverse split tunneling, which defines the network traffic that NetScaler Gateway does not intercept. If you set split tunneling to reverse, intranet applications define the network traffic that NetScaler Gateway does not intercept. When you enable reverse split tunneling, all network traffic directed to internal IP addresses bypasses the VPN tunnel, while other traffic goes through NetScaler Gateway. Reverse split tunneling can be used to log all non-local LAN traffic. For example, if users have a home wireless network and are logged on with the Citrix Secure Access client, NetScaler Gateway does not intercept network traffic destined to a printer or another device within the wireless network.

> **Note:**
>
> Citrix Secure Access client for Windows also supports FQDN based reverse split tunnel from Citrix Secure Access version 22.6.1.5 version and later.

Points to note IP-based reverse split-tunneling:

- Number of IP address-based rules is limited to 1024.
- Supported with both DNE and WFP drivers.

Host name-based reverse split-tunneling:

- The number of host names that can be accessed during a VPN session is restricted by the number of usable IP addresses specified in the FQDN spoofing range. This is because every host name

takes up one IP address from the FQDN spoofing range. Once the IP range is exhausted, the least recently assigned IP address is reused for the next new host name.

- DNS suffixes must be configured.

> **Note:**
>
> For Windows clients, host name-based reverse split-tunneling is supported only with the WFP driver. Enable the WFP driver mode by setting "EnableWFP"registry value to `1`. For more information, see Windows Citrix Secure Access client using Windows Filtering Platform.

IP-based and host name-based reverse split-tunneling:

- Supported only with the WFP driver. All the other guidelines mentioned in IP-based reverse split-tunneling and host name-based reverse split-tunneling are applicable.

Configure name service resolution

During installation of NetScaler Gateway, you can use the NetScaler Gateway wizard to configure other settings, including name service providers. The name service providers translate the fully qualified domain name (FQDN) to an IP address. In the NetScaler Gateway wizard, you can also perform the following:

- Configure a DNS or WINS server
- Set the priority of the DNS lookup
- Set the number of times to retry the connection to the server.

When you run the NetScaler Gateway wizard, you can add a DNS server then. You can add another DNS servers and a WINS server to NetScaler Gateway by using a session profile. You can then direct users and groups to connect to a name resolution server that is different from the one you originally used the wizard to configure.

Before configuring another DNS server on NetScaler Gateway, create a virtual server that acts as a DNS server for name resolution.

To add a DNS or WINS server within a session profile

1. In the configuration utility, configuration tab > **NetScaler Gateway > Policies > Session**.
2. In the details pane, on the Profiles tab, select a profile and then click Open.
3. On the Network Configuration tab, do one of the following:
    - To configure a DNS server, next to **DNS Virtual Server**, click **Override Global**, select the server, and then click **OK**.

- To configure a WINS server, next to **WINS Server IP**, click **Override Global**, type the IP address and then click **OK**.

References

- Split tunneling
- How users connect with the Citrix Secure Access client
- About NetScaler Gateway
- Select the user access method

Select the user access method

January 8, 2024

You can configure NetScaler Gateway to provide user connections through the following scenarios:

- User connections by using Citrix Workspace app. Citrix Workspace app is compatible StoreFront or the Web Interface to provide users with access to published applications or virtual desktops in a server farm. Citrix Workspace app is software that uses the ICA network protocol to establish user connections. Users install Citrix Workspace app on the user device. When users install Citrix Workspace app on their Windows-based or Mac-based computer, Citrix Workspace app subsumes all plug-ins, including the Citrix Secure Access client for user connections. NetScaler Gateway also supports connections from Citrix Workspace app for Android and Citrix Workspace app for iOS. Users can connect to their virtual desktops and Windows-based, web, mobile, and SaaS applications through Citrix Endpoint Management, StoreFront, or the Web Interface.
- User connections with Secure Hub. Users can connect to mobile, web, and SaaS applications configured in Endpoint Management. Users install Secure Hub on their mobile device (Android or iOS). When users log on to Secure Hub, they can install WorxMail and WorxWeb, along with any other mobile app you installed in Endpoint Management. Secure Hub, Secure Mail, and WorxWeb use Micro VPN technology to establish connections through NetScaler Gateway.
- User connections by using the Citrix Secure Access client as a standalone application. The Citrix Secure Access client is software that users can download and install on a user device. When users log on with the plug-in, users can access resources in the secure network as if they were in the office. Resources include email servers, file shares, and intranet websites.
- User connections by using clientless access. Clientless access provides users with the access they need without requiring installation of software, such as the Citrix Secure Access client or Citrix Workspace app, on the user device. Clientless access allows connections to a limited set

of web resources, such as Outlook Web Access or SharePoint, applications published on Citrix Virtual Apps, virtual desktops from Citrix Virtual Apps and Desktops, and file shares in the secure network through the Access Interface. Users connect by entering the NetScaler Gateway web address in a web browser and then select clientless access from the choices page.

- User connections if a preauthentication or post-authentication scan fails. This scenario is called access scenario fallback. Access scenario fallback allows a user device to fall back from the Citrix Secure Access client to StoreFront or the Web Interface, by using Citrix Workspace app, if the user device does not pass the initial endpoint analysis scan.

  If users log on to NetScaler Gateway through Citrix Workspace app, the preauthentication scan does not work. Post-authentication scans do work when NetScaler Gateway establishes the VPN tunnel.

Users can download and install the Citrix Secure Access client by using the following methods:

- Connecting to NetScaler Gateway by using a web browser.
- Connecting to StoreFront that is configured to accept NetScaler Gateway connections.
- Installing the plug-in by using a Group Policy Object (GPO).
- Uploading the NetScaler plug-in to the Merchandising Server.

Deploy Citrix Secure Access client for user access

January 8, 2024

NetScaler Gateway comes with the following plug-ins for user access:

- Citrix Secure Access client for Windows
- Citrix Secure Access client for Mac

When users log on to NetScaler Gateway for the first time, they download and install the Citrix Secure Access client from a webpage. Users log on by clicking the NetScaler Gateway icon in the notification area on a Windows-based computer. On a macOS X computer, users can log on from the **Dock or the Applications** menu. If you upgrade NetScaler Gateway to a new software version, the Citrix Secure Access client updates automatically on the user device.

Deploy the Citrix Secure Access client by using the MSI installer package

You can deploy the Citrix Secure Access client by using a Microsoft Active Directory infrastructure or a standard third-party MSI deployment tool, such as Windows Server Update Services. If you use a tool that supports Windows Installer packages, you can deploy the packages with any tool that supports

MSI files. Then, you use your deployment tool to deploy and install the software on the appropriate user devices.

Advantages of using a centralized deployment tool

- Ability to adhere to security requirements. For example, you can install user software without enabling software installation privileges for non-administrative users.
- Control over software versions. You can deploy an updated version of the software to all users simultaneously.
- Scalability. A centralized deployment strategy easily scales to support more users.
- Positive user experience. You can deploy, test, and troubleshoot installation-related issues without involving users in this process.

Citrix recommends this option when administrative control over the installation of user software is preferred and access to user devices is readily available.

For more information, see Deploying the Citrix Secure Access client from Active Directory.

Determine which software plug-in to deploy

If your NetScaler Gateway deployment does not require any software plug-in on user devices, your deployment is considered to provide clientless access. In this scenario, users need only a Web browser to access network resources. However, certain features require the plug-in software on the user's device.

Select the Citrix Secure Access client for users

January 8, 2024

When you configure NetScaler Gateway, you can choose how users log on. Users can log on with one of the following plug-ins:

- Citrix Secure Access client for Windows
- Citrix Secure Access client for macOS

You complete the configuration by creating a session policy and then binding the policy to users, groups, or virtual servers. You can also enable plug-ins by configuring global settings. Within the global or session profile, you select either Windows or macOS X as the plug-in type. When users log on, they receive the plug-in as defined globally or in the session profile and policy. Create separate profiles for the plug-in type.

Configure the plug-in globally

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Client Experience tab, next to plug-in Type, select Windows/macOS X and then click OK.

Configure the plug-in type for Windows or macOS in a session profile

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway > Policies** and then click **Session**.
2. Do one of the following:
   - If you are creating a session policy, in the details pane, click **Add**.
   - If you are changing an existing policy, select a policy, and then click **Open**.
3. Create a profile or modify an existing profile. To do so, do one of the following:
   - Next to **Request Profile**, click **New**.
   - Next to **Request Profile**, click **Modify**.
4. On the **Client Experience** tab, next to **plug-in Type**, click **Override Global** and then select **Windows/macOS X**.
5. Do one of the following:
   - If you are creating a profile, click **Create**, set the expression in the policy dialog box, click **Create,** and then click **Close**.
   - If you are modifying an existing profile, after making the selection, click OK twice.

Citrix Secure Access client for Windows

When users log on to NetScaler Gateway, they download and install the Citrix Secure Access client on the user device.

To install the plug-in, users must be a local administrator or a member of the Administrators group. This restriction applies for first-time installation only. Plug-in upgrades do not require administrator level access.

To enable users to connect to and use NetScaler Gateway, you need to provide them with the following information:

- NetScaler Gateway web address, such as https://NetScalerGatewayFQDN/
- Any system requirements for running the Citrix Secure Access client if you configured endpoint resources and policies

Depending on the configuration of the user device, you might also need to provide the following information:

- If users run a firewall on their computer, they must change the firewall settings so that the firewall does not block traffic to or from the IP addresses corresponding to the resources for which you granted access. The Citrix Secure Access client automatically handles Internet Connection Firewall in Windows XP and Windows Firewall in Windows XP Service Pack 2, Windows Vista, Windows 7, Windows 8, or Windows 8.1.
- Users who want to send traffic to FTP over a NetScaler Gateway connection must set their FTP application to perform passive transfers. A passive transfer means that the remote computer establishes the data connection to your FTP server, rather than the establishment of the data connection by the FTP server to the remote computer.
- Users who want to run X client applications across the connection must run an X server, such as `XManager`, on their computers.
- Users who install Receiver for Windows or Receiver for Mac can start the Citrix Secure Access client from Receiver or by using a web browser. Provide instructions to users about how to log on with the Citrix Secure Access client through Receiver or a web browser.

Because users work on files and applications as if they are local to the organization's network, you do not need to retrain users or configure applications.

To establish a secure connection for the first time, log on to NetScaler Gateway by using the web logon page. The typical format of a web address is https://companyname.com. When users log on, they can download and install the Citrix Secure Access client on their computer.

Install the Citrix Secure Access client for Windows

1. In a web browser, type the web address of NetScaler Gateway.
2. Type the user name and password and then click Logon.
3. Select Network Access and then click Download.
4. Follow the instructions to install the plug-in.

When the download is complete, the Citrix Secure Access client connects and displays a message in the notification area on a Windows-based computer.

If you want users to connect with the Citrix Secure Access client without using a web browser, you can configure the plug-in to display the logon dialog box when users right-click the **NetScaler Gateway** icon in the notification area on a Windows-based computer or start the plug-in from the Start menu.

Configure the logon dialog box for the Citrix Secure Access client for Windows

To configure the Citrix Secure Access client to use the logon dialog box, users must be logged on to complete this procedure.

1. On a Windows-based computer, in the notification area, right-click the NetScaler Gateway icon and then click Configure NetScaler Gateway.
2. Click the Profile tab and then click Change Profile.
3. On the Options tab, click Use the Citrix Secure Access client for logon.
   Note: If users open the
   Configure NetScaler Gateway dialog box from within Receiver, the
   Options tab is not available.

Set the interception mode for the Citrix Secure Access client for Windows

If you are configuring the Citrix Secure Access client for Windows, you also need to configure the interception mode and set it to transparent.

1. In the configuration utility, click the Configuration tab, expand **NetScaler Gateway > Resources,** and then click **Intranet Applications**.
2. In the details pane, click **Add**.
3. In **Name**, type a name for the policy.
4. Click **Transparent**.
5. In **Protocol**, select **ANY**.
6. In **Destination Type**, select **IP Address and Netmask**.
7. In **IP address** type the IP address.
8. In **Netmask**, type the subnet mask, click **Create,** and then click **Close**.

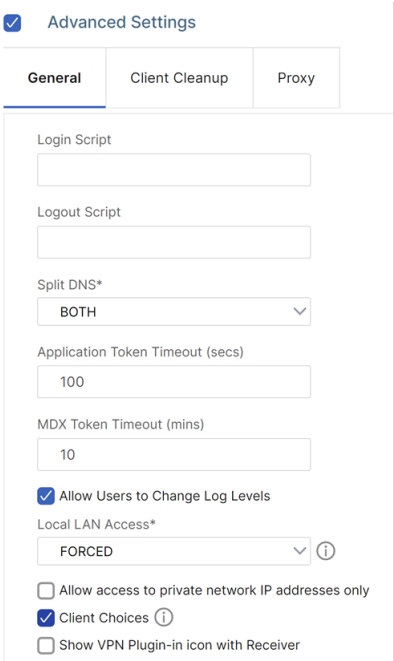
Enforce local LAN access to end users based on ADC configuration

Admins can restrict the end users from disabling the local LAN access option on their client machines. A new option, FORCED is added to the existing Local LAN Access parameter values. When the Local LAN Access value is set to FORCED, the local LAN access is always enabled for end users on the client machines. End users cannot disable the local LAN settings using the Citrix Secure Access client UI.

Admins can enable end users to access the local LAN resources on their client machine by setting the local LAN access parameter to ON. To block the end users from accessing the local LAN resources on their client machine, admins can set the Local LAN access parameter to OFF. For details about the end user configurations, see Local LAN access for macOS and Local LAN access for iOS.

To enable the Forced option by using the GUI:

1. Navigate to **NetScaler Gateway > Global Settings > Change Global Settings**.
2. Click the **Client Experience** tab and then click **Advanced Settings**.
3. In **Local LAN Access**, select **FORCED**.



To enable the Forced option by using the CLI, run the following command:

```
set vpn parameter -localLanAccess FORCED
```

> **Notes:**
>
> - Citrix Secure Access client for macOS/iOS and later versions support the local LAN access functionality of NetScaler Gateway.
> - Starting from Citrix Secure Access client for Windows 23.10.1.7, the Local LAN access is supported on a machine-level tunnel if the Local LAN Access parameter is set to **Forced** on NetScaler Gateway.

Microsoft Edge WebView support for Windows Citrix Secure Access –Preview

Microsoft Edge WebView support for Windows Citrix Secure Access introduces an enhanced end user experience. For details, see Microsoft Edge WebView support for Windows Citrix Secure Access

Windows Citrix Secure Access client using Windows Filtering Platform

The Windows Filtering Platform (WFP) is a set of API and system services that provide a platform for creating network filtering application. WFP is designed to replace previous packet filtering technolo-

gies, the Network Driver Interface Specification (NDIS) filter which was used with the DNE driver. The WFP mode is supported with the 22.6.1.5 build of the Windows Citrix Secure Access client.

Install the WFP build

You can install the WFP build using one of the following methods.

- Install the VPN plug-in with both the DNE and WFP drivers (default method)

  When the plug-in is installed with both the DNE and WFP drivers, admins can use either the WFP or the DNE driver for tunneling via a registry knob. By default, the DNE driver is used for tunneling.

- Install the VPN plug-in with just the WFP driver (Skip DNE driver installation)

  DNE drivers are not supported with some of the third-party applications even when not in use. For those deployments, admins can use this installation type. As the DNE driver is not installed, only the WFP driver is used for tunneling.

Select a WFP driver instead of a DNE driver

Perform the following steps to select the WFP driver instead of the DNE driver.

> **Note:**
>
> This works only with the default installation method.

1. Download the WFP supported VPN plug-in build and install the new VPN plug-in.
2. By default, the DNE driver is used to tunnel the traffic. To use the WFP driver for tunneling, admins must create the following registry entry:
   - REG_PATH - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
     - REG_TYPE - REG_DWORD
     - REG_NAME - EnableWFP
     - REG_VALUE –Set value to 1 to use WFP and 0 to use DNE (by default DNE is enabled if this registry value is not present or is set to 0)

> **Note:**
>
> After switching the tunneling mode from DNE to WFP or conversely, the system must be rebooted for the changes to take effect properly.

Completely skip the DNE installation

Perform the following steps to skip the DNE installation.

1. Perform a clean uninstallation of the VPN plug-in.

   a) Uninstall the current VPN plug-in present on the machine and restart the machine.

   b) Check if the DNE driver is uninstalled using either of the following options.

      - Open an elevated command prompt (or PowerShell). Run the following commands (sample output shows that the DNE based driver is installed on the system)

```
PS C:\Users\Administrator> sc qc cag
[SC] QueryServiceConfig SUCCESS
SERVICE_NAME: cag
TYPE               : 1  KERNEL_DRIVER
START_TYPE         : 2   AUTO_START
ERROR_CONTROL      : 1   NORMAL
BINARY_PATH_NAME   : \??\C:\Program Files\Common Files\
    Deterministic Networks\Common Files\cag.sys
LOAD_ORDER_GROUP   :
TAG                : 0
DISPLAY_NAME       : Citrix cag plugin for Access Gateway
DEPENDENCIES       :
SERVICE_START_NAME :
PS C:\Users\Administrator> sc qc dne
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: dne
TYPE               : 1  KERNEL_DRIVER
START_TYPE         : 1   SYSTEM_START
ERROR_CONTROL      : 1   NORMAL
BINARY_PATH_NAME   : \SystemRoot\system32\DRIVERS\dnelwf64.sys
LOAD_ORDER_GROUP   : NDIS
TAG                : 38
DISPLAY_NAME       : DNE LightWeight Filter
DEPENDENCIES       :
SERVICE_START_NAME :
```

      If the driver is not installed, the following output is displayed:

```
The specified service does not exist as an installed service.
```

Because the DNE driver (dnelwf64.sys) is also used by other vendors, it might be present even when the Citrix Secure Access client is not installed on the system. On the other hand, the CAG plug-in is only used by the Citrix Secure Access client.

- DNE presence can also be checked by trying to start the CAG and DNE drivers. Open the command prompt using admin rights and run the following commands:

```
net start cag
net start dne
```

  - If the output message indicates that the services cannot be located (The service name is invalid.), then the plug-in and driver components are uninstalled successfully. In

this case, move to step 2.
  - If the plug-in and driver components are not uninstalled successfully, run the Cleanup utility on the client machine by following the instructions provided at https://citrix.sharefile.com/d-s829800c3821a4a8f869ad324de6f0332.
    * Unzip the Cleanup utility and copy it to a folder.
    * Run nsRmSAC.exe from the command prompt.
    * Restart the client machine.

2. Create the following registry entries.

   - REG_PATH - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
     - REG_TYPE - REG_DWORD
     - REG_NAME - SkipDNE
     - REG_VALUE - Set to 1 to make sure that DNE is not installed on the machine
   - REG_PATH - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
     - REG_TYPE - REG_DWORD
     - REG_NAME - EnableWFP
     - REG_VALUE - Set to 1 to enable WFP (this entry must be created if the DNE installation is skipped)

   > **Note:**
   >
   > - If the registry entries are not created before installation, DNE is installed, by default. Also, you can check the VPN log files to validate whether WFP or DNE is used.
   > - If DNE installation is skipped, EnableWFP must be set to 1. In this case, you cannot switch to the DNE based plug-in without reinstalling the Citrix Secure Access client.

3. Install the new VPN plug-in.

4. Confirm if the WFP driver is installed on the system. Open an elevated command prompt and run the following command. The sample output shows that the WFP driver is installed on the system.

```
PS C:\Users\Administrator> sc qc ctxsgwcallout
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: ctxsgwcallout
    TYPE               : 1  KERNEL_DRIVER
    START_TYPE         : 1   SYSTEM_START
    ERROR_CONTROL      : 0   IGNORE
    BINARY_PATH_NAME   : \??\C:\Program Files\Citrix\Secure Access
        Client\ctxsgwcallout.sys
    LOAD_ORDER_GROUP   :
    TAG                : 0
    DISPLAY_NAME       : Citrix Secure Access Callout Driver
```



```
12      DEPENDENCIES       :
13      SERVICE_START_NAME :
```

If the driver is not installed, the following output is displayed:

```
The specified service does not exist as an installed service.
```

1. Restart the client machine.

Advantages of WFP

The following are some of the advantages of WFP if stand-alone WFP driver installation is done on the client.

- **FQDN based reverse split tunnel support:** The WFP driver enables support for FQDN based REVERSE split tunneling. It is not supported with the DNE driver. For more details, see Split tunneling options.
- **Wireshark support:** DNE does not allow capturing two-way traffic on a client machine because of its linking with the Ethernet/Wi-Fi adapter. This is not an issue with the new WFP driver. Any traffic capture (one-way or two-way) is encrypted and requires SSL keys to decrypt the same.
- **NMAP support:** The new WFP driver supports NMAP scanning while the VPN plug-in used to tunnel the traffic, whereas the DNE does not allow NMAP scanning, while the VPN plug-in used to tunnel the traffic.
- **Network speed:** In some scenarios, if DNE is installed on a client machine, download and upload speed are affected, which is not the case with WFP.
- **Improved nslookup performance:** Sometimes with DNE, `nslookup` fails to respond with lesser number of tries, and the same is not observed with WFP.
- **Improved iperf performance over UDP:** With DNE, some packet loss was observed during scalability tests using iperf over UDP. Packet loss is not observed with WFP.

Deploy the Citrix Secure Access client from Active Directory

January 8, 2024

If users do not have administrative privileges to install the Citrix Secure Access client on the user device, you can deploy the plug-in for users from Active Directory. When you use this method to deploy the Citrix Secure Access client, you can extract the installation program and then use a group policy to deploy the program. The general steps for this type of deployment are:

- Extracting the MSI package.
- Distributing the plug-in by using a group policy.
- Creating a distribution point.
- Assigning the Citrix Secure Access client package by using a Group Policy Object.

  Note: Distribution of the Citrix Secure Access client from Active Directory is only supported on Windows 7, Windows 8, and Windows 10.

You can download the MSI package from the configuration utility or from the Citrix website.

To download the Citrix Secure Access client MSI package from the configuration utility

1. In the configuration utility, click **Downloads**.
2. Under Citrix Secure Access client, click **Download NetScaler Gateway Plugin for Windows** and then save the file **nsvpnc_setup.exe** to your Windows server.

   Note:

   - For 64-bit machines, you must save the file Agee_setup.exe to your Windows server.
   - If the **File Download** dialog box does not appear, press the CTRL key when you click the link **Download Citrix Secure Access client for Windows**.

3. At a command prompt, navigate to the folder where you saved **nsvpnc_setup.exe** to and then type:

   ```
   nsvpnc_setup /c
   ```

   This extracts the file agee.msi.

   Note: For 64-bit machines, navigate to the folder where you saved **Agee_setup.exe** to and then type:

   ```
   Agee_setup.exe /c
   ```

   This extracts the file agee64.msi.

4. Save the extracted file to a folder on the Windows server.

After you extract the file, use a group policy on Windows Server to distribute the file.

Before starting the distribution, install the Group Policy Management Console on Windows Server 2003, Windows Server 2008, or Windows Server 2012. For more information, see the Windows online help.

Note: When you use a group policy to publish the Citrix Secure Access client, Citrix recommends assigning the package to the user device. The MSI package is installed on a per-device basis.

Before you can distribute the software, create a distribution point on a network share on a publishing server, such as the Microsoft Internet Security and Acceleration (ISA) Server.

To create a distribution point

1. Log on to the publishing server as an administrator.
2. Create a folder and share it on the network with read permission for all accounts that need access to the distribution package.
3. At the command prompt, navigate to the folder where you save the extracted file and then type: msiexec -a agee.msi
4. On the **Network Location** screen, click **Change** and then navigate to the shared folder where you want to create the administrative installation of the Citrix Secure Access client.
5. Click **OK** and then click **Install**.

After you have put the extracted package on the network share, assign the package to a Group Policy Object in Windows.

After you configure the Citrix Secure Access client successfully as a managed software package, the plug-in is installed automatically the next time the user device starts.

> **Note:** When the installation package is assigned to a computer, the user must restart the computer.

When the installation starts, users receive a message that the Citrix Secure Access client is installing.

Manage Citrix Secure Access client by using Active Directory

January 8, 2024

Each release of the Citrix Secure Access client is packaged as a full product installation, instead of as a patch. When users log on and the Citrix Secure Access client detects a new version of the plug-in, the plug-in upgrades automatically. You can also deploy the Citrix Secure Access client to upgrade by using Active Directory.

To do so, create a distribution point for the Citrix Secure Access client. Create a Group Policy Object and assign the new version of the plug-in to it. Then, create a link between the new package and the existing package. After you create the link, the Citrix Secure Access client is updated.

Remove the Citrix Secure Access client from user devices

To remove the Citrix Secure Access client from user devices, remove the assigned package from the Group Policy Object Editor.

When the plug-in is removed from the user device, users receive a message that the plug-in is uninstalling.

Troubleshoot the Citrix Secure Access client installation using Active Directory

If the assigned package fails to install when the user device starts, you might see the following warning in the application event log:

Failed to apply changes to software installation settings. Software installation policy application has been delayed until the next logon because an administrator has enabled logon optimization for group policy. The error was: The group policy framework must call the extension in the synchronous foreground policy refresh.

This error is caused by Fast Logon Optimization in Windows XP in which users are allowed to log on before the operating system initialized all the networking components, including Group Policy Object processing. Some policies might require more than one restart to take effect. To resolve this issue, disable Fast Logon Optimization in the Active Directory.

To troubleshoot other installation issues for managed software, Citrix recommends using a group policy to enable Windows Installer Logging.

Integrate the Citrix Secure Access client with Citrix Workspace app

January 8, 2024

NetScaler Gateway supports the Citrix Workspace app. The orchestrated system consists of the following components:

- Citrix Workspace app for Windows 3.4 or newer
- Citrix Workspace app for Mac
- Citrix Workspace app for Android
- Citrix Workspace app for iOS
- StoreFront 2.1 or newer
- Endpoint Management 2.8 and newer or Citrix Endpoint Management 10
- Citrix Update Service that is hosted on the Citrix website

For more information about NetScaler Gateway compatibility with NetScaler products, see Compatibility with NetScaler products.

You can configure NetScaler Gateway so that when users log on to the appliance, the Citrix Secure Access client opens a web browser that allows single sign-on to the Citrix Workspace app home page. Users can download the Citrix Workspace app from the home page.

When users log on with the Citrix Workspace app, user connections can route through NetScaler Gateway in the following manner:

- Directly to Endpoint Management
- Directly to StoreFront
- To StoreFront and then Endpoint Management if you do not configure MDX mobile apps in Endpoint Management
- To Endpoint Management and then StoreFront if you do configure MDX mobile apps in Endpoint Management

> **Note:**
>
> Connections that are routed directly to Endpoint Management are supported in Endpoint Management 2.0, Endpoint Management 2.5, Endpoint Management 2.6, Endpoint Management 2.8, and Endpoint Management 2.9 only. If you have Endpoint Management 1.1 deployed in your network, user connections must route through StoreFront.

How users connect with Citrix Workspace app

January 8, 2024

Users can connect to the following applications, desktops, and data from the Citrix Workspace app:

- Windows-based applications and virtual desktops published in StoreFront and the Web Interface
- ShareFile data accessed through Citrix Endpoint Management

Users can log on by using any of the following Citrix Workspace apps:

- Citrix Workspace app for Web
- Citrix Workspace app for Windows
- Citrix Workspace app for Mac
- Citrix Workspace app for iOS
- Citrix Workspace app for Android

Users can log on with Citrix Workspace app for Web by using a web browser or from the Citrix Workspace app icon on the user device.

When users log on with any version of Citrix Workspace app, applications, ShareFile data, and desktops appear in the browser or Citrix Workspace app window.

Decouple the Citrix Workspace app icon

January 8, 2024

When a Citrix Virtual Apps and Desktops deployment is configured with the Citrix Secure Access client integrated with the Citrix Workspace app, the plug-in's icon is not visible to a user who is connected to the VPN. The **Citrix Secure Access** icon normally resides in the Windows system tray or the macOS X Finder's menu bar. This icon is the interface into the plug-in's settings and controls. For Windows users, when the Citrix Workspace app and the Citrix Secure Access client are integrated, the **About** dialog in the Citrix Workspace app displays the controls for the Citrix Secure Access client. For macOS X users, there are no controls for the Citrix Secure Access client available after integration.

Some integrated deployments might present a need to expose the plug-in controls while retaining the integration of the underlying functionality. To do so, use the following CLI command or NetScaler configuration utility task to toggle the icon integration for VPN clients.

Set the icon integration using the CLI

At the command prompt, type;

```
set vpn parameter [-iconWithReceiver (ON/OFF)]
```

Set the icon integration using the GUI

1. On the Configuration tab, navigate to **NetScaler Gateway > Global Settings**.
2. Click **Change Global Settings**, and then select the **Client Experience** tab.
3. Click **Advanced Settings.**
4. Select **Show VPN plug-in** icon with Citrix Workspace app.

Configure IPv6 for ICA connections

January 8, 2024

NetScaler Gateway supports IPv6 addresses for ICA connections. Connections with IPv6 to the Web Interface or StoreFront work the same as IPv4 connections. When users connect by using the NetScaler Gateway web address, NetScaler Gateway proxies the connection to the Web Interface or StoreFront.

You can configure IPv6 for NetScaler Gateway deployed in one DMZ or deployed in a double-hop DMZ.

You enable IPv6 on NetScaler Gateway by using the command line. You can use the following guidelines:

- Enable IPv6 on the appliance.
- Configure subnet IP addresses.
- Set the DNS resolution order.
- Set the Web Interface or StoreFront web address.
- Bind the Secure Ticket Authority (STA) to NetScaler Gateway.

By default, the mapped IP address does not support IPv6 addresses. To route user communications to the internal network, you need to create subnet IP addresses and then and configure NetScaler Gateway to use the subnet IP addresses.

If you deploy multiple IPv6 subnets in your network, create multiple IPv6 subnet IP address on NetScaler Gateway, on for each subnet in your network. Network routing sends the IPv6 packets to the respective subnets by using the subnet IP addresses.

To configure IPv6 for ICA Proxy by using the CLI

1. Log on to NetScaler Gateway by using a Secure Shell (SSH) connection, such as from PuTTY. At the command prompt, type;

```
enable ns feature IPv6PT. This enables IPv6.

enable ns mode USNIP.

set dns parameter – resolutionOrder AAAAThenAQuery AThenAAAAQuery
    OnlyAAAAQuery OnlyAQuery

set vpn parameter -wihome `http://XD_domain/Citrix/StoreWeb`
```


Where is either the domain name or IP address of StoreFront.

Example:

```
set vpn parameter -wihome `http://storefront.domain.com/Citrix/StoreWeb`.
```

Or

```
set vpn parameter -wihome `http://[1000:2000::3000]/Citrix/StoreWeb`
```

> **Note:**
>
> If you use the IPv6 address to configure this parameter, the IP address must be contained in brackets.

Configure the Citrix Workspace app home page on NetScaler Gateway

January 8, 2024

You can configure the Citrix Workspace app home page either globally or as part of a session profile. If you want to configure Citrix Workspace app for Web and earlier Citrix Workspace app versions that do not recognize StoreFront through NetScaler Gateway, you need to create two separate session profiles. The field Citrix Workspace app Home Page needs to have the correct web address for each profile so users can log on successfully.

For Citrix Workspace apps that recognize StoreFront through NetScaler Gateway, you can have Citrix Workspace app for Web and Citrix Workspace app share a profile. However, Citrix recommends that you configure a session profile for Citrix Workspace app for Web and a separate session profile for all other Citrix Workspace apps.

To configure the Citrix Workspace app home page globally

To configure the Citrix Workspace app home page globally:

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. In the Global NetScaler Gateway Settings dialog box, click the Published Applications tab.
4. In Citrix Workspace app Home Page, type the web address for Citrix Workspace app or the Citrix Workspace app for Web home page and then click OK.

To configure the Citrix Workspace app home page in a session profile

To configure the Citrix Workspace app home page in a session profile:

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway > Policies** and then click **Session**.
2. In the details pane, on the **Profiles** tab, click **Add**.
3. In the **Create NetScaler Gateway Session Profile** dialog box, on the **Published Application** tab, next to **Citrix Receiver Home** Page, click **Override Global**.
4. In Citrix Workspace app home page, type the web address for the Citrix Workspace app or Citrix Workspace app for Web home page and then click **Create**.

Apply the Citrix Workspace app theme to the NetScaler Gateway logon page

January 8, 2024

You can use the NetScaler Gateway UI to apply the Citrix Workspace app theme to the logon page for NetScaler Gateway. You can switch between the Citrix Workspace app theme and the custom theme that you create. After the custom theme is created, clear the browser cache to prevent cached pages from appearing.

By default, the NetScaler Gateway login page uses the RfWebUI visual theme that matches the styling of the Unifed UI used by StoreFront. If you are using Citrix Workspace platform or on-prem StoreFront with the New Workspace user interface, follow the instructions provided in this Support article. Alternatively you can create your own custom theme. For details see, Create a custom theme for the NetScaler Gateway logon page.

Ensure that the NetScaler Gateway portal theme is bound to a VPN virtual server. For details, see Bind a portal theme to a VPN virtual server.

Create a custom theme for the NetScaler Gateway logon page

January 8, 2024

You can use the GUI to create a custom theme for the logon page for NetScaler Gateway. You can also leave the default theme or use the Citrix Workspace app theme. When you choose to apply a

custom theme to the logon page, you use the NetScaler Gateway command line to create and deploy the theme. You then use the GUI to set the custom theme page.

You configure the custom theme page by using NetScaler Gateway global settings.

You can use this feature with the following versions of NetScaler Gateway:

- NetScaler Gateway 10.1
- Access Gateway 10, Build 73.5002.e (you must install this build after Build 71.6104.e to use this feature with Endpoint Management Versions 2.5, 2.6, or 2.8)
- Access Gateway 10, Build 71.6104.e

Create and deploy the custom theme by using the CLI

To create and deploy the custom theme by using the command line:

1. Log on to the NetScaler Gateway command line.
2. At the command prompt, type shell.
3. At the command prompt, type `mkdir /var/ns_gui_custom; cd /netscaler; tar -cvzf /var/ns_gui_custom/customtheme.tar.gz ns_gui/*`.
4. Use the configuration utility to switch to the custom theme and then make customization changes under /var/ns_gui_custom/ns_gui/vpn. You can:
   - Make edits to the css/ctx.authentication.css file.
   - Copy a custom logo to the /var/ns_gui_custom/ns_gui/vpn/media folder. **Note:** You can use WinSCP to transfer the files.
5. If you have multiple NetScaler Gateway appliances, repeat Steps 3 and 4 for all appliances.

NetScaler Gateway Windows VPN client registry keys

July 1, 2024

The VPN client registry keys are available under **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client**. The following table lists the NetScaler Gateway Windows VPN client registry keys, values, and a brief description of each value.

Registry key	Registry type	Values and description
addedRoutes/modifiedRoutes	REG_SZ	Created for internal plug-in communication. Users must not modify this key.
AlwaysOnService	REG_DWORD	1 => Establish machine level tunnel but not user level tunnel. 2 => Establish machine level tunnel and user level tunnel.
AlwaysOnURL	REG_SZ	URL of the NetScaler Gateway virtual server the user wants to connect to. Example: `https://xyz.companyDomain.com`
AlwaysOn	REG_DWORD	1 => Allow network access on VPN failure. 2=> Block network access on VPN failure.
AlwaysOnAllowlist	REG_SZ	Semicolon separated list of IP addresses or FQDNs allowed by the driver in Always On strict mode. Examples: `*.microsoft.com`, `groupinfra.com`
ClientControl	REG_DWORD	1 => Allows users to log out or connect to other gateways. 0 => Blocks users to log out or connect to other gateways.

Registry key	Registry type	Values and description
ConfigSize	REG_DWORD	Windows client supports 64 KB configuration file size, by default. Use this registry to increase configuration file size. If the configuration file size is larger than the default value (64 KB), then the ConfigSize registry value must be set to 5 x 64 KB (after converting to bytes) for every addition of 64 KB. For example, if you are adding additional 64 KB, then you must set the registry value to 64 x 1024 x 5 = 327680. Similarly, if you are adding 128 KB, then you must set the registry value to 64 x 1024 x (5+5) = 655360.
Connected	REG_DWORD	On successful connection this key is set to 1 and else set to 0. This key is used internally. Users must not modify this key.
DisableGA	REG_DWORD	Set to 1 to disable Google analytics.
DisableCredProv	REG_DWORD	When Always On before user logon is enabled, the Windows VPN plug-in adds the credential provider to display the tunnel status on the logon screen. If you do not need this additional functionality, create and set this registry to 1.

Registry key	Registry type	Values and description
DisableIconHide	REG_DWORD	1 => The Citrix Workspace app and the gateway plug-in are displayed on the taskbar. 0 => The gateway plug-in icon is integrated with Citrix Workspace app for Windows. The gateway plug-in is not visible on the taskbar when running a full VPN session.
DisableDNSRoutes	REG_DWORD	Default value 0 => VPN plug-in adds routes for DNS servers if they are different from the default gateway for a physical interface. However, based on the Windows client machine topology, DNS server routes might not be always required. If set to 1, the VPN plug-in does not add explicit routes for the DNS servers.
DisallowCaptivePortals	REG_DWORD	1 => VPN plug-in checks for captive portals by trying to connect to the Microsoft Connect test page before starting a VPN session. 0 => VPN plug-in skips the captive portals check.
DisableIntuneDeviceEnrollment	REG_DWORD	If set to 1, Intune device enrollment is not performed.
EnableAutoUpdate	REG_DWORD	Used to control plug-in update functionality from the client side. Set to 0 to disable auto-update functionality. Set to 1 to respect ADC configuration.

Registry key	Registry type	Values and description
EnableKerberosAuth	REG_DWORD	0 => Default value. 1 => VPN client uses the Kerberos authentication method for auto-logon.
EnableVA	REG_DWORD	If Citrix Virtual adapter must be enabled when IIP is present. This key is used internally. Users must not modify this key.
EnableWFP	REG_DWORD	Default value 0 => By default, DNE is enabled. 1 => VPN plug-in uses WFP. 0 => VPN plug-in uses DNE.
ExcludeDomainsFromTunnel (Preview)	REG_SZ	Excludes traffic of specific domains from being tunneled via the Citrix Secure Access client. If `example.com` is an intranet domain and you want to exclude specific applications such as `sshhost.example.com`, `rdphost.example.com`, `*.ftphost.example.com`, you can use this registry. Ensure to set the registry value to a comma-separated list of domain names or patterns.
ForcedLogging	REG_DWORD	Set this key to 1 to enable debug logging.
HttpTimeout	REG_DWORD	HTTP timeout is configured in seconds. If timeout is not configured, the default timeout is used. The default timeout value is 100 seconds, based on Windows standards.
InstallDir	REG_SZ	Location where the Citrix Secure Access client is installed.

Registry key	Registry type	Values and description
locationDetection	REG_DWORD	1 => To enable location detection. 0 => To disable location detection.
NoDHCPRoute	REG_DWORD	If set to 1, the DHCP server route is not added.
overrideIPV6DnsDrop	REG_DWORD	1 => Allow IPv6 DNS traffic to flow over VPN. 0 => Restrict IPv6 DNS traffic flow.
OverrideSpoofIPRange	Need Eng inputs	Detects if there are conflicts in the default or admin-configured spoof IP address range and applies a new spoof IP address range.
ProductVersion	REG_SZ	Current Citrix Secure Access client installed version.
ProductCode	REG_SZ	This key is used internally. Users must not modify this key.
secureDNSUpdate	REG_DWORD	0 => The VPN plug-in tries the unsecure DNS update only. 1 => The VPN plug-in tries the unsecure DNS update first. If the unsecure DNS update fails, the VPN plug-in then tries the secure DNS update. This is the default behavior starting from the 21.3.1.2 Windows plug-in build. 2 => The VPN plug-in tries only the secure DNS update.

Registry key	Registry type	Values and description
SecureChannelResetTimeoutSeconds	REG_DWORD	By default, this registry value is not set or added. When the value of "SecureChannelReset-TimeoutSeconds"is 0xFFFFFFFF or not present in the registry, the VPN plug-in waits for the SecureChannelReset() API call to complete before starting to tunnel data traffic. This is the default behavior. Admin must set this registry on the client for the VPN plug-in to start tunneling data traffic after waiting the specified time for the API call to complete.
SecureAccessLogInScript	REG_SZ	Citrix Secure Access service accesses the login script configuration using this registry key when it connects to Citrix Secure Private Access service. For details, see Login and logout script configuration registries.
SecureAccessLogOutScript	REG_SZ	Citrix Secure Access service accesses the logout script configuration using this registry key when it connects to Citrix Secure Private Access service. For details, see Login and logout script configuration registries.
suffixList	REG_SZ	Semicolon list of intranet domains. Used when location detection is enabled.

Registry key	Registry type	Values and description
SicBeginPort	REG_DWORD	Avoids conflicts that might arise when you use ports to create sockets between Citrix Secure Access client and third party apps on the client machines. The allowed range is 49152 to 64535 (C000 to FC17 in hexadecimal format). The VPN client uses up to 1000 ports starting from `SicBeginPort` only if `EnableWFP` is also set to 1.
userCertCAList	REG_SZ	Used in the context of the Always On service where a customer can specify the list of CAs to choose the client certificate from.

Important:

- You can apply registry keys based on your deployments. For example, the AlwaysOnService registry key is applicable only to the Always on service whereas the ClientControl registry key is not applicable to the Always on service. Refer to the individual deployment documentation for more details.
- `secureDNSUpdate` is applicable only for domain joined client devices.
- For Citrix Secure Access client for Windows 23.1.1.8 and later versions, the registry key name is `overrideIPV6DnsDrop`. For Citrix Secure Access client for Windows 22.10.1.9 and prior versions, the registry key name is `overrideIP6DnsDrop`.

Enforce the HttpOnly flag on authentication cookies

January 8, 2024

Starting from NetScaler Gateway release 13.1-37.x and later, the HttpOnly flag is available on the authentication cookies of VPN scenarios that is, NSC_AAAC and NSC_TMAS cookies. The NSC_TMAS authentication cookie is used during the nFactor authentication and the NSC_AAAC cookie is used for the

authenticated session. The HttpOnly flag on a cookie restricts the cookie access using the JavaScript document cookie option. This helps in preventing cookie theft due to cross-site scripting.

Supported scenario

The HTTPOnly flag is supported for nFactor authentication.

Behavior when NetScaler AAA parameter's HttpOnlyCookie knob is used along with tmsession's HttpOnlyCookie knob:

- When the authentication, authorization, and auditing parameter's httpOnlyCookie knob is enabled and nFactor authentication is used, the authentication, authorization, and auditing parameter's HttpOnlyCookie knob overrides the TM session's HttpOnlyCookie knob. Also, both NSC_TMAS and NSC_AAAC are marked HttpOnly irrespective of the session type; whether it is a VPN session, TM session, or during nFactor authentication.
- If the HttpOnlyCookie knob is disabled, the HttpOnly flag is not set for a VPN session. For the authentication, authorization, and auditing scenario, the HttpOnly flag is set based on the TM session knob value.

Configure the HttpOnly feature by using the CLI

- Enable the HttpOnly flag

```
set aaa parameter -httpOnlyCookie ENABLED
```

- Check the status of the HttpOnly feature

```
show aaa parameter
```

Limitations

- When the HttpOnly feature is enabled, the Home Page button on the Citrix Secure Access client does not work.
- HttpOnly flag is not set in any classic authentication.

Customize the user portal for VPN users

February 20, 2024

NetScaler Gateway installations that serve the portal to VPN users include an option to select a portal theme to create a customized look and feel for the portal pages. You can select from a supplied set of themes, or you can use a theme as a template to build a customized or branded portal. Using the configuration utility, you can modify a theme by adding new logos, background images, custom input box labels, and various other attributes of the CSS-based portal design. The built-in portal themes include content for five languages: English, French, Spanish, German, and Japanese. Different users are served in different languages, depending on the locales reported by their web browsers.

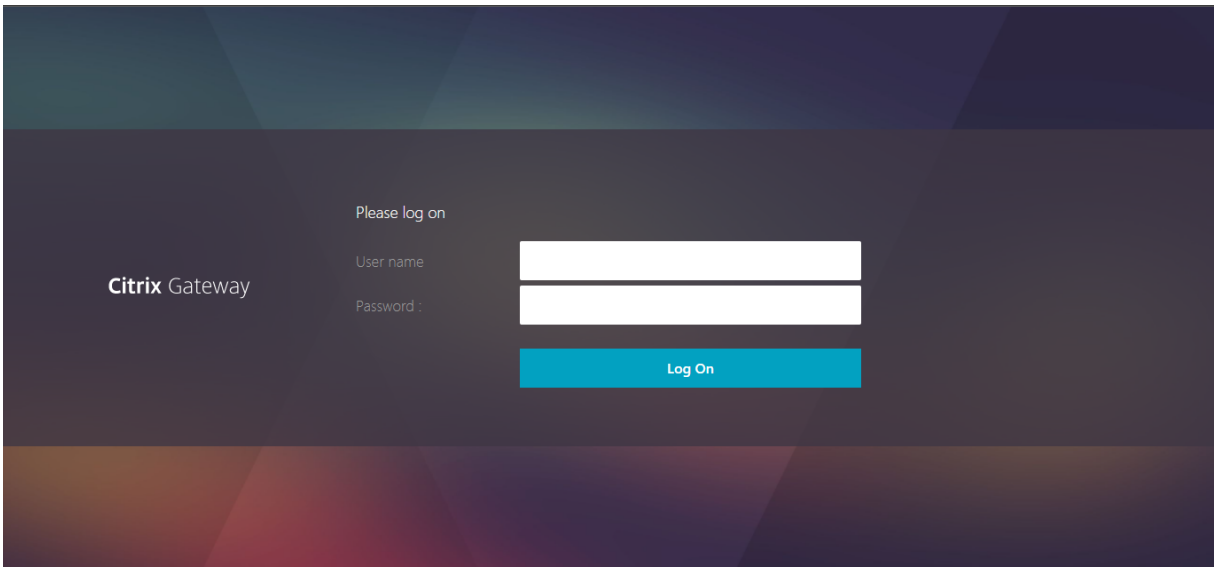
You can create a custom EULA that is presented to VPN users before they are allowed to sign in. The EULA feature supports locale-specific versions of a EULA, which are presented to users based on their web browsers reported locales.

Both portal themes and EULA configurations can be bound independently at the VPN virtual server and VPN global levels.

> **Important:**
>
> NetScaler does not support customization that requires code modifications and does not offer support to resolve issues beyond reverting to a default theme.

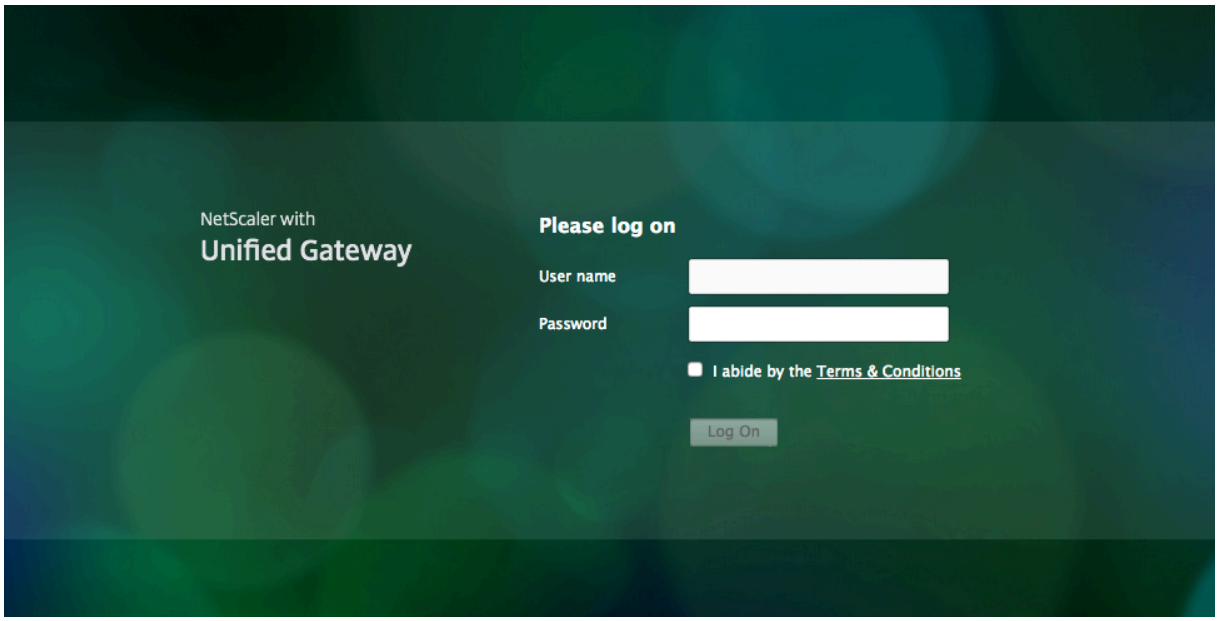
Apply a portal theme

Starting from release 13.0 build 67.43, the VPN portal is configured to use the RfWebUI theme, by default. Previously, the `Caxton theme` was the default theme. You can also apply the Green bubble and X1 themes.

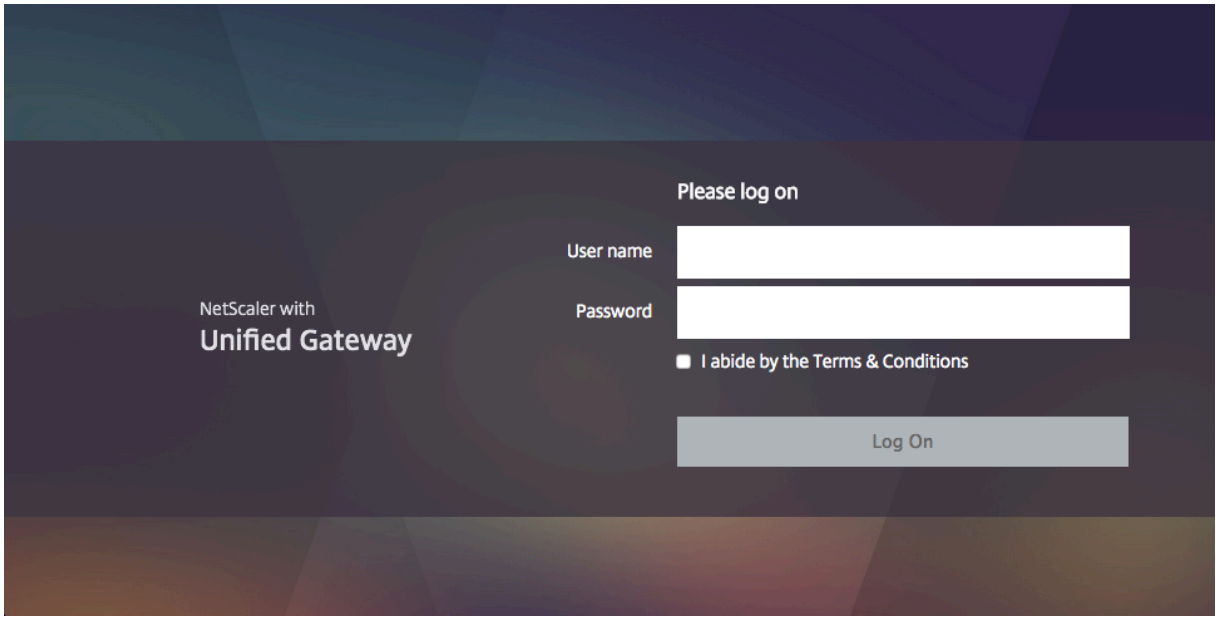


Caxton theme

Green bubble theme



X1 theme



You can apply any of the supplied themes directly to a VPN virtual server or as a global VPN binding.

Bind a portal theme to a VPN virtual server

You can bind a portal theme on an existing virtual server or when creating a new virtual server.

Bind a portal theme to a VPN virtual server by using the CLI

At the command prompt, type;

```
bind vpn vserver <name> - portaltheme <name>
```

Bind a portal theme to a VPN virtual server by using the GUI

1. On the **Configuration** tab, Navigate to **NetScaler Gateway** and click **Virtual Servers.**
2. Select a virtual server, and then click **Edit**.
3. If a portal theme has not yet been bound to the virtual server, click **Portal Theme** under **Advanced Settings** in the details pane. Otherwise, the **Portal Theme** option is already expanded in the details pane.
4. In the details pane, under **Portal Themes**, click **No Portal Theme** to expand the Portal Theme binding window.
5. `Click` **Click to select**.
6. In the **Portal Themes** window, click a theme name, and then click **Select**.

7. Click **Bind**.
8. Click **Done**.

If you are creating a VPN virtual server, you can follow the steps in the previous procedure starting with step 3 while in the **VPN virtual server edit** pane to bind a Portal Theme.

Bind a portal theme to VPN global

Bind a portal theme to VPN global by using the CLI

At the command prompt, type;

```
bind vpn global portaltheme <name>
```

Bind a portal theme to VPN global by using the GUI

1. On the **Configuration** tab, Navigate to **NetScaler Gateway.**
2. In the main details pane, click **NetScaler Gateway Policy Manager**.
3. Click the '**+**'icon.
4. In the **Bind Point** list, select **Resources**.
5. In the **Connection Type** list, select **Portal Theme.**
6. Click **Continue**.
7. In the **Bind Point** screen, click **Add Binding**.
8. Click **Click to select**.
9. In the **Portal Themes** window, click a theme name, and then click **Select**.
10. Click **Bind**.
11. Click **Close**.
12. Click **Done.**

> **Note:**
>
> After making the changes, use the 'save ns config'command on the command line or click the save icon in the configuration utility to ensure that your changes are saved to the NetScaler configuration file.

Create a portal theme

To create a custom portal design, you use one of the supplied portal themes as a template. The system makes a copy of the selected template theme with a name that you specify.

Use a stock portal theme as a template for a custom portal theme

To create a Portal Theme, you can use the configuration utility or the command line to create the theme entity. However, the detailed customization controls are available only within the configuration utility.

Create a portal theme by using the CLI

At the command prompt, type;

```
add portaltheme <name> basetheme <name>
```

Create a portal theme by using the GUI

1. On the **Configuration** tab, Navigate to **NetScaler Gateway** and click **Portal Themes**.
2. In the main details pane, click **Add**.
3. Enter a name for the theme and select a template from the template list, and then click **OK**.
4. At this point, you are presented with the first-time view of the portal theme editing window. Click **OK** to exit.

You can proceed to customize the new portal theme with the first-time view.

Once a new theme is created, you can bind it to a VPN virtual server or to VPN global. You can bind a new theme immediately after creation or after completing your customizations.

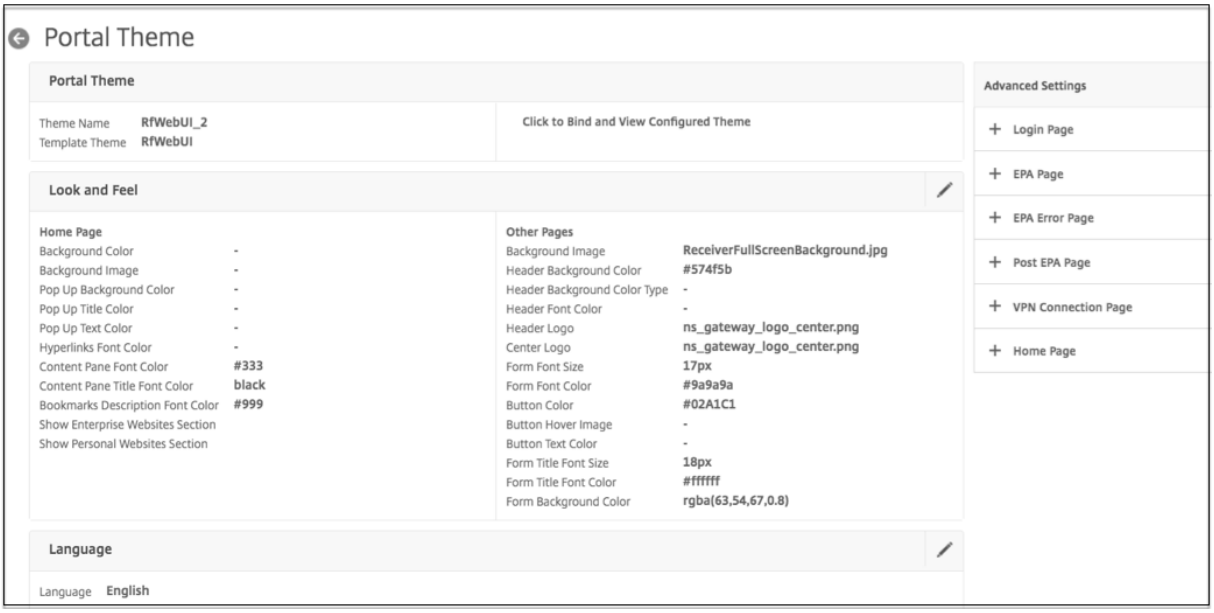
Portal theme customization

To customize a Portal Theme, use the Portal Theme interface in the configuration utility. To get the best results, you must understand the various elements of this interface before you use it.

About the portal theme interface

To open the **Portal Theme interface** in the NetScaler Gateway configuration utility, on the **Configuration** tab, Navigate to **NetScaler Gateway** and click **Portal Themes**. You can either create a theme as described in *Creating a Portal Theme* or select an existing theme in the main details pane and click **Edit**.

The portal theme customization page has four primary component panes for modifying a portal design: the **Portal Theme** pane, the Look & Feel pane, the **Advanced Settings** pane, and the **Language** pane.



The **Portal Theme** pane at the top of the page reports what theme is loaded for editing and what template theme it is based on. The viewing option here allows you to view your customizations without accessing the VPN with a user connection. Using the viewing option requires binding the theme to a VPN virtual server and the binding remains in effect after the viewing window is closed.

With the **Look & Feel** pane in the center of the page, you configure a theme's general properties, such as headers, background colors and images, font properties, and logos. When this pane is in edit mode, attribute legends are available for guidance on where the Look & Feel attributes are used on portal pages.

The **Advanced Settings** pane contains the onscreen content controls for the individual portal pages. To load a page's content for editing, click one of the pages listed. The page controls then open below the other center panes. A page remains collapsed in the **Advanced Settings** pane across Portal Theme edits as long as the page has not been modified.

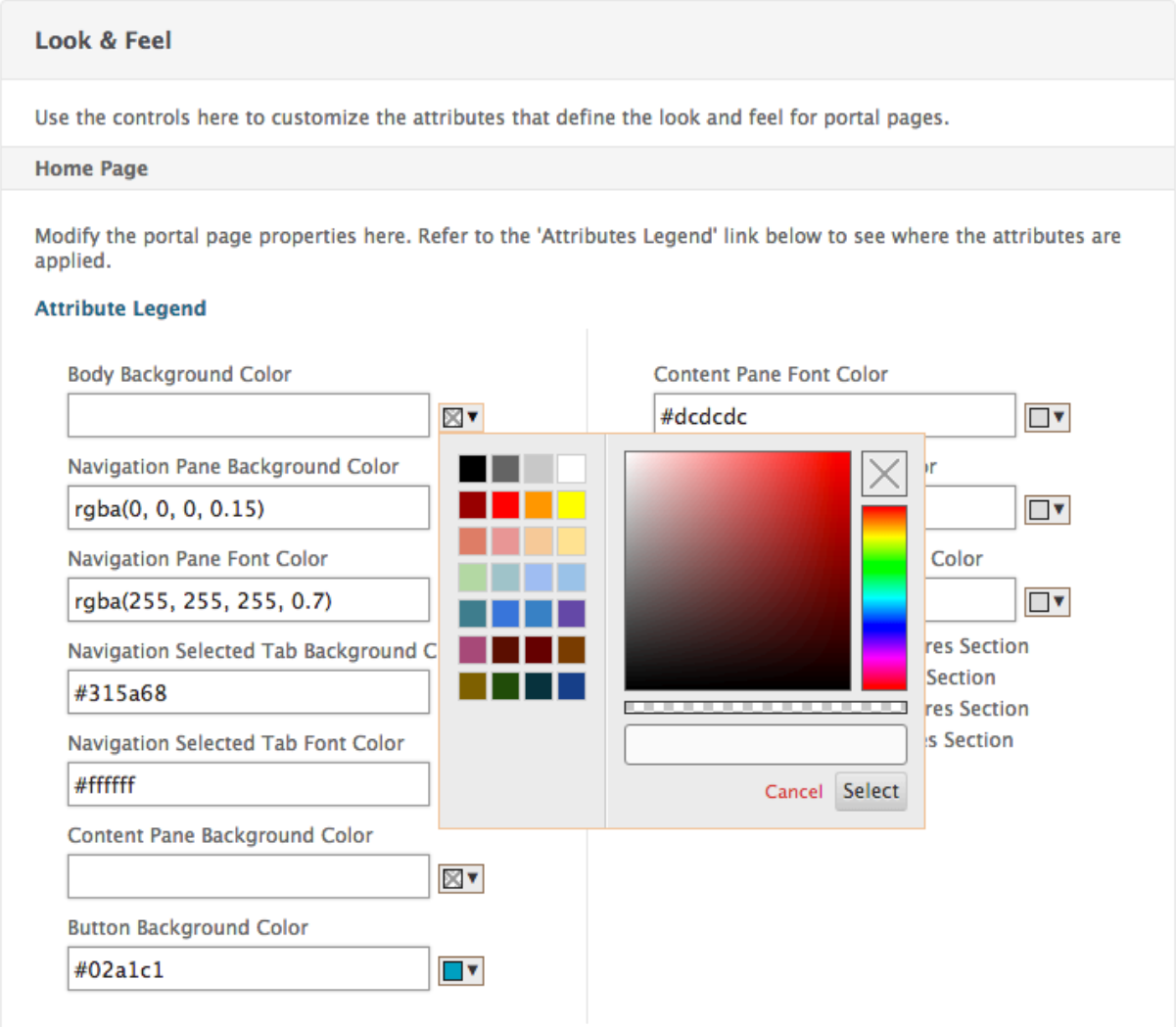
In the **Language** pane, you can select which of the languages is loaded when a page is selected for edit from the **Advanced Settings** pane. The English language pages are loaded by default.

Types of customizable page attributes

When customizing a Portal Theme, you can modify a range of attributes in the Portal Theme interface. Along with the text and the supported languages that can be edited, the graphical elements of the portal's layout can be tailored to suit your needs. Each of the page element types has parameters or recommendations to consider before modifying them.

Colors

The portal design specifies the colors for attributes such as page backgrounds, highlights, text for titles and body content, button controls, and hover responses. To customize a color attribute, you can enter a color value directly for a selected item, or you can use the supplied color picker to generate a color value. The interface supports entering valid HTML color values in RGBA format, HTML hexadecimal triplet format, and X11 color names. The color picker can be accessed for any applicable color attribute by clicking the color box next to the attribute's input field.



Fonts

Along with font colors, you can modify font sizes for some page attributes. For each of these attributes, a menu offers the sizes available for each attribute, as determined by the portal's design.

Images

For images, a pop-up description available for each control provides size recommendations and other requirements. The descriptions vary according to an attribute's location on the page and its function. You can use PNG or JPEG image file formats. You can select an image to upload by selecting the

checkbox beneath an item's file name and then browsing to where the image resides on your local computer's drive.

Labels

In the **Advanced Settings** section, you can select a specific portal page's text to modify. If you modify the default English text for a page, the text for other languages is not retranslated. The alternative language page content is provided as a convenience but requires manual updates for any customizations. To edit another language version for a page, first collapse the window, if it is open, by clicking the **X** icon for the open portal page. Then select the language in the **Language** pane and click **OK**. All the portal pages opened from the **Advanced Settings** pane is in that language until you select a different one.

> **Important**
>
> In high availability or clustered deployments, Portal Themes are distributed across the shared configuration only when Portal Theme settings are made on the primary or configuration coordinator NetScaler entities respectively.

Older portal customizations

For installations with manually modified custom portal design created in NetScaler Gateway or Access Gateway releases earlier than 11.0, NetScaler strongly recommends starting with a new portal theme in the customization interface. If you can't do that, you can apply a customization manually, but direct support for that is not provided.

When using a manually customized portal, you must set the customized portal as a global portal configuration. Doing so though means that an applied global portal configuration *cannot* be overridden with VPN virtual server level portal theme bindings. Attempting to create a VPN virtual server binding in this case with the configuration utility or the command line returns an error.

Also, in the case of high availability and cluster configurations, any manual customizations must be performed on every node in the deployment as the underlying files on the NetScaler file system are not distributed in the automatically shared configuration.

Create a custom portal configuration manually

To manually apply an older customized portal configuration after upgrading to NetScaler Gateway 11.0, you need to modify a copy of an existing portal page, put the customized portal files into the NetScaler file system, and select **CUSTOM** as the **UITHEME** parameter.

You can use WinSCP or any other secure copy program to transfer files to the NetScaler file system.

1. Log on to the NetScaler Gateway command line.

2. At the command prompt, type **shell**
3. At the command prompt, type **mkdir /var/ns_gui_custom; cd /netscaler; tar -cvzf /var/ns_gui_custom/customtheme.tar.gz ns_gui/*.**
4. At command prompt, type **cd /var/netscaler/logon/themes/**
   - If you want to customize the Green bubble theme, enter **cp -r** `Greenbubble` **Custom** to make a copy of the Green bubble theme.
   - If you want to customize the Default theme (`Caxton`), type **cp -r Default Custom.**
   - To customize the X1 theme, type **cp -r X1 Custom.**
5. Make the needed changes to the copied files under **/var/netscaler/logon/themes/Custom** to customize the theme manually.
   - Make the necessary edits to **css/base.css**.
   - Copy any custom images to the **/var/ns_gui_custom/ns_gui/vpn/media** directory.
   - Make changes to labels in the files present in the **resources/** directory. These files correspond to the portal-supported locales.
   - If changes to HTML pages or javascript files are also needed, you can make the relevant to the files in **/var/ns_gui_custom/ns_gui/**.
6. After all customization changes are complete, at the prompt enter: **tar –cvzf /var/ns_gui_custom/customth /var/ns_gui_custom/ns_gui/***

> **Important**
>
> When copying a theme directory in the preceding steps, the copied folder name must be entered exactly as 'Custom'since directory names are case-sensitive within the NetScaler shell interface. If the directory name is not entered precisely, the folder is not recognized when the **UITHEME** setting is configured to **CUSTOM**.

Select the customized theme as a VPN global parameter

Once the manually customized portal configuration is complete and copied to the NetScaler file system, it needs to be applied to the NetScaler Gateway configuration. This is done by setting the UITHEME parameter to CUSTOM and can be completed with the command line or the configuration utility.

To use the command line, enter the following command to set the **UITHEME** parameter.

```
set vpn parameter UITHEME CUSTOM
```

To set the UITHEME parameter using the configuration utility, use the following procedure.

1. On the **Configuration** tab, Navigate to **NetScaler Gateway > Global Settings**.
2. Click **Change Global Settings**.

3. Click the **Client Experience** tab.
4. Scroll to the bottom of the screen then select **CUSTOM** from the **UI Theme** list menu.
5. Click **OK**.

Your manually customized portal is now the portal design presented to VPN users.

Create an EULA

The VPN portal system provides the option to apply an EULA to a portal configuration. Once a EULA is bound to the NetScaler Gateway configuration, either at the VPN global scope or to a relevant VPN virtual server, VPN users must agree to the EULA as Terms and Conditions before they are allowed to authenticate into the VPN.

As with the portal themes, users are served a language-specific EULA based on the locale reported by their web browser. In cases of a locale that doesn't match to any of the supported languages, the default language served is English. For each EULA, you can enter a custom message in each of the supported languages. Pre-translated content is not provided for EULA configurations as it is for the portal themes. If a user's reported locale matches for a language where no EULA content is entered, the user is returned a blank page when they click the "Terms & Conditions"link in on the VPN login page.

To create a EULA, you can use either of the controls in the configuration utility on the **Configuration** tab at **NetScaler Gateway > Global Settings > EULA** or **NetScaler Gateway > Resources > EULA**. The controls in the **Global Settings** pane are used to manage VPN global EULA bindings while the control on the **Resources > EULA** node is for general operations on EULA configurations. You can manage VPN virtual server EULA bindings by editing a VPN virtual server at **NetScaler Gateway > Virtual Servers**. Some commands are also available with the command line for managing EULA entities. However, the full EULA management controls are available only in the configuration utility.

Create a EULA entity by using the CLI

At the command prompt, type;

```
add vpn eula <name>
```

Create a EULA entity by using the GUI

1. Navigate to **NetScaler Gateway > Resources > EULA**.
2. Click **Add** to create an entity.
3. Enter a name for the entity.
4. For each of the languages, paste the content under the relevant tabs.

5. Click **Create**.

Starting from release 14.1 build 17.38, the following HTML tags are re-enabled in the EULA text. These tags must be used without the HTML attributes.

```
- <html></html>
- <b></b>
- <p></p>
- <i></i>
- <ol></ol>
- <ul></ul>
- <li></li>
- <br></br><br/>
```

Once a EULA entity has been created, it can be globally bound to the VPN configuration, or can be bound to a VPN virtual server.

Bind a EULA to VPN global by using the CLI

At the command prompt, type;

```
bind vpn global eula <name>
```

Bind a EULA to VPN global by using the GUI

1. On the **Configuration** tab, Navigate to **NetScaler Gateway > Global Settings**.
2. In the main details pane, click **Configure an End User License Agreement**.
3. Click **Add Binding**.
4. Click **Click to select**.
5. Select a EULA entity then click **Select**.
6. Click **Bind**.
7. Click **Close**.

Bind a EULA to a VPN virtual server by using the CLI

At the command prompt, type;

```
bind vpn vserver <name> eula <name>
```

Bind a EULA to a VPN virtual server by using the GUI

1. At the **Configuration** tab browse to **NetScaler Gateway > Virtual Servers.**

2. In the main details pane, select a VPN virtual server and click **Edit**.
3. From the **Advanced Settings** pane on the right side of the page, click **EULA**.
4. In the newly added EULA pane, click **No EULA**.
5. `Click` **Click to select**.
6. Select a EULA entity and click **Select**.
7. Click **Bind**.
8. Click **Done**.

Prompt users to upgrade older or unsupported browsers by creating a custom page

January 8, 2024

If a client connects to a NetScaler VIP address using an insecure cipher such as SSLv3, they can be redirected to a custom page prompting them to upgrade to the latest version of Internet Explorer, Firefox, Chrome, or Safari.

Note: According to RFC6176 from the Internet Engineering Task Force (ITEF), TLS servers must not support SSLv2. Therefore, the NetScaler appliance does not support SSLv2 from release 12.1 and later.

How to create a custom page to prompt users to upgrade older unsupported browsers based on SSL

- Create a NetScaler responder policy with the rule `client.ssl.version.eq()`. The version returns the SSL protocol version.
  - Returns 0 if the transaction is not SSL based.
  - Returns 0x002 if the transaction is SSLv2.
  - Returns 0x300 if the transaction is SSLv3.
  - Returns 0x301 if the transaction is TLSv1.
- You must enable SSLv3 (or other earlier version) to trigger the responder policy.

  For example, if SSLv3 is disabled on the NetScaler appliance and a client with an older browser using SSLv3 tries to connect, then the access is denied.
- If your deployment requires SSLv3 or an earlier version for a specified period (a month or two), configure the following:
  - Enable the SSLv3 protocol.

  - Update the custom page to include information that after the specified period, the browser cannot connect to the appliance.

Configure clientless VPN access with NetScaler Gateway

January 8, 2024

Clientless access allows users the access they need without requiring them to install user software, such as the Citrix Secure Access client or Receiver. Users can use their web browser to connect to web applications, such as Outlook Web Access.

You use the following steps to configure clientless access:

- Enabling clientless access either globally or by using a session policy bound to a user, group, or virtual server.
- Selecting the web address encoding method.

To enable clientless access for only a specific virtual server, disable clientless access globally, and then create a session policy to enable it.

If you use the NetScaler Gateway wizard to configure the appliance, you have the choice of configuring clientless access within the wizard. The settings in the wizard are applied globally. Within the NetScaler Gateway wizard, you can configure the following client connection methods:

- Citrix Secure Access client. Users are allowed to log on by using the Citrix Secure Access client only.
- Use the Citrix Secure Access client and allow access scenario fallback. Users log on to NetScaler Gateway with the Citrix Secure Access client. If the user device fails an endpoint analysis scan, users are permitted to log on using clientless access. When this occurs, users have limited access to network resources.
- Allow users to log on using a Web browser and clientless access. Users can log on only by using clientless access and receive limited access to network resources.

How clientless VPN access policies Work

You configure clientless access to web applications by creating policies. You can configure the settings for a clientless access policy in the configuration utility. A clientless access policy is composed of a rule and a profile. You can use the preconfigured clientless access policies that come with NetScaler Gateway. You can also create your own custom clientless access policies.

NetScaler Gateway provides preconfigured policies for the following:

- Outlook Web Access and Outlook Web App
- SharePoint 2007
- All other Web applications

> **Note:**
>
> OWA 2016 and SharePoint 2016 are supported only using advanced clientless access.

Keep in mind the following characteristics of the preconfigured clientless access policies:

- They are configured automatically and cannot be changed.
- Each policy is bound at the global level.
- Each policy is not enforced unless you enable clientless access either globally or by creating a session policy.
- You cannot remove or modify global bindings, even if you do not enable clientless access.

Support for other web applications depends on the rewrite policies you configure on NetScaler Gateway. Citrix recommends testing any custom policies that you create to ensure that all components of the application rewrite successfully.

If you allow connections from Receiver for Android, Receiver for iOS, or Citrix Secure Hub, you must enable clientless access. For Citrix Secure Hub that runs on an iOS device, you must also enable Secure Browse within the session profile. Secure Browse and clientless access work together to allow connections from iOS devices. You do not have to enable Secure Browse if users do not connect with iOS devices.

The Quick Configuration wizard configures the correct clientless access policies and settings for mobile devices. Citrix recommends running the Quick Configuration wizard to configure the correct policies for connections to StoreFront and Citrix Endpoint Management.

You can bind custom clientless access policies either globally or to a virtual server. If you want to bind clientless access policies to a virtual server, you need to create a custom policy and then bind it. To enforce different policies for clientless access either globally or for a virtual server, change the priority number of the custom policy so it has a lower number than the preconfigured policies, thus giving the custom policy higher priority. If no other clientless access policies are bound to the virtual server, the preconfigured global policies take precedence.

> **Note:**
>
> You cannot change the priority numbers of the preconfigured clientless access policies.

Enable clientless VPN access

When you enable clientless access on a global level, all users receive the settings for clientless access. You can use the NetScaler Gateway wizard, a global policy, or a session policy to enable clientless

access.

In a global setting or a session profile, clientless access has the following settings:

- **On**. Enables clientless access. If you disable client choices and you do not configure or disable StoreFront, users log on by using clientless access.
- **Off**. Clientless access is not enabled by default. Clientless access is enabled after users log on with the Citrix Secure Access client. If you disable client choices and you do not configure or disable StoreFront, users log on with the Citrix Secure Access client. If endpoint analysis fails when users log on, users receive the choices page with clientless access available.
- **Disabled**. Clientless access is disabled. When you select **Disabled**, users cannot log on by using clientless access and the icon for clientless access does not appear on the choices page.

If you do not enable clientless access by using the NetScaler Gateway wizard, you can enable it globally or in a session policy by using the configuration utility.

To enable clientless access globally

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click **Global Settings**.
2. In the details pane, under **Settings**, click **Change global settings**.
3. On the **Client Experience** tab, next to **Clientless Access**, select **ON,** and then click **OK**.

To enable clientless access by using a session policy

If you want only a select group of users, groups, or virtual servers to use clientless access, disable or clear clientless access globally. Then, using a session policy, enable clientless access and bind it to users, groups, or virtual servers.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway > Policies > Session**.
2. In the details pane, on the Policies tab, click **Add**.
3. In **Name**, type a name for the policy.
4. Next to **Request Profile**, click **New**.
5. In **Name**, type a name for the profile.
6. On the **Client Experience** tab, next to Clientless Access, click **Override Global**, select **On,** and then click **Create**.
7. In the **Create Session Policy** dialog box, next to **Named Expressions**, select General, select True value, click Add Expression, click **Create,** and then click **Close**.
8. Click **Create,** and then click **Close**.

After you create the session policy that enables clientless access, you bind it to a user, group, or virtual server.

Encode the web address

When you enable clientless access, you can choose to encode the addresses of internal web applications or to leave the address as clear text. The settings are:

- Obscure. This uses standard encoding mechanisms to obscure the domain and protocol part of the resource.
- Clear. The web address is not encoded and is visible to users.
- Encrypt. The domain and protocol are encrypted by using a session key. When the web address is encrypted, the URL is different for each user session for the same web resource. If users bookmark the encoded web address, save it in the web browser and then log off, when users log on and try to connect to the web address again using the bookmark, they cannot connect to the web address.
  Note: If users save the encrypted bookmark in the Access Interface during their session, the bookmark works each time the user logs on.

You can configure this setting either globally or as part of a session policy. If you configure encoding as part of session policy, you can bind it to the users, groups, or a virtual server.

Configure web address encoding globally

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Client Experience tab, next to Clientless Access URL Encoding, select the encoding level and then click OK.

Configure web address encoding by creating a session policy

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway > Policies** and then click Session.
2. In the details pane, on the Policies tab, click Add.
3. In Name, type a name for the policy.
4. Next to Request Profile, click New.
5. In Name, type a name for the profile.
6. On the Client Experience tab, next to Clientless Access URL Encoding, click Override Global, select the encoding level, and then click OK.

7. In the Create Session Policy dialog box, next to Named Expressions, select General, select True value, click Add Expression, click Create, and then click Close.

Create clientless access policies

If you want to use the same settings as for the default clientless access policies but you want to bind the policy to a virtual server, you can copy the default policies, providing a new name for the policy. You can use the configuration utility to copy the default policies.

After you bind the new policy to the virtual server, you can set the priority of the policy so that it runs first when a user logs on.

Create a clientless access policy using default settings

1. In the configuration utility, on the navigation pane, expand **NetScaler Gateway > Policies** and then click Clientless Access.
2. In the details pane, on the Policies tab, click a default policy and then click Add.
3. In Name, type a new name for the policy, click Create, and then click Close.

Bind a clientless access policy to a virtual server

After you create the policy, bind it to the virtual server.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click Virtual Servers.
2. In the details pane, select a virtual server and then click Open.
3. In the configure NetScaler Gateway Virtual Server dialog box, click the Policies tab, and then click Clientless.
4. Click Insert Policy, select a policy from the list, and then click OK.

Create and evaluate clientless access policy expressions

When you create a policy for clientless access, you can create your own expression for the policy. When you are finished creating the expression, you can then evaluate the expression for accuracy.

1. In the configuration utility, on the navigation pane, expand **NetScaler Gateway > Policies** and then click Clientless Access.
2. In the details pane, on the Policies tab, click a default policy and then click Add.
3. In Name, type a name for the policy.
4. Next to Profile, click New.

5. In Name, type a name for the profile.
6. Configure the rewrite settings and then click Create.
7. In the Create Clientless Access Policy dialog box, under Expression, click Add.
8. In the Add Expression dialog box, create the expression, and then click OK.
9. In the Create Clientless Access Policy dialog box, click Evaluate, and if the expression tests as correct, click Create.

Advanced Clientless VPN access with NetScaler Gateway

January 8, 2024

Clientless VPN sees a way of providing remote access to the corporate's intranet resources through NetScaler Gateway without a VPN client application at the client machine. Clientless VPN provides remote access to enterprise web-applications, portals, and other resources using a web browser at the client's end.
Advanced clientless VPN solution eliminates the following limitations pertaining to clientless VPN:

- Relative URLs cannot be identified at times.
- Relative URLs generated dynamically cannot be identified.

The advanced clientless VPN identifies the absolute URL and host names and rewrites them in a new and unique manner instead of trying to rewrite relative URLs present in the HTTP-responses/Web-Pages. SharePoint no longer needs to use the default folder for rewriting URLs and a custom SharePoint access is supported.

Prerequisites

The following are the prerequisites to configure the advanced clientless VPN.

- **Wildcard server certificate** - The advanced clientless VPN rewrites URLs in a unique manner. This uniqueness is maintained for every URL per user. For example, if the web-application is hosted on `https://webapp.customer.com`, and the VPN virtual server is hosted on `https://vpn.customer.com`, then the advanced clientless VPN rewrites it as `https://cvpneqwerty.vpn.customer.com`. This means, every URL is rewritten as a subdomain of the VPN virtual server. In this new URL, `cvpneqwerty` can be decrypted back to `https://webapp.customer.com`. The string `cvpneqwerty` is dynamic and therefore for SSL, you must bind the VPN virtual server with a wildcard certificate.

  If the server is hosted with `https://vpn.customer.com`, then the server certificate must now have entries for (vpn.customer.com and .vpn.customer.com) as part of certificates CN or

SAN (where CN=common name, SAN= Subject Alternative Name). The process of binding this certificate remains the same on NetScaler Gateway.
Note: Wildcard certificates only support one-level (that is ..customer.com is not allowed). If you are already using a Wildcard certificate (for *.customer.com) and hosting `https://vpn.customer.com`, this does not work for the advanced clientless VPN. You must get a new certificate with `*.vpn.customer.com`.

- **WildCard DNS entry** - The clients (web browsers) must resolve the advanced clientless VPN app's FQDN. While setting up the NetScaler Gateway server, you must have configured a DNS entry to resolve vpn.customer.com. This allows the browser to resolve vpn.customer.com to your VPN virtual server's IP address. To resolve URLs like `https://cvpnqwerty.vpn.customer.com` to the same IP (VPN virtual server's IP address, you must add a new record for the domain of `vpn.customer.com`. Find the domain setting in your DNS server and add a new host record for "*"with the same IP address as before. After adding the host record, you must see successful ping responses for `https://cpvnanything.vpn.customer.com`.

Configure Advanced Clientless VPN access

To configure advanced clientless VPN access using the command line interface, at the command prompt, type:

```
set vpn parameter -clientlessVpnMode ON
set vpn parameter -advancedClientlessVpnMode ENABLED
```

If a session action is bound to the virtual server, you must enable the advanced clientless VPN Mode option for that session action as well.

Example:

```
set vpn sessionaction SessionActionName -advancedclientlessvpn ENABLED
```

To configure advanced clientless VPN access using the NetScaler GUI:

1. In the NetScaler GUI, navigate to **Configuration> NetScaler> Global Settings.**
2. On the **Global Settings page**, click **Change Global Settings**, and then select the **Client Experience** tab.
3. On the **Client Experience** tab, from the **Clientless Access** list, click **On**.
4. On the **Client Experience** tab, from the **Advanced Clientless VPN Mode** list, click **Enabled**.
   If you select **STRICT** from the **Advanced Clientless VPN Mode** list, the NetScaler appliance responds only to StoreFront URLs in classic clientless VPN form and blocks all other classic clientless VPN requests. This option provides a more secure configuration on the appliance for delivering internal web-resources.

> **Note:**
>
> - If a session action is bound to the virtual server, you must enable the **Advanced Clientless VPN Mode** option for that session action as well from the **Client Experience** tab in the **Configure NetScaler Gateway Session Profile** page.
> - You can select the **Override Global** option to override the global settings.
> - You can configure the advanced clientless VPN feature at a session level as well.

Caveats

The advanced clientless VPN is aimed at providing access to Enterprise Web apps. Such apps have only one FQDN for every kind of resource they need (JavaScript, css, images, and so on). Since we encode the complete FQDN of internal apps into a single-octet (clientless VPN), we lose out on the subdomain relationship. As a result, whenever an Enterprise WebApp is configured with CORS, sometimes you might notice issues while accessing it over the advanced clientless VPN.

Configure domain access for users

January 8, 2024

If users connect by using clientless access, you can restrict the network resources, domains, and websites users are permitted to access. You can use the NetScaler Gateway wizard or global settings to create lists for including or excluding access to domains.

You can allow access to all network resources, domains, and websites and then create an exclusion list. The exclusion list cites a specific set of resources that users are not allowed to access. Users cannot access any domains that are in the exclusion list.

You can also deny access to all network resources, domains, and websites and then create a specific inclusion list. The inclusion list cites the resources that users can access. Users cannot access any domains that do not appear on the list.

Note: If you configure clientless access policies for Citrix Endpoint Management or StoreFront and users connect with Receiver for Web, you need to allow the domains that Receiver for Web can access. This is required so NetScaler Gateway can rewrite network traffic for StoreFront and Endpoint Management.

To configure domain access by using the NetScaler Gateway wizard

1. In the configuration utility, click the Configuration tab and then in the navigation pane, click NetScaler Gateway.
2. In the details pane, under Getting Started, click NetScaler Gateway wizard.
3. Click Next and then follow the directions in the wizard until you reach the Configure clientless access page.
4. Click Configure Domains for Clientless Access and do one of the following:
   - To create a list of excluded domains, click Exclude domains.
   - To create a list of included domains, click Allow domains.
5. Under Domain Names, type the domain name and then click Add.
6. Repeat Step 5 for each domain you want to add to the list and then click OK when finished.
7. Continue configuring the appliance by using the NetScaler Gateway wizard.

To configure domain settings by using the configuration utility

You can also create or modify the domain list by using global settings in the configuration utility.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click Global Settings.
2. In the details pane, under Clientless Access, click Configure Domains for Clientless Access.
3. Do one of the following:
   - To create a list of excluded domains, click Exclude domains.
   - To create a list of included domains, click Allow domains.
4. Under Domain Names, type the domain name and then click Add.
5. Repeat Step 4 for each domain you want to add to the list and then click OK when finished.

Clientless VPN access for SharePoint 2003, SharePoint 2007, and SharePoint 2013

January 8, 2024

NetScaler Gateway can rewrite content from one or more SharePoint 2003 or SharePoint 2007 or SharePoint 2013 sites so that the content is available to users without requiring the Citrix Secure Access client. For the rewrite process to complete successfully, you must configure NetScaler Gateway with the host name for each SharePoint server in your network.

You can use the NetScaler Gateway wizard or the configuration utility to configure the host name for SharePoint sites.

In the NetScaler Gateway wizard, navigate through the wizard to configure your settings. When you come to the Configure clientless access page, type the web address for the SharePoint site and then click **Add**.

To add more websites or to configure SharePoint for the first time after running the NetScaler Gateway wizard, you use the configuration utility.

> **Important:**
>
> Classic Clientless Access supports versions until SharePoint 2013 and OWA 2013. Advanced Clientless Access supports SharePoint 2016 and OWA 2016, and later versions.

Configure clientless access for SharePoint by using the NetScaler GUI

1. Navigate to **NetScaler Gateway** > **Global Settings**.
2. In the details pane, under Clientless Access, click **Configure Clientless Access for SharePoint**.
3. Under Clientless Access for SharePoint, in Host name of the SharePoint server, type the host name for the SharePoint site and then click **Add**.
4. Repeat Step 3 for each SharePoint site you want to add to the list and then click **OK** when finished.

Set a SharePoint site as the home page

If you want to set a SharePoint site as the users' home page, configure a session profile and enter the host name of the SharePoint site.

To configure a SharePoint site as the home page

1. Navigate to **NetScaler Gateway > Policies,** and then click **Session**.
2. In the details pane, click **Add**.
3. In **Name**, type a name for the policy.
4. Next to **Request Profile**, click **New**.
5. In Name, type a name for the profile.
6. On the Client Experience tab, next to Home Page click **Override Global,** and then type the name of the SharePoint site.
7. Next to Clientless Access, click **Override Global**, select **On,** and then click **Create**.
8. In the Create Session Policy dialog box, next to Named Expressions, select **General**, select **True value**, click **Add Expression**, click **Create**, and then click **Close**.

After completing the session policy, bind it to users, groups, virtual servers, or globally. When users log on, they see the SharePoint website as their home page.

Enable name resolution for SharePoint 2007 servers

SharePoint 2007 servers send the configured server name as the host name within various URLs as part of the response. If a configured SharePoint server name is not the fully qualified domain name (FQDN), NetScaler Gateway cannot resolve the IP address using the SharePoint server name, and some user functions time out with the error message "HTTP:1.1 Gateway Time-out."These functions can include checking files in and out, viewing the workspace, and uploading multiple files when users are logged on using clientless access.

To resolve this issue, you can try one of the following:

- Configure a DNS suffix on NetScaler Gateway so that the SharePoint host name is converted to an FQDN before name resolution.
- Configure a local DNS entry on NetScaler Gateway for every SharePoint server name.
- Change all the SharePoint server names to use the FQDN, such as SharePoint.intranetdomain instead of SharePoint,

Configure a DNS suffix

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **DNS** and then click **DNS Suffix**.
2. In the details pane, click **Add**.
3. In **DNS Suffix**, type the intranet domain name as the suffix, click **Create**, and then click **Close**.

You can repeat Step 3 for each domain you want to add.

To configure a local DNS record for every SharePoint server name on NetScaler Gateway

1. In the configuration utility, in the navigation pane, expand **DNS > Records** and then click **Address Records**.
2. In the details pane, click **Add**.
3. In **Host Name**, type the SharePoint host name for the DNS address record.
4. In **IP Address**, type the IP address of the SharePoint server, click **Add**, click **Create**, and then click **Close**.

The host name for which an A record is added must not have a CNAME record. Also, there cannot be duplicate A records on the appliance.

Enable clientless VPN access persistent cookies

January 8, 2024

Persistent cookies are required for accessing certain features of SharePoint, such as opening and editing Microsoft Word, Excel, and PowerPoint documents hosted on the SharePoint server.

A persistent cookie remains on the user device and is sent with each HTTP request. NetScaler Gateway encrypts the persistent cookie before sending it to the plug-in on the user device, and refreshes the cookie periodically as long as the session exists. The cookie becomes stale if the session ends.

In the NetScaler Gateway wizard, administrators can enable persistent cookies globally. You can also create a session policy to enable persistent cookies per user, group, or virtual server.

The following options are available for persistent cookies:

- Allow enables persistent cookies and users can open and edit Microsoft documents stored in SharePoint.
- Deny disables persistent cookies and users cannot open and edit Microsoft documents stored in SharePoint.
- Prompt prompts users to allow or deny persistent cookies during the session.

Persistent cookies are not required for clientless access if users do not connect to SharePoint.

Configure persistent cookies for clientless VPN access for SharePoint

You can configure persistent cookies for clientless access for SharePoint either globally or as part of a session policy.

To configure persistent cookies globally

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Client Experience tab, next to Clientless Access Persistent Cookies, select an option and then click OK.

To configure persistent cookies as part of a session policy

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway > Policies** and then click Session.

2. In the details pane, on the Policies tab, click Add.
3. In Name, type a name for the policy.
4. Next to Request Profile, click New.
5. In Name, type a name for the profile.
6. On the Client Experience tab, next to Clientless Access Persistent Cookies, click Override Global, select an option, and then click Create.
7. In the Create authentication policy dialog box, next to Named Expressions, select General, select True value, click Add Expression, click Create and then click Close.

Citrix SSO VPN client for mobile devices

January 8, 2024

Citrix SSO is the VPN client for mobile devices (macOS, iOS, and iOS). Citrix SSO provides complete Mobile Device Management (MDM) support on macOS, iOS, and Android. With an MDM server, an admin can remotely configure and manage device level VPN profiles and per-app VPN profiles.
Citrix SSO also supports most of the commonly used features.

References

- Citrix Secure Access client
- NetScaler Gateway VPN clients and supported features

Configure the Client Choices page

January 8, 2024

You can configure NetScaler Gateway to provide users with multiple logon options. By configuring the client choices page, users have the option of logging on from one location with the following choices:

- Citrix Secure Access client for Windows
- Citrix Secure Access client for macOS X
- StoreFront
- Web Interface
- Clientless access

Users log on to NetScaler Gateway by using the web address in the certificate bound to NetScaler Gateway or the virtual server. By creating a session policy and profile, you can determine the logon choices users receive. Depending on how you configure NetScaler Gateway, the client choices page displays up to three icons representing the following logon choices:

- Network Access. When users log on to NetScaler Gateway for the first time by using a web browser and then select Network Access, the download page appears. When users click Download, the plug-in downloads and installs on the user device. When the download and installation is complete, the Access Interface appears. If you install a newer or revert to an older version of NetScaler Gateway, the Citrix Secure Access client for Windows silently upgrades or downgrades to the version on the appliance. If users connect by using the Citrix Secure Access client for Mac, the plug-in silently upgrades if a new appliance version is detected when users log on. This version of the plug-in does not silently downgrade.
- Web Interface or StoreFront. If users select the Web Interface to log on, the Web Interface page appears. Users can then access their published applications or virtual desktops. If users select StoreFront to log on, Receiver opens, and users can access applications and desktops.
  Note: If you configure StoreFront as a client choice, applications and desktops do not appear in the left pane of the Access Interface.
- Clientless access. If users select clientless access to log on, the Access Interface or your customized home page appears. In the Access Interface, users can navigate to file shares, websites, and use Outlook Web Access.

Secure Browse allows users to connect through NetScaler Gateway from an iOS device. If you enable Secure Browse, when users log on by using Secure Hub, Secure Browse disables the client choices page.

Display the Client Choices page at the logon

When you enable the client choices option, users can log on with the Citrix Secure Access client, the Web Interface, Receiver, or clientless access from one webpage after successful authentication to NetScaler Gateway. When the logon is successful, icons appear in the webpage from which users can choose the method to establish a connection.

You can enable client choices without using endpoint analysis or implementing access scenario fallback. If you do not define a client security expression, users receive connection options for the settings that are configured on NetScaler Gateway. If a client security expression exists for the user session and the user device fails the endpoint analysis scan, the choices page offers only the option to use the Web Interface if it is configured. Otherwise, users can use clientless access to log on.

You configure client choices either globally or by using a session profile and policy.

> **Important:**
>
> When configuring client choices, do not configure quarantine groups. User devices that fail the endpoint analysis scan and are quarantined and treated the same as user devices that pass the endpoint scan.

Enable client choices options globally

1. In the GUI, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway** and then click **Global Settings**.
2. In the details pane, under Settings, click **Change global settings**.
3. On the Client Experience tab, click **Advanced Settings**.
4. On the General tab, click **Client Choices,** and then click **OK**.

Enable client choices as part of a session policy

You can also configure client choices as part of a session policy and then bind it to users, groups, and virtual servers.

1. In the GUI, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway > Policies,** and then click **Session**.
2. In the details pane, on the Policies tab, click **Add**.
3. In Name, type a name for the policy.
4. Next to Request Profile, click **New**.
5. In Name, type a name for the profile.
6. On the Client Experience tab, click **Advanced**.
7. On the General tab, next to Client Choices, click **Override Global**, click **Client Choices**, click **OK,**, and then click **Create**.
8. In the Create Session Policy dialog box, next to Named Expressions, select **General**, select **True value**, click **Add Expression**, click **Create**, and then click **Close**.

Configure Client Choices options

In addition to enabling client choices by using a session profile and policy, you need to configure the settings for the user software. For example, you want users to log on using either the Citrix Secure Access client, StoreFront or the Web Interface, or clientless access. You create one session profile that enables all three options and client choices. Then, you create a session policy with the expression set to True value with the profile attached. Next, you bind the session policy to a virtual server.

Before creating the session policy and profile, you need to create an authorization group for users.

Create an authorization group

1. In the configuration utility, on the Configuration tab, in the navigation pane, **NetScaler Gateway > User Administration**, and then click **AAA Groups**.
2. In the details pane, click **Add**.
3. In **Group Name**, type the name of the group.
4. On the **Users** tab, select the users, click **Add** for each one, click **Create**, and then click **Close**.

The following procedure is an example session profile for client choices with the Citrix Secure Access client, StoreFront, and clientless access.

Create a session profile for client choices

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway > Policies > Session**.
2. In the details pane, click the **Profiles**, tab and then click **Add**.
3. In **Name**, type a name for the profile.
4. On the **Client Experience** tab, do the following:
   a) Next to Home Page, click **Override Global** and then clear **Display Home Page**. This disables the Access Interface.
   b) Next to **Clientless Access**, click **Override Global**, and then select **OFF**.
   c) Next to **Plug-in Type**, click **Override Global**, and then select Windows/Mac OS X.
   d) Click **Advanced Settings** and next to **Client Choices**, click **Override Global**, click **Client Choices**.
5. On the **Security** tab, next to **Default Authorization Action**, click **Override Global** and then select **ALLOW**.
6. On the **Security** tab, click **Advanced Settings**.
7. Under **Authorization Groups**, click **Override Global**, click **Add**, and then select the group.
8. On the **Published Applications** tab, do the following:
   a) Next to **ICA Proxy**, click **Override Global**, and then select **OFF**.
   b) Next to **Web Interface Address**, click **Override Global**, and then type the Web address of StoreFront, such as http://ipAddress/Citrix/.
   c) Next to **Web Interface Portal Mode**, click **Override Global** and then select **COMPACT**.
   d) Next to **Single Sign-On Domain**, click **Override Global**, and then type the name of the domain.
9. Click **Create**, and then click **Close**.

If you want to use the Citrix Secure Access client for Java as a client choice, on the **Client Experience** tab, in plug-in Type, select **Java**. If you select this choice, you must configure an intranet application

and set the interception mode to Proxy.

After creating the session profile, create a session policy. Within the policy, select the profile, and set the expression to True value.

To use StoreFront as a client choice, you must also configure the Secure Ticket Authority (STA) on the NetScaler Gateway. The STA is bound to the virtual server.

> **Note:**
>
> If the server running the StoreFront is not available, the Citrix Virtual Apps choice does not appear on the choices page.

Configure the STA server globally

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway**, and then click **Global Settings**.
2. In the details pane, under Servers, click **Bind/Unbind STA Servers** to be used by the Secure Ticket Authority.
3. In the **Bind/Unbind STA Servers** dialog box, click **Add**.
4. In the **Configure STA Server** dialog box, in URL, type the web address of the STA server, and then click **Create**.
5. Repeat Steps 3 and 4 to add more STA servers and then click **OK**.

Bind the STA to a virtual server

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway** and then click **Virtual Servers**.
2. In the details pane, click a virtual server, and then click **Open**.
3. On the **Published Applications** tab, under **Secure Ticket Authority**, under **Active**, select the STA servers and then click **OK**.

You can also add STA servers on the **Published Applications** tab.

Configure Access Scenario Fallback

January 8, 2024

SmartAccess allows NetScaler Gateway to determine automatically the methods of access that are allowed for a user device based on the results of an endpoint analysis scan. Access scenario fallback further extends this capability by allowing a user device to fall back from the Citrix Secure Access client

to the Web Interface or StoreFront by using Citrix Workspace app if the user device does not pass the initial endpoint analysis scan.

To enable access scenario fallback, you configure a post-authentication policy that determines whether users receive an alternative method of access when logging on to NetScaler Gateway. This post-authentication policy is defined as a client security expression that you configure either globally or as part of a session profile. If you configure a session profile, the profile is associated to a session policy that you then bind to users, groups, or virtual servers. When you enable access scenario fallback, NetScaler Gateway initiates an endpoint analysis scan after user authentication. The results for user devices that do not meet the requirements of a fallback post-authentication scan are as follows:

- If client choices are enabled, users can log on to the Web Interface or StoreFront by using Citrix Workspace app only.
- If clientless access and client choices are disabled, users can be quarantined into a group that provides access only to the Web Interface or StoreFront.
- If clientless access and the Web Interface or StoreFront are enabled on NetScaler Gateway and ICA Proxy is disabled, users fall back to clientless access.
- If the Web Interface or StoreFront is not configured and clientless access is set to allow, users fall back to clientless access.

When clientless access is disabled, the following combination of settings must be configured for the access scenario fallback:

- Define client security parameters for the fallback post-authentication scan.
- Define the Web Interface home page.
- Disable client choices.
- If user devices fail the client security check, users are placed into a quarantine group that allows access only to the Web Interface or StoreFront and to published applications.

Create policies for Access Scenario Fallback

To configure NetScaler Gateway for access scenario fallback, you need to create policies and groups in the following ways:

- Create a quarantine group in which users are placed if the endpoint analysis scan fails.
- Create a global Web Interface or StoreFront setting that is used if the endpoint analysis scan fails.
- Create a session policy that overrides the global setting and then bind the session policy to a group.
- Create a global client security policy that is applied if the endpoint analysis fails.

When configuring the access scenario fallback, use the following guidelines:

- Using client choices or access scenario fallback requires the Endpoint Analysis plug-in for all users. If endpoint analysis cannot run or if users select Skip Scan during the scan, users are denied access.
  Note: The option to skip the scan is removed in NetScaler Gateway 10.1, Build 120.1316.e
- When you enable client choices, if the user device fails the endpoint analysis scan, users are placed into the quarantine group. Users can continue to log on with either the Citrix Secure Access client or the Citrix Workspace app to the Web Interface or StoreFront.
  Note: Citrix recommends that you do not create a quarantine group if you enable client choices. User devices that fail the endpoint analysis scan are quarantined are treated in the same way as user devices that pass the endpoint scan.
- If the endpoint analysis scan fails and the user is put in the quarantine group, the policies that are bound to the quarantine group are effective only if there are no policies bound directly to the user that have an equal or lower priority number than the policies bound to the quarantine group.
- You can use different web addresses for the Access Interface and, the Web Interface or StoreFront. When you configure the home pages, the Access Interface home page takes precedence for the Citrix Secure Access client and the Web Interface home page takes precedence for Web Interface users. The Citrix Workspace app home page takes precedence for StoreFront.

Create a quarantine group

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway > User Administration**, and then click **AAA Groups**.
2. In the details pane, click **Add**.
3. In **Group Name**, type a name for the group, click **Create,** and then click **Close**.
   Important: The name of the quarantine group must not match the name of any domain group to which users might belong. If the quarantine group matches an Active Directory group name, users are quarantined even if the user device passes the endpoint analysis security scan.

After creating the group, configure NetScaler Gateway to fall back to the Web Interface if the user device fails the endpoint analysis scan.

Configure settings to quarantine user connections

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click **Global Settings**.
2. In the details pane, under **Settings**, click **Change global settings**.
3. In the **Global NetScaler Gateway Settings** dialog box, on the **Published Applications** tab, next to **ICA Proxy**, select **OFF**.
4. Next to **Web Interface Address**, type the web address for StoreFront or the Web Interface.

5. Next to **Single Sign-On Domain**, type the name of your Active Directory domain, and then click **OK**.

After configuring the global settings, create a session policy that overrides the global ICA Proxy setting and then bind the session policy to the quarantine group.

Create a session policy for Access Scenario Fallback

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway > Policies** and then click **Session**.
2. In the details pane, click **Add**.
3. In **Name**, type a name for the policy.
4. Next to **Request Profile**, click **New**.
5. On the **Published Applications** tab, next to **ICA Proxy**, click **Override Global**, select **On,** and then click **Create**.
6. In the **Create Session Policy** dialog box, next to **Named Expressions**, select **General**, select **True value**, click **Add Expression**, click **Create,** and then click **Close**.

After creating the session policy, bind the policy to a quarantine group.

Bind the session policy to the quarantine group

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway > User Administration**, and then click **AAA Groups**.
2. In the details pane, select a group, and then click **Open**.
3. Click Session.
4. On the **Policies** tab, select **Session**, and, then click **Insert Policy**.
5. Under **Policy Name**, select the policy, and then click **OK**.

After creating the session policy and profile enabling the Web Interface or StoreFront on NetScaler Gateway, create a global client security policy.

Create a global client security policy

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click **Global Settings**.
2. In the details pane, under **Settings**, click **Change global settings**.
3. On the **Security** tab, click **Advanced Settings**.
4. In **Client Security**, enter the expression. For more information about configuring system expressions, see Configuring System Expressions and Configuring Compound Client Security Expressions

5. In **Quarantine Group**, select the group you configured in the group procedure, and then click **OK**.

Configure connections for the Citrix Secure Access client

January 8, 2024

You configure user device connections by defining the resources users can access in the internal network. Configuring user device connections includes:

- Defining the domains to which users are allowed access.
- Configuring IP addresses for users, including address pools (intranet IPs).
- Configuring time-out settings.
- Configuring single sign-on.
- Configuring client interception.
- Configuring split tunneling.
- Configuring connections through a proxy server.
- Configuring user software to connect through NetScaler Gateway.
- Configuring access for mobile devices.

You configure most user device connections by using a profile that is part of a session policy. You can also define user device connection settings by using intranet applications, preauthentication, and traffic policies.

> **Note:**
>
> Windows VPN plug-in and EPA plug-ins collect telemetry data for its various operations. To disable the functionality do the following on the client machine.
>
> Set registry “HKLM\Software\Citrix\Secure Access Client\DisableGA”of type REG_DWORD to 1.

Configure the number of user sessions

January 8, 2024

You can configure the maximum number of users who are allowed to connect to NetScaler Gateway at a particular point in time, at either the global level or on a per virtual server level. Sessions are not created on NetScaler Gateway when the number of users connecting to the appliance exceeds the value that you configure. If the number of users exceeds the number you allow, users receive an error message.

To set the global user limit

When you configure the user limit globally, the restriction applies to all users who establish sessions to different virtual servers on the system. When the number of user sessions reaches the value you set, no new sessions can be established on any virtual server present on NetScaler Gateway.

You set the maximum number of users at the global level when you set the default authentication type for NetScaler Gateway.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click Global Settings.
2. In the details pane, under Settings, click Change authentication settings.
3. In the Global Authentication Settings dialog box, in Maximum Number of Users, type the number of users and then click OK.

To set the user limit per virtual server

You can also apply the user limit to each virtual server on the system. When you configure the user limit per virtual server, the restriction applies only to users who establish sessions with the particular virtual server. Users who establish sessions with other virtual servers are not affected by this limit.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click Virtual Servers.
2. In the details pane, click a virtual server and then click Open.
3. In Max Users, type the number of users and then click OK.

Configure time-out settings

January 8, 2024

You can configure NetScaler Gateway to force a disconnection if there is no activity on the connection for a specified number of minutes. One minute before a session times out (disconnects), the user receives an alert indicating the session closes. If the session closes, the user must log on again.

The following time-out options are available.

- **Forced time-out.** If you enable this setting, NetScaler Gateway disconnects the session after the timeout interval elapses regardless of what the user is doing. There is no action that the user can take to prevent the disconnection from occurring when the timeout interval elapses. This setting is enforced for users who connect with the Citrix Secure Access client, Citrix Workspace app, Secure Hub, or through a web browser. Minimum value is 1, and maximum value is 65535.

- **Session time-out.** If you enable this setting, NetScaler Gateway disconnects the session if no network activity is detected for the specified interval. This setting is enforced for users who connect with the Citrix Secure Access client, Citrix Workspace app, Citrix Secure Hub, or through a web browser. The default timeout setting is 30 minutes. Minimum value is 1, and maximum value is 65535.
- **Idle session time-out.** The duration after which the Citrix Secure Access client terminates an idle session if there is no user activity, such as from the mouse, keyboard, or touch for the specified interval. This setting is enforced for users who connect with the Citrix Secure Access client only. Minimum value is 1, and maximum value is 9999.

You can enable any of the timeout settings by entering a value between 1 and 65536 to specify the minutes for the time-out interval. If you enable more than one of these settings, the first time-out interval to elapse closes the user device connection.

You configure time-out settings by configuring global settings or by using a session profile. When you add the profile to a session policy, the policy is then bound to a user, group, or virtual server. When you configure the time-out settings globally, the settings are applied to all user sessions.

> **Note:**
>
> - In Always On (service mode or user mode), the VPN client ignores all the timeouts. Forced timeout and session timeout decisions occur on the NetScaler appliance and therefore those timeouts work as intended. If such timeout occurs, the VPN plug-in tries to perform automatic authentication.
>
> In Always On, as the user device must be connected via the VPN tunnel all the time, do not configure forced timeout or client idle timeout. However, session timeout can be configured to get rid of stale sessions.
>
> - Some applications, such as Microsoft Outlook, automatically send network traffic probes to email servers without any user intervention. Citrix recommends that you configure Idle session time-out with session time-out to ensure that a session left unattended on a user device times out in a reasonable time.

Configure forced time-outs

A forced time-out disconnects the Citrix Secure Access client automatically after a specified amount of time. You can configure a forced time-out globally or as part of a session policy.

Configure a global forced time-out

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, expand NetScaler Gateway and then click **Global Settings**.

2. In the details pane, under **Settings**, click **Change global settings**.
3. On the **Network Configuration** tab, click **Advanced Settings**.
4. In Forced Time-out (mins), type the number of minutes users can stay connected.
5. In Forced Time-out Warning (mins), type the number of minutes before users are warned that the connection is due to be disconnected and then click **OK**.

Configure a forced time-out within a session policy

If you want to have further control over who receives the forced time-out, create a session policy and then apply the policy to a user or group.

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, expand **NetScaler Gateway** > **Policies** and then click **Session**.
2. In the details pane, click **Add**.
3. In Name, type a name for the policy.
4. Next to Request Profile, click **New**.
5. In Name, type a name for the profile.
6. On the **Network Configuration** tab, click **Advanced**.
7. Under Timeouts, click **Override Global** and in Forced Time-out (mins) type the number of minutes users can stay connected.
8. Next to **Forced Time-out Warning (mins)**, click **Override Global** and type the number of minutes users are warned that the connection is due to be disconnected. Click **OK** twice.
9. In the **Create Session Policy** dialog box, next to **Named Expressions**, select General, select **True value**, click **Add Expression**, click **Create,** and then click **Close**.

Configure session or idle time-outs

You can use the NetScaler GUI to configure session and client time-out settings globally or to create a session policy. When you create a session policy and profile, set the expression to True.

> **Note:**
>
> If you do not explicitly override the global setting and set the session timeout in **Client Experience > Session Time-out(mins)**, this can result in authentication loops that require relogin. This occurs even with the default session time-out of 30 minutes.

To configure a session or client idle time-out globally by using the GUI

1. On the **Configuration** tab, in the navigation pane, expand **NetScaler Gateway** and then click **Global Settings**.
2. In the details pane, under **Settings**, click **Change global settings**.

3. On the **Client Experience** tab, do one or both of the following:
   - In **Session Time-out (mins)**, type the number of minutes.
   - In **Client Idle Time-out (mins)**, type the number of minutes and then click **OK**.

To configure session or client idle time-out settings by using a session policy by using the GUI

1. On the **Configuration** tab, in the navigation pane, expand **NetScaler Gateway** > **Policies** and then click **Session**
2. In the **NetScaler Gateway Session Policies and Profiles** page, click **Session Profiles**, and then click **Add**.
3. In Name, type a name for the profile.
4. On the **Client Experience** tab, do one or both of the following:
   - Next to **Session Time-out (mins)**, click **Override Global** and then type the number of minutes and then click **Create**.
   - Next to **Client Idle Time-out (mins)**, click **Override Global**, type the number of minutes and then click **Create**.
5. a) In the **NetScaler Gateway Session Policies and Profiles** page, click **Sessions Policies**, and then click **Add**.
6. In the **Create NetScaler Gateway Session Policy**,
   - In **Name**, enter the name for the policy.
   - In **Profile**, select the profile that specifies the action to be applied by the new session policy if the rule criteria are met.
   - select **Advanced policy**.
   - In the **Expression** field, add your expression or name of a named expression, specifying the traffic that matches the policy.
   - Click **Create**, and then click **Close**.

Connect to internal network resources

January 8, 2024

You can configure NetScaler Gateway to enable users to access resources in the internal network. If you disable split tunneling, all network traffic from the user device is sent to NetScaler Gateway and authorization policies determine whether the traffic is allowed to pass through to internal network resources. When you enable split tunneling, only traffic destined for the internal network is intercepted

by the user device and sent to NetScaler Gateway. You configure which IP addresses NetScaler Gateway intercepts by using intranet applications.

If you are using the Citrix Secure Access client for Windows, set the interception mode to transparent. If you are using the Citrix Secure Access client for Java, set the interception mode to proxy. When you set the interception mode to transparent, you can allow access to network resources using:

- A single IP address and subnet mask
- A range of IP addresses

If you set the interception mode to proxy, you can configure destination and source IP addresses and port numbers.

Configure network access to internal network resources

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, expand NetScaler Gateway, expand Resources, and then click **Intranet Applications.**
2. In the details pane, click **Add.**
3. Complete the parameters for allowing network access, click **Create** and then click **Close.**

Configure split tunneling

January 8, 2024

You can enable split tunneling to prevent the Citrix Secure Access client from sending unnecessary network traffic to NetScaler Gateway.

When you do not enable split tunneling, the Citrix Secure Access client captures all network traffic originating from a user device and sends the traffic through the VPN tunnel to NetScaler Gateway.

If you enable split tunneling, the Citrix Secure Access client sends only traffic destined for networks protected by NetScaler Gateway through the VPN tunnel. The Citrix Secure Access client does not send network traffic destined for unprotected networks to NetScaler Gateway.

When the Citrix Secure Access client starts, it obtains the list of intranet applications from NetScaler Gateway. The Citrix Secure Access client examines all packets transmitted on the network from the user device and compares the addresses within the packets to the list of intranet applications. If the destination address in the packet is within one of the intranet applications, the Citrix Secure Access client sends the packet through the VPN tunnel to NetScaler Gateway. If the destination address is not in a defined intranet application, the packet is not encrypted and the user device routes the packet appropriately. When you enable split tunneling, intranet applications define the network traffic that is intercepted.

> **Note:**
>
> If users connect to published applications in a server farm by using Citrix Workspace app, you do not need to configure split tunneling.

NetScaler Gateway also supports reverse split tunneling, which defines the network traffic that NetScaler Gateway does not intercept. If you set split tunneling to reverse, intranet applications define the network traffic that NetScaler Gateway does not intercept. When you enable reverse split tunneling, all network traffic directed to internal IP addresses bypasses the VPN tunnel, while other traffic goes through NetScaler Gateway. Reverse split tunneling can be used to log all non-local LAN traffic. For example, if users have a home wireless network and are logged on with the Citrix Secure Access client, NetScaler Gateway does not intercept network traffic destined to a printer or another device within the wireless network.

For more information about intranet applications, see Configuring Client Interception.

You configure split tunneling as part of the session policy.

To configure split tunneling

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway Policies** and then click **Session.**
2. In the details pane, on the **Profiles** tab, select a profile and then click **Open.**
3. On the **Client Experience** tab, next to **Split Tunnel**, select **Global Override**, select an option and then click **OK** twice.

Configuring Split Tunneling and Authorization

When planning your NetScaler Gateway deployment, it is important to consider split tunneling and the default authorization action and authorization policies.

For example, you have an authorization policy that allows access to a network resource. You have split tunneling set to ON and you do not configure intranet applications to send network traffic through NetScaler Gateway. When NetScaler Gateway has this type of configuration, access to the resource is allowed, but users cannot access the resource.

If the authorization policy denies access to a network resource, you have split tunneling set to ON, and intranet applications are configured to route network traffic through NetScaler Gateway, the Citrix Secure Access client sends traffic to NetScaler Gateway, but access to the resource is denied.

For more information about the split tunneling options, see Split tunneling options.

Configure client interception

January 8, 2024

You configure interception rules for user connections on NetScaler Gateway by using Intranet Applications. By default, when you configure the system IP address, a mapped IP address, or a subnet IP address on the appliance, subnet routes are created based on these IP addresses. Intranet applications are created automatically based on these routes and can be bound to a virtual server. If you enable split tunneling, you must define intranet applications for client interception to occur.

You can configure intranet applications by using the GUI. You can bind intranet applications to users, groups, or virtual servers.

If you enable split tunneling and users connect by using WorxWeb or WorxMail, when you configure client interception, you must add the IP addresses for Citrix Endpoint Management and your Exchange server. If you do not enable split tunneling, you do not need to configure the Endpoint Management and Exchange IP addresses in Intranet Applications.

For information about split tunneling configuration, see Configure split tunneling.

Configure intranet applications for the Citrix Secure Access client

You create intranet applications for user access to resources by defining the following:

- One IP address
- A range of IP addresses
- A host name

When you define an intranet application on NetScaler Gateway, the Citrix Secure Access client for Windows intercepts user traffic that is destined to the resource and sends the traffic through NetScaler Gateway.

When configuring intranet applications, consider the following:

- When Split Tunnel is ON,
  - Configure the intranet applications.
  - Assign intranet applications to every authentication, authorization, and auditing group.
- When Split Tunnel is OFF,
  - All traffic intercepts through the VPN tunnel.
  - Intranet applications need not be configured.
- When Split Tunnel is REVERSE,

- Configure the intranet applications. The traffic that is not specified by the intranet applications pass through the VPN tunnel.
- Assign the intranet applications to be excluded from VPN to every authentication, authorization, and auditing group.

> **Important:**
>
> Interception must be set to **TRANSPARENT** irrespective of the split tunnel configuration.

Note:

- When configuring an intranet application, you must select an interception mode that corresponds to the type of plug-in software used to make connections.
- You cannot configure an intranet application for both proxy and transparent interception.

To create an intranet application for one IP address

1. On the Configuration tab, in the navigation pane, expand **NetScaler Gateway Resources** and then click **Intranet Applications.**
2. In the details pane, click **Add.**
3. In Name, type a name for the profile.
4. In the **Create Intranet Application** dialog box, select **TRANSPARENT.**
5. In **Destination Type**, select **IP Address** and **Netmask.**
6. In Protocol, select the protocol that applies to the network resource.
7. In **IP Address**, type the IP address.
8. In **Netmask**, type subnet mask, click **Create** and then click **Close.**

To configure an IP address range

If you have multiple servers in your network, such as web, email, and file shares, you can configure a network resource that includes the IP range for network resources. This setting allows users access to the network resources contained in the IP address range.

1. On the **Configuration** tab, in the navigation pane, expand **NetScaler Gateway Resources** and then click **Intranet Applications.**
2. In the details pane, click **Add.**
3. In **Name**, type a name for the profile.
4. In Protocol, select the protocol that applies to the network resource.
5. In the **Create Intranet Application** dialog box, select **TRANSPARENT**.
6. In **Destination Type**, select **IP Address Range.**
7. In **IP Start**, type the starting IP address and in IP End, type the ending IP address, click **Create** and then click **Close.**

To create an intranet application for a host name

1. On the Configuration tab, in the navigation pane, expand **NetScaler Gateway Resources** and then click **Intranet Applications.**
2. In the details pane, click **Add.**
3. In **Name**, type a name for the profile.
4. In the **Create Intranet Application** dialog box, select **TRANSPARENT.**
5. In **Destination Type**, select **hostname**.
6. In Protocol, select **ANY**, click **Create,** and then click **Close.**

> **Important:**
>
> - From release 13.0 build 36.27 and later, the Windows VPN plug-in supports host name (FQDN) based rules for split tunneling. You must upgrade both the NetScaler appliance and the Windows VPN plug-in to release 13.0 build 36.27 or later.
> - Wildcard host names are also supported. For example, if an intranet application with the host name "*.example.com"is configured, `a1.example.com`, `b2.example.com`, and so on gets tunneled.
> - Host name-based intranet application works only when you have split tunneling set to ON or REVERSE.

Configure name service resolution

January 8, 2024

During installation of NetScaler Gateway, you can use the NetScaler Gateway wizard to configure other settings, including name service providers. The name service providers translate the fully qualified domain name (FQDN) to an IP address. In the NetScaler Gateway wizard, you can configure a DNS or WINS server, set the priority of the DNS lookup, and the number of times to retry the connection to the server.

When you run the NetScaler Gateway wizard, you can add a DNS server then. You can add more DNS servers and a WINS server to NetScaler Gateway by using a session profile. You can then direct users and groups to connect to a name resolution server that is different from the one you originally used the wizard to configure.

Before configuring an extra DNS server on NetScaler Gateway, create a virtual server that acts as a DNS server for name resolution.

Add a DNS or a WINS server within a session profile

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, expand **NetScaler Gateway Policies** and then click **Session.**
2. In the details pane, on the Profiles tab, select a profile and then click Open.
3. On the Network Configuration tab, do one of the following:
   - To configure a DNS server, next to DNS Virtual Server, click **Override Global**, select the server, and then click **OK.**
   - To configure a WINS server, next to WINS Server IP, click **Override Global**, type the IP address and then click **OK**.

> **Important:**
>
> Responder policies are not evaluated for non-addressable DNS virtual servers attached to the VPN session profile.

Enable proxy support for user connections

June 5, 2024

User devices can connect through a proxy server for access to internal networks. NetScaler Gateway supports the HTTP, SSL, FTP, and SOCKS protocols. To enable proxy support for user connections, you specify the settings on NetScaler Gateway. You can specify the IP address and port used by the proxy server on NetScaler Gateway. The proxy server is used as a forward proxy for all further connections to the internal network.

Proxy settings

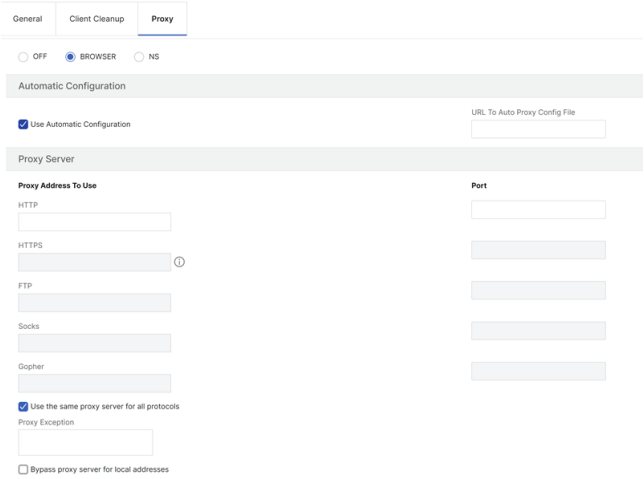
You can configure proxy settings on the browser or on the NetScaler appliance. To configure proxy settings on the browser or the appliance, navigate to **NetScaler Gateway > Global Settings > Change Global NetScaler Gateway Settings > Client Experience tab > Advanced Settings > Proxy**, and then select **Browser** or **NS** as applicable.

- **Browser**: When you choose to configure proxy settings on the browser, you can use the automatic configuration option by providing a link to the auto proxy config file. Automatic configuration might overwrite the manual settings.

  Also, when you select **Browser**, you can bypass the previously configured proxies by selecting the proxy exception option.

Note: Different types of clients have different capabilities regarding **Browser** proxy configuration. For details, see NetScaler Gateway VPN clients and supported features.

- **NS**: You cannot use the automatic configuration option if you configure proxy settings on the NetScaler appliance. You cannot bypass the previously configured proxies when you configure the proxy settings on the appliance.
- **OFF**: When this option is selected, NetScaler Gateway disables the proxy settings in the VPN plug-in.



To configure proxy support for user connections

1. In the navigation pane, expand **NetScaler Gateway** and then click **Global Settings.**
2. In the details pane, under **Settings**, click Change global settings.
3. On the Client Experience tab, click **Advanced Settings**.
4. On the **Proxy tab**, under **Proxy Settings**, select **Browser.**
5. For the protocols, type the IP address and port number and then click **OK.**

> **Note:**
>
> - If you select **NS**, you can configure proxy servers that support secure and unsecure HTTP connections only.
> - After you enable proxy support on NetScaler Gateway, you specify configuration details on the user device for the proxy server that corresponds to the protocol.
>
> After you enable proxy support, NetScaler Gateway sends the proxy server details to the client Web browser and changes the proxy configuration on the browser.
>
> – When the user device connects to NetScaler Gateway, the user device can communicate with the proxy server directly for connection to the user's network.

> – When the user device disconnects from NetScaler Gateway, the proxy settings are restored to the previous default settings, that was present before connecting to the VPN plug-in.

To configure one proxy server to use all protocols for NetScaler Gateway

You can configure one proxy server to support all the protocols that NetScaler Gateway uses. This setting provides one IP address and port combination for all the protocols.

1. In the navigation pane, expand **NetScaler Gateway** and then click **Global Settings**.
2. In the details pane, under **Settings**, click Change global settings.
3. On the **Client Experience** tab, click **Advanced Settings.**
4. On the **Proxy** tab, under **Proxy Settings**, select **Browser.**
5. For the protocols, type the IP address and port number.
6. Click Use the same proxy server for all protocols and then click **OK.**

When you disable split tunneling and set all proxy settings to On, proxy settings are propagated to user devices. If proxy settings are set to Appliance, the settings are not propagated to user devices.

NetScaler Gateway makes connections to the proxy server on behalf of the user device. The proxy settings are not propagated to the user's browser, so no direct communication between the user device and the proxy server is possible.

To configure the NetScaler Gateway to be a proxy server

When you configure NetScaler Gateway as a proxy server, unsecure and secure HTTP is the only supported protocols.

1. In the navigation pane, expand **NetScaler Gateway** and then click **Global Settings.**
2. In the details pane, under **Settings**, click Change global settings.
3. On the **Client Experience** tab, click **Advanced Settings.**
4. On the **Proxy** tab, under **Proxy Settings**, select **NS**.
5. For the protocols, type the IP address and port number and then click **OK.**

Configure address pools

January 8, 2024

In some situations, users who connect with the Citrix Secure Access client need a unique IP address for NetScaler Gateway. For example, in a Samba environment, each user connecting to a mapped

network drive needs to appear to originate from a different IP address. When you enable address pools (also known as IP pooling) for a group, NetScaler Gateway can assign a unique IP address alias to each user.

You configure address pools by using intranet IP addresses. The following types of applications might need to use a unique IP address that is drawn from the IP pool:

- Voice over IP
- Active FTP
- Instant messaging
- Secure shell (SSH)
- Virtual network computing (VNC) to connect to a computer desktop
- Remote desktop (RDP) to connect to a client desktop

You can configure NetScaler Gateway to assign an internal IP address to users that connect to NetScaler Gateway. Static IP addresses can be assigned to users or a range of IP addresses can be assigned to a group, virtual server, or to the system globally.

NetScaler Gateway allows you to assign IP addresses from your internal network to your remote users. An IP address on the internal network can address a remote user. If you choose to use a range of IP addresses, the system dynamically assigns an IP address from that range to a remote user on demand.

When you configure address pools, be aware of the following:

- Assigned IP addresses must be routed correctly. To ensure the correct routing, consider the following:
  - If you do not enable split tunneling, make sure that the IP addresses can be routed through network address translation (NAT) devices.
  - Any servers accessed by user connections with intranet IP addresses must have the proper gateways configured to reach those networks.
  - Configure gateways or a static route on NetScaler Gateway so that network traffic from user software is routed to the internal network.
- Only contiguous subnet masks can be used when assigning IP address ranges. A subset of a range can be assigned to a lower-level entity. For example, if an IP address range is bound to a virtual server, bind a subset of the range to a group.
- IP address ranges cannot be bound to multiple entities within a binding level. For example, a subset of an address range that is bound to a group cannot be bound to a second group.
- NetScaler Gateway does not allow you to remove or unbind IP addresses while they are actively in use by a user session.
- Internal network IP addresses are assigned to users by using the following hierarchy:
  - User's direct binding
  - Group assigned address pool

  - Virtual server assigned address pool
  - Global range of addresses

- Only contiguous subnet masks can be used in assigning address ranges. However, a subset of an assigned range might be further assigned to a lower-level entity.
  A bound global address range can have a range bound to the following:

  - Virtual server
  - Group
  - User

- A bound virtual server address range can have a subset bound to the following:

  - Group
  - User

A bound group address range can have a subset bound to a user.

When an IP address is assigned to a user, the address is reserved for the user's next logon until the address pool range is exhausted. When the addresses are exhausted, NetScaler Gateway reclaims the IP address from the user who is logged off from NetScaler Gateway the longest.

If an address cannot be reclaimed and all addresses are actively in use, NetScaler Gateway does not allow the user to log on. You can prevent this situation by allowing NetScaler Gateway to use the mapped IP address as an intranet IP address when all other IP addresses are unavailable.

Intranet IP DNS registration

If an intranet IP is allotted to a client machine and after VIP tunnel establishment, the VPN plug-in checks if that client machine is domain joined. If the client machine is a domain-joined machine, the VPN plug-in initiates the DNS registration process to tie the machine's host name intranet with the allotted intranet IP address. This registration is reverted before tunnel de-establishment.

For successful DNS registration, make sure that the following `nsapimgr` knobs are set. Also make sure that the authoritative DNS server is set to allow "non-secure"DNS updates.

- **`nsapimgr` -ys enable_vpn_dns_override=1**: This flag is sent to the NetScaler Gateway VPN client along with the other configuration parameters. If this flag is unset and when the VPN client intercepts a DNS/WINS request, it sends a corresponding "GET /DNS"HTTP request to the NetScaler Gateway virtual server over the tunnel to get the resolved IP address. However, if the 'enable_vpn_dnstruncate_fix'flag is set, the VPN client forwards the DNS/WINS requests transparently to the NetScaler Gateway virtual server. In this case, the DNS packet is sent as is to the NetScaler Gateway virtual server over the VPN tunnel. This helps in cases when the DNS records coming back from the name servers configured in the NetScaler Gateway are huge and

do not fit in the UPD response packet. In this case, when the client falls back to using TCP-DNS, this TCP-DNS packet reaches NetScaler Gateway server as is, and hence the NetScaler Gateway server makes a TCP-DNS query to a DNS server.

- **nsapimgr -ys enable_vpn_dnstruncate_fix=1**: This flag is used by the NetScaler Gateway server itself. If this flag is set, NetScaler Gateway overrides the destination for the "TCP-connections on DNS-port"to the DNS servers configured on NetScaler Gateway (instead of trying to send them to the DNS-server-IP originally present in the incoming TCP-DNS packet). For UDP DNS requests, the default is to use the configured DNS servers for DNS resolution. NetScaler Gateway plug-in for Windows supports both secure and non-secure DNS updates. Secure DNS update supports exists by default in 21.7.1.1 or higher builds.

  Secure DNS update on the Windows plug-in is disabled, by default. To enable it, create a value of type REG_DWORD in `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access` and set it to 1.

  - When you set the value to 1, the VPN plug-in tries the unsecure DNS update first. If the unsecure DNS update fails, the VPN plug-in tries the secure DNS update.
  - To try only the secure DNS update, you can set the value to 2.

For more information on setting these knobs, see https://support.citrix.com/article/CTX200243.

Configure address pools for a user, group, or virtual server

1. In the configuration utility, in the navigation pane, expand **NetScaler Gateway**, do one of the following:
   - Expand NetScaler Gateway User Administration and then click **AAA Users**.
   - Expand **NetScaler Gateway** > **User Administration** and then click **AAA Groups**.
   - Expand **NetScaler Gateway** and then click **Virtual Servers**.
2. In the details pane, click a user, group, or virtual server and then click **Open**.
3. On the **Intranet IPs** tab, in IP Address and Netmask, type the IP address and subnet mask and then click **Add**.
4. Repeat Step 3 for each IP address that you want to add to the pool and then click **OK**.

Configure address pools globally

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, expand **NetScaler Gateway** and then click **Global Settings**.
2. In the details pane, under **Intranet IPs**, click To assign a unique, static IP Address or pool of IP Addresses for use by all client NetScaler Gateway sessions, configure Intranet IPs.

3. In the **Bind Intranet IPs** dialog box, click **Action,** and then click **Insert**.
4. In IP Address and Netmask, type the IP address and subnet mask and then click **Add**.
5. Repeat Step 3 and 4 for each IP address that you want to add to the pool and then click **OK**.

Define address pool options

You can use a session policy or the global NetScaler Gateway settings to control whether intranet IP addresses are assigned during a user session. Defining address pool options allows you to assign intranet IP addresses to NetScaler Gateway, while disabling the use of intranet IP addresses for a particular group of users.

You can configure address pools by using a session policy in one of the following three ways:

- `Nospillover` - When you configure address pools for intranet IP address, you get a session with an available IP from the pool. For users who have used all available intranet IP addresses, the Transfer Logon page appears.
- **Spillover** - When you configure address pools and the mapped IP is used as an intranet IP address, the mapped IP address is used for users who have used all available intranet IP addresses.
- **Off** - Address pools are not configured.

> **Note:**
>
> If the mapped IP address is not configured then SNIP is used.

To define address pools

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, expand **NetScaler Gateway > Policies,** and then click **Session**.
2. In the details pane, on the **Policies** tab, click **Add**.
3. In **Name**, type a name for the policy.
4. Next to **Request Profile**, click **New**.
5. In Name, type a name for the profile.
6. On the **Network Configuration** tab, click **Advanced**.
7. Next to Intranet IP, click **Override Global** and then select an option.
8. If you select **SPILLOVER** in Step 9, next to Mapped IP, click **Override Global**, select the host name of the appliance, click **OK,** and then click **Create**.
9. In the **Create Session Policy** dialog box, create an expression. Click **Create,** and then click **Close**.

Configure the Transfer Logon page

If a user does not have an intranet IP address available and then tries to establish another session with NetScaler Gateway, the Transfer Logon page appears. The Transfer Logon page allows users to replace their existing NetScaler Gateway session with a new session.

The Transfer Logon page can also be used if the logoff request is lost or if the user does not perform a clean logoff. For example:

- A user is assigned a static intranet IP address and has an existing NetScaler Gateway session. If the user tries to establish a second session from a different device, the Transfer Logon page appears and the user can transfer the session to the new device.
- A user is assigned five intranet IP addresses and has five sessions through NetScaler Gateway. If the user tries to establish a sixth session, the Transfer Logon page appears and the user can choose to replace an existing session with a new session.

> **Notes:**
>
> - If the user does not have an assigned IP address available because of which a new session cannot be established, an error message appears.
> - Citrix Secure Access for Android 23.12.1 and later versions support the Transfer Logon functionality of NetScaler Gateway in the Always On VPN mode.

The Transfer Logon page appears only if you configure address pools and disable spillover.

Configure a DNS suffix

When a user logs on to NetScaler Gateway and is assigned an IP address, a DNS record for the user name and IP address combination is added to the NetScaler Gateway DNS cache. You can configure a DNS suffix to append to the user name when the DNS record is added to the cache. This allows users to be referenced by the DNS name, which can be easier to remember than an IP address. When the user logs off from NetScaler Gateway, the record is removed from the DNS cache.

To configure a DNS suffix

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, expand **NetScaler Gateway > Policies,** and then click **Session**.
2. In the details pane, on the **Policies** tab, select a session policy and then click **Open**.
3. Next to Request Profile, click **Modify**.
4. On the **Network Configuration** tab, click **Advanced**.
5. Next to Intranet IP DNS Suffix, click **Override Global**, type the DNS suffix and then click **OK** three times.

Support for VoIP phones

May 2, 2024

When you install NetScaler Gateway as a standalone appliance and users connect with the Citrix Secure Access client, NetScaler Gateway supports two-way communication with Voice over IP (VoIP) softphones.

Following are some of the VoIP softphones that Citrix Secure Access supports:

- Cisco Softphone
- Avaya IP Softphone

Secure tunneling is supported between the IP PBX and the softphone software running on the user device. To enable the VoIP traffic to traverse the secure tunnel, you must install the Citrix Secure Access client and one of the supported softphones on the same user device.

When the VoIP traffic is sent over the secure tunnel, Citrix Secure Access supports the following softphone features:

- Outgoing calls that are placed from the IP softphone
- Incoming calls that are placed to the IP softphone
- Bidirectional voice traffic
- TCP and UDP control flows with VoIP applications

> **Note:**
>
> For the UDP control flow with DNE, the VoIP application gets disconnected if the inactivity duration is 30 seconds or more. So, if the VoIP application supports UDP control messaging and you face any issues, we recommend you to use Citrix Secure Access in WFP mode.

Support for VoIP softphones is configured by using intranet IP addresses. You must configure an intranet IP address for each user. If you are using Cisco Softphone Communication, after configuring the intranet IP address and binding it to a user, no additional configuration is required. For more information about configuring an intranet IP address, see Configuring Address Pools.

If you enable split tunneling, create an intranet application and specify the Avaya Softphone application. In addition, you must enable transparent interception.

Configure Access Interface

January 8, 2024

NetScaler Gateway includes a default home page that appears after users log on. The default home page is called the Access Interface. You use the Access Interface as the home page, or configure the Web Interface as the home page, or a custom home page.

The Access Interface contains three panels. If you have the Web Interface in your deployment, users can log on to Receiver in the left panel of the Access Interface. If you have StoreFront in your deployment, users cannot log on to Receiver from the left panel.

The Access Interface is used to provide links to websites, both internal and external, and links to file shares in the internal network. You can customize the Access Interface in the following ways:

- Changing the Access Interface.
- Creating Access Interface links.

Users can customize the Access Interface as well by adding their own links to websites and file shares. Users can also use the home page to transfer files from the internal network to their device.

> **Note:**
>
> When users log on and attempt to open file shares from the Access Interface, the file share does not open and users receive the error message "Failed to make TCP connection to the server."To resolve this problem, configure your firewall to allow traffic from the NetScaler Gateway system IP address to the file server IP address on TCP ports 445 and 139.

Change the Access Interface

You might want to direct users to a customized home page, rather than relying on the Access Interface. To do this, install the home page on NetScaler Gateway and then configure the session policy to use the new home page.

To install a customized home page

1. In the configuration utility, click the **Configuration** tab and then in the navigation pane, click **NetScaler Gateway.**
2. In the details pane, under **Customize Access Interface**, click **Upload** the **Access Interface.**
3. To install the home page from a file on a computer in your network, in Local File, click **Browse**, navigate to the file, and then click **Select.**
4. To use a home page that is installed on NetScaler Gateway, in Remote Path, click **Browse**, select the file, and then click **Select.**
5. Click **Upload** and then click **Close.**

Replace the Access Interface with a custom home page

You can use either global settings or a session policy and profile to configure a custom home page to replace the default home page, the Access Interface. After you configure the policy, you can bind the policy to a user, group, virtual server, or globally. When you configure a custom home page, the Access Interface does not appear when users log on.

Configure custom home page globally

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, expand **NetScaler Gateway** and then click **Global Settings.**
2. In the details pane, under **Settings**, click Change global settings.
3. On the **Client Experience** tab, in **Home Page**, click **Display Home Page,** and then enter the web address of your custom home page.
4. Click **OK** and then click **Close.**

Configure a custom home page in a session profile

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, expand **NetScaler Gateway Policies** and then click **Session.**
2. In the details pane, on the **Policies** tab, click **Add.**
3. In Name, type a name for the policy.
4. Next to **Request Profile**, click **New.**
5. In **Name**, type a name for the profile.
6. On the **Client Experience** tab, next to **Home Page**, click **Override Global**, click **Display Home Page,** and then type the web address of the home page.
7. In the **Create Session Policy** dialog box, next to **Named Expressions**, select **General**, select True value, click **Add Expression**, click **Create,** and then click **Close.**

Create and apply web links

January 8, 2024

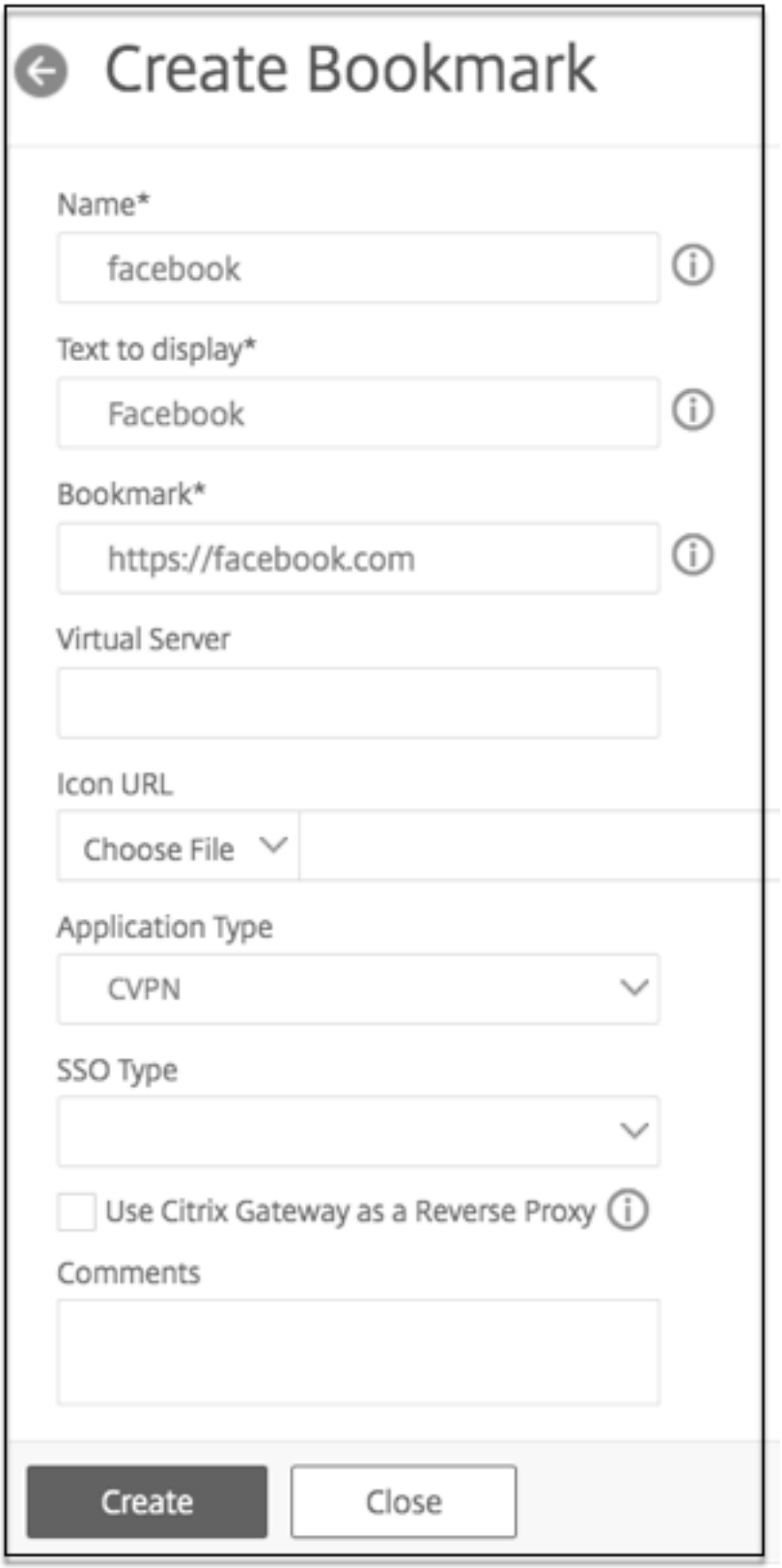
You can configure the Access Interface to display a set of links to internal resources that are available to users. Creating these links requires that you first define the links as resources. Then, you bind them to a user, group, virtual server, or globally to make them active in the Access Interface. The links you create appear on the **Web Sites** panes under **Enterprise Web Sites**.

> **Important:**
>
> From NetScaler release 13.0 build 64.xx onwards, file shares through NetScaler Gateway are not supported.

Creating Enterprise bookmarks

To create an Access Interface link in a session policy

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, expand **NetScaler Gateway > Resources** and then click **Portal Bookmarks.**
2. In the details pane, click **Add.**



3. In **Name**, type a name for the bookmark.

4. In **Text to display**, type the description of the link. The description appears in the **Access Interface.**
5. In **Bookmark**, type the web address of the application.
6. In **Virtual Server**, type the name of the associated load balancing/content switching virtual server. This field is optional.
7. In **Icon URL**, the icons uploaded are supported for all themes except the default theme. Maximum recommended size is 70x70 pixels. We recommend that you use transparent images. This field is optional.
8. In **Application Type**, select the type of application (VPN, clientless VPN, or SaaS) that the URL represents. This field is optional.
9. In **SSO Type**, select the SSO type that you want to configure for the bookmark. When SSO is configured, users can access the applications without having to enter their credentials in the subsequent logons. The following SSO types are supported:

   - Unified Gateway: This SSO configuration allows secure remote access to multiple resources of an application through a single URL.
   - Self-authentication: In this SSO configuration, NetScaler Gateway users are prompted to provide the login credentials to access the application.
   - SAML-based authentication: In this SSO configuration, NetScaler Gateway uses an IdP to validate the user details, generates a SAML assertion, and sends it to the SP. If the validation passes, the SSO is successful.

   > **Note:**
   >
   > If you enable clientless access, you can make sure that requests to websites go through NetScaler Gateway. For example, you added a bookmark for Google. Select the **Use NetScaler Gateway as a reverse proxy** check box. When you select this check box, website requests go from the user device to NetScaler Gateway and then to the website. When you clear the check box, requests go from the user device to the website. This check box is only available if you enable clientless access.

10. Click **Create** and then click **Close.**

To bind an Access Interface link

You can bind Access Interface links to the following locations:

- Users
- Groups
- Virtual servers

After you save the configuration, the links are available to users in the Access Interface on the **Home** tab, which is the first page that users see after they successfully log on.

1. In the configuration utility, in the navigation pane, do one of the following:
   - Expand **NetScaler Gateway User Administration** and then click **AAA Users.**
   - Expand **NetScaler Gateway User Administration** and then click **AAA Grpups.**
   - Expand **NetScaler Gateway** and then click **Virtual Servers.**
2. In the details pane, do one of the following:
   - Select a user and then click Open.
   - Select a group and then click Open.
   - Select a virtual server and then click Open.
3. In the dialog box, click the **Bookmarks** tab.
4. Under **Available Bookmarks**, select one or more bookmarks, click the right arrow to move the bookmarks under Configured Bookmarks and then **OK.**

To bind bookmarks globally by using the GUI

1. On the **Configuration** tab, in the navigation pane, expand **NetScaler Gateway** and then click **Global Settings.**
2. In the details pane, under **Bookmarks**, click **Create links to the HTTP and Windows File Share applications that you want to make accessible on the NetScaler Gateway portal page**.

3. In the **Configure VPN Global Binding*** dialog box, click **Add.**

4. Under **Available**, select one or more bookmarks, click the right arrow to move the bookmarks under Configured and then **OK**.

To add an Enterprise bookmark by using the CLI

At the command prompt, type:

```
add vpn url <urlName> <linkName> <actualURL>  [-ssotype <ssotype>]
```

Example:

Web bookmark

```
add vpn url google google "https://www.google.com"
```

To bind an Enterprise bookmark by using the CLI

You can bind Enterprise bookmarks to user, group, virtual server, and global level.

```
bind aaa user <userName> -urlName <string>
bind aaa group <groupName> -urlName <string>
bind vpn vserver <vserverName> -urlName <string>
bind vpn global – urlName <string>
```

Example:

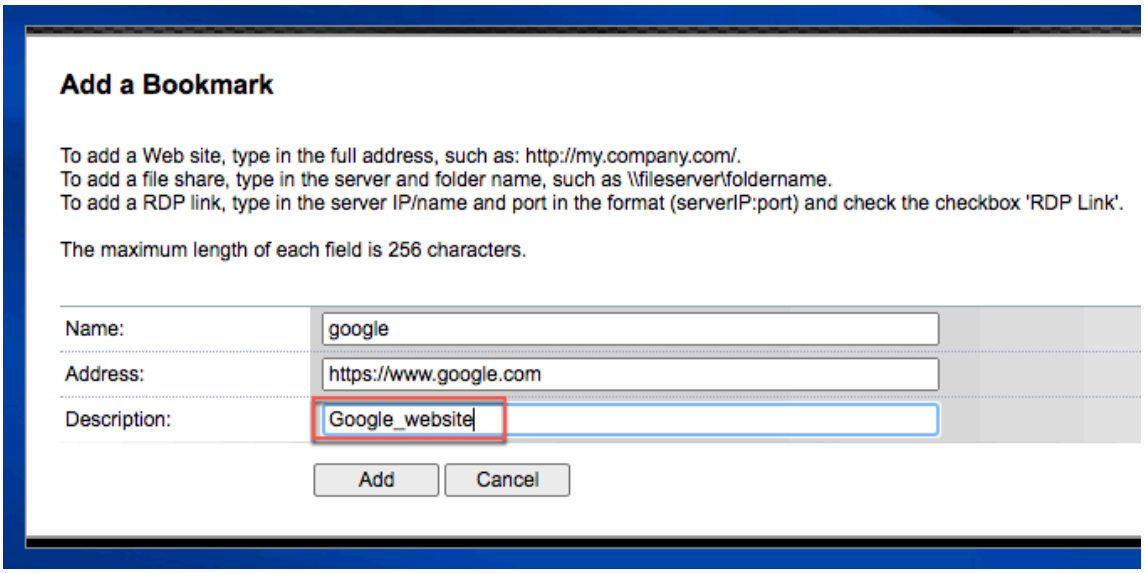
```
bind vpn global -urlName google
```

Creating Personal Bookmarks

You can create personal websites from the VPN virtual server only. There is no NetScaler Gateway admin GUI for adding personal bookmarks.

1. Log on to a VPN virtual server.
2. Click **Network Access** or **Clientless Access** to add a bookmark.
3. Click **Add**.

4. Enter the bookmark details such as website name, address, and description.



5. Click **Add**.

The websites that you added appear under the respective tabs.

Configure user name tokens in bookmarks

You can configure bookmark and file share URLs using a special token, %`username`%. When users log on, the token is replaced with each users' logon name. For example, you create a bookmark for an employee named Jack for a folder as \\EmployeeServer\%`username`%\. When Jack logs on, the file share URL is mapped to \\EmployeeServer\Jack\. When you configure user name tokens in bookmarks, keep the following situations in mind:

- If you are using one authentication type, the user name replaces the token %`username`%.
- If you are using two-factor authentication, the user name from the primary authentication type is used to replace the %`username`% token.
- If you are using client certificate authentication, the user name field in the client certificate authentication profile is used to replace the %`username`% token.

Traffic policies

January 8, 2024

Traffic policies allow you to configure the following settings for user connections:

- Enforcing shorter time-outs for sensitive applications that are accessed from untrusted networks.
- Switching network traffic to use TCP for some applications. If you select TCP, you must enable or disable single sign-on for certain applications.
- Identifying situations where you want to use other HTTP features for Citrix Secure Access client traffic.
- Defining the file name extensions that are used with file type association.

Create a traffic policy

To configure a traffic policy, you create a profile and configure the following parameters:

- Protocol (HTTP or TCP)
- Application time-out
- Single sign-on to web applications
- Form single sign-on
- File type association
- Repeater plug-in
- Kerberos Constrained Delegated (KCD) accounts

After you create the traffic policy, you can bind the policy to virtual servers, users, groups, or globally.

For example, you have the web application PeopleSoft Human Resources installed on a server in the internal network. You can create a traffic policy for this application that defines the destination IP address, the destination port, and you can set the amount of time a user can stay logged on to the application, such as 15 minutes.

If you want to configure other features, such as HTTP compression to an application, you can use a traffic policy to configure the settings. When you create the policy, use the HTTP parameter for the action. In the expression, create the destination address for the server running the application.

Sample traffic policy expressions

Following are the expression examples of traffic policies:

- `add vpn trafficPolicy trafPol1 "HTTP.REQ.URL.CONTAINS(\"/Citrix/\")|| HTTP.REQ.URL.CONTAINS(\"10.102.\")")"trafAct1`
- `add vpn trafficPolicy trafPol2 "HTTP.REQ.HOSTNAME.CONTAINS(\"portal-srv\")|| HTTP.REQ.URL.CONTAINS(\"homePage\"))"trafAct2`
- `add vpn trafficPolicy trafPol3 true trafAct3`

Configure a traffic policy by using the GUI

1. Expand **NetScaler Gateway > Policies** and then click **Traffic**.
2. In the details pane, on the **Policies** tab, click **Add**.
3. In the **Create Traffic Policy** dialog box, in **Name**, type a name for the policy.
4. Next to **Request Profile**, click **New**.
5. In **Name**, type a name for the profile.
6. In **Protocol**, select either **HTTP** or **TCP**.

   Note: If you select TCP as the protocol, you cannot configure single sign-on and the setting is disabled in the profile dialog box.
7. In **AppTimeout (minutes)**, type the number of minutes. This setting limits the time users can stay logged on to the web application.
8. To enable single sign-on to the web application, in **Single Sign-On**, select **ON**.

   Note: If you want to use form-based single sign-on, you can configure the settings within the traffic profile. For more information, see Configuring Form-Based Single Sign-On.
9. To specify a file type association, in **File Type Association**, select **ON**.
10. To use the repeater plug-in to optimize network traffic, in Citrix SD-WAN, select **ON**, click **Create**, and then click **Close**.
11. If you configure KCD on the appliance, in KCD Account, select the account.

    For more information about configure KCD on the appliance, see Configuring Kerberos Constrained Delegation on a NetScaler Appliance.
12. In the Create Traffic Policy dialog box, create or add an expression, click **Create,** and then click **Close**.

Configure form-based single sign-on

Form-based single sign-on allows users to log on one time to all protected applications in your network. When you configure form-based single sign-on in NetScaler Gateway, users can access web applications that require an HTML form-based logon without having to type their password again. Without single sign-on, users are required to log on separately to access each application.

After creating the form single sign-on profile, you then create a traffic profile and policy that includes the form single sign-on profile. For more information, see Creating a Traffic Policy.

Configure form-based single sign-on

1. Expand **NetScaler Gateway > Policies,** and then click **Traffic**.
2. In the details pane, click the **Form SSO Profiles** tab and then click **Add**.
3. In **Name**, type a name for the profile.
4. In **Action URL**, type the URL to which the completed form is submitted.

   Note: The URL is the root relative URL.
5. In **User Name**, type the name of the attribute for the user name field.
6. In **Password**, type the name of the attribute for the password field.
7. In **SSO Success Rule**, create an expression that describes the action that this profile takes when invoked by a policy. You can also create the expression by using the Prefix, Add, and Operator buttons under this field.

   This rule checks if the single sign-on is successful or not.
8. In **Name Value Pair**, type the user name field value, followed by an ampersand (&), and then the password field value.

   Value names are separated by an ampersand (&), such as name1=value1&name2=value2.
9. In **Response Size**, type the number bytes to allow for the complete response size. Type the number of bytes in the response to be parsed for extracting the forms.
10. In **Extraction**, select if the name/value pair is static or dynamic. The default setting is Dynamic.
11. In **Submit Method**, select the HTTP method used by the single sign-on form to send the logon credentials to the logon server. The default is Get.
12. Click **Create,** and then click **Close**.

Configure SAML single sign-on

You can create a SAML 1.1 or SAML 2.0 profile for single sign-on (SSO). Users can connect to web applications that support the SAML protocol for single sign-on. NetScaler Gateway supports the identity provider (IdP) single sign-on for SAML web applications.

Configure SAML single sign-on

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway \ > Policies** and then click Traffic.
2. In the details pane, click the SAML SSO Profile tab.
3. In the details pane, click Add.
4. In Name, type a name for the profile.
5. In Signing Certificate Name, enter the name of the X.509 certificate.
6. In ACS URL, enter the assertion consumer service of the identity provider or service provider. The AssertionConsumerServiceURL (ACS URL) provides SSO capability for users.
7. In Relay State Rule, build the expression for the policy from Saved Policy Expressions and Frequently Used Expressions. Select from the Operator list to define how the expression is evaluated. To test the expression, click Evaluate.
8. In Send Password select ON or OFF.
9. In Issuer Name enter the identity for the SAML application.
10. Click Create and then click Close.

Bind a traffic policy

You can bind traffic policies to virtual servers, groups, users, and to NetScaler Gateway Global. You can use the configuration utility to bind a traffic policy.

Bind a traffic policy globally by using the GUI

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway > Policies** and then click Traffic.
2. In the details pane, select a policy and then in Action, click Global Bindings.
3. In the Bind / Unbind Traffic Policies dialog box, under Details, click Insert Policy.
4. Under Policy Name, select the policy and then click OK.

Remove traffic Policies

You can use either the configuration utility to remove traffic policies from NetScaler Gateway. If you use the configuration utility to remove a traffic policy and the policy is bound to the user, group, or virtual server level, you must first unbind the policy. Then, you can remove the policy.

Unbind a traffic policy by using the GUI

1. Expand **NetScaler Gateway,** and then click **Virtual Servers**.
   - **Expand NetScaler Gateway > User Administration** and then click **AAA Groups**.
   - Expand **NetScaler Gateway > User Administration** and then click **AAA Users**.
2. In the details pane, select a virtual server, group, or user and then click **Open**.
3. In the **Configure NetScaler Gateway Virtual Server, Configure AAA Group**, or **Configure AAA User** dialog box, click the **Policies** tab.
4. Click **Traffic**, select the policy, and then click **Unbind Policy**.
5. Click **OK,** and then click **Close**.

After the traffic policy is unbound, you can remove the policy.

Remove a traffic policy by using the GUI

1. Expand **NetScaler Gateway > Policies**, and then click **Traffic**.
2. In the details pane, on the Policies tab, select the traffic policy, and then click **Remove**.

Session policies

January 8, 2024

A session policy is a collection of expressions and settings that are applied to users, groups, virtual servers, and globally.

You use a session policy to configure the settings for user connections. You can define settings to configure the software users log on with, such as the Citrix Secure Access client for Windows or the Citrix Secure Access client for Mac. You can also configure settings to require users to log on with Citrix Workspace app or Secure Hub. Session policies are evaluated and applied after the user is authenticated.

Session policies are applied according to the following rules:

- Session policies always override global settings in the configuration.
- Any attributes or parameters that are not set using a session policy are set on policies established for the virtual server.
- Any other attributes that are not set by a session policy or by the virtual server are set by the global configuration.

> **Important:**
>
> The following instructions are general guidelines for creating session policies. There are specific instructions for configuring session policies for different configurations, such as clientless access or for access to published applications. The instructions might contain directions for configuring a specific setting. However, that setting can be one of many settings that are contained within a session profile and policy. The instructions direct you to create a setting within a session profile and then apply the profile to a session policy. You can change settings within a profile and policy without creating a session policy. In addition, you can create all of your settings on a global level and then create a session policy to override global settings.

If you deploy Citrix Endpoint Management or StoreFront in your network, Citrix recommends using the Quick Configuration wizard to configure session policies and profiles. When you run the wizard, you define the settings for your deployment. NetScaler Gateway then creates the required authentication, session, and clientless access policies.

Create a session policy

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway > Policies and then click Session.
2. In the details pane, on the Policies tab, click Add.
3. In Name, type a name for the policy.
4. Next to Request Profile, click New.
5. In Name, type a name for the profile.
6. Complete the settings for the session profile and then click Create.
7. In the Create Session Profile dialog box, add an expression for the policy, click Create and then click Close.
   Note: In the expression, select
   True value so the policy is always applied to the level to which it is bound.

Sample session policy expressions

Following are the expression examples of session policies:

- `add vpn sessionPolicy sessPol1 "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\")|| HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixWorkspace\")"sessAct1`
- `add vpn sessionPolicy sessPol2 "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT"sessAct2`
- `add vpn sessionPolicy sessPol3 true sessAct3`

Bind session policies

After you create a session policy, bind it to a user, group, virtual server, or globally. Session policies are applied as a hierarchy in the following order:

- Users
- Groups
- Virtual servers
- Globally

Bind a session policy to a virtual server by using the GUI

1. Navigate to **NetScaler Gateway > Virtual Servers**.
2. Select a virtual server and click **Edit**. You can also create a new virtual server.
3. Scroll down to the **Policies** section, and click the **+** icon.
4. In **Choose Policy**, select **Session**.
5. In **Choose Type**, select **Request**, and click **Continue**.
6. In **Select Policy**, select the policy that you want to bind to this virtual server.
7. In **Priority**, enter the priority number of the policy.
8. Click **Bind**.

Bind a session policy to an authentication, authorization, and auditing group by using the GUI

1. Navigate to **NetScaler Gateway > User Administration > AAA Groups**.
2. Select an existing authentication, authorization, and auditing group, and click **Edit**. You can also create an authentication, authorization, and auditing group.
3. In **Advanced Settings**, click **Policies,** and then click the **+** icon.
4. In **Choose Policy**, select **Session**, and click **Continue**.
5. In **Select Policy**, select the policy that you want to bind to this authentication, authorization, and auditing group.
6. In **Priority**, enter the priority number of the policy.
7. Click **Bind**.

Bind a session policy to an authentication, authorization, and auditing user by using the GUI

1. Navigate to **NetScaler Gateway > User Administration > AAA Users**.
2. Select an existing NetScaler user, and click **Edit**. You can also create an authentication, authorization, and auditing user.
3. In **Advanced Settings**, click **Policies,** and then click the **+** icon.
4. In **Choose Policy**, select **Session**, and click **Continue**.
5. In **Select Policy**, select the policy that you want to bind to this authentication, authorization, and auditing user.
6. In **Priority**, enter the priority number of the policy.
7. Click **Bind**.

Note: For details on priority, see https://support.citrix.com/article/CTX214588.

Create a session profile

A session profile contains the settings for user connections.

Session profiles specify the actions that are applied to a user session if the user device meets the policy expression conditions. Profiles are used with session policies. You can use the configuration utility to create session profiles separately from a session policy and then use the profile for multiple policies. You can only use one profile with a policy.

Configure network settings for user connections in a session profile

You can use the **Network Configuration** tab in the session profile to configure the following network settings for user connections:

- DNS server
- WINS server IP address
- Mapped IP address that you can use as an intranet IP address
- Spillover settings for address pools (intranet IP addresses)
- Intranet IP DNS suffix
- HTTP ports
- Forced time-out settings

Configure connection settings in a session profile

You can use the **Client Experience** tab in the session profile to configure the following connection settings:

- Access Interface or customized home page
- Web address for web-based email, such as Outlook Web Access
- plug-in type (Citrix Secure Access client for Windows, or Citrix Secure Access client for macOS X)
- Split tunneling
- Session and idle time-out settings
- Clientless access
- Clientless access URL encoding
- plug-in type (Windows, or Mac)
- Single sign-on to web applications
- Credential index for authentication
- Single sign-on with Windows
- Client cleanup behavior
- Logon scripts
- Client debug settings
- Split DNS
- Access to private network IP addresses and local LAN access
- Client choices
- Proxy settings

For more information about configuring settings for user connections, see Configuring Connections for the Citrix Secure Access client.

Configure security settings in a session profile

You can use the **Security** tab in a session profile to configure the following security settings:

- Default authorization action (allow or deny)
- Secure Browse for connections from iOS devices
- Quarantine groups
- Authorization groups

For more information about configuring authorization on NetScaler Gateway, see Configuring Authorization.

Configure Citrix Virtual Apps and Desktops settings in a session profile

You can use the **Published Applications** tab in a session profile to configure the following settings for connections to servers running Citrix Virtual Apps and Desktops:

- ICA Proxy, which is client connections using Citrix Workspace app

- Web Interface address
- Web Interface portal mode
- Single sign-on to the server farm domain
- Citrix Workspace app home page
- Account Services Address

For more information about configuring settings for connecting to published applications in a server farm, see Providing Access to Published Applications and Virtual Desktops Through the Web Interface.

You can create session profiles independently of a session policy. When you create the policy, you can select the profile to attach to the policy.

To create a session profile by using the GUI

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway > Policies,** and then click **Session**.
2. In the details pane, click the **Profiles** tab, and then click **Add**.
3. Configure the settings for the profile, click **Create,** and then click **Close**.

After you create a profile, you can include it in a session policy.

To add a profile to a session policy by using the GUI

1. In the configuration utility, in the navigation pane, expand **Access Gateway > Policies** and then click **Session**.
2. On the **Policies** tab, do one of the following:
   - Click **Add** to create a session policy.
   - Select a policy, and then click **Open**.
3. In **Request Profile**, select a profile from the list.
4. Finish configuring the session policy, and then do one of the following:
   a) Click **Create,** and then click **Close** to create the policy.
   b) Click **OK,** and then click **Close** to modify the policy.

Advanced policy support for enterprise bookmarks

January 8, 2024

Enterprise bookmarks (VPN URLs) can be configured as advanced policies.

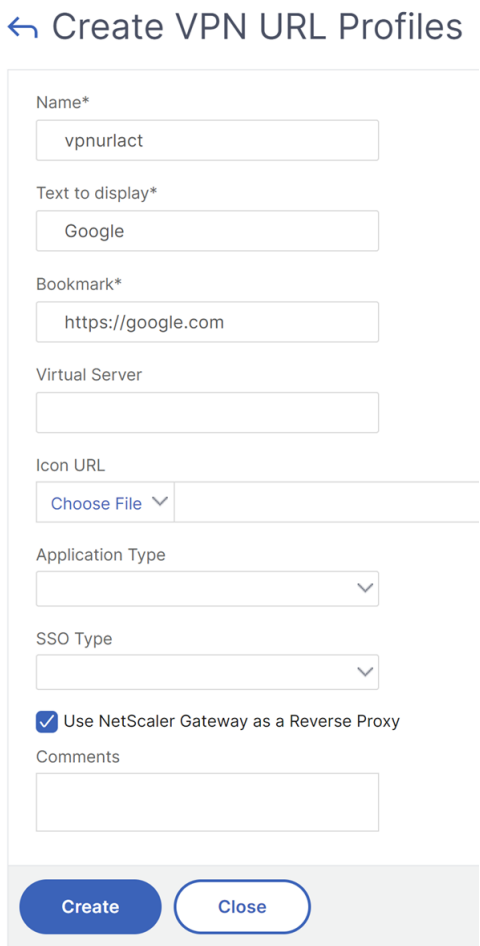
> **Notes:**
>
> - NetScaler Gateway supports HTTP, HTTPs, and RDP protocols for the enterprise bookmarks.
> - NetScaler Gateway supports only absolute URLs for the enterprise bookmarks.

Configure VPN URL as an advanced policy

On the GUI

1. Create a VPN URL Profile.
   - Navigate to **Configuration > NetScaler Gateway > Policies > VPN URL**.
   - On the **VPN URL Policies and Profiles** page, select the **VPN URL Profiles** tab and click **Add**.
   - Update the required fields and click **Create**.
     - Name: A name for the VPN URL profile.
     - Text to display: A brief description of the link. The description appears on the access interface.
     - Bookmark: Web address of the application.
     - Virtual Server: Name of the associated load balancing or content switching virtual server that is configured. This field is optional.
     - Icon URL: The icons uploaded in this field are supported for all themes except the default theme. Maximum recommended size is 70x70 pixels. We recommend that you use transparent images. This field is optional.
     - Application Type: select the type of application (VPN, clientless VPN, or SaaS) that the URL represents. This field is optional.
     - SSO Type: SSO type that you want to configure for the bookmark. When SSO is configured, users can access the applications without having to enter their credentials in the subsequent logons. The following SSO types are supported:
       * Unified Gateway: This SSO configuration allows secure remote access to multiple resources of an application through a single URL.
       * Self-authentication: In this SSO configuration, NetScaler Gateway users are prompted to provide the login credentials to access the application.
       * SAML-based authentication: In this SSO configuration, NetScaler Gateway uses an IdP to validate the user details, generates a SAML assertion, and sends it to the SP. If the validation passes, the SSO is successful.

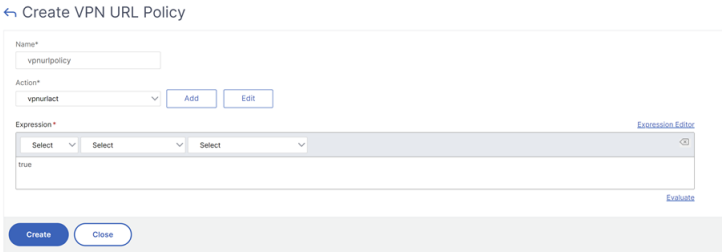
> **Note:**
>
> If you enable clientless access, you can make sure that requests to websites go through NetScaler Gateway. For example, you added a bookmark for Google. Select the Use NetScaler Gateway as a reverse proxy check box. When you select this check box, website requests go from the user device to NetScaler Gateway and then to the website. When you clear the check box, requests go from the user device to the website. This check box is only available if you enable clientless access.



2. Create a VPN URL Policy.

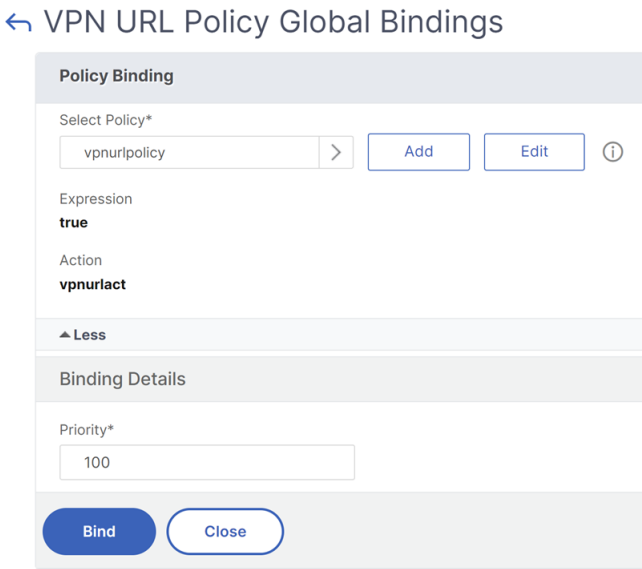
   - Navigate to **Configuration > NetScaler Gateway > Policies > VPN URL**.
   - On the **VPN URL Policies and Profiles** page, select the **VPN URL Policy** tab and click **Add**.
   - Update the required fields and click **Create**.
     - Name: A name for the VPN URL policy.
     - Action: Select the configured VPN URL profile. If there is no profile on the drop-down list, click Add and repeat step 1.

- Expression: Refer to Policies and expressions for information about the advanced policy expressions.



3. Bind the VPN URL policy to a bind point.

   - Navigate to **Configuration > NetScaler Gateway > Policies > VPN URL**.
   - On the **VPN URL Policies and Profiles** page, select the **VPN URL Policy** tab.
   - Select **Global Bindings** from the **Select Action** drop-down list.
   - Select the VPN URL policy. If there is no policy listed, click **Add** and repeat step 2.
   - In the **Binding Details** section, assign a priority to the VPN URL policy.



On the CLI

Create a VPN URL action:

At the command prompt, type the following:

```
add vpn urlAction <name> -linkName <string> -actualURL <string> \[-vServerName <string>] \[-clientlessAccess \( ON | OFF )] \[-comment <string>] \[-iconURL <URL>] \[-ssotype <ssotype>] \[-applicationtype <applicationtype>] \[-samlSSOProfile <string>]
```


NetScaler Gateway supports the following operations for VPN URL action:

- **add**

```
add vpn urlAction <name> -linkName <string> -actualURL <string>
    \[-vServerName <string>] \[-clientlessAccess \( ON | OFF )]
    \[-comment <string>] \[-iconURL <URL>] \[-ssotype <ssotype>]
    \[-applicationtype <applicationtype>] \[-samlSSOProfile <
    string>]
```

- **set**

```
set vpn urlAction <name> \[-vServerName <string>] \[-
    clientlessAccess \( ON | OFF )] \[-comment <string>] \[-
    iconURL <URL>] \[-ssotype <ssotype>] \[-applicationtype <
    applicationtype>] \[-samlSSOProfile <string>]
```

- **unset**

```
unset vpn urlAction <name> [-vServerName] [-clientlessAccess] [-
    comment] [-iconURL] [-ssotype] [-applicationtype] [-
    samlSSOProfile]
```

> **Note:**
>
> If you set clientless access to ON, you can make sure that requests to websites go from the user device to NetScaler Gateway and then to the website.

- **show**

```
show vpn urlAction [<name>]
```

- **remove**

```
remove vpn urlAction <name>
```

- **rename**

```
rename vpn urlAction <name>@ <newName>@
```

Create a VPN URL policy:

NetScaler Gateway supports the following operations for VPN URL policy:

- **add**

```
add vpn urlPolicy <name> -rule <expression> -action <string> [-
    comment <string>] [-logAction <string>]
```

- **set**


```
set vpn urlPolicy <name> [-rule <expression>] [-action <string>]
    [-comment <string>] [-logAction <string>]
```

- **unset**

```
unset vpn urlPolicy <name> [-comment] [-logAction]
```

- **show**

```
show vpn urlPolicy [<name>]
```

- **remove**

```
remove vpn urlPolicy <name>
```

- **rename**

```
rename vpn urlpolicy <name>@ <newName>@
```

- **stat**

```
stat vpn urlpolicy \[<name>] \[-detail] \[-fullValues] \[-ntimes
    <positive\_integer>] \[-logFile <input\_filename>] \[-
    clearstats \( basic | full )]
```

Bind the policy to a bind point:

NetScaler Gateway supports the following operations for VPN URL policy binding:

- **bind**

```
bind vpn vserver <vserver name> -policy <string> -priority <
    positive_integer> [-gotoPriorityExpression <expression>]
bind vpn global -policyName <string> -priority <positive_integer>
     [-gotoPriorityExpression <expression>]
bind aaa user <userName> -policy <string> [-priority <
    positive_integer>] [-type <type>] [-gotoPriorityExpression <
    expression>]
bind aaa group <groupName> -policy <string> [-priority <
    positive_integer>] [-type <type>] [-gotoPriorityExpression <
    expression>]
```

- **unbind**

```
unbind vpn vserver <name> -policy <string>
unbind vpn global -policyName <string>
unbind aaa user <name> -policy <string>
unbind aaa group <name> -policy <string>
```


> **Note:**
>
> Bind Points are `aaauser`, `aaagroup`, `vpnvserver`, and `vpnglobal`.

Endpoint policies

January 11, 2024

Endpoint Analysis (EPA) is a process that scans a user's device and detects information, such as the presence and version level of operating system updates, antivirus, firewall, and web browser software. Endpoint Analysis allows you to determine if a user's device meets your requirements before it connects to your network. It can also be configured to periodically check for any changes while the user remains connected. You can check files, processes, and registry entries on the user device during the user session to ensure that the device continues to meet the requirements.

> **Important:**
>
> - Endpoint Analysis is intended to analyze the user device against pre-determined compliance criteria and does not enforce or validate the security of end-user devices. It is recommended to use endpoint security systems to protect devices from local admin attacks.
> - The EPA client is available as a standalone client and is also bundled along with the Citrix Secure Access client. The Citrix EPA client and Citrix Secure Access client are independent from each other.

How Endpoint policies work

You can configure NetScaler Gateway to check if a user device meets certain requirements before a user logs on. This is called a pre-authentication policy. You can configure NetScaler Gateway to check a user device for antivirus, firewall, antispam, processes, files, registry entries, Internet security, or operating systems that you specify within the policy. If the user device fails the pre-authentication scan, users are not allowed to log on.

To verify other requirements that are not used in a pre-authentication policy, you can configure a session policy and bind it to a user or group. This type of policy is called a post-authentication policy, which runs during the user session to ensure the required criteria, such as antivirus software or a process, remains compliant.

When you configure a pre-authentication or post-authentication policy, NetScaler Gateway downloads the Endpoint Analysis plug-in and then runs the scan on the users'device. Each time a user logs on, the Endpoint Analysis plug-in runs automatically.

You can use the following three types of policies to configure endpoint policies:

- Preauthentication policy that uses a Yes or No parameter. The scan determines if the user device meets the specified requirements. If the scan fails, the user cannot enter credentials on the logon page.
- Session policy that is conditional and can be used for SmartAccess.
- Client device check expression within a session policy. If the user device fails to meet the requirements of the Client device check expression, you can configure users to be placed into a quarantine group. If the user device passes the scan, users can be placed into a different group that might require other checks.

You can incorporate the detected information into policies, enabling you to grant different levels of access based on the user device. For example, you can provide full access with download permission to users who connect remotely from user devices that have current antivirus and firewall software requirements. For users connecting from non-compliant devices, you can provide a more restricted level of access that allows users to edit documents on remote servers without downloading them. All devices running EPA are considered as non-compliant devices.

Endpoint Analysis performs the following basic steps:

- Examines an initial set of information about the user device to determine which scans to apply.
- Runs all applicable scans. When users try to connect, the Endpoint Analysis plug-in checks the user device for the requirements specified within the pre-authentication or session policy. If the user device passes the scan, users are allowed to log on. If the user device fails the scan, users are not allowed to log on.

  Note: Endpoint Analysis scans complete before the user session uses a license.
- Compares the property values detected on the user device with the desired property values listed in your configured scans.
- Produces an output verifying whether the desired property values are found.

> **Attention:**
>
> The instructions for creating Endpoint Analysis policies are general guidelines. You can have many settings within one session policy. Specific instructions for configuring session policies might contain directions for configuring a specific setting. However, that setting can be one of many settings that are contained within a session profile and policy.

Sample EPA expressions

Following are the expression examples of some EPA components such as kill process, delete files, and device certificate:

- Windows:
  - Kill process: `sys.client_expr(\“proc_0_perl\“)-killProcess processToKill.exe`
  - Device certificate :`sys.client_expr(“device-cert_0_0”)`
  - Delete files :`sys.client_expr(\“proc_0_perl\“)-deletefiles “C:/removefile.txt”`
- MAC
  - Kill process: `sys.client_expr(\“proc_0_perl\“)-killProcess processToKill.exe`
  - Device cert:`sys.client_expr(“device-cert_0_0”)`
  - Delete files:`sys.client_expr(\“proc_0_perl\“)-deletefiles “C:/removefile.txt”`

Evaluate user logon options

When users log on, they can choose to skip the Endpoint Analysis scan. If users skip the scan, NetScaler Gateway processes this action as a failed Endpoint Analysis. When users fail the scan, they only get access to the Web Interface or through clientless access.

For example, you want to provide users access by using the Citrix Secure Access client. To log on to NetScaler Gateway with the plug-in, users must be running an antivirus application, such as Norton Antivirus. If the user device is not running the application, users can log on with Receiver only and use published applications. You can also configure clientless access, which restricts access to specified applications, such as Outlook Web Access.

To configure NetScaler Gateway to achieve this logon scenario, you assign a restrictive session policy as the default policy. You then configure the settings to upgrade users to a privileged session policy when the user device passes the Endpoint Analysis scan. At that point, users have network layer access and can log on with the Citrix Secure Access client.

To configure NetScaler Gateway to enforce the restrictive session policy first, perform the following steps:

- Configure the global settings with ICA Proxy enabled and all other necessary settings if the specified application is not running on the user device.
- Create a session policy and profile that enables the Citrix Secure Access client.
- Create an expression within the rule portion of the session policy to specify the application, such as `(client.application.process(symantec.exe)exists)`

When users log on, the session policy is applied first. If Endpoint Analysis fails or the user skips the scan, NetScaler Gateway ignores the settings in the session policy (the expression in the session policy is considered false). As a result, users have restricted access using the Web Interface or clientless access. If Endpoint Analysis passes, NetScaler Gateway applies the session policy and users have full access with the Citrix Secure Access client.

Skip the EPA scan

You can skip the EPA scan for post-authentication and advance authentication only. Skip EPA is available on browsers of all supported operating systems. Users must click the **Skip EPA** button that appears when accessing the gateway. If users skip the scan, NetScaler Gateway processes this action as a failed Endpoint Analysis. When users fail the scan, they only get access to the Web Interface or through clientless access.

Also, see https://support.citrix.com/article/CTX200748.

Endpoint Analysis scans supported for Ubuntu

The following Endpoint Analysis (EPA) scans are supported for the EPA plug-in installed for the Ubuntu operating system. A sample expression to configure each of the scans is listed along with the EPA scans. You can configure these expressions in the authentication policies.

- **File**
  - **Existence**: sys.client_expr("file_0_/home/user/test.txt")
  - **MD5 Checksum**: sys.client_expr("file_0*/home/user/test.txt_md5* ce780e271debcc29f551546e8db3368f
)
  - **Text within a file (regular expression support)**: sys.client_expr("file_0_/home/user/test.txt_search_c
)
- **Process**
  - **Existence**: sys.client_expr("proc_0_perl")
  - **MD5 Checksum**: sys.client_expr("proc_0*perl_md5* c060d3a5f97e27066cef8c116785567a"
)
  - **Path**: sys.client_expr("proc_0*perl_path*/usr/bin/perl")
- **File system device or Mountpoint name**: sys.client_expr("mountpoint_0_/sys")

If you are using advanced policies, the expressions for each scan can be generated from the GUI (**Security > AAA > Policies > Authentication > Advanced Policies > EPA**).

Note: In the Expression Editor page, for the Linux client, you can select **Common,** and then select **Process, File** or **Mount Point**.

Preauthentication policies and profiles

January 8, 2024

> **Important:**
>
> Endpoint Analysis is intended to analyze the user device against pre-determined compliance criteria and does not enforce or validate the security of end-user devices. It is recommended to use endpoint security systems to protect devices from local admin attacks.

You can configure NetScaler Gateway to check a user's devices before they are authenticated to NetScaler Gateway. This can be used to restrict access if the user's device does not meet your organization's requirements. Device checks can be implemented using individual policies specific to a virtual server or globally, as described in the following two procedures.

Preauthentication policies consist of a profile and an expression. You configure the profile to use an expression to allow or deny a process to run on the user device. For example, the text file, clienttext.txt, is running on the user's device. When the user logs on to NetScaler Gateway, you can allow or deny access depending on whether the text file is running. If you do not want to allow users to log on when the process is running, you can configure a preauthentication profile to stop the process before users log on.

You can configure the following settings for pre-authentication policies:

- Expression. Includes the following settings to help you to create expressions:
  - Expression. Displays all expressions.
  - Match Any Expression. Configures the policy to match any of the expressions that are present in the list of selected expressions.
  - Match All Expressions. Configures the policy to match all the expressions that are present in the list of selected expressions.
  - Tabular Expressions. Creates a compound expression with the existing expressions by using the `OR` (||)`or` `AND` (&&) operators.
  - Advanced Free-Form. Creates custom compound expressions by using the expression names and the `OR` (||)`and` `AND` (&&) operators. Choose only those expressions that you require and omit other expressions from the list of selected expressions.
  - Add. Creates an expression.
  - Modify. Modifies an existing expression.
  - Remove. Removes the selected expression from the compound expressions list.
  - Named Expressions. Select a configured named expression. You can select named expressions from the menu of expressions already present on NetScaler Gateway.
  - Add Expression. Adds the selected named expression to the policy.

- Replace Expression. Replaces the selected named expression to the policy.
- Preview Expression. Displays the detailed string that is configured on NetScaler Gateway when you select a named expression.

Configure preauthentication profile

To configure a preauthentication profile globally by using the GUI

1. On the Configuration tab, click **NetScaler Gateway,** and then click **Global Settings**.
2. In the details pane, under **Settings**, click **Change pre-authentication settings**.
3. In the **Global Pre-authentication settings** dialog box, configure the settings:

   a) In **Action**, select **Allow or Deny**.

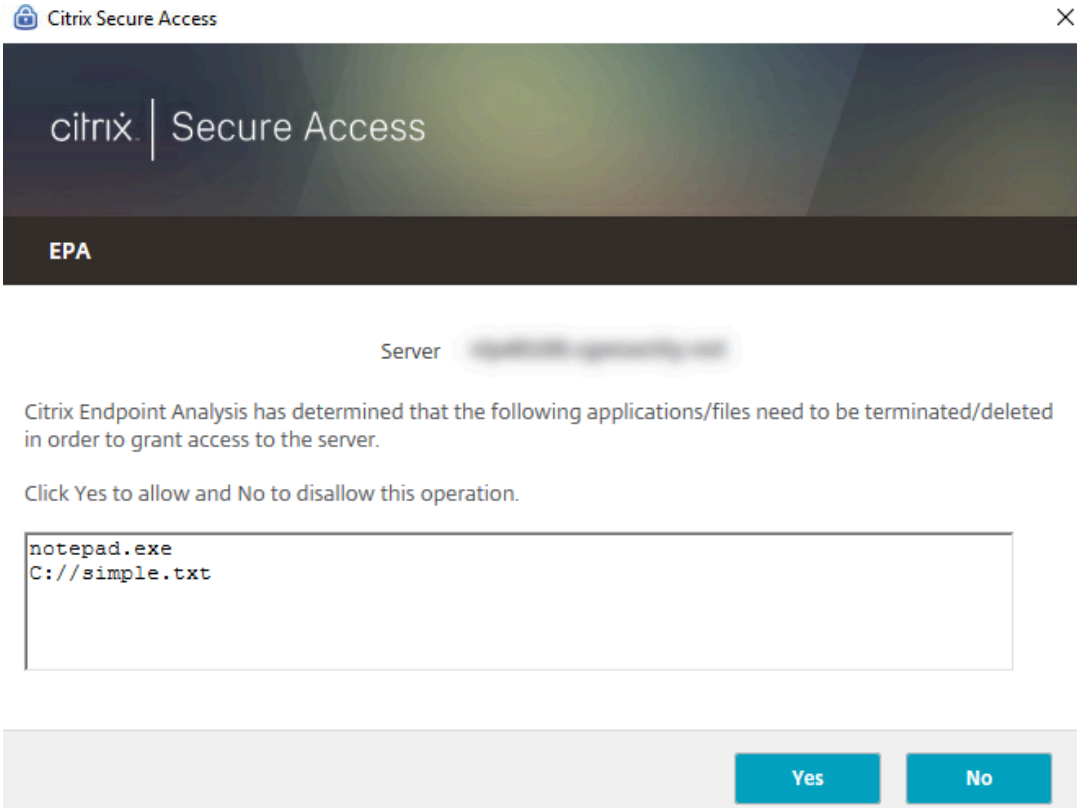
   Denies or allows users to log on after the Endpoint Analysis occurs.

   b) In **Processes to be canceled**, enter the process.

   This specifies the processes that the Endpoint Analysis plug-in must stop.

   c) In **Files to be deleted**, enter the file name.

   This specifies the files that the Endpoint Analysis plug-in must delete. When you delete or cancel a process, a notification is displayed to the end users.

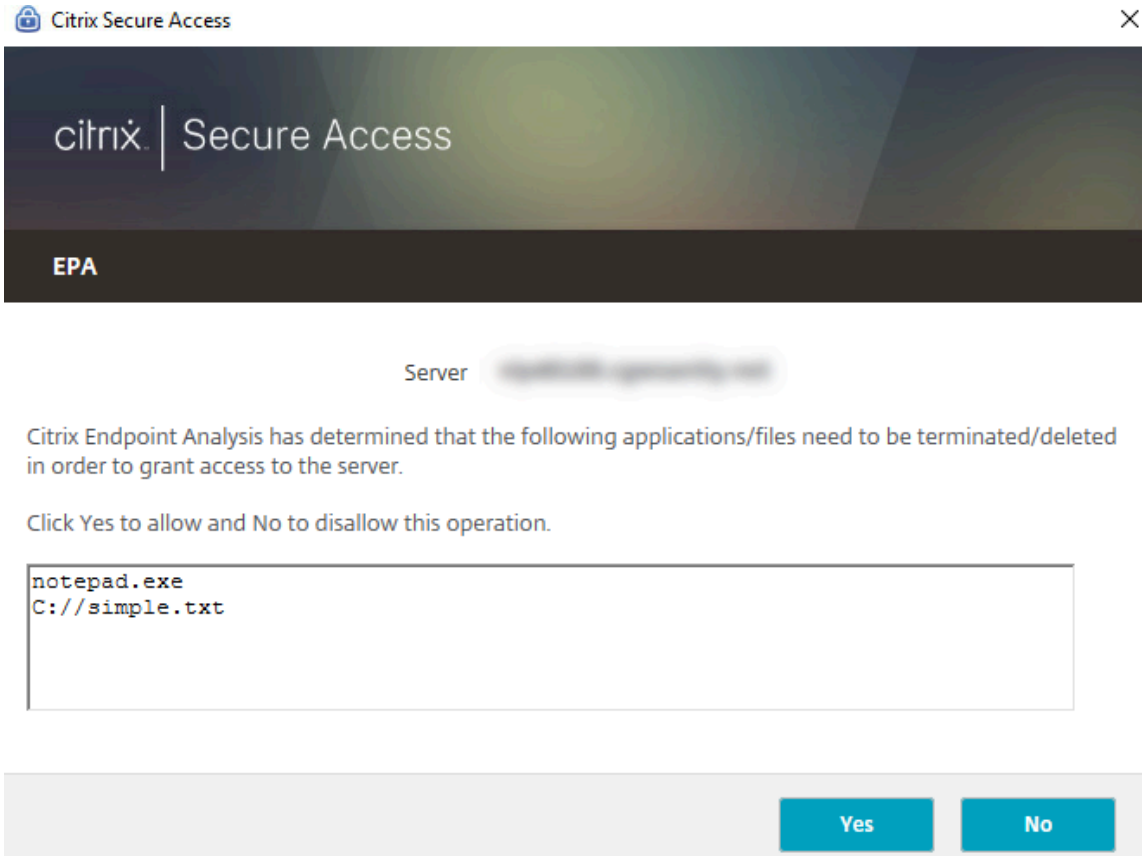


4. In Expression you can leave the expression ns_true or build an expression for a specific application, such as antivirus or security software, and then click **OK**.

To configure a preauthentication profile by using the GUI

1. Navigate to **NetScaler Gateway > Policies > Authentication/Authorization**, and then click **Pre-Authentication EPA**.
2. In the details pane, on the **Profiles** tab, click **Add**.
3. In **Name**, type the name of the application to be checked.
4. In **Action**, select **ALLOW** or **DENY**.
5. In **Processes to be canceled**, type the name of the process to be stopped.
6. In **Files to be deleted**, type the name of the file to be deleted, such as c:\clientext.txt, click **Create,** and then click **Close**.

   This specifies the files that the Endpoint Analysis plug-in must delete. When you delete or cancel a process, a notification is displayed to the end users.



If you use the GUI to configure a preauthentication profile, you then create the preauthentication policy by clicking **Add** on the **Policies** tab. In the **Create Pre-Authentication Policy** dialog box, select the profile from the **Request Profile** menu.

Add a preconfigured expression to a preauthentication policy

NetScaler Gateway comes with pre-configured expressions, called named expressions. When you configure a policy, you can use a named expression for the policy. For example, you want the preauthentication policy to check for Symantec antivirus 10 with updated virus definitions. Create a preauthentication policy and add the expression as described in the following procedure.

When you create a preauthentication or session policy, you can create the expression when you create the policy. You can then apply the policy, with the expression, to virtual servers or globally.

The following procedure describes how to add a preconfigured antivirus expression to a policy by using the configuration utility.

Add a named expression to a preauthentication policy

1. Navigate to **NetScaler Gateway > Policies > Authentication/Authorization**, and then click **Pre-Authentication EPA**.
2. In the details pane, select a policy and then click **Open**.
3. Next to **Named Expressions**, select **Anti-Virus**, select the antivirus product from the list.
4. Click **Add Expression**, click **Create,** and then click **Close**.

Configure custom expressions

A custom expression is one that you create within the policy. When you create an expression, you configure the parameters for the expression.

You can also create custom expressions to refer to commonly used strings. This eases the process of configuring preauthentication policies and also in maintaining the configured expressions.

For example, you want to create a custom expression for Symantec antivirus 10 and make sure that the virus definitions are no more than three days old. Create a policy and then configure the expression to specify the virus definitions.

The following procedure shows how to create an expression in a preauthentication policy. You can use the same steps in a session policy.

Create a preauthentication policy and custom expression

1. Navigate to **NetScaler Gateway > Policies > Authentication/Authorization**, and then click **Pre-Authentication EPA**.
2. In the details pane, click **Add**.
3. In **Name**, type a name for the policy.

4. Next to **Request Profile**, click **New**.
5. In the Create Authentication Profile dialog box, in **Name**, type a name for the profile and in **Action**, select **Allow**, and then click **Create**.
6. In the Create Pre-Authentication Policy dialog box, next to M**atch Any Expression**, click **Add**.
7. In **Expression Type**, select **Client Security**.
8. Configure the following:

   a) In **Component**, select **Anti-Virus**.
   b) In **Name**, type a name for the application.
   c) In **Qualifier**, select **Version**.
   d) In **Operator**, select **==**.
   e) In **Value**, type the value.
   f) In **Freshness**, type 3, and then click **OK**.

9. In the Create Pre-Authentication Policy dialog box, click **Create**, and then click **Close**.

When you configure a custom expression, it is added to the **Expression** box in the policy dialog box.

Configure compound expressions

A preauthentication policy can have one profile and multiple expressions. If you configure compound expressions, you use operators to specify the conditions of the expression. For example, you can configure compound expressions to require the user device to run one of the following antivirus applications:

- Symantec Antivirus 10
- McAfee Antivirus 11
- Sophos Antivirus 4

You configure the expression with the OR operator to check for the preceding three applications. If NetScaler Gateway detects the correct version of any of the applications on the user device, users are allowed to log on. The expression in the policy dialog box appears as follows:

```
av_5_Symantec_10 || av_5_McAfeevirusscan_11 || av_5_sophos_4
```

For more information about compound expressions, see Configuring Compound Expressions.

Bind preauthentication policies

After you create the preauthentication policy, bind the policy to the level to which it applies. You can bind the preauthentication policies to virtual servers or globally.

Create and bind a preauthentication policy globally

1. On the Configuration tab, click **NetScaler Gateway,** and then click **Global Settings**.
2. In the details pane, click **Change pre-authentication settings**.
3. In the Global Pre-Authentication Settings dialog box, in **Action**, select **Allow** or **Deny**.
4. In **Name**, type a name for the policy.
5. In the **Global Pre-authentication settings** dialog box, next to **Named Expressions**, select **General**, select **True** value, click **Add Expression**, click **Create**, and then click **Close**.

Bind a preauthentication policy to a virtual server

1. On the Configuration tab, click **NetScaler Gateway,** and then click **Virtual Servers**.
2. In the details pane, select a virtual server, and then click **Open**.
3. In the configure NetScaler Gateway Virtual Server dialog box, click the **Policies** tab, and then click **Pre-authentication**.
4. Under Details, click **Insert Policy**, and then under Policy Name, select the preauthentication policy.
5. Click **OK**.

Unbind and remove preauthentication policies

You can remove a preauthentication policy from NetScaler Gateway if necessary. Before you remove a preauthentication policy, unbind it from the virtual server or globally.

Unbind a global preauthentication policy

1. Navigate to **NetScaler Gateway > Policies > Authentication/Authorization**, and then click **Pre-Authentication EPA**.
2. In the details pane, select a policy and then in **Action**, click **Global Bindings**.
3. In the **Bind/Unbind Pre-authentication Policies to Global** dialog box, select a policy, click **Unbind Policy**, and then click **OK**.

Unbind a preauthentication policy from a virtual server

1. On the Configuration tab, click **NetScaler Gateway,** and then click **Virtual Servers**.
2. In the **Configure NetScaler Gateway Virtual Server** dialog box, click the **Policies** tab, and then click **Preauthentication**.
3. Select the policy and then click **Unbind Policy**.

When the preauthentication policy is unbound, you can remove the policy from NetScaler Gateway.

Remove a preauthentication policy

1. Navigate to **NetScaler Gateway > Policies > Authentication/Authorization**, and then click **Pre-Authentication EPA**.
2. in the details pane, select a policy and then click **Remove**.

Set the priority of preauthentication policies

You can have multiple preauthentication policies that are bound to different levels. For example, you have a policy that checks for a specific antivirus application bound globally and a firewall policy bound to the virtual server. When users log on, the policy that is bound to the virtual server is applied first. The policy that is bound globally is applied second.

You can change the order in which the preauthentication scans occur. To make NetScaler Gateway apply the global policy first, change the priority number of the policy bound to the virtual server, giving it a higher priority number than the policy bound globally. For example, set the priority number for the global policy to one and the virtual server policy to two. When users log on, NetScaler Gateway runs the global policy scan first and the virtual server policy scan second.

Change the priority of a preauthentication policy

1. On the Configuration tab, click **NetScaler Gateway,** and then click **Virtual Servers**.
2. In the details pane, select a virtual server, and then click **Open**.
3. On the Policies tab, click **Pre-authentication**.
4. Under Priority, type the priority number for the policy, and then click **OK**.

Post authentication policies

January 8, 2024

> **Important:**
>
> Endpoint Analysis is intended to analyze the user device against pre-determined compliance criteria and does not enforce or validate the security of end-user devices. It is recommended to use endpoint security systems to protect devices from local admin attacks.

A post-authentication policy is a set of generic rules that the user device must meet to keep the session active. If the policy fails, the connection to NetScaler Gateway ends. When you configure the

post-authentication policy, you can configure any setting for user connections that can be made conditional.

You use session policies to configure post-authentication policies. First, you create the users to which the policy applies. Then, you add the users to a group. Next, you bind session, traffic policies, and intranet applications to the group.

You can also specify groups to be authorization groups. This type of group allows you to assign users to groups based on a client device check expression within the session policy.

You can also configure a post-authentication policy to put users in a quarantine group if the user device does not meet the requirements of the policy. A simple policy includes a client device check expression and a message. When users are in the quarantine group, users can log on to NetScaler Gateway; however, they receive limited access to network resources.

You cannot create an authorization group and a quarantine group by using the same session profile and policy. The steps for creating the post-authentication policy are the same. When you create the session policy, you select either an authorization group or a quarantine group. You can create two session policies and bind each policy to the group.

Post-authentication policies are also used with SmartAccess. For more information about SmartAccess, see Configuring SmartAccess on NetScaler Gateway.

> **Note:**
>
> This functionality works only with the Citrix Secure Access client. If users log on with Citrix Workspace app, the Endpoint Analysis scan runs at logon only.

Configure a post-authentication policy

You use a session policy to configure a post-authentication policy. A simple policy includes a client device check expression and a message.

To configure a post-authentication policy by using the GUI

1. Expand **NetScaler Gateway > Policies** and then click **Session**.
2. In the details pane, on the **Policies** tab, click **Add**.
3. In **Name**, type a name for the policy.
4. Next to **Request Profile**, click **New**.
5. In **Name**, type a name for the profile.
6. On the Security tab, click **Advanced Settings**.
7. Under **Client Security**, click **Override Global,** and then click **New**.
8. Configure the client device check expression, and then click **Create**.

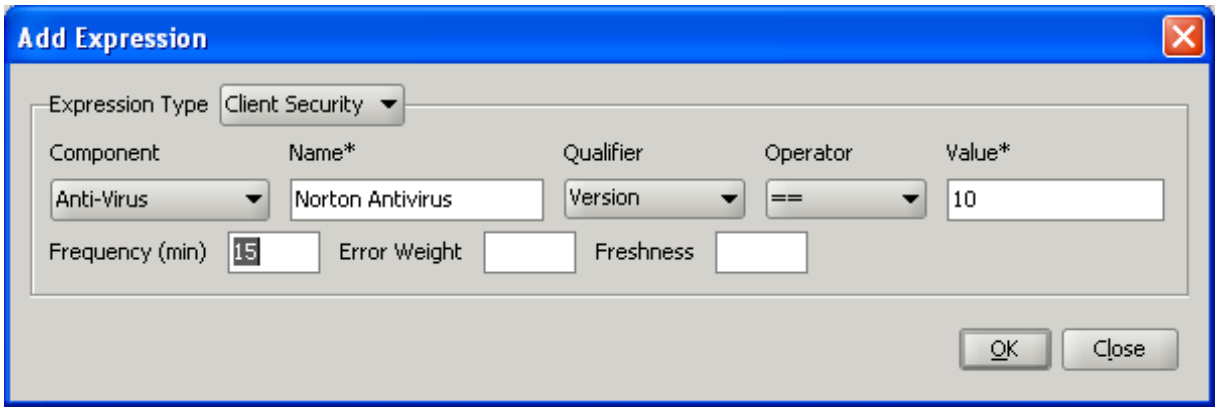
9. Under **Client Security**, in Quarantine Group, select a group.
10. In **Error Message**, type the message you want users to receive if the post-authentication scan fails.
11. Under Authorization Groups, click **Override Global**, select a group, click **Add**, click **OK**, and then click **Create**.
12. In the **Create Session Policy** dialog box, next to Named Expressions, select **General**, select **True value**, click **Add Expression**, click **Create**, and then click **Close**.

Configure the frequency of post-authentication scans

You can configure NetScaler Gateway to run the post-authentication policy at specified intervals. For example, you configured a client device check policy and want it to run on the user device every 10 minutes. You can configure this frequency by creating a custom expression within the policy.

> **Note:**
>
> The frequency check functionality for post-authentication policies works only with the Citrix Secure Access client. If users log on with Citrix Workspace app, the Endpoint Analysis scan runs at logon only.

You can set the frequency (in minutes) when you configure the client device check policy by following the procedure Configuring a Post-Authentication Policy. The following figure shows where you can enter a frequency value in the **Add Expression** dialog box.



Quarantine and authorization groups

When users log on to NetScaler Gateway, you assign them to a group that you configure either on NetScaler Gateway or on an authentication server in the secure network. If a user fails a post-authentication scan, you can assign the user to a restricted group, called a quarantine group, which restricts access to network resources.

You can also use authorization groups to restrict user access to network resources. For example, you might have a group of contract personnel having access only to your email server and a file share. When user devices pass the device check requirements that you defined on NetScaler Gateway, users can become members of groups dynamically.

You use either global settings or session policies to configure quarantine and authorization groups that are bound to a user, group, or virtual server. You can assign users to groups based on a client device check expression within the session policy. When the user is a member of a group, NetScaler Gateway applies the session policy based on group membership.

Configure authorization groups

When you configure an Endpoint Analysis scan, you can dynamically add users to an authorization group when the user device passes the scan. For example, you create an Endpoint Analysis scan that checks the user device domain membership. On NetScaler Gateway, create a local group called Domain-Joined Computers and add it as an authorization group for anyone who passes the scan. When users join the group, users inherit the policies associated with the group.

You cannot bind authorization policies globally or to a virtual server. You can use authorization groups to provide a default set of authorization policies when users are not configured to be members of another group on NetScaler Gateway.

To configure an authorization group by using a session policy

1. Navigate to **NetScaler Gateway > Policies** and then click **Session**.
2. In the details pane, on the Policies tab, click **Add**.
3. In **Name**, type a name for the policy.
4. Next to **Request Profile**, click **New**.
5. In **Name**, type a name for the profile.
6. On the Security tab, click **Advanced Settings**.
7. Under Authorization Groups, click **Override Global** and select a group from the drop-down list.
8. Click **Add**, click **OK** and then click **Create**.
9. In the **Create Session Policy** dialog box, next to Named Expressions, select **General**, select **True value**, click **Add Expression**, click **Create,** and then click **Close**.

After you create the session policy, you can bind it to a user, group, or virtual server.

To configure a global authorization group

1. Expand **NetScaler Gateway** and then click **Global Settings**.
2. In the details pane, under Settings, click **Change global settings**.
3. On the Security tab, click **Advanced Settings**.

4. Under Authorization Group, select a group from the drop-down list.
5. Click **Add,** and then click **OK**.

If you want to remove an authorization group either globally or from the session policy, in the Security Settings - Advanced dialog box, select the authorization group from the list and then click **Remove**.

Configuring Quarantine Groups

When you configure a quarantine group, you configure the client device check expression using the Security Settings - Advanced Settings dialog box within a session profile.

To configure the client device check expression for a quarantine group

1. Navigate to **NetScaler Gateway > Policies** and then click **Session**.
2. In the details pane, on the Policies tab, click **Add**.
3. In **Name**, type a name for the policy.
4. Next to **Request Profile**, click **New**.
5. In **Name**, type a name for the profile.
6. On the Security tab, click **Advanced Settings**.
7. Under **Client Security**, click **Override Global,** and then click **New**.
8. In the **Client Expression** dialog box, configure the client device check expression and, then click **Create**.
9. In **Quarantine Group**, select the group.
10. In Error Message, type a message that describes the problem for users and then click **Create**.
11. In the **Create Session Policy** dialog box, next to Named Expressions, select **General**, select **True value**, click **Add Expression**.
12. Click **Create,** and then click **Close**.

After you create the session policy, bind it to a user, group, or virtual server.

> **Note:**
>
> If the Endpoint Analysis scan fails and the user is put in the quarantine group, the policies that are bound to the quarantine group are effective only if there are no policies bound directly to the user that have an equal or lower priority number than the policies bound to the quarantine group.

To configure a global quarantine group

1. Expand **NetScaler Gateway** and then click **Global Settings**.
2. In the details pane, under Settings, click **Change global settings**.
3. On the **Security** tab, click **Advanced Settings**.

4. In **Client Security**, configure the client device check expression.
5. In **Quarantine Group**, select the group.
6. In **Error Message**, type a message that describes the problem for users, and then click **OK**.

Preauthentication device check expressions for user devices

January 8, 2024

> **Important:**
>
> Endpoint Analysis is intended to analyze the user device against pre-determined compliance criteria and does not enforce or validate the security of end-user devices. It is recommended to use endpoint security systems to protect devices from local admin attacks.

NetScaler Gateway provides various endpoint compliance checks during user logon or at other configured times during a session that help in validating the user devices. Only the user devices that pass these checks are allowed to establish a NetScaler Gateway session.

The following are the types of checks on user devices that you can configure on NetScaler Gateway:

- Antispam
- Antivirus
- File policies
- Internet security
- Operating system
- Personal firewall
- Process policies
- Registry policies
- Service policies

If a device check fails on the user device, no new connections are made until a subsequent check pass (in the case of checks that are at regular intervals); however, traffic flowing through existing connections continues to tunnel through NetScaler Gateway.

You can use the configuration utility to configure preauthentication policies or device check expressions within session policies that are designed to carry out checks on the user devices.

Configure antivirus, firewall, internet security, or antispam expressions

You configure settings for antivirus, firewall, Internet security, and antispam policies within the **Add Expression** dialog box. The settings for each policy are the same: the differences are the values that

you select. For example, if you want to check the user device for Norton antivirus version 10 and ZoneAlarm Pro, you create two expressions within the session or preauthentication policy that specify the name and version number of each application.

When you select Client Security as the expression type, you can configure the following:

- Component: The type of client security, such as antivirus, firewall, or registry entry.
- Name: The name of the application, process, file, registry entry, or operating system.
- Qualifier: The version or the value of the component for which the expression checks.
- Operator: Checks if the value exists or is equal to the value.
- Value: The application version for antivirus, firewall, Internet security, or antispam software on the user device.
- Frequency: Frequency with which a post-authentication scan is run, in minutes.
- Error weight: A weight assigned to each error message contained in a nested expression when multiple expressions have different error strings. The weight determines which error message appears.
- Freshness: Defines how old a virus definition can be. For example, you can configure the expression so virus definitions are no older than three days.

To add a client device check policy to a preauthentication or session policy

1. In the configuration utility, in the navigation pane, do one of the following:
   a) In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway > Policies** and then click **Session**.
   b) In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway > Policies > Authentication/Authorization**, and then click **Pre-Authentication EPA**.
2. In the details pane, on the Policies tab, click **Add**.
3. In Name, type a name for the policy.
4. Next to Match Any Expression, click Add.
5. In the Add Expression dialog box, in Expression Type, select **Client Security**.
6. Configure the settings for the following:
   a) In Component, select the item for which to scan.
   b) In Name, type the name of the application.
   c) In Qualifier, select **Version**.
   d) In Operator, select the value.
   e) In Value, type the client device check string, click **OK**, click **Create**, and then click **Close**.

Configure service policies

A service is a program the runs silently on the user device. When you create a session or preauthentication policy, you can create an expression that ensures that user devices are running a particular service when the session is established.

To configure a service policy

1. In the configuration utility, in the navigation pane, do one of the following:
   a) In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway > Policies** and then click Session.
   b) In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway > Policies > Authentication/Authorization**, and then click Pre-Authentication EPA.
2. In the details pane, on the Policies tab, click Add.
3. In Name, type a name for the policy.
4. Next to Match Any Expression, click Add.
5. In the Add Expression dialog box, in Expression Type, select Client Security.
6. Configure the settings for the following:
   a) In Component, select Service.
   b) In Name, type the name of the service.
   c) In Qualifier, leave blank or select Version.
   d) Depending on your selection in Qualifier, do one of the following:
      - If left blank, in Operator, select == or !=
      - If you selected Version, in Operator, in Value, type the value, click OK, and then click Close.

You can check a list of all available services and the status for each on a Windows-based computer at the following location:

Control Panel > Administrative Tools > Services

> **Note:**
>
> The service name for each service varies from its listed name. Check for the name of the service by looking at the
> Properties dialog box.

Configure process policies

When creating a session or preauthentication policy, you can define a rule that requires all user devices to have a particular process running when users log on. The process can be any application and can include customized applications.

Note: The list of all processes running on a Windows-based computer appears on the **Processes** tab of Windows Task Manager.

To configure a process policy

1. In the configuration utility, in the navigation pane, do one of the following:
   a) In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway \ > Policies** and then click Session.
   b) In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway > Policies \ > Authentication/Authorization**, and then click Pre-Authentication EPA.
2. In the details pane, on the Policies tab, click Add.
3. In Name, type a name for the policy.
4. Next to Match Any Expression, click Add.
5. In the Add Expression dialog box, in Expression Type, select Client Security.
6. Configure the settings for the following:
   a) In Component, select Process.
   b) In Name, type the name of the application.
   c) In Operator, select EXISTS or NOTEXISTS, click OK and then click Close.

When you configure an Endpoint Analysis policy (pre-authentication or post-authentication) to check for a process, you can configure an MD5 checksum.

When you create the expression for the policy, you can add the MD5 checksum to the process you are checking for. For example, if you are checking to see if notepad.exe is running on the user device, the expression is:
CLIENT.APPLICATION.PROCESS(notepad.exe_md5_388b8fbc36a8558587afc90fb23a3b00) EXISTS

Configure operating system policies

When you create a session or preauthentication policy, you can configure client device check strings to determine whether the user device is running a particular operating system when users log on. You can also configure the expression to check for a particular service pack or hotfix.

The values for Windows and Macintosh are:

Operating system	Value
macOS X	macOS
Windows 8.1	win8.1
Windows 8	win8
Windows 7	win7
Windows Vista	vista
Windows XP	winxp
Windows Server 2008	win2008
Windows Server 2003	win2003
Windows 2000 Server	win2000
Windows 64-bit platform	win64

To configure an operating system policy by using the GUI

1. In the navigation pane, do one of the following:
   a) Navigate to **NetScaler Gateway > Policies** and then click **Session**.
   b) Navigate to **NetScaler Gateway > Policies > Preauthentication**.
2. In the details pane, on the **Policies** tab, click **Add**.
3. In **Name**, type a name for the policy.
4. In **Request Action** select an existing action or create one.
5. Click **Expression Editor**.
6. In **Select Expression Type**, select **Client Security**.
7. Configure the settings for the following:
   a) In **Component**, select **Operating System**.
   b) In **Name**, type the name of the operating system.
   c) In Qualifier, do one of the following:
      - Leave the field blank
      - Select **Service Pack**
      - Select **Hotfix**
      - Select **Version** (for macOS only)
   d) Depending on your selection in step 7, in Operator, do one of the following:

- If Qualifier is blank, in Operator, select EQUAL (= =), NOTEQUAL (!=), EXISTS or NOTEXISTS.
- If you selected Service Pack or Hotfix, select the operator and in Value, type the value.

8. Click **Done** and then click **Close**.

If you are configuring a service pack, such as client.os `(winxp).sp`, if a number is not in the **Value** field, NetScaler Gateway returns an error message because the expression is invalid.

If the operating system has service packs present, such as Service Pack 3 and Service Pack 4, you can configure a check just for Service Pack 4, because the presence of Service Pack 4 automatically indicates that previous service packs are present.

Configure registry policies

When you create a session or preauthentication policy, you can check for the existence and value of registry entries on the user device. The session is established only if the particular entry exists or has the configured or higher value.

When configuring a registry expression, use the following guidelines:

- Four backslashes are used to separate keys and subkeys, such as

  HKEY_LOCAL_MACHINE\\\\SOFTWARE

- Underscores are used to separate the subkey and the associated value name, such as

  HKEY_LOCAL_MACHINE\\\\SOFTWARE\\\\VirusSoftware_Version

- A backslash (\) is used to denote a space, such as in the following two examples:

  HKEY_LOCAL_MACHINE\\\\SOFTWARE\\Citrix\\\\Secure\ Access\ Client_ProductVersion

  CLIENT.REG(HKEY_LOCAL_MACHINE\\\\Software\\\\Symantec\\Norton\ AntiVirus_Version).VALUE == 12.8.0.4 -frequency 5

The following is a registry expression that looks for the Citrix Secure Access client registry key when users log on:

CLIENT.REG(`secureaccess`).VALUE==HKEY_LOCAL_MACHINE\\\\SOFTWARE\\\\CITRIX\\\\Secure\Access\Client

> **Note:**
>
> If you are scanning for registry keys and values and you select Advanced Free-Form in the Expression dialog box, and the expression must start with CLIENT.REG.

Registry checks are supported under the following most common five types:

- HKEY_CLASSES_ROOT

- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

Registry values to be checked use the following types:

- String

  For the string value type, case-sensitivity is checked.

- DWORD

  For the DWORD type, the value is compared and must be equal.

- Expanded String

  Other types, such as Binary and Multi-String, are not supported.

- Only the '=='comparison operator is supported.
- Other comparison operators, such as <, > and case-sensitive comparisons are not supported.
- The total registry string length must be less than 256 bytes.

You can add a value to the expression. The value can be a software version, service pack version, or any other value that appears in the registry. If the data value in the registry does not match the value you are testing against, users are denied logon.

> **Note:**
>
> You cannot scan for a value within a subkey. The scan must match the named value and the associated data value.

To configure a registry policy

1. In the configuration utility, in the navigation pane, do one of the following:
   a) In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway \ > Policies** and then click Session.
   b) In the configuration utility, on the Configuration tab, in the navigation pane, expand **NetScaler Gateway > Policies \ > Authentication/Authorization**, and then click Pre-Authentication EPA.
2. In the details pane, on the Policies tab, click Add.
3. In Name, type a name for the policy.
4. Next to Match Any Expression, click Add.
5. In the Add Expression dialog box, in Expression Type, select Client Security.

6. Configure the settings for the following:
   a) In Component, select Registry.
   b) In Name, type the name of the registry key.
   c) In Qualifier, leave blank or select Value.
   d) In Operator, do one of the following:
      - If Qualifier is left blank, select EXISTS or NOTEXISTS
      - If you selected Value in Qualifier, select either == or !==
   e) In Value, type the value as it appears in the registry editor, click OK and then click Close.

Configure compound client device check expressions

You can combine client device check strings to form compound client device check expressions.

The Boolean operators that are supported in NetScaler Gateway are:

- And (&&)

Or (

-

- Not (!)

For greater precision, you can group the strings together using parentheses.

> **Note:**
>
> If you use the command line to configure expressions, use parentheses to group device check expressions together when you form a compound expression. The use of parentheses improves the understanding and debugging of the client expression.

Configure policies with the AND (&&) operator

The AND (&&) operator works by combining two client device check strings so that the compound check passes only when both checks are true. The expression is evaluated from left to right and if the first check fails, the second check is not carried out.

You can configure the AND (&&) operator using the keyword ‘AND’or the symbols ‘&&’.

Example:

The following is a client device check that determines if the user device has Version 7.0 of Sophos antivirus installed and running. It also checks if the Net Logon service is running on the same computer.


```
CLIENT.APPLICATION.AV(sophos).version==7.0 AND CLIENT.SVC(netlogon)
EXISTS
```

This string can also be configured as:

```
CLIENT.APPLICATION.AV(sophos).version==7.0 && CLIENT.SVC(netlogon)
EXISTS
```

Configure policies with the OR (||) operator

The OR (| |) operator works by combining two device check strings. The compound check passes when either check is true. The expression is evaluated from left to right and if the first check passes, the second check is not carried out. If the first check does not pass, the second check is carried out.

You can configure the OR (| |) operator using the keyword `OR` or the symbol `||`.

Example:

The following is a client device check that determines if the user device has either the file `c:\\file.txt` on it or the `putty.exe` process running on it.

```
client.file(c:\\\\\\\\\\file.txt)EXISTS)OR (client.proc(putty.exe)
EXISTS
```

This string can also be configured as

```
client.file(c:\\\\\\\\\\file.txt)EXISTS)|| (client.proc(putty.exe)
EXISTS
```

Configure policies using the NOT (!) operator

The NOT (!) or the negation operator negates the client device check string.

Example:

The following client device check passes if the file c:\sophos_virus_defs.dat file is NOT more than two days old:

```
\!(client.file(c:\\\\\\\\\\sophos\\_virus\\_defs.dat).timestamp==2dy)
```

EPA scan as a factor in nFactor authentication

June 11, 2024

> **Important:**
>
> Endpoint Analysis is intended to analyze the user device against pre-determined compliance criteria and does not enforce or validate the security of end-user devices. It is recommended to use endpoint security systems to protect devices from local admin attacks.

The following are some of the basic entities of nFactor EPA.

EPA Action: EPA Action is an action type introduced for nFactor EPA. It contains the following:

- Client device check expression: This expression is sent to the gateway EPA plug-in for evaluation.
- Success Group: This group, if configured, is inherited to the gateway session if the EPA result is true.
- Quarantine Group: This group, if configured, is inherited to the gateway session if the EPA result is false.
- killProcess: This represents the name of the process that the EPA process must terminate.
- deleteFiles: Specifies comma-separated paths to files that the EPA process must delete.

Groups can be used during the life of the session to determine whether the client meets certain EPA condition.
If at a given factor, the EPA fails and the last action does not contain "Quarantine Group", then authentication is terminated for that user.
If "Quarantine group"exists, authentication is continued and the administrator can check for the group to give limited access. For more details, see EPA execution.

To configure an authentication EPA action using the GUI:

- Navigate to **Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Actions > Authentication EPA Action**.
- Configure the following parameters:
  - Name: Name of the EPA action.
  - Default group: The default group that is chosen when the EPA check is successful.
  - Quarantine Group: The quarantine group that is chosen when the EPA check fails.
  - Kill Process: String specifying the name of a process to be terminated by the EPA tool. Multiple processes are separated by commas.
  - Delete Files: String specifying the paths and names of the files to be deleted by the EPA tool. Multiple files are separated by commas.
  - Expression: Client security expression to be sent to the client.

To configure an authentication EPA action using the CLI:

```
add authentication epaAction CWA version check scan -csecexpr sys.
client_expr("sys_0_MAC-CWA_version_>=_23.9.0.99")
```


The preceding CLI example indicates an EPA scan to verify Citrix Workspace app version on a macOS machine.

EPA Policy: In nFactor, all the policies are added with the same syntax "add authentication policy". However, the type of the action qualifies the policy as an EPA policy.

EPA Factor: EPA factor is a regular policy label. There is no entity called EPA factor. Once EPA policy is bound to a factor, it inherits certain properties that make it an EPA factor.

> **Note:**
>
> The term "EPA Factor"is commonly used in this document to refer to a factor with EPA policies.

EPA –Quarantine: If at a given factor, all client device check expressions from all actions fail, and if the last action contains "Quarantine group", that group is added to the session and the nextFactor is looked into. That is, despite the failure, the presence of the "quarantine group"qualifies the session to the next stage. However, due to the inheritance of a special group, the administrator can relegate the session to restricted access or extra authentication policies like OTP or SAML.

If there is no quarantine group at the last action, authentication terminates in a failure.

EPA in nFactor also uses the following entities:

- **LoginSchema:** XML representation of logon form. It defines the "view"of the logon form and also has properties of a "factor".
- **Policy label or policy factor:** It is a collection of policies that are tried at a given stage of authentication.
- **Virtual server label:** Virtual server is also a policy label, that is one can bind policies to virtual server. However, the virtual server is the collection of various policy labels as it is the entry point for user access.
- **next factor:** It is used to specify the policylabel/factor to be taken once the given authentication policy succeeds.
- **NO_AUTHN policy:** Special policy whose action always succeeds.
- **Passthrough factor:** Is a policylabel/factor whose login schema does not contain view. It is an indication to the NetScaler appliance to continue authentication at the given factor without user intervention.

For more information, see nFactor concepts, entities, and terminology.

EPA Factor mutual exclusivity

EPA Factor contains one or more EPA policies. Once EPA policies are bound to a factor, regular authentication policies are disallowed on that factor. This restriction is to offer the best user experience and clean separation of endpoint analysis. The only exception to this rule is the NO_AUTHN policy.

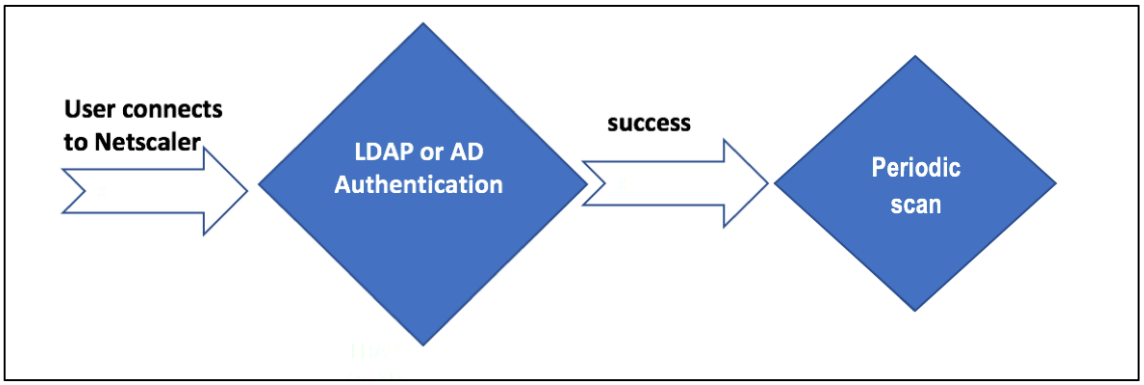
Since NO_AUTHN policy is a special policy used to simulate 'on-failure-jump', it is allowed in the EPA factor.

EPA Execution

At any given factor (including the virtual server factor), before serving the logon form, the NetScaler appliance checks if the factor is configured for EPA. If so, it sends a specific response to the client (UI) such that the EPA sequence is triggered. This sequence comprises the client requesting for client device check expressions and sending the results.
Client device check expressions for all policies in a factor are sent at once to the client. Once results are obtained at the NetScaler appliance, each of the expressions in all actions are evaluated in a sequence. The first action that results in successful EPA terminates that factor, and DefaultGroup, if configured, is inherited into the session. If NO_AUTHN policy is encountered, it qualifies as automatic success. If the nextFactor is specified, the appliance continues with that factor. Otherwise, authentication terminates.
This condition is applicable for the first factor as well. If there is no authentication policy factor after EPA at the virtual server, authentication is terminated. This is different from classic policy behavior where the user is always shown the login page after EPA.
However, in the event of no successful EPA policy, then NetScaler Gateway looks at the Quarantine Group configured for the last EPA policy in that factor or cascade. If the last policy is configured with the Quarantine Group, that group is added to the session and the nextFactor is inspected. If a nextFactor exists, authentication proceeds to that factor. Otherwise, authentication is completed.

Configure EPA scan to run after authentication

You can configure EPA scan to run after the authentication. In the following example, the EPA scan is used as a final check in a nFactor or multifactor authentication. In this setup, if the EPA scan fails during any such check, the session is terminated.



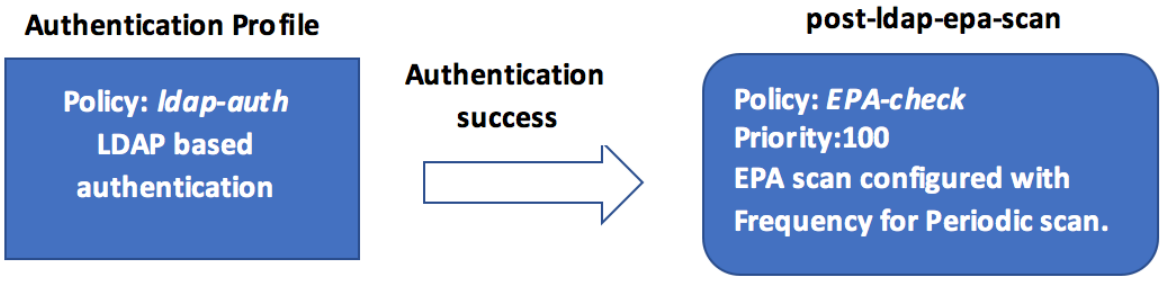
- User tries to connect to NetScaler Gateway Virtual IP.
- A login page with user name and password field is rendered to the user to provide login credentials. With these credentials, LDAP, or AD based authentication is performed at the back-end. If successful, the user is presented with a pop up to authorize the EPA scan.
- Once the user authorizes, the EPA scan is performed and based on the success or failure of user client settings, access is provided.
- If the scan is successful, the EPA scan is performed periodically to learn that the device check requirements configured are still met.
- If the EPA scan fails during any such check, the session is terminated.

Pre-requisites

It is assumed that the following configuration is in place:

- VPN virtual server, gateway, and authentication virtual server configuration
- LDAP server configurations and associated policies.

The following section captures the required policies and policy label configurations and also the mapping of policies and policy label to an authentication profile.



On the CLI

1. Create an action to perform an EPA scan before LDAP authentication and associate it with an EPA scan policy.

```
add authentication epaAction pre-ldap-epa-action -csecexpr "sys.client_expr (\"proc_2_firefox\")"

add authentication Policy pre-ldap-epa-pol -rule true -action pre-ldap-epa-action
```

   The preceding expression scans if the process ‘Firefox’is running. The EPA client checks for the process existence every 2 minutes, signified by the digit ‘2’in the scan expression.

2. Configure the policy label `pre-ldap-epa-label`, which hosts the policy for the EPA scan.


```
add authentication policylabel pre-ldap-epa-label -loginSchema
    LSCHEMA_INT
```

> **Note:**
>
> LSCHEMA_INT is an inbuilt schema with no schema(noschema), that means no additional webpage is presented to the user at this step.

3. Associate the policy configured in step 1 with the policy label configured in step 2. This completes the authentication mechanism.

```
bind authentication policylabel pre-ldap-epa-label -policyName pre
    -ldap-epa-pol -priority 100 -gotoPriorityExpression END
```

4. Configure an LDAP action and policy.

```
add authentication ldapAction ldap-act -serverIP 10.106.103.60 -
    ldapBase "dc=cgwsanity,dc=net" -ldapBindDn user1@example.net -
    ldapBindDnPassword 1.cloud -ldapLoginName samAccountName -
    groupAttrName memberOf -subAttributeName CN -passwdChange
    ENABLED

add authentication Policy ldap-pol -rule true -action ldap-act
```

5. Create a login schema with SSO enabled.

```
add authentication loginSchema ldap-schema -authenticationSchema "
    /nsconfig/loginschema/LoginSchema/SingleAuth.xml" -
    SSOCredentials Yes
```

6. Configure the policy label `ldap-pol-label`, which hosts the policy for the LDAP authentication.

```
add authentication policylabel ldap-pol-label -loginSchema ldap-
    schema
```

7. Bind the login schema configured in step 5 to the policy label configured in step 6.

```
bind authentication policylabel ldap-pol-label -policyName ldap-
    pol -priority 100 -gotoPriorityExpression NEXT
```

8. Create an action to perform an EPA scan post the LDAP authentication and associate it with an EPA scan policy.

```
add authentication epaAction post-ldap-epa-action -csecexpr "sys.
    client_expr (\"proc_2_chrome\")"

add authentication Policy post-ldap-epa-pol -rule true -action
    post-ldap-epa-action

```



```
add authentication policylabel post-ldap-epa-label -loginSchema
    LSCHEMA_INT

bind authentication policylabel post-ldap-epa-label -policyName
    post-ldap-epa-pol -priority 100 -gotoPriorityExpression
```

9. Bringing it all together, associate the policy `pre-ldap-epa-pol` to the authentication virtual server with the next step pointing to the policy label `ldap-pol-label` to do an EPA scan.

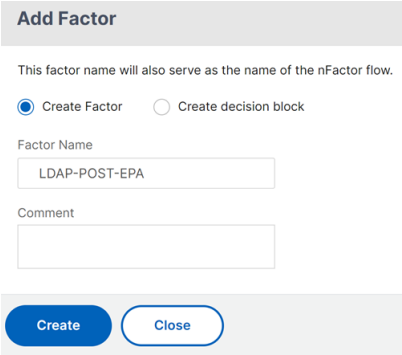
```
bind authentication vserver user.auth.test -policy pre-ldap-epa-
    pol -priority 100 -nextFactor ldap-pol-label -
    gotoPriorityExpression NEXT

bind authentication policylabel ldap-pol-label -policyName ldap-
    pol -priority 100 -gotoPriorityExpression NEXT -nextFactor post
    -ldap-epa-label
```

> **Note:**
>
> - In periodic EPA configured as multiple factors, the latest factor with periodic EPA configuration is considered.
> - Periodic scans can be run only using the EPA plug-in and not on the browser.
> - In the first example, EPA is the first factor where the scan looks for the process 'Firefox'.
> - If the EPA scan is successful, it leads to LDAP authentication, followed by the next EPA scan, that looks for the process 'Chrome'.
> - When multiple periodic scans are configured as different factors, the latest scan takes the precedence. In this case, the EPA plug-in scans for the process 'Chrome'every 2 minutes after the login is successful.

On the GUI (using nFactor Visualizer)

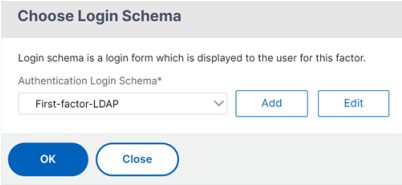
You can configure advanced EPA scan as a factor using the nFactor visualizer on the GUI. In the following example, we have used LDAP as the first factor and EPA as the next factor.

1. Create a first factor for the nFactor flow.
   - Navigate to **Security > AAA-Application Traffic > nFactor Visualizer > nFactor Flows** and click **Add**.
   - Click **+** to add the nFactor flow.
   - Add a factor and click **Create**.



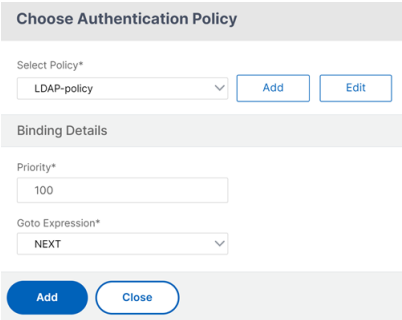
2. Create a login schema and a policy for the first factor.

   - On the first factor tile, click **Add Schema** to add a login schema. You can either select an existing authentication login schema from the drop-down list or create a login schema.
   - To create an authentication login schema, click **Add**. For detailed information about authentication login schema, see Configuring nFactor authentication.



   - Click **Add Policy** to add the LDAP policy. If the LDAP policy is already created, you can select the same. Click **Add**.

> **Note:**
>
> If an LDAP policy is not created, you can create one. Click the **Add** button next to the **Select Policy** drop-down list. In the **Action** field, select LDAP. For details about adding an authentication LDAP server, see `https://support.citrix.com/article/CTX123782`.



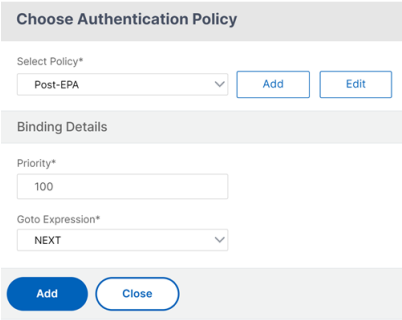
3. Create a next factor and connect it to the first factor.

   - Click the green or red colored **+** icon, to add EPA as the next factor.

- Create the next factor on the **Next Factor to Connect** page.
- Leave the **Add Schema** section blank, to have the default no schema applied for this factor.

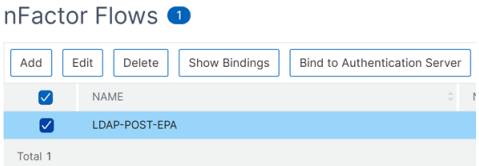
4. Add a policy for the next factor.

   - Click **Add policy** to add the post authentication EPA policy and action.
   - You can either choose from an existing list of policies or create a policy. To choose from the existing policies, select a policy from the **Select Policy** drop-down list, provide the binding details, and click **Add**.
   - To create a policy, click the **Add** button next to the **Select Policy** drop-down list.



5. After the nFactor flow is complete, click **Done**.
6. Bind the nFactor flow to an authentication server.

   - Navigate to **Security AAA - Application Traffic > nFactor Visualizer > nFactor Flows**.
   - Select the nFactor and click **Bind to Authentication Server**.



References

- nFactor concepts, entities, and terminology
- How to Configure LDAP Authentication on NetScaler Gateway
- LDAP authentication
- Advanced Endpoint Analysis scans

EPA scan classification types on Windows client

January 8, 2024

> **Important:**
>
> Endpoint Analysis is intended to analyze the user device against pre-determined compliance criteria and does not enforce or validate the security of end-user devices. It is recommended to use endpoint security systems to protect devices from local admin attacks.

The following new classification types are added to the EPA scan for missing patches. The EPA scan fails if the client has any of the following missing patches.

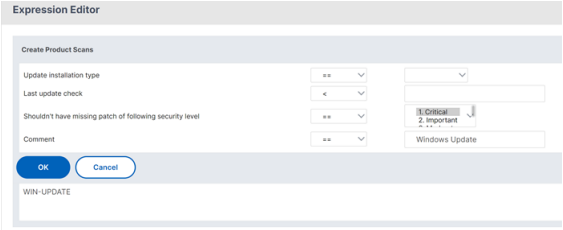
- Application
- Connectors
- CriticalUpdates
- DefinitionUpdates
- DeveloperKits
- FeaturePacks
- Guidance
- SecurityUpdates
- ServicePacks
- Tools
- UpdateRollups
- Updates

> **Notes:**
>
> - Earlier, the EPA scans for missing patches were done on the severity levels; Critical, Important, Moderate, and Low on the Windows client.
> - If you are using Citrix Secure Access for Windows 23.8.1.1 and above, the scan `CLIENT.SYSTEM('WIN-UPDATE_SCAN-TIME')` is limited to client machines that have the automatic updates enabled. If the automatic updates are disabled, this scan returns a different outcome.

Configure the EPA scan classification types by using the GUI

1. Navigate to **NetScaler Gateway > Policies > Preauthentication**.
2. Create a new preauthentication policy or edit an existing policy.
3. Click the **OPSWAT EPA Editor** link.
4. In Expression Editor, select **Windows > Windows Update**.
5. In **Shouldn't have missing patch of following windows update classification type**, select the classification type for the missing patches.

6. Click **OK**.



Customers can upgrade to the OPSWAT version 4.3.2744.0s to use these options.

References

- For details about the Windows server update services classification GUIDs, see https://docs.microsoft.com/en-us/previous-versions/windows/desktop/ff357803(v=vs.85).
- For the description of the Microsoft software updates terminology, see https://docs.microsoft.com/en-us/troubleshoot/windows-client/deployment/standard-terminology-software-updates.

Advanced Endpoint Analysis scans

February 15, 2024

Advanced Endpoint Analysis (EPA) is used for scanning user devices for the endpoint security requirement configured on NetScaler Gateway. If a user device tries to access the NetScaler Gateway, the device is scanned for security information, such as operating system, antivirus, web browser versions and so forth before an administrator can grant access to NetScaler Gateway.

The Advanced EPA scan is a policy-based scan that you can configure on NetScaler Gateway for authentication sessions. The policy performs a registry check on a user device and based on evaluation, the policy allows or denies access to the NetScaler network. For more information about the Citrix EPA client system requirements, see Endpoint Analysis requirements.

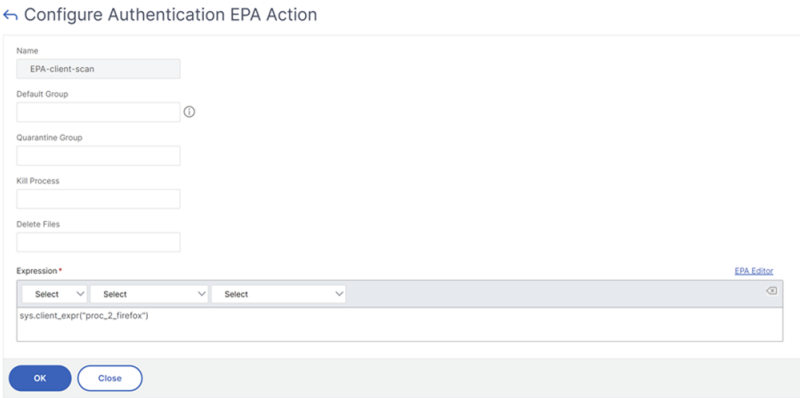
You can configure the advanced EPA scan by using the GUI or the CLI.

On the GUI

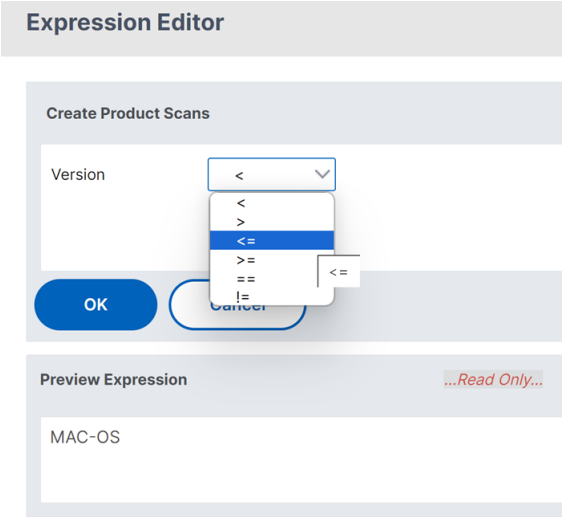
1. Create EPA action.

   Navigate to **Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Actions > EPA** and click **Add**. On the **Create Authentication EPA Action** page, update the following information and click **Create**.

- Name: Name of the EPA action.
- Default Group: The default group that is chosen when the EPA check succeeds.
- Quarantine Group: The quarantine group that is chosen when the EPA check fails.
- Kill Process: String specifying the name of a process to be terminated by the EPA plug-in. Multiple processes must be comma-separated.
- Delete Files: String specifying the paths and names of the files to be deleted by the EPA plug-in. Multiple files must be comma-separated.
- Expression: Refer to Advanced Endpoint Analysis policy expression reference for the EPA expression format.



- EPA Editor: Select the operators for the product version scan.



Note:

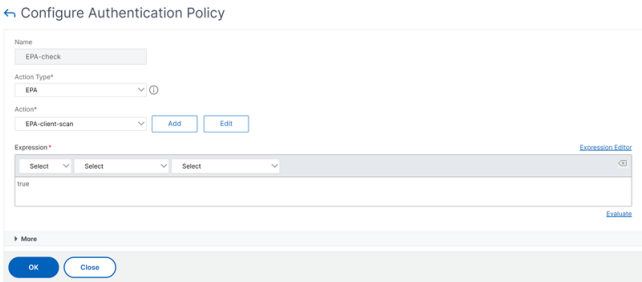
Citrix EPA client for macOS 24.2.1.5 / Citrix Secure Access client for macOS 24.02.1 and later versions support the EPA operators >, <, >=, <=, == and != on the EPA editor. Also, the **Mac OS** option is now available as a separate option on the EPA editor (**Mac > Mac OS**). Previously, the macOS product version scan had to be performed at **Common > Operating**

> **System > MacOS** using only the == and != operators. Ensure that you are using NetScaler Gateway 14.1-12.x or later to leverage this functionality.
>
> You can perform a product version scan of your macOS devices at **Mac > Mac OS** using these operators. For example, to allow the OS versions from 12.4 to 13.0, except 12.8, configure the expression `sys.client_expr("sys_0_MAC-OS_version_>=_12.4")&&sys.client_expr("sys_0_MAC-OS_version_<=_13.0")&&sys.client_expr("sys_0_MAC-OS_version_!=_12.8")` on the EPA editor.

2. Create a corresponding EPA policy.

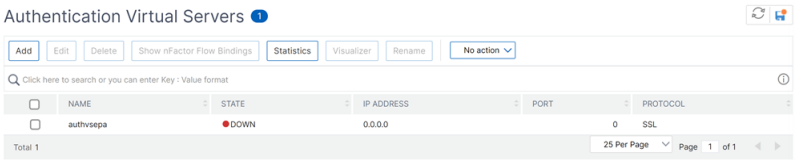
   Navigate to **Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Policies** and click **Add**. On the **Create Authentication Policy** page, update the following information and click **Create**.

   - Name: Name of the advanced EPA policy.
   - Action Type: Type of the authentication action.
   - Action: Name of the authentication action to be performed if the policy matches.
   - Expression: Refer to Advanced Endpoint Analysis policy expression reference for the EPA expression format.
   - Log Action: Name of message log action to use when a request matches this policy. Maximum allowed length is 127 characters.

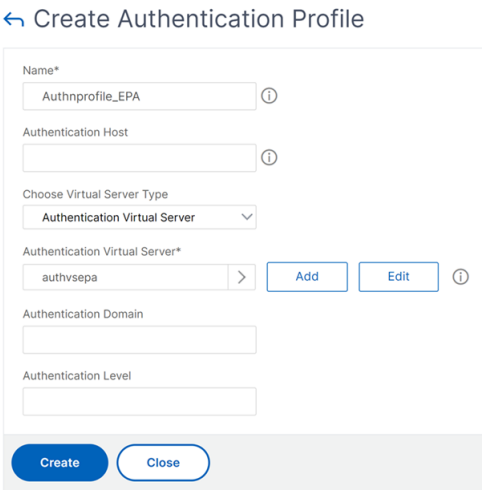


3. Configure an authentication virtual server and an authentication profile.

   - Navigate to **Security > AAA - Application Traffic > Authentication Virtual servers** and click **Add**.

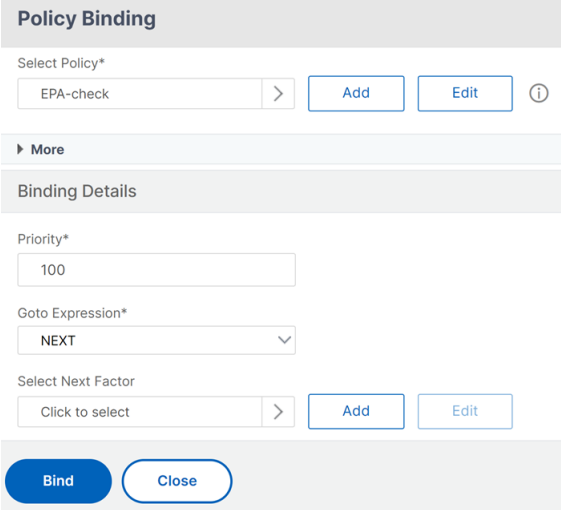


   - Navigate to **Security > AAA - Application Traffic > Authentication Profile** and click **Create**.



4. Bind the advanced EPA policy to the authentication virtual server.

   - Navigate to **Security > AAA –Application Traffic > Authentication Virtual Servers** and select the authentication virtual server.
   - Select the policy in the **Advanced Authentication Policies** section.
   - Click **Bind** in the **Policy Binding** section.



5. Bind the EPA policy to nFactor flow.

   For details about how to add an advanced EPA policy as a factor to the nFactor flow, see EPA scan as a factor in nFactor authentication.

On the CLI

1. Create an action to perform the EPA scan.

```
add authentication epaAction EPA-client-scan -csecexpr "sys.
    client_expr (\"proc_2_firefox\")"
```


The preceding expression scans if the process 'Firefox'is running. The EPA plug-in checks for the process existence every 2 minutes, signified by the digit '2'in the scan expression.

2. Associate the EPA action to an advanced EPA policy.

```
add authentication Policy EPA-check -rule true -action EPA-client-scan
```

3. Configure an authentication virtual server and an authentication profile.

```
add authentication vserver authnvsepa ssl -ip address 10.104.130.129 -port 443
```

```
add Authnprofile_EPA -authnVsName authnvsepa
```

4. Bind the advanced EPA policy to the authentication virtual server.

```
bind authentication vs authnvsepa -policy EPA-check -pr 1
```

Upgrade EPA libraries

To use the NetScaler GUI to upgrade EPA libraries:

1. Navigate to **Configuration > NetScaler Gateway > Update Client Components**.
2. Under **Update Client Components,** click **Upgrade EPA Libraries** link.
3. Choose the required file and click **Upgrade**.

> **Important:**
>
> - In a NetScaler Gateway high availability, the EPA Libraries must be upgraded on both the primary and secondary nodes.
> - In a NetScaler Gateway clustering setup, the EPA Libraries must be upgraded on all the cluster nodes.

For the list of Windows and MAC Supported applications by OPSWAT for NetScaler scans, see https://support.citrix.com/article/CTX234466.

Troubleshooting advanced Endpoint Analysis scans

To help with troubleshooting Advanced Endpoint Analysis scans, the client plug-ins write logging information to a file on client endpoint systems. These log files can be found in the following directories, depending on the user's operating system.

Windows Vista, Windows 7, Windows 8, Windows 8.1, and Windows 10:

C:\Users\<username>\AppData\Local\Citrix\AGEE\nsepa.txt

Windows XP:

C:\Documents and Settings\All Users\Application Data\Citrix\AGEE\nsepa.txt

Mac OS X systems:

~/Library/Application Support/Citrix/EPAPlugin/epaplugin.log

(Where the ~ symbol indicates the relevant macOS user's home directory path.)
(Where the ~ symbol indicates the relevant macOS user's home directory path.)

Ubuntu:

- ~/.citrix/nsepa.txt
- ~/.citrix/nsgcepa.txt

Advanced Endpoint Analysis policy expression reference

July 24, 2024

This topic describes the format and construction of Advanced Endpoint Analysis expressions. The NetScaler Gateway configuration utility automatically builds the expression elements contained here and does not require manual configuration.

Expression format

An Advanced Endpoint Analysis expression has the following format:

`CLIENT.APPLICATION (SCAN-type_ Product-id_ Method-name _ Method-comparator_ Method-param _…)`

Where:

SCAN-type is the type of application being analyzed.

Product-id is the product identification for the analyzed application.

Method-name is the product or system attribute being analyzed.

Method-comparator is the chosen comparator for the analysis.

Method-param is the attribute value or values being analyzed.

Example:

client.application(ANTIVIR_2600_RTP_==_TRUE)

> **Note:**
>
> For non-application scan types, the expression prefix is CLIENT.SYSTEM instead of CLIENT.APPLICATION.

Expression strings

Each of the supported scan types in Advanced Endpoint Analysis uses a unique identifier in the expressions. The following table enumerates the strings for each type of scan.

Scan type	Scan type expression string
Anti-phishing	ANTIPHI
Antivirus	ANTIVIR
Backup Client	BACKUP
Citrix Workspace app (macOS)	MAC-CWA
Citrix Workspace app (Windows)	WIN-CWA
Data Loss Prevention	DATA-PREV
Firewall	FIREWALL
Health Agent	HEALTH
Hard disk Encryption	HD-ENC
Instant Messenger	IM
Web Browser	BROWSER
P2P	P2P
Patch Management	PATCH
MAC address	MAC
Domain check	DOMAIN
Registry Scan	REG
Windows Update Scan	WIN-UPDATE

> **Note:**
>
> For macOS X specific scans, expressions include the prefix MAC- before the method type. Therefore, for antivirus and anti-phishing scans, the methods are MAC-ANTIVIR and MAC-ANTIPHI re-

> spectively.
>
> For example:
>
> client.application(MAC-ANTIVIR_2600*RTP*==_TRUE)

Application scan methods

In configuring Advanced Endpoint Analysis expressions, methods are used to define the parameters of the endpoint scans. These methods include a method name, a comparator, and a value. The following tables enumerate the methods available for use in expressions.

Common Scan Methods:

The following methods are used for multiple types of application scans.

Method	Description	Comparator	Possible values
VERSION*	Specifies version of application.	<, <=, >, >=, !=, ==	Version string
AUTHENTIC**	Check if the application is authentic or not.	==	TRUE
ENABLED	Check if the application is enabled.	==	TRUE
RUNNING	Check if the application is running.	==	TRUE
COMMENT	Comment field (ignored by scan). Delineated by [] within expressions.	==	Any text

* The VERSION string can specify a decimal string of up to four values, such as 1.2.3.4.

** An AUTHENTIC check verifies the authenticity of the binary files for the application.

> **Note:**
>
> You can select a generic version for application scan types. When generic scans are selected, the product ID is 0.

Gateway provides an option to configure Generic scans for each type of software. Using generic scan, an admin can scan the client machine without restricting the scanning check to any particular product.

For Generic scans, scan methods work only if the product installed on the users system supports that scan method. To know which products support a particular scan method, contact NetScaler support.

Unique Scan Methods:

The following methods are unique to the specified types of scans.

Method	Description	Comparator	Possible values
ENABLED-FOR	Check whether anti-phishing software is enabled for the selected application.	`allof`, `anyof`, `noneof`	**For Windows**: Internet Explorer, Mozilla Firefox, Google Chrome, Opera, Safari. **For Mac:** Safari, Mozilla Firefox, Google, Chrome, Opera

Table 2. Antivirus

Method	Description	Comparator	Possible values
RTP	Check whether the real time protection is on or not.	==	TRUE
SCAN-TIME	How many **minutes** since a full system scan was performed.	<, <=, >, >=, !=, ==	Any positive number
VIRDEF-FILE-TIME	How many **minutes** since virus definition file was updated (that is, Number of minutes between virus definition file stamp and current timestamp).	<, <=, >, >=, !=, ==	Any positive number
VIRDEF-FILE-VERSION	Version of definition file.	<, <=, >, >=, !=, ==	Version string
ENGINE-VERSION	Engine version.	<, <=, >, >=, !=, ==	Version string

Table 3. Backup client

Method	Description	Comparator	Possible values
LAST-BK-ACTIVITY	How many **minutes** since last backup activity was completed.	<, <=, >, >=, !=, ==	Any positive number

Table 4. Data loss prevention

Method	Description	Comparator	Possible values
ENABLED	Check whether the application is enabled or not and time protection is on or not on.	==	TRUE

Table 5. Health check agent

Method	Description	Comparator	Possible values
SYSTEM-COMPL	Check whether the system is in compliance.	==	TRUE

Table 6. Hard disk encryption

Method	Description	Comparator	Possible values
ENC-PATH	PATH for checking encryption status.	NO OPERATOR	Any text
ENC-TYPE	Check whether encryption type for specified path.	`allof`, `anyof`, `noneof`	**List with the following options**: UNENCRYPTED, PARTIAL, ENCRYPTED, VIRTUAL, SUSPENDED, PENDING

Table 7. Web browser

Method	Description	Comparator	Possible values
DEFAULT	Check whether set as default browser.	==	TRUE

Table 8. Patch management </caption>

Method	Description	Comparator	Possible values
SCAN-TIME	How many minutes since the last scan for patch was performed.	<, <=, >, >=, !=, ==	Any positive number
MISSED-PATCH	Client system is not missing patches of these types.	`anyof`, `noneof`	ANY Pre-selected (Pre-selected patches on Patch Manager server)
NON			

Table 9. MAC Address

Method	Description	Comparator	Possible values
ADDR	Check whether the client machine MAC addresses are or are not in the given list.	`anyof`, `noneof`	Editable list

Table 10. Domain membership

Method	Description	Comparator	Possible values
SUFFIX	Check whether the client machine exists or does not exist in the given list.	`anyof`, `noneof`	Editable list

Table 11. Numeric registry entry

Method	Description	Comparator	Possible values
PATH	Path for registry check. In the format: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client\EnableAutoUpdate. No escaping of special characters is required. All registry root keys: HKEY_LOCAL_MACHINE, HKEY_CURRENT_USER, HKEY_USERS, HKEY_CLASSES_ROOT, HKEY_CURRENT_CONFIG	NO OPERATOR	Any text

Method	Description	Comparator	Possible values
REDIR-64	Follow 64-bit redirection. If set to TRUE, WOW redirection is followed (that is, Registry path is checked on 32-bit systems but WOW redirected path is checked for 64-bit systems.) If not set, WOW redirection is not followed (that is, the same registry path is checked for 32-bit and 64-bit systems.) For registry entries that are not redirected this setting has no effect. See the following article for the list of registry keys that get redirected on 64-bit systems: http://msdn.microsoft.com/en-us/library/aa384253%28v=vs.85%29.aspx	==	TRUE
VALUE	Expected value for above path. This scan works only for registry types of REG_DWORD and REG_QWORD.	<, <=, >, >=, !=, ==	Any number

EPA scan for MAC addresses

January 8, 2024

Starting from NetScaler release 13.0-88.x, you can configure EPA scan configurations for the allowed or specific MAC addresses. NetScaler uses policy expressions and pattern sets to specify the list of MAC addresses.

Prior to NetScaler release 13.0-88.x, the list of all the allowed MAC addresses had to be specified as part of an EPA expression. If the customers had a huge list of allowed MAC addresses, it was cumbersome to add all the MAC addresses in one expression. Also, there was a limitation on the number of MAC addresses to be added in a single expression.

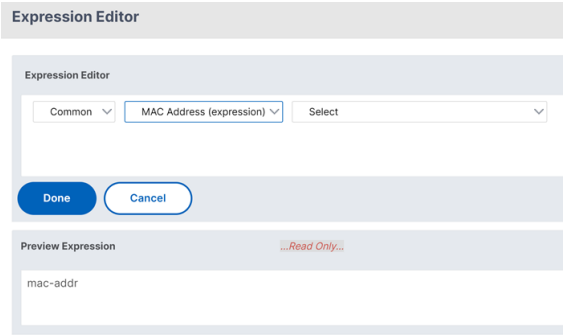
For example,

```
add authentication epaAction epa -csecexpr q/sys.client_expr("
    proc_0_notepad.exe") || sys.client_expr("proc_0_chrome") || sys.
    client_expr("proc_0_firefox") && sys.client_expr("
    sys_0_MAC_ADDR_anyof_1AC89C83BOF7,0250F20A777C[COMMENT: MAC Address]
    ")/
```

Configure the EPA scan for MAC addresses by using the GUI

The **MAC Addresses (expression)** option that was previously available in the **Windows** scan category is now available in the **Common** scan category of the NetScaler GUI. This option enables users to configure an EPA scan for a list of allowed or specific MAC addresses.

> **Note:**
>
> Citrix Secure Access client 22.10.1 and later versions support this method of NetScaler handling the EPA scan configurations on the GUI.



1. Configure a pattern set. For details, see Configuring a Pattern Set.

2. Create a corresponding policy expression for each pattern set.

   When configuring the expression, in the Expression Editor, select **AAA > LOGIN > CLIENT_MAC_ADDR > EQUAL_ANY(string) > Pattern Set**.

   For details on configuring an advanced expression, see Configure advanced policy expressions in a policy.

3. Create an EPA scan for the expression configured in the earlier steps. For details, see Advanced Endpoint Analysis scans.

Configure the EPA scan for MAC addresses by using the CLI

1. Store the MAC addresses inside pattern sets.

   At the command prompt, type;

```
add policy patset <name> [-comment <string>]
```

   Example:

```
add policy patset patset1
bind policy patset patset1 1A-C8-9C-83-BO-F7
bind policy patset patset1 02-50-F2-0A-77-7C ... and so on up to 3K entries.
add policy patset patset2
bind policy patset patset2 1A-2B-3C-4D-5E-6A
bind policy patset patset2 1A-2B-3C-4D-5E-6B ... and so on up to 3K entries.
```

2. Create a corresponding policy expression for each pattern set using AAA.LOGIN.CLIENT_MAC_ADDR.equals_a

   At the command prompt, type;

```
Add policy expression <name> <value> [-comment <string>] [-clientSecurityMessage <string>]
```

   Example:

```
add policy expression exp1 AAA.LOGIN.CLIENT_MAC_ADDR.equals_any("patset1")
add policy expression exp2 AAA.LOGIN.CLIENT_MAC_ADDR.equals_any("patset2")
```

3. Create EPA scans using the configured policy expressions

   At the command prompt, type;

```
add authentication epaAction <name>  -csecexpr <expression>
```

   Example:


```
add authentication epaAction epa -csecexpr q/sys.client_expr("proc_0_notepad.exe") || sys.client_expr("proc_0_chrome")  || sys.client_expr("mac-addr_0_exp1") || sys.client_expr("mac-addr_0_exp2") || sys.client_expr("proc_0_firefox")/
```

Configure a preauthentication policy,

```
add authentication Policy epapol -rule true -action epa
```

Bind the preauthentication policy,

```
bind authentication vserver <name> -policy epapol -priority 10 -gotoPriorityExpression NEXT
```

Points to note

- Configuring an EPA scan for an allowed list of MAC addresses is only applicable for the nFactor authentication flows.
- It is recommended to store not more than 3000 entries in a pattern set.
- The MAC addresses must be configured in the format 1A-2B-3C-4D-5E-6F.
- The format for the EPA scan is `mac-addr\\_0\\_<policy-expression-name>`. In this format, `mac-addr\\_0\\_` is a static value and you must enter the policy expression name after `mac-addr\\_0\\_`.
- The EPA scans can be separated appropriately using the symbols `\( \||, &&)`.
- To add many MAC addresses to a pattern set, you can use the file-based pattern sets import. It is recommended to store a maximum of 3000 entries/pattern set for optimal performance.
- If MAC addresses are present inside a file, you can create a pattern set by using file-based pattern sets import and specifying the appropriate delimiter during the import.

References

- Configure a pattern set.
- Create a pattern set using file-based import.

Manage user sessions

January 8, 2024

You can manage user sessions in the NetScaler GUI from the **Active Users Sessions** dialog box. This dialog box displays a list of active user sessions on the NetScaler Gateway. You can the view end user or

group sessions by using the user name, group name, or IP address. You can also view active sessions within this dialog box. Session information includes:

- User name
- IP address of the user device
- Port number of the user device
- IP address of the virtual server
- Port number of the virtual server
- Intranet IP address assigned to the user

Manage user sessions by using the GUI

To view user sessions

1. In the NetScaler GUI navigation pane, click **NetScaler Gateway**.
2. In the details pane, under Monitor Connections, click **Active user sessions**.
3. In **Active User Sessions**, select from the following types.
   - **Active Users**
   - **Active Groups**
   - **Intranet IP**- When you select Intranet IP, you must enter the intranet IP address and the subnet mask.
4. Click **Continue**.

To refresh the session list

You can retrieve updated information about sessions to NetScaler Gateway.

1. In the NetScaler GUI navigation pane, click **NetScaler Gateway**.
2. In the details pane, under Monitor Connections, click **Active user sessions**.
3. Click **Refresh**.

To end user or group sessions or a session that has a specific Intranet IP address

You can terminate user and group sessions. You can also end a session that has a specific intranet IP address and subnet mask.

1. In the NetScaler GUI navigation pane, click **NetScaler Gateway**.
2. In the details pane, under Monitor Connections, click **Active user sessions**.
3. Under Sessions, select a user, group, or a session that has a specific intranet IP address, and then click **End**.

Manage user sessions by using the CLI

You can use the following CLI commands to view user sessions, end user, or group sessions.

- `show aaa session`- Displays all NetScaler authentication, authorization, and auditing or VPN connections that are bound to the specified user, group, IP address, or IP range.
- `show vpn icaConnection` - Displays all active connections that use the ICA Proxy.
- `show system session` - Displays information about all current system sessions, or about the specified session.

Always On

January 8, 2024

The Always On feature of NetScaler Gateway ensures that users are always connected to the enterprise network. This persistent VPN connectivity is achieved by an automatic establishment of a VPN tunnel.

> **Note**
>
> Always On feature supports captive portals for NetScaler 12.0 Build 51.24 and later.

When to Use Always On

Use Always On when you need to provide seamless VPN connectivity based on user location and have to prevent network access by a user who is not connected to a VPN.

The following scenarios illustrate the use of Always On.

- An employee starts the laptop outside the enterprise network and needs assistance to establish VPN connectivity.
  Solution: When the laptop is started outside the enterprise network, Always On seamlessly establishes a tunnel and provides VPN connectivity.
- An employee using VPN connectivity moves into the enterprise network. The employee is switched to an enterprise network but remains connected to the VPN tunnel, which is not a desirable state.
  Solution: When the employee moves into the enterprise network, Always On tears down the VPN tunnel and seamlessly switches the employee to the enterprise network.
- An employee moves outside the enterprise network and closes the laptop (not shut down). The employee needs assistance to establish VPN connectivity upon resuming work on the laptop.

Solution: When the employee moves outside the enterprise network, Always On seamlessly establishes a tunnel and provides VPN connectivity.

- An enterprise wants to regulate the network access provided to its users when they are not connected to a VPN tunnel.
  Solution: Depending on the configuration, Always On restricts access, allowing users to access only the gateway network.

Understanding the Always On Framework

Always On automatically connects a user to a VPN tunnel that the client has previously established. The first time the user needs a VPN tunnel, the user must connect to the NetScaler Gateway URL and establish the tunnel. After the Always On configuration is downloaded to the client, this configuration drives the subsequent establishment of the tunnel.

The Citrix Secure Access client executable is always running on the client machine. When the user logs on or the network changes, the Citrix Secure Access client determines whether the user laptop is on the enterprise network. Depending upon the location and the configuration, the Citrix Secure Access client either establishes a tunnel or tears down an existing tunnel.

Tunnel establishment is initiated only after the user logs on to the computer. The Citrix Secure Access client uses the client machine's credentials to authenticate with the gateway server and tries to establish a tunnel.

Automatic reestablishment of a Tunnel

Automatic reestablishment of a tunnel is triggered when a VPN tunnel is torn down by NetScaler Gateway.

> **Note**
>
> When endpoint analysis fails, the NetScaler Gateway client does not reattempt tunnel establishment, but does display an error message. If there is an authentication failure, the NetScaler Gateway client prompts the user for credentials.

Supported user authentication methods for seamless tunnel establishment

The supported user authentication methods are as follows:

- User name + AD password: If the Windows user name and password are used for authentication, the Citrix Secure Access client seamlessly establishes the tunnel by using these credentials.

- User certificate: If a user certificate is used for authentication and there is only one certificate on the client machine, Citrix Secure Access client seamlessly establishes a tunnel by using this certificate. If multiple client certificates are installed, the tunnel is established after the user has selected the preferred certificate. Citrix Secure Access client uses this preferred certificate for later tunnels.

  If the smart cards share a user certificate, autologon cannot be achieved if the certificates are dynamically installed in the store as compared to the certificates being present in the store.

- User certificate and User name + AD password: This authentication method is the combination of previously described authentication methods.

> **Note**
>
> All other authentication mechanisms are supported but the tunnel establishment is not seamless for any other authentication methods.

Configuration requirements for Always On

Enterprise administrator must enforce the following for the managed devices:

- User must not be able to end the process/service for specific configuration
- User must not be able to uninstall the package for specific configuration
- User must not be able to change specific registry entries

> **Note**
>
> The feature might not work as expected if the user has administration privileges, as in the case of non-managed devices.

Considerations While Enabling the Always On feature

Review the following section before enabling the Always On feature.

Primary Network Access: When the tunnel is established, the traffic to the enterprise network is decided based on split-tunnel configuration. Other configurations are not provided to override this behavior.

Proxy settings of client machine: Proxy settings of the client machine are ignored for connecting to the gateway server.

> **Note**
>
> The NetScaler appliance's proxy configuration is not ignored. Only the proxy settings of the client machine are ignored. Users who have a proxy configured on their systems are notified that the

> VPN plug-in has ignored their proxy settings.

Configuring Always On

To configure Always On, create an Always On profile on the NetScaler Gateway appliance and apply the profile.

To create an Always On profile:

1. In the NetScaler GUI, navigate to **Configuration > NetScaler Gateway > Policies > AlwaysON.**
2. On the **AlwaysON Profiles** page, click **Add**.
3. On the **Create AlwaysON Profile** page, enter the following details:
   - **Name** –The name for your profile.
   - **Location Based VPN (client-side registry name: LocationDetection) –Select one of the following settings:
     - **Remote** to enable a client to detect whether it is in the enterprise network and establish the tunnel if not in the enterprise network. Remote is the default setting.
     - **Everywhere** to let a client skip the location detection and establish the tunnelregardless of the client's location
   - **Client Control** –Select one of the following settings:
     - **Deny** to prevent the user from logging off and connecting to another gateway. Deny is the default setting.
     - **Allow** to enable the user to log off and connect to another gateway.
   - **Network Access On VPN Failure (client-side registry name: AlwaysOn)** –Select one of the following settings:
     - **Full Access** to allow network traffic to flow to and from the client when the tunnel is not established. Full Access is the default setting.
     - **Only To Gateway** to prevent network traffic from flowing to or from the client when the tunnel is not established. However, the traffic to or from the Gateway IP address is allowed.
       Note: In **Only To Gateway** mode, only the virtual server, DNS, and DHCP traffic are unblocked. To unblock other websites, IP address ranges, or IP addresses, you must set the **AlwaysOnAllowlist** registry with a semicolon-separated list of FQDNs, IP address ranges, or IP addresses.
       For example, mycompany.com,mycdn.com,10.120.67.0-10.120.67.255,67.67.67.67
4. Click **Create** to finish creating your profile.

To apply the Always On profile:

1. In the NetScaler interface, select **Configuration > NetScaler Gateway > Global Settings**.

2. On the Global Settings page, click the **Change Global Settings** link, and then select the **Client Experience** tab.
3. From the **AlwaysON Profile Name** drop-down menu, select the newly created profile, and click **OK**.

Note: Similar configuration can be done in the Session profile to apply the policies at a group level, server lever, or a user level.

Note on IIPs

Machine level tunnel uses certificate-based authentication and the session that is created has the certificate's common name as a user name. So, if device certificates have unique common names, different machines' sessions have different user name and thus different IIPs. Ensure that you generate a device certificate with unique names. Ideally, you must use machine names as the device certificate's common name.

Behavior summary of different configurations for admin users and non-admin users

The following table summarizes the behavior for different configurations. It also details the possibility of certain user actions, which can affect Always On functionality.

networkAccessONVPNFailure	Client control	Non-admin user	Admin user
`fullaccess`	Allow	The tunnel gets established automatically. The user can log off and stay off the network. The user can also point to another NetScaler Gateway.	The tunnel gets established automatically. The user can log off and stay off the enterprise network. The user can also point to another NetScaler Gateway.
`fullaccess`	Deny	The tunnel gets establish automatically. The user cannot log off or point to another NetScaler Gateway.	The tunnel gets established automatically. The user can uninstall the Citrix Secure Access client or move to another NetScaler Gateway.

networkAccessONVPNFailure	Client control	Non-admin user	Admin user
onlyToGateway	Allow	The tunnel gets established automatically. The user can log off (no network access). The user can also point to another NetScaler Gateway, in which case, the access is given only to the newly pointed NetScaler Gateway.	The tunnel gets established automatically. The user can uninstall the Citrix Secure Access client or move to another NetScaler Gateway.
onlyToGateway	Deny	The tunnel gets establish automatically. The user cannot log off or point to another NetScaler Gateway.	The tunnel gets established automatically. The user can uninstall the Citrix Secure Access client or move to another NetScaler Gateway.

Allowing selected URLs when Always On is down

Users can access a few websites even when Always On is down and the network is locked. Admins can use the **AlwaysOnAllowlist** registry to add the websites that you want to enable access to when Always On is down.

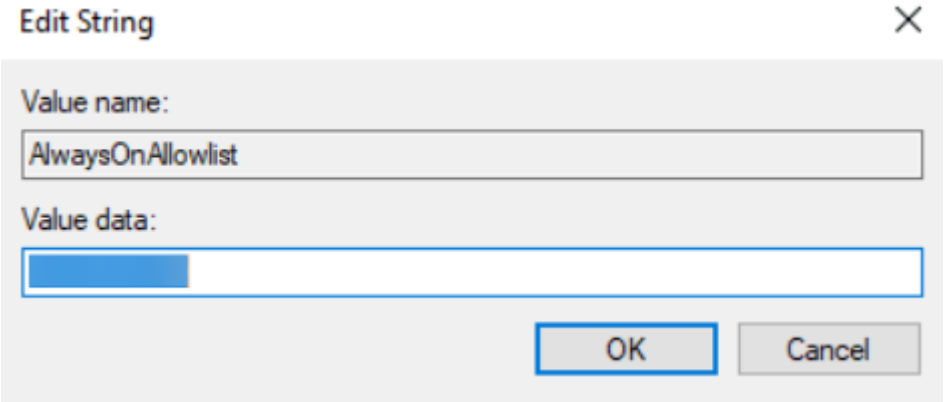
> **Note:**
>
> - **AlwaysOnAllowlist** registry is supported from release 13.0 build 47.x and later.
> - **AlwaysOnAllowlist** registry location is Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client.
> - Wildcard URLs/FQDNs are not supported in the **AlwaysOnAllowlist** registry.

To set the AlwaysOnAllowlist registry

Set the **AlwaysOnAllowlist** registry with a semicolon-separated list of FQDNs, IP address ranges, or IP addresses that you want to allow access to.

Example: example.citrix.com;10.103.184.156;10.102.0.0-10.102.255.100

The following figure displays a sample **AlwaysOnAllowlist** registry.



Always On VPN before Windows Logon (formally Always On service)

January 8, 2024

The **AlwaysOn VPN before Windows Logon** (formally Always On service) feature enables a user to establish a machine level VPN tunnel even before a user logs in to a Windows system. The tunnel remains active until the machine shuts down. After the user logs on, the machine-level VPN tunnel is taken over by a user-level VPN tunnel. After the user logs off, the user-level tunnel is torn and a machine-level tunnel is established. **Always On VPN before Windows Logon** can be configured by using advanced authentication policies only. For details see, Configure Always On VPN before Windows Logon.

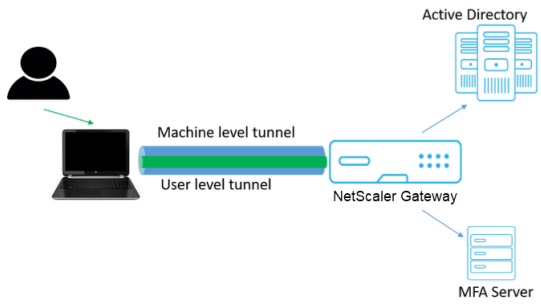
Always On VPN before Windows Logon capabilities

- Administrator can provide a one-time password to the first time users working remotely using which users can connect to the domain controller to change their password.
- Administrator can remotely manages/enforces AD policies to the device even before the user logs in.
- Administrator can provide a granular level of control to users based on the user group after the user logs on. For example, using a user-level tunnel, you can restrict or provide access for a resource to a particular user group.
- The user tunnel can be configured for MFA as per user requirements.
- Multiple users can use the same machine. Access to selective resources are provided based on the user profile. For example multiple users can use a machine in a kiosk without hassle.
- Users working remotely connect to the domain controller to change their password.

- Windows machine can verify the user's login credential using the corporate active directory (AD) and Windows credentials on the machine are not cached. Also, new corporate AD users are enabled to seamlessly log on to the machine.
- Windows machine becomes a part of the corporate intranet even before users log in, allowing IT administrators to access the client machine from the corporate network for debugging purposes.
- VPN tunnel for a Windows machine remains connected even when different users log in or log out to the machine.

Understanding Always On VPN before Windows Logon

The following is the flow of events for the **Always On VPN before Windows Logon** functionality.



- User turns on the laptop. The machine-level tunnel is established towards NetScaler Gateway using the device certificate as identity.
- User logs in to the laptop with AD credentials.
- Post login, user is challenged with MFA.
- Upon a successful authentication, the machine-level tunnel is replaced with the user-level tunnel.
- Once the user logs out, the user-level tunnel is replaced with the machine-level tunnel.

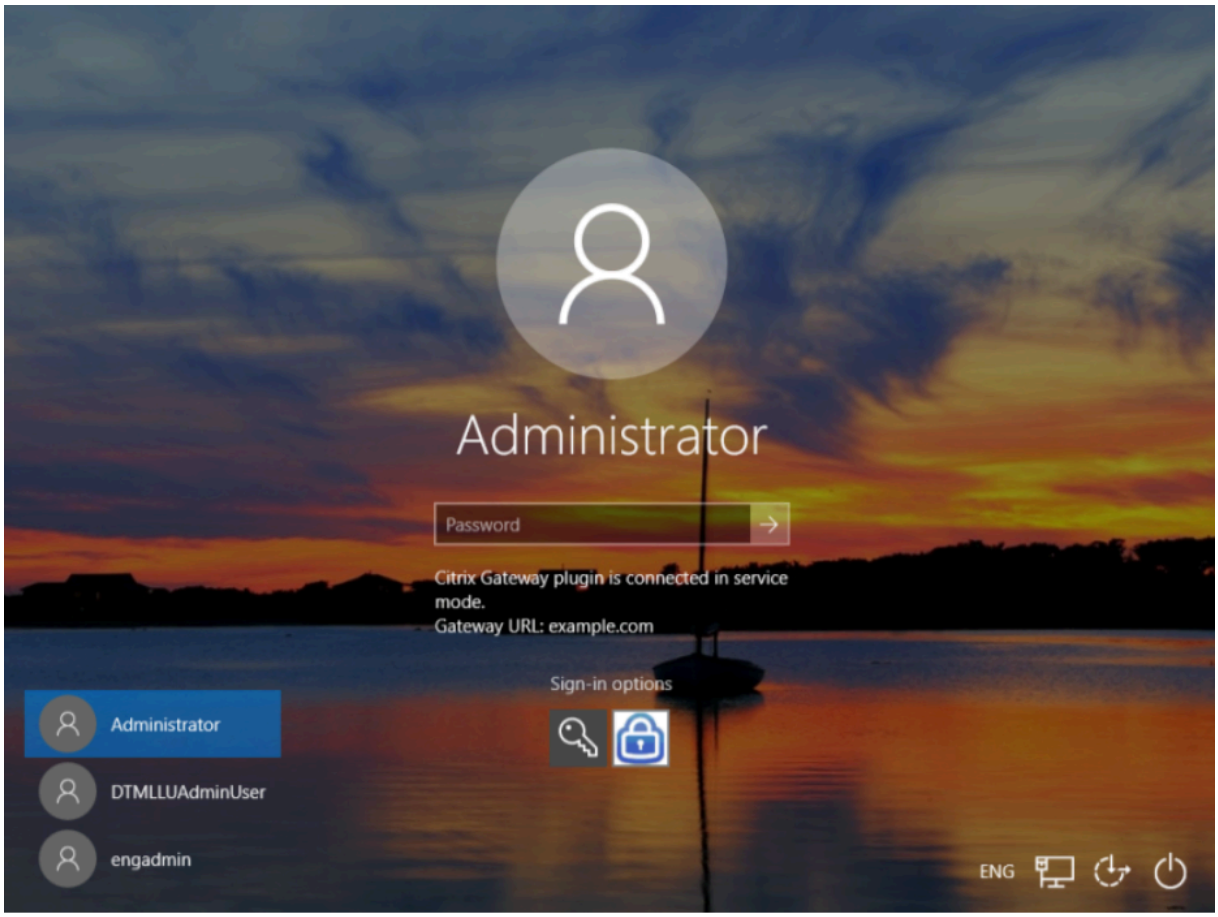
Points to note:

- NetScaler Gateway and VPN plug-in must be version 13.0.41.20 and later.
- If a client machine does not have internet connectivity, **Always On VPN before the Windows Logon** waits for the internet connectivity to become available before establishing the VPN tunnel.
- If a client machine is connected to a captive portal network, **Always On VPN before the Windows Logon** waits for the user to authenticate to the captive portal. After the user logs in and internet access is enabled, **Always On VPN before the Windows Logon** establishes the VPN tunnel.
- Always On VPN before Windows Logon feature supports captive portals for NetScaler.

- If the cached logon credentials option is not enabled for Windows, then users cannot log on in the following scenarios:
  - Machine has no internet connectivity
  - Machine is connected to a captive portal network
- Admins must check the device certificate revocation status before presenting the logon page to the end users.

Windows credential manager screen after Always On VPN before Windows Logon configuration

After the **Always On VPN before Windows Logon** feature is configured, the **Windows credentials manager** screen is modified as follows.



When you click **Sign-in options** on the logon screen, the following information is displayed:

- NetScaler Gateway icon suggests whether the machine is connected to NetScaler Gateway or not.

- Depending on the user configuration mode, one of the following statements is displayed on the logon screen.
  - NetScaler Gateway is connected in service mode
  - NetScaler Gateway is connected in user mode

Configure Always On VPN before Windows Logon

January 8, 2024

This section captures the details to configure **Always On VPN before Windows Logon** by using an advanced policy.

Prerequisites

- NetScaler Gateway and VPN plug-in must be version 13.0.41.20 and later.
- NetScaler Advanced Edition and higher is required for the solution to work.
- You can configure the functionality only by using advanced policies.
- The VPN virtual server must be up and running.

High-level configuration steps

The **Always On VPN before Windows Logon** configuration involves the following high-level steps:

1. Set up a machine level tunnel
2. Set up a user level tunnel (optional)
3. Enable user authentication
   a) Configure the VPN virtual server, install a CA certificate, and bind the certificate key to the virtual server.
   b) Create an authentication profile
   c) Create an authentication virtual server
   d) Create authentication policies
   e) Bind the policies to the authentication profile

Machine level tunnel

Machine level tunnel is established towards NetScaler Gateway using the device certificate as identity. Device certificate must be installed in the client machine under the machine store. This is applicable only for Always On before Windows Logon service.

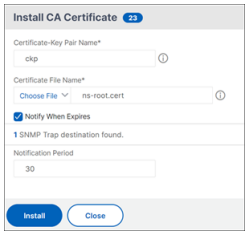
For more details on device certificate, see Use device certificates for authentication.

> **Important:**
>
> If the VPN virtual server on the NetScaler Gateway appliance is configured on a nonstandard port (other than 443), the machine-level tunnel does not work as intended.

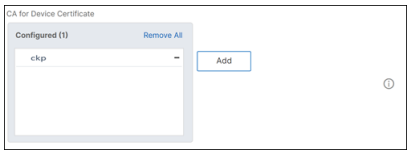
Set up machine level tunnel by using the device certificate

Device certificate based authentication configuration by using the GUI

1. On the **Configuration** tab, navigate to **NetScaler Gateway > Virtual Servers**.
2. On the NetScaler Gateway Virtual Servers page, select an existing virtual server and click **Edit**.
3. Under **Certificate**, click **CA Certicicate**.
4. On the **CA Certificate Binding** page, click **Add** next to the **Select CA Certificate** field, update the requires information, and click **Install**.



5. On the **VPN Virtual Server** page, click the edit icon.
6. In the **Basic Settings** section, click **More**.
7. Click **Add** next to the **CA for Device Certificate** section and click **OK**.



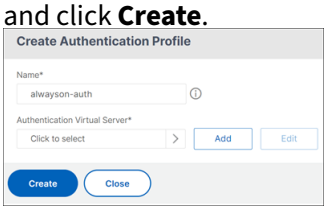
Note: Do not select the **Enable Device Certificate** checkbox.

8. For binding a CA certificate to the virtual server, click **CA certificate** under **Certificate** section. Click **Add Binding** under the **SSL Virtual Server CA Certificate Binding** page.

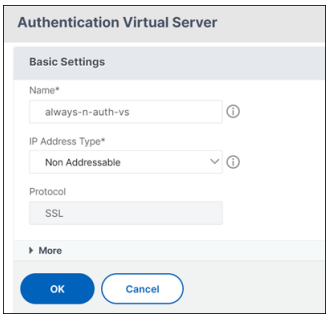
> **Note:**
>
> - The device certificate's subject common name (CN) field must not be empty. If a device tries to log in with empty CN device certificates, its VPN session is created with the user name as "anonymous". In IIP, if multiple sessions have the same user name, previous sessions are disconnected. So, when IIP is enabled, you notice the functionality impact because of an empty common name.

> - All CA certificates (Root and Intermediate) that can potentially sign the Device Certificate issued to clients must be bound under the **CA for Device Certificate** section and also the **CA Certificate binding** section for virtual server in Steps 4 and 5. For more information on linking CA certificate with intermediate / subordinate, see Install, link, and update certificates.
> - If multiple device certificates are configured, the certificate with the longest expiry date is tried for the VPN connection. If this certificate allows the EPA scan successfully, then the VPN connection is established. If this certificate fails in the scan process, the next certificate is used. This process continues until all the certificates are tried.

9. On the **CA Certificate Binding** page, select the certificate.
10. Click **Bind**.
11. Create an authentication virtual server.
    a) On the **VPN Virtual Servers** page, navigate to **Advanced Settings > Authentication Profile** and click **Add**.
    b) On the **Create Authentication Profile** page, assign a name to the authentication profile, and click **Create**.



    c) On the **Authentication Virtual Server** page, assign a name to the authentication virtual server. Select the IP Address type as **Non-Addressable,** and click **OK**.



> **Note:**
>
> The authentication virtual server always remains in the DOWN state.

12. Create an authentication policy.
    a) In the **Advanced Authentication Policies** section of the **Security > AAA-Application Traffic > Authentication Virtual Servers** page, select the authentication policy and click **Add Binding**.

b) On the **Policy Binding** page, click **Add** next to the **Select Policy** field.

c) On the Create Authentication Policy page;

i. Assign a name to the advanced authentication policy.

ii. Select **EPA** from the **Action Type** list.

iii. Click **Add** next to **Action**.

d) On the Create Authentication EPA Action page;

i. Assign a name to the EPA action.

ii. Enter `sys.client_expr("device-cert_0_0")` in the **Expression** field.

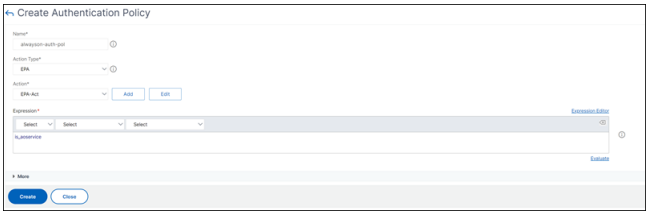
iii. Click **Create**.

13. On the **Create Authentication Policy** page;

a) Assign a name to the authentication policy.

b) Enter **is_aoservice** in the **Expression** field.

c) Click **Create**.



14. On the Policy Binding page, enter **100** in **Priority** and click **Bind**.

Device certificate based authentication configuration by using the CLI

1. Install a CA certificate on a VPN virtual server.

```
add ssl certkey ckp -cert t_CA.cer
```


2. Bind the CA certificate to the VPN virtual server.

```
bind ssl vserver <vServerName> -certkeyName <string> -ocspCheck (
    Mandatory | Optional )
```

Example

```
bind ssl vserver TestClient -CertkeyName ag51.xm.nsi.test.com -CA
    -ocspCheck Mandatory
```

3. Add an authentication virtual server.

```
add authentication authnProfile <name>  {
 -authnVsName <string> }
```

Example

```
add authentication authnProfile always_on -authnVsName
    always_on_auth_server
```

4. Create an authentication EPA action.

```
add authentication epaAction <name> -csecexpr <expression>
```

Example

```
add authentication epaAction epa-act -csecexpr      `sys.
    client_expr("device-cert_0_0")` -defaultgroup epa_pass
```

5. Create an authentication policy

```
add authentication Policy <name> -rule <expression> -action <
    string>
```

Example:

```
add authentication Policy always_on_epa_auth -rule is_aoservice -
    action epa_auth
```

Important:

- The machine-level tunnel configuration is now complete. To set up the user-level tunnel after the Windows Logon, see the section **User Level Tunnel**.
- On the client machine, the device certificate is in the .pfx format. The .pfx certificate is installed on the Windows machine as Windows understand the .pfx format. This file has the certificate and key files. This certificate must be of the same domain which is bound to the virtual server. The .pfx and server certificates and keys can be generated by using the client certificate wizard. These certificates can be used with the certificate authority to generate the respective .pfx with server certificate and domain. The certificate .pfx is installed in the

> computer account in the personal folder. The `show aaa session` command displays the device tunnel on the NetScaler appliance.

User Level Tunnel

Replace a machine-level tunnel with a user-level tunnel by using the GUI

Note: The expression `is_aoservice.not` is applicable from NetScaler Gateway version 13.0.41.20 and later.

1. Configure a policy for user authentication.

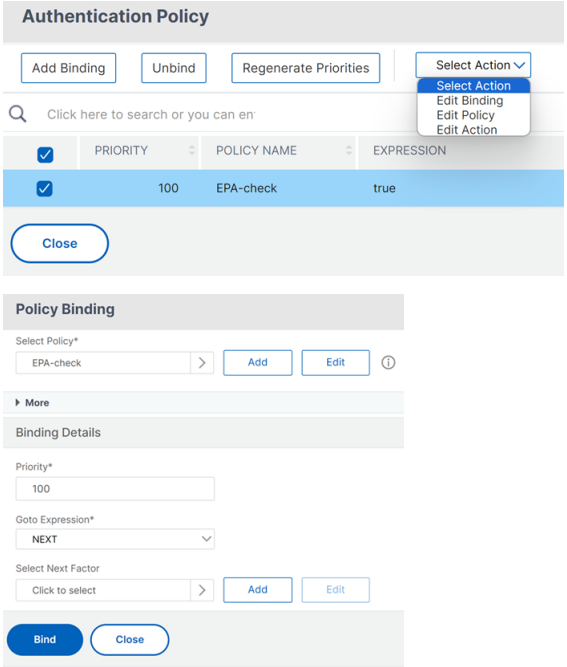
   a) Navigate to **NetScaler Gateway > Virtual Servers** and select a virtual server.

   b) In **Advanced Settings**, click **Authentication Profile**.

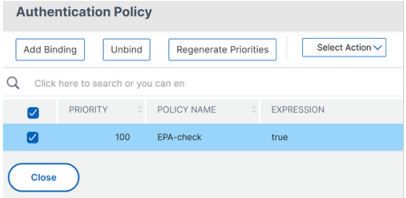
   c) Configure the authentication profile.

   d) On the **Configuration > Security > AAA-Application Traffic > Authentication Virtual Servers** page, select the authentication policy.

   e) In **Select Action**, click **Edit Binding** and change **GoTo Expression** to **NEXT** instead of **END** for the policy bound.



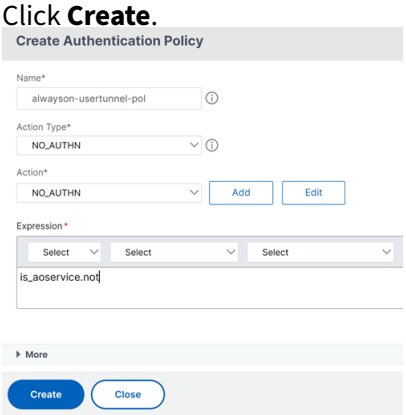
   f) Click **Bind** and then in the **Authentication Policy** page, select the authentication policy and click **Add binding**.



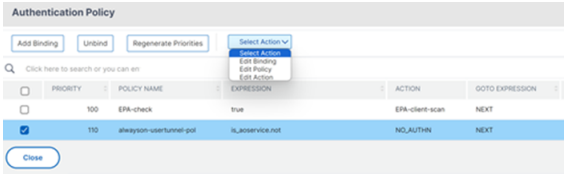
g) On the Policy Binding page, click **Add** next to **Select Policy**.

On the Create Authentication Policy page;

i. Enter a name for the "no authentication"policy to be created.
ii. Select action type as **No_AUTHN**.
iii. Enter **is_aoservice.not** in the **Expression** field.
iv. Click **Create**.



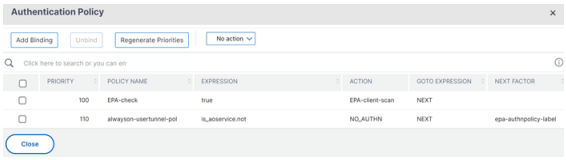
2. In **Select Action**, click **Edit Binding**.



3. On the Policy Binding page, enter **110** in **Priority**. Click **Add** next to **Select Next Factor**.

a) On the Authentication Policy Label page, enter a descriptive name for the policy label, select the login schema, and click **Continue**.
b) In **Select Policy**, click **Add** and create an LDAP authentication policy.
c) Click **Create,** and then click **Bind.**
d) Click **Done,** and then click **Bind**.

In the Authentication Policy page, the **Next Factor** column displays the configured next factor policy.



4. You can configure LDAP policy as the next factor of authentication policy.

   a) On the Create Authentication Policy page, enter a name for the LDAP policy.
   b) Select **Action Type** as **LDAP**.
   c) Enter **Action** as configured LDAP action.

> **Note:**
>
> - For creating login schema XML file, see Login schema XML file.
> - For creating policy labels, see Authenticate the policy label.
> - For creating an LDAP authentication policy, see To configure LDAP authentication by using the configuration utility.

Replace a machine-level tunnel with a user-level tunnel by using the CLI

1. Bind a policy to the authentication virtual server

```
bind authentication vserver <name> -policy <name> -priority  <positive_integer> -gotoPriorityExpression <expression>
```

   Example

```
bind authentication vserver alwayson-auth-vserver -policy alwayson-auth-pol -priority 100 -gotoPriorityExpression NEXT
```

2. Add an authentication policy with the action as `NO_AUTH` and expression `is_aoservice.not`, and bind it to the policy.

```
add authentication Policy <name> -rule <expression> -action <string>

bind authentication vserver <name> -policy <name> -priority <positive_integer> -gotoPriorityExpression <expression>
```

   Example

```
add authentication Policy alwayson-usertunnel-pol -rule is_aoservice.not -action NO_AUTHN

bind authentication vserver alwayson-auth-vserver -policy alwayson-usertunnel-pol -priority 110
```

3. Add a next factor and bind the policy label to the next factor.

```
add authentication policylabel <labelName> -loginSchema <string>

bind authentication  policylabel <string>  -policyName <string>  -priority <positive_integer> -gotoPriorityExpression <expression> -nextFactor <string>
```


Example

```
add authentication policylabel user-tunnel-auth-label -loginSchema singleauth_alwayson

bind authentication policylabel user -policyName alwayson-usertunnel-pol -priority 100
```

4. Configure an LDAP policy and bind it to the user tunnel policy label.

```
add authentication policy <name>  -rule <expression>  -action <string>

bind authentication vserver <vserver_name> -policy <string>  -priorit < positive integer>  gotoPriorityExpression <string>
```

Example

```
add authentication Policy LDAP_new -rule true -action LDAP_new

bind authentication policylabel user-tunnel-auth-label -policyName LDAP_new -priority 100 -gotoPriorityExpression NEXT
```

Client side configuration

The `AlwaysOn, locationDetection, and suffixList registries` are optional and only required if the location detection functionality is needed.

To access registry key entries, navigate to the following path: **Computer>HKEY_LOCAL_MACHINE>SOFTWARE>Ci**
Access Client

Registry key	Registry type	Values and description
AlwaysOnService	REG_DWORD	1 => Establish machine level tunnel but not user level tunnel; 2 => Establish machine level tunnel and user level tunnel

Registry key	Registry type	Values and description
AlwaysOnURL	REG SZ	URL of the NetScaler Gateway virtual server the user wants to connect to. **Example:** `https://xyz.companyDomain.com` **Important:** Only one URL is responsible for machine level tunnel and user-level tunnel. The AlwaysOnURL registry helps both the service and user-level component to work and connect a separate tunnel, that is, machine-level tunnel and user-level tunnel based on the design
AlwaysOn	REG_DWORD	1 => Allow network access on VPN failure; 2=> Block network access on VPN failure
AlwaysOnAllowlist	REG_SZ	Semi-colon separated list of IP addresses or FQDNs which must be whitelisted while the machine is running under the strict mode. **Example:** `8.8.8.8;linkedin.com`
UserCertCAList	REG_SZ	Comma or semi-colon separated list of root CA names, that is the issuer name of the certificate. Used in the context of an Always On service where a customer can specify the list of CAs to choose the client certificate from. **Example**: `cgwsanity.net;xyz.gov.in`
locationDetection	REG_DWORD	1 => To enable the location detection; 0 => To disable the location detection

Registry key	Registry type	Values and description
suffixList	REG SZ	Semicolon separated list of domains and is responsible for checking if the machine is in intranet or not at any given time when location-detection is enabled. **Example:** `citrite.net,cgwsanity.net`

For more information about these registry entries, see Always On.

> **Note:**
>
> When the Always On service is configured, the Always On profile configured on the NetScaler Gateway virtual server or on NetScaler is ignored on the client side. So, ensure that you also enable the `locationDetection` and `AlwaysOn` VPN registries when configuring the Always On service.

Using Advance Policy to Create VPN Policies

January 8, 2024

Classic Policy Engine (PE) and Advance Policy Infrastructure (PI) are two different policy-configuration-and-evaluation frameworks that NetScaler currently supports.

Advance Policy Infrastructure consists of powerful expression language. The expression language can be used to define rules in policy, define various parts of Action, and other entities supported. The expression language can parse through any part of the request or response and also enables you to look deeply through the headers and payload. The same expression language expands and works through every logical module NetScaler supports.

> **Note:**
> You are encouraged to use advanced policies for creating policies.

Why Migrate from Classic Policy to Advance Policy?

Advanced Policy has a rich expression set and offers much greater flexibility than Classic Policy. As NetScaler scales and caters to a vast variety of clients, it is imperative to support expressions which vastly exceed the Advanced Policies. For more information, see Policies and Expressions.

Following are the added capabilities for Advance Policy.

- Ability to access the body of the messages.
- Supports many other protocols.
- Accesses many other features of the system.
- Has more number of basic functions, operators, and data types.
- Caters to the parsing of HTML, JSON, and XML files.
- Facilitates fast parallel multi-string matching (`patsets`, and so forth).

Now the following VPN policies can be configured using Advance Policy.

- Session Policy
- Authorization Policy
- Traffic Policy
- Tunnel Policy
- Audit Policy

Also, End Point Analysis (EPA) can be configured as an nFactor for authentication feature. EPA is used as a gatekeeper for endpoint devices trying to connect to the Gateway appliance. Before the Gateway logon page is displayed on an endpoint device, the device is checked for minimum hardware and software requirements, depending on the eligibility criteria configured by the Gateway administrator. The access to the Gateway is granted based on the outcome of the performed checks. Previously EPA was configured as part of session policy. Now it can be linked to nFactor providing more flexibility, as to when it can be performed. For more information on EPA, see How endpoint policies work topic. For more on nFactor, see nFactor authentication topic.

Use Cases:

Pre-authentication EPA using Advanced EPA

Pre-authentication EPA scan happens before a user provides the logon credentials. For information on configuring NetScaler Gateway for nFactor authentication with pre-authentication EPA scan as one of the authentication factors, see CTX224268 topic.

Post authentication EPA using Advanced EPA

Post authentication EPA scan happens after user credentials are verified. Under the classic policy infrastructure, post authentication EPA was configured as part of the session policy or session action. Under the advanced policy infrastructure, the EPA scan is to be configured as an EPA factor in nFactor authentication. For information on configuring NetScaler Gateway for nFactor authentication with post-authentication EPA scan as one of the authentication factors, see CTX224303 topic.

Pre-authentication and post-authentication EPA using Advanced policies

EPA can be performed before authentication and post authentication. For information on configuring NetScaler Gateway for nFactor authentication with pre-authentication and post-authentication EPA scans, see CTX231362 topic.

Periodic EPA scan as a factor in nFactor authentication

Under classic policy infrastructure, periodic EPA scan was configured as part of session policy action. Under the advanced policy infrastructure, it can be configured as part of the EPA factor in nFactor authentication.

For more information on configuring Periodic EPA scan as a factor in nFactor authentication, click CTX231361 topic.

Troubleshooting:

The following points are to be kept in mind for troubleshooting.

- Classic and Advance policies of the same type (for example, Session policy) cannot be bound to the same entity/bind point.
- Priority is mandatory for all PI policies.
- Advance Policy for the VPN can be bound to all bind points.
- Advance Policy with the same priority can be bound to a single bind point.
- If none of the configured authorization policies get selected, then the global authorization action configured in the VPN parameter is applied.
- In authorization policy, the authorization action is not reversed if the authorization rule fails.

Commonly used Advanced Policy equivalent expressions for Classic Policy:

Classic Policy expressions	Advance Policy expressions
ns_true	true
ns_false	false
REQ.HTTP	HTTP.REQ
RES.HTTP	HTTP.RES
HEADER “foo”	HEADER(“foo”)
CONTAINS ”bar”	.CONTAINS(“bar”) [Note use of “..”]
REQ.IP	CLIENT.IP
RES.IP	SERVER.IP

Classic Policy expressions	Advance Policy expressions
SOURCEIP	SRC
DESTIP	DST
REQ.TCP	CLIENT.TCP
RES.TCP	SERVER.TCP
SOURCEPORT	SRCPORT
DESTPORT	DSTPORT
STATUSCODE	STATUS
REQ.SSL.CLIENT.CERT	CLIENT.SSL.CLIENT_CERT

Configure DTLS VPN virtual server using SSL VPN virtual server

January 8, 2024

You can configure a DTLS VPN virtual server for NetScaler Gateway using the same IP address and port number of a configured SSL VPN virtual server. Configuring DTLS VPN virtual servers enables you to bind the advanced DTLS ciphers and certificates to the DTLS traffic for an enhanced security.

> **Important:**
>
> - By default, the DTLS functionality is set to ON for the existing SSL VPN virtual server. Disable the functionality for the server before creating the DTLS VPN virtual server.
> - SNI for DTLS gateway virtual server is supported in NetScaler Gateway release 13.0 build 64.x and later.
> - Starting from NetScaler release 13.0 build 79.x, the `helloverifyrequest` parameter is enabled by default. Enabling the `helloverifyrequest` parameter on the DTLS profile helps mitigate the risk of an attacker or bots overwhelming the network throughput, potentially leading to outbound bandwidth exhaustion. That is, it helps mitigate the DTLS DDoS amplification attack. For details about the `helloverifyrequest` parameter, see DTLS profile.
> - When handling the UDP traffic, the NetScaler appliance memory consumption increases if the back-end servers push a lot of traffic. As a result, the NetScaler appliance cannot push this traffic to the client because of the TCP MUX connection on the client side. In such cases,

> Citrix recommends that you use the DTLS protocol.

Points to note

- DTLS VPN virtual server on a NetScaler Gateway appliance can be configured from release 13.0 build 58.x.
- Before you configure a DTLS VPN virtual server on a NetScaler Gateway appliance, you must have configured an SSL VPN virtual server on the appliance.
- The DTLS VPN virtual server uses the IP address and the port number of the configured SSL VPN virtual server.
- If the DTLS handshake fails, the connection falls back to TLS.
- To use DTLS only, you can disable TLS by binding only the DTLS ciphers to the DTLS traffic.
- DTLS multiplexing is not supported when TCP traffic is tunneled over VPN.

Configure a DTLS VPN virtual server by using the GUI

1. On the Configuration tab, navigate to **NetScaler Gateway > Virtual Servers**.
2. On the **NetScaler Gateway Virtual Servers** page, select the existing SSL VPN virtual server and click **Edit**.
3. On the **VPN Virtual Server** page, click the edit icon and clear the **DTLS** checkbox and click **OK**.
4. Navigate back to **NetScaler Gateway > Virtual Servers** and click **Add**.
5. Under **Basic Settings**, enter the values for the following fields and Click **OK**.
   - Name - A name for the DTLS VPN virtual server
   - Protocol - Select DTLS
   - IP Address –Enter the SSL VPN virtual server IP address
   - Port –Enter the SSL VPN virtual server port number
6. On the **NetScaler Gateway Virtual Servers** page, select the virtual server that you added previously and click **Edit**.
7. Under **Certificates**, click the arrow icon to select the required cert key.
8. In the **Server Certificate Binding > Select Server Certificate**, select an existing SSL cert key or create one.
9. Click **Bind** on the **Server Certificate Binding** page.

> **Note:**
>
> - To use DTLS 1.2, click the edit icon under SSL Parameters and select the **DTLS 1.2** checkbox.
> - Server name indication (SNI) is supported for VPN virtual server of type DTLS.

Configure a DTLS VPN virtual server by using the CLI

At the command prompt, type the following set of commands:

```
set vpn vserver <ssl vpnvserver name> -dtls off
add vpn vserver <dtls vpnvserver name> dtls <ssl vpn vserver IP> <ssl
    vpn vserver port>
bind ssl vservser <dtls vpnvserver name> -certkeyName <existing ssl
    cert key or newly created cert key>
```

DTLS 1.0 works as usual, to use DTLS 1.2, type the following command:

```
set ssl vserver < dtls vpnvserver name > -dtls12 ENABLED
```

Example

```
set vpn vserver vpnvserver  -dtls off
add vpn vserver vpnvserver_dtls dtls 10.108.45.220 443
bind ssl vservser vpnvserver_dtls -certkeyName sslcertkey
set ssl vserver vpnvserver_dtls -dtls12 ENABLED
```

To enable SNI for the DTLS type VPN virtual server, type the following command:

```
set ssl vserver <vServerName>@ [-SNIEnable ( ENABLED | DISABLED )
bind ssl vservser <dtls vpnvserver name> -certkeyName <existing ssl
    cert key or newly created cert key> <-SNICert>
```

Example

```
set ssl vserver _XD_10.106.40.225_443_DTLS -sniEnable eNABLED
bind ssl vserver _XD_10.106.40.225_443_DTLS -certkeyName "Insight/*.
    insight.net.cer_CERT_" -snICert
```

Supported DTLS VPN virtual server parameters

Only the following parameters are supported for the VPN virtual server of type DTLS.

- Ipaddress
- Port
- State
- Double hop
- downstateflush

- Comment
- Appflowlog
- Icmpvsrresponse

Unsupported DTLS VPN virtual server parameters

The following parameters are not supported for the VPN virtual server of type DTLS.

- LinuxEPAPluginUpgrade
- WindowsEPAPluginUpgrade
- maxAAAUsers
- icaProxySessionMigration
- loginOnce
- cginfraHomePageRedirect
- logoutOnSmartcardRemoval
- l2Conn
- MacEPAPluginUpgradeRHIstate
- icaOnly
- maxLoginAttempts
- failedLoginTimeout
- vserverFqdn
- deviceCert
- rdpServerProfileName
- pcoipVserverProfileName
- tcpProfileName
- netProfile
- authnProfile
- Listenpriority
- Listenpolicy
- ipset
- certkeyNames

Configure a DTLS virtual server using the XenApp and XenDesktop wizard

1. Click **XenApp and XenDesktop** under **Integrate with Citrix Products**.
2. On the XenApp and XenDesktop setup wizard, select **StoreFront** and click **Continue**.
3. On the **NetScaler Gateway Settings** page, enable the **Configure a DTLS Listener for this VPN VServer** checkbox and click **Continue**.

   The DTLS Listener is now configured.

4. In Server Certificate, click **Choose File** to select server certificate and click **Continue**.
5. Specify the certificate file and Key file name and click **Continue**.
6. Under the **StoreFront** section, provide the values for the required parameters as follows and click **Continue**.
7. Under the **Authentication** section, provide the values for the required parameters as follows and click **Test Connection**.

   Ensure that the server is reachable, provide Time out value and Server Logon Name Attribute, and click **Continue**.
8. Click **Done** to complete the configuration.

Limitations

- DTLS 1.2 is supported on Windows clients only.
- VPN virtual server with DTLS does not support IPv6 addresses.
- SSL policy and SSL profile are not supported on a DTLS VPN virtual server. Also, the binding of VPN virtual server policy is not supported.
- The NetScaler Gateway DTLS VPN virtual server does not support the following features. However, the NetScaler Gateway SSL VPN virtual server supports these features:
  - Unified Gateway with content switching virtual server
  - UDP MUX
  - UDP Video
  - UDP Audio
  - PCOIP
- The `stat vpn vserver` command related to the statistics for the DTLS VPN virtual server is not supported.
- HSM keys are not supported with the DTLS virtual server.
- Cluster configuration is not supported.

Integrating with NetScaler products

January 8, 2024

If you are a system administrator responsible for installing and configuring NetScaler Gateway, you can configure the appliance to support Citrix Endpoint Management, StoreFront, and the Web Interface.

Users can connect directly to Endpoint Management from the internal network or from a remote location. When users connect, they can access their web, SaaS, and mobile apps. They can also support documents located in ShareFile from any device.

To allow user connections to a server farm through NetScaler Gateway, you configure settings in either StoreFront or the Web Interface, and on NetScaler Gateway. When users connect, they have access to published applications and virtual desktops.

The configuration steps for integrating NetScaler Gateway with Endpoint Management, StoreFront, and the Web Interface assume the following:

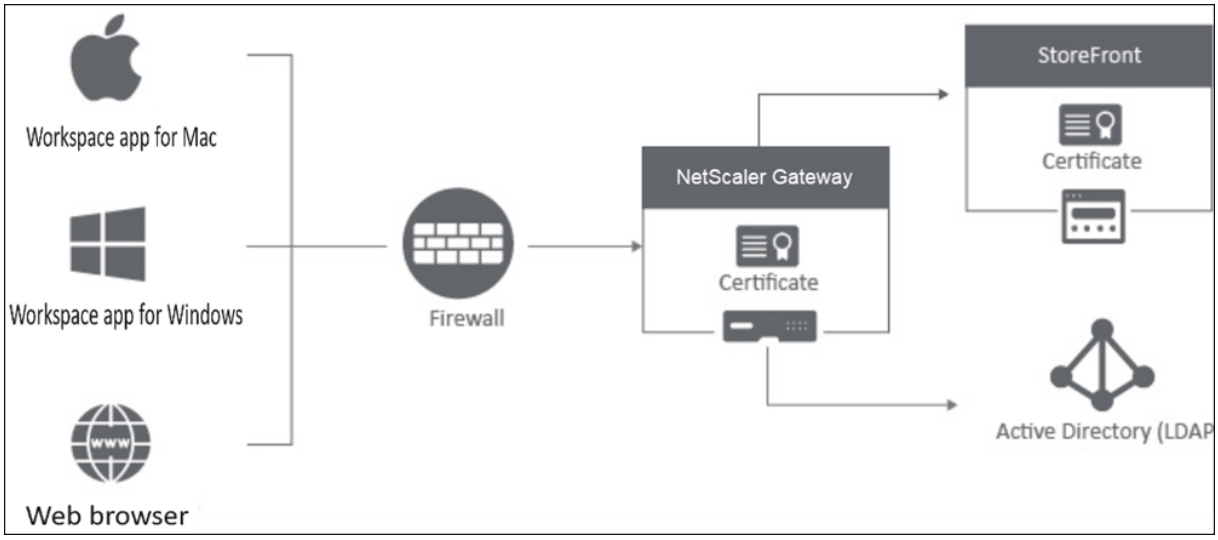
- NetScaler Gateway resides in the DMZ and is connected to an existing network.
- NetScaler Gateway is deployed as a standalone appliance and remote users connect directly to NetScaler Gateway.
- StoreFront, Endpoint Management, Citrix Virtual Apps, Citrix Virtual Desktops, and the Web Interface reside in the secure network.
- ShareFile is configured in Endpoint Management. For more information about ShareFile, see ShareFile topic and Configuring ShareFile for User Access topic.

How you deploy StoreFront and Endpoint Management depends on the apps you provide to mobile devices. If users have access to MDX apps that are wrapped with the MDX Toolkit, Endpoint Management resides in front of StoreFront in the secure network. If you are not providing access to MDX apps, StoreFront resides in front of Endpoint Management in the secure network.

Integrate NetScaler Gateway with StoreFront

January 8, 2024

This article describes how to create a NetScaler Gateway virtual server for remotely accessing StoreFront, for users who are using Citrix Workspace app or a web browser.



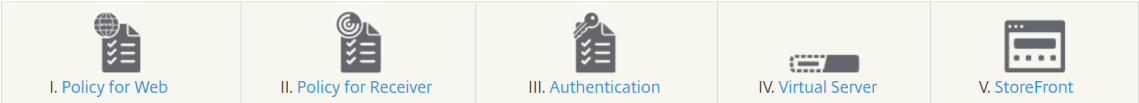
Users connect to NetScaler Gateway through a web browser or Citrix Workspace app. NetScaler Gateway authenticates users based on the configured policies. If the authentication is successful, then NetScaler Gateway enables the users to single sign-on to the store and proxies the StoreFront store to the user.

> **Important:**
>
> We recommend that you do not use the Citrix Virtual Apps and Desktops wizard to integrate NetScaler Gateway with StoreFront as it creates an invalid configuration by using the classic authentication policies (deprecated).

Configure NetScaler Gateway to use with StoreFront

To integrate NetScaler Gateway with StoreFront, complete the following steps:

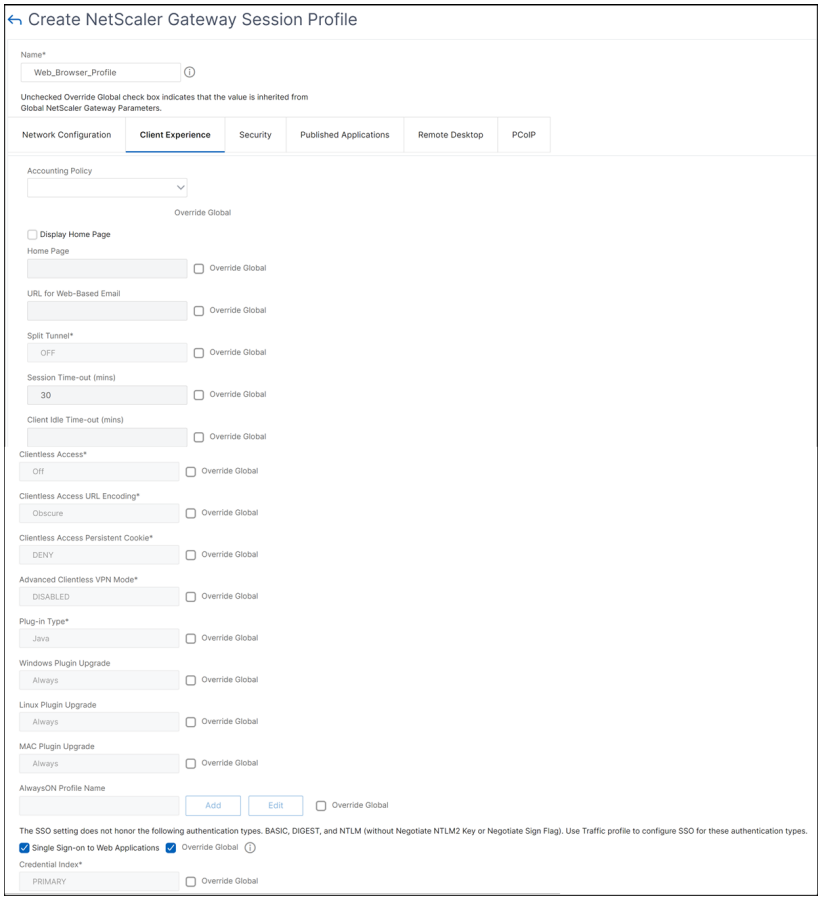
1. Create a session policy for web browser-based access
2. Create a session policy for Citrix Workspace app-based access
3. Create an authentication profile
4. Create a NetScaler Gateway virtual server
5. Add the NetScaler Gateway instance on StoreFront



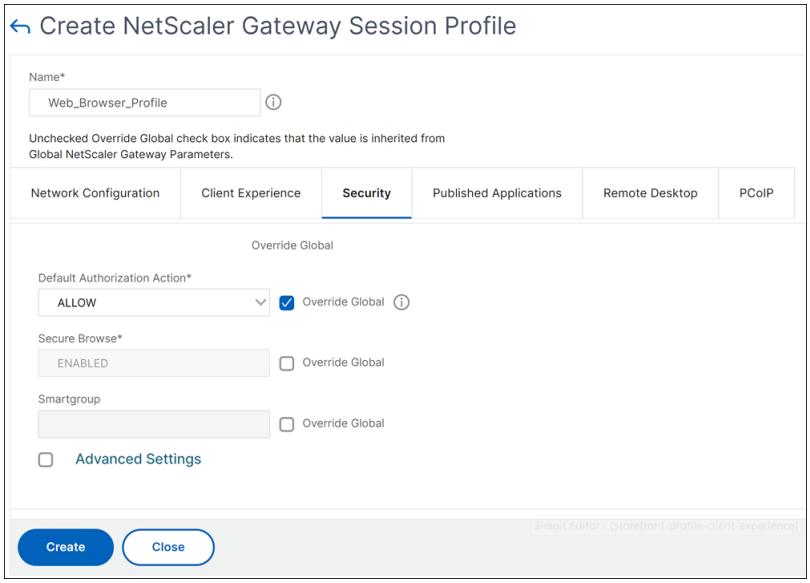
1. Create a session policy for web browser-based access

1. Navigate to **Configuration > NetScaler Gateway > Policies > Session**.

2. In the **Session Profiles** tab, click **Add**.
3. Assign a name to the session profile.
4. In the **Client Experience** tab, enable the following settings:
   - **Plug-in Type**: The plug-in type is set to **Java**, by default. Although this setting is optional, it is recommended if sers want to disable full VPN.
   - **Single Sign-on to Web Application**: By selecting this option, when a user logs on to NetScaler Gateway, it forwards the credentials to the StoreFront website. This setting avoids users from having to enter their credentials twice. However, you must also enable the Pass-through from NetScaler Gateway authentication method on StoreFront. Disable this option if you require users to log on to NetScaler Gateway and the StoreFront store with different credentials.

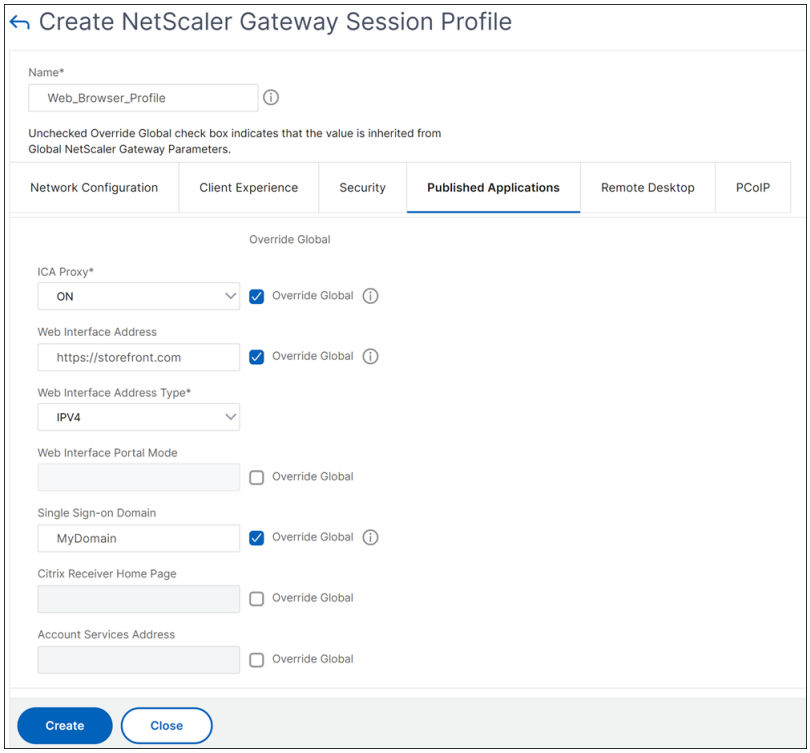


5. In the **Security** tab, enable **Default Authorization Action** and set it to **ALLOW**.



6. In the **Published Applications** tab, enable the following settings:

   - **ICA Proxy**: Set to ON.
   - **Web Interface Address**: FQDN of the StoreFront server followed by the path to the store website.
   - **Single Sign-on Domain**: If you only use one domain, optionally enter the NetBIOS name for the domain.

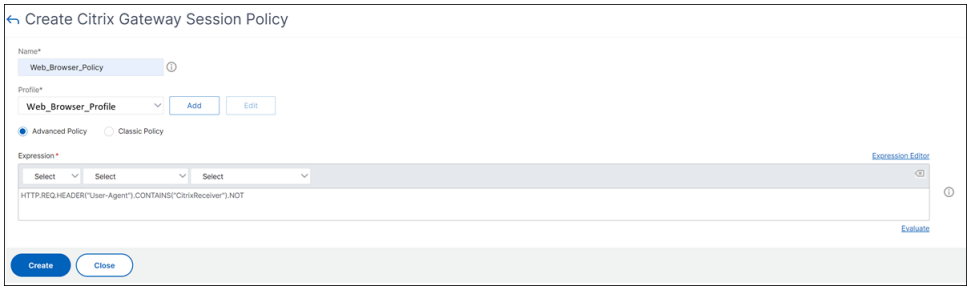


7. Click **Create**.

8. In the **Session Policies** tab, click **Add**. The session policy is required for NetScaler to differentiate between the web browser-based and Citrix Workspace app-based connections. This policy is applied to web browser-based connections.
9. In **Name**, assign a name to session policy.
10. In **Profile**, select the session profile that you created.
11. Click the **Advanced Policy** option and enter the following syntax under **Expression**:

    ```
    HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
    ```

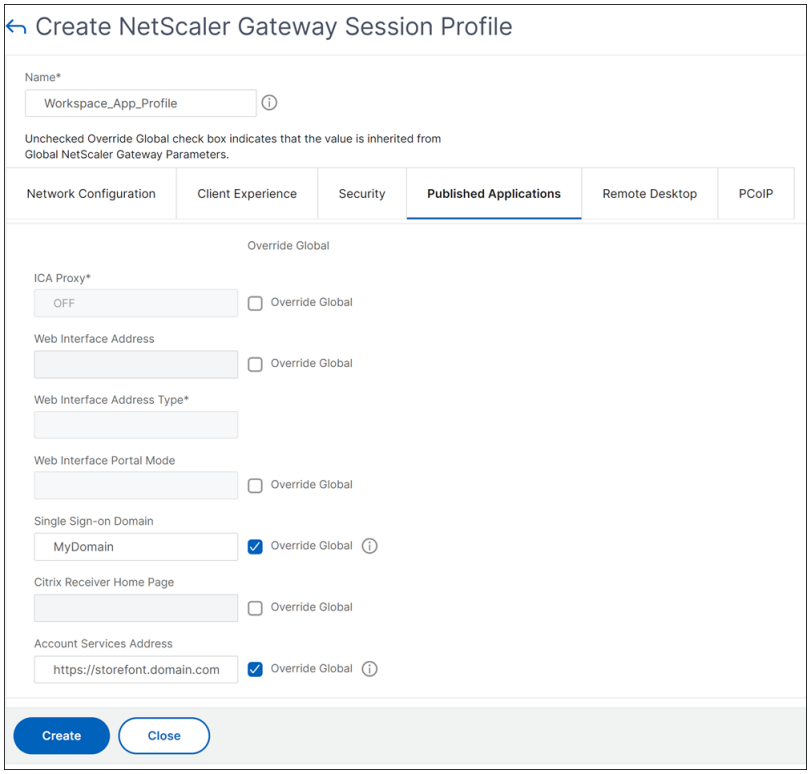
12. Click **Create**.



For more details about NetScaler Gateway session policies, see Session policies.

2. Create a session policy for Citrix Workspace app-based access

Repeat the preceding steps to create a session policy and session profile for Citrix Workspace app-based access. However, in the **Published Applications** tab, instead of configuring the web interface address, you must configure the **Account service address** setting. This step requires you to provide the FQDN of the StoreFront server. Citrix Workspace app uses this address to discover the stores that are available on the server.



3. Create an authentication profile

Create an authentication profile on NetScaler based on the type of authentication method you need to configure.

Althought this step is optional, we recommend it as a good practice to use NetScaler Gateway to authenticate identity of the users before granting access to StoreFront.

Refer to Authentication and Authorization for more details.

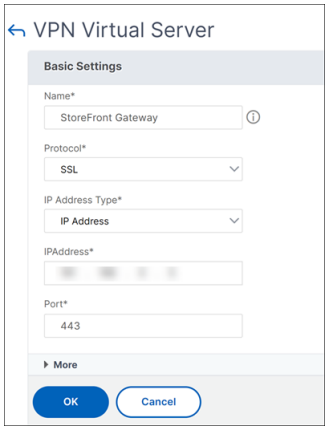
4. Create a NetScaler Gateway virtual server

1. Navigate to **NetScaler Gateway > Virtual Servers**.
2. Click **Add** to add a NetScaler Gateway virtual server.
3. Assign a name and address to the virtual server.

   > **Note:**
   >
   > If you choose not to use NetScaler Gateway to authenticate the users, click **More** and clear the **Enable Authentication** checkbox.

4. Under **Certificate**, Click **Server Certificate**.

5. Upload a server certificate and click **Bind**.
6. Add the session policies:
   a) Under **Policies**, click **+**.
   b) From the **Choose Policy** drop-down list, select **Session**. From the **Type** drop-down list, select **Request** and then click **Continue**.
   c) Under **Policy Binding**, click **Select Policy** and select the web browser-based session policy and the Citrix Workspace app-based session policy that you previously created and click **Bind** to bind the session policies to the virtual server.
7. Under **Published Applications**, click **STA Server**. Specify at least one Security Ticket Authority (STA) URL. If you are using Citrix Virtual Apps and Desktops, enter the URLs of the Desktop Delivery Controllers. If you are using Citrix DaaS, enter the URLs of the Citrix Cloud Connectors.
8. Under **Authentication Profile**, select the authentication profile you created. This step is required because classic policies are no longer supported.
9. Click **Done**.



5. Add a NetScaler Gateway instance on StoreFront

For instructions on how to add a NetScaler Gateway instance on StoreFront, see Configure NetScaler Gateways.

References

For more details on StoreFront and NetScaler Gateway integration, refer to the following topics:

- Add NetScaler Gateway
- Designing StoreFront and NetScaler Gateway Integration

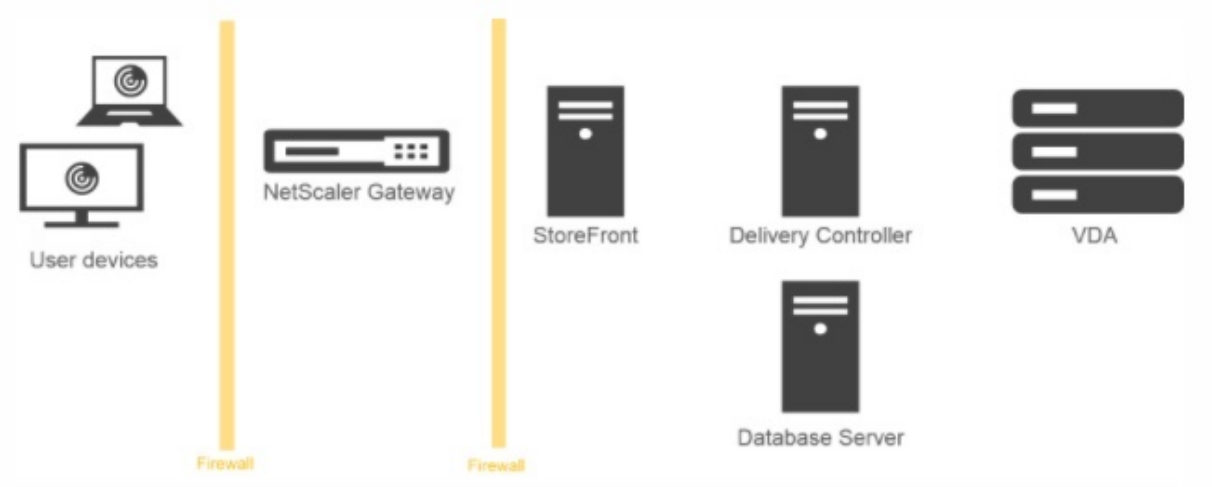
Integrate NetScaler Gateway with Citrix Virtual Apps and Desktops

January 8, 2024

StoreFront servers are deployed and configured to manage access to published resources and data. For remote access, adding NetScaler Gateway in front of StoreFront is recommended.

> **Note**
>
> For detailed configuration steps on how to integrate Citrix Virtual Apps and Desktops with NetScaler Gateway, see the StoreFront documentation.

The following diagram illustrates an example of a Citrix simplified Citrix deployment that includes NetScaler Gateway. NetScaler Gateway communicates with StoreFront to protect apps and data delivered by Citrix Virtual Apps and Desktops. The user devices run Citrix Workspace app to create a secure connection and access their apps, desktops, and files.



Users log on and authenticate using NetScaler Gateway. NetScaler Gateway is deployed and secured in the DMZ. Two-factor authentication is configured. Based on the user credentials, users are provided with the relevant resources and applications. Applications and data are on appropriate servers (not shown on the diagram). Separate servers used for security sensitive applications and data.

Deploying with Citrix Endpoint Management, Citrix Virtual Apps and Desktop

January 8, 2024

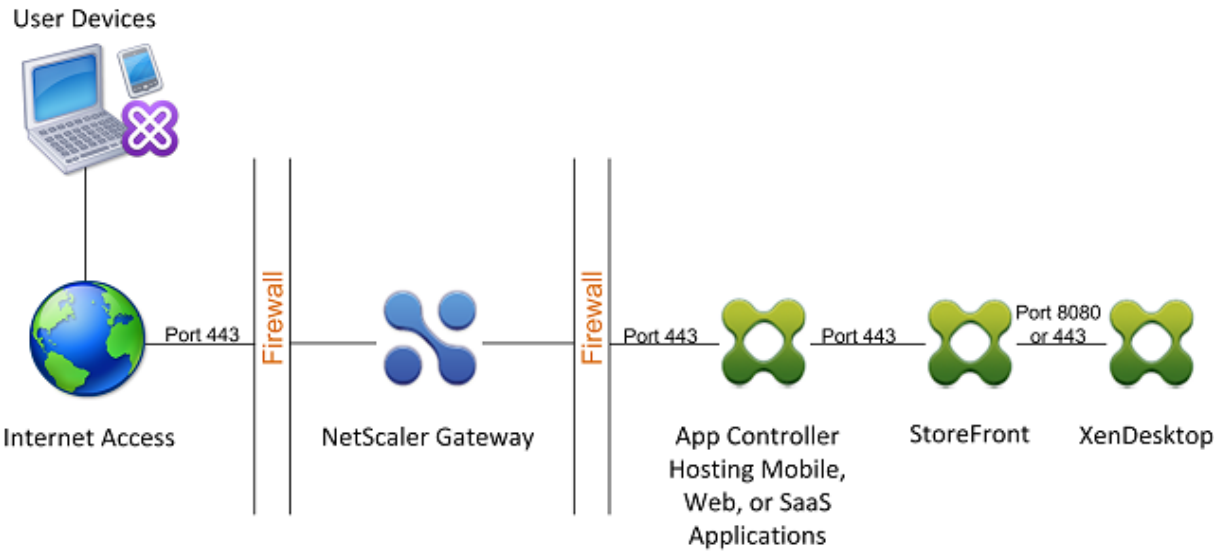
You can have users connect to Windows, web, SaaS, and mobile applications and virtual desktops hosted in your network. You can provide access to your applications and desktops for remote and internal users by using NetScaler Gateway, Citrix Endpoint Management, and Citrix Virtual Apps and Desktops. NetScaler Gateway authenticates users and then allows them to access their applications by using the Citrix Workspace app or Secure Hub.

Users connect to their Windows-based apps published in Citrix Virtual Apps and virtual desktops published in Citrix Virtual Desktops by using Citrix Workspace app and StoreFront.

Citrix Endpoint Management contains Citrix Endpoint Management, which allows users to connect to web, SaaS, and MDX applications. Endpoint Management allows you to manage web, SaaS, and MDX applications for single sign-on (SSO), along with ShareFile documents. You install Endpoint Management in the internal network. Remote users connect to Endpoint Management through NetScaler Gateway to access their applications and ShareFile data. Remote users can connect with either the Citrix Secure Access client, Citrix Workspace app, or Secure Hub to access applications and ShareFile. Users who are in the internal network can connect directly to Endpoint Management by using the Citrix Workspace app. The following figure shows NetScaler Gateway deployed with Endpoint Management and StoreFront.

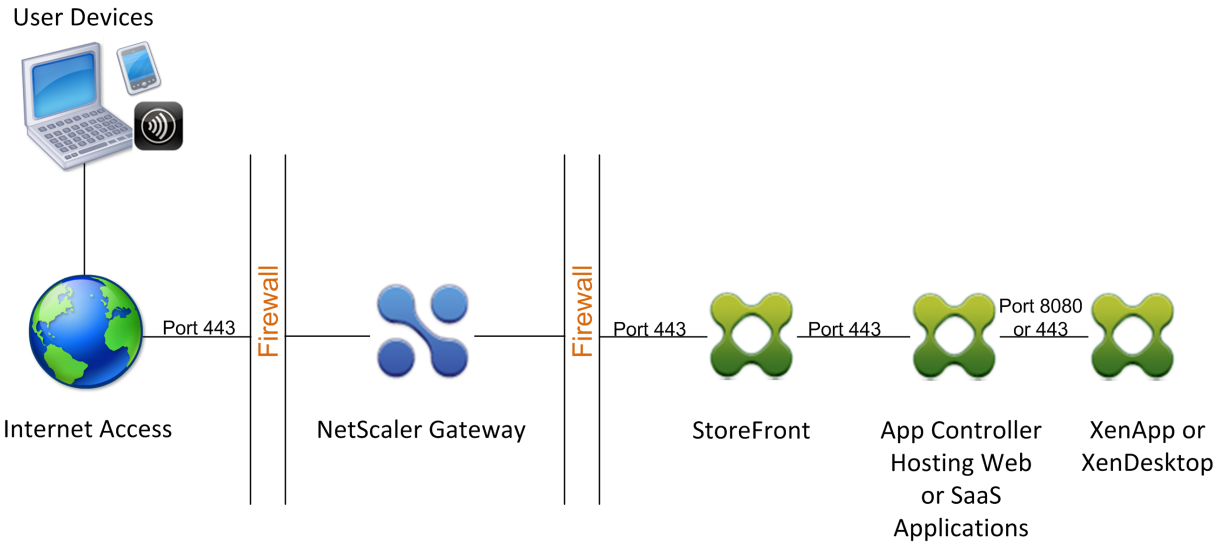
If your deployment provides access to MDX applications from Endpoint Management and access to Windows-based applications from StoreFront, you deploy Endpoint Management in front of StoreFront as shown in the following illustration:

Figure 1. Deploying NetScaler Gateway with Endpoint Management in Front of StoreFront



If your deployment does not provide access to MDX applications, StoreFront resides in front of Endpoint Management, as shown in the following illustration:

Figure 2. Deploying NetScaler Gateway with StoreFront in Front of Endpoint Management



With each deployment, StoreFront and Endpoint Management must reside in the internal network and NetScaler Gateway must be in the DMZ. For more information about deploying Endpoint Management, see Installing Endpoint Management topic.
For more information about deploying StoreFront, see StoreFront topic.

Configuring Settings for Your Citrix Endpoint Management Environment

January 8, 2024

The NetScaler for Citrix Endpoint Management wizard guides you through the configuration of NetScaler features for your Citrix Endpoint Management deployment. You can use the wizard to:

- **Set up a Micro VPN.** In this scenario, remote users can access apps and desktops in the internal network.
  - For Citrix Endpoint Management MAM-only mode, you must use NetScaler Gateway for authentication.
  - For MDM deployments, Citrix recommends NetScaler Gateway for mobile device VPN.
  - For ENT deployments, if a user opts out of MDM enrollment, the device operates in the legacy MAM mode and enrolls using the NetScaler Gateway FQDN.
- **Configure certificate-based authentication.** The default configuration for Citrix Endpoint Management is user name and password authentication. To add another layer of security for enrollment and access to the Citrix Endpoint Management environment, consider using certificate-based authentication.

- **Load balance Citrix Endpoint Management servers.** NetScaler load balancing is required for all Citrix Endpoint Management device modes if you have multiple Citrix Endpoint Management servers or if the Citrix Endpoint Management is inside your DMZ or internal network (and therefore traffic flows from devices to NetScaler to Citrix Endpoint Management). In this scenario, the NetScaler appliance resides in the DMZ between the user device and the Citrix Endpoint Management servers to load balance encrypted data sent from mobile devices to the Citrix Endpoint Management servers.
- **Load balance Microsoft Exchange servers with email filtering.** In this scenario, the NetScaler appliance is between the user device and the Citrix Endpoint Management NetScaler Connector (XNC), and between the user device and the Microsoft Exchange CAS servers. All requests from user devices go to the NetScaler Gateway appliance, which then communicates with the XNC to retrieve information about the device. Depending on the response from the XNC, the NetScaler appliance either forwards the request from a whitelisted device to the server in the internal network, or drops the connection from a blacklisted device.
- **Load balance ShareFile StorageZones Connectors based on the type of content requested.** This scenario prompts you for basic information about your storage zones controller environment and then generates a configuration that does the following:
  - Load balances traffic across storage zones controllers.
  - Provides user authentication for StorageZones Connectors.
  - Validates URI signatures for ShareFile uploads and downloads.
  - Terminates SSL connections at the NetScaler appliance.

For more information about configuring ShareFile, see Configure NetScaler for storage zones controller.

> **Important:**
>
> Before you use the Citrix Endpoint Management wizard, be sure to refer to these Citrix Endpoint Management Deployment articles for design and deployment information and recommendations:
>
> Citrix Endpoint Management Integration
>
> Integrating with NetScaler Gateway and NetScaler
>
> SSO and Proxy Considerations for MDX Apps
>
> Authentication
>
> You can use the NetScaler for Citrix Endpoint Management wizard only once. If you want multiple Citrix Endpoint Management instances, such as for test, development, and production environments, you must configure NetScaler for the additional environments manually. The following support articles list the commands run by the wizard and provide instructions for running them

> to create a NetScaler instance:
>
> Commands Generated by Citrix Endpoint Management Wizard on NetScaler - SSL Bridge
>
> Commands Generated by Citrix Endpoint Management Wizard on NetScaler - SSL Offload

License requirements for NetScaler features

You must install licenses to enable the following NetScaler features:

- Citrix Endpoint Management MDM load balancing requires a NetScaler standard license.
- ShareFile load balancing with StorageZones requires a NetScaler standard license.
- Exchange load balancing requires a NetScaler license or an Advanced license with the addition of an Integrated Caching license.

NetScaler for Citrix Endpoint Management wizard

This section provides an example of using the NetScaler for Citrix Endpoint Management wizard to:

- Set up micro VPN access for remote user connections to Citrix Endpoint Management-managed resources in your internal network
- Configure certificate-based authentication. For information about obtaining and installing a public SSL certificate, see Installing and Managing Certificates.
- Configure load balancing for Citrix Endpoint Management servers.

To use the wizard:

1. In the NetScaler GUI, click the **Configuration** tab and then click **XenMobile** in the **Integrate with Citrix Products** section.
2. Select your Citrix Endpoint Management version and then click **Get Started**.
3. Select the features that you want to configure. You can use this wizard only once, so must perform the subsequent configuration manually. These instructions assume that you select the following settings: **Access through NetScaler Gateway** (for Citrix Endpoint Management running in ENT or MAM modes) and **Load Balance Citrix Endpoint Management Servers**.
4. On the **NetScaler Gateway Configuration** page, enter values for the external facing NetScaler Gateway IP address, port, and virtual server name.
5. On the **Server Certificate for NetScaler Gateway** page, in **Certificate File**, choose the certificate file from **Local** or **Appliance**.
    - Local: Select the certificate on your computer
    - Appliance: Select the certificate on NetScaler Gateway (appliance).

6. In the **Authentication** page, in **Primary authentication method**, select **Client Certificate** and then enter a name for the certificate profile.

   The following steps assume that you already have a certificate policy.

   If you must create a certificate policy, click create a certificate policy. On the Citrix Endpoint Management Certificate screen, choose an existing server certificate or install a new certificate. If you're running multiple Citrix Endpoint Management servers, you add a certificate for each one. For Server Logon Name Attribute, specify userPrincipalName or sAMAccountName, per your requirements.

7. Click **Two Factor** to enable two-factor authentication, client certificate authentication followed by LDAP or RADIUS as the secondary authentication type.

8. In **Secondary authentication method**, select the secondary authentication method.

   - With the client certificate as your primary authentication type, you have the option of configuring LDPA (or RADIUS) as the secondary authentication type.

     To use client certificate authentication only, leave **Second authentication method** as **None** and then click **Continue**.

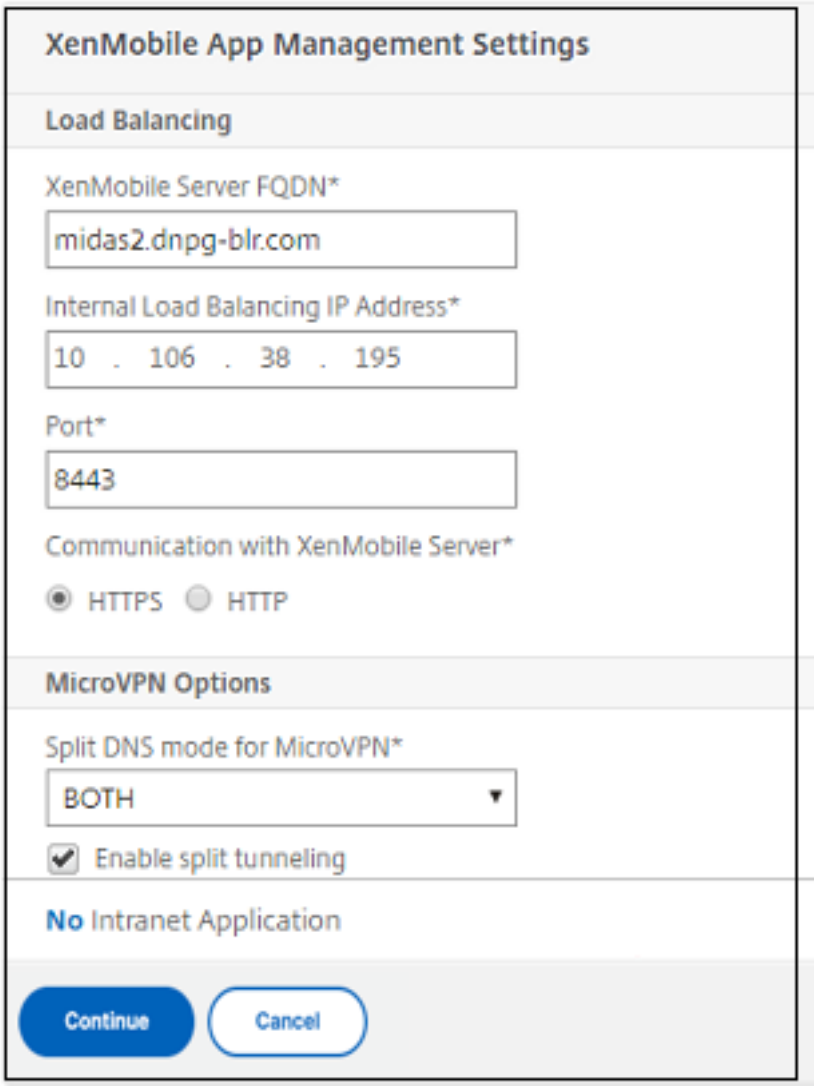
     To use client certificate + domain (LDAP) authentication, change **Secondary authentication method** to **LDAP** and configure the authentication server settings.

9. Configure the **Citrix Endpoint Management App Management Settings**.

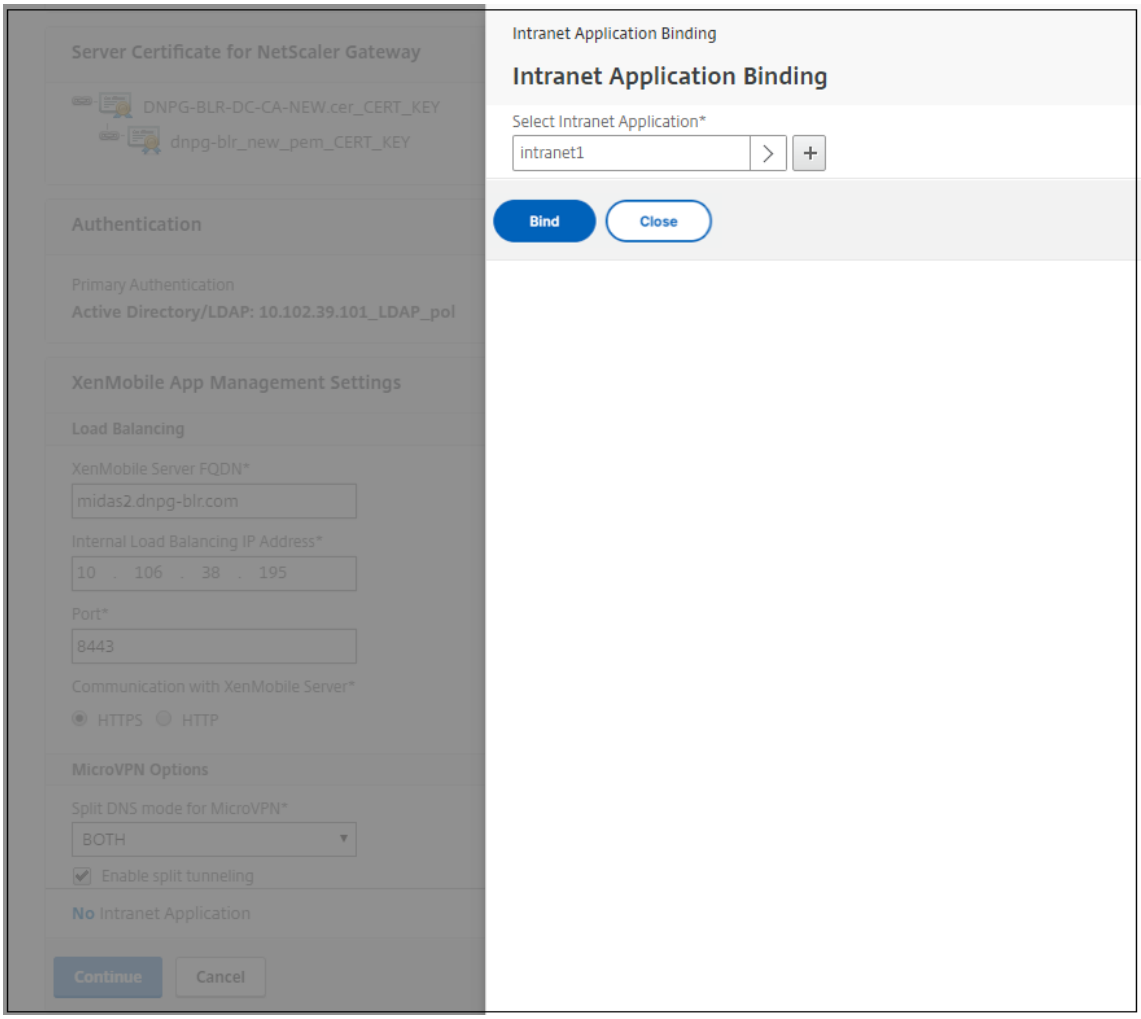
   - Enter the **Citrix Endpoint Management FQDN**. This is the load balancing FQDN for MAM.
   - Enter a MAM-only **Internal Load Balancing IP Address** for the virtual server that load balances Citrix Endpoint Management servers. NetScaler Gateway communicates with the Citrix Endpoint Management through this MAM load balancing virtual IP.
   - This is an SSL offload deployment, so select **HTTP** in **Communication with Citrix Endpoint Management Server**.
   - The **Split DNS mode for MicroVPN** field automatically sets to **BOTH**.

   If your deployment requires split tunneling, select **Enable split tunneling**. Configure Intranet Application Binding, next, if you enable split tunneling.

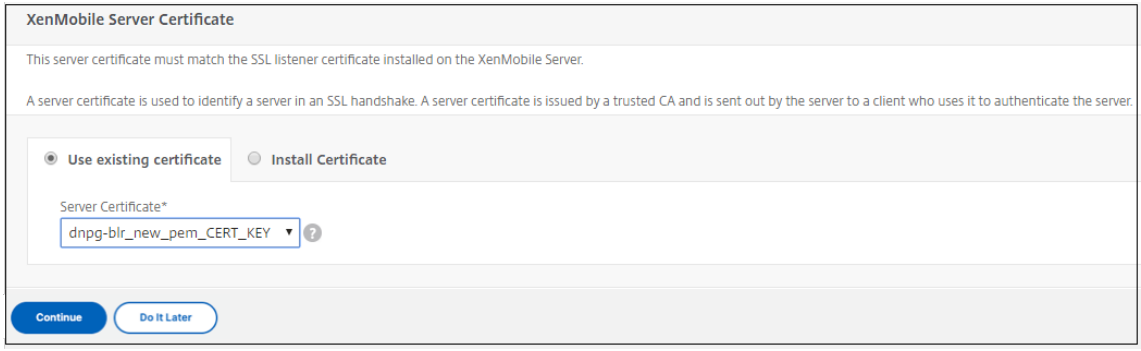
   By default, Secure Web access is tunneled to the internal network, which means that Secure Web uses a per-application VPN tunnel back to the internal network for all network access and the NetScaler appliance uses split tunnel settings.



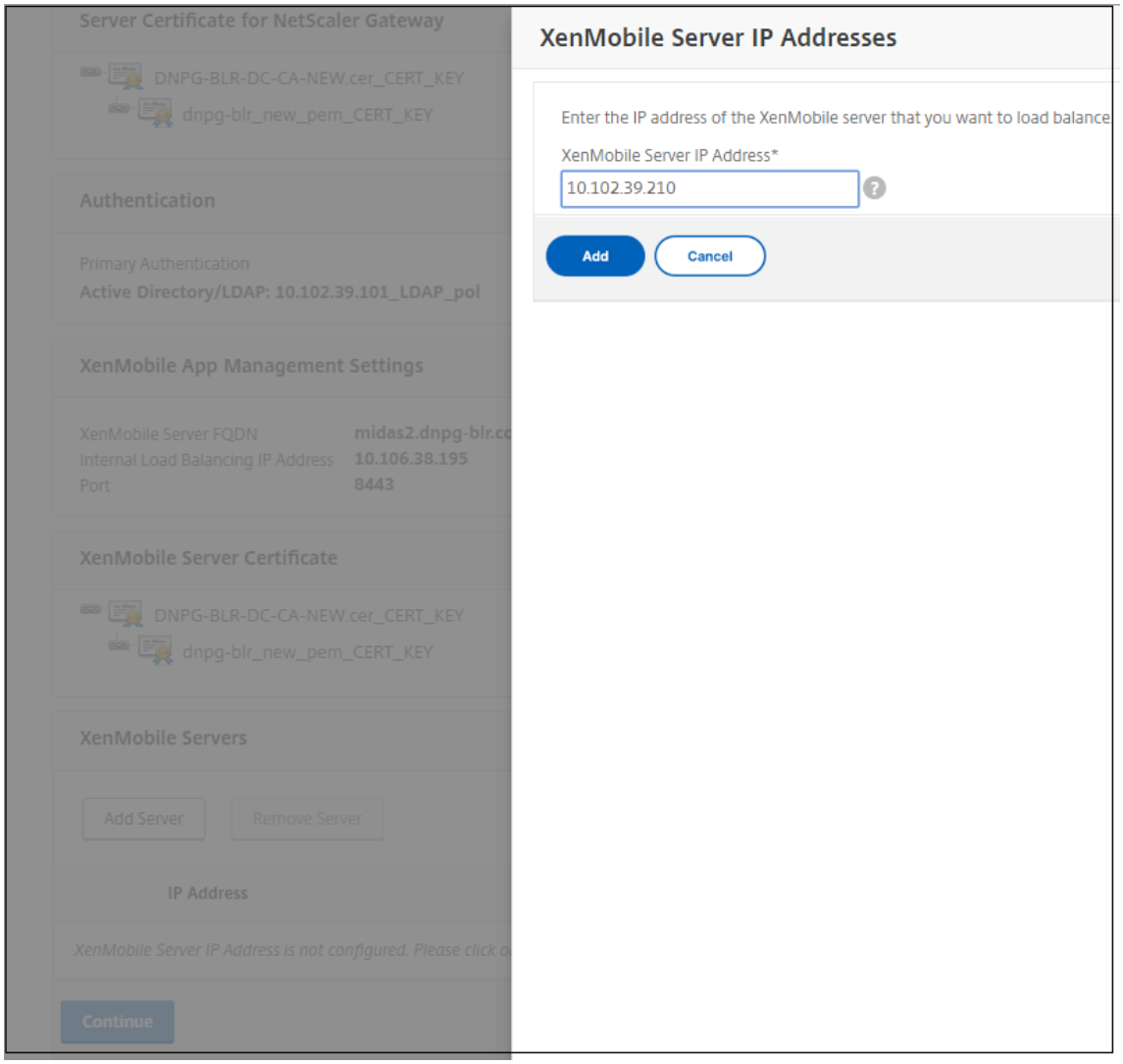
10. To configure interception rules for user connections on NetScaler Gateway, you must configure **Intranet Application Binding**. Click **+** to add a binding.



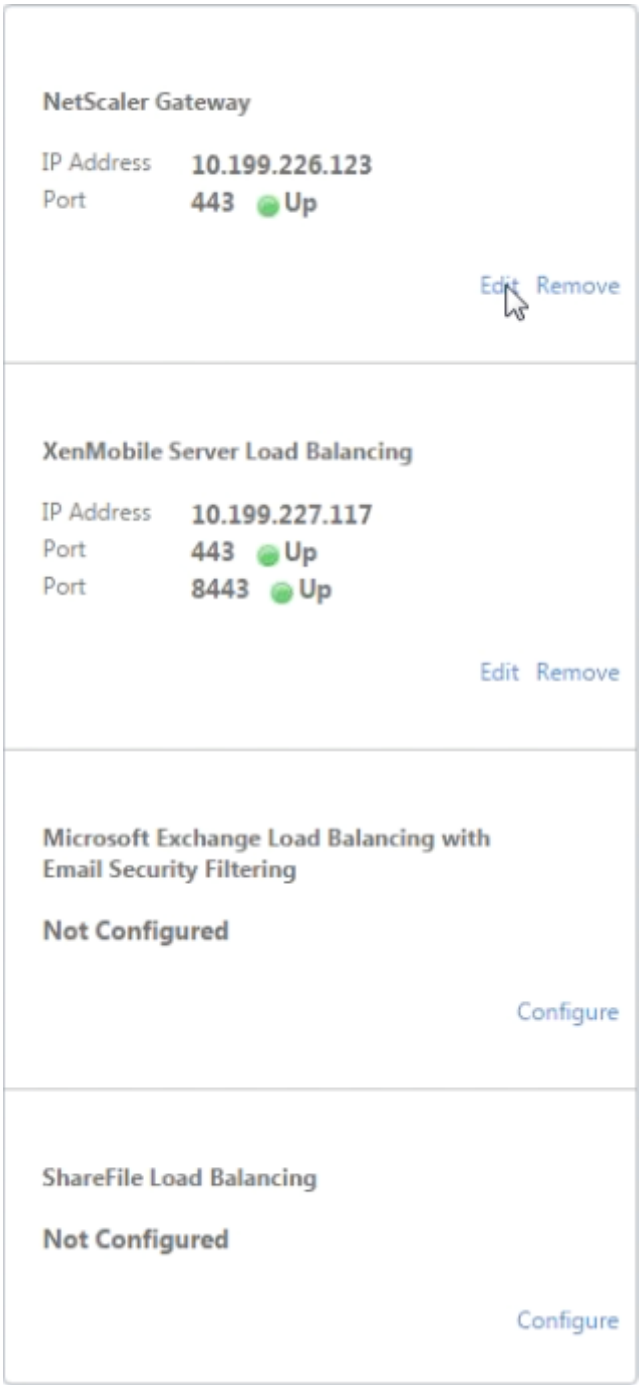
11. Complete the parameters for allowing network access and then click **Create**.
12. Add the Citrix Endpoint Management certificate. This is used for the MAM load balancing virtual server.



13. Under **Citrix Endpoint Management Servers**, click **Add Server** to add the **Citrix Endpoint Management IP Address** to bind to the load balancing virtual IP.



On the NetScaler dashboard, confirm that NetScaler Gateway and Citrix Endpoint Management load balancing are configured.



If you use the sAMAccount attributes in the user certificates as an alternative to User Principal Name (UPN), configure the certificate profile as described in Manually Configuring NetScaler Gateway for Client Certificate Authentication.

Configure load balancing servers for Citrix Endpoint Management or Citrix XenMobile Server

January 8, 2024

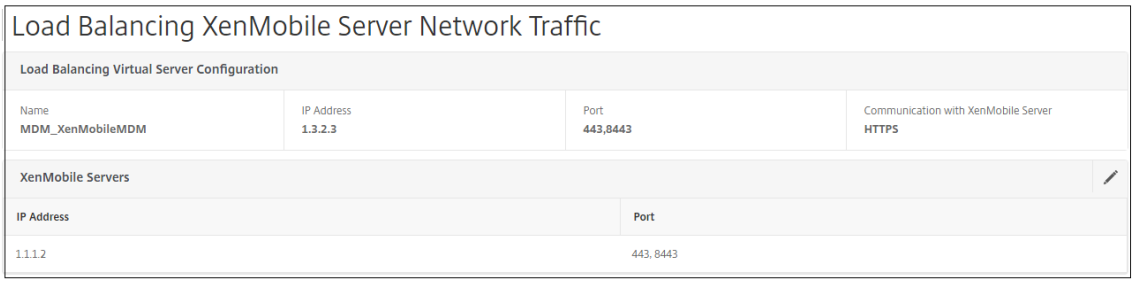
After using the **NetScaler for Citrix Endpoint Management** wizard for initial setup, use the NetScaler Gateway configuration utility to configure load balancing, as described in this section. For Citrix Endpoint Management, use SSL Offload. For Citrix Endpoint Management Server, be sure to refer to the recommendations for load balancing modes under "Deployment Summary"in Integrating with NetScaler Gateway and NetScaler.

To use SSL bridge mode for NetScaler VIPs

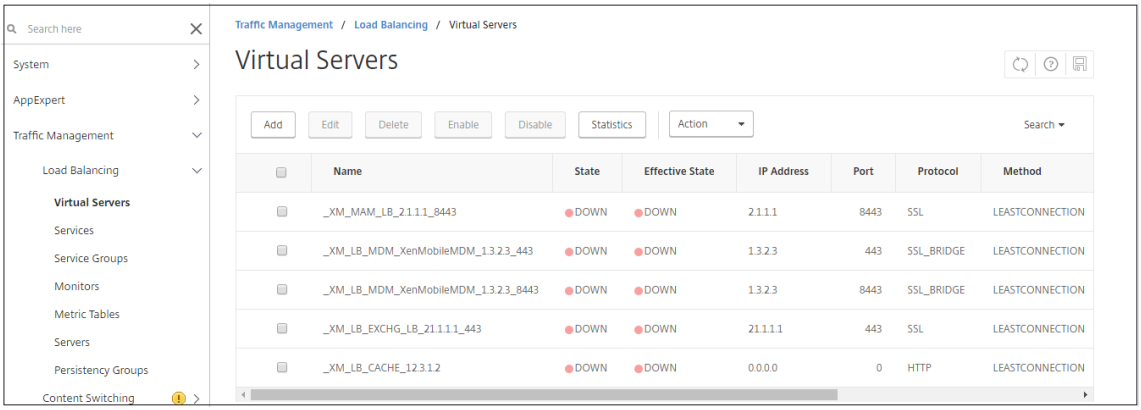
Use SSL Bridge mode if Citrix Endpoint Management is in the DMZ. When you load balance Citrix Endpoint Management with NetScaler VIPs in SSL Bridge mode, Internet traffic flows directly to the Citrix Endpoint Management server, where connections terminate. SSL Bridge mode is the simplest mode to set up and troubleshoot.

1. Before configuring SSL Bridge mode, go to **Citrix Endpoint Management App Management Settings** and verify that **Communication with Citrix Endpoint Management Server** is **HTTPS**.

2. After you log on to the configuration utility, on the **Home** tab, in **MDM Server LB**, click **Configure**.
3. Under **LB Virtual Server for Device Management**, in **Name**, type a name for the server.
4. In **IP Address**, type the IP address for the virtual server and then click **Continue**.
5. On the **Load Balance Citrix Endpoint Management MDM Servers** page, repeat Steps 3 and 4 and then click **Create**.
6. Verify that the settings are correct and then click **Done**.



7. To verify the load balancing configuration, go to **Traffic Management > Virtual Servers**.



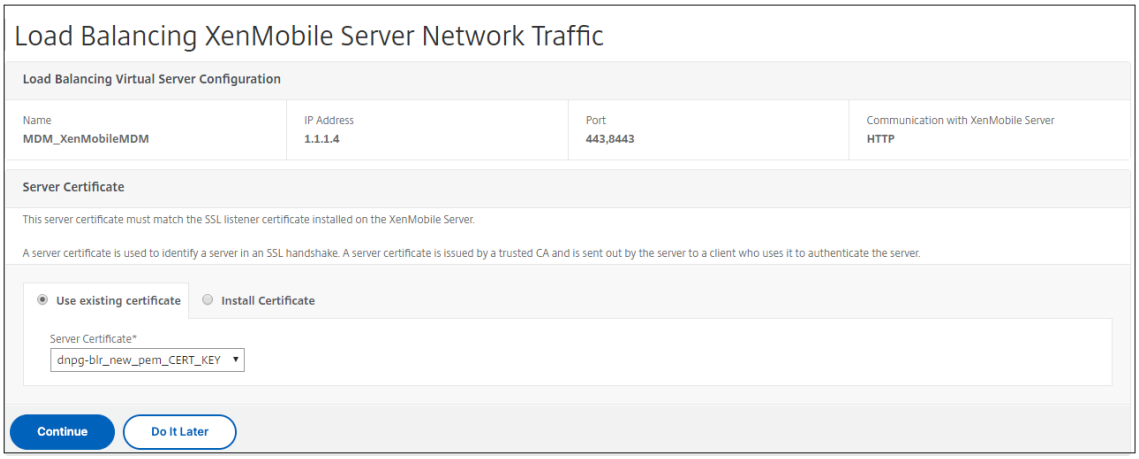
To use SSL Offload mode for NetScaler VIPs

Use SSL Offload for Citrix Endpoint Management. Also use SSL Offload, if necessary to meet security standards, when the on-premises Citrix Endpoint Management is in the internal network. When you load balance Citrix Endpoint Management with NetScaler VIPs in SSL Offload mode, Internet traffic flows directly to the NetScaler appliance, where connections terminate. NetScaler Gateway then establishes new sessions from the appliance to Citrix Endpoint Management. SSL Offload mode involves more complexity during setup and troubleshooting.

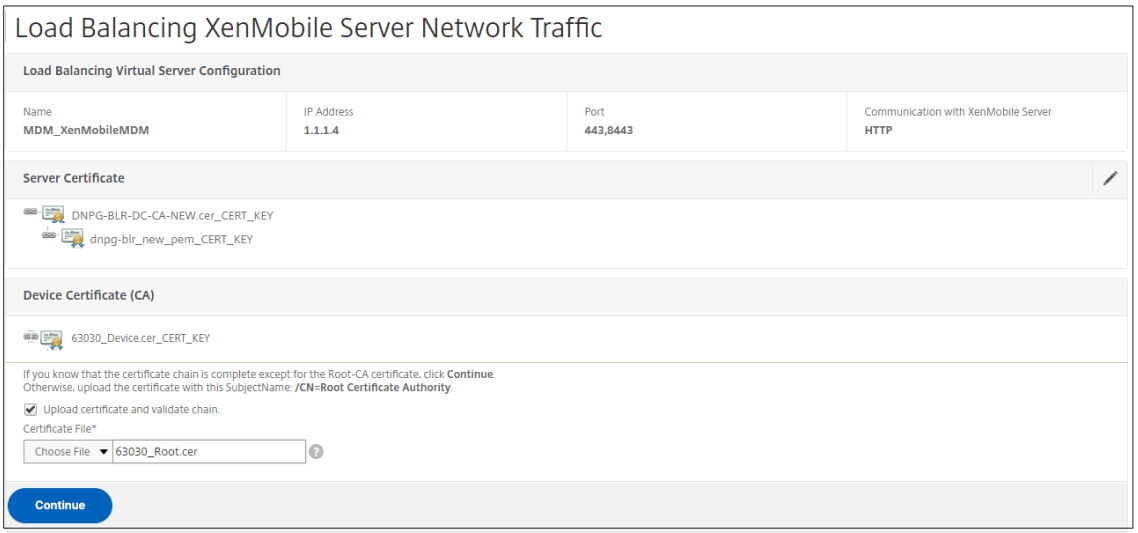
1. Before configuring SSL Offload mode, go to **Citrix Endpoint Management App Management Settings** and verify that **Communication with Citrix Endpoint Management Server** is **HTTP**.

2. Log on to the configuration utility. On the **Home** tab, in **MDM Server LB**, click **Configure**.
3. Under **LB Virtual Server for Device Management**, in **Name**, type a name for the server.
4. In **IP Address**, type the IP address for the virtual server and then click **Continue**.

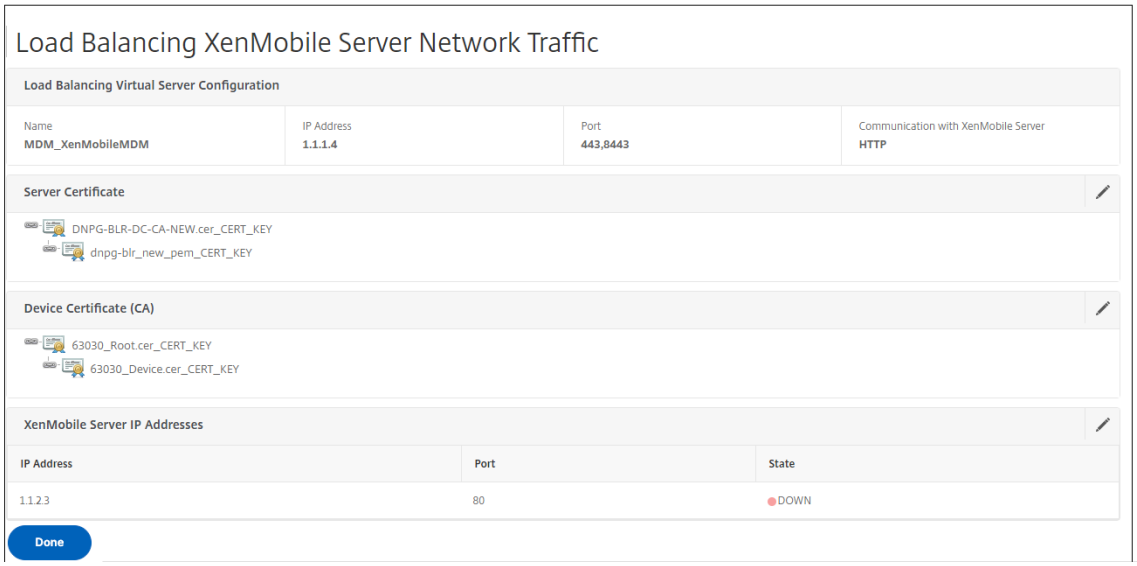
5. On the **Load Balance Citrix Endpoint Management MDM Servers** page, repeat Steps 3 and 4 and then click **Create**.
6. Verify the settings and then click **Done**.
7. When prompted to add a server certificate, choose the server certificate and click **Continue**.



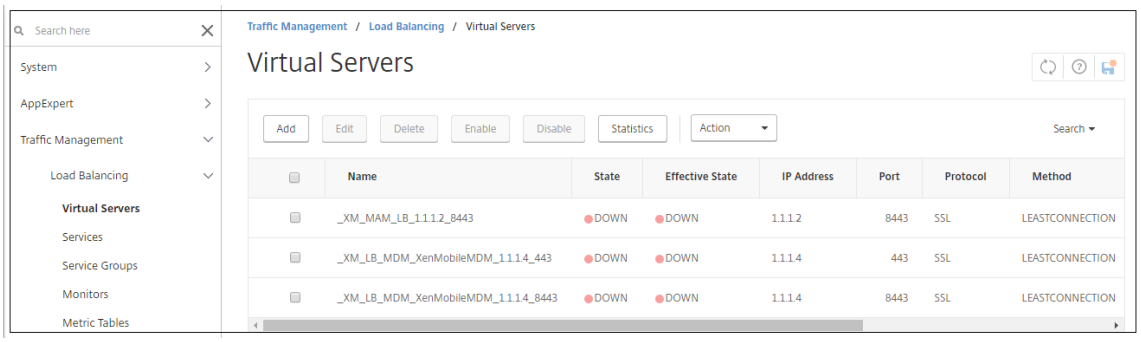
8. Specify the CA certificate and click **Continue**.



9. Keep the same Citrix Endpoint Management IP address. Click **Done**.



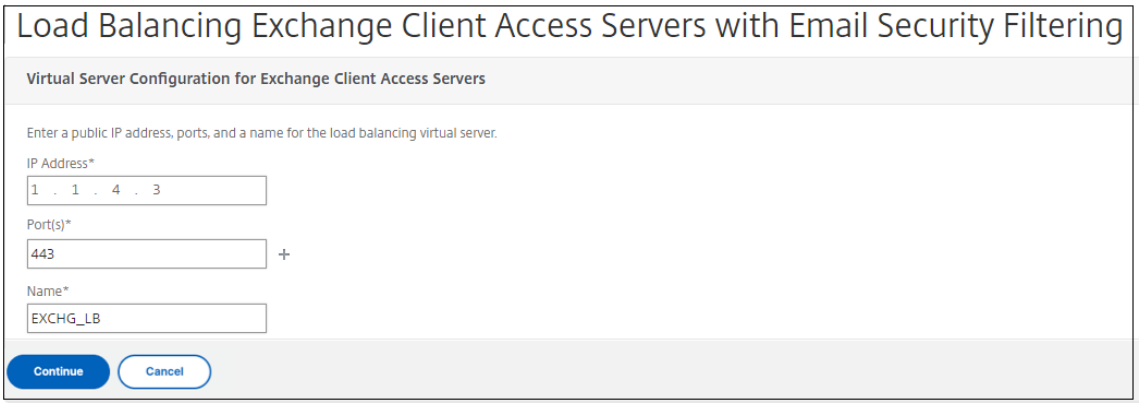
10. To verify the load balancing configuration, go to **Traffic Management > Virtual Servers**.



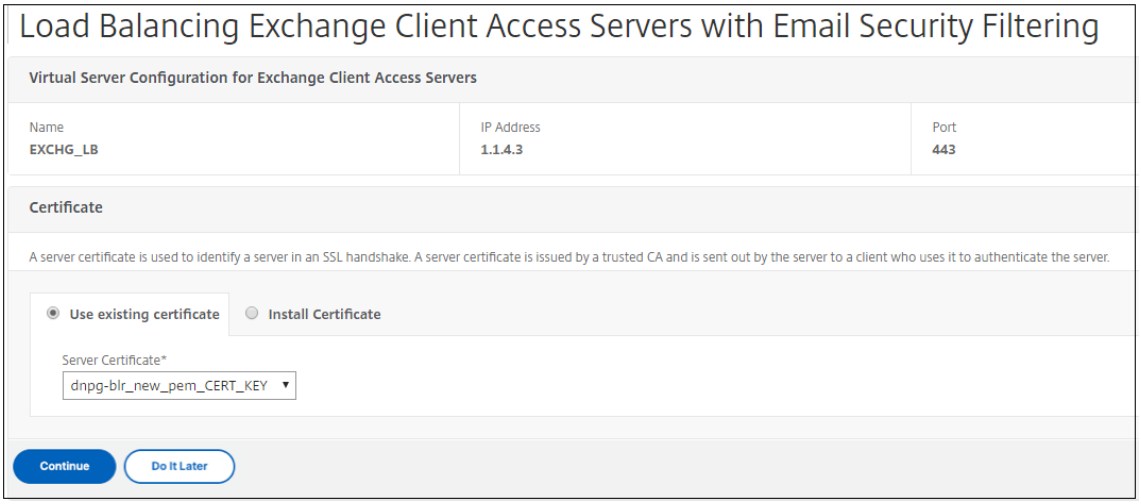
Configure load balancing servers for Microsoft Exchange with Email Security Filtering

January 8, 2024

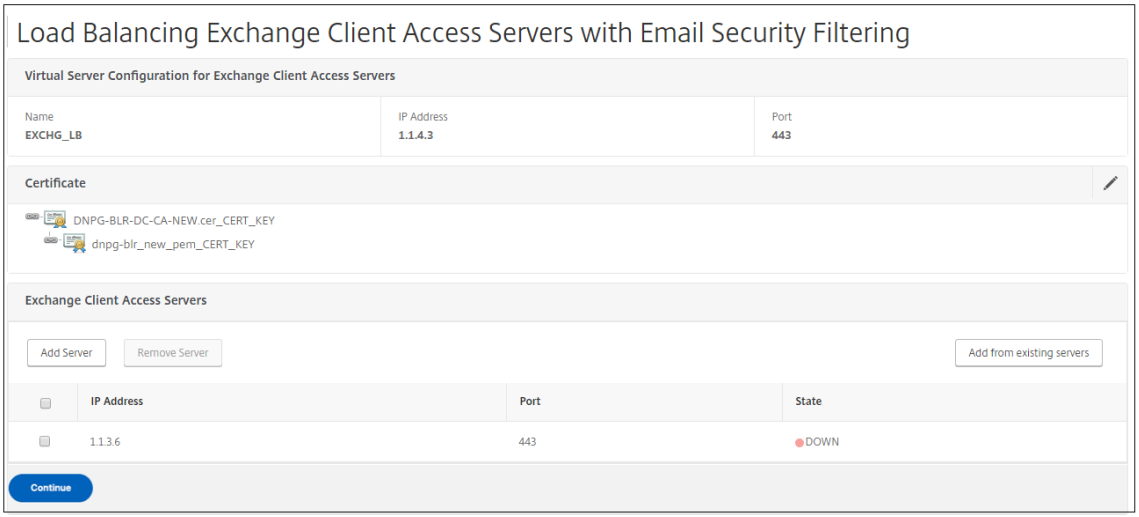
1. On the **Home** tab, in **MDM Server LB**, click **Configure**.
2. Under **LB Virtual Server for Exchange CAS**, in **Name**, type a name for the server.
3. In **IP Address**, type the IP address for the virtual server.
4. In **Port**, type the port number. To add more ports, click the plus (**+**) sign and then type the port number.
5. Click **Continue**.



6. Under **Certificates**, either choose an existing certificate or install one that's on your computer (**Local**) or on the NetScaler appliance (**Appliance**).
7. Click **Continue**.



8. Under **Exchange Citrix Analytics service Instances**, type a name, IP address, and port number for the virtual server. Then, click **Add** and **Continue**.



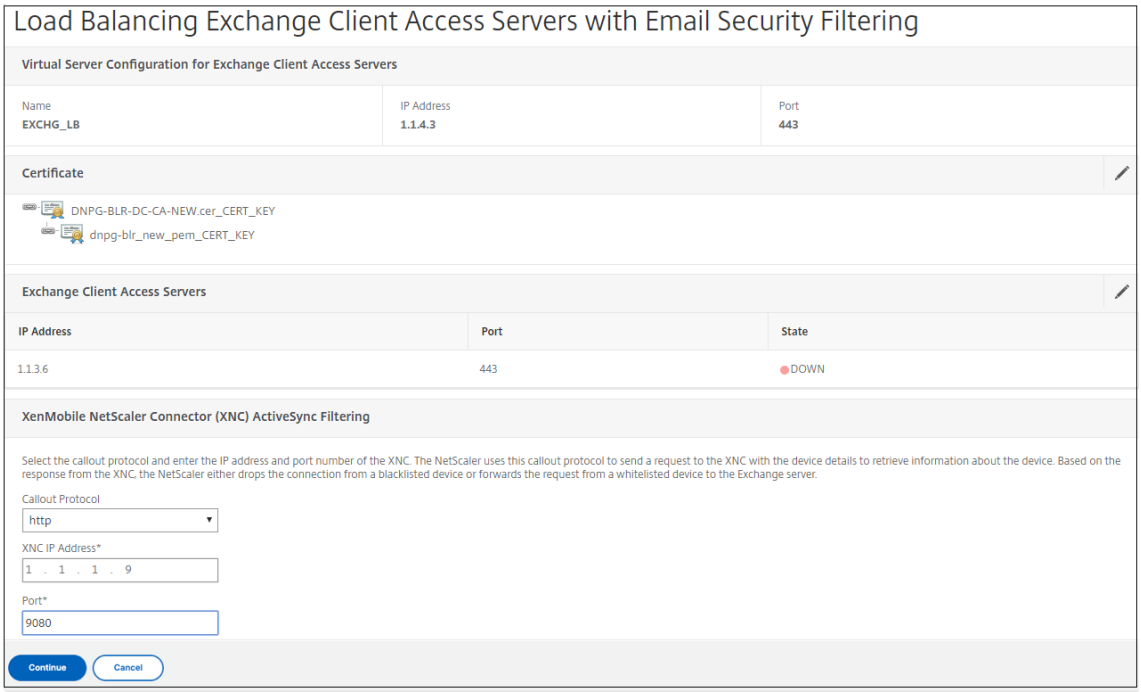
When you click **Done**, the fields for configuring the Citrix Endpoint Management NetScaler Connector (XNC) ActiveSync Filtering appear.

Configure Citrix Endpoint Management NetScaler Connector (XNC) ActiveSync Filtering

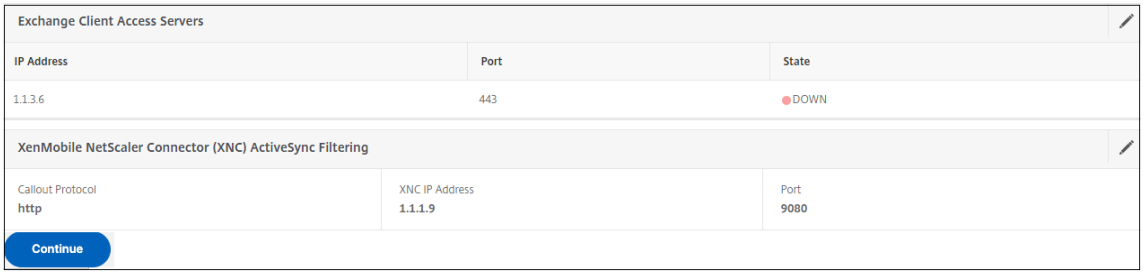
January 8, 2024

The Citrix Endpoint Management NetScaler Connector (XNC) provides a device level authorization service of ActiveSync clients to NetScaler which acts as a reverse proxy for the Exchange ActiveSync protocol. The combination of policies defined within Citrix Endpoint Management and rules defined locally by the XNC control the authorization.

1. Under **Citrix Endpoint Management NetScaler Connector (XNC) ActiveSync Filtering**, for **Callout Protocol**, select **http** or **https**.
2. In **XNC IP Address**, type the IP address of the Citrix Endpoint Management NetScaler Connector.
3. In **Port**, type **9080** for HTTP network traffic or **9443** for HTTPS network traffic, and then click **Continue**.



Your configuration appears.



Allow access from mobile devices with Citrix Mobile Productivity Apps

January 8, 2024

The NetScaler for XenMobile wizard configures the settings required to allow users to connect from supported devices through NetScaler Gateway to mobile apps and resources in the internal network. Users connect by using Secure Hub (previously, Citrix Secure Hub), which establishes a Micro VPN tunnel. When users connect, a VPN tunnel opens to NetScaler Gateway and then is passed to XenMobile in the internal network. Users can then access their web, mobile, and SaaS apps from XenMobile.

To ensure that users consume a single Universal license when connecting to NetScaler Gateway with multiple devices simultaneously, you can enable session transfer on the virtual server. For details, see Configuring Connection Types on the Virtual Server.

If you need to change your configuration after using the NetScaler for XenMobile wizard, use the sections in this article for guidance. Before changing settings, make sure that you understand the implications of your changes. For more information, refer to the XenMobile Deployment articles.

Configure Secure Browse in NetScaler Gateway

You can change Secure Browse as part of global settings or as part of a session profile. You can bind the session policy to users, groups, or virtual servers. When you configure Secure Browse, you must also enable clientless access. However, clientless access does not require you to enable Secure Browse. When you configure clientless access, set **Clientless Access URL Encoding** to **Clear**.

To configure Secure Browse globally:

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, expand **NetScaler Gateway** and then click **Global Settings**.
2. In the details pane, under **Settings**, click **Change global settings**.
3. In the **Global NetScaler Gateway Settings** dialog box, on the **Security** tab, click **Secure Browse** and then click **OK**.

To configure Secure Browse in a session policy and profile:

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, expand **NetScaler Gateway > Policies** and then click **Session**.
2. In the details pane, do one of the following:
   - If you are creating a new session policy, click **Add**.
   - If you are changing an existing policy, select a policy and then click **Open**.
3. In the policy, create a profile or modify an existing profile. To do so, do one of the following:
   - Next to **Request Profile**, click **New**.
   - Next to **Request Profile**, click **Modify**.
4. On the **Security** tab, next to **Secure Browse**, click **Override Global** and then select **Secure Browse**.
5. Do one of the following:
   - If you are creating a new profile, click **Create**, set the expression in the policy dialog box, click **Create,** and then click **Close**.
   - If you are modifying an existing profile, after making the selection, click **OK** twice.

To configure traffic policies for Secure Web in Secure Browse mode:

Use the following steps to configure traffic policies to route Secure Web traffic through a proxy server in Secure Browse mode.

1. In the configuration utility, on the **Configuration** tab, expand **NetScaler Gateway > Policies** and then click **Traffic**.
2. In the right pane, click the **Traffic Profiles** tab and then click **Add**.
3. In **Name**, enter a name for the profile, select **TCP** as the **Protocol**, and leave the rest of the settings as-is.
4. Click **Create**.
5. Click the **Traffic Profiles** tab and then click **Add**.
6. In **Name**, enter a name for the profile and then select **HTTP** as the **Protocol**.
   This Traffic Profile is for both HTTP and SSL. Clientless VPN traffic is HTTP traffic by design, regardless of the destination port or service type. Thus, you specify both SSL and HTTP traffic as **HTTP** in the traffic profile.
7. In **Proxy**, enter the IP address of the proxy server. In **Port**, enter the port number of the proxy server.
8. Click **Create**.
9. Click the **Traffic Policies** tab and then click **Add**.

10. Enter the **Name** of the traffic policy and, for **Request Profile**, select the Traffic Profile you created in Step 3. Enter the following **Expression** and then click **Create**:

```
REQ.HTTP.HEADER HOST contains ActiveSyncServer || REQ.HTTP.HEADER
    User-Agent CONTAINS WorxMail || REQ.HTTP.HEADER User-Agent
    CONTAINS com.zenprise || REQ.HTTP.HEADER User-Agent CONTAINS
    Citrix Secure Hub || REQ.HTTP.URL CONTAINS AGServices || REQ.
    HTTP.URL CONTAINS StoreWeb
```

That rule performs a check based on the host header. To bypass the active sync traffic from the proxy, replace `ActiveSyncServer` with the appropriate active sync server name.

11. Click the **Traffic Policies** tab and then click **Add**. Enter the **Name** of the traffic policy and, for **Request Profile**, select the Traffic Profile created in Step 6. Enter the following **Expression** and then click **Create**:

(REQ.HTTP.HEADER User-Agent CONTAINS Mozilla	REQ.HTTP.HEADER User-Agent CONTAINS com.citrix.browser

12. Click the **Traffic Policies** tab and then click **Add**. Enter the **Name** of the Traffic Policy and, for **Request Profile**, select the Traffic Profile created in Step 6. Enter the following **Expression** and then click **Create**:

(REQ.HTTP.HEADER User-Agent CONTAINS Mozilla	REQ.HTTP.HEADER User-Agent CONTAINS com.citrix.browser

13. Navigate to **NetScaler Gateway > Virtual Servers**, select the virtual server in the right pane, and then click **Edit**.
14. On the **Policies** row, click **+**.
15. From the **Choose Policy** menu, select **Traffic**.
16. Click **Continue**.
17. Under **Policy Binding**, across from **Select Policy**, click **>**.
18. Select the Policy you created in Step 10 and then click **OK**.
19. Click **Bind**.
20. Under **Policies**, click **Traffic Policy**.
21. Under **VPN Virtual Server Traffic Policy Binding**, click **Add Binding**.
22. Under **Policy Binding**, next to the **Select Policy** menu, click **>** to view the policy list.
23. Select the policy you created in Step 11 and then click **OK**.

24. Click **Bind**.
25. Under **Policies**, click **Traffic Policies**.
26. Under **VPN Virtual Server Traffic Policy Binding**, click **Add Binding**.
27. Under **Policy Binding**, next to the **Select Policy** menu, click **>** to view the policy list.
28. Select the policy you created in Step 12 and then click **OK**.
29. Click **Bind**.
30. Click **Close**.
31. Click **Done**.

Be sure to configure the Secure Web (WorxWeb) app in the XenMobile console. Go to **Configure > Apps**, select the Secure Web app, click **Edit**, and then make these changes:

- On the **App information** page, change **Initial VPN Mode** to **Secure Browse**.
- On the **iOS** page, change **Initial VPN Mode** to **Secure Browse**.
- On the **Android** page, change **Preferred VPN Mode** to **Secure Browse**.

Configure application and MDX token time-outs

When users log on from an iOS or Android device, an application token or an MDX token is issued. The token is similar to the Secure Ticket Authority (STA).

You can set the number of seconds or minutes the tokens are active. If the token expires, users cannot access the requested resource, such as an application or a webpage.

Token time-outs are global settings. When you configure the setting, it applies to all users who log on to NetScaler Gateway.

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, expand **NetScaler Gateway** and then click **Global Settings**.
2. In the details pane, under **Settings**, click **Change global settings**.
3. In the **Global NetScaler Gateway Settings** dialog box, on the **Client Experience** tab, click **Advanced Settings**.
4. On the **General** tab, in **Application Token Timeout (sec)** enter the number of seconds before the token expires. The default is **100** seconds.
5. In **MDX Token Timeout (mins)**, enter the number of minutes before the token expires and then click **OK**. The default is **10** minutes.

Disable Endpoint Analysis for mobile devices

If you configure endpoint analysis, you need to configure the policy expressions so that the endpoint analysis scans do not run on Android or iOS mobile devices. Endpoint analysis scans are not supported on mobile devices.

If you bind an endpoint analysis policy to a virtual server, you must create a secondary virtual server for mobile devices. Do not bind preauthentication or post-authentication policies to the mobile device virtual server.

When you configure the policy expression in a preauthentication policy, you add the User-Agent string to exclude Android or iOS. When users log on from one of these devices and you exclude the device type, endpoint analysis does not run.

For example, you create the following policy expression to check if the User-Agent contains Android, if the application virus.exe does not exist, and to end the process keylogger.exe if it is running by using the preauthentication profile. The policy expression might look like this:

```
REQ.HTTP.HEADER User-Agent NOTCONTAINS Android &&
CLIENT.APPLICATION.PROCESS(keylogger.exe) contains
```

After you create the preauthentication policy and profile, bind the policy to the virtual server. When users log on from an Android or iOS device, the scan does not run. If users log on from a Windows-based device, the scan does run.

For more information about configuring preauthentication policies, see Configuring Endpoint Polices.

Support DNS queries by using DNS suffixes for Android devices

When users establish a Micro VPN connection from an Android device, NetScaler Gateway sends split DNS settings to the user device. NetScaler Gateway supports split DNS queries based on the split DNS settings you configure. NetScaler Gateway can also support split DNS queries based on DNS suffixes you configure on the appliance. If users connect from an Android device, you must configure DNS settings on NetScaler Gateway.

Split DNS works in the following manner:

- If you set split DNS to **Local**, the Android device sends all DNS requests to the local DNS server.
- If you set split DNS to **Remote**, all DNS requests are sent to the DNS servers configured on NetScaler Gateway (remote DNS server) for resolution.
- If you set split DNS to **Both**, the Android device checks for the DNS request type.

- If the DNS request type is not “A,”it sends the DNS request packet to both local and remote DNS servers.
- If the DNS request type is “A,”the Android plug-in extracts the query FQDN and matches that FQDN against the DNS suffix list configured on the NetScaler appliance. If the DNS request’s FQDN matches, the DNS request is sent to the remote DNS server. If FQDN does not match, the DNS request is sent to local DNS servers.

The following table summarizes split DNS working based on type A record and suffix list.

Split DNS setting	Is it a type A record?	Is it on the suffix list?	Where the DNS request is sent
Local	both Yes or No	both Yes or No	Local
Remote	both Yes or No	both Yes or No	Remote
Both	No	NA	Both
Both	Yes	Yes	Remote
Both	Yes	No	Local

To configure a DNS suffix:

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, expand **NetScaler Gateway > Policies** and then click **Session**.
2. In the details pane, on the **Policies** tab, select a session policy and then click **Open**.
3. Next to **Request Profile**, click **Modify**.
4. On the **Network Configuration** tab, click **Advanced**.
5. Next to **Intranet IP DNS Suffix**, click **Override Global**, type the DNS suffix and then click **OK** three times.

To configure split DNS globally on NetScaler Gateway:

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, expand **NetScaler Gateway** and then click **Global Settings**.
2. In the details pane, under **Settings**, click **Change global settings**.
3. On the **Client Experience** tab, click **Advanced Settings**.
4. On the **General** tab, in **Split DNS**, select **Both**, **Remote**, or **Local** and then click **OK**.

To configure split DNS in a session policy on NetScaler Gateway:

1. In the configuration utility, on the **Configuration** tab, in the navigation pane, expand **NetScaler Gateway > Policies**, and then click **Session**.
2. In the details pane, on the **Policies** tab, click **Add**.

3. In **Name**, type a name for the policy.
4. Next to **Request Profile**, click **New**.
5. In **Name**, type a name for the profile.
6. On the **Client Experience** tab, click **Advanced Settings**.
7. On the **General** tab, next to **Split DNS**, click **Override Global**, select **Both**, **Remote**, or **Local** and then click **OK**.
8. In the **Create Session Policy** dialog box, next to **Named Expressions**, select **General**, select **True**, click **Add Expression**, click **Create,** and then click **Close**.

Configure domain and security token authentication for Citrix Endpoint Management

January 8, 2024

You can configure Citrix Endpoint Management to require users to authenticate with their LDAP credentials plus a one-time password, using the RADIUS protocol. This section describes the required NetScaler Gateway configuration for that two-factor authentication type.

Prerequisites

If you have not already run the NetScaler for Citrix Endpoint Management wizard, see the *NetScaler for Citrix Endpoint Management Wizard* section in Configuring Settings for Your Citrix Endpoint Management Environment. Make sure that your NetScaler configuration includes the following:

- **LDAP port number** = **636** (which is the default port for secure LDAP connections)
- **Server Logon Name Attribute** = **samAccountName** or the **userPrincipalName** as per your requirements

To configure domain and security token authentication

1. Go to **NetScaler Gateway > Virtual Servers**. Select the virtual server and then click **Edit**.
2. Click **No CA Certificate.**
3. In **Select CA Certificate**, choose a certificate, click **OK**, click **Bind**, and then click **Done**.
4. Go to **Policies > Session > Session Profiles**, select the profile, and click **Edit**.
5. Click the **Client Experience** tab.
6. In **Credential Index**, choose **SECONDARY**.

7. Click **OK**.
8. Go to **Policies > Authentication > LDAP**, click the **LDAP Policy** tab, and click **Edit**.
9. Use the following expression to use separate NetScaler Gateway VIPs for Citrix Endpoint Management and Citrix Virtual Apps and Desktops.

   REQ.HTTP.HEADER User-Agent CONTAINS `CitrixReceiver`
10. Go to **Policies > Authentication > RADIUS** and then click the **Servers** tab.
11. Click **Add**, enter the RADIUS server details, and click **Create**.
12. Go to **Policies** and then click **Add**.
13. Enter a **Name** for the policy. From the **Server** drop-down menu, select the RADIUS server name that you have created.
14. In **Expression**, enter **REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver** and click **Create**.
15. Select the virtual server and then click **Edit**.
16. Under **Primary Authentication**, click **LDAP Policy**.
17. Select the policy, click **Unbind**, and click **Close**.
18. On the **Authentication** row, click **+** to add the RADIUS authentication.
19. Under **Choose Type**, from **Choose Policy**, select **RADIUS**.
20. Click **Bind**.
21. Select the RADIUS authentication policy that you created earlier and then click **Insert**.
22. Click **OK**.
23. To add LDAP as the secondary authentication policy: On the **Authentication** row, click **+**.
24. From **Choose Policy**, choose **LDAP**.
25. From **Choose Type**, choose **Secondary**.
26. From **Select Policy**, choose the LDAP policy.
27. Select the policy and then click **OK**.
28. Click **Bind**.
29. Click **Done**.
30. Verify that the policies you created have the highest priority. This ensures that they have the highest priority even if more policies get added for non-mobile users. For more information, see Setting Priorities for Authentication Policies

Configure client certificate or client certificate and domain authentication

January 8, 2024

You can use the NetScaler for Citrix Endpoint Management wizard to perform the configuration required for Citrix Endpoint Management when using NetScaler certificate-only authentication or certificate plus domain authentication. You can run the NetScaler for Citrix Endpoint Management wizard one time only. For information about using the wizard, see Configuring Settings for Your Citrix Endpoint Management Environment.

If you've already used the wizard, use the instructions in this article for the addition configuration required for client certificate authentication or client certificate plus domain authentication.

To ensure that the user of a device in MAM-only mode can't authenticate using an existing certificate on the device, see "NetScaler Certificate Revocation List (CRL)"later in this article.

Configure NetScaler Gateway for client certificate authentication by using the GUI

1. Navigate to **Traffic Management > Load Balancing > Virtual Servers**.
2. Select the virtual server of type **SSL**, and in the **SSL Parameters** section set **Enable Session Reuse** as **DISABLED**.
3. Navigate to **NetScaler Gateway > Virtual Servers**.
4. Select the virtual server of type **SSL**, and click **Edit**.
5. In the **SSL Parameters** section, click the edit icon.
6. Select **Client Authentication** and in **Client Certificate**, select **Mandatory**.
7. Create an authentication certificate policy so Citrix Endpoint Management can extract the **User Principal Name** or the **sAMAccount** from the client certificate provided by Secure Hub to NetScaler Gateway.
8. Navigate to **NetScaler Gateway> Policies> Authentication > CERT**.
9. Click the **Profiles** tab and click **Add**.
10. Set the following parameters for the certificate profile:

    Authentication Type: **CERT**

    Two Factor: **OFF** (for certificate only authentication)

    User Name Field: Subject: **CN**

    Group Name Field: **SubjectAltName:PrincipalName**

11. Bind only the certificate authentication policy as the **Primary Authentication** in the NetScaler Gateway virtual server.
12. Bind the Root CA certificate to validate the trust of the client certificate presented to NetScaler Gateway.

Configure NetScaler Gateway for client certificate and domain authentication by using the GUI

1. Navigate to **Traffic Management > Load Balancing > Virtual Servers**.
2. Select the virtual server of type **SSL**, and in the **SSL Parameters** section set **Enable Session Reuse** as **DISABLED**.
3. Go to **NetScaler Gateway > Policies > Authentication > Cert**.
4. Click the **Profiles** tab, click **Add**.
5. Enter the **Name** of the profile, set **Two Factor** to **ON**, and from **User Name Field**, select **SubjectAltNamePrincipalName**.
6. Click the **Policies** tab and click **Add**.
7. Enter the **Name** of the policy, from **Server** select the certificate profile, set the **Expression** and click **Create**.
8. Go to **Virtual Servers**, select the virtual server of type **SSL**, and click **Edit**.
9. Beside **Authentication**, click **+** to add the certificate authentication.
10. To select the authentication method, in **Choose Policy**, select **Certificate**, and in **Choose Type** select **Primary**. This binds certificate authentication as the primary authentication with the same priority as the LDAP authentication type.
11. Under **Policy Binding**, click **Click to Select** to select the certificate policy created earlier.
12. Select the certificate policy created earlier and click **OK**.
13. Set the **Priority** to **100** and then click **Bind**. Use the same priority number when you configure the LDAP authentication policy in the subsequent steps.
14. On the row for **LDAP Policy**, click **>**.
15. Select the policy and then, from the **Edit** drop-down menu, click **Edit Binding**.
16. Enter the same **Priority** value that you specified for the certificate policy. Click **Bind**.
17. Click **Close**.
18. Click the edit icon in the **SSL Parameters** section.

19. Select the **Client Authentication** checkbox, and in **Client Certificate** choose **Mandatory**, and click **OK**.
20. Click **Done**.

NetScaler Certificate Revocation List (CRL)

Citrix Endpoint Management supports Certificate Revocation List (CRL) only for a third party Certificate Authority. If you have a Microsoft CA configured, Citrix Endpoint Management uses NetScaler to manage revocation. When you configure client certificate-based authentication, consider whether you need to configure the NetScaler Certificate Revocation List (CRL) setting, **Enable CRL Auto Refresh**. This step ensures that the user of a device in MAM-only mode can't authenticate using an existing certificate on the device. Citrix Endpoint Management reissues a new certificate, because it doesn't restrict a user from generating a user certificate if one is revoked. This setting increases the security of PKI entities when the CRL checks for expired PKI entities.

Configure SmartControl

January 8, 2024

SmartControl allows administrators to define granular policies to configure and enforce user environment attributes for Citrix Virtual Apps and Desktops on NetScaler Gateway. SmartControl allows administrators to manage these policies from a single location, rather than at each instance of these server types.

SmartControl is implemented through ICA policies on NetScaler Gateway. Each ICA policy is an expression and access profile combination that can be applied to users, groups, virtual servers, and globally. ICA policies are evaluated after the user authenticates at session establishment. To enable SmartControl, you must associate the ICA policy to a VPN virtual server.

The following table lists the user environment attributes that SmartControl can enforce:

ConnectClientDrives	Specifies the default connection to the client drives when the user logs on.

ConnectClientLPTPorts	Specifies the automatic connection of LPT ports from the client when the user logs on. LPT ports are the Local Printer Ports.
ClientAudioRedirection	Specifies the applications hosted on the server to transmit audio through a sound device installed on the client computer.
ClientClipboardRedirection	Specifies and configures clipboard access on the client device and maps the clipboard on the server.
ClientCOMPortRedirection	Specifies the COM port redirection to and from the client. COM ports are the COMmunication ports. COM ports are serial ports.
ClientDriveRedirection	Specifies the drive redirection to and from the client.
Multistream	Specifies the multistream feature for specified users.
ClientUSBDeviceRedirection	Specifies the redirection of USB devices to and from the client (workstation hosts only).
`Localremotedata`	Specifies the HTML5 file upload download capability for the Citrix Workspace app.
ClientPrinterRedirection	Specifies the client printers to be mapped to a server when a user logs on to a session.

ClientTWAINDeviceRedirection	Allows default access or disables TWAIN devices, such as digital cameras or scanners, on the client device from published image processing applications.	
WIARedirection	Allows default access or disables WIA scanner redirection.	
DragAndDrop	Allows default access or disables drag and drop between client and remote applications and desktops.	
SmartCardRedirection	Allow default access or disable smart card redirection. Smart card virtual channel is always allowed in CVAD.	
FIDO2Redirection	Allows default access or disable FIDO2 redirection.	
Policies	Action	Access Profiles
Add	Edit	Delete
Show Bindings	Policy Manager	Action

ICA Policies and Profiles

ICA policy

An ICA policy specifies an Action, Access Profile, Expression and optionally, a Log Action. You can perform the following ICA policy configurations:

Configure an ICA policy by using the GUI

1. Navigate to **NetScaler Gateway > Policies** and click **ICA**.
2. In the **ICA Policies** section, click **Add**. The **Create ICA Policy** page appears.
3. In the **Name** field, specify a name for the ICA policy.
4. Next to the **Action** field, do one of the following:

- Click the **>** icon to select an existing action.
- Click **Add** to create an action.

5. Add an expression.
6. Create a log action.
7. Configure the remaining parameters as required and click **OK**.

Configure an ICA policy by using the CLI `add ica policy smartaccess_policy -rule TRUE -action smartaccess_action`

Bind the ICA policy to a bind point by using the GUI

1. Navigate to **NetScaler Gateway > Policies > NetScaler Gateway > ICA Policies and Profiles > ICA Policies**. Click **Policy Manager**.
2. Select the bind point and the virtual server, and click **Continue**.
3. In the **Policy Binding** section, select the ICA policy that you need to associate to a bind point.
4. Click **Bind** and then click **Done**.

To verify the binding, click **Show Bindings** in the **ICA Policies** section. You can view the list of bind points associated with the ICA policy.

Bind the ICA policy to a VPN virtual server by using the CLI `bind vpn vserver vpnvserver -policy smartaccess_policy -type ICA_REQUEST -priority 10`

ICA action

Configure an ICA action by using the GUI

1. Go to **NetScaler Gateway > Policies** and then click **ICA**.
2. In the **ICA Actions** tab, click **Add**. The **Create ICA Action** page appears.
3. In the **Name** field, specify a name for the ICA policy.
4. Next to the **ICA Access Profile** field, do one of the following:

   - Click the **>** icon to select an existing ICA access profile.
   - Click **Add** to create an ICA access profile.

5. Create an ICA latency profile to associate it to the ICA action.
6. Click **Create**.

Configure an ICA action by using the CLI `add ica action smartaccess_action -accessProfileName smartaccess_profile`

ICA access profile

An ICA profile defines the settings for user connections. Access profiles specify the actions that are applied to a user's Citrix Virtual Apps and Desktops environment ICA if the user device meets the policy expression conditions. You can use the GUI to create ICA profiles separately from an ICA policy and then use the profile for multiple policies. You can only use one profile with a policy.

You can create access profiles independent from an ICA policy. When you create the policy, you can select the access profile to attach to the policy. An access profile specifies the resources available to a user.

Starting from release 14.1-8.x, NetScaler Gateway extends the capabilities of the SmartControl feature to more ICA virtual channels of Citrix Virtual Apps and Desktops. This extension improves the interaction between NetScaler Gateway and the ICA virtual channels.

To leverage the capability of the extended SmartControl feature, you can configure the following settings on the ICA access profile.

- ClientTWAINDeviceRedirection
- WIARedirection
- DragAndDrop
- SmartCardRedirection
- FIDO2Redirection

Configure an ICA access profile by using the GUI

1. Navigate to **NetScaler Gateway > Policies > NetScaler Gateway ICA Policies and Profiles > Access Profiles** and click **Add**. The **Create ICA Access Profile** page appears.
2. Provide a name for the ICA access profile, configure the following parameters, and click **Create**.
    - Connect Client LPT Ports: Allow or block the automatic connection of Line Print Terminal (LPT) ports from the client when the user logs on.
    - Client Audio Redirection: Allow or block applications hosted on a server to play sounds through a sound device installed on the client computer. This setting also allows or blocks users from recording audio inputs.
    - Local Remote Data Sharing: Allow or block file or data sharing through the Citrix Workspace app for HTML5.
    - Client Clipboard Redirection: Allow or block the clipboard on the client device to be mapped to the clipboard on the server.
    - Client COM Port Redirection: Allow or block the Communication (COM) port redirection to and from the client.
    - Client Drive Redirection: Allow or block the drive redirection to and from the client.

- Client Printer Redirection: Allow or block printers to be mapped to a server when a user logs on to a session.
- Multistream: Allow or block the multi-stream feature for the specified users.
- Client USB Drive Redirection: Allow or block the redirection of USB devices to and from the client.
- Client TWAIN Device Redirection: Allow or block TWAIN devices, such as digital cameras or scanners, on the client device from the published image processing applications.
- WIA Redirection: Allow or block the Windows Image Acquisition (WIA) scanner redirection.
- Drag and Drop: Allow or block the drag and drop action between client and remote applications and desktops.
- Smart Card Redirection: Allow or block the smart card redirection. Smart card virtual channel is always allowed in Citrix Virtual apps and Desktops.
- FIDO2 Redirection: Allow or block Fast Identity Online 2 (FIDO 2) redirections.

Configure an ICA access profile by using the CLI

```
add ica accessprofile <name> [-ConnectClientLPTPorts ( DEFAULT |
    DISABLED )] [-ClientAudioRedirection ( DEFAULT | DISABLED )][-
    LocalRemoteDataSharing ( DEFAULT | DISABLED )][-
    ClientClipboardRedirection ( DEFAULT | DISABLED )][-
    ClientCOMPortRedirection ( DEFAULT | DISABLED )][-
    ClientDriveRedirection ( DEFAULT | DISABLED )][-
    ClientPrinterRedirection ( DEFAULT | DISABLED )] [-Multistream (
    DEFAULT | DISABLED )][-ClientUSBDriveRedirection ( DEFAULT |
    DISABLED)] [-ClientTWAINDeviceRedirection ( DEFAULT | DISABLED )][-
    WIARedirection ( DEFAULT | DISABLED )] [-DragAndDrop ( DEFAULT |
    DISABLED )] [-SmartCardRedirection ( DEFAULT | DISABLED )]
[-FIDO2Redirection ( DEFAULT | DISABLED )]
```

ICA latency profile

Configure an ICA latency profile by using the GUI

1. Navigate to **NetScaler Gateway > Policies > NetScaler Gateway ICA Policies and Profiles > ICA Latency Profiles**.
2. Update the required fields and click **Create**.

Configure an ICA latency profile by using the CLI

```
add ica latencyprofile [-l7LatencyMonitoring ( ENABLED | DISABLED )]
[-l7LatencyThresholdFactor ] [-l7LatencyWaitTime ] [-l7LatencyNotifyInterval
 ] [-l7LatencyMaxNotifyCount ]
```


Microsoft Intune Integration

January 8, 2024

The integration of Microsoft Intune with NetScaler Gateway provides best-of-class application access and data protection solution offered by NetScaler Gateway and Intune.

You get the most complete suite of secure productivity apps, including email, calendar, contacts, note-taking, document editing, and remote access—all which can be centrally managed across different platforms. Intune and NetScaler Gateway integration provides world-class mobile device management (MDM) functionalities, while the Citrix Secure Access client side technology empowers these Intune enlightened applications to access corporate data and application securely through the NetScaler Gateway.

The integration allows NetScaler Gateway to pull compliance data from Intune, enabling conditional access policies. The conditional access policies give NetScaler Gateway a finer control on regulating the access based on device functionalities and so on. For example, an administrator can create a policy wherein only the devices with "Camera"disabled are granted access.

NetScaler Gateway supports Azure Active Directory Libraries (ADAL) token authentication once the NetScaler Gateway virtual server is configured. Upon configuration, a mobile application wrapped with the Citrix Network-Only wrapper or SDK accesses NetScaler Gateway by using an ADAL token that the app can fetch directly from AAD.

Citrix micro VPN integration with Microsoft Endpoint Manager

NetScaler Gateway customers can use micro VPN with Microsoft Endpoint Manager (Intune). Citrix micro VPN integration with Microsoft Endpoint Management enables your apps to access on-premises resources.

Citrix micro VPN technology provides an on-demand VPN that reduces data transfer costs and simplifies security, as the VPN tunnel isn't always active. Instead, it's only active when needed, which reduces risk and optimizes the performance of the device for a better user experience. This also helps improve mobile battery life. The micro VPN technology from NetScaler provides mobile users with secure access to internal business resources while providing them with the best user experience.

Micro VPN is supported only for following use cases:

- Intune mobile application management (MAM) only
- Intune mobile device management (MDM) and mobile application management (MAM)

> **Important:**
>
> For the SSL VPN functionality, micro VPN requires a NetScaler Gateway Advanced or Premium edition (VPX 3000 or higher) and a Citrix Endpoint Management entitlement. The Citrix Endpoint Management entitlement ensures continued support to the micro VPN SDK on a Microsoft Edge mobile browser (iOS and Android). For more information, contact your Sales, Account, or Partner representative.

For details about setting up Citrix micro VPN integration with Microsoft Endpoint Manager, see Set up NetScaler Gateway for using micro VPN with Microsoft Endpoint Manager.

When to Use the Integrated Intune MDM Solution

January 8, 2024

The following scenarios illustrate the use of the integrated Intune MDM Solution:

- A new customer decides to onboard Intune with on-prem NetScaler Gateway deployment
- An existing NetScaler Gateway user wants to add mobile device management with Intune
- An existing Intune user wants to allow mobile device or applications to access data located inside company network with a NetScaler Gateway physical or virtual appliance in the company DMZ

> **Note**
>
> Only iOS and Android clients are supported.

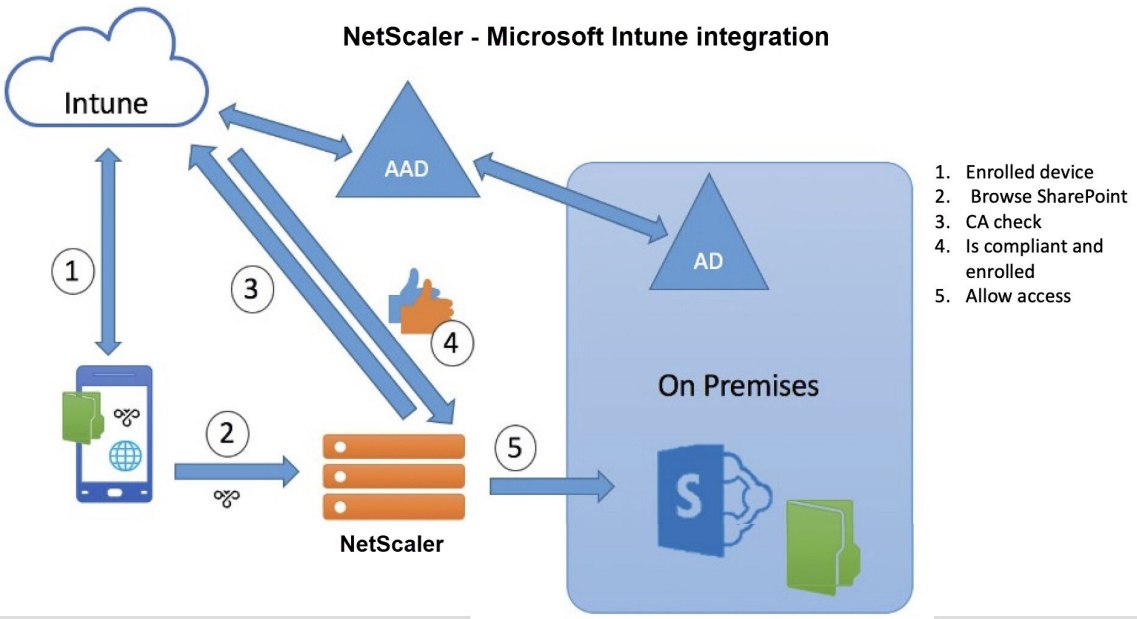
Understanding the NetScaler Gateway MDM Integration with Intune

January 8, 2024

The following is an example flow of events in a typical NetScaler Gateway MDM Integration with Intune:

1. Enroll a mobile device with Intune.
2. Corporate approved applications and device policies are pushed to the device.
3. Browse SharePoint (on-premises application) from the device.
4. The browser request goes to NetScaler Gateway.
5. The NetScaler Gateway appliance checks with Intune for the enrollment status of the device.

6. If a compliant device is enrolled successfully, the SharePoint access is granted.



When a device doesn't meet a conditional access policy, the NetScaler Gateway VPN client displays an error message. The message provides a link from the device to a page hosted by Intune that gives the user the option to enroll or to remediate the device's compliance status.

> **Note:**
>
> Administrators must ensure the following while pushing the certificates to Intune so that the users can differentiate between the various certificates on their device.

- Certificates must have a subject summary.
- The subject summaries for different certificates must be distinct.

Intune NAC v2 API support

As part of Intune NAC v2 API support, you must bind a Certificate Authority file (CA certificate) to ensure that the NetScaler appliance gets a valid certificate from mobile devices. In Intune NAC v2, the mobile devices send device IDs as part of the CA certificate. The CA certificate bound here must be the one used to issue client certificates to the end-user iOS and Android devices. If there are intermediate certificates, those must also be bound here.

For more details, see Intune NAC v2 API support

Configure Network Access Control device check for NetScaler Gateway virtual server for single factor login

January 8, 2024

This topic provides information on configuring the NetScaler Gateway to connect to an internal network from a mobile device (iOS and Android) with the Network Access Compliance (NAC) security offered by Microsoft Intune. When a user tries to connect to NetScaler Gateway from an iOS or Android VPN client, the gateway first checks with the Intune service if the device is a managed and a compliant device.

- Managed: The device is enrolled using the Intune Company Portal client.
- Compliant: Required policies pushed from the Intune MDM server are applied.

Only if the device is both managed and compliant, the VPN session is established and the user is provided access to the internal resources.

> **Note:**
>
> - In this setup, NetScaler Gateway at the back-end talks to the Intune service. The SSL profiles handle the incoming connections to the NetScaler Gateway. The NetScaler Gateway back-end communication handles any SNI requirements of the back-end cloud services (Intune).
> - SNI for DTLS gateway virtual server is supported in NetScaler Gateway release 13.0 build 64.x and later.
> - Intune NAC check, for the per-app VPN or even device wide VPN, is supported only when the VPN profile is provisioned by the Intune management portal (now known as, Microsoft Endpoint Manager). These features are not supported for end-user added VPN profiles. The end user device must have the VPN profile deployed to their device from Microsoft Endpoint Manager by their Intune administrator to use the NAC check.

Licensing

Citrix Enterprise Edition license is required for this functionality.

System requirements

- NetScaler Gateway release 11.1 build 51.21 or later
- iOS VPN –10.6 or later
- Android VPN –2.0.13 or later
- Microsoft

  - Azure AD access (having tenant and admin privileges)
  - Intune enabled tenant

- Firewall
  Enable firewall rules to all DNS and SSL traffic from subnet IP address to `https://login.microsoftonline.com` and `https://graph.windows.net` (port 53 and port 443)

Prerequisites

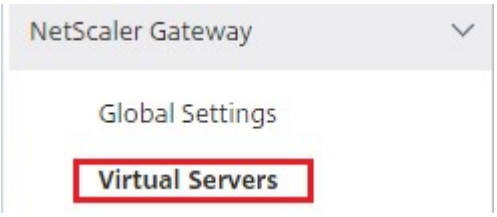
- All existing authentication policies must be converted from classic to advanced policies. For information on how to convert from classic policies to advanced policies, see https://support.citrix.com/article/CTX131024.
- Create a NetScaler Gateway application on the Azure portal. For details, see Configuring a NetScaler Gateway application on the Azure portal.
- Configure the OAuth policy on the NetScaler Gateway application that you created using the following application specific information.
  - Client ID / Application ID
  - Client secret / Application key
  - Azure tenant ID

References

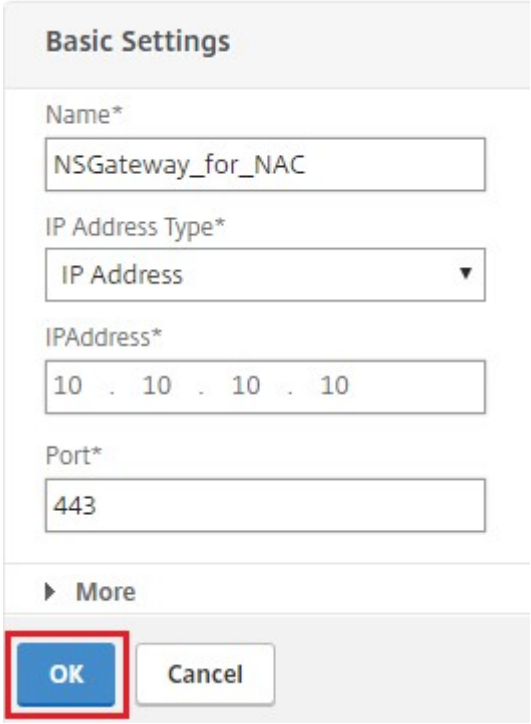
- This document captures the NetScaler Gateway setup configuration. Most of the Citrix SSO client (iOS/Android) configuration is done on the Intune side. For details on Intune VPN configuration for NAC, see https://docs.microsoft.com/en-us/mem/intune/protect/network-access-control-integrate.
- To configure the VPN profile for an iOS app, see https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-ios.
- To set up the NetScaler Gateway application on the Azure portal, see Configuring a NetScaler Gateway application on the Azure portal.

To add a NetScaler Gateway virtual server with nFactor for gateway deployment

1. Navigate to **NetScaler Gateway > Virtual Servers**.

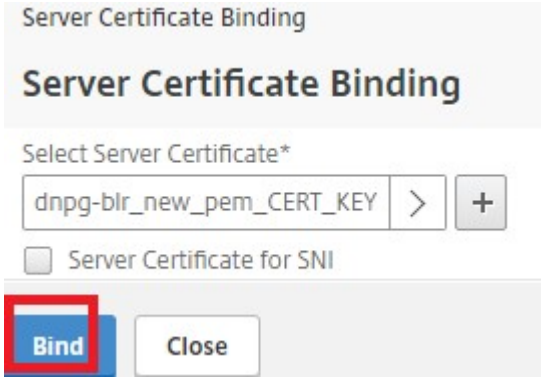


2. Click **Add**.
3. Provide the required information in the **Basic Settings** area and click **OK**.



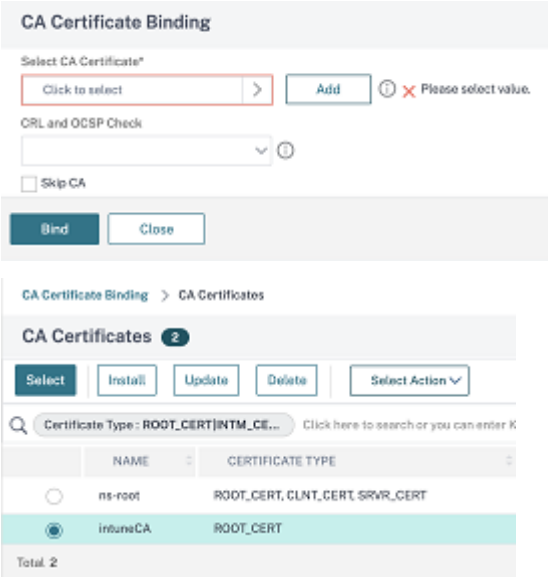
4. Select **Server Certificate**.

5. Select required server certificate and click **Bind**.



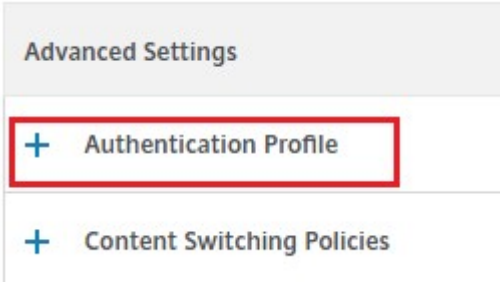
6. As part of Intune NAC v2 API support, you must bind a Certificate Authority file (CA certificate) to ensure that the NetScaler appliance gets a valid certificate from mobile devices. In Intune

NAC v2, the mobile devices send device IDs as part of the client certificate. The CA certificate bound here must be the one used to issue client certificates to the end user iOS and Android devices. If there are intermediate certificates, those must also be bound here. For more on Intune configuration, see Configuring a NetScaler Gateway application on the Azure portal. For Intune NAC v2 API support, select the required CA certificate and click **Bind**.

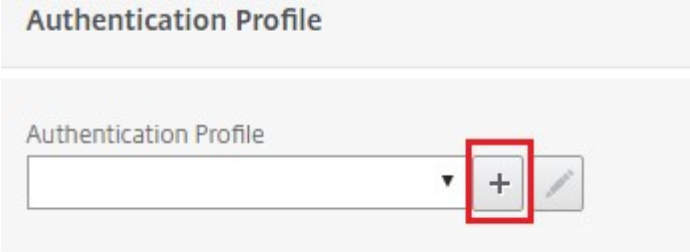


7. Click **Continue**.
8. Click **Continue**.
9. Click **Continue**.
10. Click the plus icon **[+]** next to **Policies** and select **Session** from the **Choose Policy** list and select **Request** from the **Choose Type** list and click **Continue**.
11. Click the plus icon **[+]** next to **Select Policy**.
12. On the **Create NetScaler Gateway Session Policy** page, provide a name for the Session policy.
13. Click the plus icon [+] next to **Profile** and on the **Create NetScaler Gateway Session Profile** page, provide a name for the Session profile.
14. On the **Client Experience** tab, click the check box next to **Clientless Access** and select **Off** from the list.
15. Click the check box next to **Plug-in Type** and select Windows/Mac OS X from the list.
16. Click **Advanced Settings** and select the check box next to **Client Choices** and set its value to **ON**.
17. On the **Security** tab, click the check box next to **Default Authorization Action** and select **Allow** from the list.

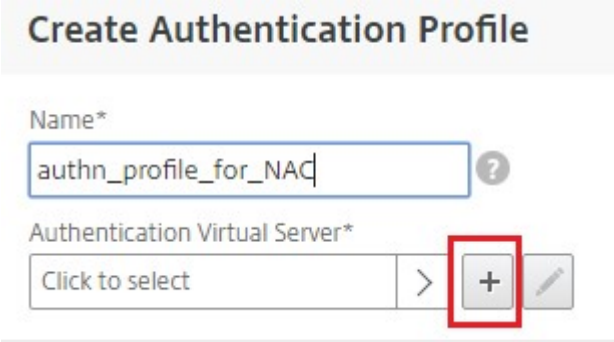
18. On the **Published Applications** tab, click the check box next to **ICA Proxy** and select **OFF** from the list.
19. Click **Create.**
20. On the **Create NetScaler Gateway Session Policy** page, In the **Expression** area, configure the qualifying expression.
21. Click **Create**.
22. Click **Bind**.
23. Select **Authentication Profile** in **Advanced Settings**.



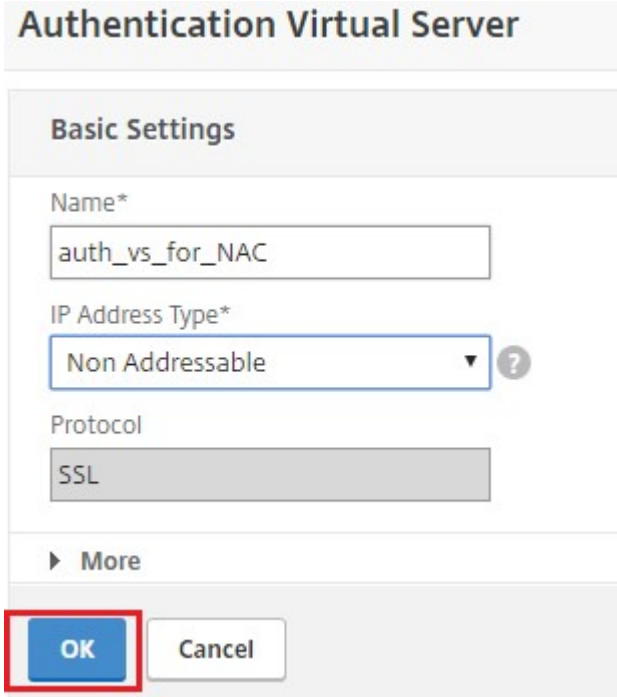
24. Click the plus icon **[+]** and provide a name for the Authentication Profile.



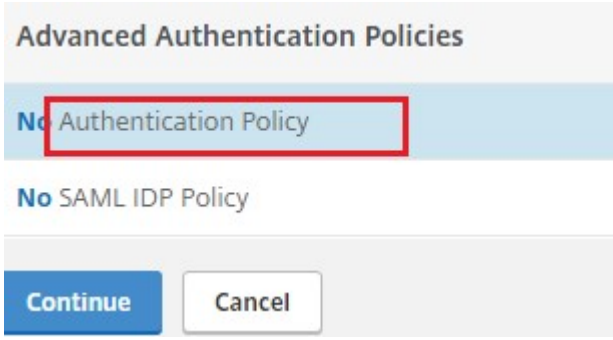
25. Click the plus icon **[+]** to create an authentication virtual server.



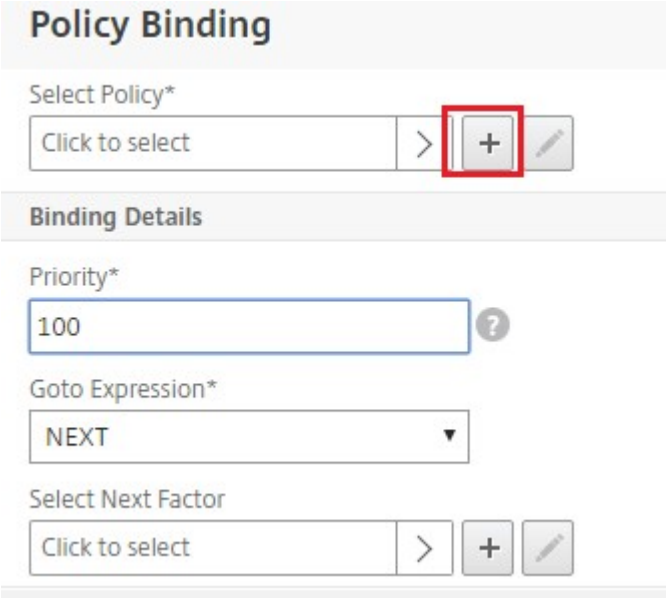
26. Specify name and IP address type for authentication virtual server under **Basic Settings** area and click **OK**. The IP address type can be **Non Addressable** as well.



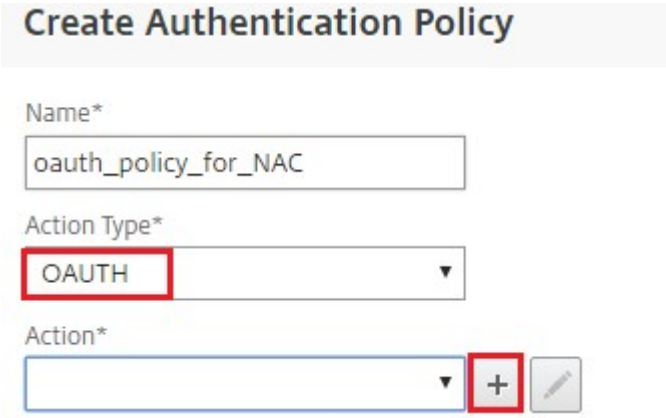
27. Click **Authentication Policy**.



28. Under the Policy Binding view, click the plus icon **[+]** to create an authentication policy.



29. Select **OAUTH** as an **Action Type** and click the plus icon **[+]** to create an OAuth action for NAC.

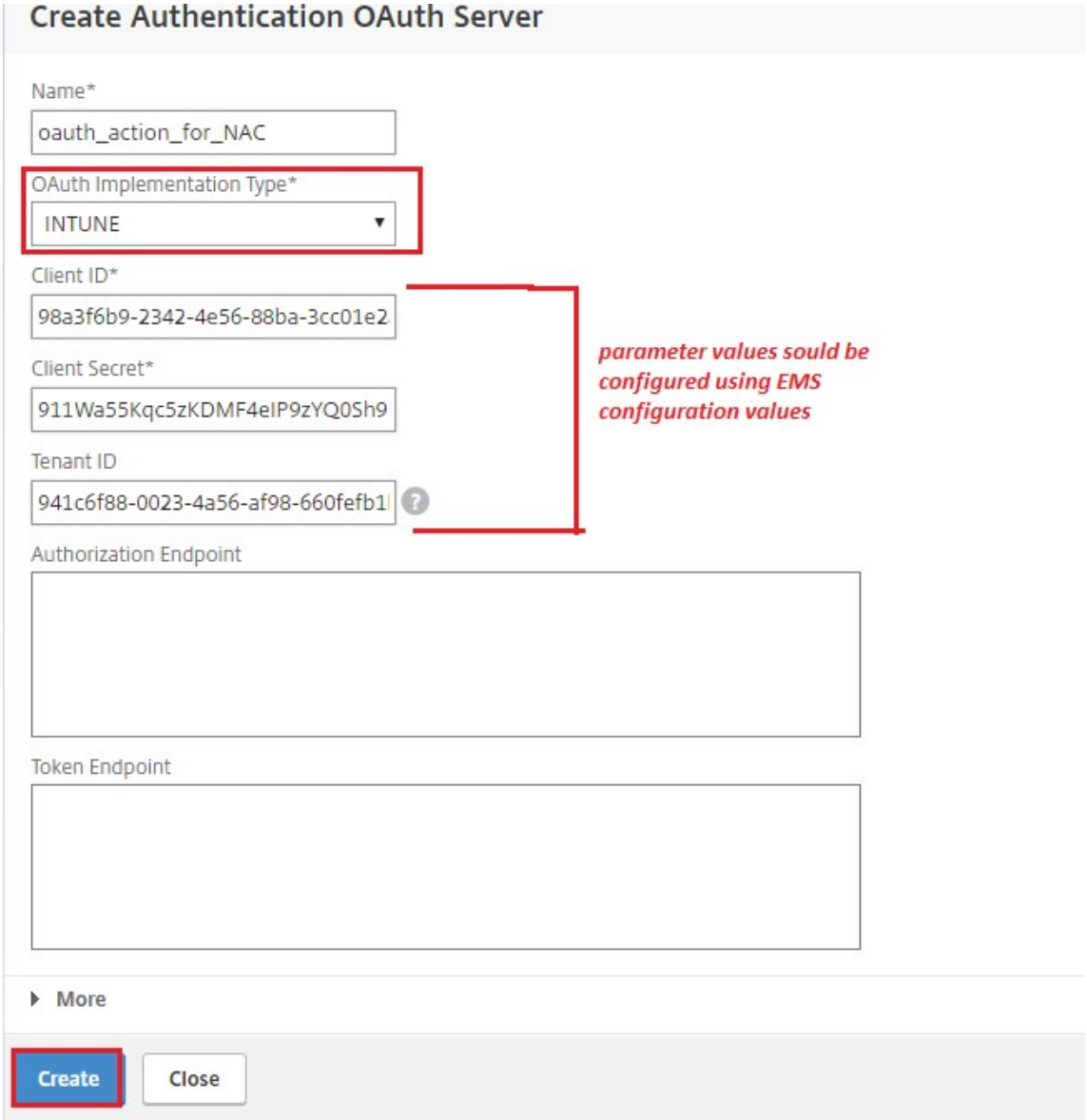


30. Create an OAuth action using **Client ID**, **Client Secret**, and **Tenant ID**.

> **Note:**
>
> - **Client ID**, **Client Secret,** and **Tenant ID** are generated after configuring the NetScaler Gateway application on the Azure portal.
> - Note down the Client ID/Application ID, Client Secret/Application Secret, and Azure tenant ID information as they are required when creating an OAuth action on NetScaler Gateway later.

Ensure that you have an appropriate DNS name server configured on your appliance to resolve and reach;

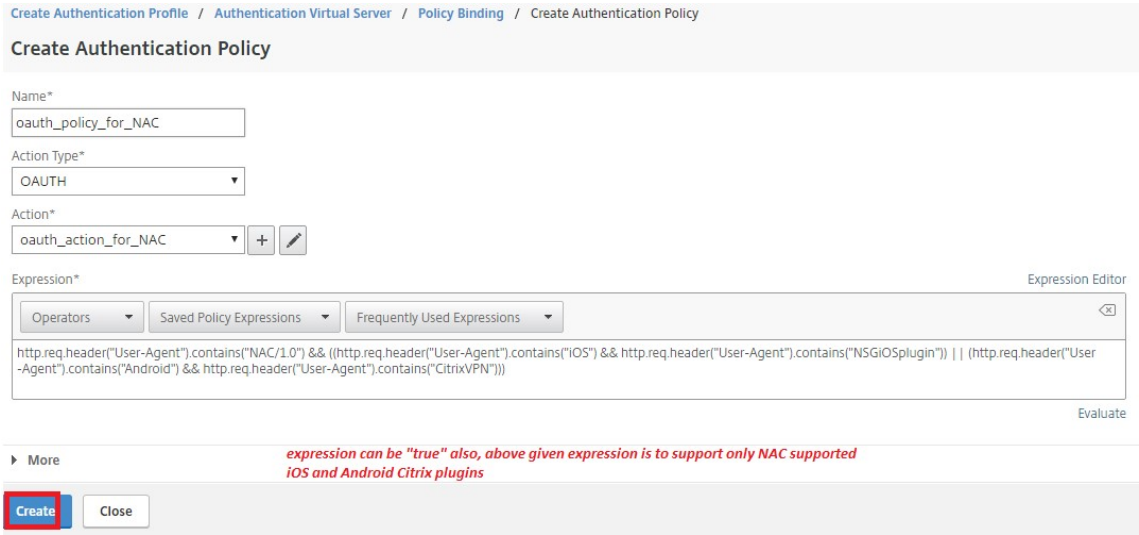
- `https://login.microsoftonline.com/`,
- `https://graph.windows.net/`,
- *.manage.microsoft.com.



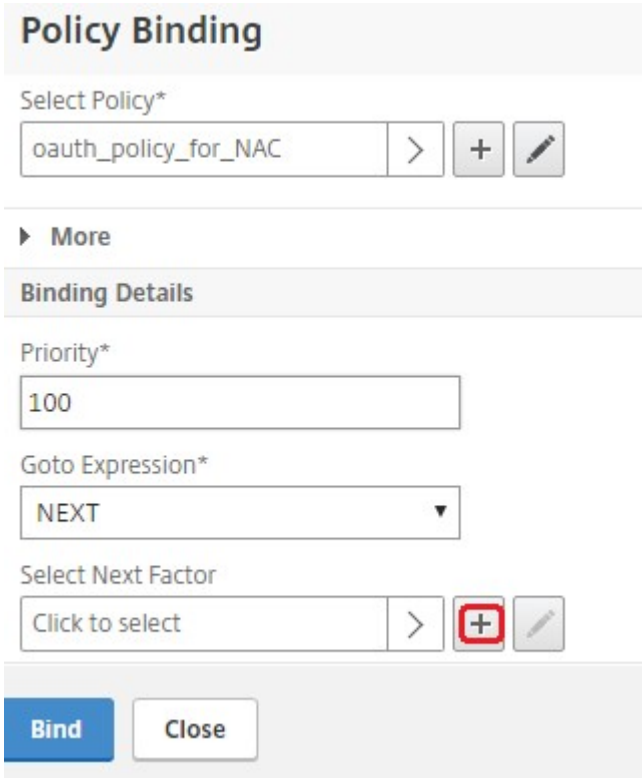
31. Create authentication policy for **OAuth Action**.

Rule:

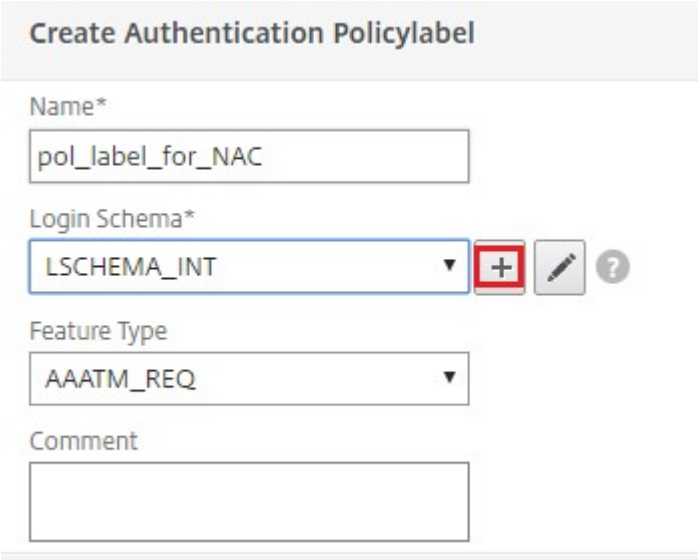
```
http.req.header("User-Agent").contains("NAC/1.0")&& ((http.req.header("User-Agent").contains("iOS") && http.req.header("User-Agent").contains("NSGiOSplugin")) || (http.req.header("User-Agent").contains("Android") && http.req.header("User-Agent").contains("CitrixVPN")))
```

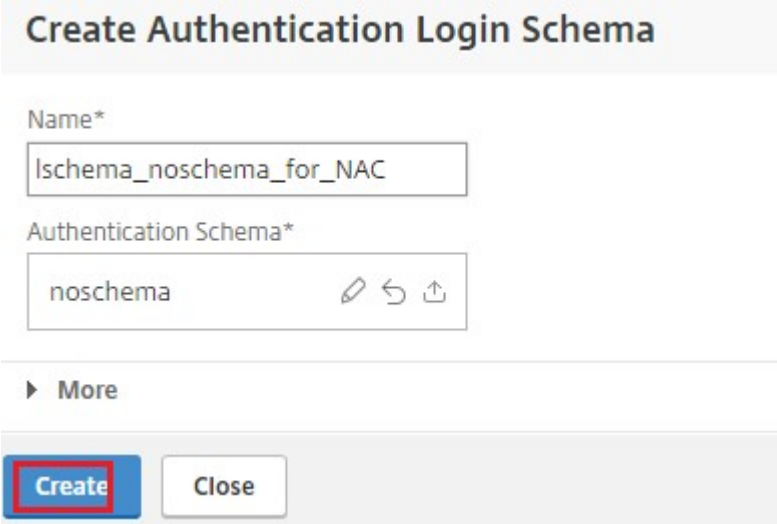
32. Click the plus icon **[+]** to create a nextFactor policy label.



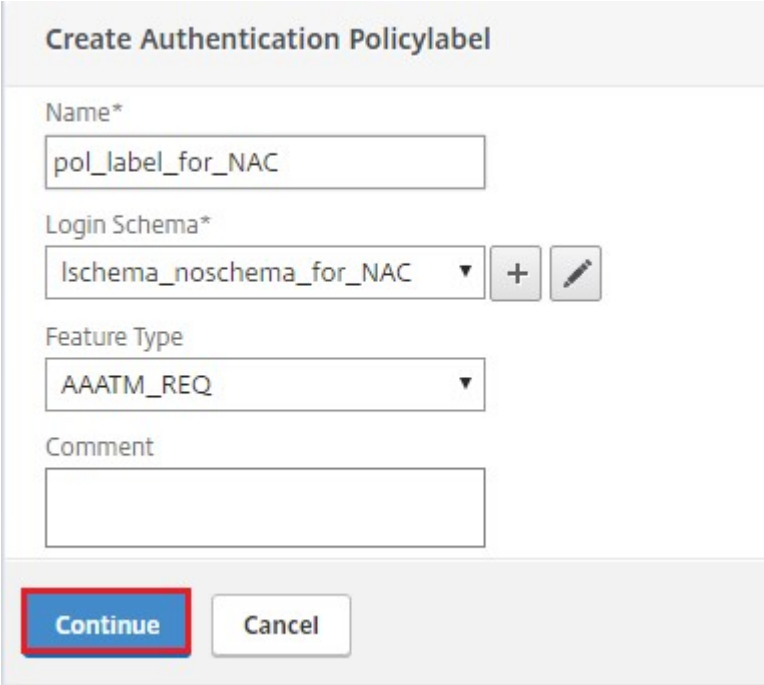
33. Click the plus icon **[+]** to create a login schema.



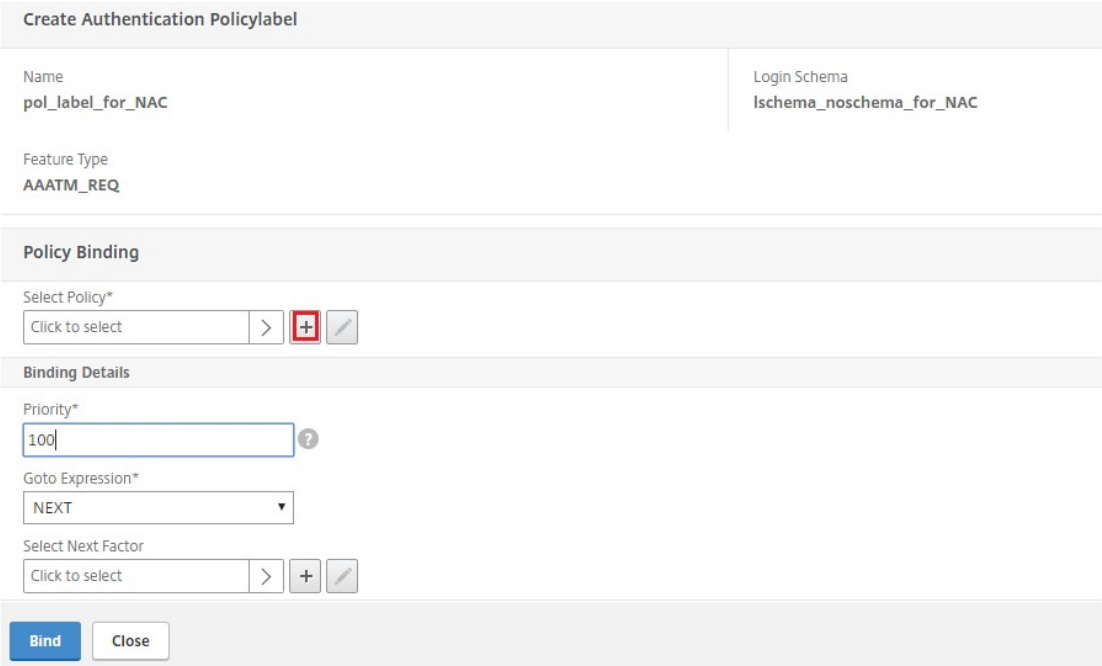
34. Select **noschema** as an authentication schema and click **Create**.



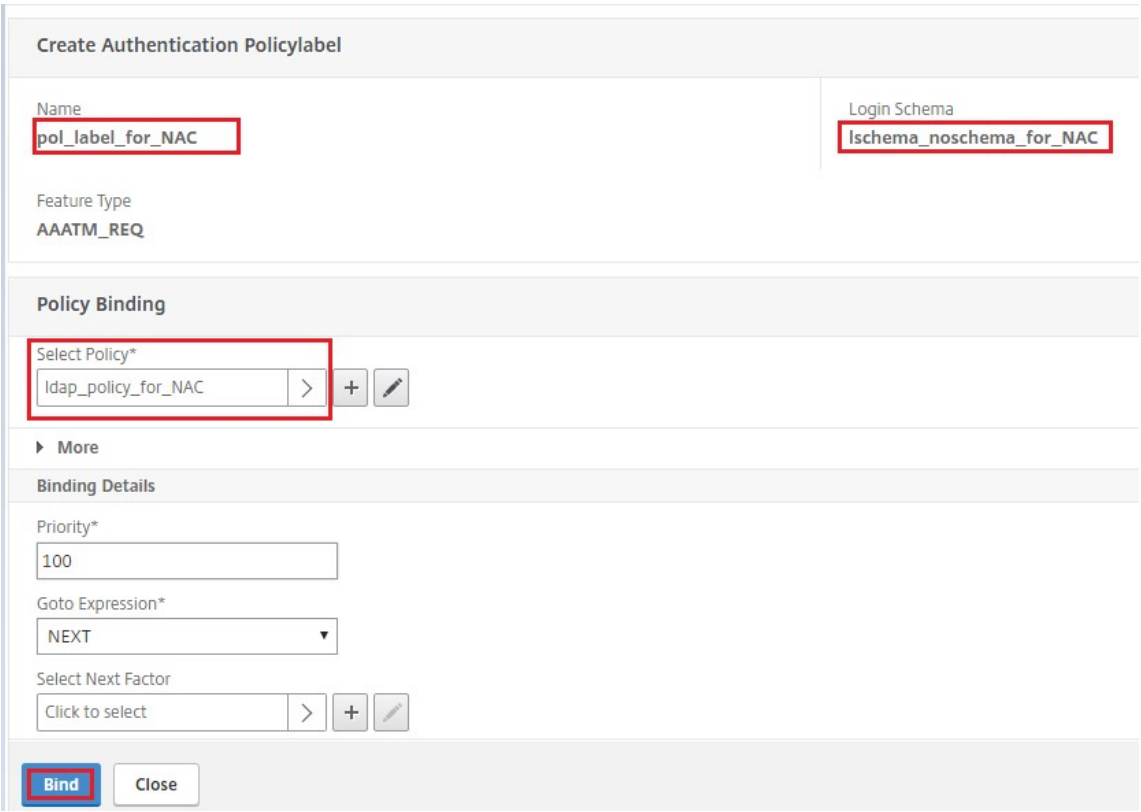
35. After selecting the created login schema, click **Continue**.



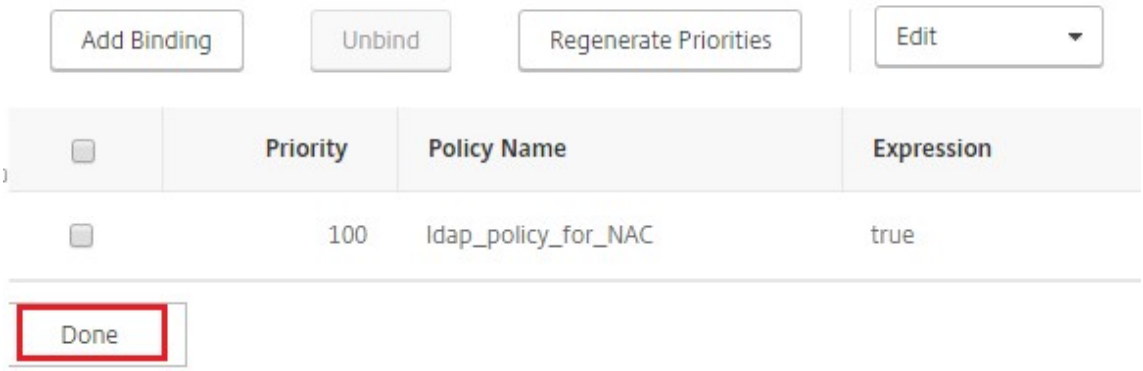
36. In **Select Policy**, select an existing authentication policy for user login or click the plus icon **+** to create an authentication policy.
    For details on creating an authentication policy, see Configuring advanced authentication policies and Configuring LDAP Authentication.



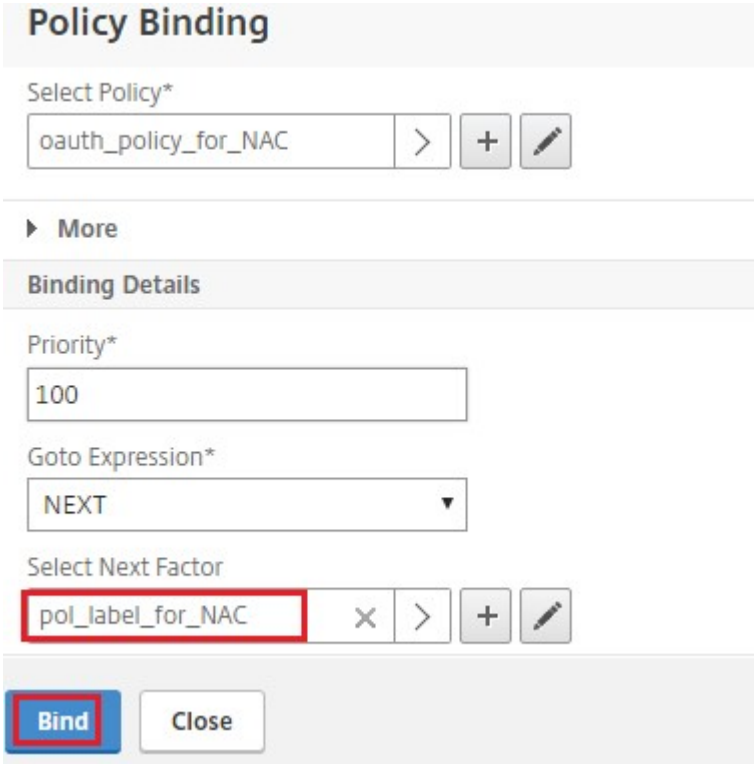
37. Click **Bind**.



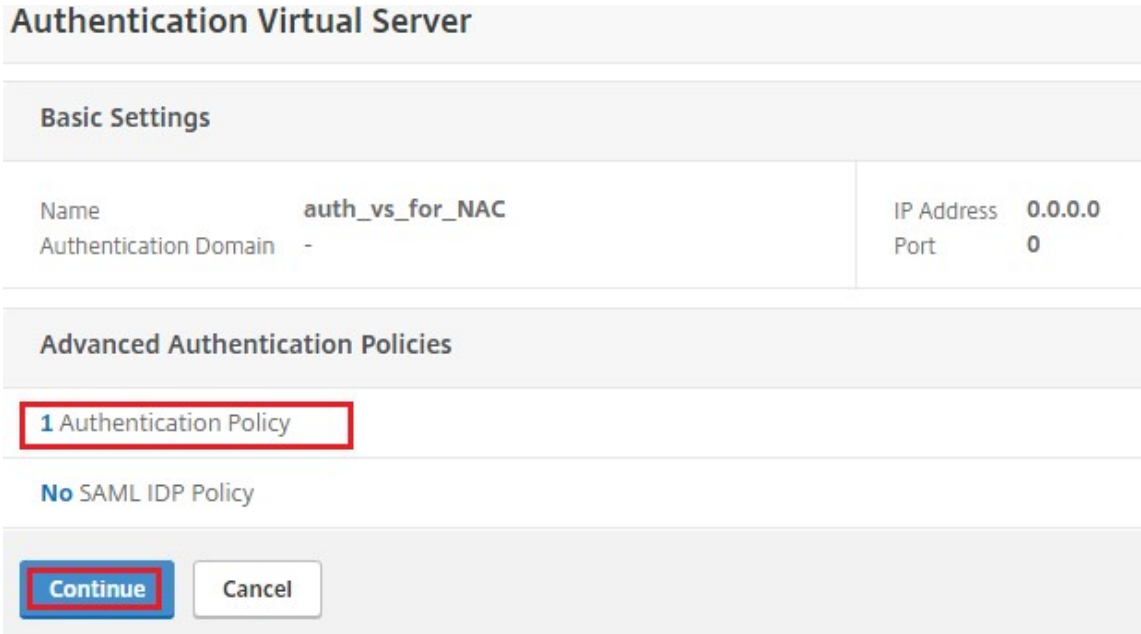
38. Click **Done**.



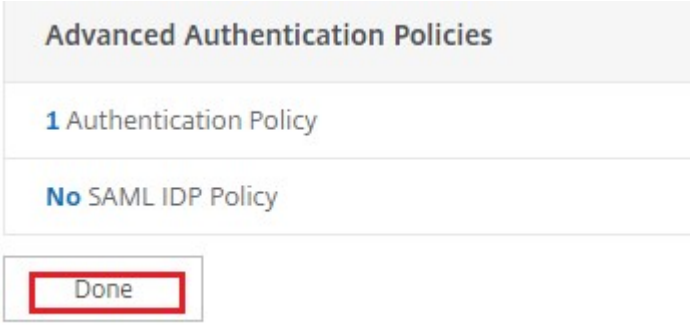
39. Click **Bind**.



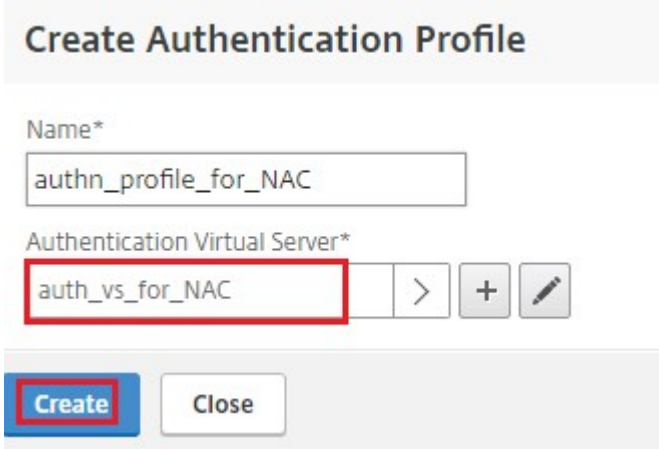
40. Click **Continue**.



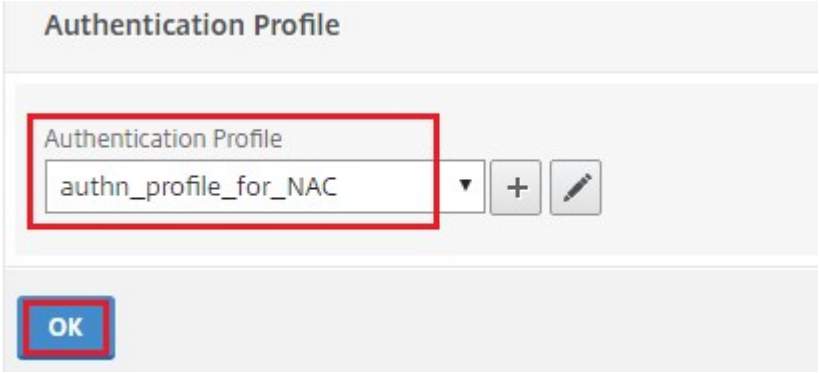
41. Click **Done**.



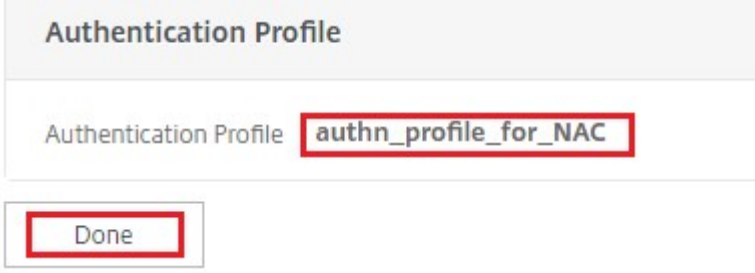
42. Click **Create**.



43. Click **OK**.



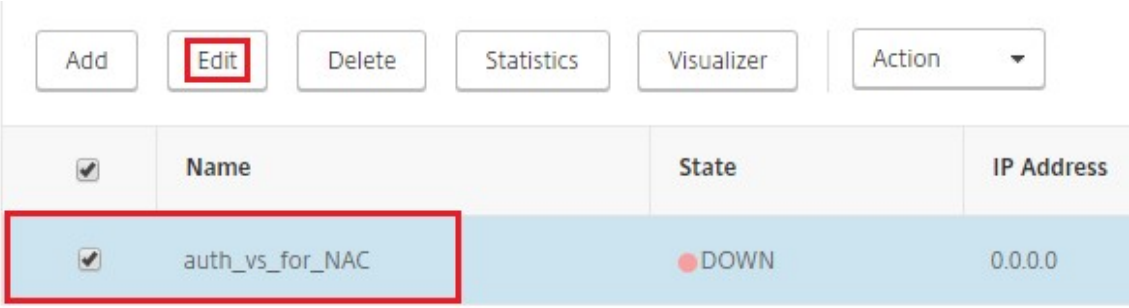
44. Click **Done**.



To bind authentication login schema to authentication virtual server to indicate VPN plug-ins to send device ID as part of /cgi/login request

1. Navigate to **Security** > **AAA - Application Traffic** > **Virtual Servers**.

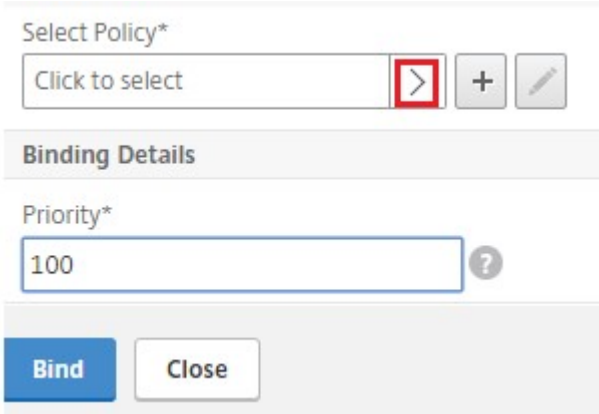
2. Select the previously selected virtual-server and click **Edit**.



3. Click **Login Schemas** under **Advanced Settings**.

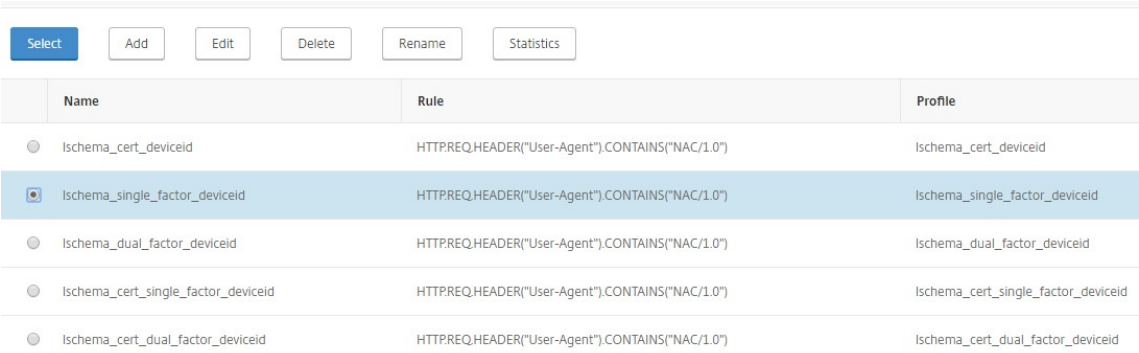
4. Click **Login Schemas** to bind.

5. Click **[>]** to select and bind the existing build in login schema policies for NAC device check.

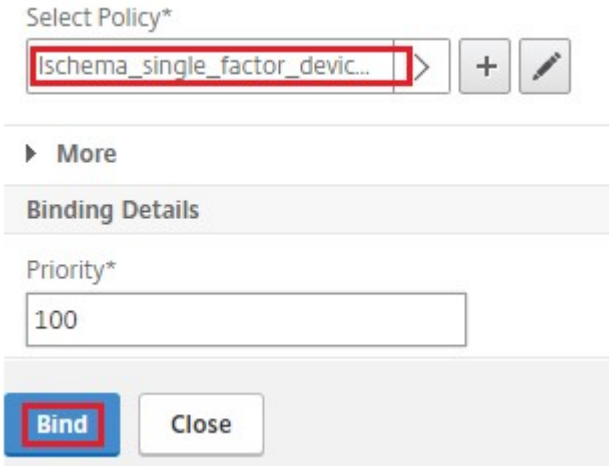


6. Select the required login schema policy appropriate for your authentication deployment and click **Select**.

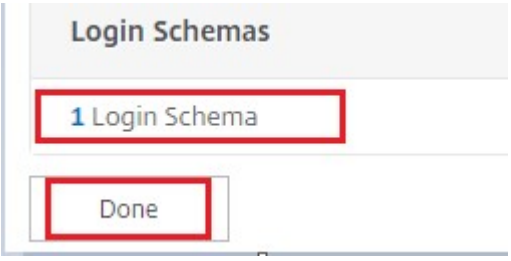
   In the previous explained deployment, single factor authentication (LDAP) along with a NAC OAuth Action policy is used. Hence **lschema_single_factor_deviceid** is selected.



7. Click **Bind**.



8. Click **Done**.



Intune NAC v2 API support

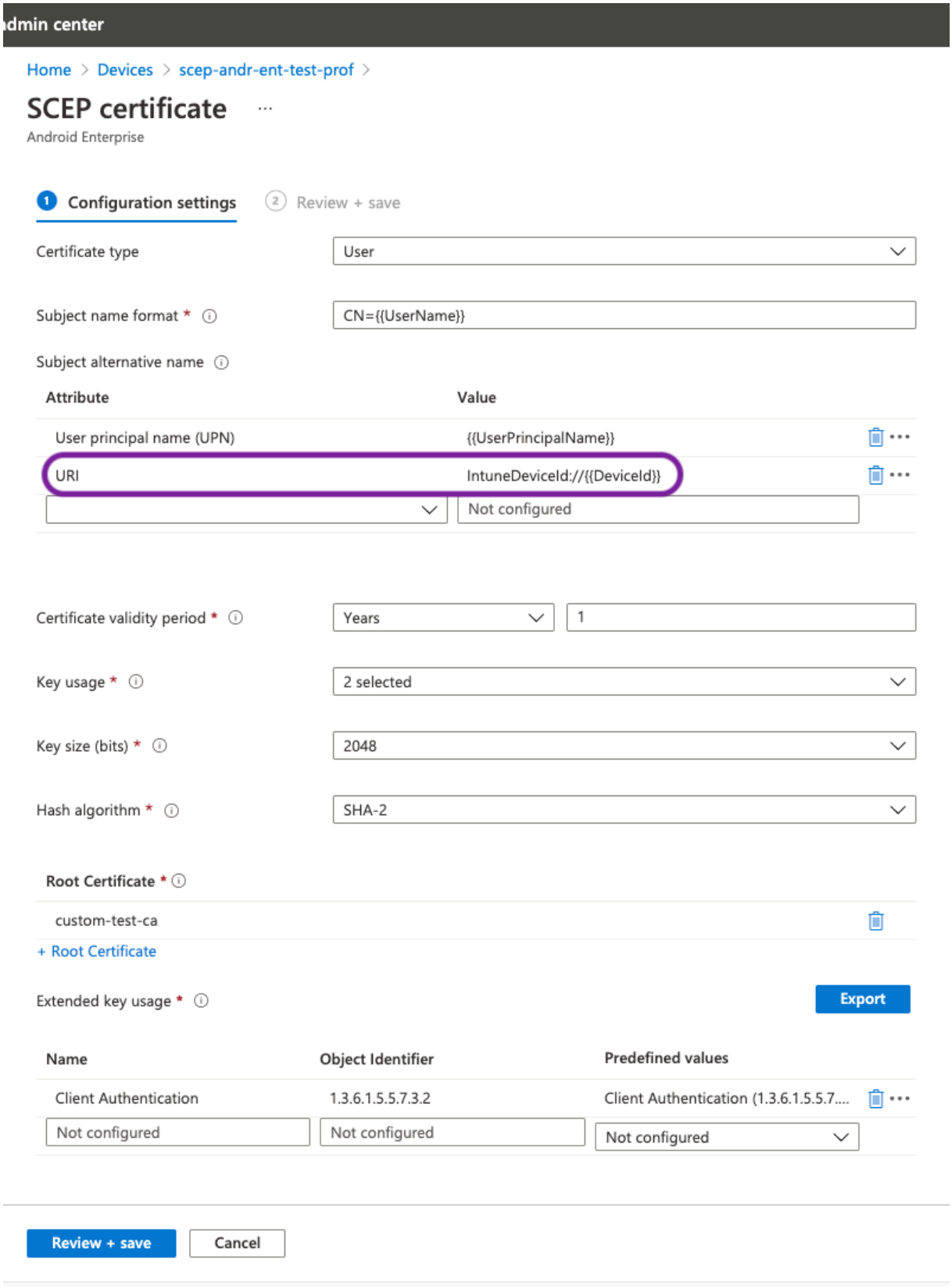
As part of Intune NAC v2 API support, you must bind a Certificate Authority file (CA certificate) to ensure that the NetScaler appliance gets a valid certificate from mobile devices. In Intune NAC v2, the mobile devices send device IDs as part of the CA certificate. The CA certificate bound here must be the one used to issue client certificates to the end-user iOS and Android devices. If there are intermediate certificates, those must also be bound here.

You can use the following sample command to bind your CA certificate.

```
bind ssl vserver intune_nac_check_443 -certkeyName clientca -CA -
    ocspCheck Optional
```

Important:

- Intune NAC v2 API support is available in the NetScaler Gateway versions 13.1 build 12.50 or later and 13.0 build 84.11 or later.
- You must enable client certificate based authentication by setting `clientAuth` to ENABLED and `clientCert` to OPTIONAL on the VPN and authentication virtual servers. The `clientCert` parameter is set to OPTIONAL so that other endpoints which do not need the Intune NAC check can authenticate via the same virtual server without providing the client certificate. Android and iOS devices must provide the client certificate. Otherwise the Intune NAC check fails.
- You must ensure that the client certificates provisioned via Intune on the mobile device must have Intune Device ID in the SAN field of URI type as called out in the New Microsoft Intune service for network access control document. For details, see https://techcommunity.microsoft.com/t5/intune-customer-success/new-microsoft-intune-service-for-network-access-control/ba-p/2544696.
  The format of the URI value field must be same as indicated in the following figure. Also, the Citrix SSO app must use the same certificate for authenticating with the gateway.



Troubleshooting

General issues

Issue	Resolution
The “Add Policy Required”message appears when you open an app	Add policies in the Microsoft Graph API
There are policy conflicts	Only a single policy per app is allowed
Your app can’t connect to internal resources	Ensure that the correct firewall ports are open, used correct tenant ID, and so on

NetScaler Gateway issues

Issue	Resolution
The permissions required to be configured for the gateway app on Azure are unavailable.	Check if a proper Intune license is available. Try using the manage.windowsazure.com portal to see if the permission can be added. Contact Microsoft support if the issue persists.
NetScaler Gateway cannot reach `login.microsoftonline.comandgraph.windows.net`.	From NS Shell, check if you are able to reach the following Microsoft website: cURL -v -k https://login.microsoftonline.com. Then, check whether DNS is configured on NetScaler Gateway. Also check that the firewall settings are correct (in case DNS requests are firewalled).
An error appears in ns.log after you configure OAuthAction.	Check if Intune licensing is enabled and the Azure Gateway app has the proper permissions set.
`Sh OAuthAction` command does not show OAuth status as complete.	Check the DNS settings and configured permissions on the Azure Gateway App.
The Android or iOS device does not show the dual authentication prompt.	Check if the Dual Factor Device ID logonSchema is bound to the authentication virtual server.

NetScaler Gateway OAuth status and error condition

Status	Error condition
AADFORGRAPH	Invalid secret, URL not resolved, connection timeout
MDMINFO	`*manage.microsoft.com`is down or unreachable
GRAPH	Graph endpoint is down unreachable
CERTFETCH	Cannot talk to "Token Endpoint: https://login.microsoftonline.com because of a DNS error. To validate this configuration, go to the Shell prompt and type cURL https://login.microsoftonline.com. This command must validate.

Note: When the OAuth status is successful, the status is displayed as COMPLETE.

Intune configuration check

Make sure to select the **I agree** check box in **Base iOS VPN configuration for Citrix SSO > Enable network access control (NAC)**. Else, the NAC check does not work.

Configuring a NetScaler Gateway application on the Azure portal

January 8, 2024

The following section lists steps to configure a NetScaler Gateway application on the Azure portal.

Prerequisites

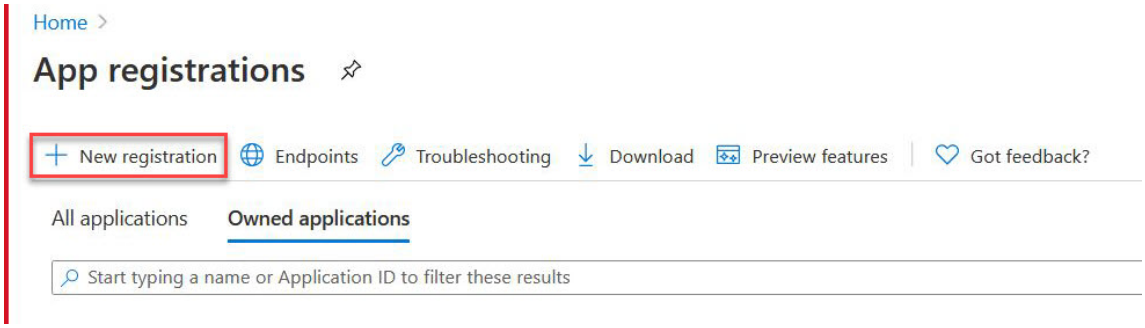
- Azure global admin credentials
- Intune licensing is enabled
- For Intune Integration you must create a NetScaler Gateway application on the Azure portal.
- Once the NetScaler Gateway application is created, configure the OAuth policy on NetScaler Gateway using the following application specific information:
  - Client ID / Application ID
  - Client Secret / Application Key

  - Azure Tenant ID

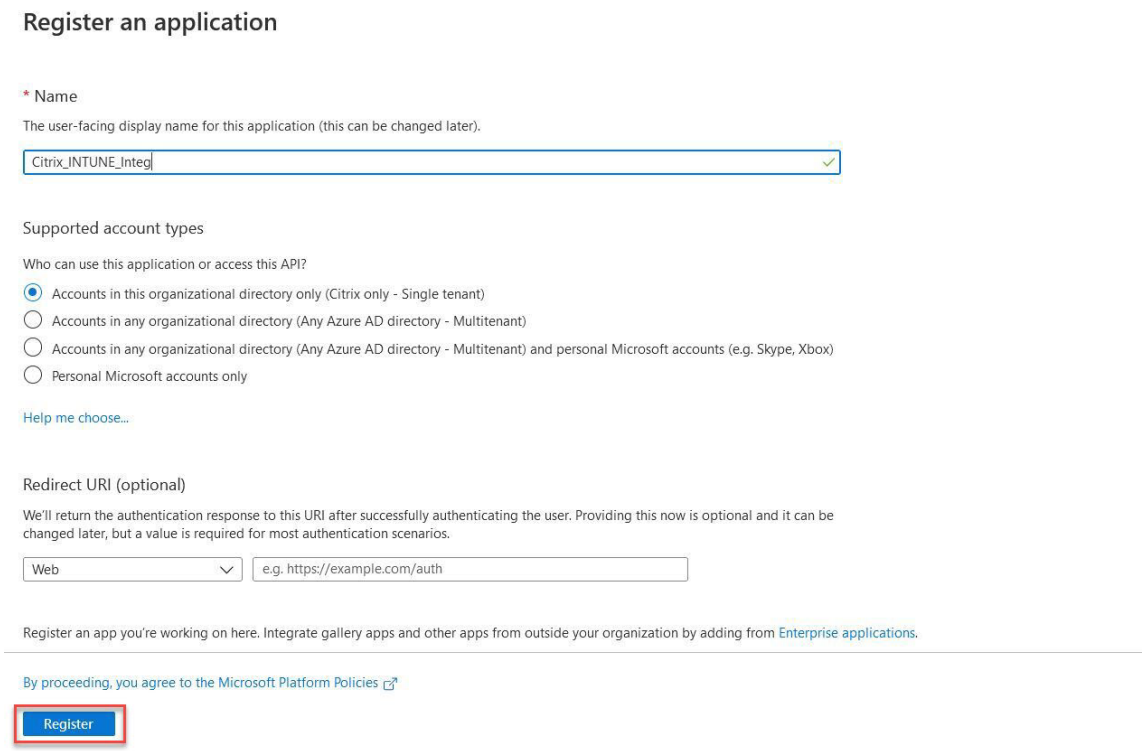
- NetScaler Gateway uses the app client id and client secret to communicate with Azure and check for NAC compliance.

To create a NetScaler Gateway app on Azure

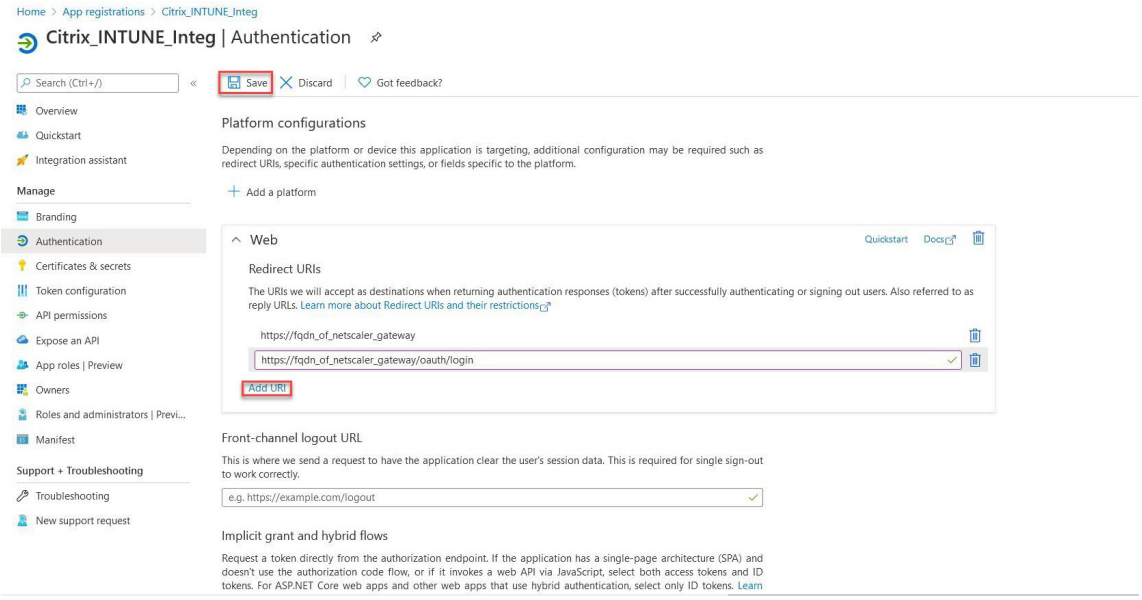
1. Log in to portal.azure.com
2. Click **Azure Active Directory**.
3. Click **App registrations** and click **New registration**.



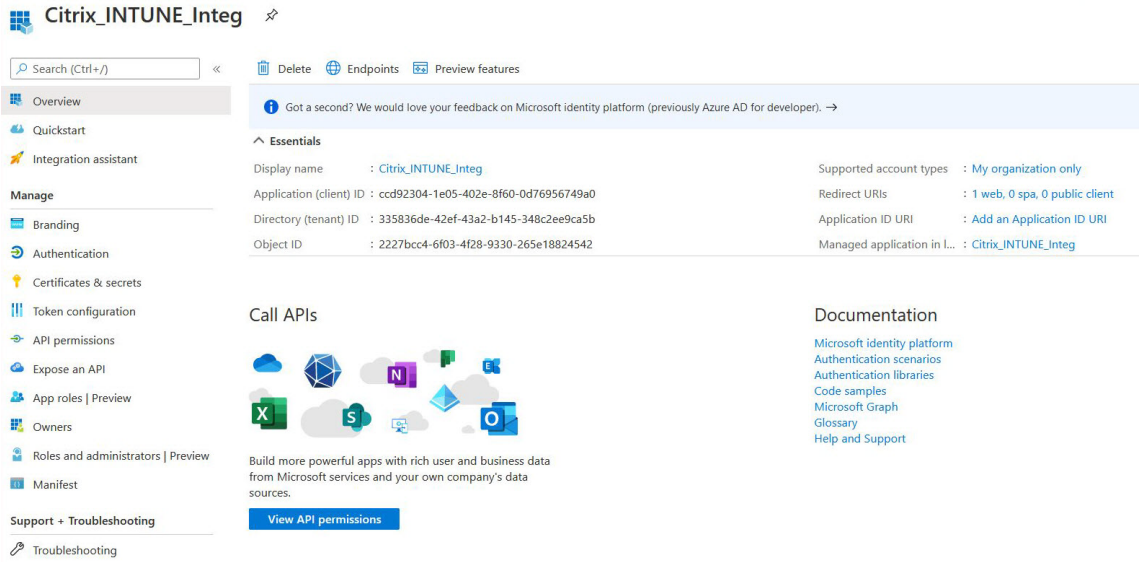
4. On the **Register an application** page, enter an app name and click **Register**.



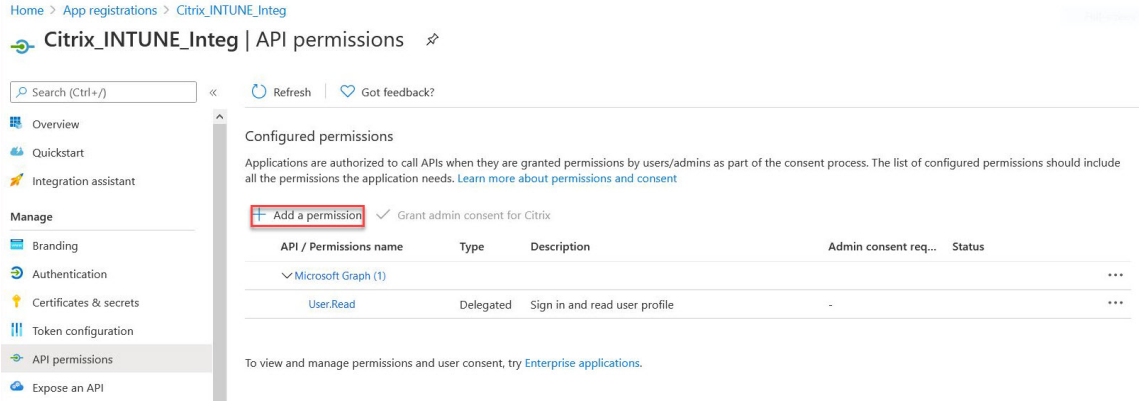
5. Navigate to **Authentication**, click **Add URI**, enter FDQN for NetScaler Gateway, and click **Save**.



6. Navigate to the **Overview** page to get Client ID, Tenant ID, and Object ID.

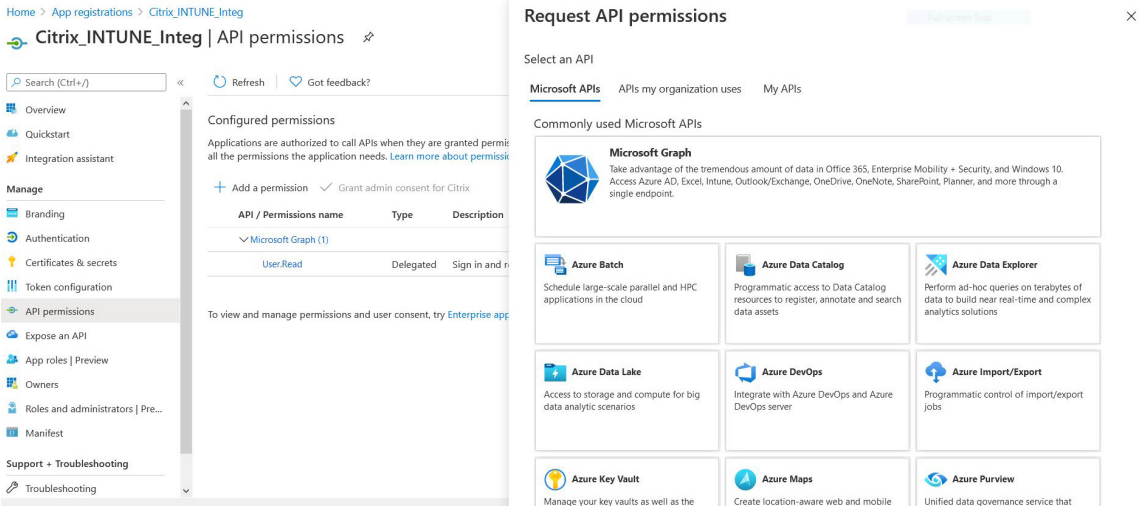


7. Navigate to **API permissions** and click **Add a permission**.

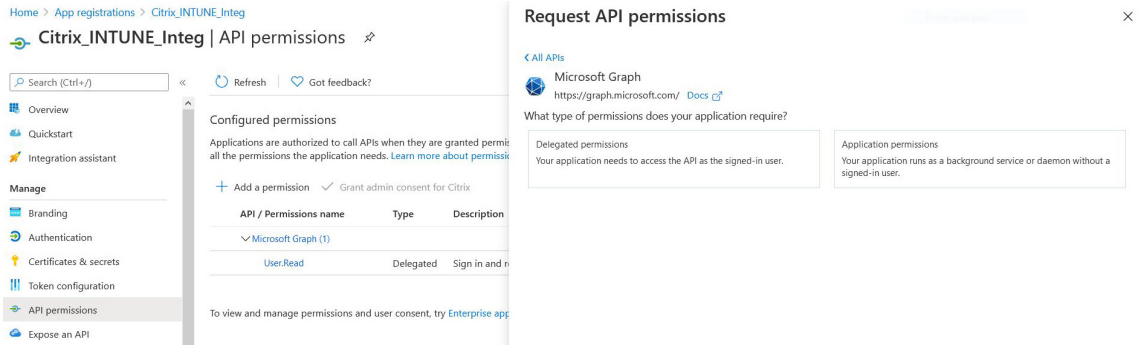


> **Note:**
>
> All Azure AD applications that call the `https://login.microsoftonline.com`, `https://graph.microsoft.com`, or `https://graph.windows.net` service endpoints require the API permission to be assigned for the gateway to be able to call the NAC API. The available API Permissions are:
>
> - Application.Read.All
> - Application.ReadWrite.All
> - Application.OwnedBy
> - Directory.Read.All
>
> The preferred permission is **Application.Read.All**.
>
> For more details, see https://techcommunity.microsoft.com/t5/intune-customer-success/support-tip-intune-service-discovery-api-endpoint-will-require/ba-p/2428040

8. Click the **Microsoft Graph** tile to configure API permissions for Microsoft Graph.

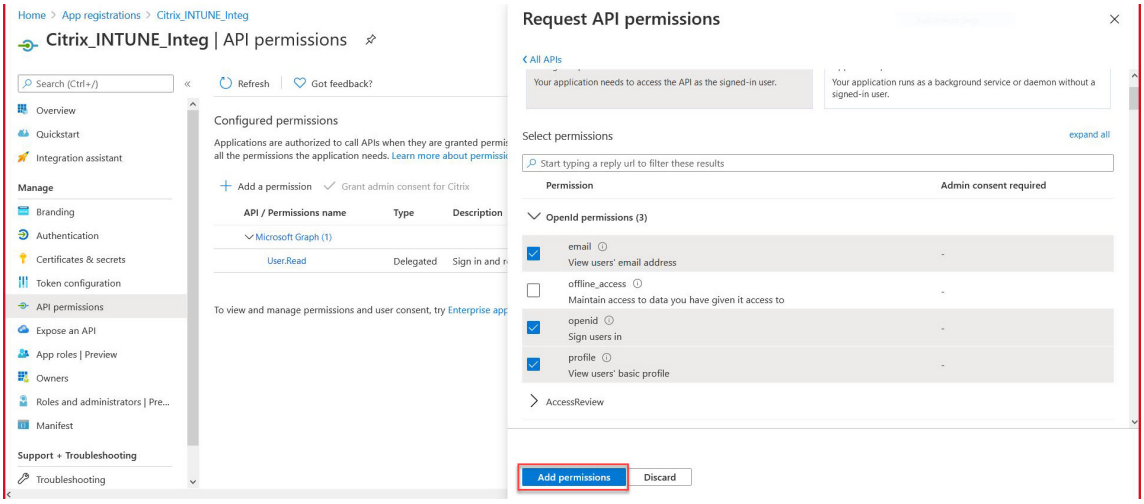


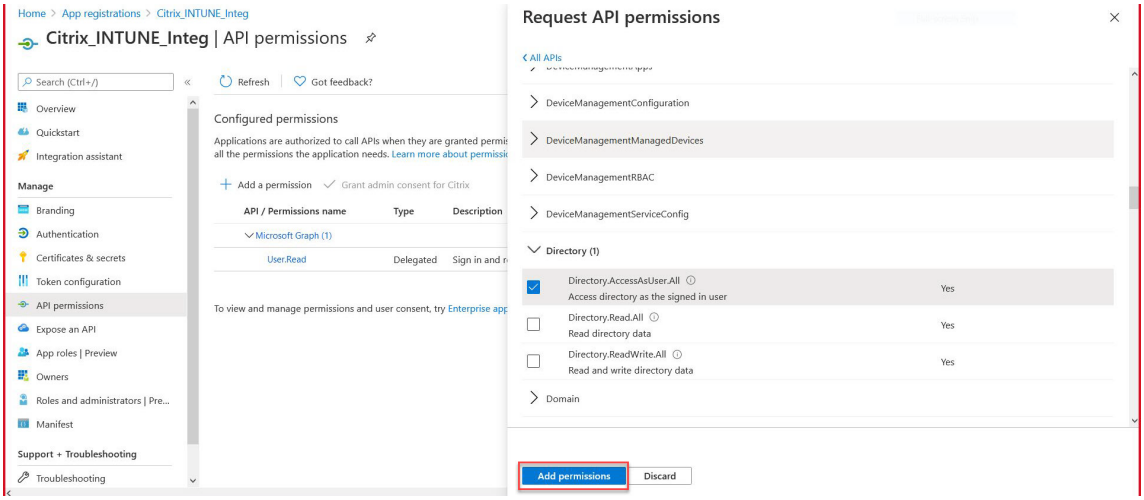
9. Click the **Delegated permissions** tile.

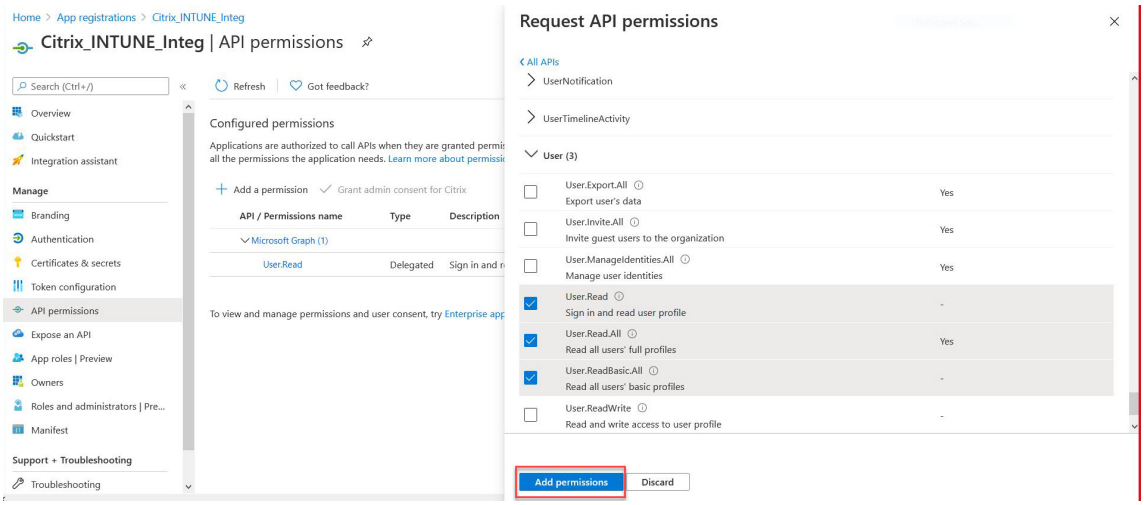


10. Select the following permissions and click **Add permissions**.

    - Email
    - `openid`
    - Profile
    - Directory.AccessAsUser.All
    - User.Read
    - User.Read.All
    - User.ReadBasic.All







Permissions for Intune NAC check:

All Azure AD applications that call the `https://login.microsoftonline.com`, `https://graph.microsoft.com`, or `https://graph.windows.net` service endpoints require the API permission to be assigned for the gateway to be able to call the NAC API. The available API Permissions are:

- Application.Read.All
- Application.ReadWrite.All
- Application.OwnedBy
- Directory.Read.All

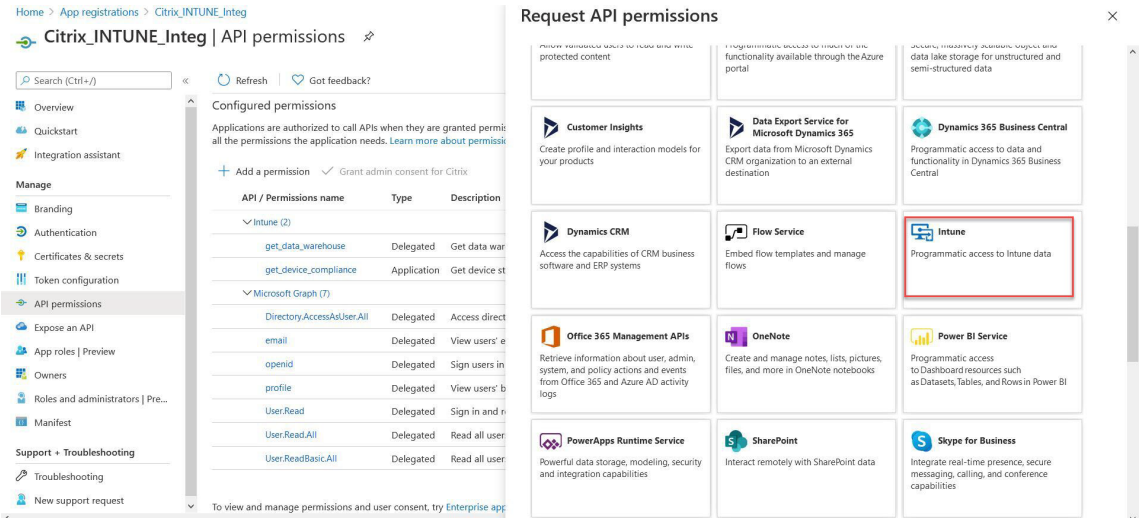
The preferred permission is **Application.Read.All**.

For more details, see https://techcommunity.microsoft.com/t5/intune-customer-success/support-tip-intune-service-discovery-api-endpoint-will-require/ba-p/2428040

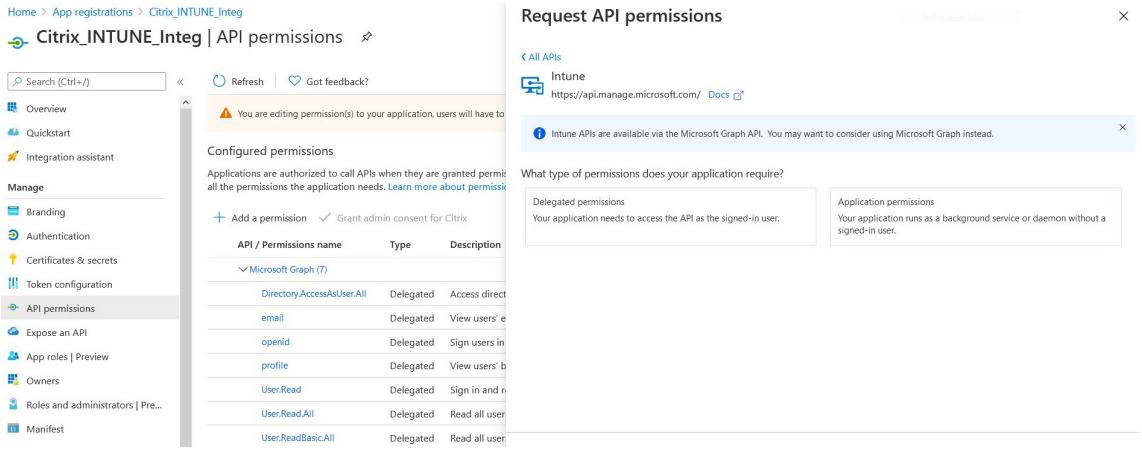
Note:

> If a customer is only using the Intune Action for NAC check, then the only permission required is **Application.Read.All** in Microsoft Graph.

11. Click the **Intune** tile to configure API permissions for Intune.



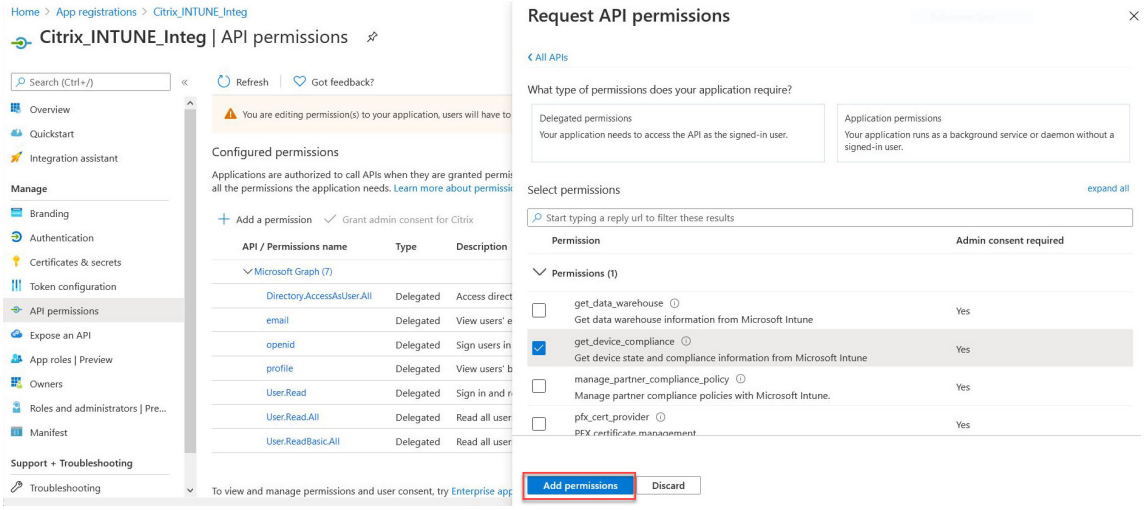
12. Click the **Application permissions** tile and the **Delegated permissions** tile to add permissions for Get_device_compliance and Get_data_warehouse respectively.

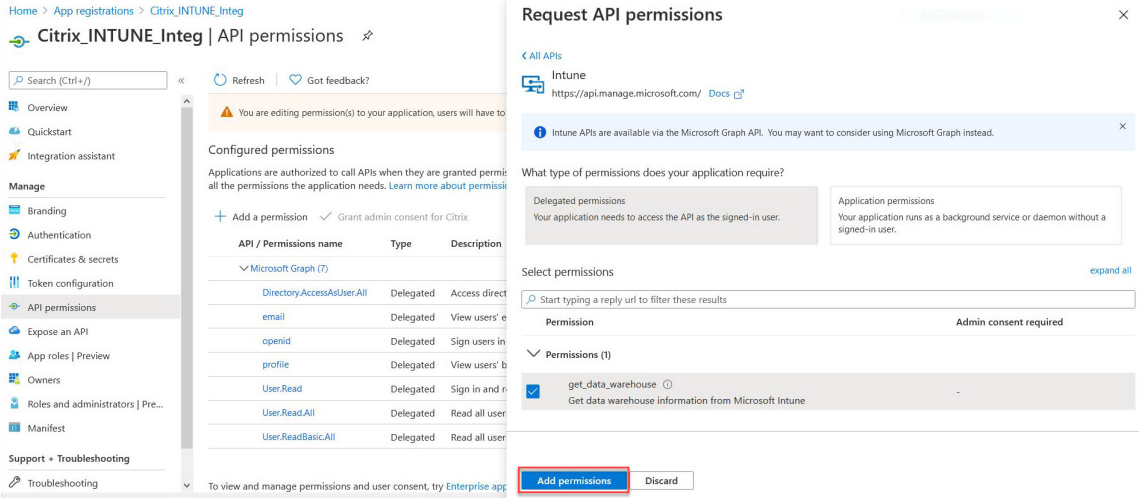


13. Select the following permissions, and click **Add permissions**.

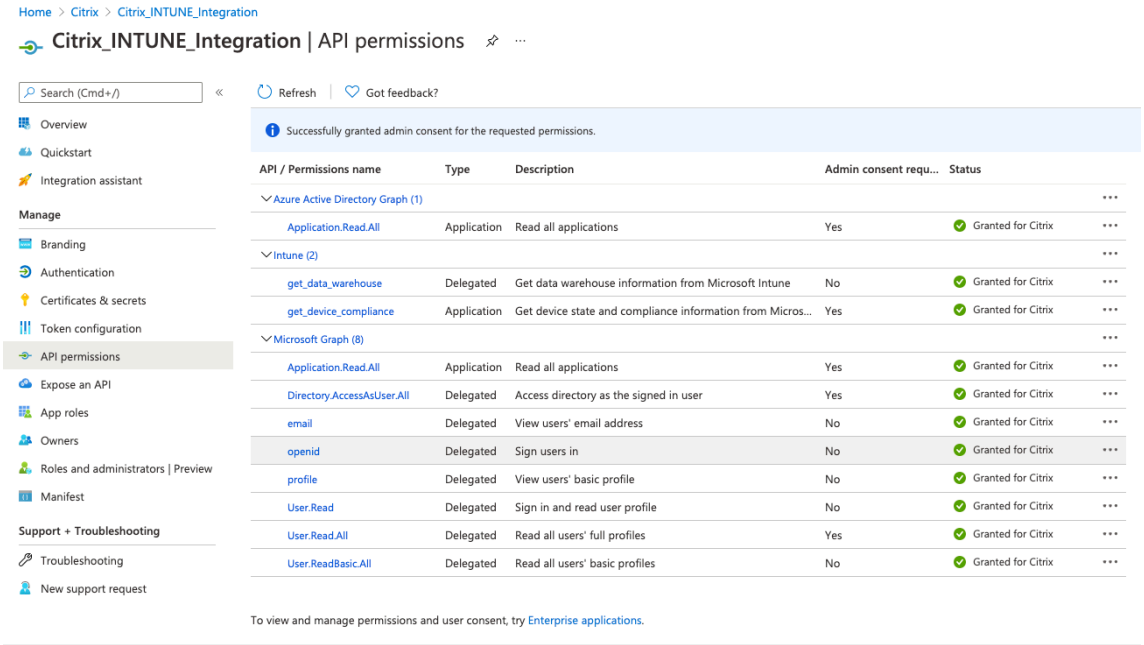
    - Get_device_compliance - Application permissions
    - Get_data_warehouse - Delegated permissions

> **Note:**
>
> For the Intune NAC check, the only permission required is **Get_device_compliance**.

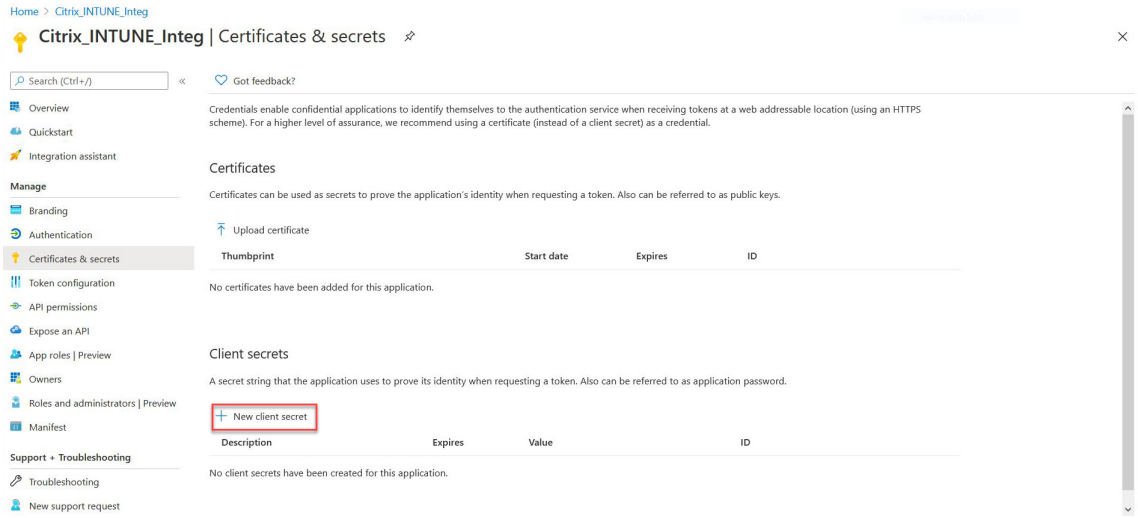




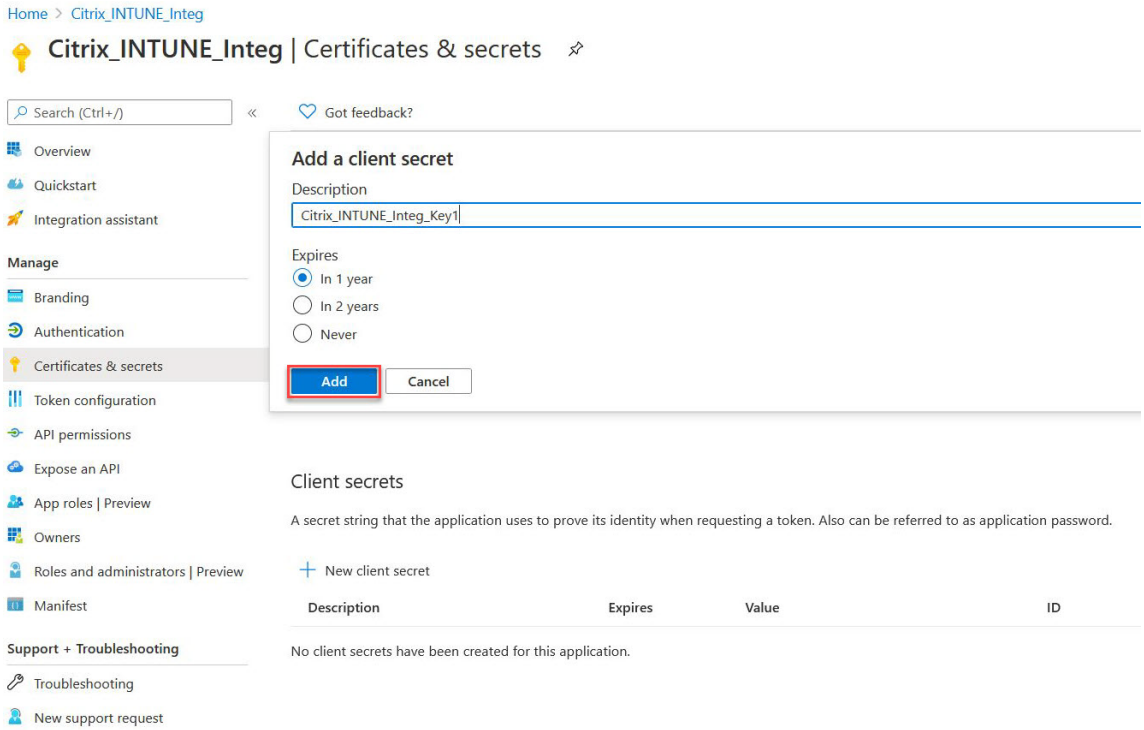
14. The following page lists the configured API permissions.



15. Navigate to **Certificates & secrets** and click **New client secret**.

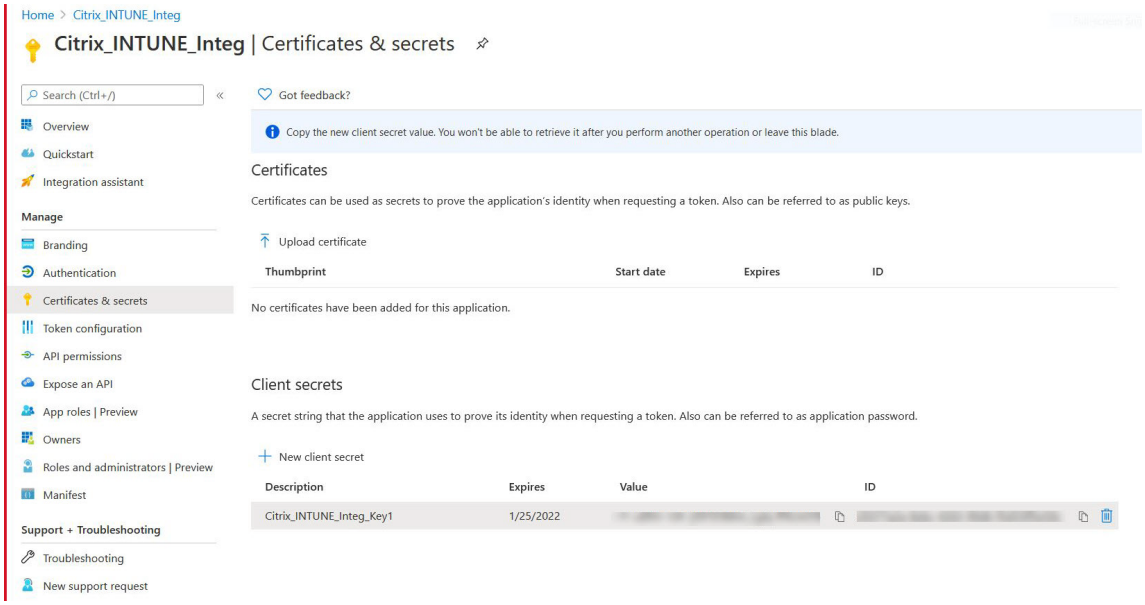


16. Under the **Add a client secret** page, enter description, select expiry, and click **Add**.



17. The following screen shows the configured client secret.

> **Note**
>
> The client secret is displayed only once when it is generated. Copy the displayed client secret locally. Use the same client secret along with the client ID associated with the newly registered app while configuring the OAuth action on the NetScaler Gateway appliance for Intune.



The application configuration on the Azure portal is now complete.

Understanding Azure ADAL Token Authentication

January 8, 2024

Following is the flow of events in a typical NetScaler Gateway-Microsoft ADAL token authentication:

1. When an app is launched in iOS or Android, the app contacts Azure. The user is prompted to log on with user credentials. After a successful logon, the app gets an ADAL token.
2. This ADAL token is presented to a NetScaler Gateway, which has been configured to validate the ADAL token.
3. NetScaler Gateway validates the signature of the ADAL token with the corresponding certificate from Microsoft.
4. After a successful validation, NetScaler Gateway extracts the User's Principal Name (UPN) and grants the app VPN access to the internal resources.

Configuring NetScaler Gateway Virtual Server for Microsoft ADAL Token Authentication

January 8, 2024

To configure a NetScaler Gateway virtual server for monitoring Microsoft ADAL token authentication, you need the following information:

- **certEndpoint**: The URL of the endpoint that contains the JSON Web Key (JWK) for ADAL token verification.
- **Audience**: FQDN of the NetScaler virtual server to which the app sends the ADAL token.
- **Issuer**: Name of the AAD issuer. Gets populated by default.
- **TenantID**: Tenant ID for Azure ADAL registration.
- **ClientID**: A unique ID given to the Gateway app as part of ADAL registration.
- **ClientSecret**: A secret key given to the Gateway app as part of ADAL registration.
- **ResourceURI**: An optional parameter to capture the resource URI. If not configured, NetScaler uses Azure commercial resource URI.

Perform the following steps using the command line interface:

1. Create an OAuth action.


```
add authentication OAuthAction <oauth-action-name> -OAuthType <INTUNE> – clientid <clientID> -clientsecret <client-secret> -audience <audience name> -tenantid <tenantID> -issuer <issuer-name> -userNameField <upn> -certEndpoint <certEndpoint-name> -resourceURI <name of resource URI>
```

2. Create an authentication policy to associate with the newly created OAuth action.

```
add authentication Policy <policy-name> -rule <true> -action <oauth intune action>
```

3. Bind the newly created OAuth to AuthVS.

```
bind authentication vserver <auth-vserver> -policy <oauth-intune-policy> -priority 2 -gotoPriorityExpression END
```

4. Create a LoginSchema.

```
add authentication loginSchema <loginSchemaName> -authenticationSchema <authenticationSchema " location " >
add authentication loginSchemaPolicy <loginSchemaPolicyName> -rule true -action <loginSchemaName>
```

5. Bind AuthVS with LoginSchema.

```
bind authentication vserver <auth-vs> -policy <oauth-pol> -priority 2 -gotoPriorityExpression END
```

6. Add an authentication profile and assign it to a VPN virtual server.

```
add authnprofile <nfactor-profile-name> -authnvsName <authvserver>
set vpn vserver <vserver-name> -authnprofile <nfactor-profile-name>
```

Sample configuration

```
add authentication OAuthAction tmp-action -OAuthType INTUNE -clientid id 1204 -clientsecret a -audience "[http://hello](http://hello/)" -tenantid xxxx -issuer "[https://hello](https://hello/)" -userNameField upn -certEndpoint https://login.microsoftonline.com/common/discovery/v2.0/keys --resourceURI htpps://api.manage.microsoft.com

add authentication Policy oauth-intune-pol -rule true -action tmp-action
bind authentication vserver auth-vs-for-gw1-intune -policy oauth-pol -priority 2 -gotoPriorityExpression END

add authentication loginSchema oauth-loginschema -authenticationSchema "/nsconfig/loginschema/LoginSchema/OnlyOAuthToken.xml"

```



```
add authentication loginSchemaPolicy oauth-loginschema-pol -rule true -action oauth-loginschema `

bind authentication vserver auth-vs-for-gw1-intune -policy oauth-loginschema-pol -priority 2 -gotoPriorityExpression END

add authnprofile nfactor-prof-intune -authnvsName auth-vs-for-gw1-intune

set vpn vserver gw1-intune-authnprofile nfactor-prof-intune
```

Set up NetScaler Gateway for using micro VPN with Microsoft Endpoint Manager

February 19, 2024

Citrix micro VPN integration with Microsoft Endpoint Management enables your apps to access on-premises resources. For details see, Citrix micro VPN integration with Microsoft Endpoint Manager.

System requirements

- NetScaler Gateway versions
  - 13.1
  - 13.0
  - 12.1.50.x or later
  - 12.0.59.x or later

  You can download the latest version of NetScaler Gateway from the NetScaler Gateway download page.
- A Windows desktop running Windows 7 or later (for Android app wrapping only)
- Microsoft
  - Azure AD access (with Tenant Admin privileges)
  - Intune-enabled tenant
- Firewall rules
  - Enable a firewall rule to SSL traffic from a NetScaler Gateway subnet IP to `*.manage.microsoft.com`, `https://login.microsoftonline.com`, and `https://graph.windows.net` (port 443)
  - NetScaler Gateway must be able to externally resolve the preceding URLs.

Prerequisites

- **Intune environment:** If you don't have an Intune environment, set up one. For instructions see the Microsoft documentation.
- **Edge Browser App:** The Micro VPN SDK is integrated within the Microsoft Edge app and Intune Managed Browser app for iOS and Android. For more information about the Managed Browser, see the Microsoft Managed Browser page.
- **Citrix Endpoint Management entitlement**: Ensure to have an active Citrix Endpoint Management entitlement for continued support to the micro VPN SDK on a Microsoft Edge mobile browser (iOS and Android). For more information, contact your Sales, Account, or Partner representative.

Grant Azure Active Directory (AAD) application permissions

1. Consent to Citrix multitenant AAD application to allow NetScaler Gateway to authenticate with the AAD domain. The Azure Global Administrator must visit the following URL and consent:

   https://login.windows.net/common/adminconsent?client_id=b6a53a76-5d50-499e-beb3-c8dbdad5c40b&redirect_uri=https://www.citrix.com&state=consent.

2. Consent to Citrix multitenant AAD application to allow mobile applications to authenticate with the NetScaler Gateway micro VPN. This link is only required if the Azure Global Admin has changed the default value for Users can register applications from Yes to No.
   This setting can be found in the Azure portal under **Azure Active Directory > Users > User Settings**.
   The Azure global administrator must visit the following URL and consent (add your Tenant ID) https://login.microsoftonline.com/%5Btenant_id%5D/adminconsent?client_id=9215b80e-186b-43a1-8aed-9902264a5af7.

Configure NetScaler Gateway for micro VPN

To use micro VPN with Intune, you must configure NetScaler Gateway to authenticate to Azure AD. An existing NetScaler Gateway virtual server does not work for this use case.
First, configure Azure AD to sync with the on-premises Active Directory. This step is necessary to ensure that authentication between Intune and NetScaler Gateway occurs properly.

Download script: The .zip file includes a readme with instructions for implementing the script. You need to manually enter the information the scripts require and run the script on the NetScaler Gateway to configure the service. You can download the script file from the NetScaler downloads page.

> **Important:** After you have completed the NetScaler Gateway configuration, and if you see the OAuth Status other than COMPLETE, see the Troubleshooting section.

Configuring Microsoft Edge Browser

1. Sign in to https://endpoint.microsoft.com/ and then navigate to **Intune > Mobile apps**.
2. Publish the Edge App as you normally do and then add an app configuration policy.
3. Under **Manage**, click **App configuration policies**.
4. Click **Add** and then enter a name for the policy you want to create. In **Device enrollment type**, select **Managed apps**.
5. Click **Associated App.**
6. Select the apps to which you want to apply the policy (Microsoft Edge or Intune managed browser) and then click **OK**.
7. Click **Configuration Settings**.
8. In the **Name** field, enter the name of one of the policies listed in the following table.
9. In the **Value** field, enter the value you want to apply for that policy. Click off the field to add the policy to the list. You can add multiple policies.
10. Click **OK** and then click **Add**.

The policy is added to your list of policies.

Name (iOS/Android)	Value	Description
MvpnGatewayAddress	`https://external.companyname.com`	External URL of your NetScaler Gateway
MvpnNetworkAccess	MvpnNetworkAccessTunneledWebSSO or Unrestricted	MvpnNetworkAccessTunneledWebSSO is the default for tunneling
MvpnExcludeDomains	Comma-separated list of domain name to be excluded	Optional. Default=blank

Name (iOS/Android)	Value	Description
TunnelExcludeDomains	Use this client property to override the default list of domains excluded. Default=app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis-test.citrix.com,clientstream.launchdarkly.com,crashlytics.com,events.launchdarkly.com,fabric.io,firehose.launchdarkly.com, hockeyapp.net,mobile.launchdarkly.com,pushreg.xm.citrix.com,rttf.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.com,ssl.google-analytics.com,stream.launchdarkly.com	

> **Note:** Web SSO is the name for Secure Browse in the settings. The behavior is the same.

- **MvpnNetworkAccess** - MvpnNetworkAccessTunneledWebSSO enables HTTP/HTTPS redirection through the NetScaler Gateway, also known as Tunneled-Web SSO. The gateway responds to HTTP authentication challenges inline, providing a single-sign-on (SSO) experience. To use Web SSO, set this policy to **MvpnNetworkAccessTunneledWebSSO**. Full tunnel redirection is currently not supported. Use **Unrestricted** to leave micro VPN tunneling off.
- **MvpnExcludeDomains** - Comma-separated list of host or domain names to be excluded from being routed through the NetScaler Gateway reverse web proxy. The host or domain names are excluded even though the NetScaler Gateway configured split DNS settings might otherwise select the domain or host.

  > **Note:**
  >
  > – This policy is only enforced for **MvpnNetworkAccessTunneledWebSSO** connections.

> If `MvpnNetworkAccess` is **Unrestricted**, this policy is ignored.
>
> – This policy applies only to the Tunneled-Web SSO mode with NetScaler Gateway configured for reverse split tunneling.

- **TunnelExcludeDomains** - By default, MDX excludes some service endpoints from micro VPN tunneling. The mobile app SDKs and the apps use these service endpoints for various features. For example, the service endpoints include services that do not require routing through enterprise networks, such as Google Analytics, Citrix Cloud services, and Active Directory services. Use this client property to override the default list of excluded domains.

  To configure this global client policy, on the Microsoft Endpoint Management console, navigate to **Settings > Client Properties**, add the custom key **TUNNEL_EXCLUDE_DOMAINS**, and set the value.

  Value: To replace the default list with the domains that you want to exclude from tunneling, type a list of domain suffixes separated by commas. To include all domains in tunneling, type none. Default is:

  `app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis-test.citrix.com,clientstream.launchdarkly.com,crashlytics.com,events.launchdarkly.com,fabric.io,firehose.launchdarkly.com,hockeyapp.net,mobile.launchdarkly.com,pushreg.xm.citrix.com,rttf.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.com,ssl.google-analytics.com,stream.launchdarkly.com`

Troubleshooting

General issues

Issue	Resolution
The “Add Policy Required”message appears when you open an app	Add policies in the Microsoft Graph API
There are policy conflicts	Only a single policy per app is allowed
The “Failed to package app”message appears when wrapping an app. For the complete message, see the following table	The app is integrated with the Intune SDK. You do not need to wrap the app with the Intune
Your app can’t connect to internal resources	Ensure that the correct firewall ports are open, you correct tenant ID, and so on

Failed to package app error message:

Failed to package app. com.microsoft.intune.mam.apppackager.utils.AppPackagerException: This app already has the MAM
SDK integrated.
com.microsoft.intune.mam.apppackager.AppPackager.packageApp(AppPackager.java:113)
com.microsoft.intune.mam.apppackager.PackagerMain.mainInternal(PackagerMain.java:198)
com.microsoft.intune.mam.apppackager.PackagerMain.main(PackagerMain.java:56)
The application cannot be wrapped.

NetScaler Gateway issues

Issue	Resolution
The permissions required to be configured for the gateway app on Azure are unavailable.	Check if a proper Intune license is available. Try using the manage.windowsazure.com portal to see if the permission can be added. Contact Microsoft support if the issue persists.
NetScaler Gateway cannot reach `login.microsoftonline.com and graph.windows.net`.	From NS Shell, check if you are able to reach the following Microsoft website: cURL -v -k https://login.microsoftonline.com. Then, check whether DNS is configured on NetScaler Gateway. Also check that the firewall settings are correct (in case DNS requests are firewalled).
An error appears in ns.log after you configure OAuthAction.	Check if Intune licensing is enabled and the Azure Gateway app has the proper permissions set.
Sh OAuthAction command does not show OAuth status as complete.	Check the DNS settings and configured permissions on the Azure Gateway App.
The Android or iOS device does not show the dual authentication prompt.	Check if the Dual Factor Device ID logonSchema is bound to the authentication virtual server.

NetScaler Gateway OAuth status and error condition

Status	Error condition
AADFORGRAPH	Invalid secret, URL not resolved, connection timeout
MDMINFO	`*manage.microsoft.com`is down or unreachable

Status	Error condition
GRAPH	Graph endpoint is down unreachable
CERTFETCH	Cannot talk to "Token Endpoint: https://login.microsoftonline.com because of a DNS error. To validate this configuration, go to shell and type cURL https://login.microsoftonline.com. This command must validate.

Note: When the OAuth status is successful, the status is displayed as COMPLETE.

Extended support for Azure AD Graph

January 8, 2024

As the Azure AD Graph is deprecated, customers triggering a new application cannot use the earlier permissions that were available with the Azure AD graph. However, customers with existing applications who want to use the old permissions of the Azure AD Graph for some more time can continue to do so by making some configuration changes on the gateway appliance. This configuration is supported in NetScaler Gateway release 13.1-27.xx and later.

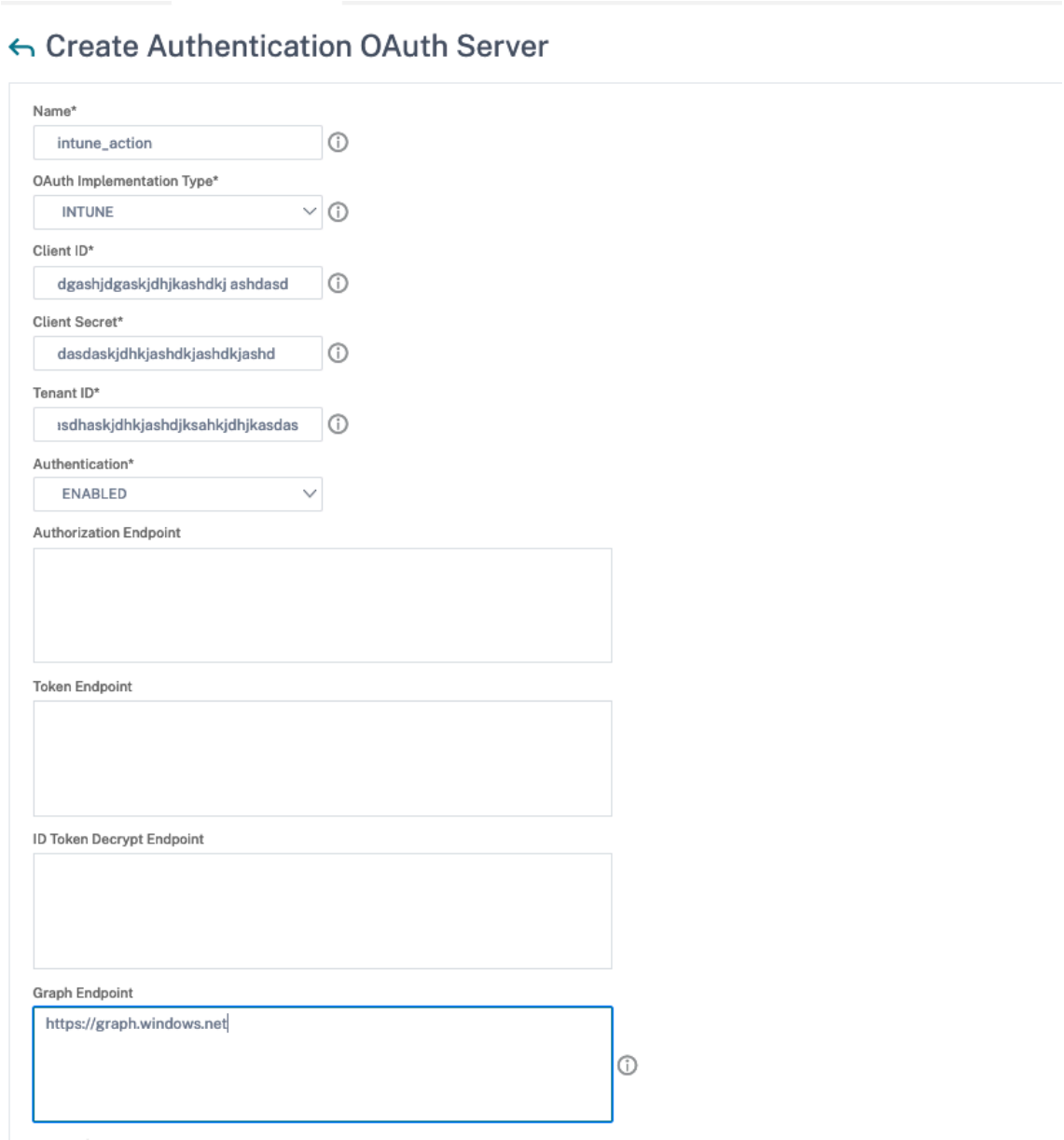
Perform the following configuration changes on the NetScaler Gateway appliance:

1. In the command prompt, run the following command.

```
shell nsapimgr_wr.sh -ys call= " ns_intune_enable_old_endpoints "
```

2. Navigate to **Security > AAA-Application Traffic > Policies > Authentication > Advanced Policies > Actions > OAUTH Actions**.

   a) Select an existing OAuth server.
   b) Click **More**.
   c) In **Graph Endpoint**, ensure that the URL looks like the one displayed in the figure.



HDX enlightened data transport support

January 8, 2024

Enlightened Data Transport (EDT) support for NetScaler Gateway ensures a high definition in-session user experience of virtual desktops for users running the Citrix Workspace app.

Also, end-to end encryption with the DTLS 1.0 for EDT termination between Citrix Workspace app and VDA is facilitated. For more information, see Support for DTLS protocol.

EDT enabled NetScaler Gateway delivers a good user experience on both LAN and WAN conditions. With EDT, you do not need any administrative or user configuration when roaming from one to the other. The benefit is most visible in high-latency networks with moderate packet loss, where user experience would generally lag with alternatives.

When to Use Enlightened Data Transport Support

January 8, 2024

The following scenarios illustrate the use of EDT enabled NetScaler Gateway.

- A user wants an experience as good as in a LAN environment while remotely accessing business resources.
- A user wants a rich virtual application and desktop user experience on Wi-Fi and cellular networks where network quality is poor because of congestion, high packet loss, and high latency.

The following points are to be kept in mind while using EDT.

- The DTLS knob at the virtual server level is enabled by default.
- IPv6 with DTLS is not supported.
- The appliance can now be configured for Double-hop functionality for EDT traffic between Receiver and VDA. For more information, click Deploying in a Double-Hop DMZ.

Note: EDT is supported on the MPX FIPS platform in release 12.1 build 49.xx and later. On the Intel Coleto SSL chip based MPX devices, EDT is supported from release 12.1 build 51.16 and later.

Configure NetScaler Gateway to support Enlightened Data Transport and HDX Insight

January 8, 2024

EDT traffic through Gateway now has end-to-end visibility. Availability of both real-time and historical visibility data enables NetScaler ADM to support a wide variety of use cases.

The following scenarios are supported:

Scenario	EDT support
NetScaler Gateway	Yes

Scenario	EDT support
NetScaler Gateway with High Availability (HA)	Yes
NetScaler Gateway with High Availability (HA) optimization	Yes
NetScaler with Unified Gateway	Yes
NetScaler Gateway with GSLB	Yes
NetScaler Gateway with Cluster	Yes
Citrix Workspace app to NetScaler Gateway DTLS encryption	Yes
Dual Secure Ticket Authority (STA) on NetScaler Gateway	Yes
NetScaler Gateway ICA session timeout	Yes
NetScaler Gateway Multi-Stream ICA	No
NetScaler Gateway session reliability (Port 2598)	Yes
NetScaler Gateway Double-Hop	Yes
NetScaler to VDA DTLS encryption	Yes
HDX Insight	Yes
NetScaler Gateway in IPv6 mode	No
NetScaler Gateway SOCKS (Port 1494)	No
NetScaler pure LAN proxy (see note)	No

> **Note:**
>
> EDT is not supported if NetScaler LAN proxy is configured in the LAN User mode or Transparent mode. However, TCP is supported. For more information, see:
>
> - Configuring outbound ICA Proxy
> - Gathering HDX Insight Analytics for LAN Users with NetScaler Using SOCKS

Configure NetScaler Gateway to support Enlightened Data Transport

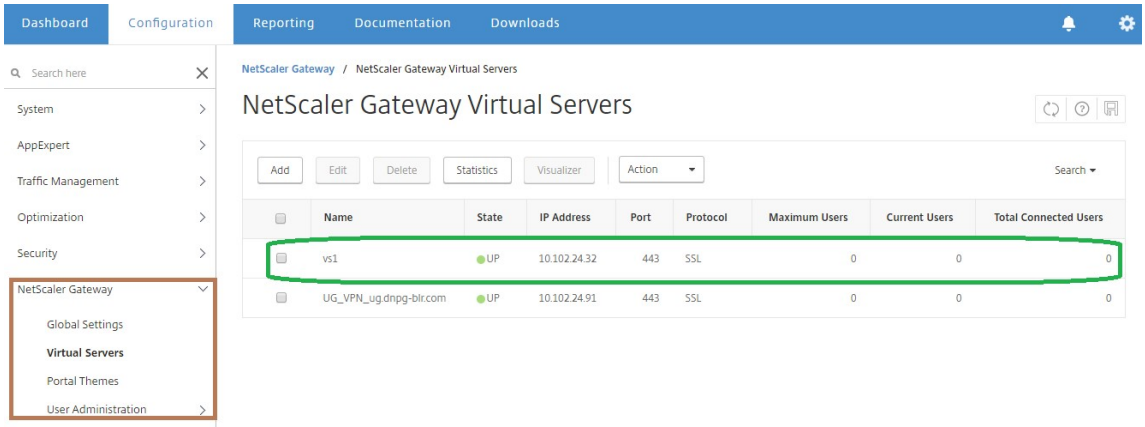
If you use Enlightened Data Transport (EDT), Datagram Transport Layer Security (DTLS) must be enabled to encrypt the UDP connection used by EDT. The DTLS parameter must be enabled at the Gateway VPN virtual-server level. Also, the Citrix Virtual Apps and Desktops components must be correctly

upgraded and configured to achieve encrypted traffic between the Gateway VPN virtual server and the user device.

> **Note:** UDP port (for example port 443) configured for the NetScaler Gateway front end virtual server must be opened in the DMZ for the virtual server to receive the DTLS connections. DTLS and CGP are prerequisites for EDT to be compatible with NetScaler Gateway.

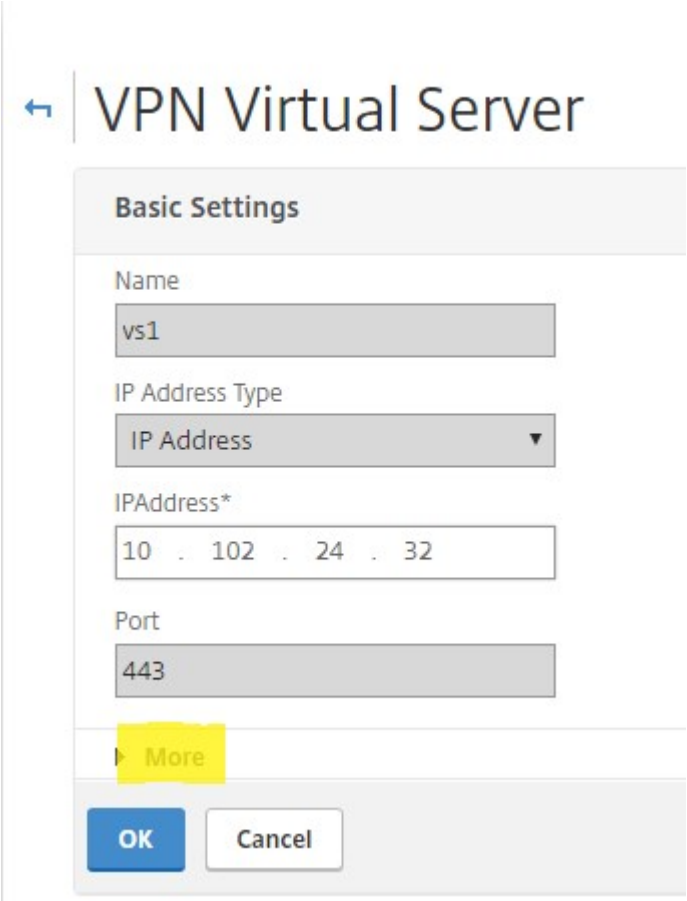
To configure NetScaler Gateway to support EDT using GUI

1. Deploy and configure NetScaler Gateway to communicate with StoreFront and authenticate users for Citrix Virtual Apps and Desktops.
2. On the Configuration tab in the NetScaler GUI, expand **NetScaler Gateway** and select **Virtual Servers**.



3. Click **Edit** to display Basic Settings for the VPN Virtual Server, and then verify the state of the DTLS setting.

4. Click **More** to display other configuration options.



5. Select **DTLS** to provide communications security for datagram protocols. Click **OK**. The **Basic Settings** area for the VPN virtual server shows that the DTLS flag is set to **True**.

To configure NetScaler Gateway for EDT support using CLI

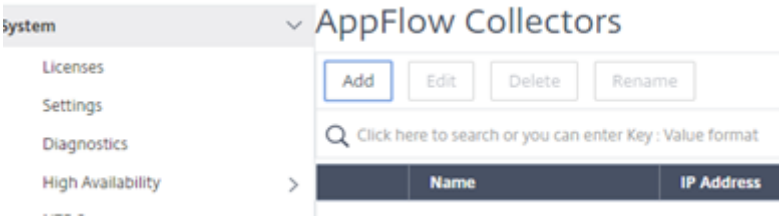
```
set vpn vserver vs1 -DTLS ON
```

Configure NetScaler Gateway to support HDX Insight

HDX Insight provides end-to-end visibility for HDX traffic to virtual apps and desktops passing through NetScaler. It also enables administrators to view real-time client and network latency metrics, historical reports, end-to-end performance data, and troubleshoot performance issues.

To configure NetScaler Gateway to support HDX Insight using GUI

1. On the **Configuration** tab navigate to **System> AppFlow>Collectors**, and click **Add**.



2. On the **Create AppFlow Collector** page, populate the following fields, and click **Create**.

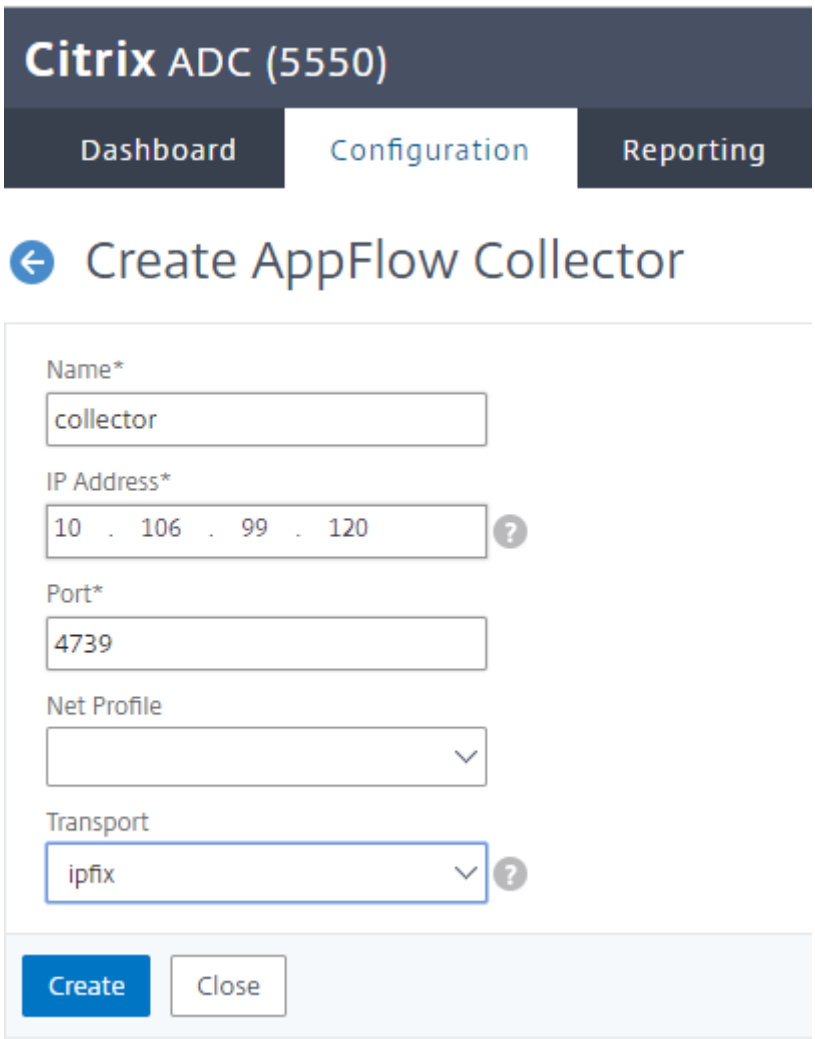
   Name –Name for the collector

   IP address –IPv4 address of the collector

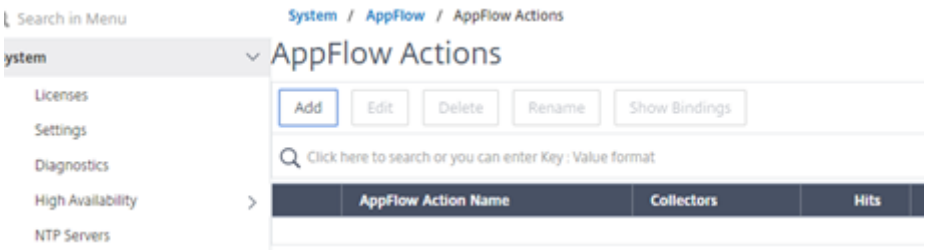
   Port –Port on which the collector listens

   Net Profile - Net profile to associate with the collector. The IP address defined in the profile is used as the source IP address for AppFlow traffic for this collector. If you do not set this parameter, the NetScaler IP (NSIP) address is used as the source IP address.

Transport –Transport type of collector.



3. Navigate to **System> AppFlow>Actions**, click **Add**.

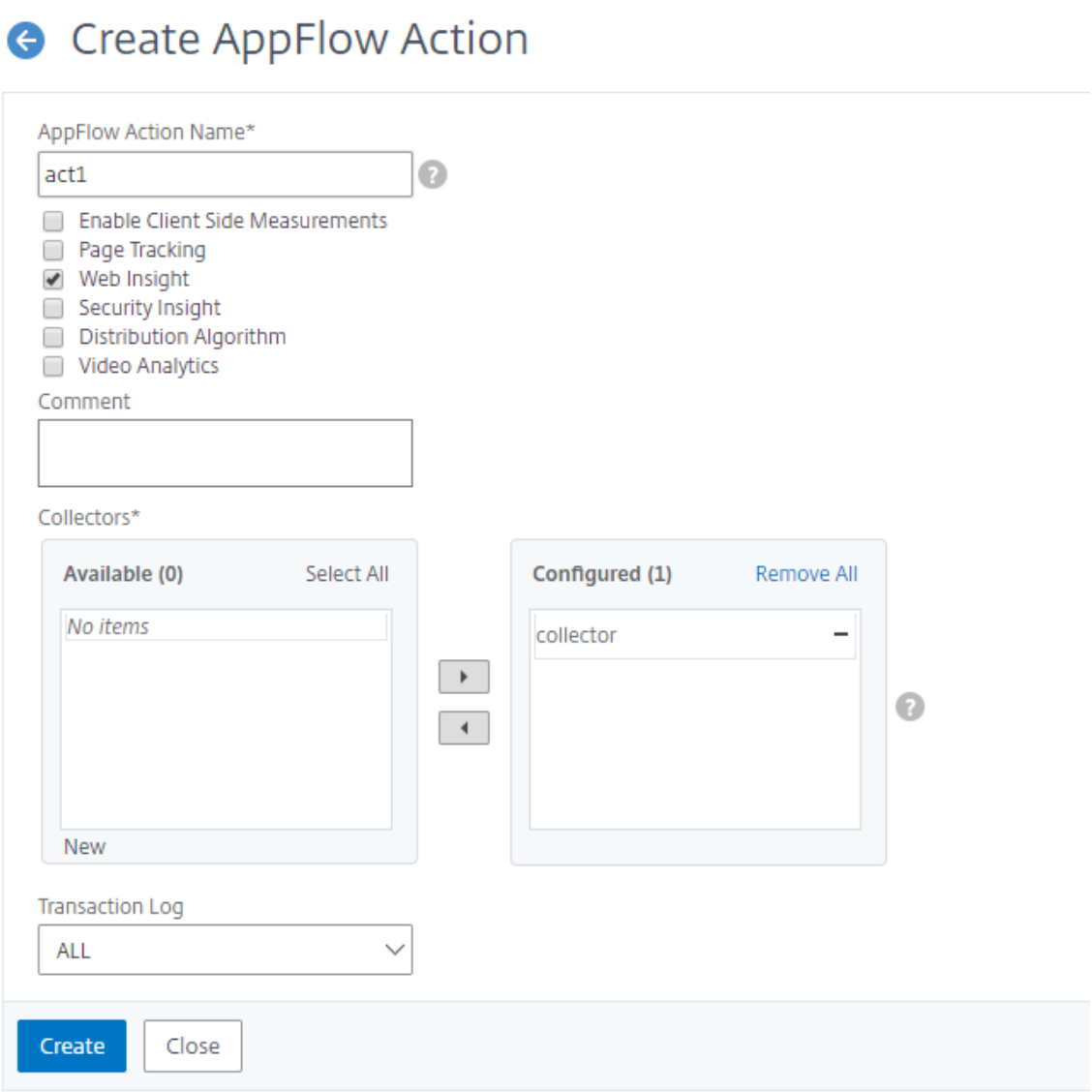


4. On the **Create AppFlow Action** page, populate the following fields, and click **Create**.
   AppFlow Action Name –Name for the action

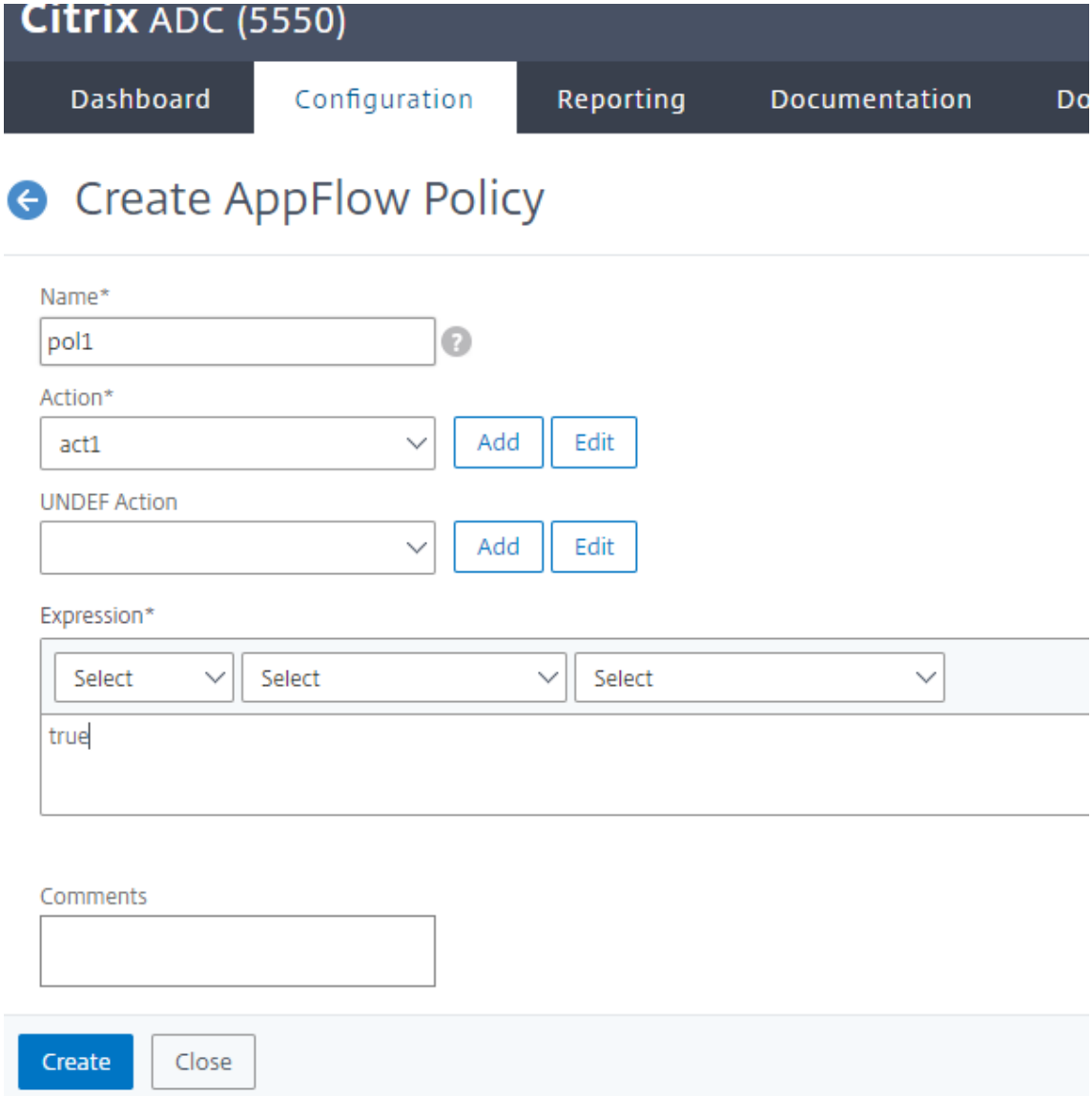
   Comment –Any comment about the action

   Collector –Select the names of collectors to be associated with the AppFlow action.

Transaction Log –Transactions type to be logged.



5. Navigate to **System> AppFlow>Policies**, click **Add**.



6. On the **Create AppFlow Policy** page, populate the following fields, and click **Create**.

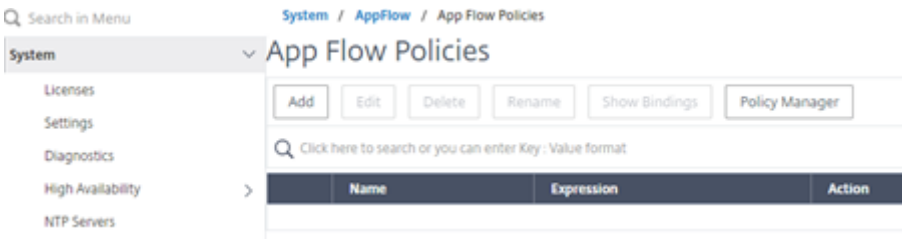
   Name –Name for the policy.

   Action –Name of the action to be associated with the policy.

   UNDEF - Name of the AppFlow action to be associated with this policy when an undefined event occurs.

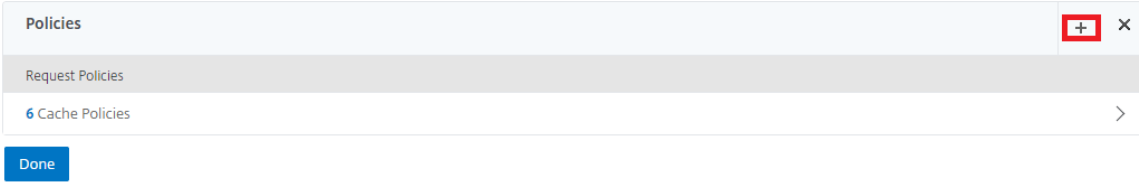
   Expression - Expression or other value against which the traffic is evaluated. Must be a Boolean expression.

   Comments –Any comments about this policy.

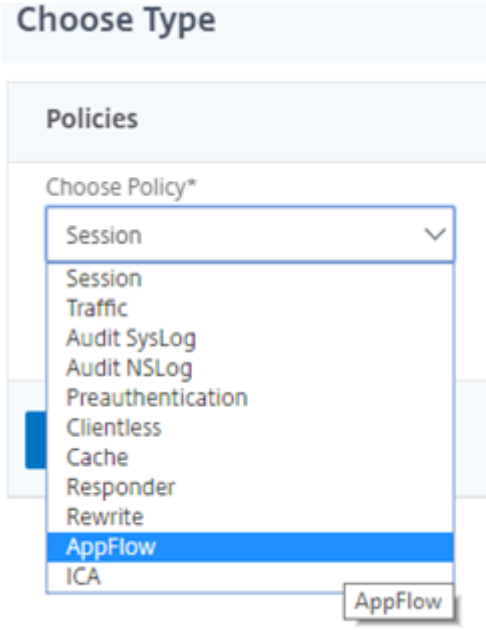


7. Navigate to **NetScaler Gateway>Virtual Servers**, select the virtual server and click **Edit**.

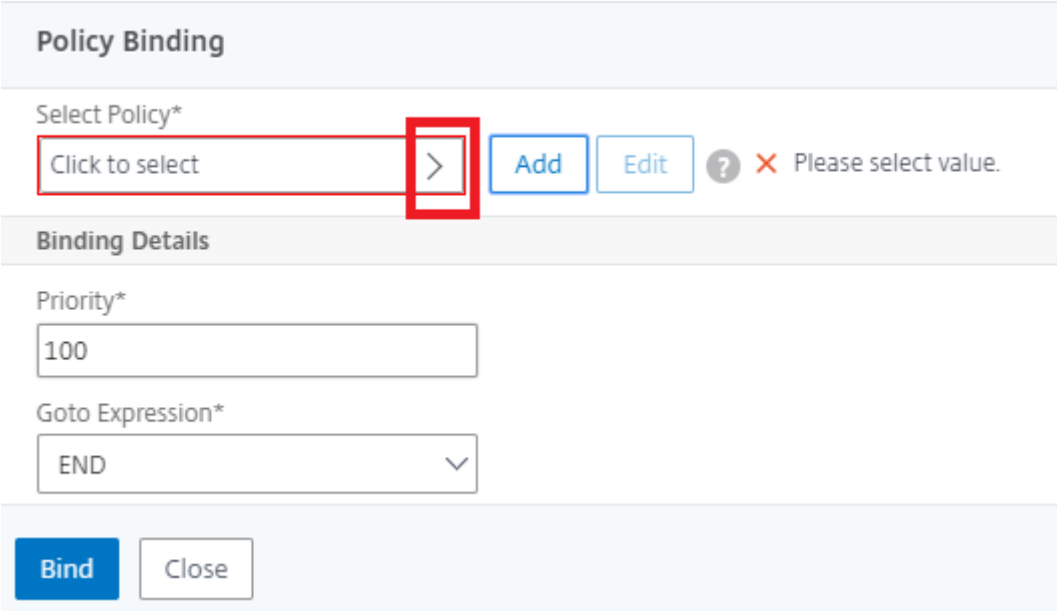
8. Scroll down the **VPN Virtual Server** page and under **Policies** section, click **+**.



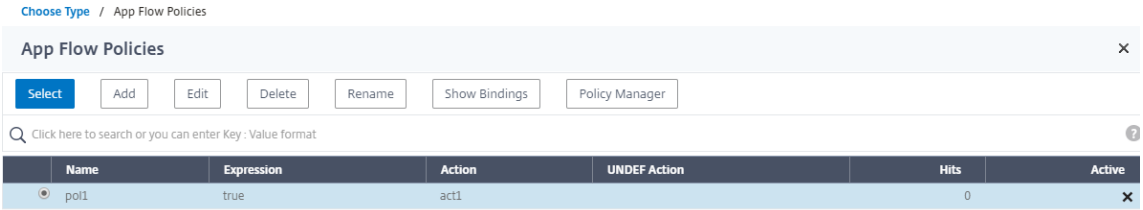
9. On the **Choose Type** screen, in the **Choose Policy** drop-down menu, select **AppFlow**. In the **Choose Type** drop-down menu, choose **Request** or **ICA Request** and click **Continue**.



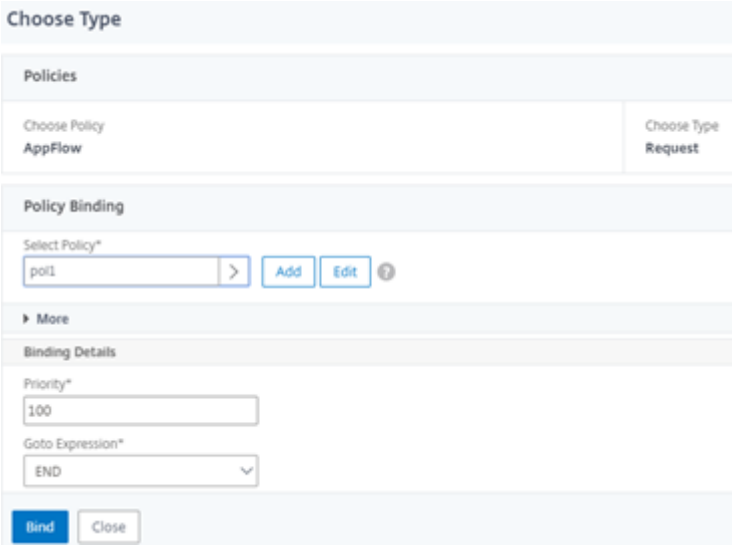
10. Click the highlighted arrow under **Select Policy**.



11. Select the **AppFlow policy** and click **Select**.



12. Finally click **Bind**.



To configure NetScaler Gateway for HDX Insight support using the CLI, type the following command


```
add appflow collector col3 -IPAddress<ip_mas>
add appflow action act1 <action_name>
add appflow policy <policy_name> true <action_name>
bind vpn Vserver <vserver_name>  -pol <policy_name> - priority101 END -
    type <ICA_Request>
```

Disable HDX Insight for non-NSAP HDX session

In a NetScaler appliance, you can now disable HDX Insight for the non-NSAP HDX sessions.

At the command prompt, type:

```
set ica parameter HDXInsightNonNSAP (YES | NO )
```

By default, HDX Insight for non-NSAP session is enabled.

PMTUD discovery and DF bit propagation for EDT over NetScaler Gateway

May 7, 2024

From release 13.1 build 17.x, the NetScaler Gateway appliance supports DF bit enforcement for the EDT path maximum transmission unit discovery (PMTUD). Path MTU discovery helps in dynamically determining the maximum transmission unit (MTU) when establishing a session. The DF bit enforcement prevents EDT fragmentation that might result in performance degradation or failure to establish a session.

In earlier releases, NetScaler Gateway supported EDT path MTUD but did not support DF bit enforcement.

For more details, see EDT MTU discovery.

Enable the PMTUD support by using the CLI

At the command prompt, type;

```
set ica parameter [-EnableSRonHAFailover ( YES | NO )] [-
    HDXInsightNonNSAP ( YES | NO )] [-EDTPmtudDF ( ENABLED | DISABLED )]
     [-EDTPmtudDFTimeout <positive_integer>] [-L7LatencyFrequency <
    positive_integer>]
```

Example:

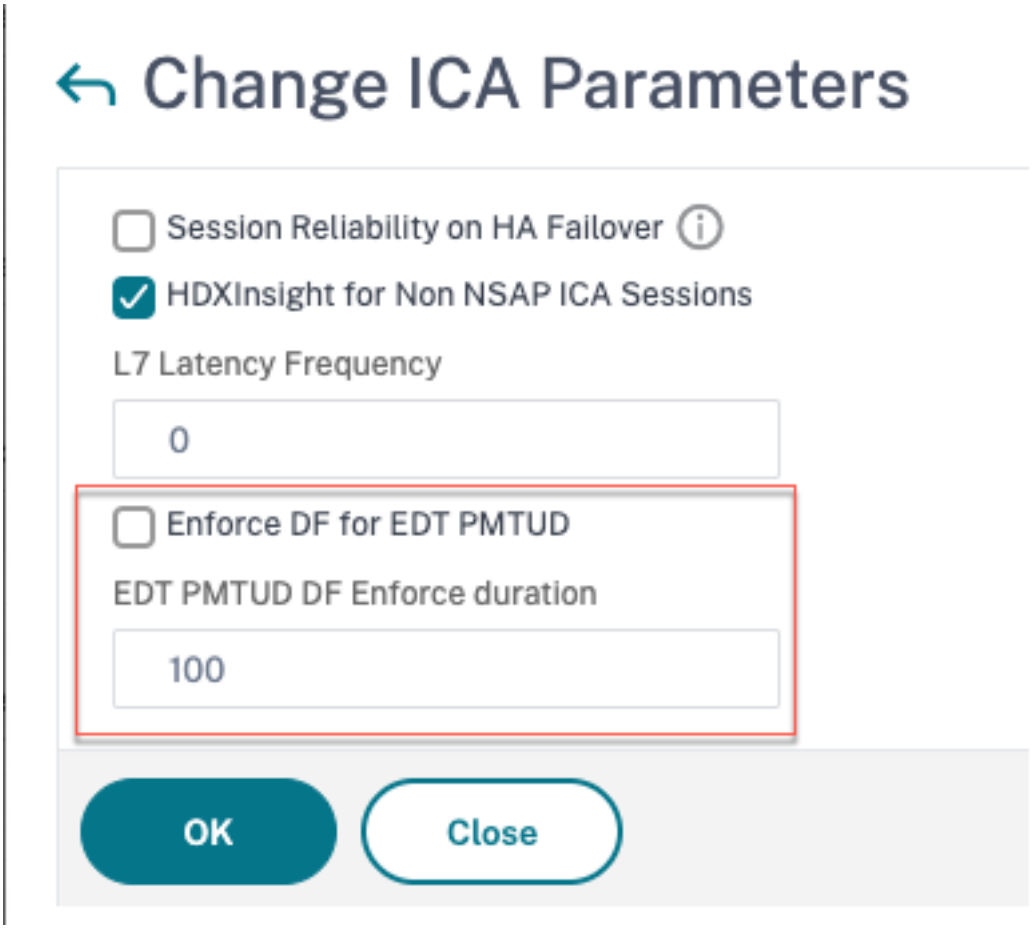

```
set ica parameter -EnableSRonHAFailover YES -EDTPmtudDF ENABLED -
    EDTPmtudDFTimeout 100
```

> **Note:**
>
> From release 13.1 build 42.x and later, the EDTPmtudDF parameter is enabled, by default. Previously, this option was disabled, by default.

Enable the PMTUD support by using the GUI

1. Navigate to **System > Settings > Change ICA Parameters**.
2. In **EDT PMTUD DF Enforce duration**, enter the time-out in seconds for the PMTUD DF enforcement.

> **Note:**
>
> From release 13.1 build 42.x and later, the **Enforce DF for EDT PMTUD** option is enabled, by default. Previously, this option was disabled, by default.



L7 Latency Thresholding

January 8, 2024

The L7 latency thresholding feature in HDX Insight actively detects end-to-end network latency issues at the application level and takes proactive actions. The L7 latency thresholding feature performs live latency monitoring to detect the spikes and sends out notifications to HDX Insight if the latency exceeds the minimum observed latency.

Previously, average client side and server side L7 latency values were sent every 60 sec to HDX Insight. Any spikes seen within this interval were averaged out and hence remained undetected. Also, there was no live latency monitoring to detect these spikes.

How L7 latency is different from L4 latency

Network latencies are captured and displayed at the L4 level as well. These latencies are calculated from the TCP layer and do not require parsing of the ICA traffic. Therefore, they are relatively easy to obtain and are less CPU intensive. However, the major drawback of L4 latency is understanding end-to-end latency. If there are TCP proxies in the path, the L4 latency captures only the latency from the NetScaler to the TCP proxy. This might result in incomplete information and hence result in difficulties in debugging the issue.

L7 latency is calculated by parsing ICA traffic. L7 latency calculation is done at the ICA layer, and therefore intermediate proxies do not result in incomplete latency values. Thus, provides end-to-end latency detection.

The following figures display a deployment type with and without TCP proxies.

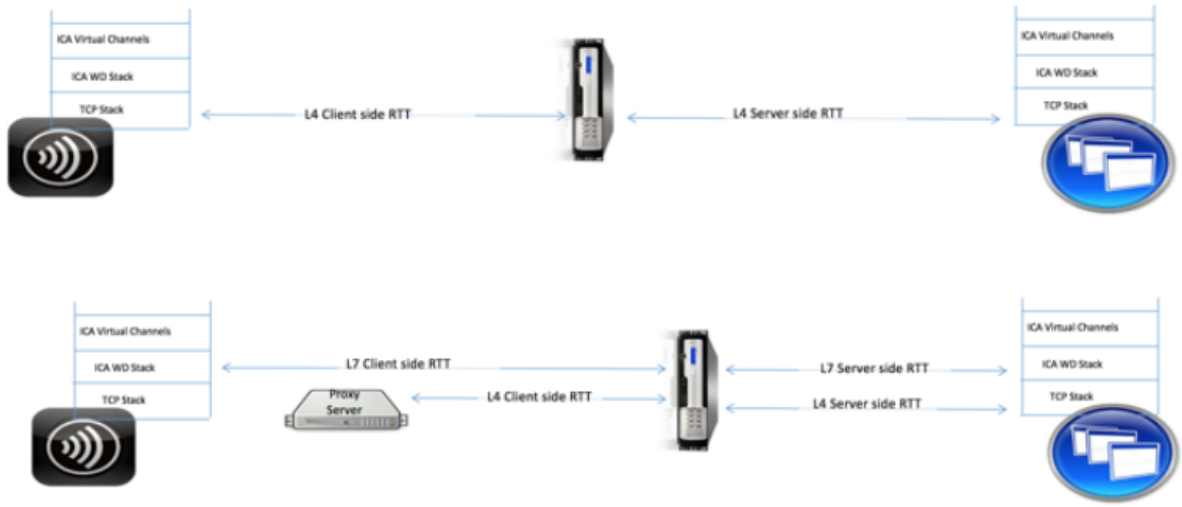


Fig 2. Deployment with TCP Proxies

Difference between ICA RTT and L7 latency calculations

ICA RTT represents the total round trip time from the Citrix Workspace app to Virtual Delivery Agent (VDA). L7 latency provides granular details regarding latencies on the client side and the server side. L7 client latency is the latency between Citrix Workspace app to NetScaler Gateway. L7 Server latency is the latency between NetScaler Gateway to VDA.

> **Note**: Server side L7 latency calculation for the server is supported only for the Citrix Virtual Apps and Desktops versions 7.13 and later.

Configure L7 latency thresholding using the CLI

1. Add an ICA latency profile.

```
add ica latencyprofile <name> [-l7LatencyMonitoring ( ENABLED |
    DISABLED )] [-l7LatencyThresholdFactor <positive_integer>] [-
    l7LatencyWaitTime <positive_integer>] [-l7LatencyNotifyInterval
     <positive_integer>] [-l7LatencyMaxNotifyCount <
    positive_integer>]
```

2. Add an ICA action.

```
add ica action <name> [-latencyprofileName <string>]
```

3. Add an ICA policy.

```
add ica policy <name> -rule <expression> -action <string> [-
    comment<string>] [-logAction <string>
```

4. Bind ICA policy to the VPN server or to the ICA global bind point.

```
bind ica global -policyName <string> -priority <positive_integer>
    [-gotoPriorityExpression <expression>] [-type (
    ICA_REQ_OVERRIDE | ICA_REQ_DEFAULT )]
```

Or

```
bind vpn vserver <name> -policy <string>  [-priority <
    positive_integer>]
```

Or

```
bind cr vserver <name> -policy <string> [-priority <positive
    _integer>]
```


Arguments

- **Latency Monitoring**: Parameter to enable or disable L7 threshold monitoring. When this parameter is enabled, notifications are sent to HDX Insight when the set conditions are met.

  Default value: DISABLED

- **LatencyThresholdFactor**: Factor by which the active latency must be greater than the minimum observed latency to conclude that the threshold is exceeded and therefore notification must be sent to HDX Insight.

  Default value: 4

  Minimum value: 2

  Maximum value: 65535

- **LatencyWaitTime**: Time in seconds for the appliance to wait after the latency threshold is exceeded to send notification to HDX Insight.

  Default value: 20

  Minimum value: 1

  Maximum value: 65535

- **LatencyNotifyInterval**: Time interval in seconds for the appliance to send subsequent notifications to HDX Insight after the wait time has passed.

  Default value: 20

  Minimum value: 1

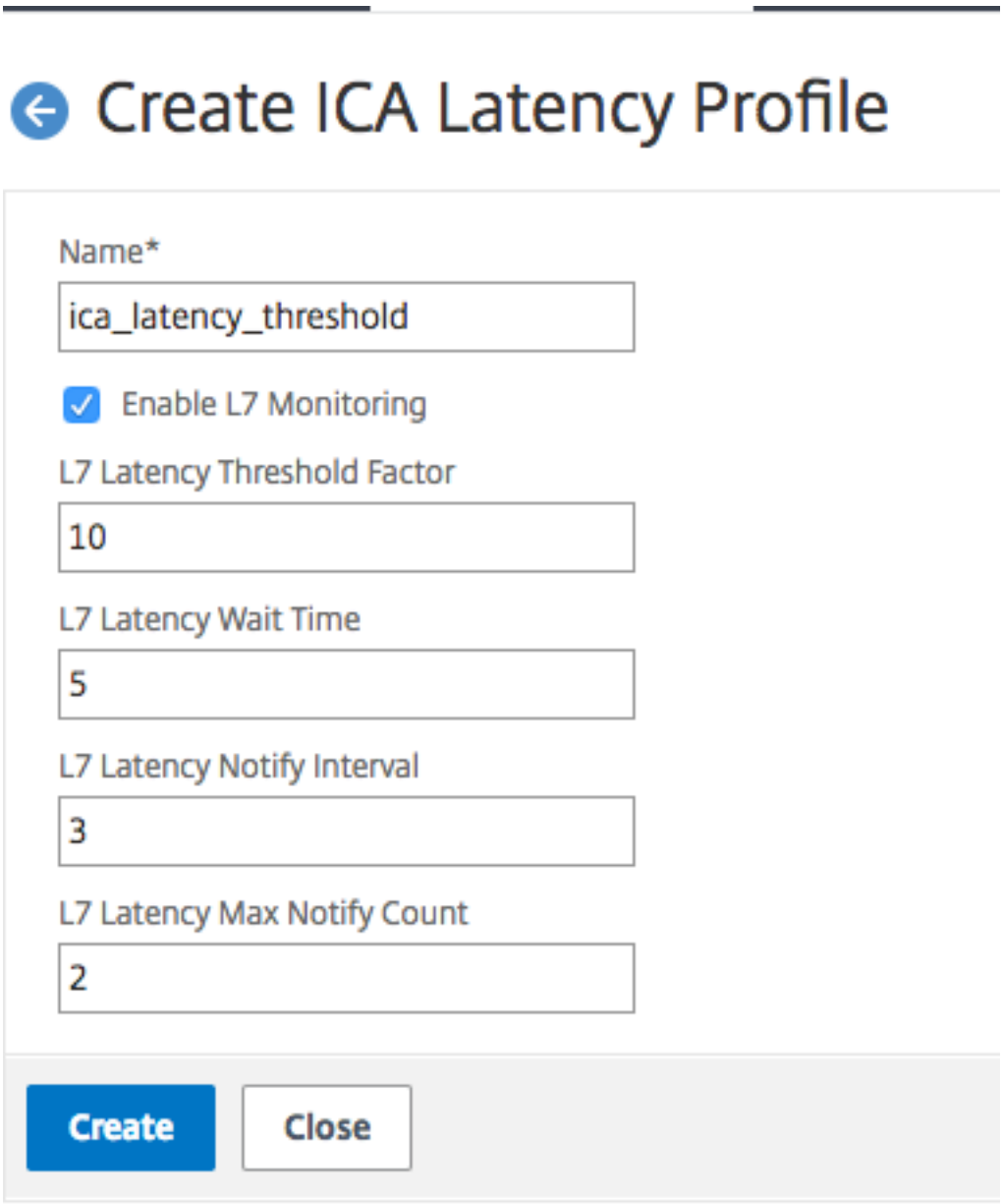
  Maximum value: 65535

- **LatencyMaxNotifyCount**: Maximum number of notifications that can be sent to HDX Insight within an interval where the latency is above the threshold.

  Default value: 5

Configure L7 latency thresholding using the GUI

1. Navigate to **Configuration** > **NetScaler Gateway** > **Policies** > **ICA**.
2. Select **ICA Latency Profiles** tab and click **Add**.
3. In the **Create ICA Latency Profile** page, perform the following.



- Select **L7 Latency Monitoring** to enable L7 Threshold monitoring.
- In **L7 Threshold Factor**, enter the value by which the active latency must exceed the minimum observed latency to send notification to HDX Insight.
- In **L7 Latency Wait Time**, enter the time in seconds for the appliance to wait after the threshold is exceeded to send out a notification to HDX Insight.
- In **L7 Latency Notification Interval**, enter the time in seconds for the appliance to send subsequent notifications to HDX Insight after the wait time has passed.
- In **L7 Latency Maximum Notify Count**, enter the maximum number of notifications that can be sent to HDX Insight within an interval where the latency is above the threshold.
  Note: The L7 latency maximum notify count is applicable once the threshold is exceeded

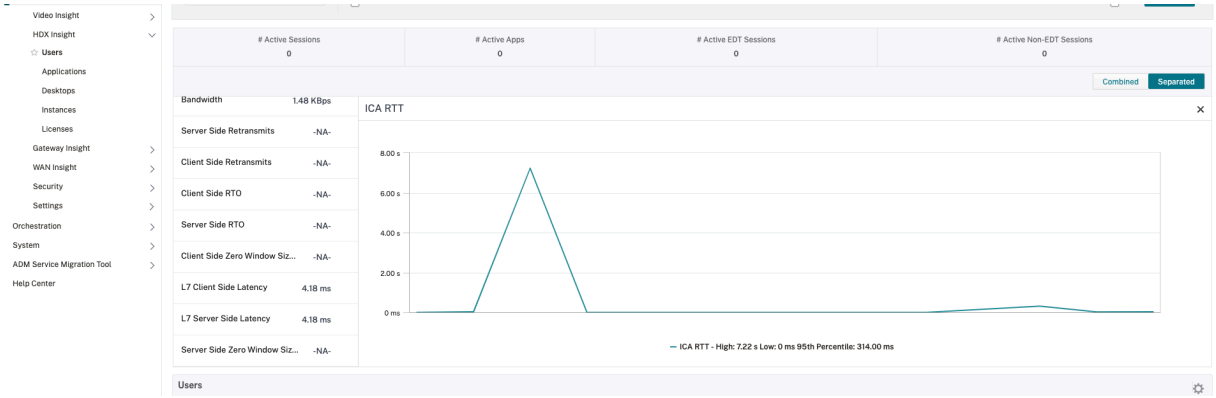
and is reset when the active latency falls below the threshold. Periodicity of these notifications is governed by the notification interval.

4. Click **Create**.

> **Important:**
>
> After configuring the L7 latency threshold parameters, you must configure HDX Insight. For details, see Configure NetScaler Gateway to support HDX Insight.

View L7 latency parameters in NetScaler ADM

To view the L7 latency parameters in NetScaler ADM, navigate to **Analytics > HDX Insight > Applications** or **Analytics > HDX Insight > Users**.

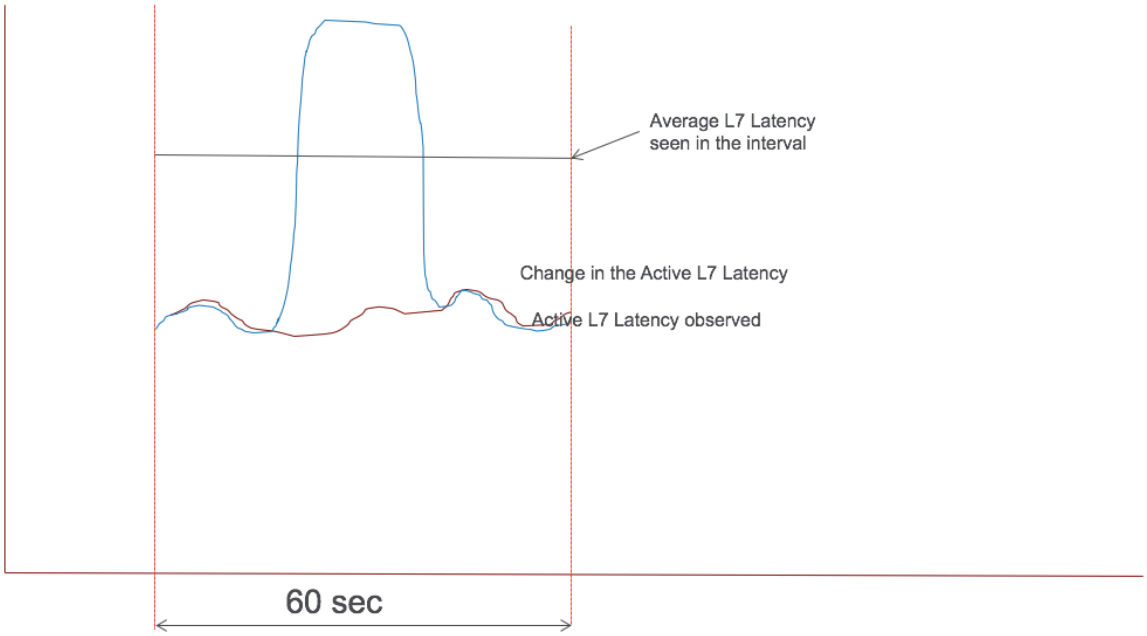


The L7 Latency measurement model versus the L7 latency threshold reporting model

The L7 Latency measurement model

In the L7 latency measurement module, average client side and server side L7 latency values are sent to HDX Insight every 60 seconds. As a result, spikes seen within this interval are averaged out and hence remain undetected. Also, the L7 latency measurement module does not have the live latency monitoring capability.

The following figure illustrates a sample L7 latency measurement model.

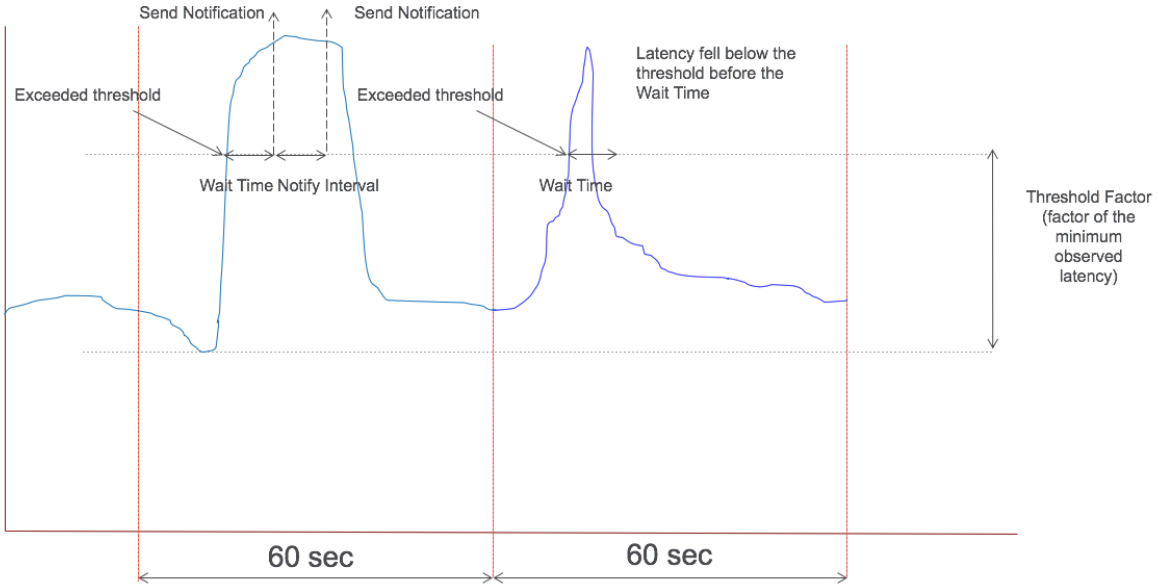


L7 latency threshold reporting model

The L7 latency threshold reporting model has the live latency monitoring capability to detect spikes. Notifications are sent to HDX Insight if the latency exceeds the minimum observed latency.

Whenever a threshold factor is exceeded, the latency increase is detected. After the configured threshold wait time expires, a notification is sent to HDX Insight. A subsequent notification is sent to HDX Insight after the wait time has expired and the threshold factor is still exceeded.
In case the latency value falls below the threshold factor before the wait time expires, no notification is sent to HDX Insight.

The following figure illustrates a sample L7 latency threshold reporting model.



The following parameters can be configured at run time:

- Threshold monitoring (ON/OFF)
- Threshold factor
- Threshold wait time
- Notification interval
- Maximum notification count

Reducer for HDX

January 17, 2024

Reducer for HDX is a general purpose compressor managed by Citrix Virtual Apps and Desktops that works across virtual channels.

The NetScaler Gateway 14.1–8.50 and later versions support the latest version of the reducer for HDX. The latest reducer improves the overall performance of NetScaler Gateway with the following capabilities:

- Reduces the network bandwidth utilization for ICA sessions.
- Provides a faster response as the packets take lesser time to transmit.

For details on how to use the latest reducer, see How to Use the New Reducer.

The following software versions support the latest reducer.

- Citrix Virtual Apps and Desktops 7 2303 (Windows) and later.

- Citrix Workspace app 2303 (Windows) and later.

> **Note:**
>
> If you are using Citrix Workspace app 2311 (Windows) and Citrix Virtual Apps and Desktops 7 2311 (Windows) versions, the latest reducer is enabled, by default.

The following table describes the status of ICA session launches and HDX insights using the latest reducer, on the NetScaler Gateway 14.1 version.

Latest reducer	NetScaler Gateway 14.1
Latest reducer negotiation + NSAP HDX insight	ICA connection launch is successful. HDX insight is supported.
Latest reducer negotiation + NSAP HDX insight + SmartControl	ICA connection launch is successful. HDX insight is supported.
Latest reducer negotiation + non-NSAP HDX insight	ICA connection launch is successful. HDX insight is not supported.

> **Note:**
>
> NetScaler Gateway 13.1 and prior versions do not support HDX Insight and SmartControl with the latest reducer.

For details on HDX insight configuration, see Configure NetScaler Gateway to support HDX Insight.

RDP Proxy

January 8, 2024

The RDP Proxy functionality is provided as part of the NetScaler Gateway. In a typical deployment, the RDP client runs on a remote user's machine. The NetScaler Gateway appliance is deployed within the DMZ, and the RDP server farm is in the internal corporate network.

The remote user;

1. connects to the NetScaler Gateway public IP address
2. establishes an SSL VPN connection
3. authenticates
4. accesses the remote desktops through the NetScaler Gateway appliance

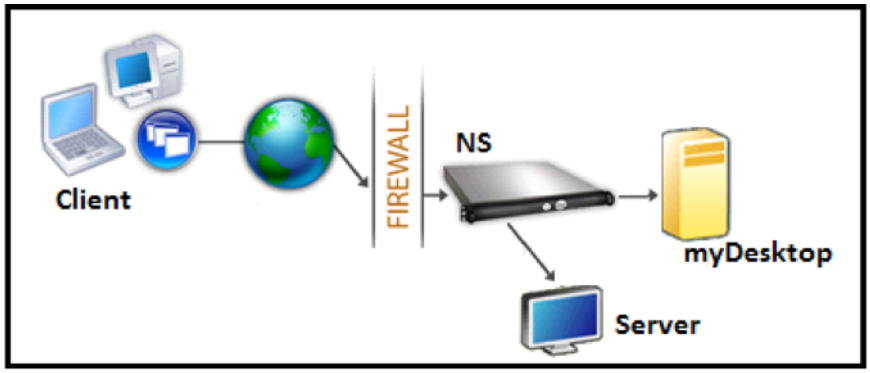
The RDP-proxy feature is supported in clientless VPN and ICA Proxy modes.

> **Note:**
>
> NetScaler Gateway does not support Remote Desktop Session Host (RDSH), Remote App, RDS multiuser, RDP sessions, or RDP apps.

The following RDP Proxy features provide access to a remote desktop farm through the NetScaler Gateway.

- Secure RDP traffic through clientless VPN or ICA Proxy mode (without Full Tunnel).
- SSO (single sign-on) to RDP servers through NetScaler Gateway. Also provides an option to disable SSO if needed.
- Enforcement (SmartAccess) feature, where the NetScaler administrators can disable certain RDP capabilities through the NetScaler Gateway configuration.
- Single/Stateless(Dual) Gateway solution for all needs (VPN/ICA/RDP/Citrix Endpoint Management).
- Compatibility with native Windows MSTSC client for RDP without the need for any custom clients.
- Use of existing Microsoft-provided RDP client on MACOSX, iOS, and Android.

The following figure depicts an overview of the deployment:



Deployment through clientless VPN

In this mode the RDP links are published on the Gateway home page or portal, as bookmarks, through the `add vpn url` configuration or through an external portal. The user can click these links to get access to the Remote Desktop.

Deployment through ICA Proxy

In this mode a custom home page is configured on the Gateway VIP by using the `wihome` parameter. This home page can be customized with the list of Remote desktop resources that the user is allowed

to access. This custom page can be hosted on NetScaler, or if external, it can be an iFrame in the existing Gateway portal page.

In either mode, after the user clicks the provisioned RDP link or icon, an HTTPS request for the corresponding resource arrives at the NetScaler Gateway. The Gateway generates the RDP file content for the requested connection and pushes it to the client. The native RDP client is invoked, and it connects to an RDP listener on Gateway. Gateway does SSO to the RDP server by supporting enforcement (SmartAccess). The gateway blocks client access to certain RDP features, based on the NetScaler configuration, and then it proxies the RDP traffic between the RDP client and the server.

Enforcement details

The NetScaler administrator can configure certain RDP capabilities through the NetScaler Gateway configuration. NetScaler Gateway provides the "RDP enforcement"feature for important RDP parameters. NetScaler ensures that the client cannot enable blocked parameters. If the blocked parameters are enabled, the RDP enforcement feature supersedes the client-enabled parameters, and they are not honored.

> **Important:** Enforcement feature is applicable only if SSO is enabled.

Supported RDP parameters for enforcement

Enforcement for following redirection parameters is supported. These parameters are configurable as part of an RDP client profile.

- Redirection of clipboard
- Redirection of printers
- Redirection of disk drives
- Redirection of COM ports
- Redirection of PNP devices

Connection flow

Connection flow can be divided into two steps:

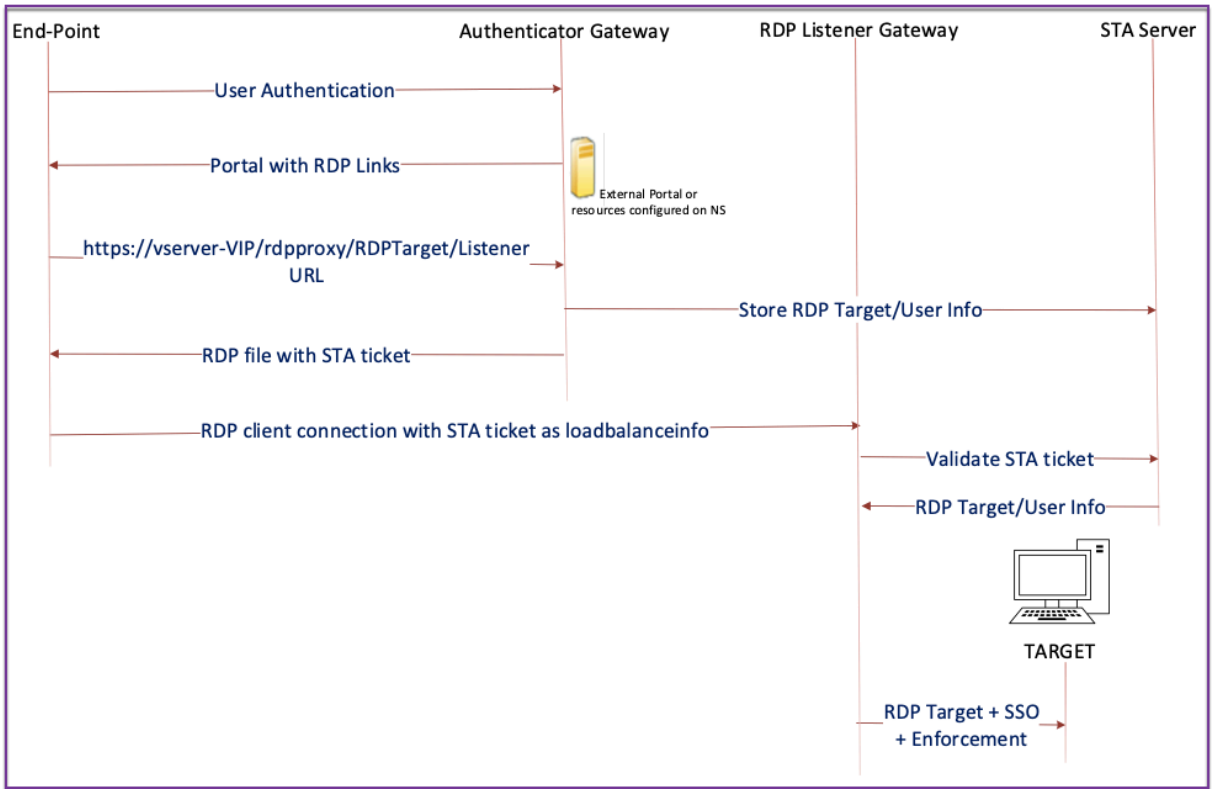
- RDP resource enumeration and RDP file download.
- RDP connection launch.

Based on the preceding connection flow, there are two deployment solutions:

- Stateless (Dual) gateway solution - the RDP resource enumeration and RDP file download happens through the authenticator gateway but RDP connection launch happens through the RDP Listener gateway.
- Single gateway solution - the RDP resource enumeration, RDP file download, and RDP connection launch happen through the same gateway.

Stateless (dual) gateway compatibility

The following figure depicts the deployment:



- A User connects to the Authenticator Gateway VIP and provides the credentials.
- After a successful login to the gateway, the user is redirected to the home page or external portal, which enumerates the remote desktop resources that the user can access.
- Once the user selects an RDP resource, the Authenticator Gateway VIP receives the request in the format `https://vserver-vip/rdpproxy/rdptarget/listener` indicating the published resource that the user clicked. This request has the information about the IP address and port of the RDP server that the user has selected.
- The Authenticator Gateway processes the /rdpproxy/ request. Because the user is already authenticated, this request comes with a valid Gateway cookie.

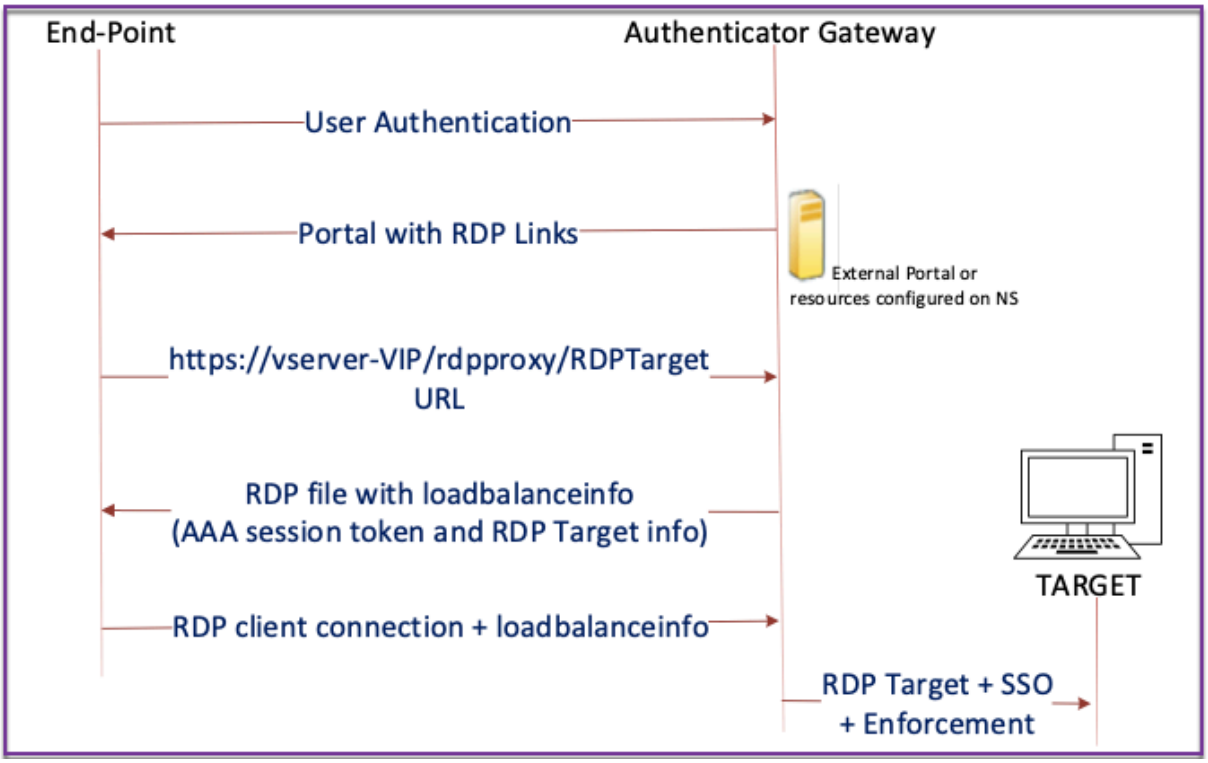
- The `RDPTarget` and `RDPUser` information is stored on the STA server, and an STA Ticket is generated. The information stored on the STA server is encrypted by using the configured pre-shared key. The Authenticator Gateway uses one of the STA servers that is configured on the gateway virtual server.
- The 'Listener'info obtained in the /rdpproxy/ request is put into the `.rdp file` as the "`fulladdress`,"and the STA ticket (pre-pended with the STA AuthID) is put into the `.rdp file` as the "`loadbalanceinfo`."
- The `.rdp file` is sent back to the client end-point.
- The native RDP client launches and connects to the `RDPListener Gateway`. It sends the STA ticket in the initial packet.

  The `RDPListener` Gateway validates the STA ticket and obtains the `RDPTarget` and `RDPUser` information. The STA server to be used is retrieved by using the 'AuthID'present in the `loadbalanceinfo`.
- A gateway session is created for storing authorization/auditing policies. If a session exists for the user, it is reused.
- The `RDPListener` Gateway connects to the `RDPTarget` and single signs on using CREDSSP.

> **Important:**
>
> - For stateless RDP proxy, the STA Server validates the STA ticket, sent by the RDP client, to obtain the `RDPTarget`/`RDPUser` information. You must bind the STA server in addition to the VPN virtual server.

Single gateway compatibility

The following figure depicts the deployment:



> **Important:**
>
> In the case of a single gateway deployment, the STA server is not required. The authenticator gateway encodes the `RDPTarget` and the NetScaler authentication, authorization, and auditing session cookie securely and sends them as the `loadbalanceinfo` in the `.rdp file`. When the RDP Client sends this token in the initial packet, the authenticator gateway decodes the `RDPTarget` information, looks up the session, and connects to the `RDPTarget`.

Support for single listener

- Single Listener for Both RDP and SSL Traffic.
- The RDP file download and RDP traffic can be handled through the same 2 tuple (that is, IP and Port) on the NetScaler appliance.

License requirements for RDP Proxy

Premium edition, Advanced edition

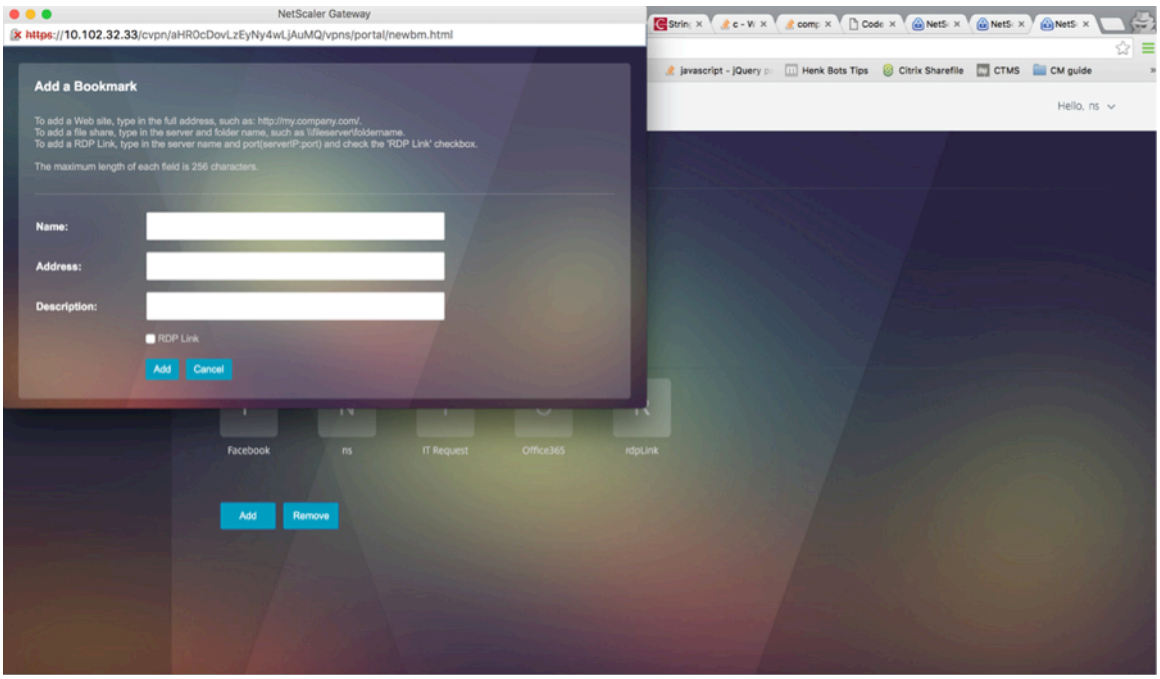
> **Note:**
>
> RDP Proxy function is not available to customers who have only a Gateway platform license or only the Standard edition.

You can use the following command to enable RDP proxy.

```
enable feature rdpProxy
```

Bookmark

RDP link generation through Portal. Instead of configuring the RDP links for the user or publishing the RDP links through an external portal, you can give users an option to generate their own URLs by providing `targerIP:Port`. For stateless RDP-proxy deployment, the administrator can include RDP listener information in FQDN: Port format as part of the RDP Client Profile. This is done under the `rdpListener` option. This configuration is used for the RDP link generation through the portal in Dual Gateway mode.



Create bookmarks

1. Create bookmarks on the portal page to access the RDP resources: (The actualURL starts with `rdp://`).
2. Add VPN url `<urlName> <linkName> <actualURL>`
   - The URL must be in the following format: `rdp://<TargetIP:Port>`.
   - For Stateless RDP proxy mode, The URL must be in the following format: `rdp://<TargetIP:Port>/<ListenerIP:Port>`

- The URL is published on the portal in the format:
  `https://<VPN-VIP>/rdpproxy/<TargetIP:Port>`
  `https://<VPN-VIP>/rdpproxy/<TargetIP:Port>/<ListenerIP:Port>`

3. Bind the bookmarks to the user, or group, or the VPN virtual server, or VPN global.

Features and modes to be enabled for RDP Proxy

```
- enable ns feature ssl

- enable ns feature sslvpn

- enable ns feature rdpproxy

- enable mode usnip
```

RDP Proxy high-level configuration steps

The following high-level steps involved in the stateless RDP proxy configuration.

- Create an RDP server profile
- Create an RDP client profile
- Create and bind a virtual server
- Create a bookmark
- Create or edit a session profile or policy
- Bind a bookmark

Configure a client profile

Configure the client profile on the authenticator gateway. The following is a sample configuration:

```
add rdpClient profile <name> [-addUserNameInRdpFile ( YES | NO )] [-
    audioCaptureMode ( ENABLE | DISABLE )] [-keyboardHook <keyboardHook
    >] [-multiMonitorSupport ( ENABLE | DISABLE )] [-psk <string>] [-
    rdpCookieValidity <positive_integer>] [-rdpCustomParams <string>] [-
    rdpFileName <string>] [-rdpHost <optional FQDN that will be put in
    the RDP file as ‘ fulladdress>] [-rdpUrlOverride ( ENABLE | DISABLE
    )] [-redirectClipboard ( ENABLE | DISABLE )] [-redirectComPorts (
    ENABLE | DISABLE )] [-redirectDrives ( ENABLE | DISABLE )] [-
    redirectPnpDevices ( ENABLE | DISABLE )] [-redirectPrinters ( ENABLE
     | DISABLE )] [-videoPlaybackMode ( ENABLE | DISABLE )]
```

Associate the RDP client profile with the VPN virtual server.

This can be done either by configuring a sessionAction+sessionPolicy or by setting the global VPN parameter.

Example:

```
add vpn sessionaction <actname> -rdpClientprofile <rdpprofilename>

add vpn sessionpolicy <polname> NS_TRUE <actname>

bind vpn vserver <vservername> -policy <polname> -priority <
    prioritynumber>
```

OR

```
set vpn parameter -rdpClientprofile <name>
```

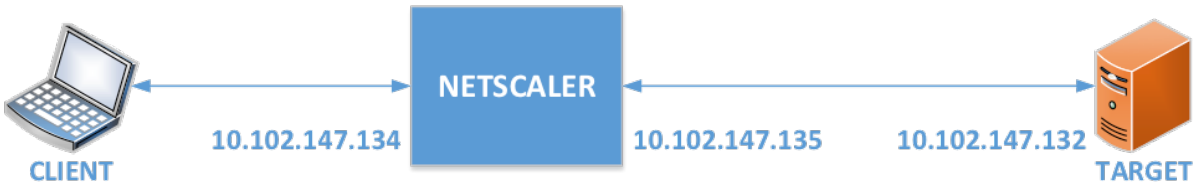
Configure a server profile

Configure the server profile on the listener gateway.

```
add rdp ServerProfile <profilename> -rdpIP <IPV4 address of the RDP
    listener> -rdpPort <port for terminating RDP client connections> -
    psk <key to decrypt RDPTarget/RDPUser information, needed while
    using STA>`
```

The `rdp ServerProfile` must be configured on the VPN virtual server.

```
add vpn vserver v1 SSL <publicIP> <portforterminatingvpnconnections> -
    rdpServerProfile <rdpServer Profile>`
```



RDP Proxy configuration by using the CLI

The following is a sample RDP Proxy configuration by using the CLI.

- Add the VPN URL for the user with the target information.

```
add aaa user Administrator -password freebsd123$%^

add vpn url rdp RdpLink rdp://rdpserverinfo

add dns addrec rdpserverinfo 10.102.147.132

```



```
bind aaa user Administrator  -urlName rdp
```

- Configure RDP client and server profile for the VPN connection.

```
add rdp clientprofile p1 -psk citrix -redirectClipboard ENABLE

add rdp serverprofile p1 -rdpIP 10.102.147.134 -psk citrix

add vpn vserver mygateway SSL  10.102.147.134 443 -
    rdpserverprofile p1

set vpn parameter -clientlessVpnMode ON -
    defaultAuthorizationAction ALLOW -rdpClientProfileName p1

add ssl certKey gatewaykey -cert rdp_rootcert.pem  -key
    rdp_rootkey

bind ssl vserver mygateway -certkeyName gatewaykey
```

- ADD SNIP for connection from NetScaler to target.

```
add ns ip 10.102.147.135  255.255.255.0 -type SNIP
```

RDP proxy configuration by using the GUI

1. Navigate to **NetScaler Gateway > Policies**, right-click **RDP**, and click **Enable Feature**.
2. Click RDP on the navigation pane. On the right, select the **Client Profiles** tab and click **Add**.
3. Enter a name for the client profile a name and configure it.

Configure RDP Client Profile

Name

RDPs

URL Override*

ENABLE

Redirect Clipboard*

ENABLE

Redirect Drives*

DISABLE

Redirect Printers*

ENABLE

Redirect comports*

DISABLE

Redirect PNP Devices*

DISABLE

Keyboard Hook*

InFullScreenMode

Audio Capture Mode*

DISABLE

Video Playback Mode*

ENABLE

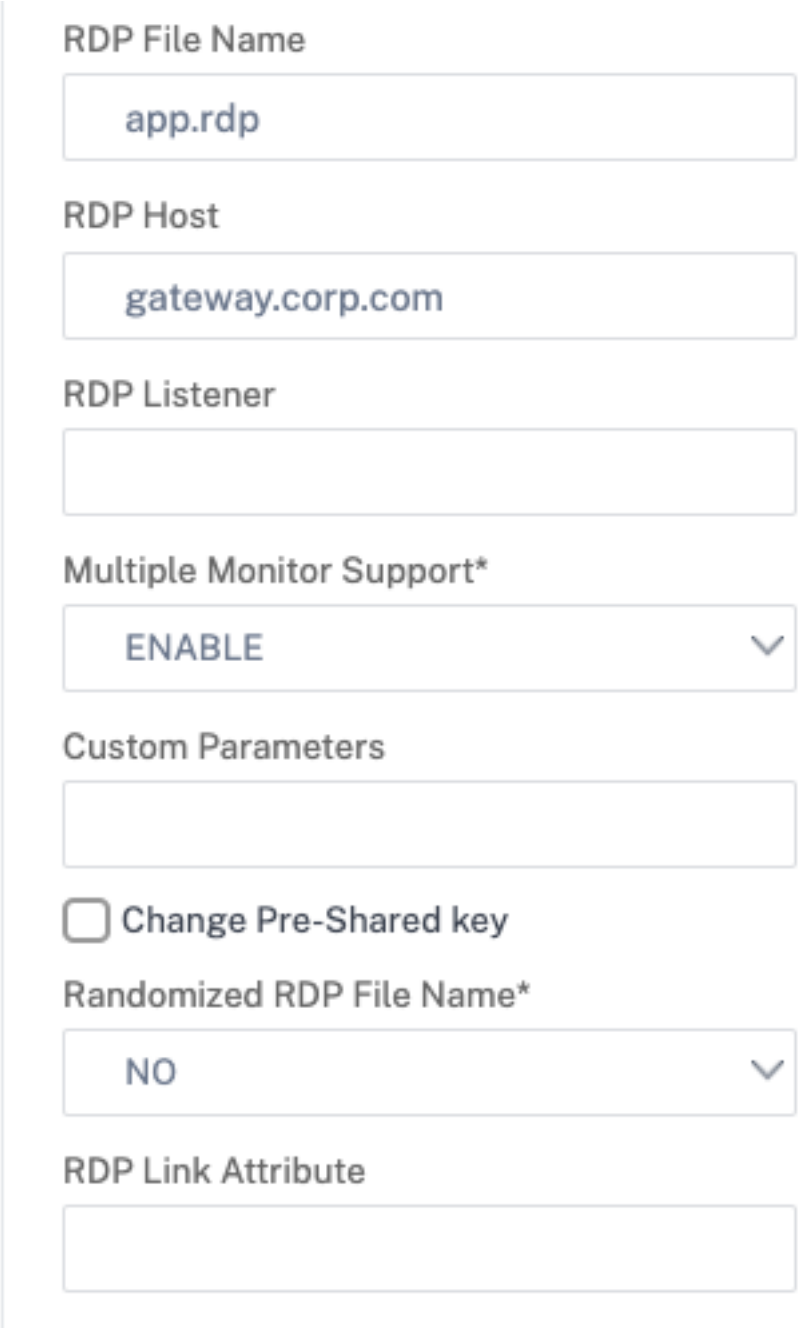
RDP Cookie Validity (seconds)

60

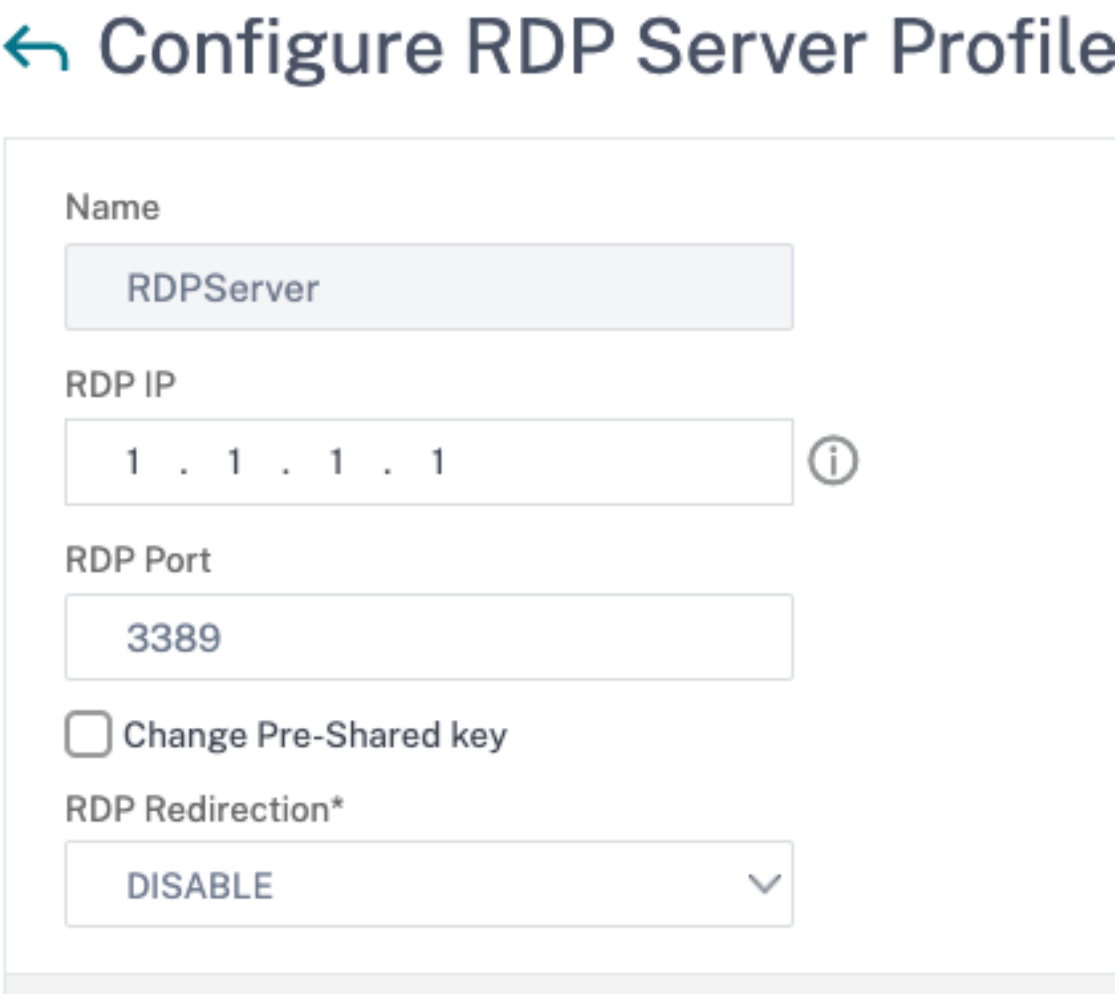
Add Username In RDP File*

NO

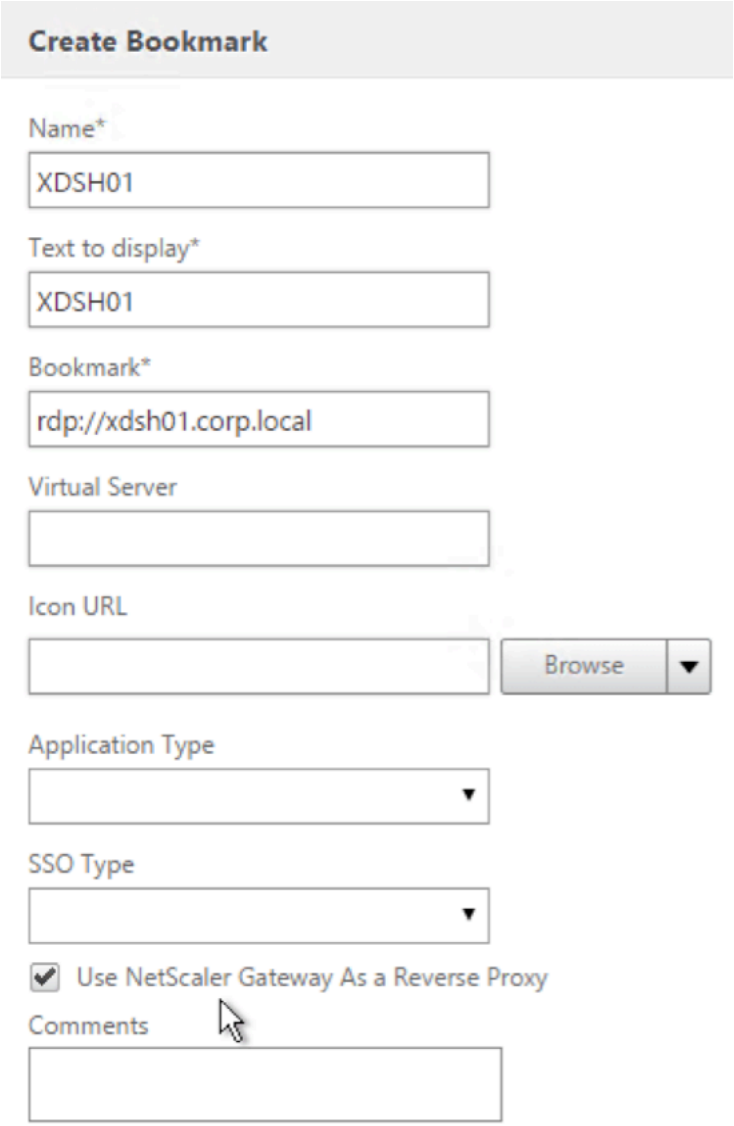
4. In the RDP Host field, enter the FQDN that resolves to the RDP Proxy listener, which is typically the same FQDN as the NetScaler Gateway appliance's FDQN.
5. In **Pre Shared Key**, enter a password and click **OK**.



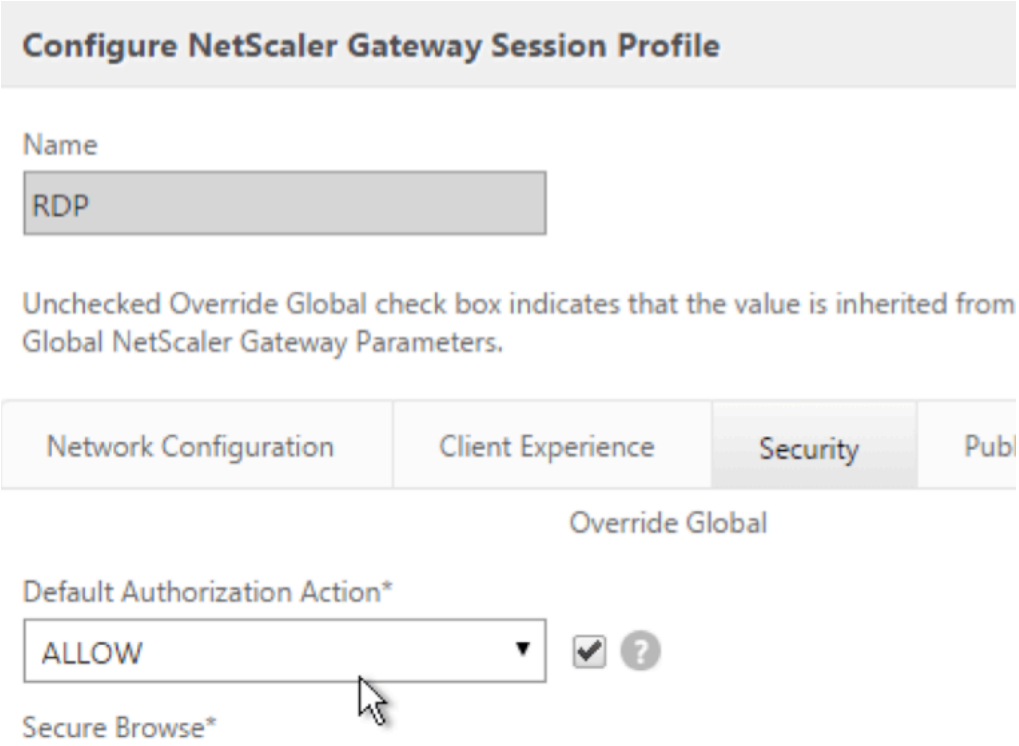
6. Enter the server profile a name.
7. Enter the IP address of the gateway virtual server you're going to bind this profile.
8. Enter the same preshared key you configured for the RDP client profile. Click **Create**.



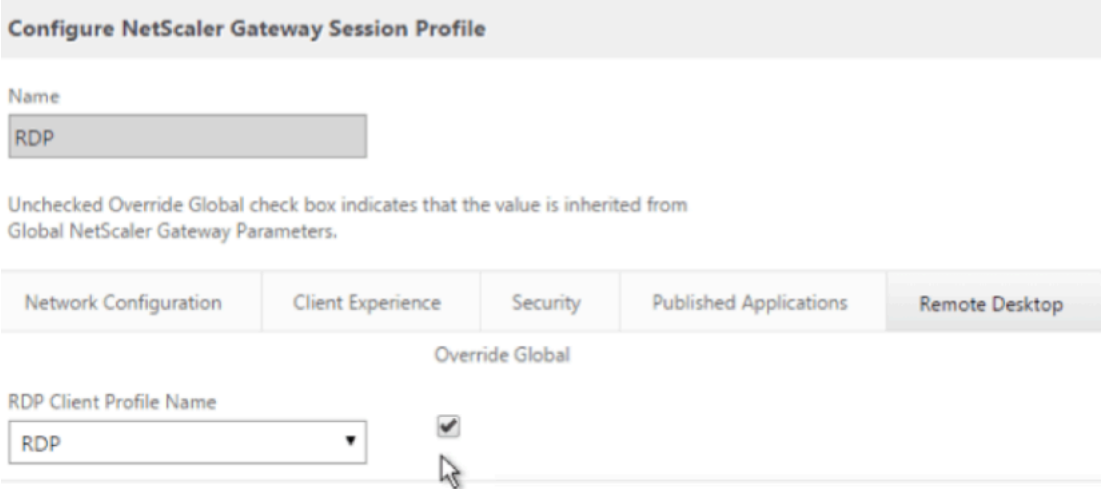
9. If you want to add RDP bookmarks on the Clientless Access portal page, on the left, expand **NetScaler Gateway**, expand **Resources**, and click **Bookmarks**.
10. On the right, click **Add**.
11. Give the Bookmark a name.
12. For the URL, enter **rdp://MyRDPServer using IP or DNS**.
13. Select Use **NetScaler Gateway As a Reverse Proxy** and click **Create**.
14. Create bookmarks as per your requirement.



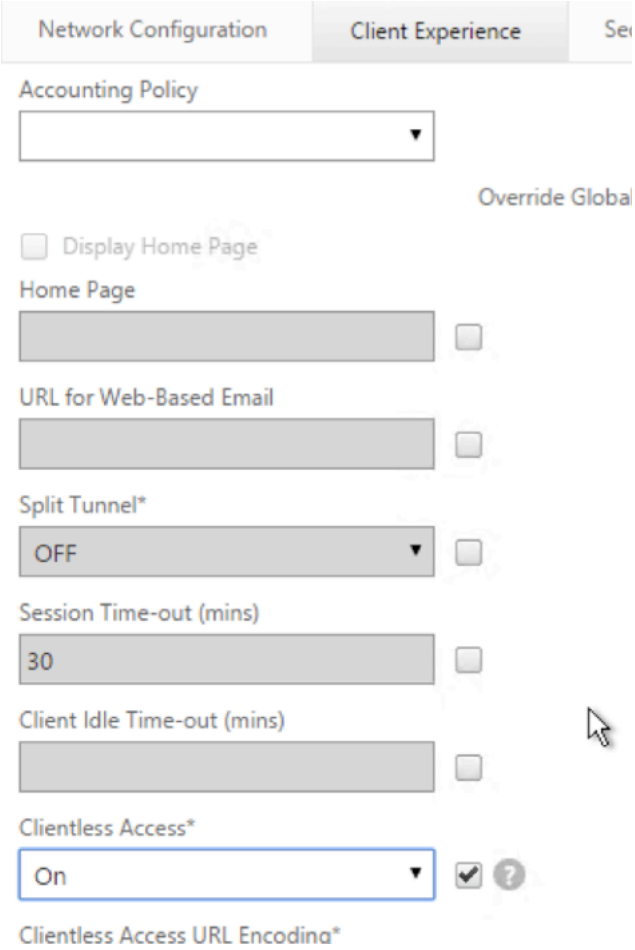
15. Create or edit a session profile. Navigate to **NetScaler Gateway > Policies > Session**.
16. On the Security tab, set **Default Authorization Action** to **ALLOW**. Or you can use authorization policies to control access.



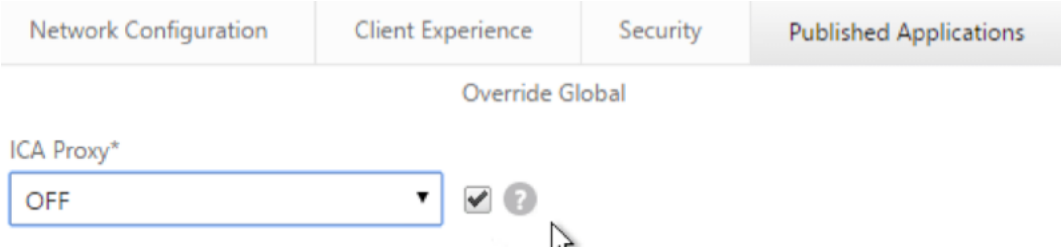
17. On the Remote Desktop tab, select the RDP client profile you created earlier.



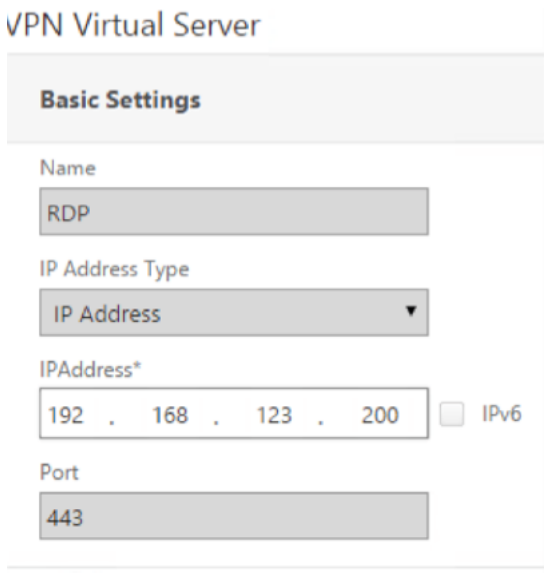
18. If you want to use bookmarks, on the **Client Experience** tab, set **Clientless Access** to **On**.



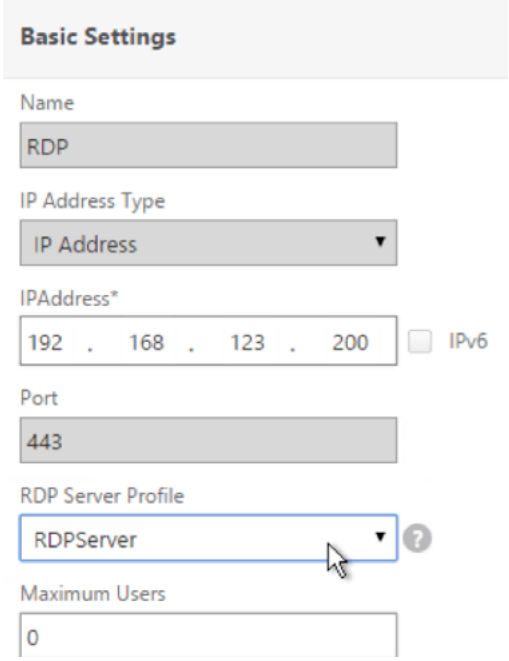
19. On the **Published Applications** tab, make sure that ICA Proxy is **OFF**.



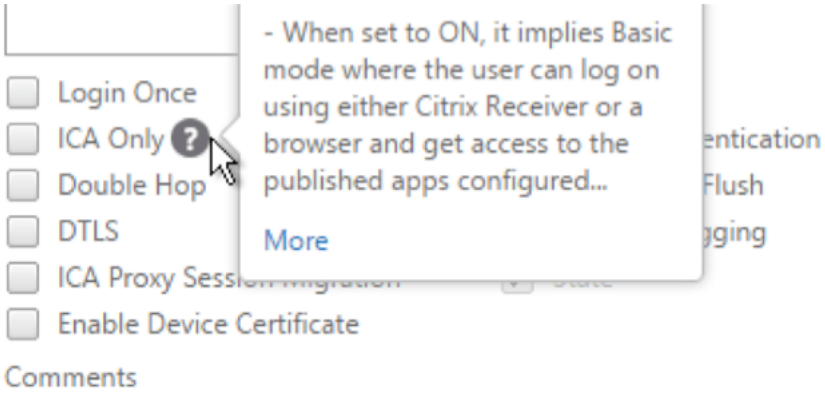
20. Modify or create your gateway virtual server.
21. In the **Basic Settings** section, click **More**.



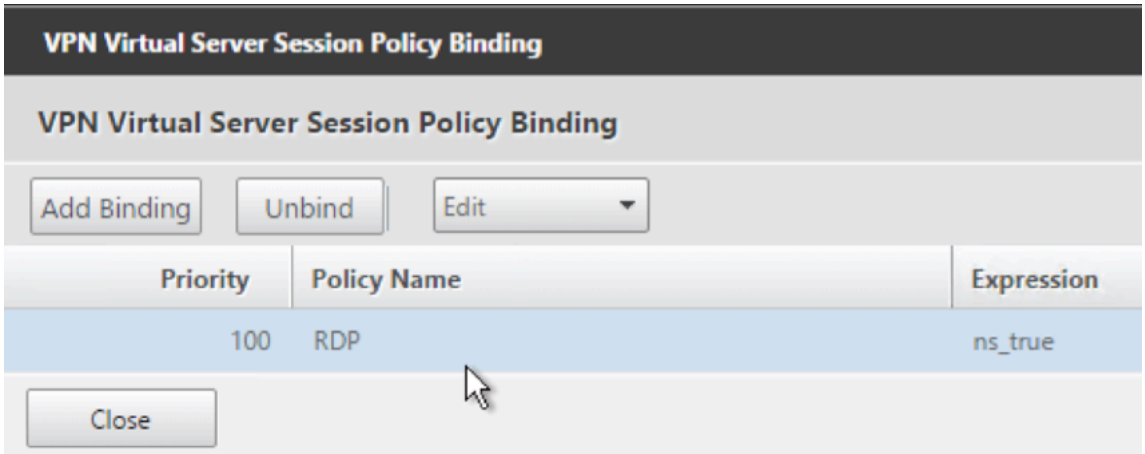
22. Use the RDP server profile list to select the RDP server profile you created earlier.



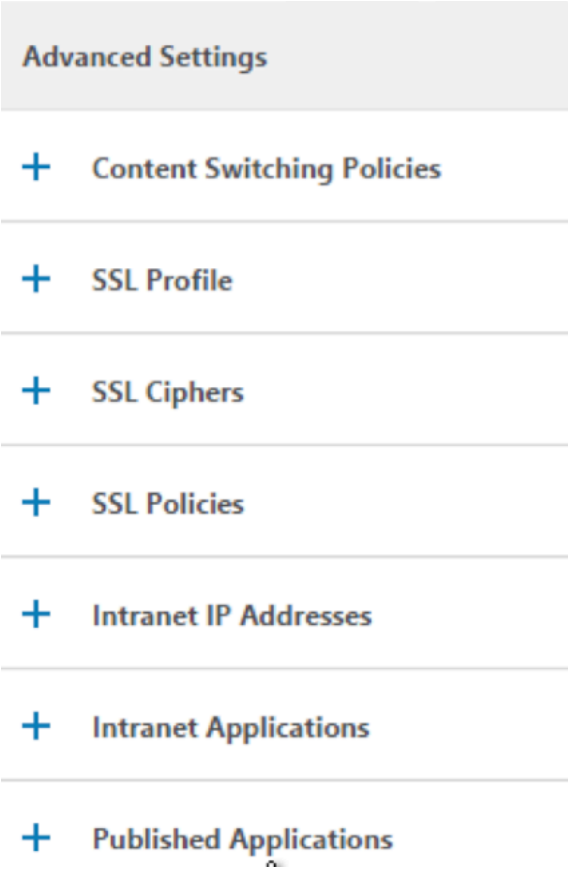
23. Scroll down. Make sure that **ICA Only** is not checked.



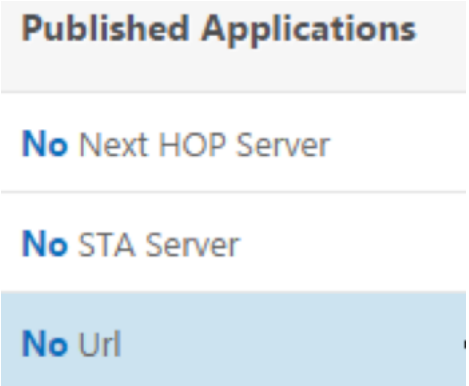
24. Bind a certificate.
25. Bind authentication policies.
26. Bind the session policy/profile that has the RDP client profile configured.



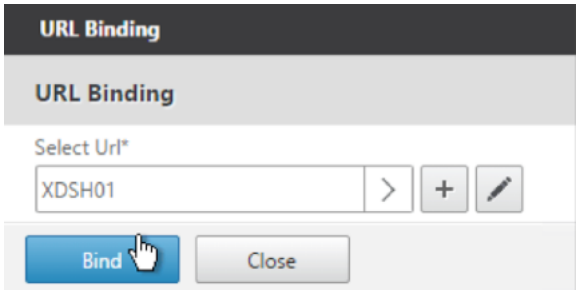
27. You can bind bookmarks to either the NetScaler Gateway virtual server or to an authentication, authorization, and auditing group. To bind to the NetScaler Gateway virtual server, on the right, in the Advanced Settings section, click **Published Applications**.



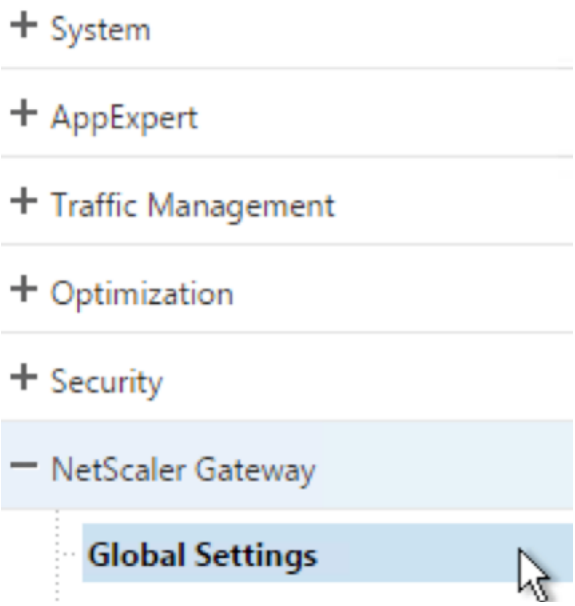
28. On the left, in the **Published Applications** section, click **No Url**.



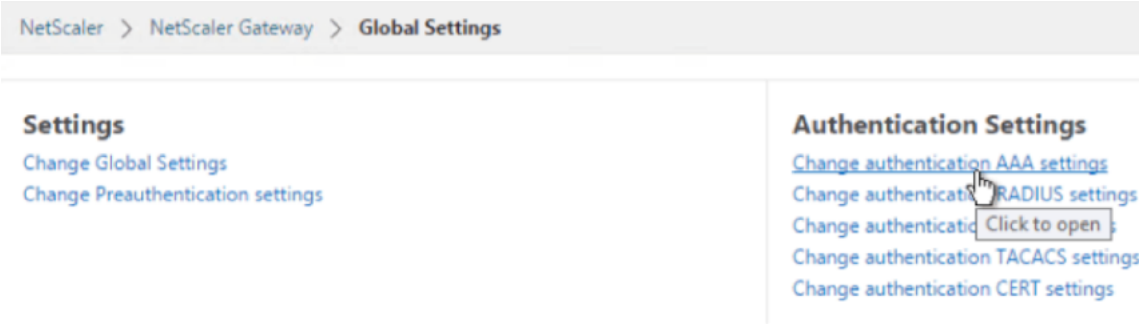
29. Bind your bookmarks.



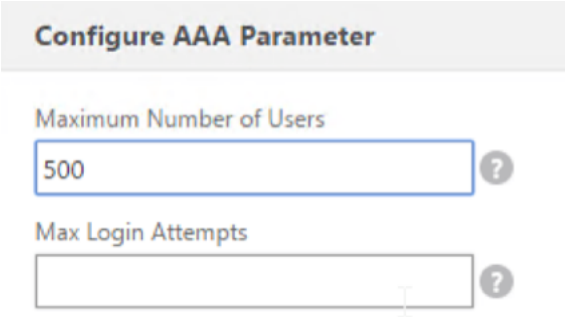
30. Because ICA Only is not specified for this NetScaler Gateway virtual server, make sure that your NetScaler Gateway Universal licenses are configured correctly. On the left, expand **NetScaler Gateway** and click **Global Settings**.



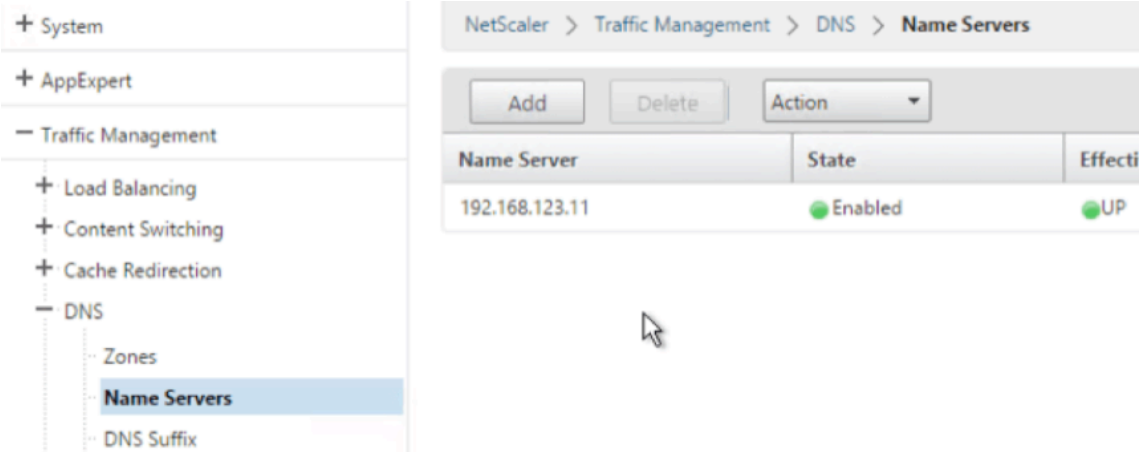
31. On the right, click **Change authentication AAA settings**.



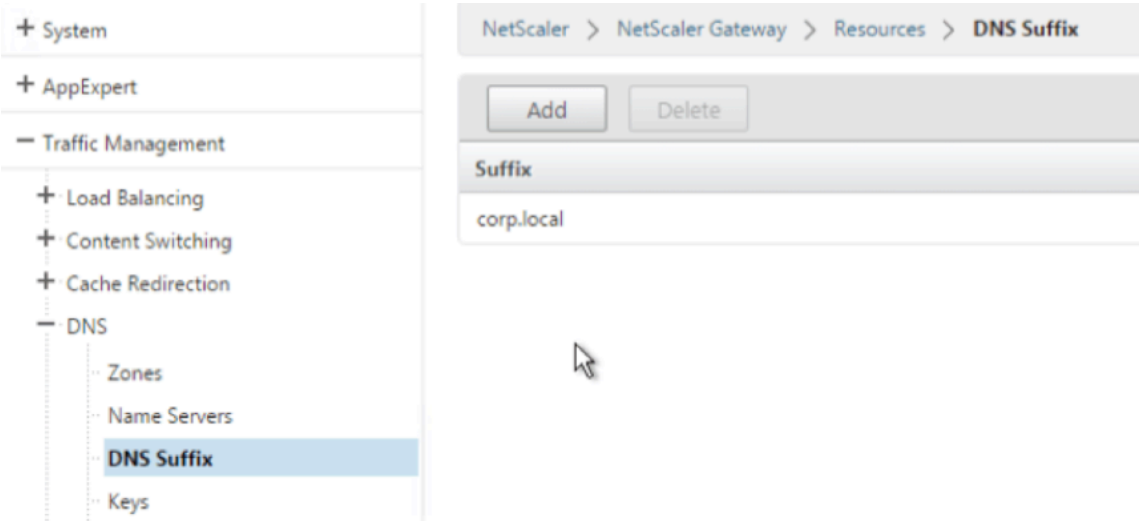
32. Change the **Maximum Number of Users** to your licensed limit.



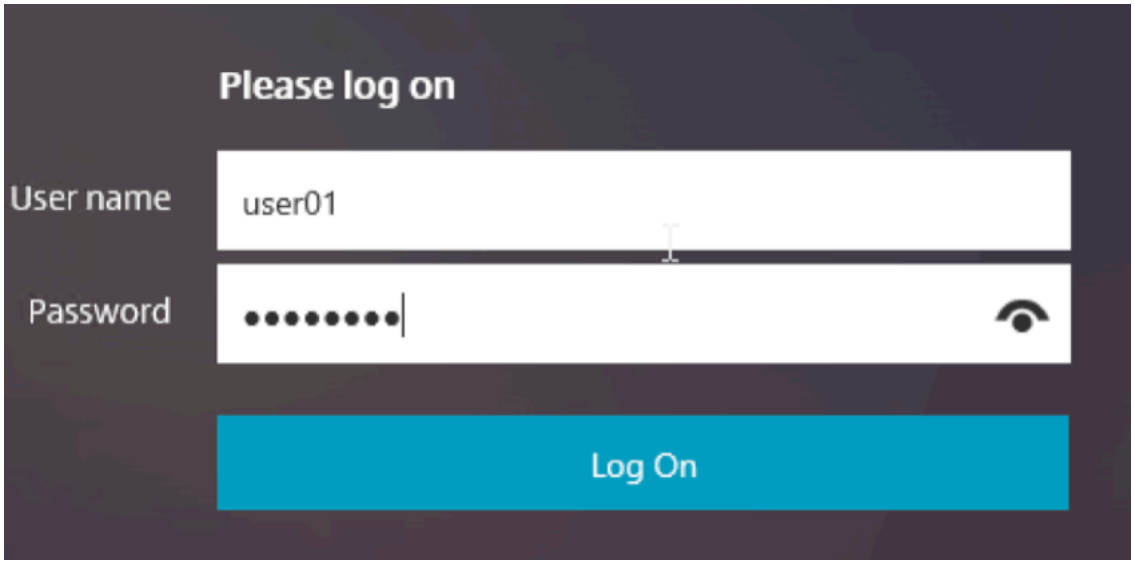
33. If you want to connect to RDP servers by using DNS, make sure that DNS servers are configured on the appliance (**Traffic Management > DNS > Name Servers)**.



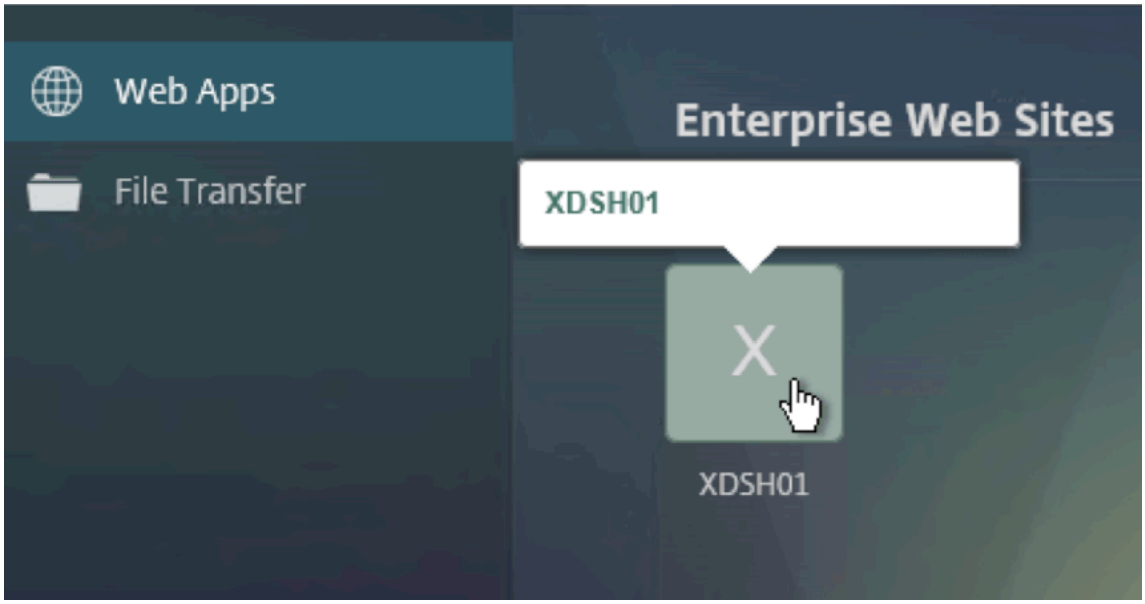
34. If you want to use the short names instead of FQDNs, add a **DNS Suffix (Traffic Management > DNS > DNS Suffix)**.



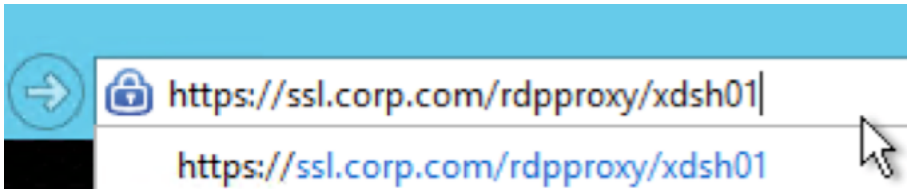
35. Connect to your gateway and log on.



36. If you configured **Bookmarks**, click the **Bookmark**.

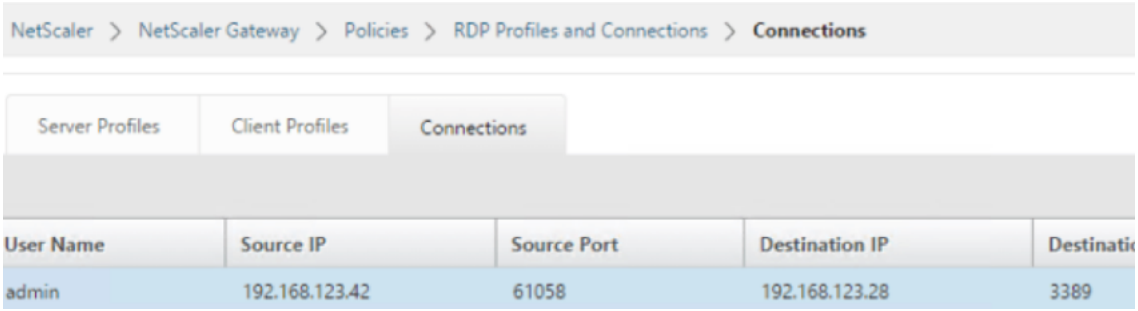


37. You can change the address bar to **/rdpproxy/MyRDPServer**. You can enter an IP address (for example rdpproxy/192.168.1.50) or DNS name (/rdpproxy/myserver).



38. Open the downloaded `.rdp file`.

39. You can view the currently connected users by going to **NetScaler Gateway Policies > RDP.** On the right is the **Connections** tab.



Option to disable SSO

The SSO (single sign-on) feature with RDP proxy can be disabled by configuring NetScaler traffic policies so the user is always prompted for credentials. When SSO is disabled, RDP enforcement (SmartAccess) doesn't work.

Example:

```
add vpn trafficaction <TrafficActionName> HTTP -SSO OFF
```

Traffic policy can be configured as per the requirement, the following are two examples:

- To disable SSO for all the traffic:

```
add vpn trafficpolicy <TrafficPolicyName>  "url contains rdpproxy
    " <TrafficActionName>
```

- To disable SSO based on Source/Destination IP/FQDN

```
add vpn trafficPolicy <TrafficPolicyName>  "HTTP.REQ.URL.CONTAINS
    (\"rdpproxy\") && CLIENT.IP.SRC.EQ(<IP>)" <TrafficActionName>
bind vpnvserver rdp -policy <TrafficPolicyName> -priority 10
```

Stateless RDP Proxy

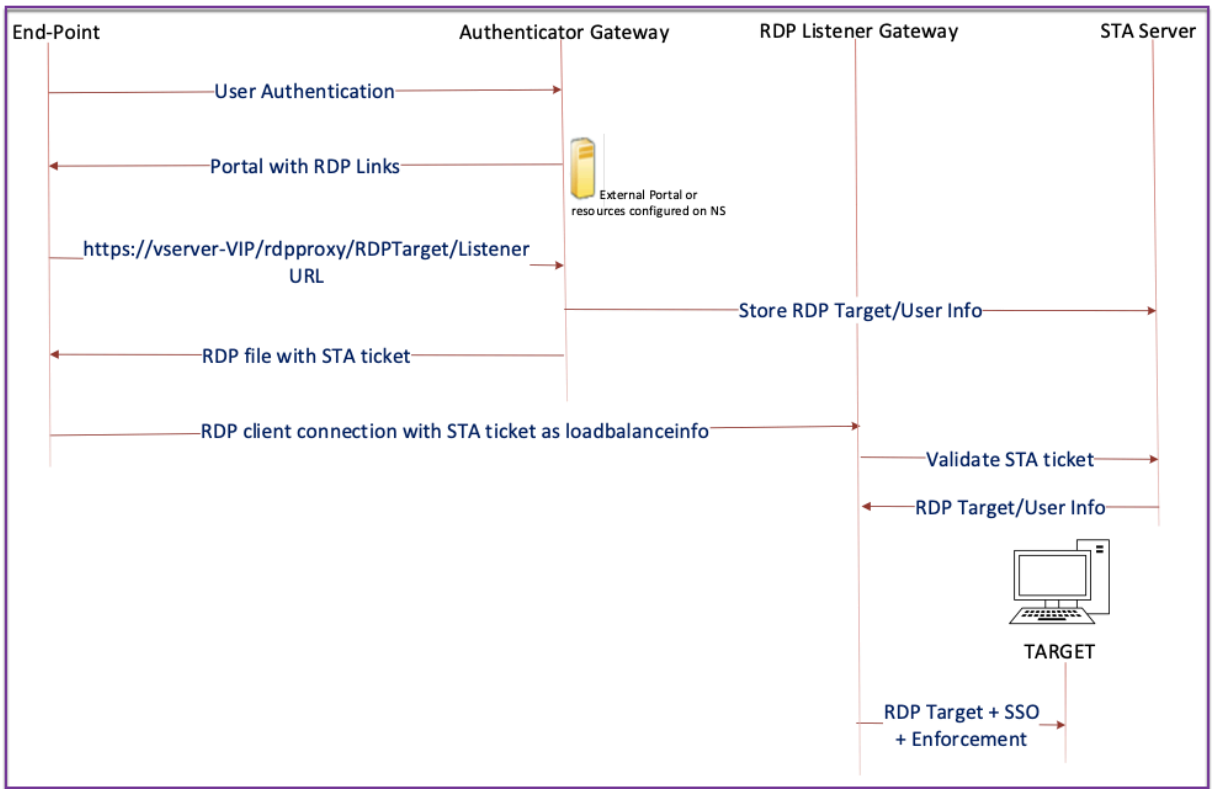
January 8, 2024

The Stateless RDP Proxy accesses an RDP host. Access is granted through the `RDPListener` on NetScaler Gateway when the user authenticates on a separate NetScaler Gateway Authenticator. The information required by the `RDPListener` for NetScaler Gateway is securely stored on a STA server. A STA server can be placed anywhere as long as the NetScaler Gateway and application enumeration servers can reach it. For details see, https://support.citrix.com/article/CTX101997.

Connection flow

There are two connections involved in the RDP Proxy flow. The first connection is the user's SSL VPN connection to the NetScaler Gateway VIP, and enumeration of the RDP resources.

The second connection is the native RDP client connection to the RDP listener (configured using rdpIP and rdpPort) on the NetScaler Gateway, and subsequent proxying of the RDP client to server packets securely.



1. The User connects to the Authenticator Gateway VIP and provides the credentials.
2. After successful login to the gateway, the user is redirected to the homepage/external portal which enumerates the remote desktop resources that the user can access.
3. Once the user selects an RDP resource, a request is received by the Authenticator Gateway VIP, in the format `https://AGVIP/rdpproxy/ip:port/rdptargetproxy` indicating the published resource that the user clicked. This request has the information about the IP and port of the RDP server that the user has selected.
4. The authenticator gateway processes the /rdpproxy/ request. Because the user is already authenticated, this request comes with a valid gateway cookie.
5. The `RDPTarget` and `RDPUser` information is stored on the STA server and a STA Ticket is generated. The information is stored as an XML blob which is optionally encrypted using the configured pre-shared key. If encrypted, the blob is base64 encoded and stored. The Authenticator

Gateway uses one of the STA servers that is configured on the Gateway virtual server.

6. The XML blob is in the following format

```
<Value name=" IPAddress " >ipaddr</Value>\n<Value name=" Port " >
    port</Value\>n

<Value name=" `Username` " >username</Value\>\n<Value name=" 
    Password " >pwd\</Value\>
```

7. The `rdptargetproxy` obtained in the /rdpproxy/ request is put as the '`fulladdress`'and the STA ticket (pre-pended with the STA AuthID) is put as the `loadbalanceinfo` in the.rdp file.
8. The `.rdp` file is sent back to the client end-point.
9. The native RDP client launches and connects to the `RDPListener Gateway`. It sends the STA ticket in the initial x.224 packet.
10. The `RDPListener Gateway` validates the STA ticket and obtains the `RDPTarget` and `RDPUser` information. The STA server to be used is retrieved using the 'AuthID'present in the `loadbalanceinfo`.
11. A Gateway session is created for storing authorization/auditing policies. If a session exists for the user, it is reused.
12. The `RDPListener Gateway` connects to the `RDPTarget` and single signs on using CREDSSP.

Prerequisites

- User is authenticated on the NetScaler Gateway authenticator.
- The initial /rdpproxy URL and RDP Client are connected to a different `RDPListener NetScaler Gateway`.
- The Authenticator Gateway using a STA Server securely passes the `RDPListener Gateway` information.

Configure stateless RDP Proxy by using the CLI

- Add a `rdpServer` profile. The server profile is configured on the `RDPListener Gateway`.

  Note:

  - Once the rdpServer Profile is configured on the VPN virtual server, it cannot be modified. Also, the same serverProfile cannot be reused on another VPN virtual server.


```
add rdpServer Profile [profilename] -rdpIP [IPV4 address of the RDP listener] -rdpPort [port for terminating RDP client connections] -psk [key to decrypt RDPTarget/RDPUser information, needed while using STA].
```

Configure the RDP server profile on the VPN virtual server using the following command:

```
add vpn vserver v1 SSL [publicIP] [portforterminatingvpnconnections] -rdpServerProfile [rdpServer Profile]
```

Example

```
add vpn vserver v1 SSL 1.1.1.1 443 -rdpServerProfile rdp_server_prof
```

> **Important:**
>
> - The same STA server must be bound to both RDP authenticator gateway and listener gateway.
> - For stateless RDP proxy, the STA Server validates the STA ticket that is sent by the RDP client to obtain the RDP Target server and RDP user's information. You must bind the STA server in addition to the VPN virtual server. In the following example, the RDP target server is 1.1.1.0 and the RDP listener gateway virtual server 1.1.1.2.
>
> ```
> add vpn url url4 RDP2 "rdp://1.1.1.0/1.1.1.2:443"
> ```

Configure the client profile on the authenticator Gateway using the following command:

```
add rdpClient profile <name> -rdpHost <optional FQDN that will be put in the RDP file as ‘fulladdress’> [-rdpUrlOverride ( ENABLE | DISABLE )] [-redirectClipboard ( ENABLE | DISABLE )] [-redirectDrives ( ENABLE | DISABLE )]

        [-redirectPrinters ( ENABLE | DISABLE )] [-keyboardHook <keyboardHook>] [-audioCaptureMode ( ENABLE | DISABLE )] [-videoPlaybackMode ( ENABLE | DISABLE )]

        [-rdpCookieValidity <positive_integer>][-multiMonitorSupport ( ENABLE | DISABLE )] [-rdpCustomParams <string>]
```

The –rdpHost configuration is used in a single Gateway deployment. Only `psk` is a mandatory argument and it must be the same PSK that is added in the RDP server profile in the RDP listener gateway.

- Associate the RDP Profile with the VPN virtual server.

You can associate an RDP profile either by configuring a sessionAction+sessionPolicy or by setting the global VPN parameter.

Example:

```
add vpn sessionaction <actname> -rdpClientprofile <rdpprofilename>

add vpn sessionpolicy <polname> NS_TRUE <actname>

bind vpn vserver <vservername> -policy <polname> -priority <
    prioritynumber>
```

OR

```
set vpn parameter – rdpClientprofile <name>
```

Configure stateless RDP proxy by using the GUI

The following high-level steps are involved in the stateless RDP proxy configuration. For the detailed steps, see RDP Proxy configuration.

- Create an RDP server profile
- Create an RDP client profile
- Create a virtual server
- Create a bookmark
- Create or edit a session profile or policy
- Bind a bookmark

> **Important:**
>
> For stateless RDP proxy, you must bind a STA server in addition to the VPN virtual server.

Connection counter

A new connection counter ns_rdp_tot_curr_active_conn was added, which keeps the record of the number of active connections in use. It can be viewed as a part of the `nsconmsg` command on the NetScaler shell. CLI command to view these counters is planned to be added later.

Upgrade notes

The rdpIP and rdpPort, which were previously configured on the VPN virtual server is part of the rdpServerProfile. The `rdp Profile` is renamed as `rdp ClientProfile` and the parameter clientSSL is removed. Therefore, the earlier configuration does not work.

RDP connection redirection

January 8, 2024

A NetScaler Gateway appliance now supports RDP connection redirection in the presence of a connection broker or session directory. An RDP proxy communication no longer requires an exclusive URL for every connection from the client to the server. Instead, the proxy uses a single URL to connect to an RDP server farm, reducing the maintenance and configuration overhead for an administrator.

Point to note:

- RDP connection redirection is supported only when SSO is enabled and is supported in both single Gateway and Stateless or Dual Gateway mode along with enforcement (SmartAccess).
- RDP Proxy feature is supported only with token-based redirection supporting IP cookies. IP-based routing tokens "msts="are handed back by the Windows session broker or Connection broker when the **Use IP Address Redirection** functionality is disabled.
- You can disable the **Use IP Address Redirection** setting to enable token-based redirection in the following location.
  `Computer Configuration` > `Policies` > `Administrative Templates` > `Windows Components` > `Remote Desktop Services` > `Remote Desktop Session Host` > `RD Connection Broker`.
- Disable the Use IP Address Redirection setting on the RDSH machines and not the connection broker machine.
- Dedicated redirectors for RDP Proxy connection can be configured.

Prerequisites

- Create an RDP server profile to enable the 3389 listener on the NetScaler Gateway virtual server. If the machine that you want to RDP is not a member of any RDS connection broker infrastructure, then you do not need the 3389 listener.
- Enable RDP connection redirection on the NetScaler Gateway appliance to support RDP Proxy in the presence of a connection broker.

Deploy RDP Proxy in the presence of a connection broker

RDP Proxy in the presence of a connection broker can be deployed in the following two ways.

- With RD session host servers participating in RD connection broker load-balancing.

- In the presence of the RDP load balancing feature.

With RD session host servers participating in RD connection broker load balancing:

In this case, the RDP URL link can be configured to point to one of the RDP servers as the destination server, which acts as redirector. Also, it is possible to have one of the RDP servers in the farm as destination server (in this case the server does not accept any RDP session).

In the presence of the RDP load-balancing feature:

When connection broker load-balancing is not enabled, we can have the RDP load-balancing feature available on NetScaler to do the required load-balancing of the RDP sessions in the presence of a connection broker. In this case, the RDP URL link has to be configured to have the RDP load balancer as destination server. The RDP load-balancer can be on the same NetScaler Gateway appliance as the RDP Proxy. For more information, refer Loading balancing RDP servers.

Configure RDP Proxy in the presence of a connection broker by using the CLI

At the command prompt, type;

```
add rdpserverprofile <Name> -psk <string> -rdpRedirection ( ENABLE |
    DISABLE )

add rdpserverprofile serverProfileName -psk " secretString " -
    rdpRedirection ENABLE
```

Configure RDP connection redirection by using the NetScaler GUI

1. Navigate to **NetScaler Gateway > Policies > RDP**.
2. Right-click **RDP** to **Enable** or **Disable** the RDP redirection functionality.

Populate RDP URLs based on LDAP attribute

January 8, 2024

You can configure a NetScaler Gateway appliance to retrieve a list of RDP servers (IP/FQDN) from an LDAP server attribute. Based on the retrieved list, the appliance displays the RDP URLs for the servers that can be accessed by a user.

To populate RDP URLs based on the LDAP attribute by using the CLI

At the command prompt, type:

```
add rdpclientprofile <Name> – rdpUrlLinkAttribute <string>

add rdpclientprofile clientProfileName – rdpUrlLinkAttribute
    rdpServerAttribute
```

In the previous example, rdpServerAttribute corresponds to the RDP server details for a given user on the LDAP server.

Note: To fetch the LDAP attribute details from the LDAP server, the LDAP action must be configured with the same string that is configured with `pUrlLinkAttribute` as follows.

```
add authentication ldapAction dnpg_ldap -serverIP <IP address>-ldapBase
     <"domain name"> -ldapBindDn <username> -ldapLoginName
    sAMAccountName -ldapbindDnpassword <password>

add authentication ldapAction dnpg_ldap -serverIP 10.102.39.101 -
    ldapBase "dc=dnpg-blr,dc=com" -ldapBindDn sqladmin@dnpg-blr.com -
    ldapLoginName sAMAccountName -ldapbindDnpassword xxxx

add authentication ldapPolicy dnpg_ldap_pol ns_true dnpg_ldap

bind vpn vs vserver<name> -pol dnpg_ldap_pol

set ldapaction dnpg_ldap -attributes "rdpServerAttribute"

set rdpclientprofile ldap -rdpLinkAttribute rdpServerAttribute
```

LDAP server configuration

On the LDAP server, perform the following steps:

1. Navigate to a particular **User**.
2. In **AD users and computers**, click **View**, and click **Detail.**
3. Right-click **user name** and click **Attribute Editor.**
4. Change the required attribute (displayName) value and click **OK.**

To populate RDP URLs based on the LDAP attribute by using the GUI

1. Navigate to **NetScaler Gateway > Policies > RDP**.
2. On the **RDP Profiles and Connections** page, click the **Client Profiles** tab and select the client profile where you want to configure the RDP link attribute.

3. In the **Configure RDP Client Profile** page, in **RDP Link Attribute**, enter the LDAP attribute name.

   Note: The LDAP attribute value can be a comma separated list.

Randomize RDP file name with RDP proxy

January 8, 2024

When you click an RDP URL, an RDP file is downloaded. Upon clicking the **RDP URL** again a new RDP file with the same name is downloaded, resulting in a pop-up for the replacement of the new file with the existing file. To avoid this, the administrator can opt for randomizing the RDP file name. The file name is now randomized by appending the output of the time () function in the format <rdpFileName>_<outputof time()>.rdp. By doing this, the appliance generates a unique RDP file name every time you download a file.

Configure support for randomizing RDP file name with RDP proxy

To configure support for randomizing RDP file name with RDP proxy by using the command line interface at the command prompt, type:

```
add rdpclientprofile <profileName> -rdpfileName <filename> -randomizeRDPFilename <YES/NO>

add rdpclientprofile clientProfileName -rdpfileName testRDP -randomizeRDPFilename YES
```

To configure support for randomizing RDP file name with RDP proxy by using the NetScaler GUI:

1. Navigate to **NetScaler Gateway** > **Policies** > **RDP**.
2. On the **RDP Profiles and Connections** page, click **Client Profiles** tab and select the client profile where you want to configure randomizing RDP file name functionality.
3. On the **Configure RDP Client Profile** page, select **YES** in the menu next to the **Randomized RDP Filename** field.

Configure the name for RDP files

January 8, 2024

Upon downloading an RDP file, it can be stored locally with the configured file name.

Configure a name for RDP files

To configure a name for RDP files using the CLI, at the command prompt, type**:

```
set rdpclientprofile <Name> -rdpfilename <filename>.rdp
```

To configure a name for RDP files using the GUI:

1. Navigate to **NetScaler Gateway** > **Policies** > **RDP**.
2. On the **RDP Profiles and Connections** page, click **Client Profiles** tab. Select the client profile where you want to configure a randomizing RDP file name functionality.
3. On the **Configure RDP Client Profile** page, enter a name for the RDP profile in the **RDP File Name** field. The name of the file must be in the following format, . A maximum of 31 characters are allowed for the name.

Outbound ICA Proxy support

January 8, 2024

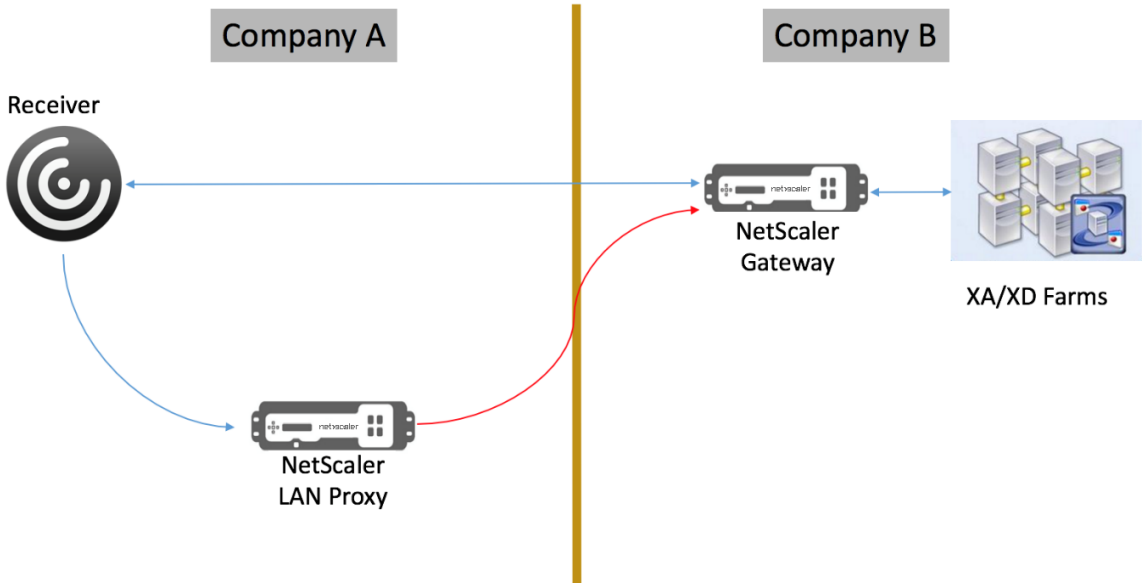
Outbound ICA Proxy support for NetScaler Gateway enables the network administrators to avail SmartControl functionalities even when Receiver and NetScaler Gateway are deployed in different organizations.

The following scenario illustrates the use of the Outbound ICA Proxy solution:

A network administrator requires control over the ICA session related capabilities when Receiver and NetScaler Gateway are deployed in different organizations.

Understanding the Outbound ICA Proxy support

To bring the SmartControl functionality to the enterprise organization, company A, which has the receiver, we need to add a NetScaler appliance which acts as a LAN Proxy. The NetScaler LAN Proxy enforces SmartControl and proxies the traffic to the NetScaler Gateway of Company B. In this deployment scenario, the Receiver forwards the traffic to the NetScaler LAN Proxy which allows the network administrator of Company A to enforce SmartControl. The deployment is depicted in the following figure.



In this scenario, the traffic between the LAN Proxy and the NetScaler Gateway is over SSL.

> **Note:** Do not enable client certificate based authentication on the NetScaler Gateway.

SSL support on NetScaler LAN proxy

From release 13.0 build xx.xx, traffic between Citrix Workspace app and NetScaler LAN proxy is supported over SSL as well. The Citrix Workspace app encrypts the traffic it sends to LAN Proxy over SSL. SSL support on LAN proxy can co-exist with the existing deployment.

To enable traffic encryption over SSL between Citrix Workspace app and NetScaler LAN proxy, you must perform the following on the NetScaler LAN proxy:

- Disable authentication and enable double-hop on the VPN virtual server.
- Set the host on the Windows client to the IP address of the VPN virtual server.
- Enable SNI and certificate validation.
- Add appropriate CA certificates and enable them globally.

Configuring outbound ICA Proxy

February 20, 2024

Outbound ICA Proxy configuration involves configuring the NetScaler LAN proxy and NetScaler Gateway.

Configure NetScaler LAN Proxy for ICA outbound proxy

You can perform the following steps to configure outbound ICA Proxy by using the CLI.

- Add a VPN virtual server.

```
add vpn vserver <name> <serviceType> [<IPAddress> [-range <
    positive_integer>] [-ipset <string>]] [<port>] [-state (
    ENABLED | DISABLED )] [-authentication ( ON | OFF )] [-
    doubleHop ( ENABLED |DISABLED )]
```

- Set the VPN parameters.

```
set vpn parameter[-backendServerSni ( ENABLED | DISABLED )][-
    backendCertValidation ( ENABLED | DISABLED )]
```

- Add an SSL certificate-key pair.

```
add ssl certKey ca_cert_verify -cert <certificate name>
```

- Bind the SSL certificate-key pair globally.

```
bind vpn global -cacert ca_cert_verify
```

Example:

```
- add vpn vserver ssl_lan_proxy SSL 65.219.17.34 443 -authentication
  OFF - doubleHop ENABLED

- set vpn parameter backendserverSni ENABLED backendcertValidation
  ENABLED

- add ssl certKey dnpg_ca -cert dnpg_ca_cert.cer

- bind vpn global -cacert dnpg_ca
```

> **Note:**
>
> For SSL support on NetScaler LAN proxy, no changes are required in the NetScaler Gateway configuration.

NetScaler Gateway Enabled PCoIP Proxy Support for VMware Horizon View

January 8, 2024

NetScaler Gateway 12.0 supports the PC-over-IP (PCoIP) protocol, which is the remote display protocol for several non-Citrix VDI solutions, including VMware Horizon View. PCoIP is analogous to Citrix HDX/ICA protocol and Microsoft RDP protocol. PCoIP uses UDP port 4172.

When PCoIP is proxied through NetScaler Gateway, NetScaler Gateway can replace the traditional PCoIP remote access solutions, like View Security Server, or VMware Access Point.

The following scenarios illustrate the use of NetScaler Gateway enabled VMWare Horizon View Solution.

- VMware Horizon PCoIP users needing to remotely access VMware Horizon View desktop pools and application pools through the NetScaler Gateway without deploying a Horizon View Security Server or VMware Access Point.
- PCoIP users remotely accessing other PCoIP-based virtual desktop solutions through NetScaler Gateway.

> **Note**
>
> NetScaler Gateway is deployed as a remote access solution.

Configure NetScaler Gateway enabled PCoIP proxy for VMware Horizon View

January 8, 2024

Prerequisites

Version - NetScaler 12.0 or above

Universal License - PCoIP Proxy uses the Clientless Access feature of NetScaler Gateway, which means every NetScaler Gateway connection must be licensed for NetScaler Gateway Universal. On the NetScaler Gateway virtual server, ensure **ICA Only** is cleared.

Horizon View infrastructure - A functional internal Horizon View infrastructure. Ensure you are able to connect to Horizon View Agents internally without NetScaler Gateway. Ensure that the Horizon View **HTTP(S) Secure Tunnel** and **PCoIP Secure Gateway** are not enabled on the View Connection Servers that NetScaler will proxy connections to.
Following versions of VMware Horizon view are supported.

- Connection Server: 7.0.1 and above
- Horizon Client: 4.2.0 and above (Windows and Mac)

Firewall Ports:

Ensure the following:

- UDP 4172 and TCP 443 must be open from Horizon View Clients to the NetScaler Gateway VIP.
- UDP 4172 must be open from the NetScaler SNIP to all internal Horizon View Agents.
- PCoIP Proxy is supported on NetScaler deployed behind NAT. Following are the important points to consider:
  - Support is based on VPN virtual server FQDN parameter setting
  - Supports only publicly accessible FQDN and not IP
  - Supports only 443 and 4172 ports
  - Must be a static NAT

Certificate –A valid certificate for the NetScaler Gateway virtual server.

Authentication –An LDAP authentication policy/server using advanced syntax.

Unified Gateway (optional) –If Unified Gateway, create the Unified Gateway before adding PCoIP functionality.

RfWebUI Portal Theme –For web browser access to Horizon View, the NetScaler Gateway virtual server must be configured with the RfWebUI theme.

Horizon View Client –The Horizon View Client must be installed on the client device, even if accessing Horizon published icons using the NetScaler RfWebUI portal.

To configure NetScaler Gateway to support PCoIP proxy for VMWare Horizon View:

1. Navigate to **Configuration > NetScaler Gateway Policies > PCoIP**.
2. Create a virtual server profile and a PCoIP profile on the **PCoIP Profiles and Connections** page.
   a) To create a virtual server profile, on the **VServer Profiles** tab, click **Add**.
   b) Enter a name for the virtual server profile.
   c) Enter an Active Directory Domain Name that is used for single sign-on to View Connection Server, and then click **Create.**
      Note: Only a single Active Directory domain is supported per NetScaler Gateway virtual server. Also, the domain name specified here is displayed in the Horizon View Client.
   d) Click **Login**.
   e) To create a PCoIP profile, on the **Profiles** tab, click **Add**.
      i. Enter a name for the PCoIP profile.
      ii. Enter the connection URL for the internal VMware Horizon View Connection Server, and then click **Create**.

f) Navigate to **Configuration > NetScaler Gateway > Policies > Session**.

g) On the right, select the **Session Profiles** tab.

h) On the **NetScaler Gateway Session Policies and Profiles** page, create or edit a NetScaler Gateway session profile.

   i. To create a NetScaler Gateway session profile, click **Add**, and provide a name.

   ii. To edit a NetScaler Gateway session profile, select the profile, and click **Edit**.

i) On the **Client Experience** tab, ensure that the **Clientless Access** value is set to **On**.

j) On the **Security** tab, ensure that the **Default Authorization Action** value is set to **ALLOW**.

k) On the **PCoIP** tab, select the required PCoIP profile, and then click **Create**. You can also create or edit PCoIP Profiles from this tab.

l) Click **Create** or **OK** to finish creating or editing the Session Profile.

m) If you have created a session profile, then you must also create a corresponding session policy.

   i. Navigate to **Configuration > NetScaler Gateway > Policies > Session**.

   ii. select the **Session Policies** tab and then click **Add**.

   iii. In the Create NetScaler Gateway Session Policy page, enter a name for the policy.

   iv. In **Profile**, select an existing profile or click **Add** and create a profile.

   v. Add an expression.

      A. Click **Advanced Policy** and then click **Expression Editor**.
      B. In **Expression**, select the expression as per your requirement.

   vi. Click **OK.**

n) Bind the created PCoIP virtual server profile and session policy to a NetScaler Gateway virtual server.

   i. Go to **NetScaler Gateway > Virtual Servers**.

   ii. On the right, either **Add** a new NetScaler Gateway virtual server, or **Edit** an existing NetScaler Gateway virtual server.

   iii. If you are editing an existing NetScaler Gateway virtual server, in the **Basic Settings** section, click the pencil icon.

   iv. For both adding and editing, in the **Basic Settings** section, click **More**.

   v. Use the **PCoIP VServer Profile** menu to select the required PCoIP virtual server Profile.

vi. Scroll down and ensure that ICA Only is cleared. Then click **OK** to close the **Basic Settings** section.

vii. If you are creating a NetScaler Gateway virtual server, bind a **certificate**, and bind an LDAP authentication policy.

viii. Scroll down to the **Policies** section and click the plus icon.

ix. The **Choose Type** page defaults to **Session** and **Request**. Click **Continue**.

x. In the **Policy Binding** section, click **Click to select**.

xi. Select the required Session Policy that has the PCoIP Profile configured, and click **Select**.

xii. In the **Policy Binding** page, click **Bind**.

xiii. If you want to use a web browser to connect to VMware Horizon View, under **Advanced Settings**, add the **Portal Themes** section. If you are only using the Horizon View Client to connect to NetScaler Gateway, then you don't must perform this step.

xiv. Use the **Portal Theme** menu to select **RfWebUI** and click **OK**.

xv. Horizon View published icons are added to the RfWebUI portal.

> **Note:** VMware uses two or more protocols when using any protocol other than RDP. This can cause the requests to be load balanced across two different back-end servers. You can resolve this issue by setting up a single persistency group across all protocols ensuring all connections remain on the same Citrix virtual server.

Steps to enable USB redirection

USB devices connected to the client machine can be accessed from the virtual desktops and apps. Following are the steps to enable USB redirection:

1. Log in to VMware Horizon Administrator Console.
2. Navigate to **Inventory > View Configuration Servers**.
3. Select the **Connection Servers** tab.
4. Select a listed Connection Server and Click **Edit**.
5. Under the **General** tab, select **Use Secure Tunnel connection to machine** option under **HTTP(S) Secure Tunnel**. Provide NetScaler Gateway external URL in the **External URL** field.

Update content switching expression for Unified Gateway

If your NetScaler Gateway virtual server is behind a Unified Gateway (Content Switching Virtual Server), then you must update the Content Switching Expression to include the PCoIP URL paths.

1. In the NetScaler GUI, navigate to **Configuration > Traffic Management > Content Switching > Policies**.
2. Append the following expression under the **Expression** area, and then click **OK**.

http.req.url.path.eq("/broker/xml")	http.req.url.path.contains("/broker/resources")	http.req.url.path.eq("/pcoip-client")

Use PCoIP gateway

1. To connect, you must have the Horizon View Client installed on the client device. Once installed, you can either use the Horizon View Client's User Interface to connect to NetScaler Gateway, or you can use the NetScaler Gateway RfWebUI portal page to view the icons published from Horizon.
2. To view the active PCoIP connections, go to **NetScaler Gateway > PCoIP.**
3. On the right, switch to the **Connections** tab. The active sessions are displayed with the following data: user name, Horizon View Client IP, and Horizon View Agent Destination IP.
4. To terminate a connection, right-click the **Connection** tab, and click **Kill Connection**. Or click **Kill All Connections** to terminate all PCoIP connections.

Configuring VMware Horizon View Connection Server

January 8, 2024

To support PCoIP Proxy through NetScaler Gateway:

1. Login to **VMware Horizon Administrator Console**.
2. Navigate to I**nventory** –> **View Configuration** –> **Servers**.
3. Select **Connection Servers** tab.
4. Select a listed Connection Server and Click **Edit**.
5. Under **General** tab, deselect **Use Secure Tunnel connection** to machine option under HTTP(S) Secure Tunnel.
6. Click **OK** to close the **Edit Connection Server Settings** window.
7. Run through Steps from 4 to 6 on all listed Connection Servers.

Proxy Auto Configuration for Outbound Proxy support for NetScaler Gateway

January 8, 2024

When you configure the NetScaler Gateway appliance to support Proxy Auto Configuration (PAC), the URL of a PAC file is pushed to the client browser. The traffic from the client is then redirected to the respective proxies as determined by the conditions defined in the PAC file.

Following are some common use cases for PAC for outbound proxy:

- To configure multiple proxy servers that handle client traffic.
- To load-balance the proxy traffic across subnets.

Configure NetScaler Gateway global parameters to support PAC for outbound proxy by using the CLI

At the command prompt, type:

```
set vpn parameter -proxy BROWSER -autoProxyUrl <URL>
```

Configure NetScaler Gateway to support PAC in a session profile by using the CLI

At the command prompt, type:

```
add vpn sessionAction <name> -proxy BROWSER -autoProxyUrl <URL>
```

Where;

- **URL** –URL for the proxy server
- **Name** –Name of the VPN sessionAction

Configure NetScaler Gateway global parameters to support PAC for outbound proxy by using the GUI

1. Navigate to **Configuration > NetScaler Gateway > Global Settings**.
2. On the **Global Settings** page, click **Change Global Settings**, and then select the **Client Experience tab**.
3. On the **Client Experience** tab, select **Advanced Settings**, and then select the **Proxy tab**.
4. On the **Proxy tab**, select **Browser**, and then select **Use Automatic Configuration**.
5. In the **URL To Auto Proxy Config File** field, type the URL for the required PAC file.

6. Click **Create**.

Configure NetScaler Gateway to support PAC on Session Profile by using the GUI

1. Navigate to **Configuration> NetScaler Gateway> Policies> Session**.
2. On the NetScaler Gateway **Session Policies and Profiles** page, create a NetScaler Gateway Session Profile.
3. Select the **Session Profiles** tab, click **Add**, and enter a name.
4. On the **Client Experience** tab, select **Advanced Settings** and then select the **Proxy** tab.
5. On the **Proxy** tab, select **Browser**, and then select **Use Automatic Configuration**.
6. In the **URL To Auto Proxy Config File** field, type the URL for the required PAC file.
7. Click **Create**.
8. Click **Create**.

Configuration support for SameSite cookie attribute

January 8, 2024

The `SameSite` attribute indicates the browser whether the cookie can be used for cross-site context or only for same-site context. If an application intends to be accessed in the cross-site context then it can do so only via the HTTPS connection. For details, see RFC6265.

Until Feb 2020, the `SameSite` attribute was not explicitly set in the NetScaler appliance. The browser took the default value (None). The non-setting of `SameSite` attribute did not impact the NetScaler Gateway and NetScaler AAA deployments.

With certain browsers upgrade, such as Google Chrome 80, there is a change in the default cross-domain behavior of cookies. The `SameSite` attribute can be set to one of the following values. Default value for Google Chrome is set to Lax. For certain version of other browsers, the default value for `SameSite` attribute might still be set to None.

- **None**: Indicates the browser to use the cookie in cross-site context only on secure connections.
- **Lax**: Indicates the browser to use the cookie for requests on the same-site context. In the cross-site context, only safe HTTP methods like GET request can use the cookie.
- **Strict**: Use the cookie only in the same site context.

If there is no `SameSite` attribute in the cookie, the Google Chrome assumes the functionality of `SameSite` = Lax.
As a result, for deployments within an iframe with cross-site context that require cookies to be inserted by the browser, Google Chrome does not share cross site cookies. As a result, the iframe within the website might not load.

Configure the `SameSite` cookie attribute

A new cookie attribute named `SameSite` is added to the VPN and NetScaler AAA virtual servers. This attribute can be set at the global level and at the virtual server level.

To configure `SameSite` attribute, you must perform the following:

1. Set the `SameSite` attribute for the virtual server
2. Bind cookies to the `patset` (if the browser drops cross-site cookies are dropped by the browser)

Setting the `SameSite` attribute by using the CLI

To set the `SameSite` attribute at the virtual server level, use the following commands.

```
set vpn vserver VP1 -SameSite  [ STRICT | LAX | None ]
set aaa vserver VP1 -SameSite  [ STRICT | LAX | None ]
```

To set the `SameSite` attribute at the global level, use the following commands.

```
set vpn param VP1 -SameSite  [ STRICT | LAX | None ]
set aaa param VP1 -SameSite  [ STRICT | LAX | None ]
```

Note: The virtual server level setting takes preference over the global level setting. Citrix recommends setting the `SameSite` cookie attribute at the virtual server level.

Binding cookies to the `patset` by using the CLI

If the browser drops cross-site cookies, you can bind that cookie string to the existing `ns_cookies_SameSite` `patset` so that the `SameSite` attribute is added to the cookie.

Example:

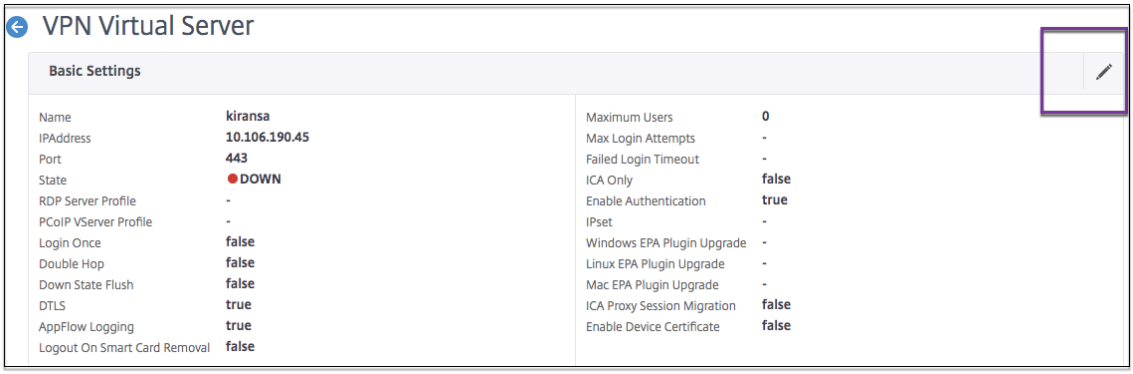
```
bind patset ns_cookies_SameSite "NSC_TASS"
bind patset ns_cookies_SameSite "NSC_TMAS"
```

Setting the SameSite attribute by using the GUI

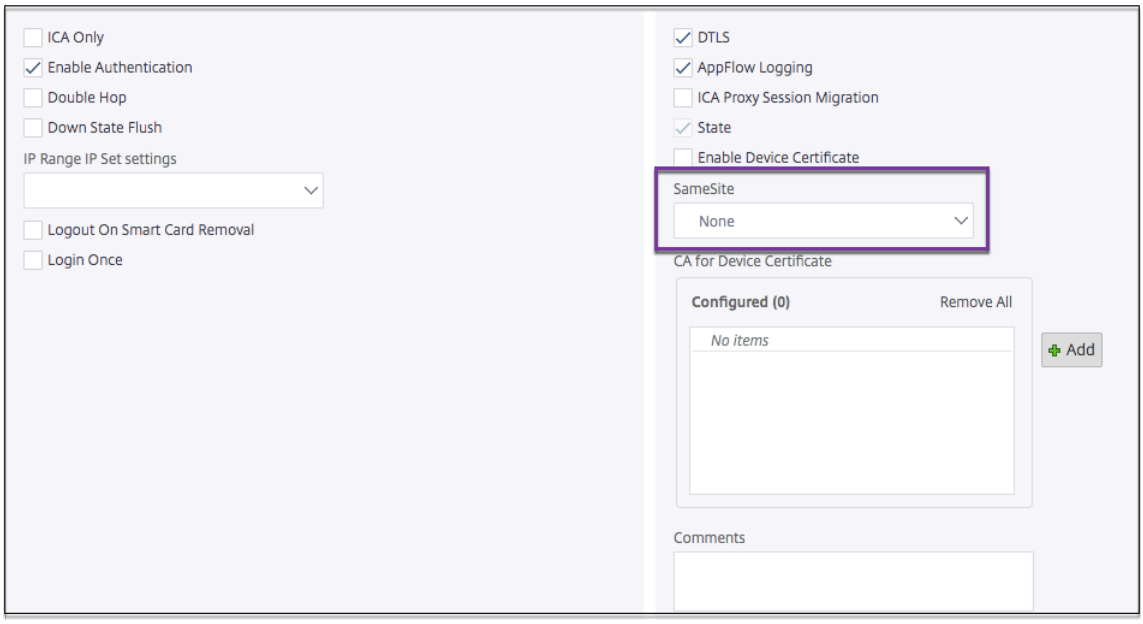
To set the `SameSite` attribute at the virtual server level:

1. Navigate to **NetScaler Gateway > Virtual Servers**.
2. Select a virtual server and click **Edit**.

3. Select the edit icon in the **Basic Settings** section and click **More**.

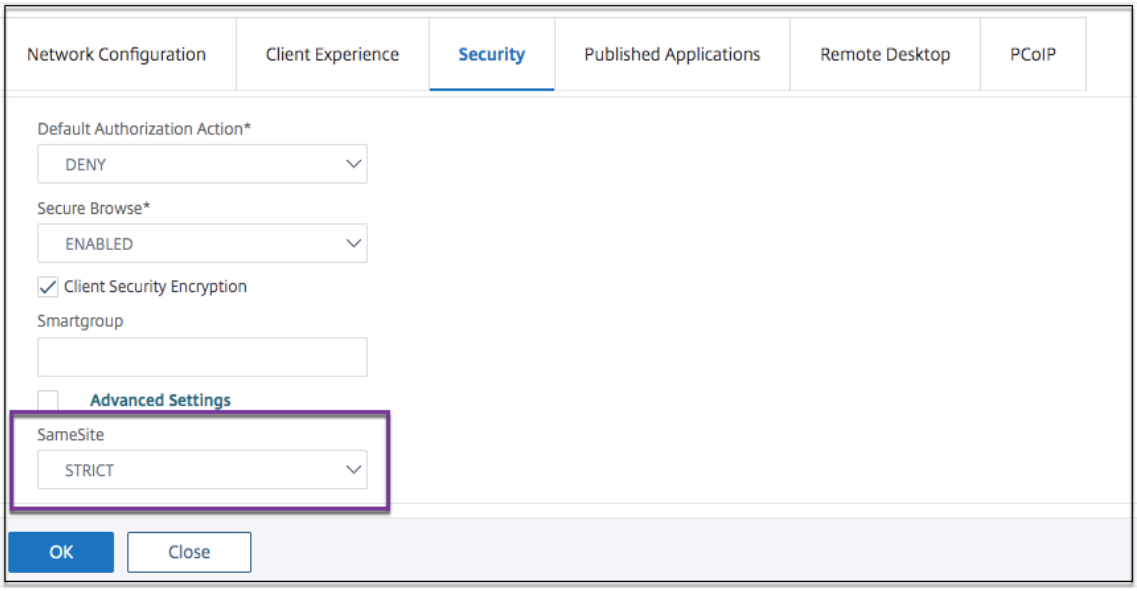


4. In **SameSite**, select the option as required.



To set the `SameSite` attribute at the global level:

1. Navigate to **NetScaler Gateway > Global Settings > Change Global Settings.**
2. Click the **Security** tab.
3. In `SameSite`, select the option as required.



RfWebUI Persona on Gateway UX Configuration

January 8, 2024

RfWebUI Persona is a theme that provides a new logon and portal page for NetScaler Gateway users logging on through NetScaler Gateway. The portal presents Receiver, StoreFront, and Citrix Endpoint Management users with the same GUI as when they access one of those products directly.

When to Use RfWebUI Persona

Use the RfWebUI persona in NetScaler Gateway when you need a single-pane view of all the applications provided by different NetScaler products, such as web and Software as a Service (SaaS) applications, virtual Windows applications, and desktops.

The following scenarios illustrate the use of RfWebUI Persona.

- A user accesses StoreFront using Gateway and finds a GUI different than the one they see upon accessing the product without Gateway.
  Solution: When the user accesses StoreFront using the Gateway, the RfWebUI theme provides a similar user interface as they see upon accessing the product without using the Gateway.
- A user accesses the Citrix Workspace app, StoreFront, and Citrix Endpoint Management applications using Gateway and struggles to locate the desired applications as the applications are not grouped in a logical fashion.

Solution: The RfWebUI persona provides a single pane view user experience by creating a logical bundling of applications provided by different products, such as Receiver, StoreFront, Citrix Endpoint Management and so on.

Functionalities Provided by RfWebUI Persona

The new RfWebUI provides the following features:

- GO
- Aggregation of applications
- User Configured Remote Desktop Protocol (RDP) proxy links
- Favorite applications

GO

GO: The Go feature provides access to webpages through clientless VPN. The user just types the URL in the **URL** section on the **Bookmark** tab and clicks **GO**.

Currently, the **GO** feature supports only Outlook Web Application (OWA) and SharePoint URLs.

> **Note**
> The **GO** tab is visible only if the `clientlessAccessVPNMode` parameter in the session policy is **Enabled**.

Aggregation of applications

Aggregation of applications: The RfWebUI theme provides a single-pane view by bundling the applications provided by different products under descriptive banners. For example, all the VPN URLs configured by a NetScaler administrator are in a bundle named **Web and SaaS Applications**, and user-specific web bookmarks are under **Personal Bookmarks**. If Citrix Virtual Apps and Desktops application bundles are configured in StoreFront, the single pane view in NetScaler Gateway lists these bundles as well.

User Configured RDP Proxy Links

Users can add an RDP Proxy link as personal bookmarks. The personal bookmarks appear under the **Desktops** tab.

The following RDP modes are supported:

- Single gateway
- Stateless (Dual) gateway

> **Note:** A user can add RDP Proxy Links only if an `RDPclientprofile` is configured. For more information on RDP configurations, see RDP Proxy documentation.

Favorite applications

Users can add the desired applications listed under **Web and SaaS Application** and under **Personal Bookmarks** to **FAVORITES** tab by clicking the **Add to Favorites** link present next to the application name. The applications once added can be seen under **FAVORITES** tab. The same can also be removed from the **FAVORITES** tab by clicking the **REMOVE** link present next to the application inside the **FAVORITES** tab.

Considerations While Enabling the RfWebUI Persona

The RfWebUI persona does not fully support the following:

Fileshare feature: The fileshare feature, for accessing SMB file shares, is not supported.
Email Home: The **Email Home** VPN parameter is not available as an embedded view for the NetScaler Gateway portal. It can be accessed as an application in the **Web and SaaS Apps** bundle under the **APPS** tab of RfWebUI.
Java Client: The browser based Java client for establishing an SSL tunnel is not available in this theme.

Configuring RfWebUI Persona

To apply the RfWebUI Persona:

1. In the NetScaler interface, navigate to **Configuration > NetScaler Gateway Portal Themes**.
2. On the **Portal Themes** page, select the **RfWebUI** check box.
3. Click the **Save** icon on the top right corner of the **Portal Themes** page.
4. In the **Save Confirmation** dialog box, click **Yes**.

RfWebUI configuration parameters

January 8, 2024

The overall behavior of the NetScaler Gateway portal is influenced by two configuration files: the local NetScaler Gateway configuration file and the StoreFront file.

Depending on your deployment, you can modify the NetScaler Gateway portal behavior by changing the properties in the "plugins.xml"file. This file appears as a configuration file on the browser which is the request for `/var/netscaler/logon/themes/<custom_theme>/plugins.xml`.

During logon, the NetScaler Gateway configuration files are used. But when connected to StoreFront, StoreFront sends a new configuration and the earlier configuration is overwritten. This behavior differs for clientless VPN and ICA.

For ICA, the StoreFront configuration always takes precedence but some of the behaviors in the clientless VPN that are influenced by the NetScaler Gateway configuration are retained even after the new configuration is updated from the StoreFront.

The following table lists the parameters describing the configuration that takes precedence over clientless VPN and ICA.

Config type	sub config type	Parameter	Clientless VPN	ICA	Description
Session for clientless VPN / AuthManager for ICA	-	loginFormTimeout	NetScaler Gateway	-	Defines the time in minutes for the logon page timeout
Plug-in assistant	-	enabled	StoreFront	StoreFront	Enable or disable the plug-in assistant
Plug-in assistant	-	upgradeAtLogin	StoreFront	StoreFront	Prompts for upgrade of the plug-in at login
Plug-in assistant	-	showAfterLogin	NetScaler Gateway	StoreFront	Displays the plug-in prompt after login
Plug-in assistant	-	showOnlyIfRequiredByApps	NetScaler Gateway	StoreFront	Displays the plug-in prompt after login, if required by the apps

Config type	sub config type	Parameter	Clientless VPN	ICA	Description
Plug-in assistant	macOS/win32	path	NetScaler Gateway	StoreFront	Defines the download path for the plug-ins
Plug-in assistant	protocolHandler	enabled	NetScaler Gateway	StoreFront	Toggle the protocol handler page before launching the plug-in
Plug-in assistant	protocolHandler	platforms	NetScaler Gateway	StoreFront	Identifies the supported platform for the plug-in
Plug-in assistant	-	skipDoubleHopCheck	• WhenDisabled • NetScaler Gate-way	StoreFront	Toggle the double hop NetScaler Gateway config check for ICA passthrough
User interface	-	frameOptions	NA	NA	-
User interface		autoLaunchDesktop	StoreFront	StoreFront	Enable or disable the desktop launch
User interface	workspaceControl	enabled	StoreFront	StoreFront	Enable or disable the workspace control
User interface	workspaceControl	autoReconnectAtLogon	StoreFront	StoreFront	Toggle to auto-reconnect the previous session if available

Config type	sub config type	Parameter	Clientless VPN	ICA	Description
User interface	workspaceControl	logoffAction	StoreFront	StoreFront	Defines the logoff behavior of Citrix Workspace
User interface	workspaceControl	showReconnectButton	StoreFront	StoreFront	Display or hide the **Reconnect** Button
User interface	workspaceControl	showDisconnectButton	StoreFront	StoreFront	Display or hide the **Disconnect** Button
User interface	workspaceControl	showDesktopsView	StoreFront	StoreFront	Display or hide the Desktops view
User interface	workspaceControl	showAppsView	StoreFront	StoreFront	Display or hide the Apps view
User interface	workspaceControl	defaultView	StoreFront	StoreFront	Select either the Desktop view or the App view
User interface	receiverConfiguration	enabled	StoreFront	StoreFront	Toggle the receiver configuration
User interface	receiverConfiguration	showOnlyIfRequiredByApps	NetScaler Gateway	NetScaler Gateway	Display the receiver prompt if required by the apps
User interface	receiverConfiguration	downloadURL	StoreFront	StoreFront	Download the URL for the receiver

Config type	sub config type	Parameter	Clientless VPN	ICA	Description
User interface	appShortcuts	enabled	StoreFront	StoreFront	Enable or disable the app shortcut tab
User interface	appShortcuts	allowSessionReconnect	StoreFront	StoreFront	Allow session reconnect

Gateway portal customization using custom plug-ins

May 10, 2024

NetScaler Gateway RfWebUi framework provides the ability to add the custom plug-ins to customize their gateway portal. These custom plug-ins can be used to add large functionality to the gateway, such as if you want to add an entire new page in the gateway flow. For other use cases the code can be added to the custom script file provided for gateway themes at the location `/var/netscaler/logon/themes/<custom_theme>/script.js`.

> **Note:**
>
> NetScaler Gateway only supports the creation and usage custom plug-ins for the portal customization. NetScaler Gateway does not create or provide any custom plug-ins based on customer requirements.

1. To add a custom plug-in, create the JavaScript file at the location `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/`. For example, you can find the following plug-ins in `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/`.

   - ns-nfactor.js
   - nsg-epa.js
   - nsg-setclient.js

   It is recommended to enter the plug-in name in the format `<plugin_name>`.js.

   All these plug-in files are fetched by the RfWebUI framework required by the functionality.

2. After creating the plug-in file, use the following code as an example to register the plug-in with the RfWebUI framework.


```
        (function ($) {

                    CTXS.ExtensionAPI.addPlugin( {

                                Name : " plugin name " ,
                                initialize: function() {
  }

                     }
 );
              }
 )(jQuery);
```

where,

name is the name given to the plug-in. It is used as the identifier to the plug-in.

initialize takes the function as the parameter which is used to initialize the plug-in.

3. Enter the plug-in name and initialization function in the `CTXS.ExtensionAPI.addPlugin()` function to register the plug-in.
   The added plug-in name and location must be registered to the plugins.xml file at the location `/var/netscaler/logon/themes/<custom_theme>/plugins.xml`.
4. After writing the plug-in code, the newly added plug-in name and location must be registered with the `plugins.xml` file at the location `/var/netscaler/logon/themes/<custom_theme>/plugins.xml`. The plug-in must be registered with the `plug-in` tag.

```
<plugins>
<plugin name="nsg-epa" src="plugins/ns-gateway/nsg-epa.js"/>
<plugin name="nsg-setclient" src="plugins/ns-gateway/nsg-setclient
    .js"/>
<plugin name="ns-nfactorn" src="plugins/ns-gateway/ns-nfactor.js"
    />
</plugins>
```

5. Enter a name and src for the plug-in so that RFWebUI can identify and fetch the plug-in.

Example configuration

The following example configurations can be used to add a custom plug-in to add a footer to the NetScaler Gateway logon page.

1. Create the JavaScript plug-in file in the location, `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/`.
2. Name the plug-in as ns-footer.js
   `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/ns-footer.js`

3. Add the following code to the registered plug-in to the RfWebUI and in the initialization function add the footer to the gateway.

```
(function ($) {

CTXS.ExtensionAPI.addPlugin({

    name: "ns-footer", // Name of plugin - must match name sent in configuration
    initialize: function () {

        CTXS.Extensions.beforeLogon = function (callback) {

            $("#customExplicitAuthBottom").append("<div style='text-align:center;color:white;font-size:15px;'><br>Disclaimer<BR><BR>"+
                " Access to this website is restricted to employees of Login Consultants<BR></div>");
            callback();
         }
 ;
     }

 }
 );
 }
 )(jQuery);
```

4. Save the file.

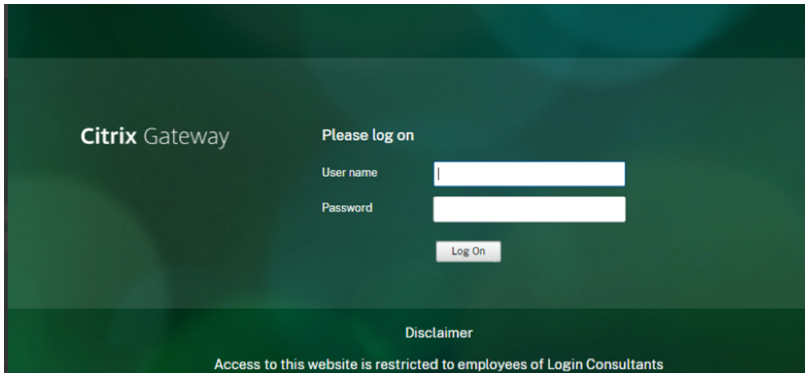
5. Add the name and src in the plugins.xml at the location `var/netscaler/logon/themes/<custom_theme>/plugins.xml`.

```
<plugins>
<plugin name="nsg-epa" src="plugins/ns-gateway/nsg-epa.js" />
<plugin name="nsg-setclient" src="plugins/ns-gateway/nsg-setclient.js" />
<plugin name="ns-nfactor" src="plugins/ns-gateway/ns-nfactor.js" />
<plugin name="ns-footer" src="plugins/ns-gateway/ns-footer.js" />
</plugins>
```

6. Configure the custom theme for which the plug-in is added.

7. Flush the cache using the command `flush cache contentgroup loginstaticobjects`.

8. Reload the portal screen.
   The footer is added to the NetScaler Gateway login page.



Create and customize login schema

January 8, 2024

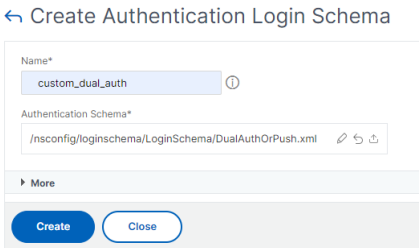
Login Schema is the XML file that provides the structure to the form-based authentication. Users can use a wide range of authentication forms using a set of user interface constructs that are similar to basic HTML forms.

In nFactor authentications, authentication factors are chained together. Each factor can have different login schema pages or files. In some authentication scenarios, users can be presented with multiple logon screens. You can also have one login schema gather the information that can be passed on to multiple factors so that the latter factors do not have to display another login schema.

The login schema XML files are included with the NetScaler appliance in `/nsconfig/loginschema/LoginSchema`.

Create a login schema profile

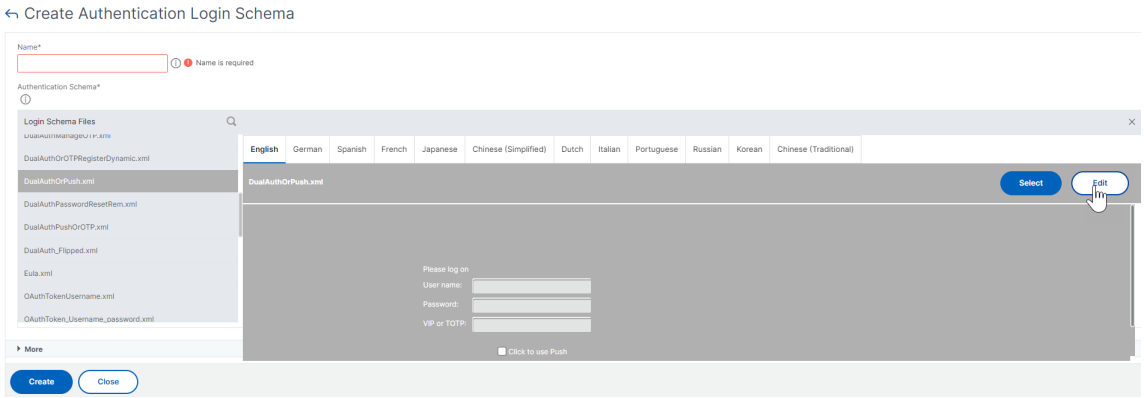
1. Navigate to **Security > AAA - Application Traffic > Login Schema**.
2. Click the **Profiles** tab, and then click **Add**.
3. In **Authentication Schema**, click the pencil icon.

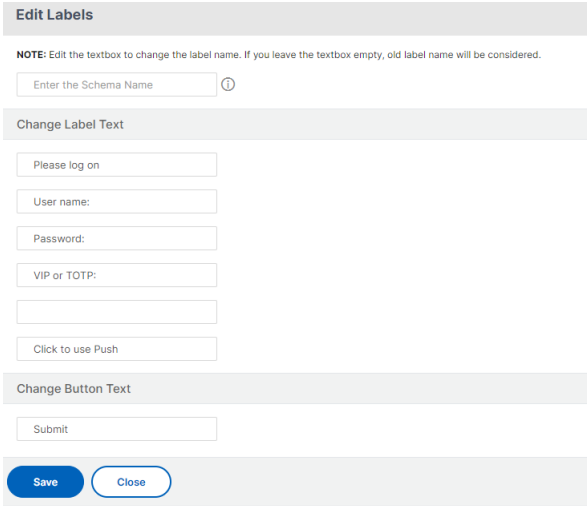


4. Click the **LoginSchema** folder to view the files in it.

5. Select one of the files and perform the changes as required.

   - Change the labels by clicking the Edit button on the top right.
   - Edit the scheme by selecting the language.



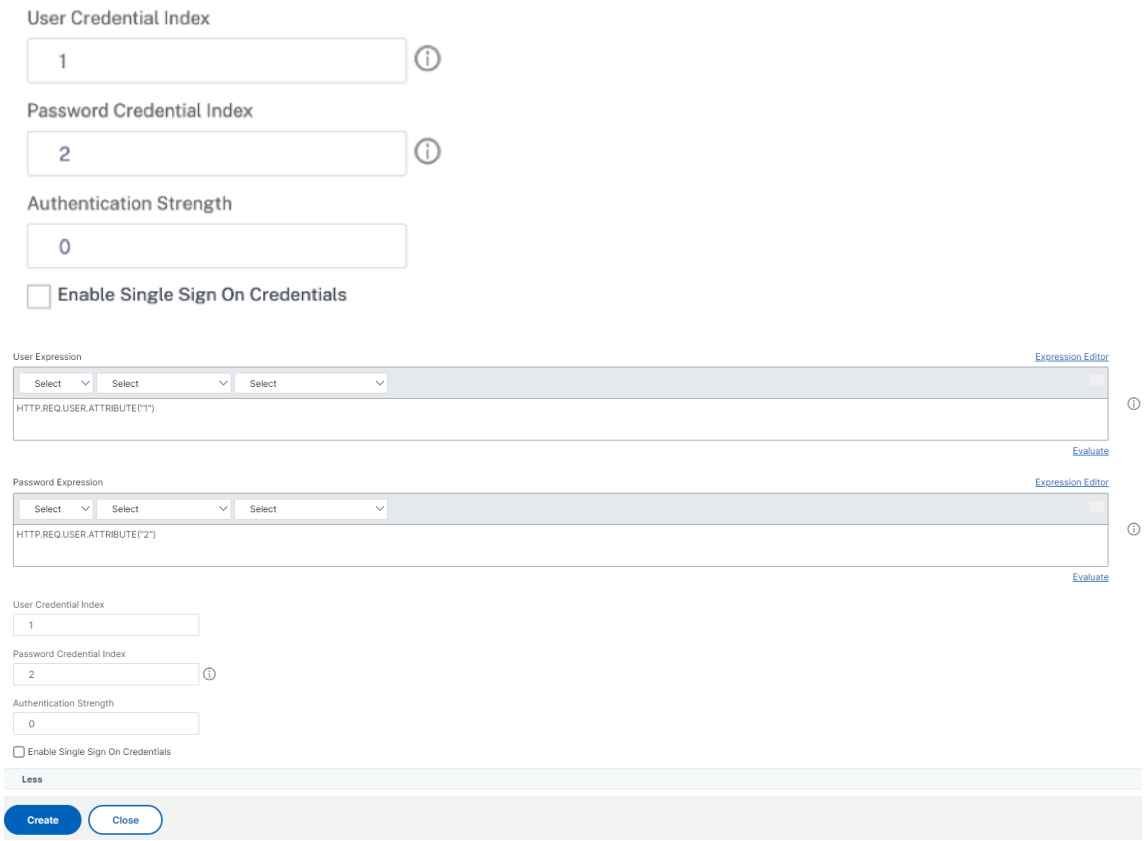


   Note: When you save the changes after modification, a new schema XML file is created with the changes.

6. On the top right, click **Select** to select the modified schema XML.

7. Enter a login schema name, and click **More**.

   Note: You can use the already entered credentials elsewhere. For example, you can use the user name and one of the passwords for single sign-on to StoreFront. You can click **More** and enter unique values for the indexes. These values can be between 1 and 16. You can reference these index values in a traffic policy or profile by using the expression REQ.USER.ATTRIBUTE(#).



8. Click **Create** to create the login schema profile.

Bind a login schema profile to an authentication, authorization, and auditing virtual server

To bind a login schema profile to an authentication, authorization, and auditing virtual server, you must first create a login schema policy. Login schema policies are not required when binding the login schema profile to an authentication policy label.

To create and bind a Login Schema Policy:

1. Navigate to **Security > AAA > Login Schema**.
2. Click the **Policies** tab, and then click **Add**.
3. In **Profile**, select the login schema profile created earlier.
4. In **Rule**, enter the default syntax expression and click **Create**.

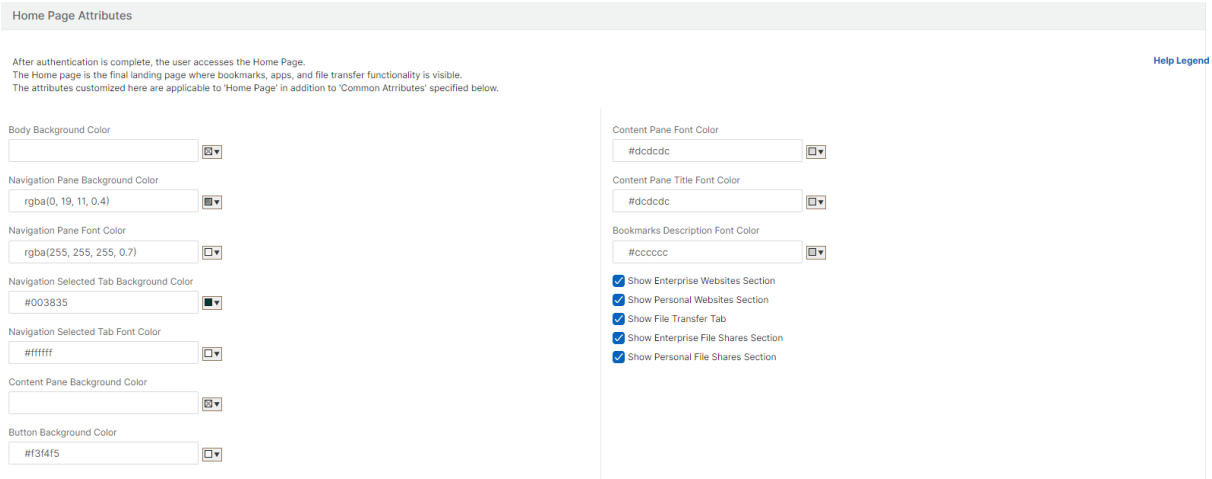
Portal customizations from the Admin UI

January 8, 2024

Admins can customize the portal themes by creating the custom themes to achieve the personalized look and feel of the user portal. Custom themes can be created based on the RfWebUI, Default, X1, and GreenBubble themes.

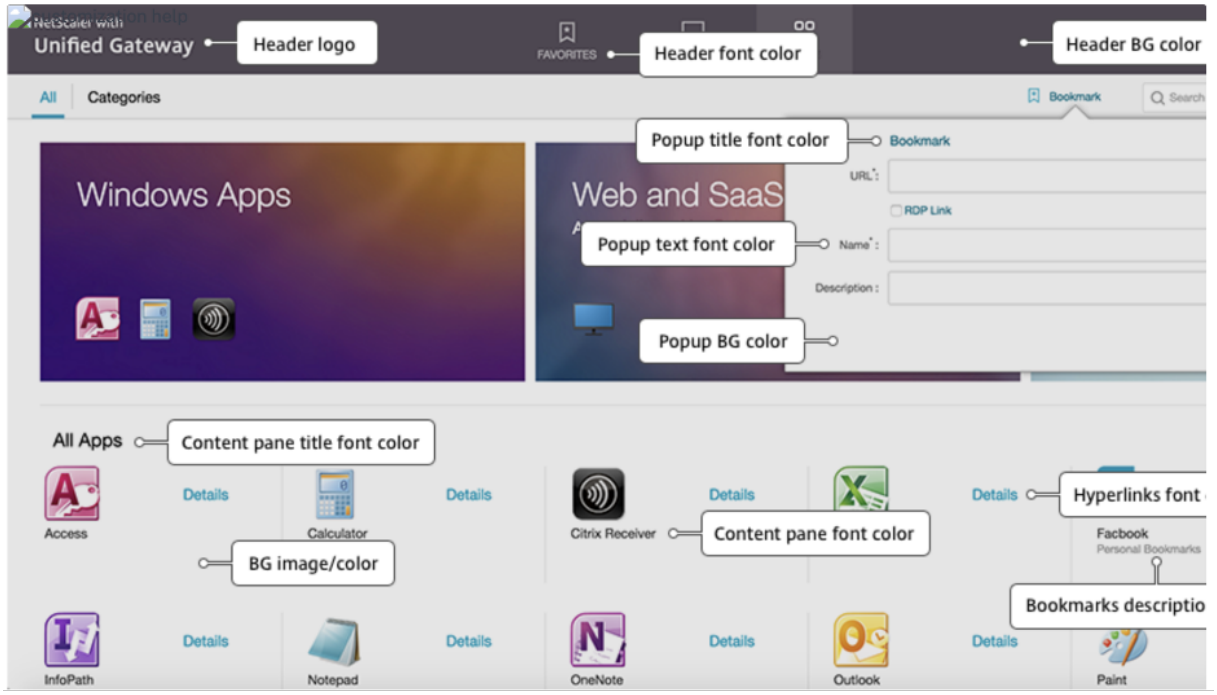
To create the custom themes:

1. In the Configuration tab, navigate to **NetScaler Gateway > Portal Themes** and click **Add**.
2. Enter a name for the custom theme name.
3. In **Template Theme**, select the base theme, as per your requirement. **RfWebUI** is selected by default.
4. Click **OK**.
5. In the **Look and Feel** section, modify the attributes as per your requirement for the home page and click **OK**.



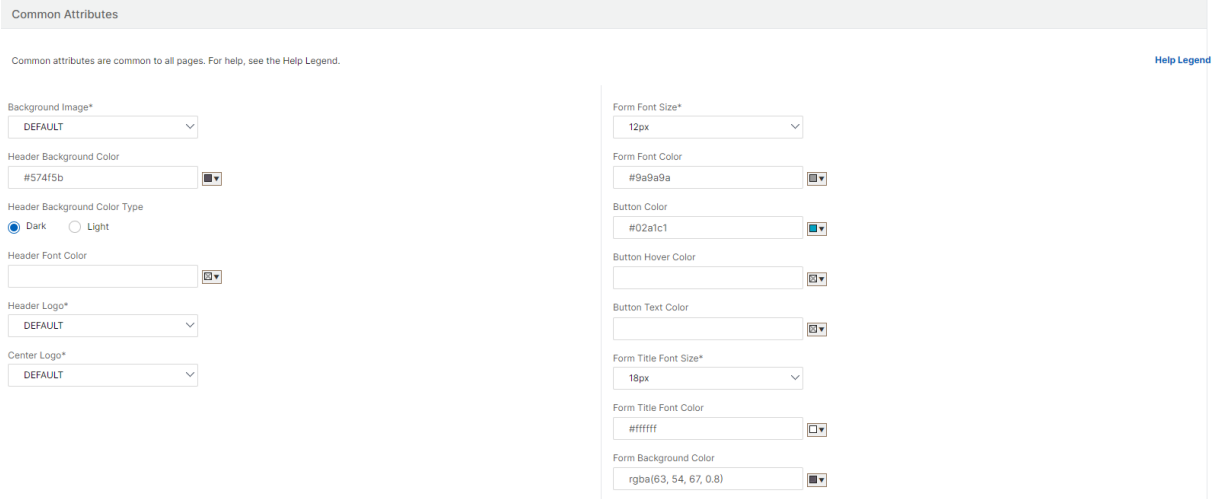
The following figure displays the RfWebUi based custom theme.

The **Help Legend** link displays the graphical page display with the section names to help you choose what you want to edit.

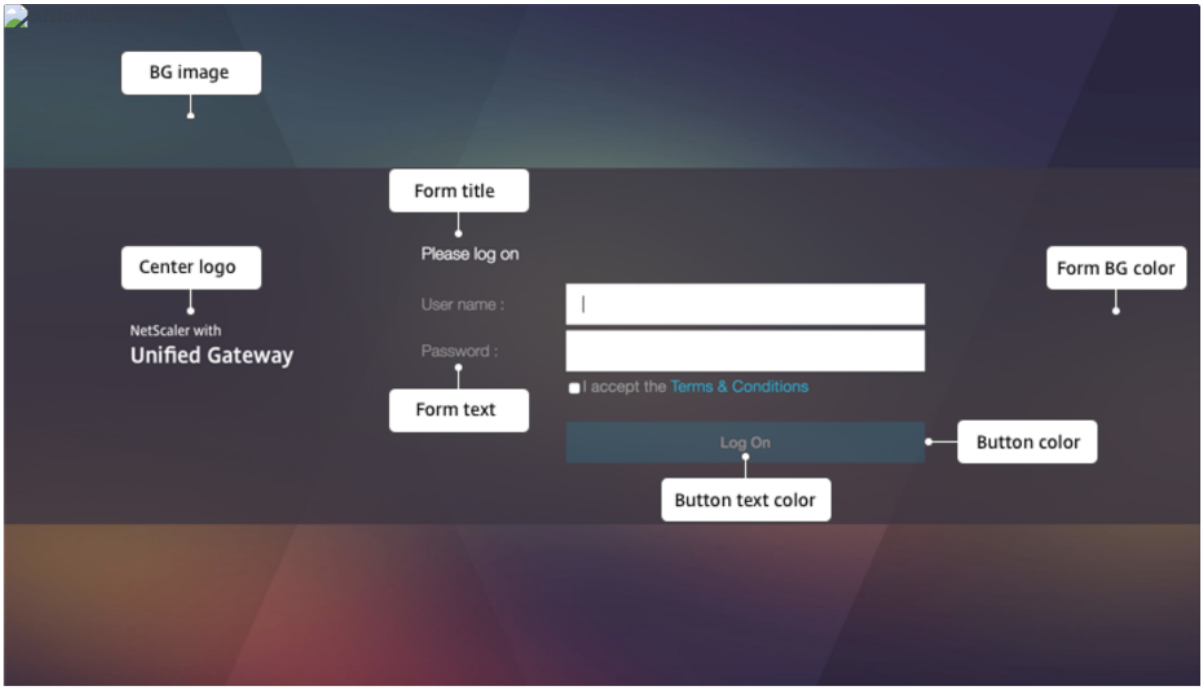


Common attributes

The **Common Attributes** section provides the configurable settings that are common to all NetScaler Gateway logon pages.

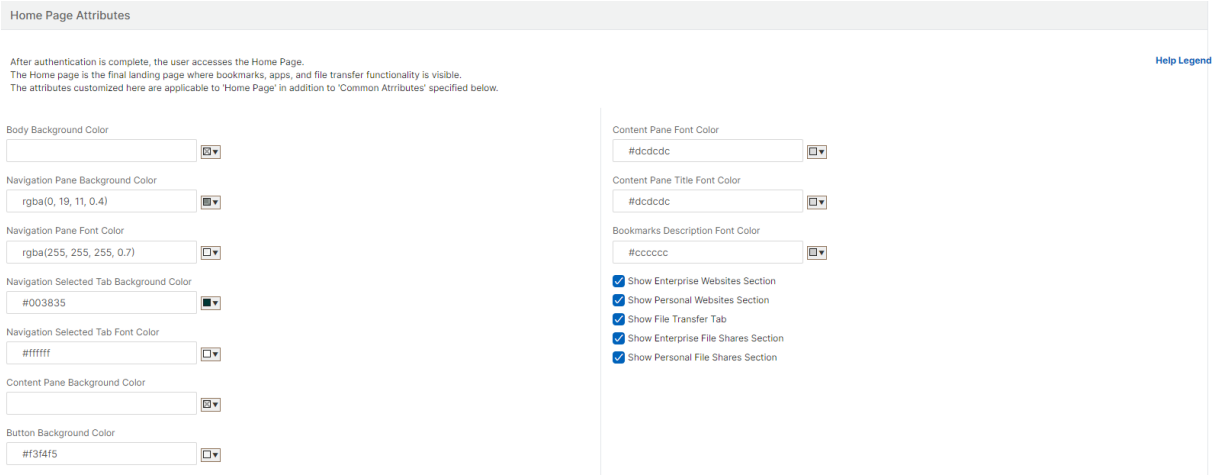


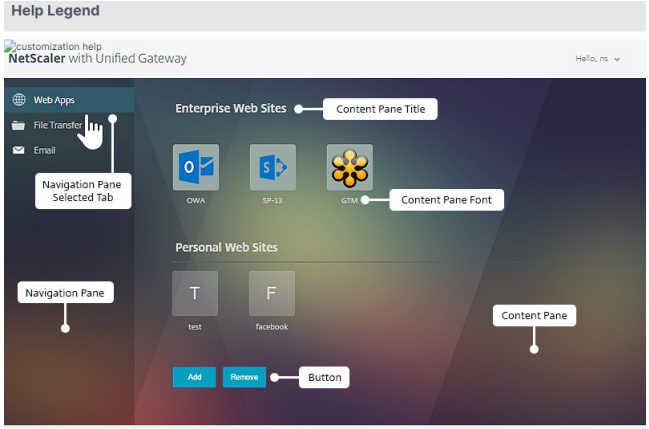
Click the **Help Legend** link to view each common configurable parameter.

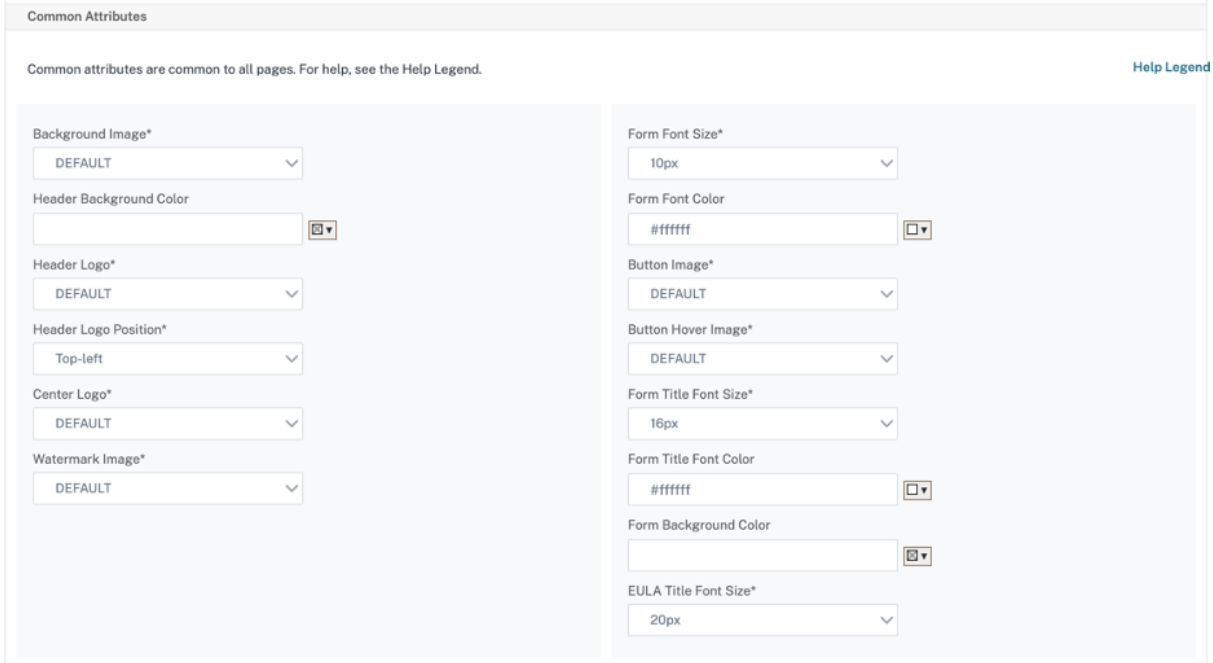


Similarly, for the custom theme based on **Default**, the following figure displays the available configuration for the home page.

Note: This configuration is different for the x1 and GreenBubble.





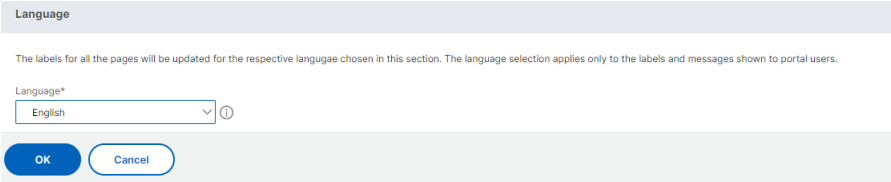


String customizations

In addition to the look and feel of the gateway portal home pages, the admin UI also enables string customization on all the pages.

Perform the following steps to customize the strings:

1. Select the language for which you want to edit the string. The strings are displayed in the selected language. English is selected by default.



   Note: The language that you select does not define the portal theme language. It is the language for which the strings are being customized.

2. On the right, in **Advanced Setting**, the pages that are available for string customization are listed.

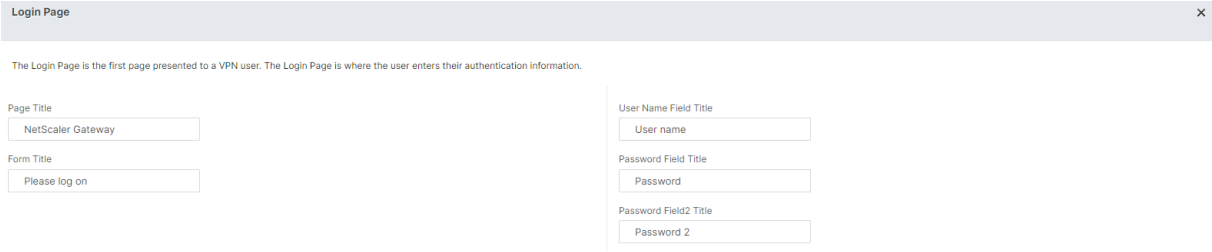
   - Login page
   - EPA page
   - EPA Error Page
   - Post-EPA Page
   - VPN Connection page
   - Home page

3. Select the page for which you want to customize the strings, and click the edit icon. A form with prefilled string customizations is displayed.
4. Select the field and add or edit the string as per your requirement.
5. Click **Done** to complete the custom portal theme creation. You can edit the themes later from **NetScaler Gateway > Portal Themes**.

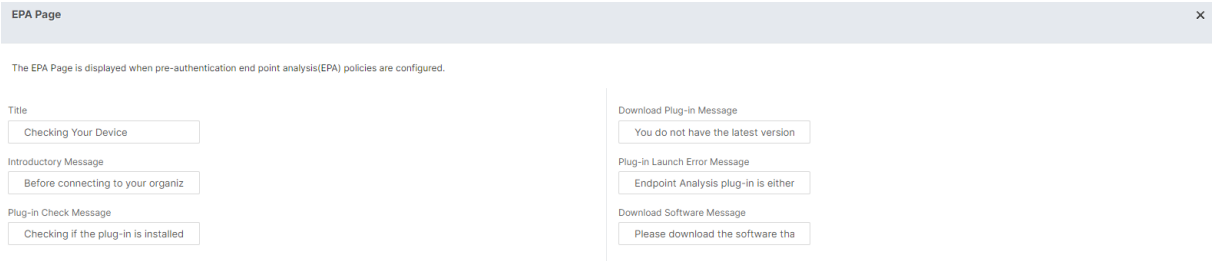
Note: If the section still displays the strings in the previously selected language, it might be that the section was already open when the language was changed. In this case, close the section, select the language, and again open the page from **Advanced Setting**.

The following screenshots display the available set of customizable strings for each page.

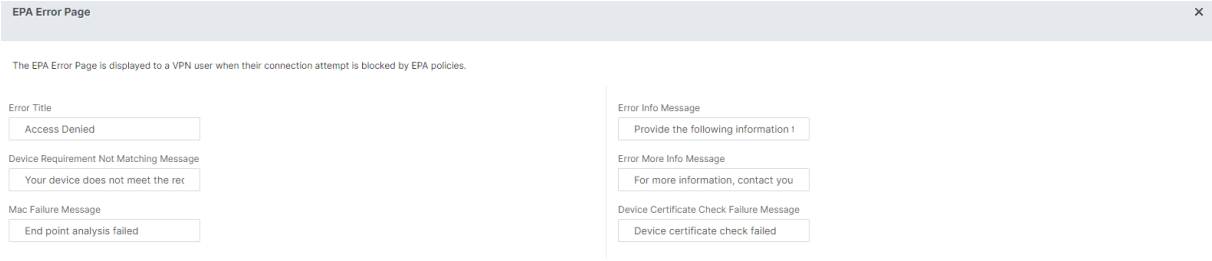
Login page:



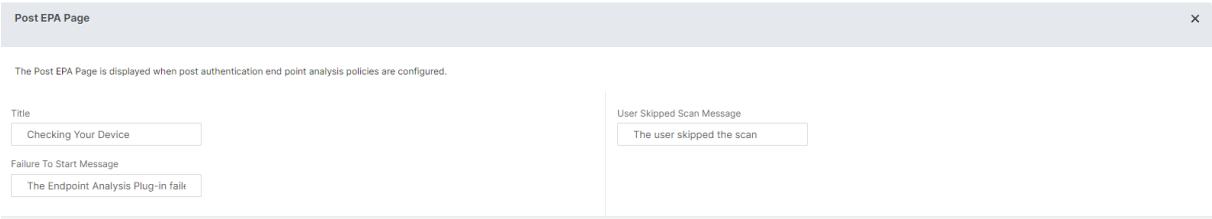
EPA page:



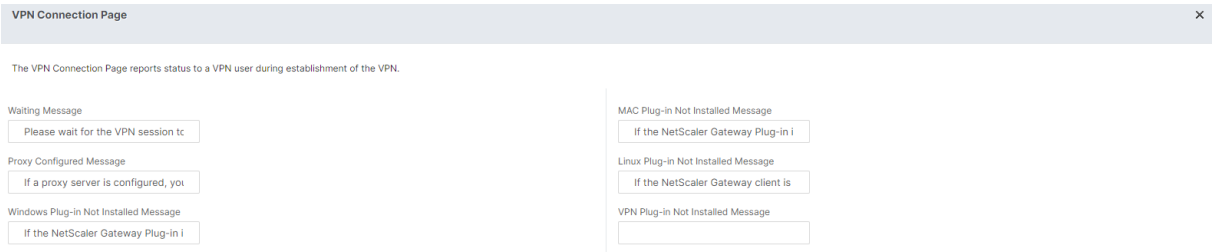
EPA Error page:



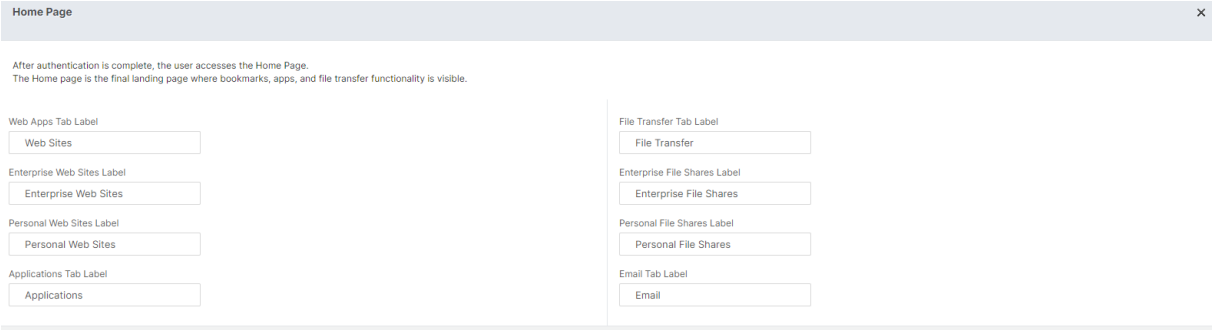
Post-EPA page:



VPN Connection page:



Home page:



Optimizing NetScaler Gateway VPN split tunnel for Office365

January 8, 2024

As organizations are adapting to the remote work options more rapidly than before, the remote access infrastructure must be optimized to facilitate seamless connectivity during increased traffic load conditions.

> **Important:**
>
> Microsoft recommends excluding traffic destined to key Office 365 services from the scope of VPN connection by configuring split tunneling using published IPv4 and IPv6 address ranges. For best performance and most efficient use of VPN capacity, traffic to the dedicated IP address ranges associated with the following applications must be routed directly, outside of the VPN tunnel:
>
> - Office 365 Exchange Online
> - SharePoint Online
> - Microsoft Teams (referred to as Optimize category in Microsoft documentation)
>
> Refer to Microsoft guidance for more detailed information about this recommendation.

Microsoft's recommendation in NetScaler Gateway is achieved by routing the Microsoft provided list of IP addresses directly to the internet for the O365 traffic by using the split tunnel reverse configuration.

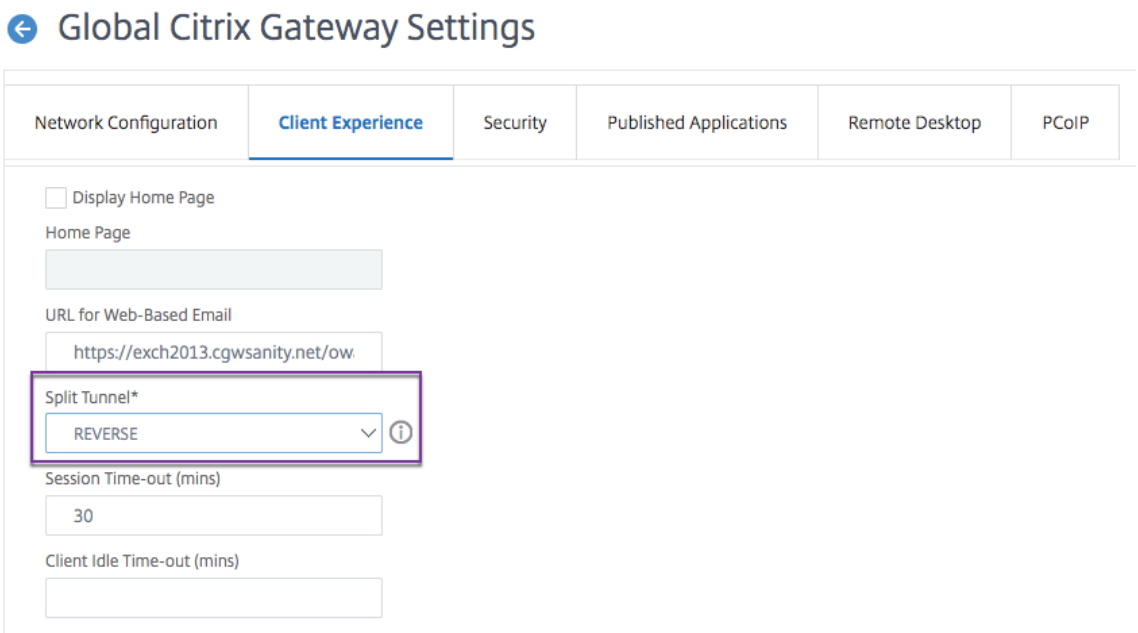
The configuration involves the following that can be performed manually by using the GUI or the CLI:

- Configure split tunnel for reverse configuration. For details, see Split tunneling options.
- Configure intranet applications for user access to resources.

Configuration by using the GUI

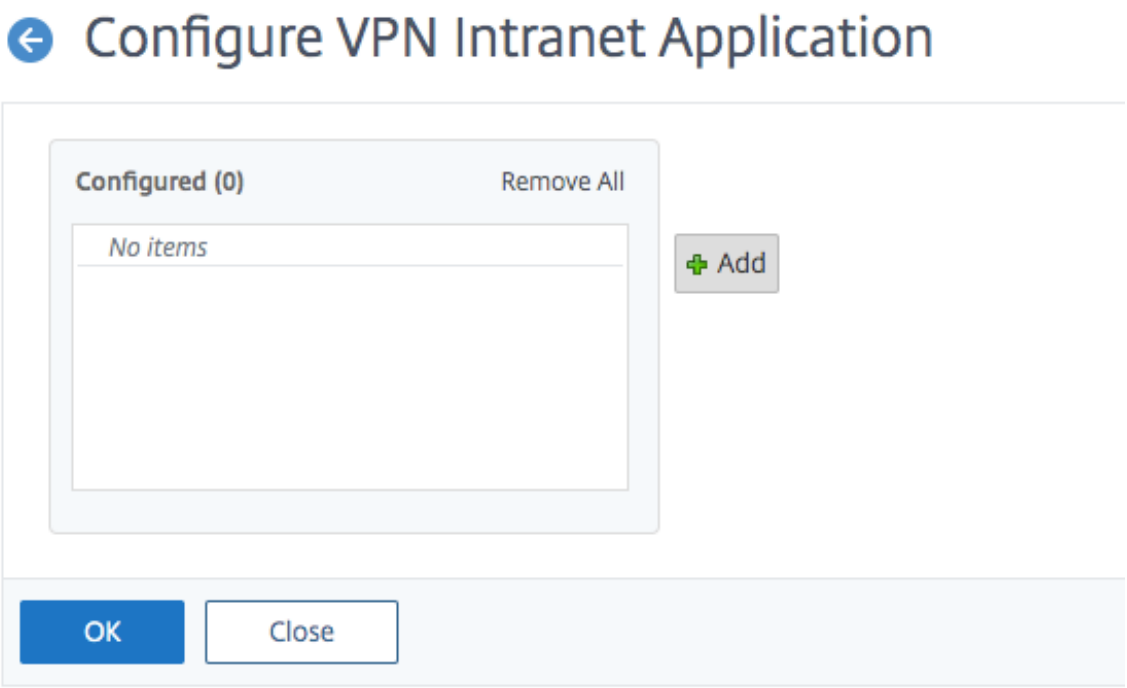
To configure split tunneling by using the GUI

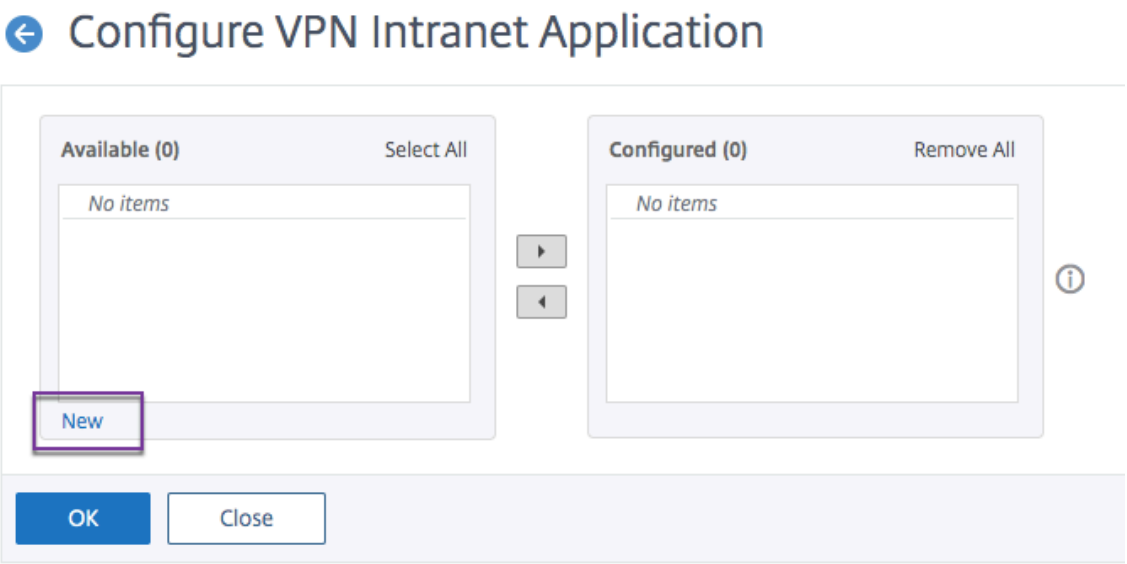
1. On the Configuration tab, Navigate to **NetScaler Gateway > Global Settings**.
2. In the details pane, under **Settings**, click **Change Global Settings**.
3. On the **Client Experience** tab, in **Split Tunnel**, select **Reverse**.
4. Click **OK**.



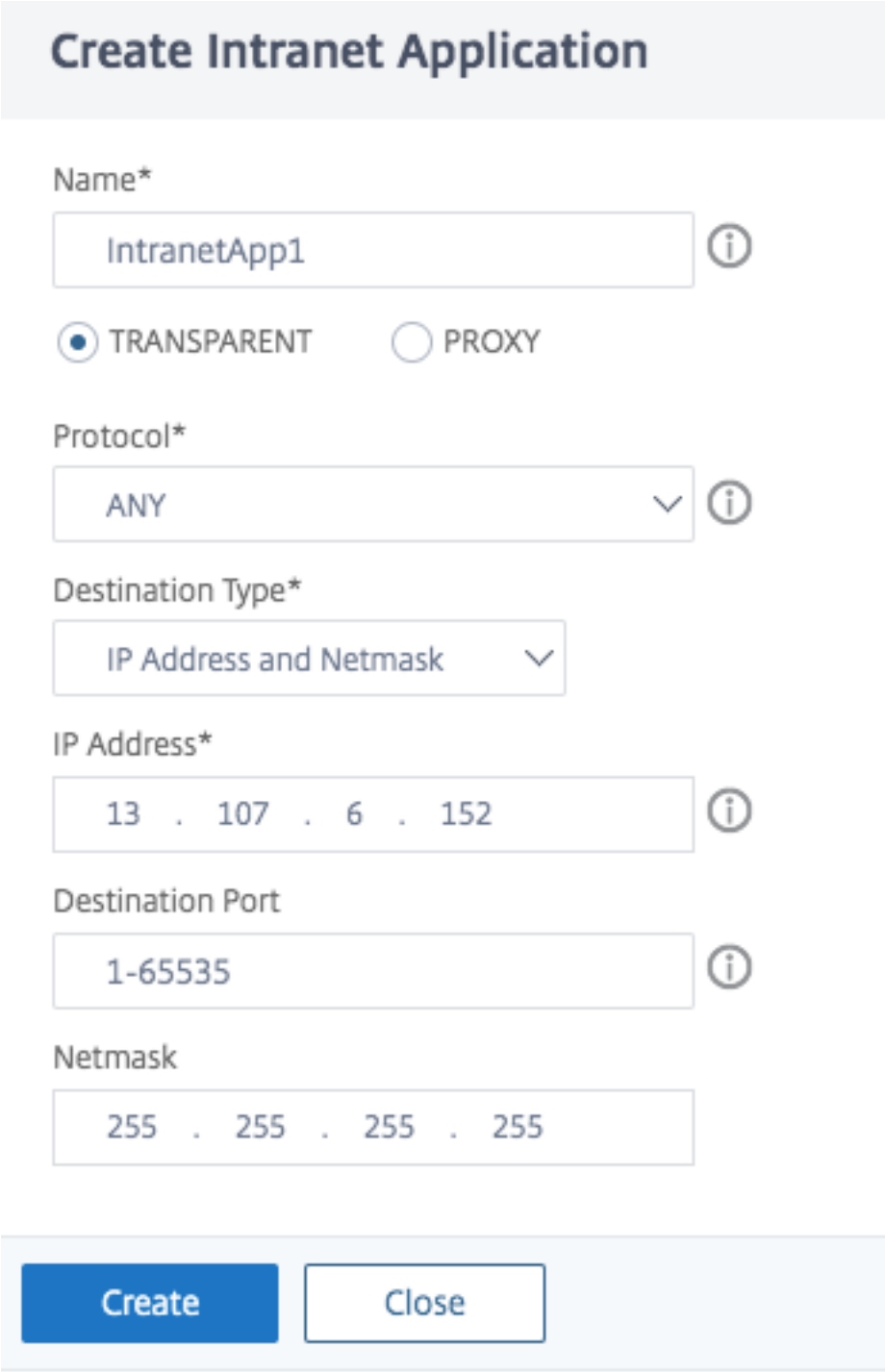
To create a VPN intranet application by using the GUI

1. On the Configuration tab, Navigate to C**itrix Gateway > Global Settings**.
2. In the details pane, under **Intranet Applications**, click the link.
3. In the **Configure VPN Intranet Application** page, click **Add**, and then click **New**.





4. In **Name**, type a name for the profile.
5. In **Protocol**, select the protocol that applies to the network resource.
6. In **Destination Type**, select **IP Address and Netmask**.
7. In **IP Address**, enter the IP address that must be routed directly to the internet for O365 traffic. For the list of IP address, see List of IP addresses.
8. In **Netmask**, enter the netmask IP address.



9. Click **Create** and then click **Close**.

Note: Repeat this procedure for all the IP addresses.

Configuration by using the CLI

- To set split tunnel to reverse, at the command prompt, type;

```
set vpn parameter -splitTunnel REVERSE
```

- To add VPN intranet application, at the command prompt, type;

```
add vpn intranetApplication intranetapp1 ANY 13.107.6.152 -netmask
    255.255.255.254 -destPort 1-65535 -interception TRANSPARENT
```

Note: Repeat this procedure for all the IP addresses.

- To bind the intranet application, at the command prompt type;

```
bind vpn global -intranetApplication intranetapp1
```

List of IP addresses of Office 365 services (EXO, SPO, and Microsoft Teams)

Reference: https://docs.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges

> **Note from Microsoft:**
>
> As part of Microsoft's response to the COVID-19 situation, Microsoft has declared a temporary moratorium on some planned URL and IP address changes. This moratorium is intended to provide customer IT teams with confidence and simplicity in implementing recommended network optimizations for work-from-home Office 365 scenarios. From March 24, 2020 through June 30, 2020 this moratorium will halt changes for key Office 365 services (Exchange Online, SharePoint Online, and Microsoft Teams) to IP ranges and URLs included in the Optimize category.

IPv4 address range

104.146.128.0/17
13.107.128.0/22
13.107.136.0/22
13.107.18.10/31
13.107.6.152/31
13.107.64.0/18
131.253.33.215/32
132.245.0.0/16
150.171.32.0/22
150.171.40.0/22
191.234.140.0/22

204.79.197.215/32
23.103.160.0/20
40.104.0.0/15
40.108.128.0/17
40.96.0.0/13
52.104.0.0/14
52.112.0.0/14
52.96.0.0/14
52.120.0.0/14|

IPv6 address range

2603:1006::/40
2603:1016::/36
2603:1026::/36
2603:1036::/36
2603:1046::/36
2603:1056::/36
2603:1096::/38
2603:1096:400::/40
2603:1096:600::/40
2603:1096:a00::/39
2603:1096:c00::/40
2603:10a6:200::/40
2603:10a6:400::/40
2603:10a6:600::/40
2603:10a6:800::/40
2603:10d6:200::/40
2620:1ec:4::152/128
2620:1ec:4::153/128
2620:1ec:c::10/128
2620:1ec:c::11/128
2620:1ec:d::10/128
2620:1ec:d::11/128
2620:1ec:8f0::/46
2620:1ec:900::/46
2620:1ec:a92::152/128
2620:1ec:a92::153/128
2a01:111:f400::/48

2620:1ec:8f8::/46
2620:1ec:908::/46
2a01:111:f402::/48

Type of Service Support for UDP traffic

January 8, 2024

Type of Service (ToS) support for UDP ensures that once a ToS value is configured for a UDP packet by a sender, NetScaler Gateway retains the value until the packet reaches its destination. On the basis of the configured value and the destination network's configuration, the destination network places the UDP packet in a prioritized outgoing queue.

> **Note:**
> Using ToS information, you can assign a precedence to each IP packet and request a specific treatment such as high throughput, high reliability, low latency, and so on.

Configuring Server Name Indication Extension

January 8, 2024

A NetScaler Gateway appliance can now be configured to include a server name indication (SNI) extension in the SSL "client hello"packet sent to the back end server. The SNI extension helps the back end server identify the FQDN being requested during the SSL handshake and respond with the respective certificates.

> **Note**
>
> Enable SNI support when multiple SSL domains are hosted on the same server.

To configure NetScaler Gateway to support SNI using GUI:

1. In the NetScaler GUI, navigate to **Configuration> NetScaler> Global Settings.**
2. Click the **Change Global Settings** link and from the **Backend Server SNI** menu, select **Enabled**.

To configure NetScaler Gateway to support SNI using the command line interface, at the command prompt, type:

```
set vpn parameter backendServerSni <ENABLED><DISABLED>
```


Validating the Server Certificate During an SSL Handshake

January 8, 2024

The NetScaler Gateway appliance can now be configured to validate the server certificate provided by the back-end server during an SSL handshake.

To configure NetScaler Gateway global parameters to support PAC for outbound proxy by using the configuration utility

Bind the CA certificate

1. Navigate to **Configuration** > **NetScaler Gateway** > **NetScaler Gateway Policy Manager** > **Certificate Bindings**.**
2. On the **Certificate Bindings** screen, click the **+** icon.
3. On the **CA Certificate(s) Binding** screen, click **Add Binding** and click **Install**.
4. Select the certificate file name in the **Certificate File Name** field and click **Install**.
5. On the **CA Certificate(s) Binding** screen, select the certificate and click **Bind**.
6. Click **Done**.

Enabling the certificate validation:

1. Navigate to **NetScaler Gateway> Global settings.**
2. Click **Change Global Settings**.**
3. Select **Enabled** from the **Backend Server Certificate Validation** drop-down menu and click **OK**.

To configure NetScaler Gateway global parameters to support server certificate with the command line

At the command prompt, type the following commands:

```
bind vpn global cacert DNPGCA1

set vpn parameter backendcertValidation ENABLED
```

Simplified SaaS app configuration using a template

January 8, 2024

SaaS apps configuration with single sign-on on NetScaler Gateway is simplified by provisioning a template drop-down menu for popular SaaS apps. The SaaS app to be configured can be selected from

the menu. The template pre-fills much of the information required for configuring applications. However, the information specific to the customer must still be provided.

> **Note:**
>
> To configure and publish SaaS apps, configure and publish on the NetScaler Gateway and then on the app server.
>
> The steps in the next section help you configure and publish apps on NetScaler Gateway using a template. Then move on to the section that explains how to configure and publish on the app server.

Configuring and publishing apps using template - NetScaler Gateway specific configuration

The following configuration uses the AWS Console app as an example for how to configure and publish an app using a template.

Before you start, you need the following:

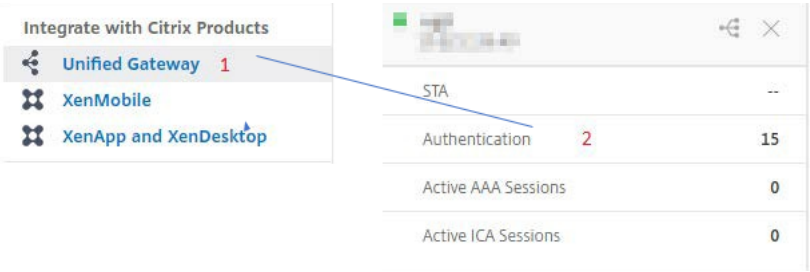
- An admin account for the AWS Console
- An admin account for NetScaler Gateway

The AWS Console configuration steps are as follows:

1. Configure the AWS Console with the App catalog.
2. Export AWS Console IdP metadata from NetScaler.
3. Configure IdP into AWS Console.

STEP 1: Configure AWS Console with App Catalog

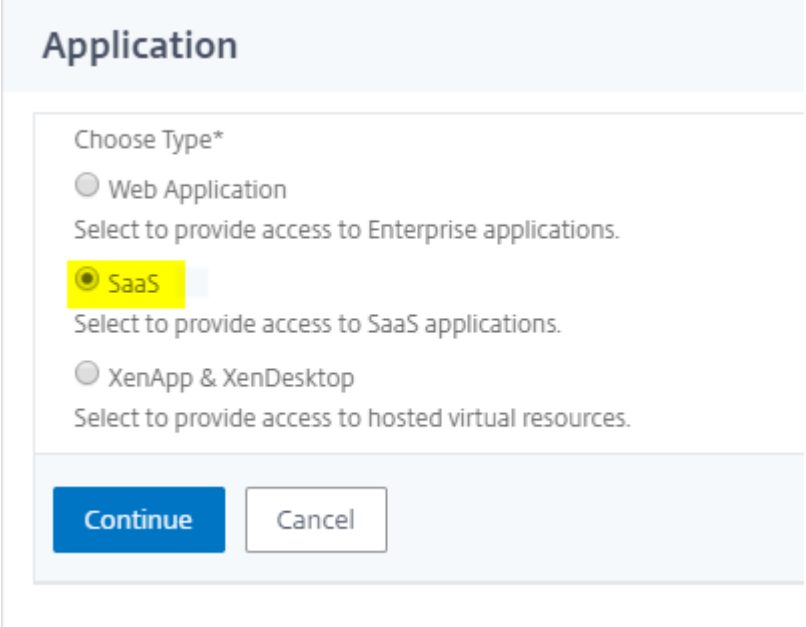
1. Click **Unified Gateway > Authentication**.



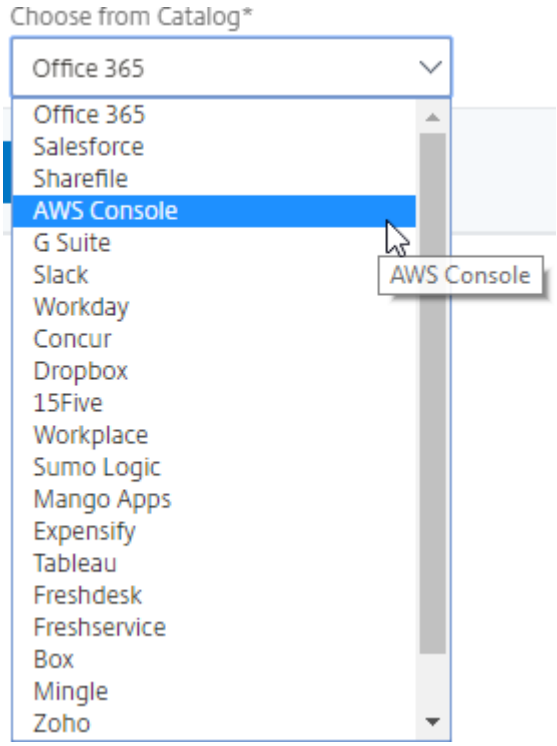
   The Unified Gateway Configuration screen appears.

2. On the **Applications** section, click the edit icon. Now, click the plus icon. The Application window appears.

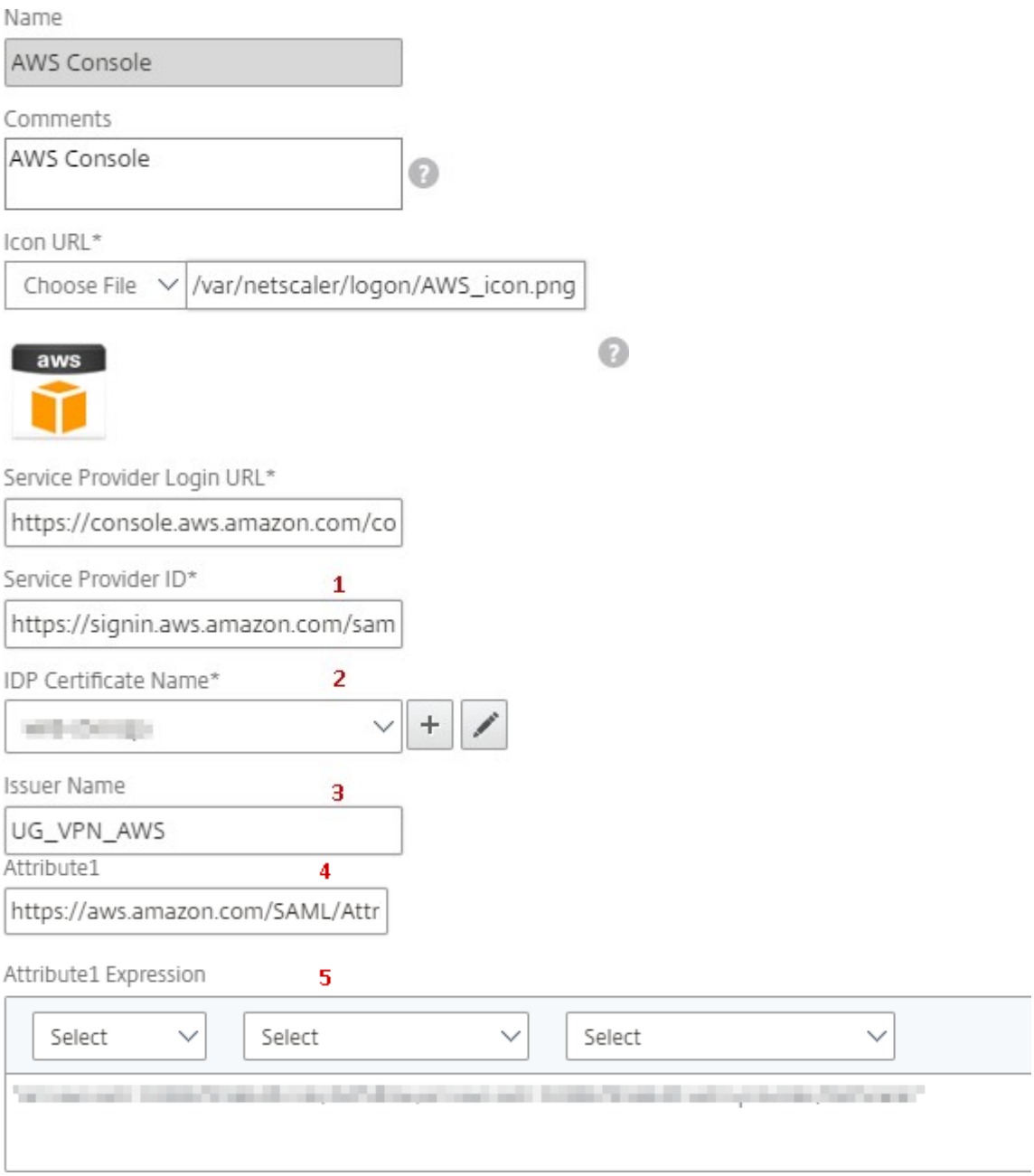
3. Select **SaaS** from the Application type.



4. Select **AWS Console** from the drop-down list.



5. Fill the application template with appropriate values.



6. Enter the following SAML configuration details and click **Continue**.

   Service Provider ID –https://signin.aws.amazon.com/saml

   Signing Certificate Name –IdP certificate must be selected

   Issuer Name –Issuer name can be filled as per your choice

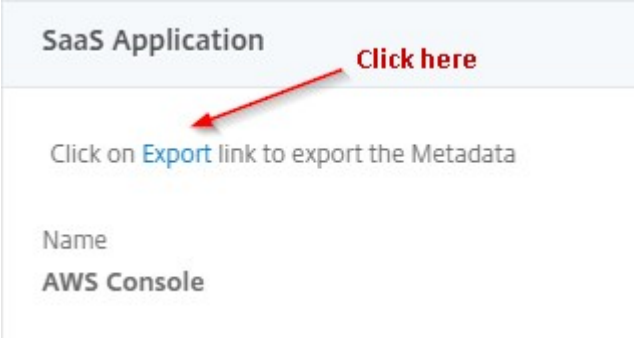
   Attribute1 –`https://aws.amazon.com/SAML/Attributes/Role`

   Attribute1 Expression – `Role ARN, IdP ARN`, as shown in step 3

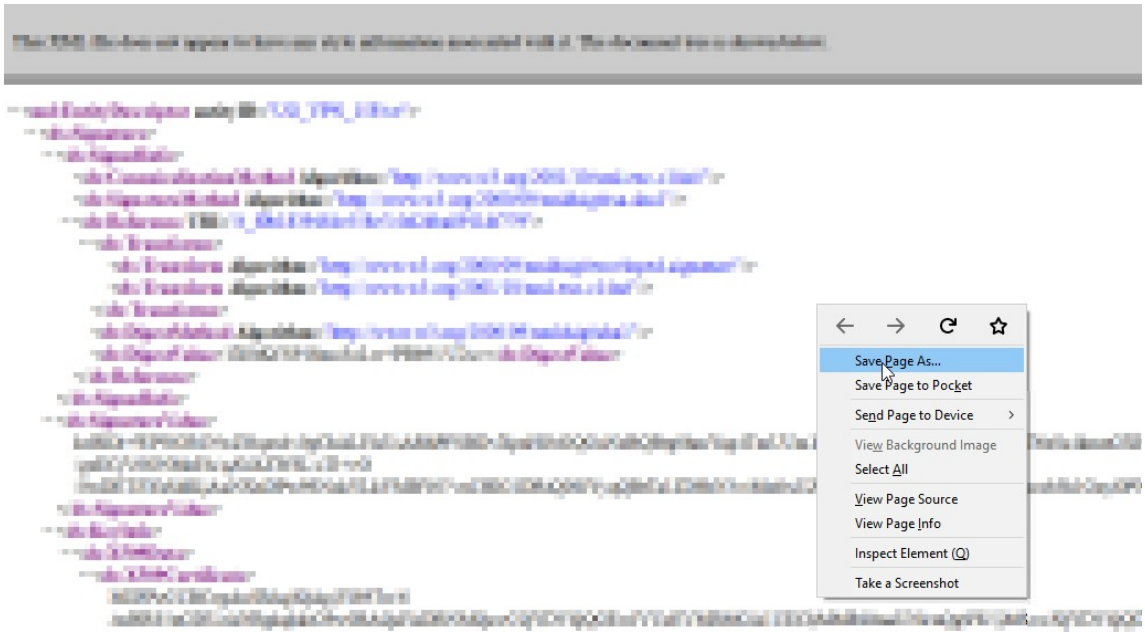
7. Click **Done**.

STEP 2: Export AWS Console IdP metadata from NetScaler Gateway.

1. Click **Unified Gateway > Authentication**.
2. Scroll down and click **AWS Console** template. The SaaS Application window appears. Click **Export** link.



3. **Metadata** opens in a different window. Save the **IdP Metadata** file



STEP 3: Configure IdP into AWS Console.

Configuring and publishing apps using template - App server specific configuration

The following links open PDF documents that provide specific guidance for configuring and publishing popular SaaS apps using templates.

- 15Five
- Absorb

- Accompa
- Adobe Captivate Prime
- Adobe Creative Cloud
- Aha
- AlertOps
- Allocadia
- Ariba
- Assembla
- AWS Console
- BambooHR
- Base CRM
- BitaBIZ
- BlueJeans
- Blissbook
- Bonusly
- Box
- Bugsnag
- Buildkite
- CakeHR
- Cardboard
- Cedexis
- Celoxis
- Cisco Meraki
- ClearSlide
- CloudCheckr
- ConceptShare
- Concur
- Confluence
- Contactzilla

- Convo
- Circonus
- Dashlane
- Datadog
- Deskpro
- Deputy
- DigiCert
- DocuSign
- Domo
- Dropbox
- Duo
- eFront
- Ekarda
- Envoy
- ERP
- Expensify
- EZOfficeInventory
- EZRentOut
- Favro
- Federated Directory
- Feedly
- Fivetran
- Flatter Files
- Flowdock
- Freshdesk
- Front
- G-Suite
- GitHub
- GlassFrog

- GotoMeeting
- HappyFox
- Helpjuice
- Help Scout
- Hoshinplan
- Humanity
- Igloo
- Illumio
- Image Relay
- iMeet Central
- InteractGo
- iQualify One
- Jira
- Kanban Tool
- Keeper Security
- Kentik
- Kentik
- Kissflow
- KnowBe4
- KnowledgeOwl
- Kudos
- LaunchDarkly
- Lifesize
- Litmos
- LiquidPlanner
- LogDNA
- Mango
- Manuscript
- Marketo

- Mingle
- Mixpanel
- MuleSoft
- MyWebTimesheets
- New Relic
- Nmbrs
- Nuclino
- Office365
- OneDesk
- OpsGenie
- Orginio
- PagerDuty
- Panorama9
- ParkMyCloud
- Peakon
- People HR
- Pingboard
- Pipedrive
- PlanMyLeave
- PlayVox
- Podio
- ProdPad
- Proto.io
- Proxyclick
- PurelyHR
- Quandora
- Rackspace
- RealtimeBoard
- Remedyforce

- Robin
- Rollbar
- Salesforce
- Samanage
- Samepage
- Sentry
- ServiceDesk Plus
- ServiceNow
- Shufflrr
- Skeddly
- Skills Base
- Slack
- Slemma
- Sli.do
- Smartsheet
- Spoke
- Spotinst
- SproutVideo
- StatusCast
- Status Hero
- StatusHub
- Statuspage
- Sumo Logic
- Supermood
- Syncplicity
- Tableau
- Targetprocess
- Teamphoria
- Testable

- TestFairy
- TextExpander
- TextMagic
- ThousandEyes
- Thycotic Secret server
- Tinfoil Security
- Trisotech
- Trumba
- TwentyThree
- UniFi
- UserEcho
- UserVoice
- Velpic
- VictorOps
- VIDIZMO
- Visual Paradigm
- Weekdone
- Wepow
- When I Work
- Workday
- Workpath
- Workplace
- Workstars
- Workteam
- XaitPorter
- Ximble
- XMatters
- Yodeck
- Zendesk

- ZIVVER
- Zoho One
- ZIVVER
- Zoom